PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

Modelo ProLab: PYMESHIELD, propuesta de modelo de negocio sostenible de ciberseguridad para Pymes

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRA EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS

QUE PRESENTA:

Diana Gisela, Mateus Villamil, CE 001818463

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS

QUE PRESENTA:

Guillermo Enrique, Cigaran Ricaldi, 43933141

Brandon Paul, Rodríguez González, 72294434

ASESOR

Sandro Alberto, Sánchez Paredes

Surco, octubre, 2024

Declaración Jurada de Autenticidad

Yo, Sandro Alberto Sánchez Paredes, docente del Departamento Académico de Posgrado en Negocios de la Pontificia Universidad Católica del Perú, asesor de la tesis titulada Modelo Prolab: PYMESHIELD, propuesta de modelo de negocio sostenible de ciberseguridad para Pymes de los(as) autores(as)

- Guillermo Enrique Cigaran Ricaldi
- Brandon Paul Rodríguez González
- Diana Gisela Mateus Villamil

Dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 19%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 11/10/2024.
- He revisado con detalle dicho reporte y confirmó que cada una de las coincidencias detectadas no constituyen plagio alguno.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 11 de octubre de 2024

Sánchez Paredes, Sandro Alberto	
DNI: 09542193	Firma 
ORCID: 0000-0002-6155-8556	

Agradecimientos

Agradecimiento a todas las personas que han sido parte fundamental en este camino hacia la culminación de mi MBA. Sin su apoyo, comprensión y amor, no habría sido posible alcanzar este objetivo. Agradezco especialmente a Dios por ser mi pilar, a mi amado esposo por toda su paciencia y apoyo, a mi madre, hermana y sobrina por toda su comprensión y ánimo para seguir adelante, y a Patricia por su constante apoyo y aliento.

Diana Mateus Villamil

Agradecer a todas las personas que han formado parte de este largo camino del MBA. Sin en el empuje y motivación no habría sido posible lograrlo, quiero agradecer a mi familia, esposa e hija que siempre han estado motivándome a continuar en este gran desafío.

Guillermo Cigaran Ricaldi

Agradezco a Dios y a mi familia, por permitieron llegar hasta estas instancias. Sin su apoyo no hubiera logrado todo lo que me estoy proponiendo.

Brandon Paul Rodríguez González

Dedicatorias

Dedico principalmente la culminación del MBA a Dios, por ser mi guía y mi fuente de fortaleza en todo momento. Agradezco todas las bendiciones que ha derramado sobre mi vida y la de mi familia.

A mi mamita, hermana y mi amada sobrina por haberme apoyado en todo momento y por los momentos de ausencia que han sabido comprender, las amo.

A mi esposo por su aliento constante para no desfallecer y por ser mi compañero de vida en este camino, lo amo.

Diana Mateus Villamil

Dedico este trabajo a mi familia, quienes siempre han sido mi inspiración constante. A mi esposa e hija por su comprensión y paciencia durante el MBA.

A mis padres por siempre tener una fe inquebrantable sobre mí.

Guillermo Cigaran Ricaldi

Dedico este logro principalmente a mis padres que me brindaron las herramientas para mi futuro, siendo el sostén de mi vida profesional. A mis hermanos que me acompañaron en este proyecto de vida y a mis sobrinos que son el motor e inspiración para ser mejor cada día. Son mi motivación.

Brandon Paul Rodríguez González

Resumen Ejecutivo

El mundo viene en un constante cambio y evolución digital, esta evolución ha traído consigo el uso de tecnologías emergentes, una mayor exposición en internet y la interacción de las empresas en redes sociales con sus clientes, lo que conlleva a un incremento en la probabilidad de sufrir un ataque cibernético.

El presente estudio tiene como objetivo resaltar la importancia asociada a la implementación de servicios diseñados para minimizar el nivel de exposición de los riesgos cibernéticos en las compañías PYMES. En un ecosistema con un incremento constante de amenazas, es crucial que las empresas incorporen estrategias de ciberseguridad que les permitan proteger sus activos críticos.

En conclusión, los análisis financieros realizados en el marco de esta investigación confirman la viabilidad del proyecto. PYMESHIELD está muy bien posicionada para ingresar en el mercado de las PYMES peruanas, desempeñando un papel crucial en el fortalecimiento de la economía del país. Dado que las PYMES representan más del 90% de la economía peruana, proteger sus activos tecnológicos es esencial para asegurar su continuidad operativa. Este proyecto demuestra sostenibilidad, respaldado por su contribución a los Objetivos de Desarrollo Sostenible (ODS) 9 y 16.

Abstract

The world is experiencing constant change and a digital evolution, which has brought with it the advent of emerging technologies, increased exposure on the internet, and the interaction of companies with their customers on social media. This leads to a higher probability of experiencing a cyber-attack.

This study aims to highlight the critical importance of implementing services designed to minimize the exposure level to cybersecurity risks in small and medium-sized enterprises (SMEs). In an ecosystem with a steadily increasing number of threats, it is crucial for companies to incorporate cybersecurity strategies that enable them to protect their critical assets.

In conclusion, the financial analyses carried out within the framework of this research confirm the viability of the project. PYMESHIELD is very well positioned to enter the Peruvian SME market, playing a crucial role in strengthening the country's economy. With SMEs accounting for more than 90% of the Peruvian economy, protecting their technology assets is essential to ensure their operational continuity. This project proves to be sustainable, supported by its contribution to Sustainable Development Goals (SDGs) 9 and 16. In conclusion, the financial analyses carried out within the framework of this research confirm the viability of the project. PYMESHIELD is very well positioned to enter the Peruvian SME market, playing a crucial role in strengthening the country's economy. With SMEs accounting for more than 90% of the Peruvian economy, protecting their technology assets is essential to ensure their operational continuity. This project proves to be sustainable, supported by its contribution to Sustainable Development Goals (SDGs) 9 and 16.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Capítulo I: Definición del problema

El presente capítulo expone la importancia de resolver los ciberataques a las pequeñas y medianas empresas con presencia de venta online. Un alto porcentaje de PYMES poseen plataformas con problemas de uso y medios de venta con déficit de seguridad informática, por lo que son víctimas de ataques por estos canales.

1.1. Contexto del problema a resolver

Las empresas están en constante evolución, ajustándose a las realidades cambiantes del mercado y adaptándose de manera natural a las nuevas necesidades. Sin embargo, en situaciones extraordinarias, como la crisis sanitaria del COVID-19, estos cambios ocurren de manera abrupta. Las PYMES (pequeñas y medianas empresas), que representan el 99.5% de la estructura empresarial en el Perú, sufrieron una reducción del 75% durante esta crisis (Produce, 2023).

A pesar de esta disminución, las empresas de venta presencial y virtual continuaron operando, y el comercio electrónico alcanzó un movimiento de 9,300 millones de dólares en 2021. Esto representa un crecimiento del 55% en comparación con el año 2020 (Gestión, 2022). En otras palabras, la crisis impulsó un cambio que algunas PYMES aprovecharon, utilizando exclusivamente canales digitales para mantener o incrementar sus ventas. La transformación digital se convirtió en una necesidad imperiosa.

Sin embargo, pocas empresas alcanzaron el nivel de madurez digital requerido por el mercado. Este concepto se define como una combinación de ajustes en estrategias, modelos de negocio, organización de procesos y cultura empresarial a través de la implementación de tecnologías digitales (Lahrmann, Mettler y Wortmann, 2011). Solo entre el 51% y el 59% de las PYMES alcanzaron un índice de madurez digital, lo que indica que la mayoría aún se encuentra en un nivel intermedio.

Figura 1

Índice de madurez digital según tamaño de empresa

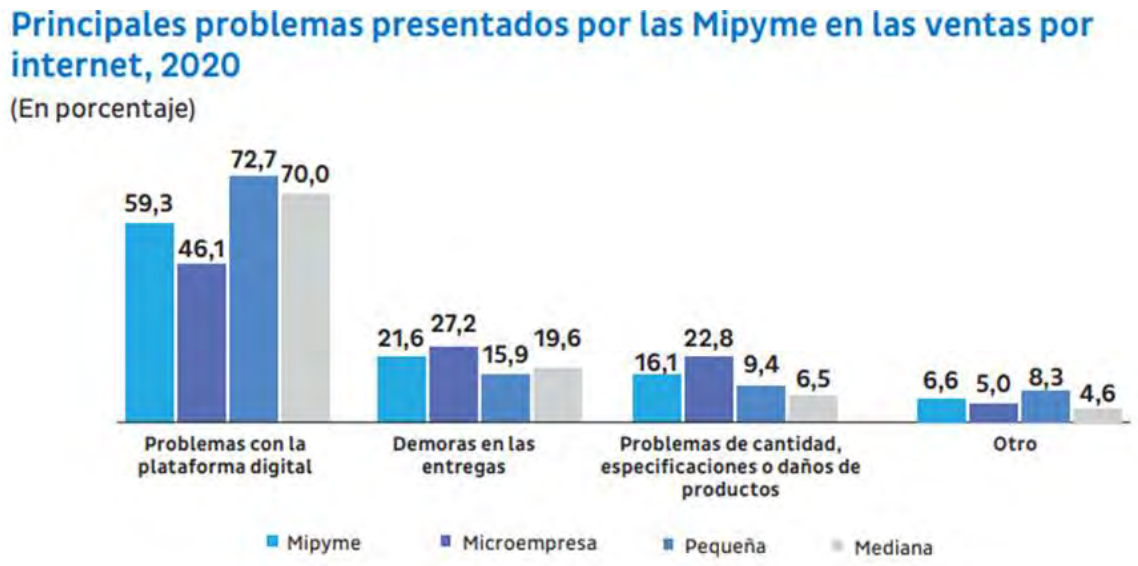
Nota. Adaptado de *Madurez digital en las empresas peruanas (p. 84)*, por Ministerio de la Producción (2023)

Este contexto explica las dificultades que las PYMES han enfrentado en sus ventas por internet. Al ser un canal relativamente nuevo para muchas de ellas, la digitalización de sus negocios ha presentado varios desafíos. Las PYMES han sido particularmente afectadas, con problemas en sus plataformas digitales, lo que ha incrementado el riesgo de vulneración de información, afectando negativamente a sus clientes.

En la Figura 2, se presentan los principales problemas que enfrentaron las MIPYMES en las ventas por internet en 2020. Como se puede observar, los problemas más comunes incluyen dificultades con la plataforma digital y demoras en las entregas, lo que refleja un claro desafío tecnológico para este sector. Un canal de ventas con deficiencias tecnológicas, además de ser vulnerable a la pérdida de información confidencial de los clientes, no solo perjudica las ventas de las empresas, sino que también impacta negativamente en su reputación institucional.

Figura 2

Índice de los Principales Problemas de las Mipyme en las Ventas por Internet en el Año 2020



Nota. Adaptado de Las Mipyme en cifras 2021(p. 108), por Ministerio de la Producción, 2022, Produce

Por otro lado, la formalidad en las operaciones de las PYMES no se da completamente. Un alto porcentaje de empresas en el Perú no utiliza software con licencia, lo que representa un riesgo considerable para la seguridad de la información interna. De hecho, el 63% de las empresas usa aplicaciones ilegales en todas sus áreas, desde directores hasta empleados de primera línea, quienes han afirmado instalar estos programas sin licencia (El Peruano, 2017). Esta práctica incrementa la vulnerabilidad de las empresas, especialmente en un contexto donde las ventas online de las PYMES han crecido un 52% en el año 2023.

A nivel de Hyspamérica, el 90% de las empresas considera que la digitalización es fundamental para su desarrollo (Telefónica, 2024). Sin embargo, muchas pequeñas y

medianas empresas no cuentan con las protecciones adecuadas contra ataques cibernéticos, lo que las expone a importantes riesgos. La falta de protección no solo compromete la seguridad de sus operaciones, sino también la reputación de las empresas ante sus clientes y socios.

1.2. Presentación del problema a resolver

La principal problemática identificada es la vulnerabilidad de las micro y pequeñas empresas en el Perú frente a los ataques cibernéticos. La implementación de nuevos canales de venta, como las plataformas web o las aplicaciones de registro de información, ha generado retos adicionales para los empresarios. Según la Gerente General de Microsoft Perú, en un artículo para El Peruano, los principales desafíos a los que se enfrentan las PYMES peruanas son la ciberseguridad (40%), el volumen de ventas (34%) y la productividad/eficiencia del negocio (34%) (El Peruano, 2023).

A nivel mundial, la ciberseguridad es también un desafío crucial. De acuerdo con el World Economic Forum, los riesgos cibernéticos estarán en el TOP 10 de amenazas globales durante los próximos 10 años. Esto resalta la necesidad urgente de que las PYMES adopten medidas preventivas y refuercen su seguridad digital para enfrentar estos riesgos.

Figura 3

Riesgos Globales Clasificados por Gravedad a Corto y Largo Plazo a Partir del 2024

Nota. Adaptado de *The Global Risks Report 2024 19th Edition (p. 8),* por World Economic Forum (2024)

A nivel regional, Perú es el cuarto país con más ciberataques por minuto (107), solo superado por Brasil, México y Colombia (Forbes, 2023). Desde 2022, cinco de cada diez PYMES peruanas han sufrido ciberataques, muchos de ellos ocurridos en los primeros años de constitución de las empresas (Gestión, 2022). En 2023, Kaspersky registró un total de 9.6 millones de ataques contra este tipo de empresas, lo que equivale a un promedio de 26,487 ataques diarios, o 18 ataques por minuto (Quispe, 2023).

Dentro de estos ataques se incluyen robos de información bancaria, hurto de identidad e información privada, lo que genera pérdidas económicas considerables. Según Alberto Gómez, Gerente de Operaciones de Seguridad y Ciberseguridad de CANVIA, el éxito de una empresa depende en gran medida de su madurez en ciberseguridad. La falta de protocolos adecuados puede derivar en pérdidas que van desde 13,000 hasta más de 5 millones de dólares por ataque (Gómez, 2023). Además, de acuerdo con Kaspersky, las PYMES pueden experimentar pérdidas económicas y de reputación de hasta 155,000 dólares tras un ciberataque (Pichihua, 2022). Por ello, es crucial identificar y gestionar las

vulnerabilidades tecnológicas para prevenir ataques que podrían provocar daños económicos y reputacionales, así como multas regulatorias.

1.3. Sustento de la complejidad y relevancia del problema a resolver

La vulnerabilidad de las pequeñas y medianas empresas (PYMES) frente a los ciberataques es alarmante, con 9.6 millones de intentos registrados en 2023, lo que constituye una señal crítica a nivel empresarial. Según Kaspersky (2021), es imprescindible que las PYMES adopten medidas concretas para mitigar estos riesgos. Estas organizaciones son particularmente vulnerables debido a la gestión inadecuada del flujo de información, exacerbada por el uso inapropiado de dispositivos móviles por parte de sus empleados.

Además de las pérdidas económicas, los ciberataques implican riesgos significativos como el deterioro de la reputación y la interrupción de las operaciones (Kaspersky, 2021). En España, un ciberataque cuesta a una PYME un promedio de 35,000 euros, y el 60% de las empresas afectadas cesan sus actividades dentro de los seis meses posteriores al incidente (Google, 2023). Aunque estos datos provienen de un contexto con mayor madurez tecnológica que el de Perú, sirven como una referencia crítica para entender el impacto potencial que estos ataques podrían tener en las PYMES peruanas.

1.4. Resumen del capitulo

En este capítulo, se ha evidenciado el impacto global de los ataques informáticos, que figuran en el top 10 del *World Economic Forum* por los próximos 10 años. Además, se ha resaltado el enfoque de los atacantes en países en desarrollo como Perú y los posibles impactos económicos en las PYMES. Esto subraya que la ciberseguridad es una problemática real y significativa para este tipo de empresas.

Capítulo II: Análisis de mercado

En este capítulo se analizará la vulnerabilidad de las PYMES frente a ciberataques y las soluciones disponibles. Se examina cómo la falta de conciencia sobre seguridad digital ha aumentado los riesgos en los últimos diez años. Además, se revisarán las principales medidas de defensa y los servicios más recomendados para mitigar estos ataques.

2.1. Descripción del mercado o industria

Según el Instituto Nacional de Estadística e Informática (INEI), en 2022 el Perú contaba con 3.1 millones de empresas. De ellas, las microempresas representaban el 88.9%, las pequeñas el 9.4%, las medianas el 0.4% y las grandes empresas solo el 1.3%. Las pequeñas y medianas empresas ocupan el tercer y cuarto nivel en términos de aporte al producto bruto interno. No obstante, cinco de cada diez PYMES han sido víctimas de ciberataques, y el 15.4% de ellas sufrieron pérdidas financieras como consecuencia (El Peruano, 2024).

El mercado de la ciberseguridad, altamente dinámico, ha experimentado un crecimiento sostenido debido al aumento exponencial de las amenazas digitales. Esta evolución ha consolidado a la ciberseguridad como un sector clave. Entre 2012 y 2021, la tendencia a no actualizar sistemas operativos y aplicaciones contribuyó a que el porcentaje de detección de ciberataques fuera un 8% más elevado a nivel mundial (Solar, 2024). En respuesta a estas amenazas, los gobiernos han implementado regulaciones más estrictas, buscando proteger los activos críticos tanto de organizaciones como de países. Estas medidas han impulsado la adopción de controles que reducen la probabilidad de incidentes cibernéticos. Ejemplos de estas regulaciones incluyen el GDPR en Europa, la Ley de

Protección de Datos Personales en Perú y Colombia, y el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

En el contexto de Latinoamérica, las PYMES también han mostrado preocupación por los riesgos cibernéticos. Según el "Primer Estudio de Riesgos para Empresas Nacionales y Familiares Latinoamericanas 2023-2024" (McLennan, 2023), el 45% de las PYMES latinoamericanas señalaron que la ciberseguridad es una de sus principales preocupaciones. En 2022, el 10.5% de sus prioridades de inversión se centraron en la gestión de riesgos vinculados a la ciberseguridad, seguridad de la información y tecnologías.

En los últimos 3 años postpandemia, las PYMES han generado cambios donde el 60% adquirió sistemas de seguridad. Respecto a la inversión presupuestaria dedicada a las capacidades de tecnología, las empresas invierten en promedio un 25% en temas de ciberseguridad. De este modo y desde el año 2020, las compañías se centraron en:

- 89% de las PYMES crearon nuevas reglas de acceso a la información.
- 85% asegura que la ciberseguridad es una prioridad en su empresa.
- 83% reporta tener políticas de ciberseguridad en su empresa.
- 78% de los líderes se preocupa y habla de ciberseguridad.

Es importante establecer la existencia de marcos de referencia que las empresas adoptan para poder gestionar sus ciber riesgos y en éste sentido uno de los principales es el Cybersecurity Framework del NIST (NIST, 2023) basado en 5 funciones principales:

- Identificar: Establecer los principales activos de la organización a fin de identificar los activos más valiosos a ser cuidados.

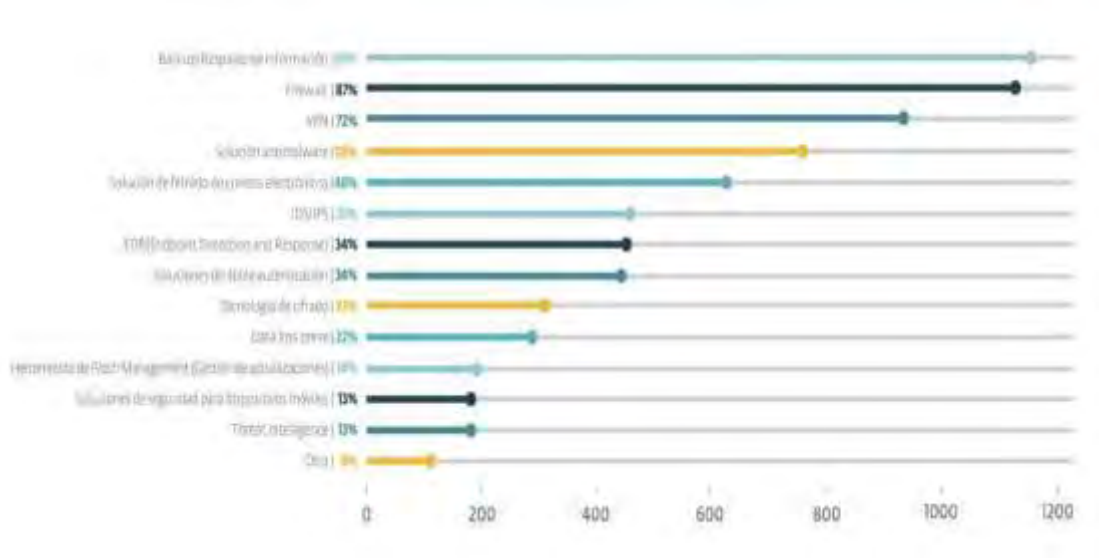
- Proteger: Activar y desarrollar controles que permitan cuidar los activos de información identificados como críticos para una compañía.
- Detectar: Capacidad de conocer potenciales eventos maliciosos que pudieran generar algún impacto a la compañía y de forma proactiva tomar acción.
- Responder: Acción de actuar ante un incidente de ciberseguridad organizando las capacidades para lograr contener y erradicar una amenaza de ciberseguridad en progreso.
- Recuperar: Volver a la normalidad en el menor tiempo posible, luego de que una amenaza de ciberseguridad se haya materializado y generado potenciales impactos.

Actualmente, las compañías emplean este tipo de frameworks para evaluar el nivel de madurez de sus procesos y capacidades en ciberseguridad. Esto les permite tomar decisiones estratégicas y definir su plan director o estrategia de ciberseguridad a corto, mediano y largo plazo. En este contexto, diferentes fabricantes han desarrollado herramientas y soluciones tecnológicas para apoyar las diversas funciones del Cybersecurity Framework del NIST. Estas soluciones facilitan la gestión de riesgos, optimizan la operación y permiten a las empresas anticiparse a las amenazas cibernéticas.

