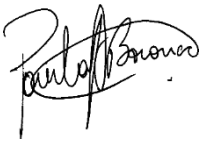
Plan de negocios de implementación de un servicio de *cibersoporte* para pymes en Lima

Trabajo de investigación presentado en satisfacción parcial de los requerimientos para obtener el grado de Maestro en Administración por:

Paula Anabella Borowiec



Kassandra Georgina Jaramillo Calvo

Jaime Gabriel Mendoza Butron

Christian Americo Perez Solis

MAESTRÍA EN ADMINISTRACIÓN A TIEMPO PARCIAL 71

Lima, 21 de septiembre de 2023

Version sustentada y corregida

INFORME DE ORIGINALIDAD

11%	11%	1%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	gestion.pe Fuente de Internet	1%
2	www.bcrp.gob.pe Fuente de Internet	<1%
3	www.coursehero.com Fuente de Internet	<1%
4	hdl.handle.net Fuente de Internet	<1%
5	repositorio.esan.edu.pe Fuente de Internet	<1%
6	peru21.pe Fuente de Internet	<1%
7	elcomercio.pe Fuente de Internet	<1%
8	prezi.com Fuente de Internet	<1%
9	Submitted to Universidad ESAN -- Escuela de Administración de Negocios para Graduados	<1%

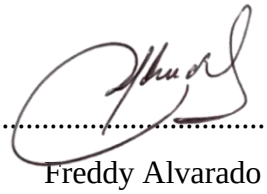
Este trabajo de investigación

Plan de negocios de implementación de un servicio de *cibersoporte* para pymes en Lima

ha sido aprobado.

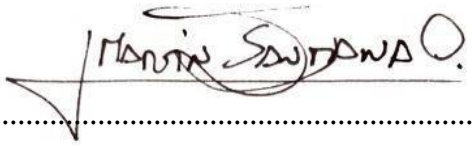
.....

Walter Martin Palomino Tamayo



.....

Freddy Alvarado Vargas



.....

Jorge Martín Santana Ormeño (Asesor)

Universidad
ESAN

A Dios, porque el día que salí de casa en Buenos Aires, prometió nunca dejarme, y acá sigue, cuidado mis pasos. A papá y mamá, que aun en la distancia me acompañan. A mi Santi, mi pequeño valiente, lleno de personalidad y alegría. Mi compañero en tantas clases y tareas, lleno de ternura y cariño. Que este logro sea un testimonio de compromiso y un legado de aprendizaje y lucha para que sepas que podés alcanzar tus sueños con esfuerzo, dedicación y sobre todo mucha fe. Con gratitud en mi corazón a mi equipo, por todo lo que representa este logro. Por haberme inspirado y apoyado en cada paso.

Paula Anabella Borowiec

Agradezco en primer lugar a Dios por haberme dado salud para concluir esta etapa satisfactoriamente y le pido que siga guiándome para tomar las mejores decisiones. Agradezco a mis seres llenos de luz, que tengo la suerte de llamar familia, mi hermano Jeffrey, mi mamá Giovanna, mi papá Miguel y mi gatito Vodki. Gracias por su apoyo constante, su motivación y esa tacita de café justa y necesaria. A mi enamorado, quien con su apoyo, comprensión y empuje me ha apoyado incondicionalmente en esta etapa. A mi ángel que llevo en el corazón, mi querido tío William, porque sé que ilumina mis pasos. A mi tío Rafael, quien siempre ha alimentado mi mente de curiosidad. A mi equipo y amigos, mi *Dream Team*, que se aventuraron a emprender esta historia conmigo que hoy llega a su epílogo. A mis amigos, sin cuyo apoyo y continuo aliento no habría podido mantener viva la esperanza de concluir esta maravillosa etapa.

Kassandra Georgina Jaramillo Calvo

A Dios, por su guía y bendición. A mis padres, Jaime y Charo, por su apoyo incondicional en todo sentido, así como su ejemplo profesional y personal, espero retribuirles el amor y la confianza siempre que tenga la oportunidad de hacerlo. A mis hermanos, Raúl y Desi, son el motor que mantienen unida a la familia y deseo que siempre puedan seguir su corazón porque llegarán lejos. A mi familia y amigos, que siempre estuvieron para alentarme. Al *Dream Team* de ESAN con el que viví todo este proceso siempre admirado de sus cualidades personales. A mi abuelita Berthita, quien me sigue guiando desde el cielo, y a mi novia Carla, a quien amo y ha sido mi motivación y cómplice durante esta experiencia.

Jaime Gabriel Mendoza Butrón

Dedico este logro con profundo agradecimiento a mis amados padres, Anita y Américo, cuyo amor inquebrantable y apoyo constante han sido una fuente de inspiración en mi vida. A mi querido hermano Ronaldo, por su aliento incondicional y apoyo invaluable en cada momento en que lo he necesitado. A mi amada enamorada, cuyo amor, motivación y esfuerzo han sido pilares fundamentales para alcanzar este logro. A mi querida abuelita Rosa, a quien agradezco su empuje constante y espero que pueda ver concluida esta etapa. A mi *Dream Team*, quienes han demostrado un esfuerzo incansable y una resiliencia admirable a lo largo de este proyecto.

Christian Américo Pérez Solís

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

PAULA ANABELLA BOROWIEC

Arquitecta colegiada con más de 13 años de experiencia en el sector inmobiliario, construcción, gestión y desarrollo de proyectos. Experiencia liderando áreas de proyectos a nivel corporativo en puestos gerenciales en empresas del sector inmobiliario y construcción. Amplia experiencia en gestión integral de proyectos bajo estándares del PMI durante todas las instancias de los proyectos, amplia experiencia trabajando con distintas entidades públicas para la obtención de permisos, licencias y categorizaciones. Manejo de presupuestos por proyectos y designación de recursos. Encargada de la toma de decisiones y presentación de resultados a la gerencia y directorio. Sólidos conocimientos en gestión de indicadores, control y reducción de costos, administración y proyección de presupuesto. Profesional enfocado en el cumplimiento de objetivos y mejora continua. Graduada de la Facultad de Arquitectura, Diseño y Urbanismo de la ciudad de Buenos Aires (FADU– UBA), colegiada en el Colegio de Arquitectos de Perú, con postgrado en gestión de proyectos.

EXPERIENCIA PROFESIONAL

LLOSA EDIFICACIONES S.A.C/ MIRAFLORES, PERÚ 10/2022 – Actualidad

Empresa inmobiliaria dedicada al desarrollo y gerencia de proyectos residenciales de alto estándar.

Gerencia de proyectos:

Principal objetivo dirigir el proceso de desarrollo de proyectos residenciales, a través de todas sus etapas, cuidando el plazo y costo objetivo y la entrega para operación de los mismos. Velar por el desarrollo de todas las etapas del proyecto manejo de plazo y presupuesto objetivo. Desarrollo y control de cronogramas de proyecto. Control y desarrollo de la construcción e implementación de los mismos. 1 persona a cargo y el equipo de obras, 15 personas.

Proyectos a cargo:

- S29 Etapa 1 / Magdalena del Mar / COSTO DE CONSTRUCCIÓN: S/36,000,000.00 + IGV

- S29 Etapa 2 / Magdalena del Mar / COSTO DE CONSTRUCCIÓN: S/20,000,000.00 + IGV

OPTIMIZA CONSTRUCCIÓN Y SERVICIOS S.A.C/ SAN ISIDRO, PERÚ 06/2022 – 10/2022

Empresa dedicada a la gerencia de proyectos, manejo de proyectos de alta complejidad en Banca Industria y Construcción. Remodelamos de oficinas y aprovechando eficientemente los espacios.

Gerencia de proyectos:

Principal objetivo dirigir el proceso de desarrollo de proyectos de implementación de proyectos especiales e híbridos de banca industria y construcción, a través de todas sus etapas, cuidando el plazo y costo objetivo y la entrega para operación de los mismos. Velar por el desarrollo de todas las etapas del proyecto manejo de Capex y presupuesto objetivo. Desarrollo y control de cronogramas de proyecto. Control y desarrollo de la construcción e implementación de los mismos. 3 personas a cargo.