Entre las tecnologías más implementadas por las empresas en América Latina durante 2022 se incluyen soluciones avanzadas para la protección de la información, detección de amenazas y respuesta a incidentes (ESET, 2023). Estas tecnologías, que se describen en la Figura 4, permiten a las compañías fortalecer su seguridad cibernética y responder de manera más efectiva ante posibles ataques.

Figura 4

Tecnologías implementadas en América Latina en el 2022 – ESET



Nota. Adaptado de Security Report Latinoamérica 2023(p. 13), por ESET (2023).

En el mercado, las soluciones de ciberseguridad van desde herramientas básicas de protección como antivirus, firewalls, Data Loss Prevention, hasta tecnologías avanzadas que usan inteligencia artificial y aprendizaje automático para detener y responder a las amenazas. También evidenciamos que las compañías están adoptando soluciones de seguridad gestionada, lo que les permite tercerizar parte de la operación de ciberseguridad.

2.2. Análisis competitivo detallado

En nuestro análisis, hemos identificado a los principales competidores potenciales mediante una búsqueda de los servicios que se deben de realizar para satisfacer el mercado de PYMES con ataques cibernéticos. Todo esto adaptado a las necesidades específicas de cada empresa. Estos servicios son únicos en el mercado peruano porque nos permite

adaptar nuestro servicio a las necesidades de cada PYME y están respaldados por un equipo de expertos en seguridad de la información y ciberseguridad.

- **Securesoft:** Es una compañía, con más de 19 años de experiencia en el mercado de la ciberseguridad. Cuentan con servicios especializados y soluciones de ciberseguridad, utilizan las mejores tecnologías de vanguardia para ofrecer sus servicios. Esta compañía ofrece servicios en Colombia, Chile y Perú. Este proveedor ofrece soluciones para el análisis de vulnerabilidades en infraestructura, componentes de red y aplicaciones, sin embargo, las PYMES no tienen el presupuesto suficiente para adquirir este tipo de herramientas, dedicar recursos para la identificación, análisis de impacto hasta finalmente su remediación. Por lo que consideramos que este no es un servicio que pueda competir directamente con el nuestro.
- **Neosecure**: Es una compañía que ofrece un portafolio de soluciones, servicios y consultoría soportados en las mejores tecnologías, sumado a esto cuentan con un equipo de profesionales expertos en ciberseguridad. Este proveedor tiene un servicio llamado Risk Monitor, el cual compite parcialmente con nuestro servicio de inteligencia de amenazas, ya que este proveedor solo se encarga de identificar amenazas relevantes para los clientes, luego informan a los clientes para que realicen la investigación con mayor profundidad y mitigación.
- **ETEK:** Esta empresa de servicios de ciberseguridad gestionados, líder en su campo, ofrece soluciones de seguridad de la información que combinan la experiencia humana con la automatización para garantizar la protección de los sistemas de sus clientes. Uno de sus servicios clave es la Gestión Proactiva de Amenazas, que se

basa en realizar ejercicios de ingeniería social y pruebas de penetración para evaluar el comportamiento y las respuestas de los usuarios en escenarios reales. Este servicio tiene un enfoque diferente al nuestro, ya que su propósito principal es generar conciencia sobre la ciberseguridad entre los empleados de sus clientes y evaluar la vulnerabilidad de las redes de la compañía, buscando posibles puntos de ingreso para fortalecerlas.

Como parte del análisis de competidores, se obtuvieron cotizaciones de dos proveedores, lo que permitió identificar que nuestros costos para el servicio de inteligencia de amenazas estaban significativamente por debajo de los de ellos. Sin embargo, esta información no puede ser presentada debido a que las cotizaciones incluyen una cláusula de confidencialidad.

2.3. Resumen del capitulo

En conclusión, hemos identificado competencia con presencia en internet, pero destacamos la falta de un servicio que combine de manera integral y personalizada la inteligencia de amenazas, el monitoreo de marca, la identificación de activos críticos para las PYMES y que se complementa con capacitación para la primera línea de defensa. Además, el servicio de remediación de vulnerabilidades, actualmente no está disponible en el mercado.

Capítulo III: Investigación del usuario (cliente)

En el presente capítulo describiremos al usuario final, por lo cual debemos definir nuestro perfil de usuario, mapa de experiencia y la identificación de la necesidad. La recolección de información se realizó mediante entrevistas con la finalidad de definir en un principio el perfil de usuario y en segunda instancia, reforzar la necesidad de resolver el problema social relevante.

3.1. Perfil del usuario

Para resolver potencialmente el problema social relevante encontrado, realizamos encuestas con el objetivo de conocer mejor a los empresarios dueños de algunas de las PYMES en el entorno peruano. De esta forma se aplicaron 20 entrevistas con 18 preguntas (Anexo A). Dentro de las respuestas más relevantes encontramos lo siguiente:

- El 90% de los encuestados se encuentra en un rango de edad entre los 20 a 65 años.
- La población encuestada se compone de un 60% de hombres y un 40% de mujeres. Además, respecto al estado civil de los consultados, un 65% son casados, 30% son solteros y 5% viudos.
- El 70% tiene una formación educativa universitaria o superior, el 20% tiene una formación técnica y el 10% no tiene una formación educativa mayor a la de secundaria completa.
- Los encuestados indican que dentro de sus pasatiempos más comunes se encuentran, el de pasar tiempo con la familia, realizar actividades deportivas, organizar actividades para sus empleados, buscar información sobre las condiciones de su mercado y viajes de relacionamiento.

- Nombran dentro de sus mayores motivadores el de mejorar la calidad de vida de su familia, hacer crecer a su empresa y a sus colaboradores.
- El 35% de las respuestas emitidas por los empresarios indican que su mayor preocupación es la continuidad de su negocio, el 30% indica qué les preocupa adaptarse a los cambios del mercado, el 20% indica que le preocupa innovar en nuevas tecnologías y el 15% indica que le preocupa la sostenibilidad de la empresa.
- El 55% de encuestados consideró que la característica que más los identifica es la resiliencia, seguido por el 20% quienes se consideran a sí mismos como personas de familia, luego un 10% mantienen un estilo conservador, otro 10% se considera intuitivo y un 5% se describe como audaz.
- Los encuestados asociados a los rubros de negocio de consultoría empresarial y servicios de alimentación, representan un 35% cada uno, siendo los dos rubros una agrupación del 70%, los demás encuestados hacen parte del sector de comercio minorista con un 25% y salud y bienestar con un 5%.
- Identificamos que el 40% de las empresas tienen entre los 9 y 10 años en el mercado.
- Se identificó que el 70% de las personas encuestadas realizan en sus empresas las ventas a través de canales digitales como páginas web, WhatsApp y redes sociales en más del 50%. Por otro lado, el 30% de las empresas realiza menos del 50% de la venta de sus productos y/o servicios a través de canales digitales.
- El 90% de empresarios encuestados indica que el número de sus trabajadores se encuentra entre 51 y 100 colaboradores.

- El 65% de las personas encuestadas afirma contar con entre 11 y 30 computadoras que son empleadas por los colaboradores de sus empresas. Un 20% indica contar con entre 6 y 10 computadoras, mientras que el 10% cuenta con entre 1 y 5 computadoras, y solo un 5% cuenta con más de 30 computadoras para sus colaboradores.
- El 80% de los encuestados fueron víctimas de ataques cibernéticos o experimentaron intentos de ataque cibernéticos hacia sus empresas en los últimos 5 años. Entre los ataques más destacados se encuentran aquellos dirigidos a la plataforma web y casos de suplantación de identidad.
- El 35% de las respuestas a la encuesta indica que la alternativa que podría materializarse como la de mayor impacto para la compañía en caso de un ciberataque es económica. El 30% de las respuestas considera que el mayor impacto sería reputacional, un 25% opina que el mayor impacto estaría dirigido a la continuidad del negocio y un 10% a la vulnerabilidad de la información.
- El 50% de las personas encuestadas indica que el mayor punto de vulnerabilidad de sus empresas, y que las hace susceptibles a un ciberataque, son las computadoras de la compañía, seguido por los correos corporativos en un 35%. Otros activos potencialmente vulnerables serían los servidores con un 10% y los dispositivos móviles de los empleados en un 5%.

Con los resultados de las entrevistas logramos identificar las principales características del usuario final. Como consecuencia de esto, en la Figura 5 podemos observar el lienzo Meta de Usuario.

Figura 5

Perfil del Usuario

BIOGRAFIA:	CIRCULO SOCIAL:
• Hombre Adulto • Edad: 40 años. • Casado sin hijos. • Reside en Lima. • Empresario dueño de una consultoria.	• Familia. • Colaboradores. • Empresarios de la localidad. • Competidores.
ACTIVIDADES:	**CARACTERISTICAS:**
• Realiza deporte los fines de semana. • Organiza actividades fuera del trabajo para sus colaboradores. • Sale a pasear con su pareja. • Investiga sobre las condiciones de su mercado.	• Resilente. • Liderazgo. • Se considera una persona con fuerte etica. • Precavido.

MOTIVADORES U OBJETIVOS :	MAYORES PREOCUPACIONES:
• Mejor la calidad de vida de la Familia. • La empleabilidad de sus trabajadores y su contuinidad. • Liderar su mercado.	• La continuidad de sus operaciones. • La viabilidad de su negocio. • La reputacion de su empresa.

3.2. Mapa de experiencia de usuario

En el primer movimiento, se evidenció que los usuarios están interesados en la creación de productos innovadores, lo que les genera una sensación de satisfacción. Esto se debe a que la innovación les otorga un propósito y los desafía. Cuando los usuarios trabajan en proyectos innovadores, se sienten motivados y comprometidos. En el segundo movimiento, se identificó que los usuarios captan las necesidades y la información de sus clientes para ofrecer productos adecuados, lo que asegura la continuidad de su negocio. Esto les permite adaptarse a los cambios del mercado, manteniendo la sostenibilidad de su empresa a largo plazo.

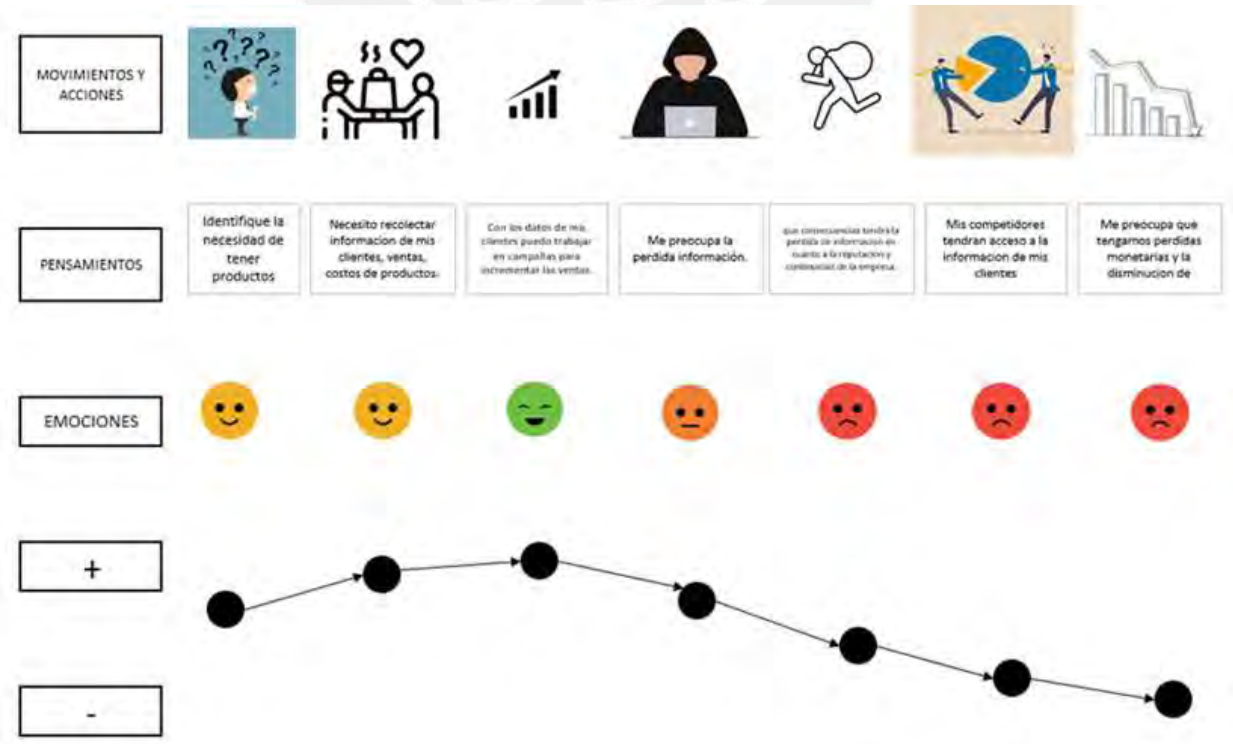
El tercer movimiento también generó satisfacción entre los usuarios, ya que los datos recopilados les permiten tomar decisiones más acertadas, como la personalización de campañas mediante correos electrónicos simulados. Estos correos electrónicos, con

apariencia de maliciosos, se envían a los colaboradores como parte de su entrenamiento en ciberseguridad. Sin embargo, una de las principales preocupaciones que surgió es la posibilidad de un ataque cibernético que afecte las operaciones de la empresa, provocando la pérdida de información clave, como datos financieros y de clientes.

Otra preocupación relevante está relacionada con el posible daño reputacional derivado de la pérdida de información, lo que genera desconfianza entre clientes, inversores y empleados. Finalmente, la última preocupación es la pérdida de clientes, ya que un daño reputacional puede hacer que los consumidores dejen de adquirir los productos debido a la falta de confianza en la empresa. Como se muestra en la Figura 6, los mapas de experiencia son herramientas valiosas que permiten comprender las emociones de los clientes a lo largo de su interacción con un producto o servicio. Identificar estas emociones nos ayuda a entender mejor sus necesidades y preocupaciones, lo que nos permite orientar el servicio para satisfacerlas de manera más efectiva.

Figura 6

Mapa de Experiencia Usuario



3.3. Identificación de la necesidad

La información que manejan los usuarios se almacena en diversos equipos como Data Centers, servicios en la nube contratados, dispositivos extraíbles y de almacenamiento local, entre otros. Al no estar protegidos de manera adecuada, estos sistemas corren el riesgo de ser vulnerados, lo que puede generar incidentes de ciberseguridad que comprometan la confidencialidad, integridad y disponibilidad de los activos de información de la compañía. Esta falta de protección facilita a los ciberdelincuentes aprovechar las debilidades de la plataforma tecnológica, poniendo en riesgo el logro de los objetivos empresariales.

La ausencia de medidas de protección adecuadas expone a las compañías a riesgos reputacionales, legales, financieros, operativos y de continuidad. Estos riesgos, si no son gestionados de manera efectiva, pueden llevar incluso a la disolución de la empresa. A partir del análisis del mapa de experiencia de usuario, hemos logrado un mejor entendimiento de las principales necesidades, las cuales están relacionadas principalmente con la protección de la información y la garantía de la disponibilidad operativa. Este entendimiento es fundamental para evitar daños a la reputación y posibles sanciones de los entes reguladores, asegurando así la continuidad del negocio.

En este contexto, hemos identificado que el objetivo principal del servicio que ofrecemos es gestionar las amenazas cibernéticas más significativas, tales como la fuga de información por ataques cibernéticos, fraudes dirigidos a los clientes e infecciones por malware, entre otros. La ciberseguridad requiere una combinación de controles técnicos, administrativos y servicios especializados. Sin embargo, las PYMES a menudo no pueden implementar todas estas medidas debido a sus limitaciones presupuestarias. Por ello, hemos identificado los servicios que pueden generar mayor valor para proteger tanto la reputación

como los procesos de una empresa. Estos servicios se centran en identificar y corregir vulnerabilidades técnicas en activos críticos, complementados con inteligencia de amenazas y monitoreo de la marca para evitar la suplantación de dominios.

3.4. Resumen de capitulo

En este capítulo se destaca la importancia de comprender al usuario final para poder abordar sus necesidades de protección de información y seguridad cibernética, ofreciendo servicios que se adapten a sus presupuestos limitados y desafíos específicos. Detectamos que la información que manejan los usuarios se encuentra almacenadas en la nube, Data Center y dispositivos extraíbles, los cuales corren el riesgo de ser vulnerados ya que no se encuentran protegidos de forma correcta y con ello corren el riesgo de tener incidentes que ponen en peligro la integridad y disponibilidad de activos de información de las PYMES. Para poder comprender y resolver el problema social relevante, nos apoyamos en las encuestas las cuales fueron realizadas a 20 empresarios dueños de PYMES en nuestro país, en las mismas contamos con 18 preguntas las cuales se encuentran en el Anexo A.

Capítulo IV: Diseño del producto o servicio

En este capítulo, se describe el proceso de diseño de la propuesta de servicio en ciberseguridad para PYMES. Se abordan los principales retos que enfrentan estas empresas, como la falta de conocimientos técnicos y las limitaciones presupuestarias, y se proponen soluciones adaptadas a sus necesidades. A través de este análisis, se detallan los mecanismos y estrategias que permitirán ofrecer un servicio accesible y eficaz para proteger sus activos críticos e información sensible.

4.1. Concepción del producto o servicio

Para elaborar nuestra propuesta de servicios, hemos empleado el enfoque de *Design Thinking,* orientando a crear un servicio de ciberseguridad completamente integrado y personalizado para PYMES, Como parte de la identificación de necesidades, hemos reconocido la importancia de cumplir con la Ley N° 29733 de Protección de Datos en Perú. Además, es crucial asegurar la confidencialidad e integridad de la información para prevenir el acceso no autorizado por parte de atacantes informáticos, garantizar la disponibilidad de la información y recursos esenciales para la continuidad del negocio. Igualmente detectar actividades sospechosas frente al aumento global de ataques cibernéticos, y asegurar la seguridad de las transacciones en línea para fomentar el crecimiento de ventas por los canales digitales.

En línea con las necesidades identificadas, proponemos un servicio completamente diseñado para proteger los activos más críticos de la PYME, que van desde datos personales de clientes o colaboradores, información financiera, hasta el know-how del negocio. La esencia de nuestro proyecto es un servicio de inteligencia de amenazas y de concientización hacía los colaboradores, que inicia con un análisis detallado de los activos tecnológicos de la compañía. Este paso inicial nos facilita una comprensión de las

tecnologías utilizadas por nuestros clientes, a partir de esta información, diseñaremos un servicio capaz de identificar y mitigar proactivamente las amenazas cibernéticas, protegiendo así la confidencialidad, disponibilidad e integridad de la información.

4.2. Desarrollo de la narrativa

El desarrollo del lienzo 6x6 constituyó un paso fundamental en la evolución de nuestra propuesta de servicio, ya que nos permitió obtener una perspectiva más clara y detallada. A través de este método, analizamos diversas variables interrelacionadas, lo que facilitó una comprensión más profunda de la idea original. Esta herramienta también nos ayudó a organizar y sintetizar las diferentes ideas y estrategias de manera clara y eficiente.

Con la inclusión de datos clave, que luego convertimos en preguntas específicas, el lienzo 6x6 nos ayudó en la creación de una estructura sólida para nuestro análisis. Este enfoque fue no solo enriquecedor, sino también práctico, ya que permitió que la estructura inicial de nuestro servicio evolucionara con mayor claridad. A medida que avanzábamos, identificamos y eliminamos procesos de menor relevancia, al tiempo que incorporamos nuevos elementos que surgieron como resultado del análisis del lienzo.

El lienzo 6x6 no solo nos permitió afianzar de manera efectiva la concepción de nuestro servicio, sino que también nos brindó una estructura que facilita la planificación, el análisis y la implementación del negocio. Ayudó a definir los elementos esenciales del proyecto, asegurando que todos los aspectos estén alineados con la visión general. Como resultado del análisis del lienzo, destacamos los siguientes puntos clave:

- El lienzo 6x6 se realizó para poder tener una idea mayor de nuestro servicio, donde se consideraron diferentes variables, que fuimos cruzando para poder aterrizar de una mejor forma la idea inicial.

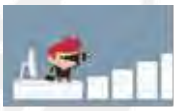
- Con ello podemos visualizar diferentes ideas y estrategias de una manera más organizada y concisa.
- En la misma se consideraron los datos más importantes, los mismos que se transformaron en preguntas para poder realizar el lienzo 6x6.
- Fue muy interesante y de utilidad realizar este lienzo ya que como primer bosquejo del servicio que implementaremos, se pudo ir descartando algunos procesos que no tenían mucha importancia y se agregaron otros que salieron posterior a realizar el lienzo.
- Adicionalmente con el lienzo realizado se aterrizó con mayor determinación el bosquejo para el servicio a implementar

Este lienzo nos permitió identificar que el robo de información tecnológica es un desafío clave para la mayoría de las PYMES en la era digital. Las principales amenazas abarcan desde la filtración de datos confidenciales hasta la infección de sistemas, lo que puede generar pérdidas financieras significativas, así como daños a la reputación y pérdida de confianza de los clientes. Ante los constantes intentos de intrusión por parte de atacantes mediante técnicas como ciberataques e ingeniería social, las PYMES enfrentan riesgos que comprometen la integridad, disponibilidad y confidencialidad de su información. En la Tabla 1 se presenta el lienzo 6x6, que detalla las principales vulnerabilidades y áreas de mejora identificadas en este análisis.