Proyectos a cargo:

- Implementación de pisos gerenciales y directorio / Lima / COSTO DE CONSTRUCCIÓN: $3,000,000.00 + IGV
- Implementación pisos híbridos / Lima / COSTO DE CONSTRUCCIÓN: $ 3,947,368.42+ IGV

INVERSIONES Y RENTAS PERU S.A.C/ SAN ISIDRO, PERÚ 05/2016 – 12/2021

Empresa dedicada a la gestión y desarrollo inmobiliario de hoteles, oficias y otros desarrollos inmobiliarios. Subsidiaria de Inversiones y Rentas Ingevec SPA Chile, del grupo Ingevec, una de las empresas constructoras e inmobiliarias más grandes de Chile. https://www.ingevec.cl/empresas/index.html

Jefe / gerencia de proyectos:

Principal objetivo es dirigir el desarrollo de proyectos inmobiliarios hoteleros, supervisando todas las etapas, asegurando plazos, costos y entregas para la operación. Encargado de implementar y supervisar el área de proyectos, desde factibilidad hasta

licencias, construcción, optimizaciones y cierre. Coordinación con especialistas, obtención de servicios, licitación, control de costos y curva S. Responsable de contratos, estándares de seguridad, auditorías internas y cumplimiento de metas. Lidera equipos, entrega activos y presenta resultados a la dirección. 2 personas a cargo.

Proyectos a cargo:

- Hotel Ibis Rojo Trujillo (112 habitaciones) / Trujillo / COSTO DE CONSTRUCCIÓN: $7,772,637.37 + IGV
- Hotel Ibis Budget Miraflores (164 Habitaciones) / Miraflores / COSTO DE CONSTRUCCIÓN: $ 8,032,162.63 + IGV
- Hotel Ibis Styles San Isidro (184 Habitaciones) / San Isidro / COSTO DE CONSTRUCCIÓN: $ 11,232,036.32 + IGV
- Hotel Ibis Budget Centro de Lima (112 Habitaciones) / Miraflores / COSTO DE CONSTRUCCIÓN: $ 6,646,087.66 + IGV

Principales logros:

- 572 habitaciones entregadas y habilitadas
- Proyecto Trujillo:
    - Optimización de presupuesto en $1,091,074.61 + IGV
    - Obtención de anteproyecto en 3 semanas y obtención de licencia de construcción en 1 mes
- Proyecto Miraflores:
    - Optimización de presupuesto en $ 800,000.00 +IGV
    - Obtención de anteproyecto en 15 días y obtención de licencia de construcción en 1 mes.
    - Rectificación de linderos con resolución de controversias en 9 meses
    - Demolición de 4 casas de 3 pisos en 15 días, con obtención de licencia de demolición y permisos de uso de vías.
- Proyecto San Isidro:
    - Optimización de presupuesto en $ 1,000,000.00 +IGV
    - Obtención de anteproyecto en 15 días.
    - Implementación de metodología VDC en las etapas iniciales del proyecto para reducción de adicionales y RFI de obra.

- Proyecto Centro de Lima:
    - Obtención del anteproyecto en 8 días y licencia de construcción en 1 mes.

TEKTON DESARROLLOS INMOBILIARIOS S.A.C/ SAN ISIDRO, PERÚ 09/2015 – 04/2016

Empresa dedicada al desarrollo y construcción de proyectos inmobiliarios residenciales, oficinas etc con más de 15 años de experiencia en Perú, más de 770 unidades inmobiliarias gestionadas, 90.000 mt2 desarrollados, 25 proyectos inmobiliarios desarrollados. https://tekton.com.pe/

Jefe de proyectos

El principal objetivo es liderar el desarrollo y gestión de proyectos inmobiliarios en todas las etapas, asegurando plazos y costos. Implementación de procedimientos y políticas, manejo de perfiles económicos y propuestas de mejora para optimizar costos, plazos y calidad. Amplio conocimiento técnico, administrativo y legal. Responsable del cumplimiento de plazos, costos y calidad. Encargado de obtención de permisos, coordinación con entidades y obtención de servicios esenciales para los proyectos. 3 personas a cargo.