Tabla 1

Lienzo 6X6

¿Cómo podría el usuario mantener la información segura?	¿Cómo se podría mantener la integridad y confidencialidad de la información?	¿Cómo se podría mantener la disponibilidad de la información?	¿Cómo se podría mantener la reputación para la compañía?	¿Cómo se podría monitorizar comportamientos sospechosos?	¿Cómo se podría asegurar que las transacciones en línea sean seguras?
Evitando el Phishing, en los correos y mensajes sospechosos y de dudosa procedencia	Implementando medidas para monitorizar comportamientos anómalos en la red o en la infraestructura.	Implementar controles a nivel de acceso para evitar que accedan de forma no autorizada a la información.	Mantener métodos y enfoques de seguridad empleados, y comunicar eficazmente las medidas implementadas para proteger la información.	Monitorear el entorno, donde se proporcione información como nuevas vulnerabilidades, vulnerabilidades explotadas, exploits, técnicas, origen de ataques, etc	Concientizando a los clientes respecto a la página real de la compañía
Implementando controles de seguridad para proteger la información de los clientes, colaboradores, socios, etc	Identificar el tipo de información que se requiere proteger.	Gestionar las vulnerabilidades de acuerdo a las buenas prácticas de la industria.	Cuidando la calidad del servicio y la experiencia del consumidor.	Monitoreando el comportamiento del usuario para detectar actividades sospechosas.	Implementando mecanismos de autenticación y autorización
Que solo las personas que requieran	Identificando los flujos por donde la	Tener infraestructura actualizada y	Cuidando los activos e información	A través de herramientas tecnológicas	Implementando controles de seguridad

¿Cómo podría el usuario mantener la información segura?	¿Cómo se podría mantener la integridad y confidencialidad de la información?	¿Cómo se podría mantener la disponibilidad de la información?	¿Cómo se podría mantener la reputación para la compañía?	¿Cómo se podría monitorizar comportamientos sospechosos?	¿Cómo se podría asegurar que las transacciones en línea sean seguras?
acceso a la información cuenten con los permisos para acceder. 	información viaja para identificar las personas o tecnología que transmiten, procesan o almacenan esa información. 	con soporte 	de la compañía. 	o servicios que pueden detectar este tipo de comportamientos 	como certificados digitales 
Concientizando a los colaboradores de la compañía	Almacenando la información solo en recursos autorizados por la compañía	Contar con un proceso de gestión de incidentes de ciberseguridad	Incorporando controles de seguridad para proteger la información.	Implementando y configurando alertas de seguridad que notifiquen de inmediato cuando se detectan actividades sospechosas	Monitorizar el comportamiento de la marca en internet.

Después de definir las diversas alternativas de servicio, procedimos a la creación del lienzo blanco de relevancia y a su correspondiente descripción. Durante esta fase, al desarrollar los primeros prototipos del proyecto, realizamos entrevistas con distintos usuarios con el objetivo de comprender sus expectativas y opiniones sobre nuestro servicio inicial. A partir de estas conversaciones, surgieron los siguientes insights clave:

En primer lugar, se identificó que la máxima prioridad para las PYMES es garantizar la resiliencia frente a un incidente de seguridad. En este sentido, se destacó la necesidad de asegurar que, en caso de suceder un ataque, la operatividad de la empresa no se vea comprometida y, mucho menos, su continuidad. Asimismo, se detectó que otra prioridad para la mayoría de los usuarios es implementar las protecciones necesarias para los datos más sensibles de la empresa, tales como la información financiera, los datos personales de clientes y colaboradores, así como el know-how empresarial. El objetivo principal es prevenir accesos no autorizados que puedan comprometer dichos activos.

Además, se subrayó la necesidad de entender cómo los ataques informáticos podrían afectar a la organización. Sin embargo, se evidenció cierta incertidumbre entre los usuarios respecto a las acciones concretas que se deben tomar para evitar que los colaboradores caigan en prácticas como hacer clic en enlaces maliciosos que contengan malware. Estas malas prácticas pueden desencadenar infecciones en los activos tecnológicos de la compañía. Por otro lado, se observó que las PYMES han enfrentado incidentes de ciberseguridad relacionados con correos electrónicos engañosos, lo que pone de manifiesto el bajo nivel de conciencia entre los colaboradores para identificar direcciones de correo sospechosas. Esto ha facilitado el acceso indebido a información sensible, lo cual resalta la necesidad de integrar en el servicio estrategias

específicas contra el phishing, enfocadas en elevar la cultura de ciberseguridad dentro de la organización.

Asimismo, respecto a la cultura de ciberseguridad, se identificó la urgencia de que los usuarios implementen contraseñas robustas, dado que las contraseñas débiles han resultado en pérdidas de información importantes. En este contexto, también se sugirió que el servicio incluya un programa de entrenamiento para los colaboradores, centrado en las mejores prácticas de seguridad. Finalmente, se destacó la importancia de incorporar en el servicio estrategias de capacitación y preparación para empleados y colaboradores. Estas estrategias deben permitir que los usuarios actúen de manera adecuada ante incidentes o ataques cibernéticos. En consecuencia, se enfatiza la necesidad de implementar campañas de concientización y protección de datos como parte integral de la formación en seguridad.

Figura 7

Lienzo Blanco de Relevancia

De acuerdo con nuestro análisis del lienzo blanco de relevancia, los usuarios consideran que la protección cibernética que ofrecemos es segura y se adapta adecuadamente a las

necesidades específicas de cada empresa, ya que el servicio es completamente personalizable. Es fundamental considerar aspectos clave, como la magnitud de la amenaza cibernética a la que la empresa está expuesta, identificando los activos críticos que requieren protección. Asimismo, es esencial implementar un plan de respuesta ante incidentes, que permita actuar de manera efectiva en caso de brechas de seguridad.

Para garantizar la viabilidad de nuestro proyecto, es imprescindible cumplir con las regulaciones y normativas vigentes aplicables al sector. Esto asegurará que el servicio no solo sea efectivo, sino también conforme a los estándares legales y de seguridad. Finalmente, nuestros clientes deben ser conscientes de los riesgos económicos asociados a la falta de protección cibernética. Es importante que valoren el impacto económico de no contar con medidas de seguridad adecuadas y comprendan el valor agregado que nuestro servicio aporta en términos de protección y continuidad operativa.

4.3. Carácter innovador y disruptivo del producto o servicio

Nuestro servicio se considera disruptivo, ya que introduce innovaciones y enfoques que transformarán significativamente la manera en que las PYMES gestionan su seguridad digital. Las soluciones actuales no logran satisfacer por completo las necesidades de este sector, principalmente porque no ofrecen personalización, lo que genera barreras que disminuyen el valor que aportan. A diferencia de la competencia, que se dirige principalmente a segmentos con alto poder adquisitivo, nuestro servicio se enfocará en ofrecer soluciones accesibles a empresas que, hasta ahora, no han podido acceder a este tipo de protección. De esta manera, atenderemos un nicho de mercado desatendido por las compañías del sector. Nuestro servicio disruptivo se caracteriza por los siguientes aspectos clave:

- Cambio en el paradigma del mercado: Nuestro enfoque será distinto al tradicional, ya que personalizaremos el servicio según las necesidades específicas de cada usuario, ofreciendo soluciones adaptadas que permiten una protección más efectiva.
- Accesibilidad o democratización: Nos enfocamos en brindar un servicio accesible para las PYMES, y también para un sector más amplio, eliminando las barreras de entrada que limitan el acceso a soluciones de ciberseguridad de alta calidad.
- Innovación tecnológica: Integramos tecnologías emergentes, como la inteligencia artificial (IA), para detectar y responder a amenazas activas en el entorno digital. Esta IA no solo evaluará la vulnerabilidad de los activos de la compañía, sino que también ejecutará acciones preventivas, desde la simulación de remediaciones para asegurar la integridad de los activos, hasta la implementación de medidas correctivas o restricciones de acceso, garantizando así la continuidad operativa y la seguridad de la empresa.
- Mejora en la experiencia del usuario: Nuestro servicio ofrece una experiencia significativamente mejorada para el usuario en comparación con las propuestas actuales del mercado. Al ofrecer opciones personalizadas para cada cliente, las soluciones serán más prácticas y fáciles de implementar.
- Reducción de costos: Proporcionaremos un servicio de calidad similar, pero a un costo más bajo que las alternativas actuales. Además, brindaremos diversas opciones para adaptarnos a los presupuestos y necesidades de nuestros clientes.

4.4. Propuesta de valor

Nuestro lienzo de la propuesta de valor se divide en dos partes principales: el Perfil del Cliente y el Mapa de Valor. Este lienzo fue elaborado tras identificar los servicios enfocados en

la protección de la información y la ciberseguridad para PYMES. Nos diferenciamos por ofrecer un servicio personalizado que se adapta a las necesidades específicas de cada cliente. Además, nuestro servicio se enriquece constantemente con el feedback que recibimos, lo que nos permite mejorar de manera continua las soluciones que brindamos. Este enfoque genera un elemento diferenciador frente a otras compañías, que suelen ofrecer soluciones estandarizadas sin considerar la satisfacción y particularidades de cada cliente.

Figura 8

Lienzo de propuesta de valor

Nuestro servicio se especializa en implementar soluciones y medidas de ciberseguridad para proteger la información y datos de las PYMES, enfocándonos en los siguientes servicios:

- Inteligencia de Amenazas y remediación de vulnerabilidades
- Detección y Respuesta a Incidentes.
- Concientización relacionada a ciberseguridad para los colaboradores de la compañía.

Nuestros clientes valoran enormemente la seguridad cibernética de sus datos disponible 24/7, lo que no solo reduce las pérdidas económicas, sino que también mitiga el riesgo de robo de información, una preocupación crítica que puede llevar a la pérdida de clientes y dañar la reputación de la empresa y colocar en riesgo la continuidad de la empresa. La ciberseguridad es el activo más preciado que tienen nuestros clientes, es por ello que debemos asegurar que los datos están protegidos de accesos no autorizados, generando de esta forma tranquilidad a los clientes.

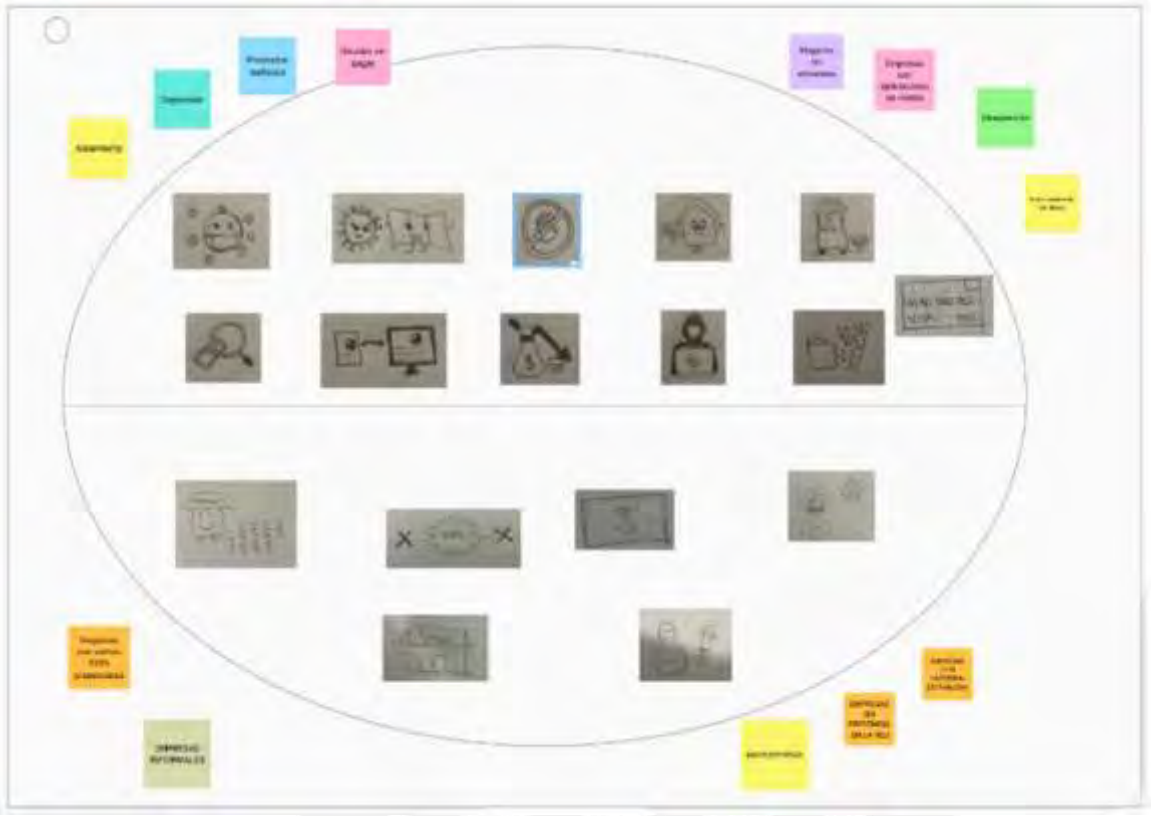
El lienzo también nos indica las frustraciones de los usuarios que invierten dinero en ciberseguridad como antivirus y capacitaciones, sin poder lograr el principal valor que es la protección de su información y esto se ve reflejado en mayores gastos económicos. Nuestro servicio, por tanto, no solo mejora la seguridad, sino que también optimiza los costos y la gestión de recursos de seguridad de nuestros clientes.

4.5. Producto mínimo viable (PMV)

La Figura 9, ilustra el Producto Mínimo Viable (MVP) que fue inicialmente desarrollado. Esta incluye un análisis de las principales preocupaciones y limitaciones identificadas durante el proceso de recopilación y evaluación de información proporcionada por diversos *stakeholders.* Dicha figura destaca cómo la pandemia ha impulsado principalmente la digitalización de las PYMES.

Figura 9

Producto mínimo viable (PMV)



Para definir el Producto Mínimo Viable (PMV), adoptamos la metodología SCRUM, lo que nos permitió desarrollar un servicio de ciberseguridad dirigido específicamente a PYMES, con el objetivo principal de fortalecer la protección de su información. Nuestra propuesta aporta un valor distintivo al negocio al incorporar una interfaz diseñada tanto para el uso gerencial como técnico. A través de esta plataforma, el gerente general puede acceder a noticias relevantes sobre ciberseguridad, visualizar el número de activos integrados al servicio, su estado actual de seguridad, y el número de empleados capacitados, además de varios indicadores de concienciación sobre ciberseguridad (Ver Figuras 10, 11 y 12).

Es importante destacar que esta versión inicial del servicio se ajustará en función del feedback que recibamos de los usuarios y de las nuevas funcionalidades que requieran nuestros clientes. Para el desarrollo de este prototipo, utilizamos tecnologías HTML y JavaScript. Nuestro servicio de ciberseguridad ofrece una solución integral, diseñada específicamente para proteger los sistemas tecnológicos y los datos críticos de las PYMES. Mediante un enfoque proactivo y flexible, proporcionamos tecnologías que son capaces de identificar, prevenir y responder a amenazas cibernéticas, garantizando así la continuidad operativa y brindando total tranquilidad a nuestros clientes.

Funcionalidades

- Acceso a noticias de ciberseguridad**:** La página web proporciona un flujo continuo de noticias relevantes a ciberseguridad, ayudando a los usuarios a mantenerse informados sobre las últimas amenazas y tendencias.
- Visualización de activos integrados**:** Permite a los gerentes ver el número de activos que están siendo protegidos bajo el servicio de ciberseguridad.
- Monitoreo del estado de seguridad**:** Los usuarios pueden revisar el estado actual de la postura de seguridad de cada activo integrado, lo que facilita la detección temprana de posibles vulnerabilidades.
- Reporte de capacitación de empleados**:** Indica el número de empleados que han sido capacitados en prácticas de ciberseguridad, contribuyendo a una mejor cultura de seguridad dentro de la empresa.

- Indicadores de concientización sobre ciberseguridad**:** Incluye métricas y estadísticas que resaltan el nivel de concientización sobre ciberseguridad dentro de la empresa, permitiendo ajustes en las campañas de educación y prevención.
- Acciones realizadas como parte del servicio para mejorar la ciberseguridad**:** Eventos identificados como parte del servicio de inteligencia de amenazas y acciones correctivas realizadas dentro de la organización, por ejemplo, remediación de vulnerabilidades por activos.
- Acuerdos de nivel de servicio (SLAs)**:** Estos acuerdos especifican los tiempos de respuesta comprometidos por nuestro servicio, garantizando el cumplimiento de nuestros compromisos de manera clara y medible en términos de calidad y tiempo.

Reconociendo la vulnerabilidad inherente del factor humano, decidimos expandir nuestro Producto Mínimo Viable (PMV) incorporando dos servicios. Estos están diseñados para sensibilizar y educar a los usuarios que interactúan con las tecnologías de la compañía. Ofrecidos a través de la misma plataforma, estos servicios permitirán a los colaboradores acceder a cursos de ciberseguridad que les ayudarán a profundizar sus conocimientos mediante videos, juegos, exámenes y otros recursos educativos.

El segundo servicio, enfocado en la concientización de los usuarios, tiene el objetivo de verificar la adopción de buenas prácticas de ciberseguridad por parte de los colaboradores de la compañía. Por esta razón, implementaremos ejercicios de phishing simulados. Esta iniciativa busca garantizar que los empleados estén preparados para identificar y responder adecuadamente ante este tipo de ataques cibernéticos. Estas simulaciones se llevarán a cabo directamente desde nuestra plataforma. Los indicadores resultantes se recopilarán y presentarán a través de la interfaz de gestión para la gerencia de la compañía.

Figura 10

Interfaz plataforma: Inicio

Figura 11

Interfaz plataforma: Servicios

Figura 12

Interfaz Plataforma: PYMESHIELD

4.6. Resumen del capitulo

En este capítulo se ha presentado un enfoque integral para el diseño de un servicio de ciberseguridad que responda a las necesidades específicas de las PYMES, garantizando la protección de la información y la continuidad del negocio. Esto se logra mediante una planificación estructurada y un análisis detallado de las amenazas actuales. Además, se ha destacado la naturaleza disruptiva y personalizada del servicio, adaptándose a los requerimientos particulares de cada empresa, cumpliendo con las normativas exigidas y ofreciendo soluciones innovadoras a un costo accesible.

El servicio propuesto no solo mejora la seguridad cibernética de las PYMES, sino que también optimiza el uso de recursos y reduce los costos asociados. El análisis del Producto Mínimo Viable (PMV) desarrollado demuestra cómo el servicio se ajusta a la creciente digitalización de las empresas, abordando eficazmente las preocupaciones y limitaciones identificadas a lo largo del proceso.

Capítulo V. Modelo de negocio

En este capítulo, se presentará el modelo de negocio del servicio enfocado en la identificación y contención de amenazas cibernéticas. Se hará énfasis en la protección de la información crítica y la continuidad operativa de las PYMES bajo condiciones óptimas. A través del modelo Canvas, se identificaron los socios clave, actividades esenciales, y la estructura de costos, que sustentan la viabilidad, escalabilidad y sostenibilidad del servicio propuesto.

5.1. Lienzo del modelo de negocio

Para este análisis, hemos empleado el *Business Model Canvas*, cuyos doce componentes clave se detallan en la Figura 14. Nuestra propuesta de servicio está diseñada específicamente para PYMES que procesan, almacenan o transmiten datos personales de clientes o colaboradores, así como información de know-how que requiere controles de seguridad robustos o información financiera y plataformas web para las ventas en línea. Para este segmento de clientes, buscamos ofrecer un servicio integrado y personalizado de ciberseguridad, diseñado para satisfacer las necesidades actuales del mercado y adaptado al incremento de los ataques informáticos a nivel global.

Nuestro principal propósito como empresa es proporcionar un servicio que proporcione una postura de seguridad robusta, permitiendo a las compañías proteger su información confidencial contra filtraciones de datos y accesos no autorizados. Aunque el mercado de ciberseguridad en nuestro país no ha sido ampliamente explorado y nuestro servicio no cuenta con competidores directos, es importante destacar que existen empresas de ciberseguridad con capacidades similares a las nuestras. Sin embargo, nosotros diferenciamos nuestro servicio al incorporar inteligencia artificial (IA), para simular remediaciones de vulnerabilidades e impactos de la remediación sobre las plataformas tecnológicas. Además, utilizamos IA para centralizar las

fuentes de amenaza externas en una compañía, lo que nos permite ofrecer servicios de clase mundial a costos más bajos.

Somos una empresa dedicada al monitoreo en tiempo real de todas las posibles amenazas de nuestros clientes, identificando peligros potenciales para asegurar su seguridad. Para ello, contamos con capacidades computacionales escalables y confiables, capaces de procesar grandes volúmenes de información. Además, la robustez de nuestra red es vital, dado que incluso breves interrupciones pueden significar brechas significativas en los activos críticos de nuestros clientes. Complementamos estos recursos tecnológicos claves con personal altamente capacitado, indispensable para supervisar y optimizar nuestro servicio automatizado y garantizar la protección. En nuestra estructura de costos, los costos fijos incluyen gastos como mano de obra, impuestos, software, hardware y licencias. Por otro lado, los costos variables comprenden los gastos relacionados con marketing, así como los salarios del equipo de ventas y administrativo, entre otros.

Figura 13

Lienzo del modelo de negocio (BMC)

5.2. Viabilidad financiera del modelo de negocio

Durante la evaluación del proyecto, se determinaron los recursos mínimos necesarios para establecer el servicio. Aunque nuestro servicio usa una plataforma web, los costos de desarrollo de software no se incluyen, dado a que contamos con un equipo de ingenieros de sistemas que se encargará del diseño correspondiente. Para establecer los precios del servicio a nivel de concientización, llevamos a cabo un análisis de los costos actuales del software KnowBe4, el cual está enfocado en la capacitación de usuarios en temas de ciberseguridad.

Se elaboró una proyección de cinco años con un VAN de PEN 1.027.546. La estrategia definida consiste en el crecimiento de suscriptores. En el primer año, se estima la suscripción de 1,712 activos tecnológicos integrados a nuestro servicio de inteligencia de amenazas y de 933 usuarios en el servicio de concientización de ciberseguridad. El periodo de recuperación será en el año 2 y un TIR de 67,02%, de esta forma y con estos indicadores se puede considerar el proyecto como viable.