Proyectos a cargo:

- Residencial Valle Alto (72 departamentos) / El Tambo / Huancayo / ETAPA PREOPERATIVA
- Residencial Malecón Pazos (19 departamentos) / Barranco / Lima / ETAPA PREOPERATIVA
- Conjunto Habitacional Chiclayo (288 departamentos) / Chiclayo / Chiclayo / ETAPA PREOPERATIVA
- Conjunto Habitacional Piura (92 departamentos) / Urbanización Miraflores / Piura / ETAPA PREOPERATIVA

Principales logros:

- 471 departamentos desarrollados y gestionados.
- 5 licencias de construcción emitidas en un plazo de 2 meses previos al objetivo principal.

- Creación del área de proyectos.

CONSTRUCTORA RISCHMOLLER S.A.C/ SAN ISIDRO, PERÚ 06/2011-10/2015

Empresa dedicada al desarrollo, gestión integral y construcción de proyectos inmobiliarios. Cuenta con más de 20 proyectos desarrollados, ejecutados y entregados desde el 2003, año de su fundación. https://www.linkedin.com/company/constructora-einmobiliaria-rischmoller/about/

Jefe de área de arquitectura y proyectos

El objetivo es liderar el área de arquitectura para implementar proyectos inmobiliarios. Responsable de supervisar y gestionar proyectos, con especialización en sectores residenciales de alta gama y oficinas. Encargado de obtener permisos, licencias, desarrollar expedientes para entidades públicas, gestionar servicios y legalizar terrenos. Controla valorizaciones, curva S, utiliza *last planner* y gestiona aspectos económicos.

Proyectos a cargo:

- Residencial San Antonio (15442m2) / Miraflores / Lima / $ 11,800,000.00
- Residencial La Planicie / La Planicie / Lima / $ 1,600,000.00 + IGV
- Oficinas Basadre / San Isidro / Lima / GESTION INTEGRAL 2015
- Residencial Sterling (14054m2) / San Isidro / Lima / $ 12,500,000.00
- Santo Toribio (8534m2) / San Isidro / Lima / $10,500,000.00
- Parque Melitón Porras / Miraflores / Lima / $ 12,000,000.00

Principales logros:

- 50000m2 construidos y entregados
- Entrega de más de 300 departamentos a sus propietarios y atención de postventa en sectores A+, A y B.
- Reducción de las solicitudes de postventa en un 5% respecto de la gestión anterior.

GE EDIFICACIONES S.A.C / SAN BORJA, PERÚ 03/2011 – 05/2011

Jefe de área técnica

Funciones:

- Elaboración de metrados y presupuestos, valorizaciones.
- Desarrollo técnico para construcción de obra y especificaciones contractuales.
- Compatibilizaciones e interpretación de planos para su coordinación con especialistas.
- Programación de obra: suministro de materiales y equipos, y tareas del personal.
- Coordinación con ingenieros residentes, contratistas, subcontratistas y capataces.
- Desarrollo de diseño y modificaciones generadas según propuestas del cliente.

FORMACIÓN PROFESIONAL

UNIVERSIDAD ESAN (2021 - 2023)
MBA - Maestría en Administración de Negocios

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS - UPC – 02/2015-09/2015
Programa de Especialización en Gerencia de Proyectos (222 hs)

FACULTAD DE ARQUITECTURA DISEÑO Y URBANISMO (FADU-UBA) 2003 – 2009 Titulada de la carrera de Arquitectura Concluido 11.2009 - Titulada: 11.2011 - Colegiada: 05.2013

KASSANDRA GEORGINA JARAMILLO CALVO

Titulada de la carrera de Ingeniería de Sistemas de la Universidad de Lima con experiencia en rubros como Banca, Educación, Servicios Logísticos, Consumo Masivo, Agrícola, Energía, entre otros. Soy capaz de hallar soluciones basadas en tecnologías de la información, alto nivel de adaptabilidad, eficiencia, disposición para trabajar en equipo y bajo presión. Líder en la Comunidad de CISLATINAS - Mujeres en *Ciberseguridad*.