5.3. Escalabilidad/exponencialidad del modelo de negocio

Un negocio escalable se caracteriza por su amplio potencial de crecimiento. Nuestro modelo de negocio es innovador, en un mercado nuevo y aun no atendido en su totalidad por otras empresas del rubro, lo cual nos posiciona como una empresa con amplias posibilidades de crecimiento desde el inicio. Esta afirmación se fundamenta en los siguientes puntos claves:

- Mercado inexplorado**:** Competimos en un nicho de mercado aún no saturado, donde no existen empresas que ofrezcan servicios especializados de ciberseguridad similares a los nuestros. En este contexto, las pequeñas y medianas empresas (PYMES) son el motor financiero del país, y, según un artículo publicado por Noticias Perú, estas empresas, en un lapso de cinco años, logran convertirse en proveedoras de grandes corporaciones

(Noticias Perú, 2024). Estas últimas mantienen procesos de contratación rigurosos que incluyen la evaluación de medidas de ciberseguridad, subrayando la importancia de la gestión de riesgos en la cadena de suministro.

- Demanda en aumento constante**:** Además, la demanda de ciberseguridad continúa creciendo en respuesta al incremento de las amenazas y vulnerabilidades en el entorno. La creciente dependencia de la tecnología por parte de empresas intensifica la necesidad de soluciones de ciberseguridad efectivas que faciliten la consecución de los objetivos de las compañías.
- Sin fronteras: Las amenazas cibernéticas trascienden las fronteras geográficas, proporcionando a las compañías especializadas en ciberseguridad la oportunidad de expandir su alcance a nivel mundial. Estas empresas pueden ofrecer servicios a diversas organizaciones en distintos países, lo que incrementa significativamente su potencial de crecimiento.

Como competencia indirecta podemos mencionar a SECURESOFT, quienes tienen más de 19 años en el mercado enfocados en ciberseguridad, ofreciendo servicios en los mercados de Perú, Colombia y Chile. Su portafolio de servicios ofrece soluciones para analizar las vulnerabilidades en la infraestructura y componentes de red, entre otros. Sin embargo, su nicho de negocio no son las Pymes, por lo que no ofrecen soluciones a este mercado, el cual a su vez no puede acceder a estos servicios por el costo y también porque no son personalizados.

Los principales clientes actuales de SECURESOFT son:

- Entel
- Banco Ripley

- BBVA
- Grupo Romero
- BCP
- DP World Callao
- Terminales Portuarios

A su vez, en el mercado local, existen otras empresas que ofrecen servicios de ciberseguridad. En primer lugar, Neosecure es una compañía dedicada a enfrentar las amenazas y proteger los activos y sistemas de las organizaciones. Esta empresa tiene operaciones en varios países de Latinoamérica, como Argentina, Chile, Perú y Colombia, con un enfoque en el desarrollo de soluciones de ciberseguridad.

Por otro lado, ETEK es una multinacional con más de 30 años de experiencia brindando soluciones de ciberseguridad en la región y en otros mercados internacionales. Con un equipo de más de 200 especialistas en tecnologías avanzadas, tiene oficinas en países como Colombia, Perú, México, India y Estados Unidos. Sus clientes principales provienen de sectores como banca, finanzas, seguros, retail y oil & gas. Sin embargo, estas empresas están principalmente enfocadas en grandes clientes corporativos y no se centran en las necesidades de las PYMES. Dado el alto costo de sus servicios, no resultan viables para las pequeñas y medianas empresas, ya que no ofrecen alternativas personalizadas que se ajusten a su tamaño y presupuesto.

En cuanto a nuestra estrategia de expansión, en primer lugar, nos enfocaremos en consolidar nuestro servicio dentro de Perú. Esto nos permitirá fortalecer nuestras soluciones y optimizarlas con base en el feedback de los clientes locales. Posteriormente, consideraremos expandirnos hacia mercados internacionales, con un enfoque inicial en la región latinoamericana.

5.4. Sostenibilidad social del modelo del negocio

PYMESHIELD no solo es una idea de negocio con fines financieros, sino sostenible en su afán de brindar un servicio de calidad mitigando el impacto de potenciales ciberataques para las Pymes. Nos alineamos con los Objetivos de Desarrollo Sostenible (ODS) número 9 y número 16. Específicamente con el objetivo 9 (Industria, innovación e infraestructura) en línea con las metas número 9.1, 9.3 y 9.5; ya que ayudamos a la promoción de nuevas tecnologías, fortalecimiento de infraestructura digital, fomentamos la conectividad segura y apoyamos el emprendimiento.

En referencia a la meta 9.1, nos enfocaremos en desarrollar infraestructura resiliente, sostenible apoyándonos en el componente digital, para poder garantizar que la conectividad sea segura y eficiente, incluyendo sistemas de gestión de incidentes y soluciones de recuperación ante ataques cibernéticos. Con la meta 9.3, buscaremos mejorar la conectividad digital, impulsando la inclusión social para todas las Pymes y generando servicios de ciberseguridad personalizados para los diferentes presupuestos de nuestros clientes. En referencia a la meta 9.5, buscaremos mediante alianzas estratégicas con el estado y empresas privadas poder aumentar el gasto en investigación y desarrollo (I + D) y fomentar la innovación para el sector de las Pymes.

En cuanto al objetivo 16 (Paz, justicia e instituciones sólidas) nos alineamos en esta con las metas número 16.6 y 16.10; ya que estamos comprometidos con la promoción de la seguridad y estabilidad digital, protección de derechos digitales y el fomento de la transparencia. En la meta 16.6, nuestro lineamiento principal es el de fomentar la transparencia a través de sistemas de monitoreo y prevención cibernéticos. Desarrollando sistemas de seguridad que aseguren la eficacia y la responsabilidad en la prestación de servicios. Fomentar la implementación de sistemas de gestión de calidad como el ISO 27001 para poder garantizar prácticas efectivas y responsables en la gestión de seguridad de la información. El enfoque con la meta 16.10, es que

nuestros clientes puedan tener la información clara y accesible sobre las políticas de ciberseguridad y procedimientos de respuesta ante incidentes. También debemos asegurarnos que las herramientas y soluciones de ciberseguridad, no limiten de forma injusta el acceso a la información o libertad en línea.

5.5. Resumen del capitulo

En este capítulo, el modelo de negocio se centra en ofrecer un servicio de ciberseguridad innovador y adaptado a las necesidades de las PYMES, utilizando tecnologías avanzadas para poder proporcionar una protección robusta y personalizada a un costo competitivo. Nuestra estructura de costos y el análisis del Canvas permiten una comprensión clara de los recursos, actividades y estrategias necesarias para poder implementar el servicio eficazmente.

El modelo de negocio muestra viabilidad financiera sólida y un alto potencial de crecimiento. Considerando una mezcla de un nicho de mercado no saturado, una demanda creciente y la posible expansión internacional posiciona al servicio como una solución escalable y prometedora en el ámbito de la ciberseguridad para PYMES. Podemos decir que PYMESHIELD se compromete a no solo ofrecer servicios de ciberseguridad de alta calidad, sino también a contribuir al desarrollo sostenible y a la promoción de prácticas responsables y transparentes en el ámbito digital, alineándose con las ODS para un impacto positivo en la comunidad y en el sector de las PYMES.

Capítulo VI: Solución Deseable, Factible y Viable

En este capítulo, evaluaremos la deseabilidad, factibilidad y viabilidad de los servicios de ciberseguridad ofrecidos por PYMESHIELD. Analizaremos específicamente si las PYMES tienen la capacidad financiera para costear estos servicios, asegurando que nuestros productos y servicios sean accesibles para este segmento del mercado.

6.1. Validación de deseabilidad de la solución

En este capítulo, se validará la deseabilidad de nuestra propuesta mediante un análisis exhaustivo del Modelo de Negocio Canvas, enfocándonos específicamente en la propuesta de valor, la relación con el cliente y los canales de atención. A partir de estos elementos, se han formulado tres hipótesis que serán evaluadas mediante experimentos diseñados específicamente para este propósito. La validación exitosa de estas hipótesis demostrará la deseabilidad de nuestra solución.

6.1.1. Hipótesis para validar la deseabilidad de la solución

Utilizando el Modelo de Negocio Canvas, se generaron diversas ideas que posteriormente se emplearon para formular hipótesis.

Tabla 2

Ideas para Hipótesis de Deseabilidad

Modelo de Negocio Canvas	Ideas para Hipótesis de Deseabilidad
Segmentos de Mercado	Dirigimos nuestros servicios a MYPES formales que poseen activos tecnológicos utilizados para almacenar información crítica. Esto incluye datos de clientes y colaboradores, aplicaciones que soportan ventas en línea, las cuales manejan información sensible como datos personales y

	datos de tarjetas, know-how del negocio, que puede abarcar fórmulas, recetas y herramientas personalizadas empleadas en la prestación de sus servicios.
Propuesta de Valor	El mercado de ciberseguridad en nuestro país aún está en desarrollo. Aunque no tenemos competidores directos, existen empresas de seguridad que podrían ofrecer servicios similares a los nuestros. Nuestra principal diferencia radica en la personalización del servicio y en la identificación y remediación de vulnerabilidades con el apoyo de inteligencia artificial. Ofrecemos servicios de clase mundial a costos accesibles, que incluyen inteligencia de amenazas, identificación y remediación de vulnerabilidades, y un programa de concientización que abarca simulaciones de phishing y capacitación en ciberseguridad.
Canales de Distribución	Los servicios de nuestra empresa se distribuyen principalmente de forma virtual, utilizando conexiones de internet públicas. Este enfoque incluye la realización de reuniones a través de plataformas como Microsoft Teams, así como interacciones directas mediante visitas de nuestro equipo comercial o llamadas telefónicas. Esta combinación de métodos nos permite mantener una comunicación eficaz y adaptable con nuestros clientes.
Relaciones con los Clientes	Para PYMESHIELD es esencial establecer una relación estrecha con nuestros clientes, por lo tanto, tenemos: ● Servicios personalizados. ● Fomentamos una relación basada en la confianza. ● Mantenemos a nuestros clientes informados. ● Implementamos IA para optimizar nuestros procesos.
Flujos de Ingresos	Los ingresos de PYMESHIELD se derivan de la venta de servicios de ciberseguridad, los cuales ofrecemos en diversos paquetes y a precios diferenciadores. Esta estructura permite adaptar nuestras soluciones a las necesidades y presupuestos de diferentes clientes, asegurando accesibilidad y flexibilidad en nuestras ofertas

A continuación, presentamos las hipótesis fundamentadas en las ideas desarrolladas a partir del Modelo de Negocio Canvas.

H_1: La disposición de los clientes a pagar aproximadamente 200 soles por la gestión de cada uno de los activos tecnológicos refleja una valoración positiva y una clara preferencia por las soluciones que ofrece nuestra empresa.

H_2: La estrategia de distribuir nuestros servicios a través de nuestra plataforma virtual, complementada con un servicio personalizado y asistencia permanente, fortalece la preferencia de los clientes por nuestras soluciones.

H_3: Más del 50% de las pequeñas y medianas empresas (PYMES) han recibido algún intento o han experimentado una actividad relacionada con un ciberataque.

Tabla 3

Hipótesis 1, 2 y 3

Concepto	Hipótesis 1	Hipótesis 2	Hipótesis 3
Hipótesis	La disposición de los clientes a pagar aproximadamente 200 soles por la gestión de cada uno de los activos tecnológicos refleja una valoración positiva y una clara preferencia por las soluciones que ofrece nuestra empresa	La estrategia de distribuir nuestros servicios a través de nuestra plataforma virtual, complementada con un servicio personalizado y asistencia permanente, fortalece la preferencia de los clientes por nuestras soluciones.	Más del 50% de las pequeñas y medianas empresas (PYMES) han recibido algún intento o han experimentado una actividad relacionada con un ciberataque.

Diseño del experimento	Para verificar esta hipótesis haremos una encuesta a 20 personas de PYMES a los que explicaremos las bondades de nuestro servicio.	Para verificar esta hipótesis, proponemos que 20 encuestados utilicen nuestra plataforma en el contexto de una Prueba de Concepto (POC). Durante este período, harán uso de nuestro servicio por un lapso de 15 días.	Para verificar esta hipótesis, incluimos una pregunta específica en el contexto de una encuesta dirigida a PYMES. En esta pregunta, proporcionamos una explicación clara de lo que podría constituir un incidente o intento de ciberataque. Esto incluye ejemplos de actividades sospechosas, como intentos de phishing, accesos no autorizados, malware, y cualquier otra actividad que pueda comprometer la seguridad de la información.
Métrica	Mediremos la aceptación del precio propuesto por nuestro servicio, contabilizando el número de CEOs que lo aprueban.	Mediremos la percepción de la intuitividad y el valor agregado de nuestra plataforma entre el personal de TI y administrativo, según la estructura organizacional de cada PYME, tras la finalización de la Prueba de Concepto (POC). Además, cuantificamos cuántos de ellos estarán	El porcentaje de PYMES que reportan estar en un nivel de riesgo alto, medio o bajo en relación con ciberataques e incidentes de seguridad informática.

		dispuestos a contratar el servicio al concluir el período de prueba	
Criterio	La hipótesis se considerará validada si más del 80% de los encuestados indican que el precio propuesto es adecuado.	Consideraremos que la hipótesis ha sido validada si más del 80% de los encuestados informan que la aplicación es fácil de usar, demostrando su usabilidad, y si más del 50% expresan su intención de contratar nuestros servicios.	La hipótesis se considerará validada si más del 50% de los encuestados indican que han experimentado un ciberataque o un intento de ciberataque.

6.1.2. Experimentos empleados para validar la deseabilidad de la solución

Para validar las hipótesis, realizamos encuestas a 20 personas pertenecientes a diversas PYMES. Dependiendo de la estructura organizacional de cada empresa, los encuestados variaron entre personal de tecnología, administrativos y, en ausencia de departamentos tecnológicos, directamente a los CEOs. Esta flexibilidad nos permitió adaptarnos al perfil específico de cada organización y asegurar la relevancia de nuestro estudio. En la Tabla 4, se describen los resultados de la encuesta y las respuestas relacionadas con las hipótesis. Toda la información detallada de la encuesta se puede encontrar en el Apéndice A.

Tabla 4

Resultado de las preguntas para probar las hipótesis

Pregunta	Análisis de resultados
En los últimos 5 años, ¿fueron víctimas o han tenido	El 80% de los encuestados ha

intentos de ataques a su plataforma web, suplantación de identidad, hurto de información personal o cualquier otra actividad que se considere como ciberataque?	utilizado nuestra plataforma para registrar la información
En una escala del 1 al 5, ¿qué tan satisfecho/a estás con la facilidad de uso de la plataforma para registrar a tu empresa y solicitar nuestros servicios?	El 100% de los encuestados que utilizó nuestra plataforma consideró que esta, es muy fácil de usar.
Considerando que nuestros servicios de gestión de vulnerabilidades se aplican por equipo (servidor o computadora) y que realizamos seguimientos constantes de las actividades en tiempo real para prevenir y mitigar la materialización de riesgos, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características?	El 85% de los encuestados se encuentra dispuesto a pagar un precio más alto por un servicio especializado que mejore la seguridad de sus operaciones en la red.
Considerando que ofrecemos un servicio de concientización en ciberseguridad para los colaboradores, que incluye capacitación regular y simulaciones de phishing para mejorar la seguridad de la empresa, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características por colaborador?	El 70% de los encuestados estarían dispuesto a pagar un precio de más de 40 soles por un servicio de concientización.

Según los resultados de la encuesta, identificamos que los participantes no cuentan con servicios de ciberseguridad. Tras proporcionarles contexto sobre los posibles impactos en sus organizaciones, la percepción fue notablemente positiva. Además, mostraron disposición a asumir un costo adicional. Esto indica que nuestros servicios son altamente valorados por los clientes, quienes consideran que el valor ofrecido justifica el costo. Como parte de la interfaz gráfica que desarrollamos para este servicio, se incluyeron detalles sobre los servicios que ofrecemos actualmente, además de una sección de contacto, tal como se documenta en el punto 4.5 de este proyecto.

Los resultados de la encuesta indican que nuestra estrategia de comunicación y distribución, que incorpora el uso de la plataforma digital, alcanza eficazmente a nuestro público objetivo en el ámbito de la ciberseguridad. Esto demuestra que nuestra estrategia es exitosa en la comunicación efectiva de los servicios disponibles y en la captación de clientes potenciales. Tras la interacción de los encuestados con la interfaz de nuestro producto, la encuesta nos permitió identificar un alto nivel de satisfacción con la plataforma y la experiencia de usuario. Los datos muestran que los usuarios están generalmente satisfechos con la facilidad de uso de nuestra plataforma para acceder a los servicios de ciberseguridad. Esta satisfacción indica que la plataforma cumple efectivamente con las expectativas de los usuarios en términos de accesibilidad y funcionalidad.

En conclusión, los resultados de la encuesta revelan que los servicios especializados que ofrecemos en PYMESHIELD son altamente valorados por nuestros encuestados. Además, nuestra estrategia de comunicación y distribución ha demostrado ser efectiva para alcanzar a nuestro público objetivo. La experiencia positiva de usuario en nuestra plataforma contribuye significativamente a nuestro posicionamiento, lo cual es fundamental para alcanzar las metas establecidas en nuestra proyección de ventas y para satisfacer las demandas del mercado en materia de ciberseguridad. Por lo tanto, podemos afirmar que nuestra solución es deseable y ha sido bien recibida por los clientes potenciales.

En cuanto a las métricas establecidas en nuestras hipótesis, tenemos los siguientes resultados:

- H1: Criterio de aceptación 80% calificación final 90%
- H2: Criterio de aceptación 80% calificación final 90%
- H3: Criterio de aceptación 50% calificación final 80%

6.2. Validación de la factibilidad de la solución

Para analizar la factibilidad de nuestro proyecto utilizaremos el plan del mercado y el plan de operaciones para validar las hipótesis definidas.

6.2.1. Plan de mercadeo

En las siguientes secciones, describiremos nuestro plan de mercadeo, poniendo especial énfasis en el mix de marketing. Este enfoque integral contempla estrategias detalladas relacionadas con el producto, el precio y las promociones, siguiendo las directrices establecidas por Kotler (2021). Nuestra propuesta de servicios está diseñada para un modelo de negocio B2B, dirigido inicialmente a las MYPES en Perú. Según la definición de la SUNAT (2024), las MYPES son entidades económicas, ya sean personas naturales o jurídicas, que operan en diversas formas organizativas legales. Su objetivo principal es realizar actividades que incluyen la extracción, transformación, producción, comercialización de bienes o la prestación de servicios. De acuerdo con datos de la Encuesta Nacional de Hogares (ENHAHO) de 2022, existen aproximadamente 6.1 millones de MYPES distribuidas en todo el país.

6.2.2. Producto

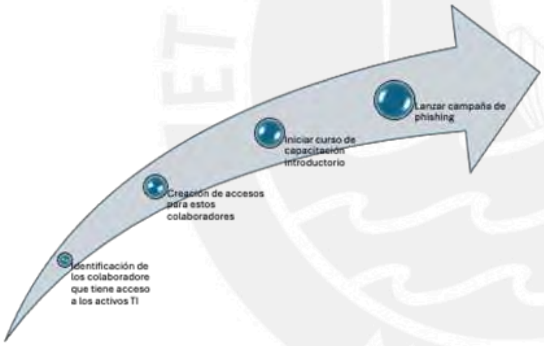
Ofrecemos una propuesta integral de ciberseguridad diseñada específicamente para PYMES, que incluye tres servicios clave: inteligencia de amenazas, remediación de vulnerabilidades y concientización en ciberseguridad. Este enfoque proactivo está diseñado para proteger los sistemas y datos críticos de manera eficaz, adaptándose a las necesidades específicas de cada negocio. Nuestra solución avanzada permite identificar, prevenir y responder a las amenazas cibernéticas, asegurando así la continuidad operativa de nuestros clientes.

Figura 14

Proceso de entrega del producto de inteligencia de amenazas y remediación de vulnerabilidades

Figura 15

Proceso de entrega del producto de concientización



Como mencionamos anteriormente, nuestro producto es integral y se fundamenta en varios procesos distintos. Para mayor claridad, hemos documentado estos procesos en dos figuras distintas.

6.2.3. Precio

Nuestra política de precios está influenciada por varios factores clave. Estos incluyen el costo de los servicios que ofrecemos, el alto valor que nuestros clientes perciben en ellos, y la segmentación del mercado donde operamos. Dado que nuestras soluciones de ciberseguridad

conllevan costos significativos, también hemos analizado los precios de la competencia para asegurarnos de que nuestros precios sean competitivos en el mercado.

Después de este análisis, hemos definido una lista de precios, los cuales presentamos en la siguiente tabla.

Tabla 5

Tabla de precios

Servicio	Precio
Servicio de inteligencia de amenazas y remediación de vulnerabilidades	S/ 160
Servicio de concientización en ciberseguridad	S/ 25
Servicio de simulación de phishing	S/ 25

Al evaluar estos criterios y realizar un análisis exhaustivo del mercado, incluyendo nuestra competencia y la demanda de los servicios por los clientes, nuestra empresa de ciberseguridad para PYMES podrá establecer una política de precios que sea coherente con el sector y competitiva en el mercado. Esta política estará diseñada para reflejar adecuadamente el valor de nuestros servicios especializados, asegurando así que las empresas puedan mantener una imagen positiva, operar eficientemente, y percibir un retorno de la inversión (ROI).

6.2.4. Ubicación

La pandemia ha traído beneficios laborales para algunas empresas. Las compañías tecnológicas, en particular, han reconocido que el teletrabajo es una opción favorable para sus colaboradores. Esta modalidad reduce los gastos administrativos al eliminar gastos como alquiler, servicios y otros gastos asociados con la presencialidad. Por esta razón, PYMESHIELD optará por no contar con oficinas físicas.