FORMACIÓN PROFESIONAL

GLOBAL BRIDGE CONNECTIONS

CISO **07/2022 – Actualidad**

- Dirección de los Programas de Seguridad de la Información, *Ciberseguridad*, Protección de Datos Personales y Continuidad del Negocio en pos del cumplimiento normativo.
- Establecimiento y supervisión de la Arquitectura de Seguridad de la Información y *Ciberseguridad* de la empresa.
- Gestión de riesgos y vulnerabilidades en proyectos estratégicos de seguridad, tecnología y del negocio y revisión de controles, así como gestión de incidentes y *ciberfraudes*.
- Gestión continua del Plan de Recuperación ante Desastres y el Plan de Continuidad del Negocio.
- Implementación y gestión de herramientas de *Ciberseguridad* en *cloud* y *on-premise*, monitoreos de *Ciberseguridad* SOC, aplicación de línea base de seguridad, *Ethical Hacking* y codificación segura (*OWASP*), *DevSecOps*, gestión de vulnerabilidades en los servicios de nube *GCP* y *AWS*, y securización de Microsoft 365.
- Liderazgo del proyecto de recertificación de *PCI-DSS*, revisión del cumplimiento de sus controles como de la ISO 27001:2013, 27002:2022, *NIST CSF* y la Ley N° 29733, implementación de la gestión documental y el programa de concientización, implementación de mesas ágiles bajo metodología *SCRUM*,

y la gestión de ciber riesgos en canales digitales y aplicación de controles para marketing digital.

ICPNA

Coordinador de Seguridad de la Información **04/2020 – 07/2022**

- Alineamiento de las iniciativas de seguridad con los programas empresariales y los objetivos comerciales asegurando los activos de información.
- Definición, implementación y mantenimiento del Plan Director en pos del cumplimiento del marco metodológico y normativo de Seguridad de la Información, *Ciberseguridad* y Privacidad.
- Establecimiento y supervisión de la Arquitectura de Seguridad de la Información que soporta a la Institución.
- Dirección y gestión de riesgos de Seguridad de la Información en proyectos estratégicos de seguridad, tecnología y negocio, así como gestión de incidentes dentro de la institución.
- Administración de controles de seguridad en *Azure* y *M365*.
- Participación en la revisión del cumplimiento de controles de la ISO 27001:2013, NIST CSF, Ley N° 29733 para proveedores y socios estratégicos de la institución y revisión de controles de *Ciberseguridad* para marketing digital.

SCOTIABANK

Analista Sr. de Seguridad de la Información **03/2019 – 03/2020**

- Administración del marco metodológico, normativo y el programa de concientización de Seguridad de la Información, *Ciberseguridad* y Privacidad para todas las empresas del grupo Scotiabank. Gestión de la implementación de controles regulatorios referentes a lineamientos de *frameworks* y estándares como *PCI-DSS, SWIFT Security, LPDP* y *Ciberseguridad*.
- Análisis y gestión de riesgos de seguridad de información a productos, procesos y canales, así como a nuevos proyectos y cambios significativos transversales a todas las empresas.
- Participación en la revisión del cumplimiento de controles tecnológicos de *PCI-DSS*, ISO 27001:2013 y *EMV* para proveedores y socios estratégicos del grupo

Scotiabank, y en la gestión de la implementación de planes de acción transversales al negocio producto de análisis de riesgos, inspecciones de seguridad, auditorías internas y externas, y gestión de riesgos para campañas de marketing digital.

COMPARTAMOS FINANCIERA

Analista Sr. de Seguridad de la Información **07/2018 – 02/2019**

- Gestión continua del marco metodológico, normativo y el programa de concientización de Seguridad de la Información, *Ciberseguridad* y *LPDP*.
- Evaluación e identificación de nuevos riesgos y controles relacionados a nuevos servicios, proyectos, sistemas y soluciones transversales a todas las áreas de la financiera.
- Implementación de los planes de acción producto de los análisis de riesgos e inspecciones de seguridad.
- Participación en proyectos internos del área de SI, así como en proyectos transversales del negocio, el más resaltante la Implementación del entorno *CDE* e Implementación de *PCI-DSS* y *EMV*, Reingeniería del Sistema de Gestión de Seguridad de la Información de acuerdo con el Plan *ASA – SBS* y la Adecuación a la Ley de Protección de Datos Personales.