- Presencia online**:** La presencia en línea es fundamental para la prestación de nuestros servicios y la operatividad de nuestros productos. Según el feedback obtenido en nuestras encuestas, nuestro sitio web es fácil de navegar. En él, los usuarios pueden encontrar información sobre nuestros servicios, formularios de contacto, y próximamente, testimonios de clientes. Además, optimizaremos nuestro sitio web para los motores de búsqueda (SEO), con el fin de aumentar nuestra visibilidad en línea.
- Redes sociales: Para establecer una presencia activa y comprometida en línea, utilizaremos redes sociales profesionales como LinkedIn y Twitter. Publicaremos regularmente contenido relevante sobre ciberseguridad, compartiremos noticias de la industria y participaremos en conversaciones pertinentes, con el objetivo de aumentar nuestra visibilidad y alcance. Optaremos por no usar Facebook o Instagram, dado que buscamos mantener un perfil profesional y estas plataformas no se alinean con nuestro mercado objetivo.
- Colaboraciones y asociaciones: Buscaremos colaborar con empresas, organizaciones y líderes de opinión en el ámbito de la tecnología y la ciberseguridad. Nuestras actividades de colaboración incluirán participar en webinars, asistir a eventos de tecnología y ciberseguridad, participar en podcasts especializados, y contribuir en blogs de la industria. Además, colaboraremos con organizaciones estatales para influir en la regulación y con asociaciones para escalar nuestros servicios en las PYMES.
- Listados en directorios y plataformas especializadas**:** Garantizamos figurar en las listas de empresas destacadas de nuestro sector y en aquellas que son consultadas frecuentemente por las PYMES. Además, buscaremos tener una posición destacada en los principales motores de búsqueda, como Google.

- Atención al cliente y soporte: Nuestro soporte y atención al cliente se ofrecerán telefónicamente y también a través de un chat integrado en nuestra plataforma. Además, estableceremos Acuerdos de Nivel de Servicio (SLAs) personalizados con cada PYME, adaptándose a las necesidades específicas de su empresa.

6.2.5. Promoción

Para promocionar los servicios de nuestra empresa, enfocados en PYMES con más de 50 trabajadores, implementaremos una estrategia de promoción integral que combina medios tradicionales y digitales. A continuación, mencionaremos algunas prácticas que planteamos usar:

- Marketing de contenidos**:** Desarrollaremos contenido enfocado en sensibilizar sobre ciberseguridad, mediante artículos que aborden nuevas vulnerabilidades y cómo remediarlas, además de ofrecer consejos útiles sobre el tema. Esta iniciativa permitirá a las empresas reconocer nuestro conocimiento técnico y especializado, fortaleciendo nuestra posición como expertos en la industria.
- Presencia en redes sociales**:** Utilizaremos redes sociales como LinkedIn y Twitter para compartir contenido relevante y fomentar la interacción. Además, consideraremos la participación activa en comunidades en línea relacionadas con la ciberseguridad, con el objetivo de contribuir a mejorar el ecosistema global en esta área
- Publicidad online**:** Invertiremos en publicidad de pago por clic (PPC) a través de Google Ads y en plataformas de redes sociales para alcanzar a clientes potenciales interesados en servicios de ciberseguridad. Esta estrategia nos permitirá segmentar nuestra audiencia eficazmente y mostrar anuncios relevantes en momentos clave, maximizando la relevancia y el impacto de nuestras campañas

- Email marketing: Crearemos una lista de suscriptores y enviaremos correos electrónicos de manera mensual para evitar saturación y evitar que nuestros mensajes sean percibidos como SPAM. Los contenidos incluirán información sobre nuevas amenazas en el mercado y actualizaciones de nuestros servicios. Esta estrategia de email marketing no solo demostrará nuestro compromiso con la investigación continua de amenazas, sino que también ayudará a fomentar una cultura de ciberseguridad y mantener un contacto cercano con nuestros clientes.
- Eventos y webinars: En el Perú, se están llevando a cabo numerosos eventos de ciberseguridad tanto presenciales como en formato de webinars, reflejando una tendencia significativa en la industria. Por esta razón, planeamos organizar tanto webinars como eventos presenciales sobre temas relevantes de ciberseguridad. Estos nos ofrecerán la oportunidad de compartir conocimientos, demostrar el valor de nuestros servicios y conectar directamente con clientes potenciales, facilitando la creación de relaciones duraderas.
- Alianzas estratégicas: Estableceremos colaboraciones con el Estado peruano para promover prácticas de ciberseguridad. Esto no solo ampliará nuestra red de contactos, sino que también nos permitirá influir en las relaciones y asociaciones existentes con PYMES, abriendo caminos hacia nuevos clientes.

Al combinar estas técnicas para promocionar nuestros servicios, podemos desarrollar una estrategia integral de marketing que nos permita llegar eficazmente a nuestro mercado objetivo y destacarnos en el sector de la ciberseguridad para PYMES. Ver Tabla 6 la cual se describe a continuación.

Tabla 6

Mix de Marketing

	2024	2025	2026	2027	2028
Producto					
Diseño del producto	S/48.000	S/ 9.600	S/ 10.080	S/ 10.584	S/ 11.113
Promoción					
Video de lanzamiento	S/ 7.200	S/ 7.920	S/ 8.712	S/ 9.583	S/ 10.542
Google Adwords	S/ 1,44	S/ 2.640	S/ 2,90	S/ 3.194	S/ 3.514
Instagram	S/ 1.680	S/ 2.640	S/ 2.904	S/ 3.194	S/ 3.514
Twitter	S/ 1.680	S/ 2.640	S/ 2.904	S/ 3.194	S/ 3.514
Distribución					
Canales de distribución (Correo)	S/ 6.000	S/ 1.320	S/ 1.452	S/ 1.597	S/ 1.757
Total	S/ 64.561	S/ 26.760	S/ 26.055	S/ 31.350	S/ 33.957

La proyección del CAC (Costo de Adquisición de Cliente) y del VTVC (Valor Total de la Vida del Cliente) en nuestro plan de marketing para PYMESHIELD muestra un desempeño excepcional. El “ratio” entre estas dos métricas es significativamente mayor que 1, indicando que nuestro plan de marketing está generando resultados efectivos. Estamos adquiriendo clientes a un costo relativamente bajo en comparación con el valor total que aportan durante su relación con nuestra empresa. Esta favorable relación entre el costo de adquisición y el valor del tiempo de vida del cliente es un indicador sólido de la salud y el crecimiento de nuestro negocio.

En conclusión, nuestro plan de marketing ha demostrado ser efectivo en atraer a clientes con alto potencial de gasto sostenido, lo que augura un crecimiento constante y sostenible para nuestro negocio. Las mejoras en la eficiencia de la adquisición de clientes y el aumento en la rentabilidad de nuestra base de clientes existentes son claros indicadores de nuestro éxito.

6.3. Plan de operaciones

Hemos desarrollado un plan de operaciones estratégico con el fin de fortalecer nuestra empresa a corto plazo. Este plan tiene como objetivo principal garantizar la eficacia, seguridad y calidad de nuestros servicios mediante el desarrollo de una infraestructura tecnológica robusta. En este contexto, hemos decidido desarrollar una solución de software como servicio (SaaS) para crear y entrenar un modelo de inteligencia artificial generativa. Este modelo será capaz de identificar y remediar vulnerabilidades de manera automática, teniendo en cuenta tanto la viabilidad técnica como el impacto potencial de estas acciones.

Para lograrlo, emplearemos simulaciones que nos permitan prever y optimizar el impacto de las acciones de remediación, mejorando así la seguridad de nuestros sistemas de manera eficiente y proactiva. Hemos seleccionado Google AI Platform para implementar esta solución de IA generativa, lo que complementa nuestra estrategia de optimización de procesos operativos y la contratación de un equipo altamente calificado. El plan operativo se desarrolló considerando criterios esenciales para identificar los recursos tecnológicos, actividades, canales y la estructura de costos. A continuación, se detallan los requerimientos indispensables de este plan operativo:

6.3.1. Ubicación física

Nuestro modelo de trabajo se basa en el trabajo remoto debido a la flexibilidad que nos brinda para alcanzar nuestros objetivos, como se menciona en el capítulo 7.2.4. Sumado a esto, nos permite involucrar talento de cualquier parte del mundo.

6.3.2. Inversión

Para poder implementar nuestros servicios es requerido contar con la tecnología, personas y herramientas (Ver tabla 08 y 09).

6.3.3. Mano de obra

Para el desarrollo del servicio, se ha asignado un ingeniero y un analista de ciberseguridad encargados de llevar a cabo las actividades pertinentes. Aunque el equipo puede parecer reducido, es importante recordar que este servicio se basa principalmente en el uso de inteligencia artificial y la automatización de procesos, lo cual optimiza significativamente los recursos humanos necesarios. Dentro de las certificaciones hemos considerado la compra de dominio y certificado digital y licenciamiento de Microsoft.

Tabla 7

Costos fijos

Costos Fijos	Año 1
Vendedor	S/36.000,00
Ingeniero y analista de ciberseguridad	S/132.000,00
Certificaciones	S/8.400,00
TOTAL	S/176.400,00

6.3.4. Gastos de administración

Dentro de los gastos administrativos, hemos considerado el servicio de internet para los doce colaboradores que formarán parte de la compañía.

6.3.5. Gastos de intangibles

En los gastos intangibles, hemos incluido los costos relacionados con los trámites para la constitución de la compañía y la página web. (Ver Tabla 8).

Tabla 8

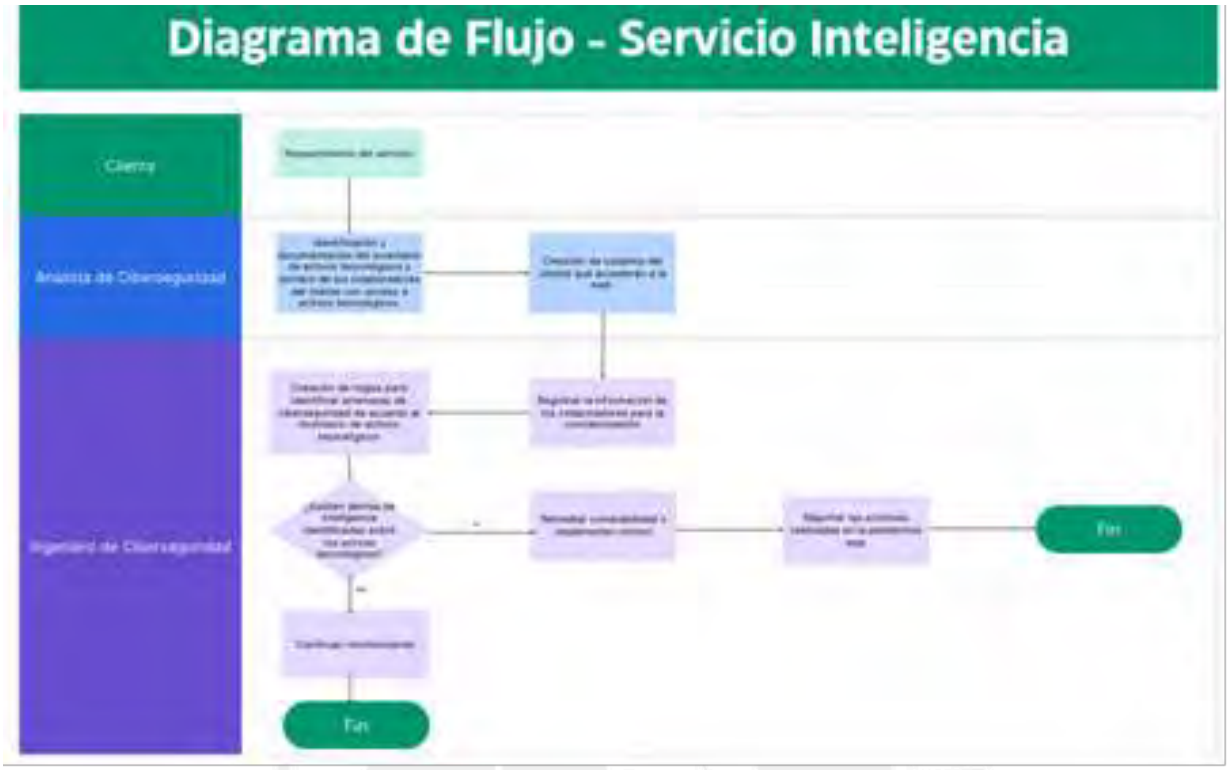
Activos no corrientes

Activo No Corriente: Intangibles	Monto sin IGV	Cantidades	Subtotal
Página web	S/2.000,00	1	S/2.000,00
Trámites de constitución	S/1.500,00	1	S/1.500,00
Trámite de licencia	S/1.200,00	1	S/1.200,00
Total			S/4.700,00

A través de este plan, buscamos no solo mejorar nuestra capacidad para enfrentar las amenazas cibernéticas, sino también fortalecer nuestra posición en el mercado y satisfacer las necesidades de nuestros clientes de manera efectiva. Con un enfoque centrado en la excelencia operativa y la innovación continua, estamos comprometidos con el éxito y la seguridad de nuestros clientes. Por otro lado, hemos desarrollado procesos eficientes para nuestro servicio de inteligencia de amenazas de ciberseguridad. Este servicio comienza con un levantamiento de activos tecnológicos, una actividad fundamental que marca el punto de partida y requiere la participación activa del cliente.

Figura 16

Diagrama de Flujo - Servicio de Inteligencia



6.3.6. Proceso de implementación

El proceso de implementación inicia luego de recibir la orden de compra por parte del cliente y considera las siguientes fases:

- Inventario de Activos**:** En colaboración con la empresa, procederemos a desarrollar la Base de Datos de Gestión de Configuración (CMDB, por sus siglas en inglés). Este proceso se llevará a cabo mediante la aplicación de un cuestionario detallado, cuyo propósito es identificar las tecnologías que utilizan tanto a nivel de sistema operativos como de aplicaciones. Este enfoque nos permite tener un entendimiento integral de la infraestructura tecnológica existente para las fases de implementación.
- Valoración del riesgo por activos**:** Luego de tener documentada la tecnología existente de la compañía evaluaremos en conjunto con la empresa el nivel de la criticidad de los

activos tecnológicos. Esto será a partir de entender cuáles activos tecnológicos procesan información sensible para la compañía y cuáles activos soportan aplicaciones críticas.

- Identificación de herramientas de ciberseguridad**:** Durante esta etapa, procederemos a verificar la existencia y el tipo de herramientas de seguridad implementadas por las empresas, especialmente aquellas que tienen la capacidad de generar alertas de seguridad relevantes. El objetivo es determinar la viabilidad y los requisitos para integrar estas herramientas con nuestra solución de ciberseguridad, asegurando así una protección óptima a los activos.
- Recolección y entendimiento de información**:** En esta etapa, procedemos a la recopilación de eventos de seguridad a partir de las herramientas empleadas por la compañía. Posteriormente, esta información se integra con nuestro servicio de inteligencia de amenazas para realizar un análisis exhaustivo. Al cruzar ambas fuentes de datos, desarrollamos casos de uso personalizados para cada compañía. Por ejemplo, si una empresa utiliza Java 8.0, nuestros casos de uso específicos nos permitirán identificar los riesgos existentes en el mercado que podrían ser explotados y representar una amenaza para este activo en particular.
- Remediación: La fase de remediación de vulnerabilidades representa uno de los aspectos más críticos de nuestro servicio. Sin embargo, existe el riesgo de que algunas aplicaciones puedan verse afectadas negativamente. Para mitigar este riesgo, nuestra estrategia incorpora el uso de inteligencia artificial (IA) generativa. Esta tecnología se diseña para aprender de incidentes previos en otras compañías y de información relevante extraída de foros de seguridad, con el fin de prever posibles impactos en la operatividad de nuestra

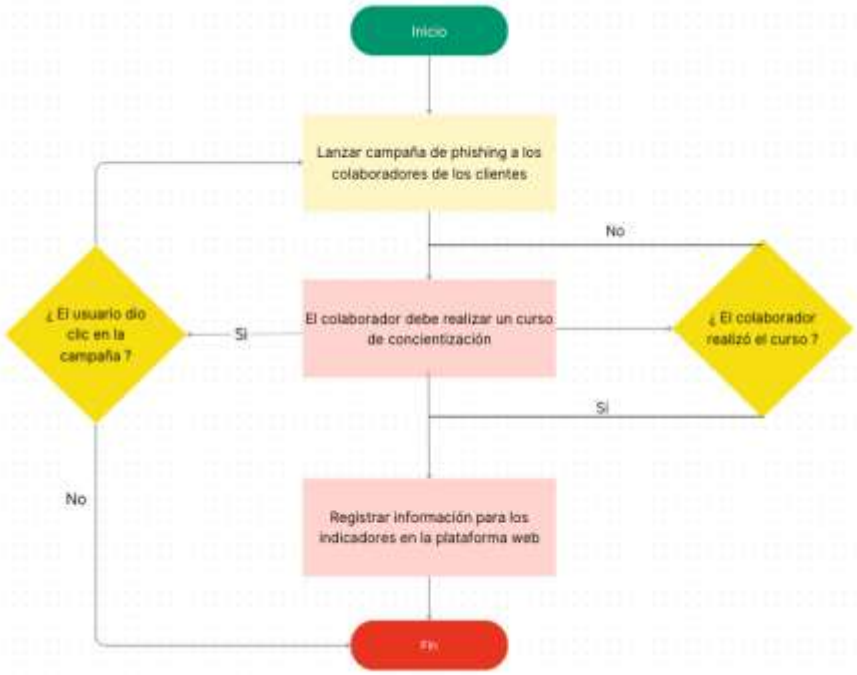
empresa cliente mediante simulaciones detalladas. Este enfoque proactivo nos permite anticipar y ajustar nuestras acciones de remediación para minimizar interrupciones y garantizar la continuidad del negocio.

- Seguimiento y satisfacción del servicio: Durante esta fase, nuestro objetivo es evaluar la satisfacción de nuestros clientes utilizando una variedad de herramientas. Nos esforzamos por ofrecer una experiencia excepcional con nuestro servicio, poniendo gran énfasis en comprender el entorno de nuestros clientes y garantizar la operación de sus negocios.

En lo que respecta al servicio de concientización, el proceso comienza con la identificación y registro de los usuarios que tendrán acceso a la plataforma. Esto les permitirá realizar sus capacitaciones en materia de ciberseguridad de manera eficiente y segura

Figura 17

Diagrama de Flujo - Servicio de concientización



6.3.7. Simulaciones empleadas para validar las hipótesis

Hemos llevado a cabo una evaluación exhaustiva del plan de marketing para verificar nuestra hipótesis utilizando el Método de Montecarlo, una técnica estadística de simulación. Durante este proceso, analizamos el impacto en el EBITDA. Aunque nuestras inversiones en marketing son conservadoras, ya que confiamos en que el boca a boca contribuirá significativamente a las ventas de nuestra marca, es importante destacar que durante el primer año proyectamos un EBITDA negativo. Esta situación se debe principalmente a nuestra estrategia prudente de venta de servicios a las compañías. Para el primer año, prevemos gestionar 1712 activos de información dentro del Servicio de Inteligencia de Amenazas y Remediación de Vulnerabilidades, así como 933 usuarios en los servicios de Concientización en Ciberseguridad y Simulación de Phishing.

La inversión para el primer año en marketing es de S/ 66.240. El CAC por cada usuario es de S/110,40 teniendo en cuenta un número inicial de 600 usuarios en el primer mes. Por otro lado, como lo señalamos anteriormente para el primer año tendremos un EBITDA negativo por lo tanto el VTVC es de -S/41,15. En conclusión, no se espera obtener un retorno asociado al plan de marketing durante el primer año. La hipótesis que planteamos es que el cociente entre el Valor Total de la Vida del Cliente (VTVC) y el Costo de Adquisición del Cliente (CAC) sea mayor a 3. Esto implica que el valor que un cliente aporta durante su relación con nuestra empresa sea, al menos, tres veces mayor que el costo invertido para adquirirlo.

- Generación de datos aleatorios**:** Utilizaremos el Método de Montecarlo para generar un gran volumen de números aleatorios que representan el VTVC y el CAC de los clientes potenciales. Estos números serán generados dentro de un rango basado en

datos históricos y proyecciones futuras, para esto usamos un generador de frecuencias con distribución normal de media 3 y desviación 2.

- Cálculo del Cociente VTVC/CAC: Para cada conjunto de números aleatorios generados, calcularemos el cociente VTVC/CAC. Esto nos dará una muestra de los posibles cocientes entre el valor de vida del cliente y el costo de adquisición para diferentes escenarios simulados.
- Análisis de la Distribución: Analizaremos la distribución de los cocientes VTVC/CAC obtenidos a través de la simulación de Montecarlo. Observaremos la frecuencia con la que los cocientes son mayores que 3 y evaluaremos la consistencia de estos resultados.
- Evaluación de la Hipótesis: Basándonos en la distribución de los cocientes VTVC/CAC, evaluaremos la probabilidad de que el cociente sea mayor que 3. Si la mayoría de los resultados de la simulación indican un cociente superior a 3, tendremos mayor confianza en nuestra hipótesis.

Tabla 9

Resultados del Montecarlo para el cociente VTVC/CAC

Estadísticos	
Media	34,47
Error típico	0,72
Mediana	33,95
Moda	#N/D
Desviación estándar	22,74
Varianza de la muestra	517,09

Curtosis		0,14
Coeficiente de asimetría	-	0,06
Rango		148,06
Mínimo	-	46,98
Máximo		101,08
Suma		34.469,93
Cuenta		1.000,00
Nivel de confianza (95.0%)		1,41
Mínimo		33,06
Máximo		35,88
PROB(VTVC/CAC>3) =		**0,91**

En base al análisis realizado, los resultados obtenidos son sumamente positivos. La hipótesis que pretendíamos demostrar, es decir, que el cociente entre el valor total del cliente a lo largo del tiempo (VTVC) y el costo de adquisición de clientes (CAC) sea mayor a 3, ha sido validada utilizando una distribución normal con una media de 3 y una desviación estándar de 2. Este hallazgo nos brinda una mayor confianza en la rentabilidad y el valor a largo plazo de nuestros esfuerzos de adquisición de clientes. Observamos que en el 91% de las simulaciones, el cociente VTVC/CAC supera el valor de 3. Esto confirma que nuestra estrategia de marketing es robusta y está alineada con los objetivos establecidos, justificando así la continuación de nuestras inversiones en esta área. No obstante, es crucial monitorizar periódicamente esta estrategia, dado que existe un 9% de probabilidad de que el cociente sea menor a 3, por lo tanto, es necesario gestionar este riesgo y ajustar la estrategia de marketing si se producen variaciones significativas.