CORPORACIÓN GRUPO ROMERO - EXCELLIA

Analista de Seguridad de la Información **06/2016 – 07/2018**

- Gestión y mantenimiento del Modelo de Autorizaciones SAP en los Proyectos de las 17 Empresas del Grupo Romero.
- Gestión de requerimientos de auditoría.
- Análisis de riesgos a proyectos e iniciativas de Grupo Romero.
- Gestión de incidentes de seguridad.
- Revisar, actualizar y elaborar normativas asociadas a las normas y políticas de Seguridad de la Información y Riesgos.
- Participación en proyectos internos del área de SI, así como en proyectos transversales del negocio, los más resaltantes son la implementación de *GRC* e Implementación de la Segregación de Funciones *SAP*.

ISEC DEL PERÚ - CLIENTE: INTERBANK

Consultor Jr. de Seguridad de la Información **07/2015 – 03/2016**

- Revisión de controles de Seguridad de la Información en los contratos del Banco y normativas asociadas a SI.
- Análisis de riesgos del negocio y a proyectos tecnológicos.
- Monitoreo de logs y generación de reportes para auditoría.
- Gestión y generación de llaves criptográficas para negocio. Administración de herramientas de Seguridad (*Antivirus, Antispam* y *Firewall*).
- Participación en el Proyecto de Migración de Datos de Tarjetas del Banco, el proyecto de Ley de Protección de Datos Personales y la implantación de la metodología de Análisis y Gestión de Riesgos.

FORMACIÓN PROFESIONAL

UNIVERSIDAD ESAN (2021 - Actualidad)
MBA - Maestría en Administración de Negocios

UNIVERSIDAD ESAN (2018)
Programa de Especialización en la Implementación de un SGSI, Óptica ISO 27001:2013

UNIVERSIDAD DE LIMA (2010 – 2023)
Ingeniería de Sistemas - Título obtenido en 2017

CERTIFICACIONES

ISO/IEC 31000:2018 GERENTE DE RIESGOS PECB Prime Profesional (2021)
LEAD CYBERSECURITY PROFESSIONAL CERTIFICATE (LCSPC) CertiProf (2020)
ISO/IEC 27001:2013 LÍDER IMPLEMENTADOR PECB Prime Profesional (2019)
ITIL FOUNDATIONS PeopleCert (2019)

JAIME GABRIEL MENDOZA BUTRÓN

Ingeniero Industrial y Comercial de la Universidad ESAN, con estudios en Francia por la Modalidad de Doble Grado, donde realicé estudios para la obtención del título de Bachiller en Ciencias de la Gestión Internacional. Soy una persona perseverante y capaz, con aptitudes y disposición a colaborar en el trabajo de equipo, así como de establecer adecuadas relaciones a todo nivel y accesible al diálogo.

EXPERIENCIA PROFESIONAL

BANCO DE CRÉDITO DEL PERÚ (BCP)

Sub-Gerente de Planeamiento y Gestión IT, Data y Ops 05/2023 – Actualidad

Responsable de apoyar en elaboración de Estrategia de TI, Data y Ops y seguimiento a evolución de entregables, gestión UDF: Solicitudes de fondeo y gestión del comité UDF, tableros de indicadores de la división, consolidación de QBR Memo de la División de TI y gestión de dependencias de iniciativas TI gestionadas por Project Managers

Sub-Gerente Adjunto de Mission Control 02/2022 – 05/2023

Responsable de la metodología de análisis financiero de iniciativas propuestas por la Arq. Empresarial para facilitar toma de decisiones, mantenimiento de ceremonias y artefactos que promuevan el alineamiento temprano de la Arq. Empresarial y visibilidad y mantenimiento del Roadmap de Arquitectura Tecnológica/Funcional con vista multianual

Sub-Gerente Adjunto de Eficiencia 11/2020 – 02/2022

Responsable de la elaboración de un Portafolio de Gestión, como miembro del Agile Porfolio Management, que permita asegurar la asignación óptima de los recursos para el cumplimiento de los objetivos estratégicos del banco. Control de Gestión de las Tribus, participando en la asesoría y soporte en la normativa, con visión estratégica.