Tabla 10

Resultados del VTVC/CAC

	2025	2026	2027	2028	2029
Inversión en marketing anual	S/66.240,00	S/26.760,00	S/28.956,00	S/31.346,00	S/33.954,00
Número de clientes	600,00	660,00	726,00	798,60	878,46
CAC	S/110,40	S/40,55	S/39,88	S/39,25	S/38,65
Ticket promedio	S/2.520,00	S/2.508,55	S/2.498,49	S/2.489,76	S/2.482,31
Frecuencia	3,00	3,00	3,00	3,00	3,00
Margen	-0,60	0,25	1,28	2,83	5,19
VTVC	-S/4.543,14	S/1.898,54	S/9.557,95	S/21.127,68	S/38.682,53
Total, de Ingresos	S/1.512.000,00	S/1.655.643,00	S/1.813.903,14	S/1.988.323,27	S/2.180.612,05
VTVC/CAC	- 41,15	46,82	239,64	538,27	1.000,80

6.3.8. Validación de la viabilidad de la solución

Para validar la viabilidad financiera de nuestro proyecto, hemos proyectado un panorama a cinco años, considerando tanto ingresos como egresos en soles, dado que el servicio se ofrecerá inicialmente solo en Perú. Los resultados evidencian que obtendremos un VAN de S/1.027.546 con un TIR de 67,02%.

6.3.9. Presupuesto de inversión

La inversión inicial requerida para este proyecto es de 34,400 soles, una cantidad relativamente baja en comparación con otros negocios. Esto se debe a que nuestro modelo operativo no requiere de infraestructura física significativa y el 95% de las operaciones se realizan a través de servicios en la nube. La siguiente tabla detalla los gastos iniciales o la inversión inicial necesaria.

Tabla 11

Presupuesto de Inversión

Activo no corriente: Inmuebles, maquinaria y equipo	Monto sin IGV S/	Cantidades	subtotal S/
Computadoras	1,750.00	12	21,000.00
Impresoras	700.00	2	1,400.00
Celulares	1,500.00	8	12,000.00
Total, Inversiones fijas	**3,950.00**		**34,400.00**

6.3.10. Análisis financiero

Nuestro análisis financiero comienza con la estimación y proyección de nuestras ventas. Hemos previsto un crecimiento diferenciado para cada uno de los tipos de productos que ofrecemos, basándonos en el análisis de comportamientos históricos de empresas similares y en la expansión de las PYMES en Perú. Este análisis nos ha llevado a concluir que nuestras ventas seguirán la tendencia detallada en la tabla a continuación:

Tabla 12

Proyección de ventas a 5 años

Ingresos Proyectados	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Cantidad Vendida					
Servicio de inteligencia de amenazas y remediación de vulnerabilidades	1,712	2,397	3,355	4,697	6,576
Servicio de concientización en ciberseguridad	933	1,027	1,130	1,242	1,367
Servicio de simulación de phishing	933	1,027	1,130	1,242	1,367
Precio De Venta					
Servicio de inteligencia de amenazas y remediación de	S/ 175	S/ 193	S/ 212	S/ 233	S/ 257

vulnerabilidades					
Servicio de concientización en ciberseguridad	S/ 27	S/ 30	S/ 33	S/ 36	S/ 40
Servicio de simulación de phishing	S/ 27	S/ 30	S/ 33	S/ 36	S/ 40
Ingresos Por Producto/Servicio					
Servicio de inteligencia de amenazas y remediación de vulnerabilidades	S/300,079	S/462,122	S/ 711,668	S/1,095,969	S/1,687,792
Servicio de concientización en ciberseguridad	S/ 25,568	S/ 30,937	S/ 37,434	S/ 45,295	S/ 54,807
Servicio de simulación de phishing	S/ 25,568	S/ 30,937	S/ 37,434	S/ 45,295	S/ 54,807
Ingresos Totales	S/351,215	S/523,996	S/ 786,536	S/1,186,559	S/1,797,406

Por otro lado, hemos considerado aportes propios de S/ 65.498,80 para el cálculo del WACC que tuvo un resultado de 8.35% para el primer año y un préstamo bancario por un valor de S/ 98.248,20.

Tabla 13

Aportes

Préstamo	S/ 98.248,20	60%
Aportes propios	S/ 65.498,80	40%

De acuerdo al análisis financiero el CAPM es de 13.91% el cual se ajustó con la tasa de riesgo país del Perú 1.26% para determinar el WACC donde se obtuvo 8.34%. Como parte del Análisis Financiero, la propuesta de negocio de PYMESHIELD muestra un cálculo aproximado del Valor Actual Neto (VAN) de S/ 1.027.546. A continuación, presentamos los detalles de estos resultados:

Tabla 14

Detalle de Costos y Gastos

Detalle de Costos y Gastos	Monto	C o G	V o F
Gastos por alquiler de local	-	GASTO	FIJO
Internet	450,00	COSTO	VARIAB
Compra de dominio y certificado digital	100,00	COSTO	FIJO
Licenciamiento de Microsoft	600,00	COSTO	FIJO
Electricidad	0 -	GASTO	FIJO
Agua y alcantarillado	0 -	GASTO	FIJO
Artículos de limpieza	0 -	GASTO	FIJO
Marketing	5.380,12	GASTO	FIJO
Vendedor	3.000,00	GASTO	FIJO
Gerente General	10.000,00	GASTO	FIJO
Analista contable	3.000,00	GASTO	FIJO
Analista de nómina y marketing	3.000,00	GASTO	FIJO
Ingeniero y Analista de Ciberseguridad	11.000,00	COSTO	FIJO
TOTAL, S/	S/36.530,12		

6.3.11. Flujo de caja anual

El flujo de efectivo de la empresa muestra un aumento significativo a partir del segundo año y un crecimiento progresivo del saldo final de caja cada año, indicando una sólida salud financiera y un manejo eficiente del efectivo. En general, estos resultados reflejan una empresa de ciberseguridad con un crecimiento sostenido y una gestión financiera prudente, posicionándose bien para continuar su expansión y alcanzar sus objetivos financieros a largo plazo, como se evidencia en la siguiente tabla.

Tabla 15

Flujo de Caja Anual

Actividades de operación	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos por ventas		351.215	523.996	786.536	1.186.559	1.797.406
Pago costo de ventas		-181.800	-181.962	-182.129	-182.301	-182.478
Pago de Gastos administrativos		-258.240	-258.240	-258.240	-258.240	-258.240
Pago de Impuesto a la renta		0	-19.208	-97.180	-215.772	-396.625
Pago de Participación trabajadores		0	0	0	0	0
Total, Actividades de Operación		-88.825	64.586	248.987	530.247	960.064
Actividades de inversión						
Compra de activos fijos	-163.747					
Total, Actividades de Inversión	-163.747	0	0	0	0	0
Actividades de financiamiento		0	0	0	0	0
Aporte de capital de los socios	65.499	0	0	0	0	0
ingresos por Préstamos	98.248	0	0	0	0	0
Amortización deuda		-15.750	-17.496	-19.434	-21.588	-23.980
Intereses		-10.887	-9.142	-7.203	-5.049	-2.657
Pago de dividendos						
Total, Actividades de financiamiento	163.747	-26.637	-26.637	-26.637	-26.637	-26.637
Aumento (disminución de efectivo)	0	-115.462	37.949	222.350	503.610	933.426
más saldo inicial de caja	0	0	-115.462	-77.513	144.837	648.446
Saldo final de caja	0	-115.462	-77.513	144.837	648.446	1.581.873

Los resultados acumulados reflejan las ganancias acumuladas de la empresa a lo largo del tiempo. Estos resultados muestran una tendencia positiva, lo que indica un crecimiento rentable y sostenible de la empresa. No se registran dividendos por pagar en este estado financiero.

Tabla 16

Estado anual de la situación financiera

	Año 1	Año 2	Año 3	Año 4	Año 5
Activos					
Activos Corrientes					
Efectivo	-115.462	-77.513	144.837	648.446	1.581.873
Activo No corriente					
Activos fijos	163.747	163.747	163.747	163.747	163.747
Depreciación	-8.600	-17.200	-25.800	-34.400	-43.000
Amortización	-940	-1.880	-2.820	-3.760	-4.700
Total, activos	38.745	67.154	279.964	774.033	1.697.920
Pasivos					
Pasivo Corriente					
Deuda corto plazo	0	0	0	0	0
Impuestos a la renta	0	0	0	0	
Pasivo No corriente					
Deuda Largo Plazo (préstamo bancario)	82.498	65.002	45.568	23.980	0
Total, pasivos	82.498	65.002	45.568	23.980	0
Patrimonio					
Capital social	65.499	65.499	65.499	65.499	65.499
Resultados acumulados	-109.252	-63.347	168.897	684.555	1.632.421
Dividendos por pagar					
Total, patrimonio	-43.753	2.152	234.396	750.053	1.697.920
Pasivos + Patrimonio	38.745	67.154	279.964	774.033	1.697.920

Valor Presente Neto (VAN) y Tasa Interna de Retorno (TIR): El VAN positivo de S/1.027.546 sugiere que el proyecto de inversión es rentable y genera valor para los accionistas. La TIR del 67,02% indica la tasa de rendimiento esperada del proyecto, que es significativamente superior al costo de capital (WACC) del 8.34%, lo que sugiere que el proyecto es financieramente atractivo.

Tabla 17

Evaluación económica y financiera, en soles

	2024	2025	2026	2027	2028	2029
Total Ingresos		351.215	523.996	786.536	1.186.559	1.797.406
Costos		-181.800	-181.962	-182.129	-182.301	-182.478
Margen Bruto		169.415	342.034	604.407	1.004.258	1.614.929
Gastos fijos - Administrativos		-258.240	-258.240	-258.240	-258.240	-258.240
EBITDA		-88.825	83.794	346.167	746.018	1.356.689
Amortización de inversiones		-940	-940	-940	-940	-940
Depreciación		-8.600	-8.600	-8.600	-8.600	-8.600
EBIT		-98.365	74.254	336.627	736.478	1.347.149
Impuestos		-	-21.905	-99.305	-217.261	-397.409
Depreciación y amort		9.540	9.540	9.540	9.540	9.540
NOPAT		-88.825	61.889	246.862	528.757	959.280
Inversión Inicial	-163.747					
FCF	-163.747	-88.825	61.889	246.862	528.757	959.280
Préstamo	98.248					
Pago de Intereses		-10.887	-9.142	-7.203	-5.049	-2.657
Escudo fiscal de los intereses		3.212	2.697	2.125	1.490	784
Amortizaciones de préstamos		-15.750	-17.496	-19.434	-21.588	-23.980
Flujo de caja del accionista (FCA)	-65.499	-112.250	37.949	222.350	503.610	933.426
Utilidad Neta		-77.022	45.905	232.244	515.658	947.866

6.3.12. Simulaciones empleadas para validar las hipótesis

En esta fase de nuestro análisis, la hipótesis planteada es que el Valor Actual Neto (VAN) de nuestro proyecto debe superar los 200,000 soles. Para verificar esto, emplearemos una simulación de Montecarlo. Determinaremos la media y la desviación estándar del VAN. Con estos parámetros, generamos un VAN aleatorio siguiendo una distribución normal. Los resultados de esta simulación se presentan en la siguiente tabla.

Tabla 18

Simulación Monte Carlo para el VAN

Años	0	1	2	3	4	5
Flujo de caja neto	-163.747	-88.824	61.889	246.862	528.757	959.280
Promedio ponderado de capital	8,34%					
Valor Actual Neto (VAN)	1.027.546,30					
Tasa Interna de Retorno (TIR)	67,02%					
Período de retorno (en años)	7,43					

Tabla 19

Simulación Monte Carlo para el VAN Promedio

	VAN-Prom	VAN-DE
	1.265.765,67	249.239,35
Primera simulación	1.676.051,96	
VAN promedio simulado	2.045.851,34	
VAN desviación estándar simulada	410339,8887	
VAN mínimo	778.351,34	

VAN máximo	3.415.174,10
Riesgo de pérdida: VAN < 200,000	0,00%

Como se puede apreciar en la Tabla 20, la probabilidad de obtener menos de 200 mil soles es nula, lo cual valida nuestra hipótesis y, en consecuencia, demuestra la factibilidad del proyecto. Después de realizar 500 simulaciones del VAN, la desviación estándar se mantuvo consistentemente por encima de los 200 mil soles. Esto indica una percepción positiva del valor y una disposición por parte de los clientes a pagar un precio cercano a los 200 soles por los servicios brindados por nuestra empresa, reflejando una clara preferencia por nuestra oferta.

Tabla 20

Simulación del VAN - Análisis de sensibilidad

Análisis de sensibilidad	Crecimiento	VAN
	0,00	1.027.546,30
	0,05	1.078.923,61
	0,10	1.186.815,97
	0,15	1.364.838,37
	0,20	1.637.806,04
	Promedio	1.259.186,06
	DesvEstand	247.943,77

6.4. Resumen del capitulo

En conclusión, todos los análisis financieros han mostrado resultados positivos. Aunque la meta para este proyecto es alcanzar un VAN mínimo de S/ 1.000.000, se ha logrado este objetivo con un crecimiento bastante conservador. Las simulaciones realizadas han validado las hipótesis de manera favorable. Sin embargo, se destaca que no se tendrán ganancias en los primeros años.

Por lo tanto, es crucial aumentar el número de clientes para generar rápidamente valor hacia los inversionistas.

Capítulo VII. Solución sostenible

Actualmente, las compañías generan valor no solo a través de cifras financieras, que, aunque importantes, no son el único factor, sino también mediante el impacto social que sus servicios o productos pueden tener. En este capítulo, abordaremos las prácticas de sostenibilidad que hemos integrado en este proyecto. Dado que se trata de un servicio digital, estas prácticas se manifiestan en el valor que generamos a nuestros clientes y en el medio ambiente. El Lienzo del Negocio Próspero (Flourishing Business Canvas) reconoce que la propuesta de negocio de nuestra empresa de ciberseguridad se considera socialmente sustentable debido al compromiso voluntario de la empresa con un conjunto de normas y principios que abarcan aspectos sociales, económicos y ambientales basados en valores.

Nuestra empresa fundamenta su visión y compromiso en programas sociales que no solo benefician al negocio haciéndolo más productivo, sino que también impacta positivamente a las personas, su entorno medio ambiental y las comunidades donde opera. Nos enfocamos en prácticas empresariales responsables que van más allá de la rentabilidad financiera, incorporando consideraciones éticas y sociales en todas las facetas de nuestras operaciones. Por ejemplo, nos comprometemos a proteger la privacidad y seguridad de los datos de nuestros clientes, así como a contribuir activamente a la concienciación sobre la importancia de la ciberseguridad en la sociedad.

Además, nuestra empresa busca activamente oportunidades para involucrarse en iniciativas comunitarias y proyectos sociales que generen un impacto positivo en nuestra sociedad. Esto puede incluir programas de educación en ciberseguridad para escuelas y organizaciones locales, así como colaboraciones con instituciones benéficas que trabajan para proteger a grupos vulnerables contra amenazas cibernéticas.

7.1. Relevancia social de la solución

Este proyecto tiene como objetivo social el fortalecimiento de las capacidades de ciberseguridad de las PYMES, para gestionar el riesgo tecnológico en el camino a la consecución de sus objetivos financieros, riesgo que de no ser gestionado adecuadamente puede causar grandes pérdidas a propietarios y trabajadores, como vimos en el capítulo 1, lo que puede generar en la mayoría de los casos, incluso la quiebra de estos negocios.

7.1.1. Objetivo ODS 9

En este sentido nuestro proyecto se encuentra alineado con el objetivo ODS 9, dado que el desarrollo y despliegue de PYMESHIELD se vincula estrechamente con "Industria, Innovación e Infraestructura". A continuación, se detallan algunas formas en las que nuestro proyecto contribuye a este objetivo:

Promoción de la Innovación Tecnológica. Nuestra empresa está dedicada a desarrollar soluciones innovadoras en el campo de la ciberseguridad. Esto incluye el desarrollo de tecnologías avanzadas de protección de datos, detección de amenazas y respuesta ante incidentes. Al promover la innovación en este campo, contribuimos al avance tecnológico y al desarrollo de nuevas infraestructuras digitales más seguras.

Fortalecimiento de la Infraestructura Digital. Nuestros servicios de ciberseguridad ayudan a fortalecer la infraestructura digital tanto a nivel empresarial como a nivel comunitario. Al proteger las redes, sistemas y datos contra amenazas cibernéticas, contribuimos a la construcción de una infraestructura digital más robusta y resistente a los potenciales ciberataques.

Fomento de la Conectividad Segura. En un mundo cada vez más interconectado, es crucial garantizar que la conectividad sea segura y confiable. Nuestra empresa proporciona

servicios que ayudan a asegurar la comunicación y la transferencia de datos en línea, lo que promueve una conectividad más segura y protegida.

Apoyo al Emprendimiento y la Innovación: Como empresa innovadora en el campo de la ciberseguridad, contribuimos al ecosistema del emprendimiento y la tecnología. Al fomentar la creación de nuevas empresas y el desarrollo de soluciones tecnológicas innovadoras, ayudamos a impulsar el crecimiento económico y la generación de empleo en el sector tecnológico.

De las ocho metas mencionadas por la Organización de las Naciones Unidas en su portal de Objetivos de Desarrollo Sostenible para 2030, impactamos en las siguientes dentro del ODS 9:

- Meta 9.1: Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, con un enfoque en el acceso asequible y equitativo para todos.
- Meta 9.3: Aumentar el acceso de las pequeñas empresas industriales, en particular en los países en desarrollo, a los servicios financieros, incluidos los créditos asequibles, y su integración en las cadenas de valor y los mercados.
- Meta 9.5: Mejorar la investigación científica, mejorar la capacidad tecnológica de los sectores industriales en todos los países, en particular los países en desarrollo, incluso mediante el acceso a tecnologías industriales y conocimientos técnicos.

Hemos logrado impactar en 4 de las 8 metas, lo que nos permitirá establecer un Índice de Relevancia Social que será el siguiente:

- IRS= 4/8x100%= 50%.

7.1.2. Objetivo ODS 16

Además, nos alineamos con el Objetivo de Desarrollo Sostenible (ODS) número 16, "Paz, Justicia e Instituciones Sólidas", que busca promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir instituciones efectivas, responsables e inclusivas en todos los niveles. Aunque a primera vista un proyecto de ciberseguridad pueda parecer indirectamente relacionado con esta meta, en realidad puede contribuir de diversas maneras.

Promoción de la Seguridad y Estabilidad Digital. Nuestro proyecto de ciberseguridad fortalece la seguridad digital, creando un entorno en línea más protegido y confiable. Al mitigar los riesgos de ataques cibernéticos en diversos sectores, ayudamos a preservar la estabilidad de la industria, lo que impacta positivamente en la economía peruana. Además, al garantizar un entorno digital seguro, promovemos sociedades más pacíficas e inclusivas, facilitando el desarrollo sostenible y la confianza en las tecnologías digitales.

Protección de los Derechos Digitales. La ciberseguridad desempeña un papel fundamental en la protección de los derechos digitales, como la privacidad de la información, entre otros. Al salvaguardar estos derechos, contribuimos a construir un entorno digital más justo y equitativo.

Combate al Cibercrimen. Nuestro proyecto ayuda a combatir el cibercrimen y promover la aplicación efectiva de la ley en el ámbito digital. Al fortalecer la capacidad de las instituciones para investigar y enjuiciar delitos cibernéticos, contribuimos a la creación de instituciones sólidas y responsables.

Fomento de la Transparencia y la Integridad. La ciberseguridad también desempeña un papel clave en fomentar la transparencia y la integridad de la información en línea. Al proteger

sistemas y datos contra intrusiones maliciosas, aseguramos la veracidad de la información y prevenimos su manipulación.

Por otro lado, dentro de las ocho metas destacadas por la Organización de las Naciones Unidas en su portal de Objetivos de Desarrollo Sostenible para 2030, impactamos en las siguientes dentro del ODS 16:

- Meta 16.6 - Desarrollar instituciones efectivas, donde nuestro proyecto puede contribuir al desarrollo de instituciones efectivas al fortalecer la capacidad de las organizaciones para protegerse contra amenazas cibernéticas, al promover prácticas de ciberseguridad sólidas y al garantizar la integridad y la confiabilidad de los sistemas y datos.
- Meta 16.10 - Garantizar el acceso público a la información, al proteger los sistemas y datos contra intrusiones maliciosas, nuestro proyecto puede ayudar a garantizar el acceso público a la información al prevenir la manipulación y el acceso no autorizado a la información en línea, promoviendo así la transparencia y la libertad de información en el entorno digital.

De esta manera, podemos determinar el Índice de Relevancia Social, el cual calculamos de la siguiente forma:

- IRS= 2/12x100%= 16.67%.

7.2. Rentabilidad social de la solución

En la Tabla 21 muestra una estimación del flujo de beneficios sociales para los años 2025 a 2029, desglosados por diferentes criterios:

- Cantidad de clientes y ahorro por cliente: Proyectamos el número de clientes que atenderá nuestra compañía, junto con el ahorro estimado por cliente cada año. Por ejemplo, en

2025 se espera atender a 1,712 clientes, con un ahorro anual de S/ 389 por cliente. Para calcular este ahorro, nos basamos en la propuesta presentada por uno de los posibles competidores. Este valor fue determinado exclusivamente para los servicios de simulación de phishing y capacitación en ciberseguridad.

- Costo del impacto sobre los trabajadores por un día sin acceso a su computador: Este costo social refleja la paralización que pueden experimentar los empleados de PYMES que dependen de un computador para realizar sus funciones administrativas. En caso un incidente de ciberseguridad les impida acceder a su computador, se estima el impacto basado en un día de inactividad. Es importante señalar que, aunque este cálculo se basa en un día, la erradicación completa de un incidente de ciberseguridad puede tardar varios días dependiendo de la complejidad. Para calcular este valor, consideramos el costo de ausentismo tomando como referencia un salario minimo legal vigente en Perú, asumiendo que el colaborador no tiene acceso a su computador debido a la materialización de un incidente de ciberseguridad.
- Valor total ahorrado por los clientes y valor total de los beneficios sociales: Finalmente, se calcula el total del ahorro proyectado para los clientes y se suman los beneficios sociales estimados para cada año.

Al interpretar la tabla, observamos que el flujo de beneficios sociales refleja el valor añadido que la empresa aporta tanto a su ecosistema como a la comunidad en general a lo largo del tiempo.

Tabla 21

Estimación del flujo de beneficios del emprendimiento, en soles

Criterio	2025	2026	2027	2028	2029
Cantidad de clientes	1.712	2.397	3.355	4.697	6.576
Ahorro por cliente	389	389	389	389	389
Total, de ahorro	666.521	933.130	1.306.382	1.828.935	2.560.509
Costo de efecto sobre trabajadores por un día sin acceso a su computador	66	66	66	66	66
Número de trabajadores	1.712	2.397	3.355	4.697	6.576
Valor del efecto ahorrado por incidentes de ciberseguridad	112.983	158.177	221.448	310.027	434.037
Valor total de los beneficios sociales	779.504,81	1.091.306,73	1.527.829,42	2.138.961,19	2.994.545,67

En la Tabla 21 se presenta una estimación del flujo de costos sociales asociados a intrusiones de seguridad cibernética para los años 2025 a 2029, desglosados de la siguiente manera:

- Total de intrusiones: Se proyecta el número total de intrusiones de seguridad cibernética para cada año. Estas intrusiones representan amenazas a la seguridad informática que podrían comprometer la integridad, confidencialidad o disponibilidad de la información de las PYMES. Tomando en cuenta 25 intentos por minuto que es la cuarta parte de los intentos que se registraron para explotar la vulnerabilidad Log4Shell, según se menciona en el informe de Prey Project (Prey Project, 2022.)
- Emisión de CO2 por intrusión: Se estima la cantidad de emisión de dióxido de carbono (CO2) en gramos por cada intrusión de seguridad cibernética, utilizando un valor de 0.2 gramos de CO2 por evento, según lo informado por National Geographic (2019). Este valor representa el impacto ambiental asociado a las intrusiones de seguridad cibernética.

- Valor del gramo de emisión de CO2: Se proporciona el valor monetario del gramo de emisión de CO2, que se utiliza para calcular el costo social de las emisiones de CO2 asociadas a las intrusiones de seguridad cibernética.
- Valor total de los costos sociales: Se calcula el valor total de los costos sociales estimados para cada año, considerando tanto el número de intrusiones como el impacto ambiental de las emisiones de CO2 asociadas.

Al interpretar la tabla, se observa que los costos sociales asociados a las intrusiones de seguridad cibernética aumentan progresivamente con el tiempo, reflejando el crecimiento de nuestro servicio. Estos costos no solo incluyen los impactos económicos directos, sino también los impactos ambientales, como las emisiones de CO2 derivadas de dichas intrusiones.

Tabla 22

Estimación de los costos sociales del emprendimiento, en soles

Criterio	2025	2026	2027	2028	2029
Total, de intrusiones	22.493.972.111	31.491.560.955	44.088.185.338	61.723.459.473	86.412.843.262
Emisión de CO2 en gr/intrusión	0.2	0.2	0.2	0.2	0.2
Valor del gramo de emisión de CO2	0,0000975	0,0000975	0,0000975	0,0000975	0,0000975
Valor total de los costos sociales(soles)	438.632	614.085	859.720	1.203.607	1.685.050

Finalmente, la última tabla presenta el cálculo del VAN social de nuestro emprendimiento, obtenido al restar los costos sociales de los beneficios. Para ello, utilizamos la tasa de rentabilidad social aprobada por el MEF, que es del 8%. Esto nos dio un VAN social de aproximadamente 3 millones de soles, superando significativamente nuestras expectativas.

Tabla 23

Cálculo del VAN social

Criterio	2025	2026	2027	2028	2029
Valor total de los beneficios sociales	779.505	1.091.307	1.527.829	2.138.961	2.994.546
Valor total de los costos sociales	438.632	614.085	859.720	1.203.607	1.685.050
Flujo Social	340.872	477.221	668.110	935.354	1.309.495
Tasa Social	8%				
VAN Social	2.833.863				

En conclusión, este proyecto impulsa la sostenibilidad en relación con los ODS 9 y 16. El análisis presentado en este capítulo demuestra que el proyecto es tanto sostenible como rentable, alcanzando un VAN que supera la meta definida. Generando un impacto positivo medio ambiente.

Capítulo VIII. Decisión e implementación

En el presente capítulo se describirá el plan detallado para la implementación de PYMESHIELD, destacando la metodología seleccionada y los requerimientos funcionales de los servicios a ofrecer. Asimismo, se presentará el diseño de la arquitectura, el desarrollo de la interfaz web, la integración con servicios de inteligencia de amenazas, y las pruebas funcionales que se llevarán a cabo.

8.1. Plan de Implementación de los Servicios:

El proyecto se ejecutará empleando la metodología Scrum, a fin de hacer ágil y eficiente el desarrollo del mismo, lo que nos permitirá perfeccionar continuamente nuestra interfaz y el servicio en general, buscando la flexibilidad, adaptabilidad, mejora continua y entrega de valor constante, entre otros. Este enfoque se basa en la retroalimentación que nuestros clientes y nosotros como fundadores de la empresa, proporcionaremos al equipo de desarrollo.

En referencia al plan específico de trabajo para el desarrollo de los servicios contamos con las siguientes actividades:

Hito 1 (Preparación); en esta actividad se llevarán a cabo dos subactividades principales:

- Proceso de selección: Seleccionar e incorporar el talento humano que será parte del desarrollo del proyecto.
- Adquisición y activación del equipamiento tecnológico: asegurando la disponibilidad y puesta en marcha de los recursos necesarios para alcanzar los objetivos establecidos.

Hito 2 (Diseño de Servicios), dentro de las actividades a efectuar se encuentran las siguientes:

- Contexto: Ejecución de reuniones para contextualizar las necesidades específicas e identificar requerimientos funcionales y no funcionales que serán parte del servicio y

que permitan refinar el alcance, junto a priorizar los componentes y servicios requeridos para plasmar el cumplimiento de las expectativas de los clientes.

- Diseño arquitectónico: Establecimiento de una arquitectura que brinde y provea las capacidades requeridas dentro del servicio. Así mismo el diseño de modelos de prueba y versiones para garantizar la validación de la funcionalidad, usabilidad y operatividad del servicio.
- Módulos para la gestión de identidades: Creación y desarrollo del módulo de autenticación de usuarios, considerando el perfilamiento adecuado de usuarios, que brindan características de ciberseguridad desde el diseño y que permiten la usabilidad del producto.
- Módulo de administración: Desarrollo de la interfaz del administrador generando un adecuado menú de navegación que le permita consultar información de valor, aportando datos de relevancia para la toma de decisiones en la gestión técnica y operativa de los diferentes clientes.
- Módulo del cliente: Desarrollo de la interfaz del cliente con datos e información de interés sobre las amenazas, incidentes gestionados y niveles de riesgo de ciberseguridad de su compañía, de forma práctica y ejecutiva, ayudándolo a la toma de acción. Así mismo la información sobre la adopción, sensibilización y capacitación de los colaboradores en materia de ciberseguridad para su empresa.
- Validaciones: Pruebas funcionales que permitan verificar la usabilidad, función y entrega de valor para la compañía.

Hito 3 (Identificación y Análisis de Amenazas); *p*ara el desarrollo de esta actividad es necesaria la integración con servicios a través de Application Programming Interface (APIs).

Estas APIs se conectarán con plataformas externas que proporcionan datos clave, como indicadores de compromisos y alertas sobre amenazas cibernéticas, los cuales se integrarán directamente con nuestro servicio. En mi anterior corrección les mencione…No párrafos de menos de tres oraciones

Así se busca efectuar dos tareas específicas:

- Lograr identificar fuentes confiables de amenazas cibernéticas, centralizando los datos en un sistema para su análisis, correlación, explotación y segmentación de acuerdo a las tecnologías empleadas por los clientes.
- Activar la capacidad de integración que permita adicionar fuentes de relevancia para las empresas cliente y que mejoren la calidad de la data de amenazas, a fin de facilitar el análisis de la misma.

Hito 4 (Integración con Inteligencia Artificial en la Gestión de Amenazas); en esta actividad se busca incorporar el uso de Inteligencia Artificial para la gestión adecuada de las amenazas de ciberseguridad, identificando soluciones especializadas que mejoren los análisis a fin de lograr una ciberseguridad predictiva, así mismo crear y entrenar un modelo de Inteligencia Artificial para la simulación de remediaciones en activos de información con el objetivo de identificar, valorar el impacto y efectuar el control de riesgos de forma automática.

Hito 5 (Diseño de Servicios Personalizados); dentro de esta actividad se encuentran las siguientes subactividades:

- Establecer un alcance de servicio enfocado en las necesidades puntuales de cada compañía a fin de lograr efectividad en la atención.

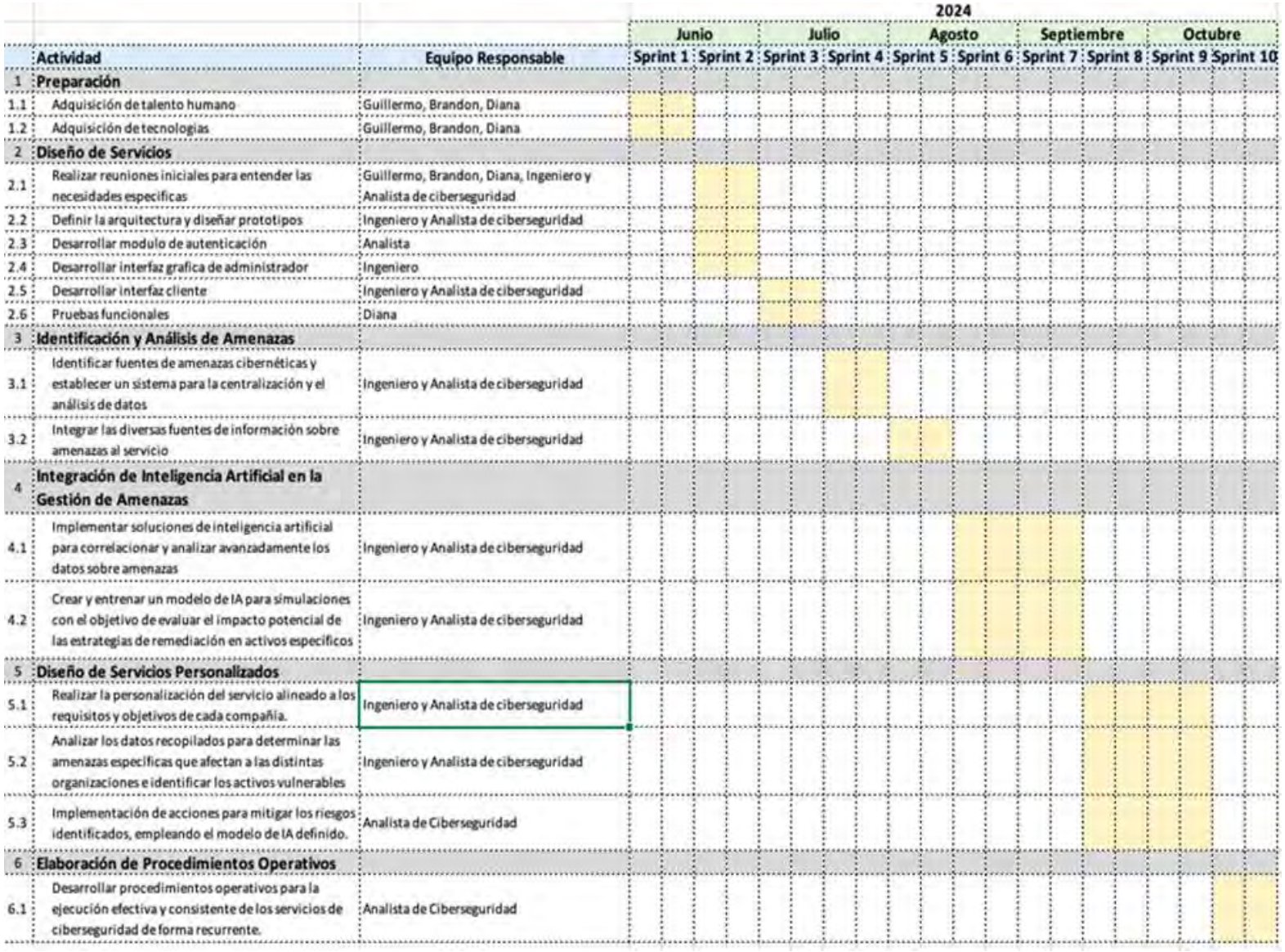
- En base a la cantidad de información que se correlaciona asociada a amenazas se debe efectuar una priorización orientada al impacto sobre los activos específicos de la compañía, considerando la relevancia y criticidad del activo para la misma.
- Mitigación de riesgos identificados y priorizados, usando el modelo de Inteligencia Artificial para el uso específico.

Hito 6 (Elaboración de Procedimientos Operativos); dentro de esta actividad se busca el establecimiento y desarrollo de los procedimientos para la operación, administración y mantenimiento efectivo de la solución de ciberseguridad, donde se garantice la gestión y continuidad de la misma para el éxito en la remediación de los riesgos observados.

Para asegurar una implementación exitosa, es crucial contar con un equipo que posea el conocimiento y la experiencia tecnológica requerida y que sea proactivo en la investigación en caso de desconocimiento. Aunque emplearemos una metodología ágil (SCRUM), esto no implica la ausencia de documentación. Las mejores prácticas de la industria sugieren que debe existir una documentación adecuada como base para la mejora continua y para garantizar que el equipo pueda actuar de manera organizada ante situaciones complejas, minimizando el riesgo de fallos para servicios tan críticos como los nuestros.

Figura 18

Plan de trabajo para la implementación de los servicios



			2024									
			Junio		Julio		Agosto		Septiembre		Octubre	
	Actividad	Equipo Responsable	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5	Sprint 6	Sprint 7	Sprint 8	Sprint 9	Sprint 10
1	**Preparación**											
1.1	Adquisición de talento humano	Guillermo, Brandon, Diana										
1.2	Adquisición de tecnologías	Guillermo, Brandon, Diana										
2	**Diseño de Servicios**											
2.1	Realizar reuniones iniciales para entender las necesidades especificas	Guillermo, Brandon, Diana, Ingeniero y Analista de ciberseguridad										
2.2	Definir la arquitectura y diseñar prototipos	Ingeniero y Analista de ciberseguridad										
2.3	Desarrollar modulo de autenticación	Analista										
2.4	Desarrollar interfaz grafica de administrador	Ingeniero										
2.5	Desarrollar interfaz cliente	Ingeniero y Analista de ciberseguridad										
2.6	Pruebas funcionales	Diana										
3	**Identificación y Análisis de Amenazas**											
3.1	Identificar fuentes de amenazas cibernéticas y establecer un sistema para la centralización y el análisis de datos	Ingeniero y Analista de ciberseguridad										
3.2	Integrar las diversas fuentes de información sobre amenazas al servicio	Ingeniero y Analista de ciberseguridad										
4	**Integración de Inteligencia Artificial en la Gestión de Amenazas**											
4.1	Implementar soluciones de inteligencia artificial para correlacionar y analizar avanzadamente los datos sobre amenazas	Ingeniero y Analista de ciberseguridad										
4.2	Crear y entrenar un modelo de IA para simulaciones con el objetivo de evaluar el impacto potencial de las estrategias de remediación en activos especificos	Ingeniero y Analista de ciberseguridad										
5	**Diseño de Servicios Personalizados**											
5.1	Realizar la personalización del servicio alineado a los requisitos y objetivos de cada compañía.	Ingeniero y Analista de ciberseguridad										
5.2	Analizar los datos recopilados para determinar las amenazas especificas que afectan a las distintas organizaciones e identificar los activos vulnerables	Ingeniero y Analista de ciberseguridad										
5.3	Implementación de acciones para mitigar los riesgos identificados, empleando el modelo de IA definido.	Analista de Ciberseguridad										
6	**Elaboración de Procedimientos Operativos**											
6.1	Desarrollar procedimientos operativos para la ejecución efectiva y consistente de los servicios de ciberseguridad de forma recurrente.	Analista de Ciberseguridad										

8.2. Conclusiones

En este trabajo hemos utilizado diversas metodologías y herramientas para evaluar la viabilidad técnica y económica del proyecto PYMESHIELD. Esta compañía tiene como objetivo reducir los riesgos cibernéticos derivados de la falta de concientización y de una gestión deficiente o ausente de amenazas cibernéticas. Además, el proyecto ha superado las expectativas en términos de deseabilidad y forma de abordar las preocupaciones de los diferentes sectores de las PYMES.

A pesar del aumento en la oferta de productos y servicios de ciberseguridad, nuestro servicio se distingue por su innovación, ya que utiliza inteligencia artificial para simular la probabilidad de que una compañía enfrente un riesgo y el impacto de remediar una vulnerabilidad, servicio que actualmente no existe en el mercado. Los resultados del proyecto demuestran que los servicios propuestos son viables y altamente efectivos para abordar las preocupaciones de las PYMES en torno a la ciberseguridad con costos accesibles para el sector. Desde el punto de vista financiero, la viabilidad del proyecto muestra un VAN de S/1.027.546 y una TIR de 67,02% en un escenario de crecimiento muy conservador.

8.3. Recomendaciones

Este trabajo de investigación subraya la importancia crítica de las micro, pequeñas y medianas empresas (PYMES) en la economía, destacando su contribución sustancial al Producto Interno Bruto (PIB). En vista de su relevancia económica, se recomienda que el gobierno y el sector privado se unan en el mejoramiento del ecosistema empresarial peruano a fin de facilitar la implementación de una estructura y regulaciones específicas que brinden apoyo robusto para fortalecer la infraestructura de ciberseguridad en este tipo de empresas. Se recomienda a las

PYMES la adopción de controles de ciberseguridad básicos que garanticen la protección continua de sus operaciones en un balance costo y beneficio respecto a la gestión de sus riesgos de ciberseguridad, Estableciendo medidas que no solo protejan los activos financieros de las PYMES, sino que también aseguren su sostenibilidad y resiliencia en el ámbito digital, contribuyendo con una buena economía.

Con los resultados de este proyecto, buscamos sensibilizar sobre el aumento de ataques informáticos y recomendamos la implementación de capacidades de ciberseguridad en las PYMES, con el fin de reducir los riesgos que podrían afectar su reputación y resiliencia operativa, teniendo en cuenta que las PYMES representan un 99,7% de la clasificación empresarial y contribuyen con cerca del 32% del PBI en el Perú.

Es recomendable que las PYMES adquieran productos y servicios tipo PYMESHIELD, que contribuyan con las capacidades de gestión de la ciberseguridad de sus compañías. Al ser un servicio tercerizado, que reducirá la carga operativa para las empresas, permitiéndoles enfocarse en su proceso de negocio principal. Además, este servicio se encargará de facilitar la protección de sus activos de información.