Analista Senior de Eficiencia 02/2019 – 11/2020

Responsable de desafiar a la organización a través del análisis y cuestionamiento de las solicitudes de gastos e inversiones, previo a la presentación en instancias de aprobación.

Análisis, identificación y proposición de oportunidades de mejora de productividad dentro de las categorías de gasto asignadas.

CCR S.A.

Ejecutivo de cuentas de Modern Trade **09/2015 – 02/2019**

Responsable del manejo de cartera de clientes, compuesta por las principales Cadenas de Supermercados, Cadenas de Farmacias y Tiendas de Conveniencia. Análisis y evaluación de la información de las principales categorías del mercado y su comportamiento.

Ejecutivo de Nuevos Negocios **04/2015 – 09/2015**

Responsable de la actualización de sistemas de información gerenciales (SIG). Análisis de variables para cada categoría de acuerdo a la solicitud del cliente, estructuración y seguimiento de cotizaciones y facturación de las ventas, responsable de la supervisión y manejo de indicadores ISO.

Practicante Pre y Profesional Comercial **07/2014 – 04/2015**

Responsable del diseño y presentación de informes, sobre el comportamiento en el mercado de las principales cuentas de consumo masivo. Manejo de base de datos (QlikView) para el levantamiento y análisis de la información.

FORMACIÓN PROFESIONAL

UNIVERSIDAD ESAN (2021 – 2023)
MBA - Maestría en Administración de Negocios
UNIVERSIDAD ESAN (2017)
Titulado en Ingeniería Industrial y Comercial

SUP DE CO MONTPELLIER BUSINESS SCHOOL (2013-2014)
Bachiller en Ciencias de la Gestión Internacional

UNIVERSIDAD ESAN (2009-2014)
Bachiller en Ingeniería Industrial y Comercial

CHRISTIAN AMÉRICO PEREZ SOLIS

Especialista en la gestión de proyectos e iniciativas para el análisis, diseño y optimización de procesos y servicios, con enfoque en la digitalización y creación de valor. Con experiencia aplicando frameworks ágiles como Scrum, Lean Six Sigma, Design Thinking, Service Design y Kanban.

EXPERIENCIA PROFESIONAL

MOVENTICORP

Project Manager **01/2023 – 05/2023**

- Planificar las tareas, actividades y la asignación de recursos del proyecto. Coordinar las actividades del equipo de trabajo, asegurando que se cumplan los plazos y los entregables planificados.
- Gestionar el presupuesto del proyecto, asegurando que los recursos se usen forma eficiente y se cumpla con el presupuesto.
- Sostener una comunicación constante con los miembros del equipo y los stakeholders del proyecto.
- Monitorear el progreso del proyecto, identificando problemas y riesgos, y tomar medidas para mitigarlos.
- Gestionar cambios en el proyecto, actualizando el backlog, priorizando las nuevas tareas y actualizando el impacto en costos, tiempo y recursos.

MINISTERIO PUBLICO - FISCALIA DE LA NACION

Especialista de Procesos y Proyectos **01/2022 – 10/2022**

- Planificar los sprints y actividades del proyecto para el equipo asignado.
- Gestionar y monitorear el avance diario del equipo y los riesgos. Asesorar en el uso correcto de los formatos, estándares y metodologías por parte de todos los miembros del equipo.
- Realizar entrevistas a usuarios y clientes del proceso, para levantar información e identificar Insights sobre los procesos fiscales.
- Diagramar los procesos analizados a través de Customer Journey Maps, Service blueprints y Modelos BPMN.

- Recopilar y analizar información del desempeño de los procesos asignados. Identificar problemas en los procesos y causas raíz, realizando un análisis end-to-end.
- Idear propuestas de mejora en los procesos y realizar la validación con los usuarios y dueños del proceso.
- Presentar el Sprint Review a los stakeholders del proyecto.