Referencias

Bolívar, U. A. (2011). *Observatorio de la PyME.* Recuperado de https://www.uasb.edu.ec/observatorio-pyme/wp-content/uploads/sites/6/2021/04/faq_53.pdf

Cabas, S. (27 de junio de 2023). *La creación de las Mipyme ha tenido una leve reducción de 4,7% en lo corrido de 2023.* Recuperado de https://www.larepublica.co/empresas/dia-de-las-microempresas-y-de-las-pequenas-y-medianas-empresas-en-colombia-se-han-creado-cerca-de-141-867-mipyme-en-2023-3645612

Calidad, I. N. (26 de octubre de 2023). *Inacal aprueba nueva Guía Peruana para implementar la gestión por procesos en las MIPYMES.* Recuperado de https://www.gob.pe/institucion/inacal/noticias/856910-inacal-aprueba-nueva-guia-peruana-para-implementar-la-gestion-por-procesos-en-las-mipymes

División de Evaluación Social de Inversiones. (2017, febrero). *Estimación del precio social del CO2*. Santiago. https://sni.gob.cl/storage/docs/Precio%20Social%20del%20CO2.pdf

Duchamp, S. (22 de marzo de 2023). *Transformación digital para MiPyMes.* Recuperado de https://news.microsoft.com/es-xl/pymes-peruanas-considera-que-transformacion-digital-impacta-su-negocio/

ECommerceDB. (2023). *eCommerce market in Peru*. https://ecommercedb.com/markets/pe/all

El Peruano. (2018, mayo 8). *El 63% de empresas peruanas usan software ilegal*. https://www.elperuano.pe/noticia/60693-el-63-de-empresas-peruanas-usa-software-ilegal

ESET. (2023). *Security Report Latinoamérica 2023.* Recuperado de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Fernández, R. (23 de febrero de 2024). *Ranking de países con mayor producto interior bruto (PIB) estimado de 2022 a 2028.* Recuperado de https://es.statista.com/estadisticas/600234/ranking-de-paises-con-el-producto-interior-bruto-pib-mas-alto-en/

Forum, W. E. (2022). *The Global Risks Report 2022 17th Edition - 95% cybersecurity issues traced to human error.* Recuperado de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Forum, W. E. (enero de 2023). *The Global Risks Report 2023 18th Edition.* Recuperado de https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Gestión. (10 de marzo de 2022). *E-commerce en Perú creció 55% en el 2021.* Recuperado de https://www.eleconomista.com.mx/empresas/E-commerce-en-Peru-crecio-55-en-el-2021-20220309-0127.html

Gestión. (2023, julio 19). *Ciberataques a pymes peruanas: La importancia de la ciberseguridad para las pymes y cómo evitar un ciberataque*. https://gestion.pe/economia/empresas/ciberataques-a-pymes-peruanas-la-importancia-de-la-cibersegurad-para-las-pymes-como-evitar-un-ciberataque-noticia/?ref=gesr

Gómez, A. (2023). *El futuro de una empresa está ligado al nivel de madurez de ciberseguridad que tengan*. CANVIA. https://elcomercio.pe/tecnologia/ciberseguridad/ciberseguridad-empresas-pueden-perder-desde-us-13-mil-hasta-mas-de-us-5-millones-por-ataque-ciberdelincuencia-malware-phishing-suplantacion-de-identidad-noticia/

Google. (s.f.). *Panorama actual de la Ciberseguridad en España.* Recuperado de Retos y oportunidades para el sector público y privado:

https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Gutiérrez, N. (17 de febrero de 2022). *30 estadísticas sobre seguridad informática*. Prey Project. https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Hernández, M. (22 de agosto de 2023). *Estos son los países de Latinoamérica con más ciberataques.* Recuperado de https://forbes.co/2023/08/22/tecnologia/estos-son-los-paises-de-latinoamerica-con-mas-ciberataques

Kaspersky. (s.f.). *Por qué las pequeñas empresas deben tomarse en serio la ciberseguridad.* Recuperado de https://latam.kaspersky.com/resource-center/preemptive-safety/small-business-security

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. (2011). *Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research.* Recuperado de https://link.springer.com/chapter/10.1007/978-3-642-20633-7_13

Lozano, I. (22 de abril de 2024). *Mypes logran ser proveedoras de la gran empresa en primeros 5 años.* Recuperado de https://servicios.noticiasperu.pe/medios/Recortes1/2024/04/22/2024-04-2200100300100405314_1_1.jpg

Lozano, V. (28 de junio de 2022). *INEI.* Recuperado de Unidades productivas afrontaron difícil coyuntura MYPES: https://www.inei.gob.pe/media/inei_en_los_medios/28-jun-el-peruano-8-9.pdf

Marshmclennan. (04 de abril de 2023). *Estudio de Riesgos para Pequeñas y Medianas Empresas.* Recuperado de https://www.marsh.com/mx/services/small-business-insurance/insights/small-and-medium-sized-companies-risk-study.html

Metalmecánicos, A. d. (07 de diciembre de 2022). *ASIMET.* Recuperado de Radiografía tributaria de las empresas en Chile: Las MIPYME representan el 79% del total, pero apenas el 12.8% de las ventas: https://www.asimet.cl/radiografia-tributaria-de-las-empresas-en-chile-las-mipyme-representan-el-79-del-total-pero-apenas-el-128-de-las-ventas/

NIST. (2023). *Cybersecurity Framework.* Recuperado de https://www.nist.gov/cyberframework

ONU. (s.f.). *Objetivo 16: Promover sociedades justas, pacíficas e inclusivas*. Recuperado de https://www.un.org/sustainabledevelopment/es/peace-justice/

ONU. (s.f.). *Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación*. Recuperado de https://www.un.org/sustainabledevelopment/es/infrastructure/

Pérez, C. (septiembre de 2019). *CIEN.* Recuperado de: https://www.cien.adexperu.org.pe/wp-content/uploads/2019/09/Comparacion-Internacional-del-aporte-de-las-MIPYMES-a-la-Economia-DT-2019-03.pdf

Peruano, E. (06 de mayo de 2023). *Mypes representan 21% del PBI y 99% del empleo formal.* Recuperado de https://www.elperuano.pe/noticia/211984-mypes-representan-21-del-pbi-y-99-del-empleo-formal

Peruano, E. (2023, julio 19). *Las pymes peruanas en la era digital*. https://www.elperuano.pe/noticia/213817-las-pymes-peruanas-en-la-era-digital

Peruano, E. (2023, julio 19). *Pymes en la mira de la ciberdelincuencia*. https://www.elperuano.pe/noticia/168541-pymes-en-la-mira-de-la-ciberdelincuencia

Peruano, E. (24 de diciembre de 2022). *Valor de la Unidad Impositiva Tributaria durante el año 2023.* Recuperado de https://busquedas.elperuano.pe/dispositivo/NL/2137588-1

Producción. (2022). *Las MIPYME en cifras 2021.* Ministerio de la producción.

Quispe, J. (23 de noviembre de 2023). *Pymes fueron las más afectadas por ciberataques en el 2023: los ataques más comunes.* Recuperado de https://gestion.pe/tecnologia/pymes-fueron-las-mas-afectadas-por-ciberataques-en-el-2023-por-que-empresas-peruanas-emprendimientos-negocios-noticia/?ref=gesr

Schwaber, K., & Sutherland, J. (noviembre de 2020). *La Guía Scrum.* Recuperado de La Guía Definitiva de Scrum: Las Reglas del Juego: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Spanish-European.pdf

Stats, I. W. (2023). *INTERNET USAGE STATISTICS.* Recuperado de The Internet Big Picture: https://www.internetworldstats.com/stats.htm

SUNAT. (14 de enero de 2024). *Tipos de empresa (Razón Social o Denominación).* Recuperado de https://www.gob.pe/254-tipos-de-empresa-razon-social-o-denominacion

SUNAT. (28 de mayo de 2021). Recuperado de https://www.sunat.gob.pe/legislacion/oficios/2021/informe-oficios/i057-2021-7T0000.pdf

Telefónica. (2023, julio 19). *52% de las pymes peruanas aumentaron sus ventas y productividad con la digitalización de Movistar Empresas*. https://telefonica.com.pe/52-pymes-peruanas-aumentaron-ventas-productividad-digitalizacion-movistar-empresas/

Yale University. (27 de enero de 2021). *Surge in digital activity has hidden environmental costs*. https://news.yale.edu/2021/01/27/surge-digital-activity-has-hidden-environmental-costs

Apéndice A: Encuesta para obtener Perfil de Usuario

I. Elaboración de la encuesta:

Plataforma**:** Se seleccionó Google Forms debido a que no representa un costo y por su facilidad de uso en la elaboración de encuestas.

II. Antes de la encuesta:

Confidencialidad: Se informó a los encuestados que la información recopilada sería anónima, especialmente debido a la naturaleza sensible de algunas preguntas, como si han experimentado incidentes de ciberseguridad. La sensibilidad de estas respuestas podría tener un impacto significativo en sus clientes o proveedores. Por esta razón, nos comprometimos a manejar toda la información de manera anónima para proteger la privacidad de los participantes.

III. Indicaciones generales:

Envío: Se distribuyó la encuesta a través de Whatsapp, para que el encuestado pudiera tener la información de manera rápida.

Tiempo: El tiempo para contestar la encuesta es de aproximadamente 10 minutos.

IV. Información de la encuesta:

Datos Generales: A continuación, presentamos la encuesta realizada. En esta sección, se incluyen preguntas orientadas a conocer mejor a nuestros usuarios, sin relación con aspectos tecnológicos.

1. ¿Cuál es su edad?
2. ¿Cuál es su género?
3. ¿Estado civil?
4. ¿Cuál es su formación educativa?

5. ¿Cómo pasa el tiempo libre?
6. ¿Cuál es su motivación para seguir adelante?
7. ¿Con cuál de las siguientes opciones se siente más identificado?
8. ¿Con cuál de las siguientes características se siente más identificado?

Sobre la PYME

9. ¿Cuál es su mayor preocupación de cara al futuro en cuanto a su empresa?
10. ¿Rubro del negocio?
11. ¿Cuál es el promedio de ventas que se han dado por canales digitales, página web, WhatsApp, Redes Sociales?
12. ¿Edad de la empresa?
13. ¿Cuáles son sus canales de venta actualmente?
14. ¿La mayoría de sus ingresos se realiza a través de las ventas en los canales digitales como la página web, WhatsApp y redes sociales?
15. ¿Cuántas personas trabajan dentro de la empresa?

Aspectos tecnológicos

16. ¿Cuánto es la inversión en tecnología en un periodo anual?
17. ¿Cuentan con computadoras? De ser el caso positivo: ¿Cuántos colaboradores tienen acceso a estas?

Sobre nuestro servicio

18. En los últimos 5 años, ¿fueron víctimas de ataques a su plataforma web, suplantación de identidad, hurto de información personal o cualquier otra actividad que se considere como ciberataque?

19. ¿Cuál de las siguientes alternativas considera que podría afectar más a su empresa en caso de un ciberataque?
20. ¿Considera que su empresa es vulnerable a ciberataques?
21. Estaría dispuesto a contratar un servicio de ciberseguridad. Elija un porcentaje:
22. Considerando que nuestros servicios de gestión de vulnerabilidades se aplican por equipo (servidor o computadora) y que realizamos seguimientos constantes de las actividades en tiempo real para prevenir y mitigar la materialización de riesgos, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características?
23. Considerando que ofrecemos un servicio de concientización en ciberseguridad para los colaboradores, que incluye capacitación regular y simulaciones de phishing para mejorar la seguridad de la empresa, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características por colaborador?
24. ¿Tiene su empresa un área de TI, que se encargue de la administración y la seguridad de los servicios en línea de la empresa?
25. ¿Has utilizado algún servicio especializado en seguridad cibernética para tu MYPE en el pasado?
26. ¿Has escuchado la propuesta de servicio de nuestra empresa, como un servicio especializado en ciberseguridad antes de completar esta encuesta?
27. En una escala del 1 al 5, ¿qué tan importante crees que es recibir servicios de una empresa de ciberseguridad?

28. ¿Consideras que nuestro producto ofrece un servicio especializado y de calidad en ciberseguridad para tu empresa?
29. ¿Qué tan informado/a estás sobre las ventajas que nuestro servicio te ofrece?
30. ¿Has utilizado nuestra plataforma para registrar la información de la empresa?
31. En una escala del 1 al 5, ¿qué tan satisfecho/a estás con la facilidad de uso de la plataforma para registrar a tu empresa y solicitar nuestros servicios? Siendo 1 la menor nota
32. ¿Recomendarías nuestro servicio de ciberseguridad a otros colegas suyos?

Tabla 24

Respuestas de las preguntas 1, 2, 3, 4, 5, 6, 7 y 8

No	Pregunta	Criterios de Respuesta	Resultado	Porcentaje	Análisis de resultados
1	¿Cuál es su edad?	20-35	3	15%	El 90% de los encuestados se encuentra en un rango de edad entre los 20 a 65 años.
		36-50	9	45%	
		51-65	6	30%	
		Más de 65	2	10%	
2	¿Cuál es su género?	Hombre	8	40%	La población encuestada se compone de un 60% de hombres y un 40% de mujeres.
		Mujer	12	60%	
3	¿Estado civil?	Soltero	6	30%	Respecto al estado civil de los consultados, un 65% son casados, 30% son solteros y 5% viudos.
		Casado	13	65%	
		Viudo	1	5%	
4	¿Cuál es su formación educativa?	Secundaria Completa	2	10%	El 70% tiene una formación educativa universitaria o superior, el 20% tiene una formación técnica y el 10% no tiene una formación educativa mayor a la de secundaria completa.
		Formación Técnica	4	20%	
		Educación Universitaria o Superior	14	70%	
5	¿Cómo pasa el tiempo libre?	Investigando	6	30%	Los encuestados indican que dentro de sus pasatiempos más
		Cursos	4	20%	

		Compartiendo con la familia	1	5%	comunes se encuentran, el de pasar tiempo con la familia, realizar actividades deportivas, organizar actividades para sus empleados, buscar información sobre las condiciones de su mercado y viajes de relacionamiento.
		Deportes	1	5%	
		No tengo tiempo libre	8	40%	
6	¿Cuál es su motivación para seguir adelante?	Mejorar la calidad de vida de su familia	0	0%	Nombran dentro de sus mayores motivadores el de mejorar la calidad de vida de su familia, hacer crecer a su empresa y a sus colaboradores.
		Crecimiento de la empresa y de sus colaboradores	0	0%	
		Crecimiento de sus colaboradores	0	0%	
7	¿Con cuál de las siguientes opciones se siente más identificado?	Soy una persona que se siente cómoda con el menor riesgo posible. Siempre trato de tener control de las cosas.	8	40%	El 60% de los encuestados se siente cómodo asumiendo riesgos y está dispuesto a aprovechar oportunidades de negocio de alto riesgo. Esto indica una mentalidad emprendedora y un apetito al riesgo.
		Soy una persona que es indiferente al riesgo. Trato de	0	0%	

		ser lo más neutral posible.			
		Soy una persona que se siente cómoda con los riesgos. Si encuentro una oportunidad de negocio de alto riesgo la tomo	12	60%	
8	¿Con cuál de las siguientes características se siente más identificado?	Conservador	2	10%	El 55% de encuestados consideró que la característica que más los identifica es la resiliencia, seguido por el 20% quienes se consideran a sí mismos como personas de familia, luego un 10% mantienen un estilo conservador, otro 10% se considera intuitivo y un 5% se describe como audaz.
		Resiliencia	11	55%	
		Audaz	1	5%	
		Familiar	4	20%	
		Intuitivo	2	10%	

Tabla 25

Respuestas de las preguntas 9, 10, 11, 12, 13, 14, 15, 16, 17 y 18

No	Pregunta	Criterios de Respuesta	Resultado	Porcentaje	Análisis de resultados
9	¿Cuál es su mayor preocupación de cara al futuro en cuanto a su empresa?	Continuidad	7	35%	Las principales preocupaciones están relacionadas a la continuidad y la adaptación de las compañías.
		Sostenibilidad	3	15%	
		Adaptación	6	30%	
		Innovación	4	20%	
10	¿Rubro del negocio?	Comercio minorista	5	25%	Los encuestados asociados a los rubros de negocio de consultoría empresarial y servicios de alimentación, representan un 35% cada uno, siendo los dos rubros una agrupación del 70%, los demás encuestados hacen parte del sector de comercio minorista con un 25% y salud y bienestar con un 5%.
		Consultoría empresarial	7	35%	
		Salud y bienestar	1	5%	
		Servicios de alimentación	7	35%	
11	¿Cuál es el promedio de ventas que se han dado por canales digitales, página web, WhatsApp, Redes Sociales?	Menos del 50%	7	35%	Se identificó que el 70% de las personas encuestadas realizan en sus empresas las ventas a través de canales digitales como páginas web, whatsapp y redes sociales en más del 50%. Por otro lado, el 30% de las empresas realiza menos del 50% de la venta de
		Más del 50%	13	65%	

					sus productos y/o servicios a través de canales digitales.
12	¿Edad de la empresa?	1 a 2	1	5%	El 70% de las empresas tiene más de 7 años en el mercado
		3 a 4	2	10%	
		5 a 6	3	15%	
		7 a 8	6	30%	
		9 a 10	8	40%	
13	¿Cuáles son sus canales de venta actualmente?	Virtual	0	0%	El 100% de las empresas utiliza canales digitales para la venta de productos o servicios
		Presencial	2	10%	
		Ambos	18	90%	
14	¿La mayoría de sus ingresos se realiza a través de las ventas en los canales digitales como la página web, WhatsApp y redes sociales?	Menos del 50%	6	30%	Más del 50% de los ingresos del 70% de las compañías se hace a través de canales digitales
		Más del 50%	14	70%	
16	¿Cuántas personas trabajan dentro de la empresa?	10 – 50	2	10%	El 90% de empresarios encuestados indica que el número de sus trabajadores se encuentra entre 51 y 100 colaboradores.
		51 - 100	18	90%	
		101 - 150	0	0%	

		151 - 200	0	0%	
15	¿Cuánto es la inversión en tecnología en un periodo anual?	Entre el 1% y 3% del presupuesto anual	18	90%	El 90% de las empresas tienen entre un 1% y un 3% del presupuesto total de la compañía asignado a tecnología.
		Entre el 3% y 5% del presupuesto anual	2	10%	
		Ninguno	0	0%	
17	¿Cuentan con computadoras? De ser el caso positivo: ¿Cuántos colaboradores tienen acceso a estas?	1 – 5	2	10%	El 65% de las personas encuestadas afirma contar con entre 11 y 30 computadoras que son empleadas por los colaboradores de sus empresas. Un 20% indica contar con entre 6 y 10 computadoras, mientras que el 10% cuenta con entre 1 y 5 computadoras, y solo un 5% cuenta con más de 30 computadoras para sus colaboradores.
		6 – 10	4	20%	
		11 – 20	6	30%	
		21 – 30	7	35%	
		Más de 30	1	5%	

Tabla 26

Respuestas de las preguntas 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31 y 32

No	Pregunta	Criterios de Respuesta	Resultado	Porcentaje	Análisis de resultados
18	En los últimos 5 años,	Si	16	80%	El 80% de los encuestados

	¿fueron víctimas o tuvieron algún intento de ataques a su plataforma web, suplantación de identidad, hurto de información personal o cualquier otra actividad que se considere como ciberataque?	No	4	20%	fueron víctimas de ataques cibernéticos o experimentaron intentos de ataque a sus empresas en los últimos cinco años. Entre los ataques más destacados se encuentran aquellos dirigidos a la plataforma web y casos de suplantación de identidad
19	¿Cuál de las siguientes alternativas considera que podría materializarse como el mayor impacto para su empresa en caso de un ciberataque?	Económico	7	35%	El 35% de los encuestados considera que el impacto en un ciberataque está relacionado con los aspectos económicos
		Reputacional	6	30%	
		Vulnerabilidad de información	2	10%	
		Continuidad del negocio	5	25%	
20	Considera que su empresa es vulnerable a ciberataques.	Computadores	10	50%	El 50% cree que sus computadoras son vulnerables a ciberataques, mientras que el otro 50% percibe otros posibles vectores de ataque.
		Servidores	2	10%	
		Dispositivos móviles de los empleados	1	5%	
		Correo corporativo (correos electrónicos con virus)	7	35%	

21	Estaría dispuesto a contratar un servicio de Ciberseguridad. Elija un porcentaje:	0% - 20%	1	5%	El 95% de las PYMES tiene entre un 60% y un 80% de probabilidad de contratar un servicio de ciberseguridad.
		20% - 40%	0	0%	
		40% - 60%	0	0%	
		60% - 80%	19	95%	
		80% - 100%	0	0%	
22	Considerando que nuestros servicios de gestión de vulnerabilidades se aplican por equipo (servidor o computadora) y que realizamos seguimientos constantes de las actividades en tiempo real para prevenir y mitigar la materialización de riesgos, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características?	S/150 - S/200	17	85%	El 85% de las compañías considera que un monto adecuado para el servicio de ciberseguridad por activo está entre S/150 y S/200.
		S/200 - S/250	2	10%	
		S/250 - S/300	1	5%	
		S/300 - S/350	0	0%	
		S/350 - S/400	0	0%	
23	Considerando que	S/20 - S/40	3	15%	El 70% de las compañías

	ofrecemos un servicio de concientización en ciberseguridad para los colaboradores, que incluye capacitación regular y simulaciones de phishing para mejorar la seguridad de la empresa, ¿cuál sería el monto adecuado que estaría dispuesto a pagar por un servicio de estas características por colaborador?	S/40 - S/60	14	70%	considera que un monto adecuado para el servicio de ciberseguridad por activo está entre S/40 y S/60.
		S/60 - S/80	3	15%	
		S/80 - S/100	0	0%	
		S/100 - S/120	0	0%	
24	¿Tiene su empresa un área de TI, que se encargue de la administración y la seguridad de los servicios en línea de la empresa?	Si	0	0%	El 100% de los encuestados respondió afirmativamente en cuanto a la existencia de un equipo de TI, sin embargo, aclararon que no se trata de un equipo totalmente dedicado, sino de una persona que desempeña múltiples roles dentro de la compañía.
		No	20	100%	
25	¿Has utilizado algún servicio especializado en seguridad	Si	18	90%	El 90% de los encuestados contestaron que sí han usado algún servicio
		No	2	10%	

	cibernética para tu PYME en el pasado?				personalizado.
26	¿Has escuchado la propuesta de servicio de nuestra empresa, como un servicio especializado en ciberseguridad antes de completar esta encuesta?	Si	20	100%	Todos los participantes de la encuesta fueron documentados sobre las características de nuestro servicio, previo a resolver las encuestas
		No	0	0%	
27	En una escala del 1 al 5, ¿qué tan importante crees que es recibir servicios de una empresa de ciberseguridad?	Si	17	85%	El 85% de las compañías considera que es importante recibir servicios de ciberseguridad
		No	3	15%	
28	¿Consideras que nuestro producto ofrece un servicio especializado y de calidad en ciberseguridad para tu empresa?	Si	18	90%	El 90% de los clientes considera que nuestro servicio es especializado y cumple con la calidad necesaria para sus empresas
		No	2	10%	
29	¿Qué tan informado/a estas sobre las ventajas que nuestro servicio te ofrece?	Bien	19	95%	El 95% de las personas comprendieron las ventajas de nuestro servicio
		Aún no tengo el contexto completo	1	5%	
30	¿Has utilizado nuestra	Si	16	80%	El 80% de los encuestados

	plataforma para registrar la información de la empresa?	No	4	20%	logró ingresar al prototipo de la aplicación
31	En una escala del 1 al 5, ¿qué tan satisfecho/a estás con la facilidad de uso de la plataforma para registrar a tu empresa y solicitar nuestros servicios? Siendo 1 la menor nota	1	0	0%	El 100% de los clientes estuvo satisfecho
		2	0	0%	
		3	0	0%	
		4	12	60%	
		5	8	40%	
32	¿Recomendarías nuestro servicio de ciberseguridad a otros colegas suyos?	Si	20	100%	El 100% recomendaría nuestro servicio
		No	0	0%	