NIUBIZ

Analista de Procesos y Canales Masivos **10/2020 – 01/2022**

- Monitorear e Identificar desviaciones en los KPI's Operativos y de Satisfacción, para identificar desviaciones y oportunidades de mejora. Extraer y analizar información de las aplicaciones utilizadas, a fin de identificar problemáticas en los productos y servicios.
- Proponer proyectos e iniciativas de mejora, con enfoque en la autogestión y experiencia del cliente.
- Planificar iniciativas y gestionalas con las áreas involucradas, monitoreando su oportuna implementación y despliegue.
- Participar en proyectos de lanzamiento de productos y campañas comerciales, planificando la gestión del frente de canales y postventa. Actualizar la documentación de procesos; Comunicar y capacitar sobre cambios en los procesos, para su despliegue hacia la Operación.

BANCO FALABELLA

Analista de Procesos **01/2020 – 07/2020**

- Realizar el análisis y diagnóstico de la situación actual (AS-IS) de los procesos.
- Participar en proyectos para el lanzamiento de nuevos productos, planificando las actividades en el frente de procesos.
- Realizar el Diseño To-Be de los procesos, en sesiones de creación con las áreas de negocio para asegurar una visión End-to-End del proceso. Asesorar en la definición de KPI's e identificación de Riesgos Operativos. Realizar el despliegue de mejoras y nuevos procesos hacia las áreas operativas

RIPLEY

Analista de Procesos Postventa **07/2018 – 01/2020**

- Monitorear los niveles de servicio y generar alertas oportunas a las áreas resolutoras.
- Analizar la información de los tickets de atención post-venta y las interacciones con los clientes, a fin de identificar insights.
- Diseñar y proponer iniciativas y proyectos, enfocados en la optimización de los procesos de Post Venta, en conjunto con las áreas de negocio, canales de atención y áreas operativas.
- Gestionar e implementar los proyectos asignados y llevar a cabo la gestión del cambio con los usuarios.
- Solicitar cambios en las aplicaciones de negocio orientados en eficiencia y automatización. Dar seguimiento al equipo TI para su ejecución.

CORPORACION GRUPO ROMERO

Analista de PMO y Auditoria **05/2014 – 05/2018**

- Monitorear los indicadores de desempeño de los proyectos asignados y gestionando desviaciones y controles de cambio.
- Gestionar la creación, mantenimiento y actualización de la documentación de gestión de proyectos.
- Capacitar a los miembros de equipos de proyectos (programadores, analistas, jefes) en la metodología y uso de aplicativos para la gestión.
- Proponer e implementar mejoras en la metodología y en los aplicativos de gestión de proyectos a través reuniones con usuarios clave.
- Participación en el Plan Anual de Auditoría (SOX), coordinando con los dueños de los procesos de Operaciones y Accesos, y los auditores externos.
- Realizar el seguimiento de los acuerdos y planes de acción para las iniciativas y proyectos asignados.
- Programar y ejecutar auditorías internas a los procesos de: Gestión de Iniciativas y proyectos, gestión de cambios, operaciones y Accesos.

FORMACIÓN PROFESIONAL

UNIVERSIDAD ESAN (2021 – 2023)

MBA - Maestría en Administración de Negocios

CENTRUM BUSINESS SCHOOL (2015 –2016)
Diplomado en Gestión de Procesos

UNIVERSIDAD MAYOR DE SAN MARCOS (2008 – 2012)
Ingeniería Industrial

CERTIFICACIONES

LEAN SIX SIGMA GREEN BELT
LIT - ASQ | 2020

SCRUM PRODUCT OWNERPROFESSIONAL (SPOPC)
Certiprof | 2020

DESIGN THINKING PROFESSIONALCERTIFIED (DTPC)®
Certiprof | 2020

RPA FUNDAMENTALS
Ui Path Academy| 2020

KANBAN FOUNDATIONS (KIKF)™
Kanban Institute - Certiprof | 2020

SCRUM MASTER CERTIFIED (SCM)® Scrumstudy | 2019

RESUMEN EJECUTIVO

Grado:	Maestro en Administración
Título de la tesis:	Plan de negocios de implementación de un servicio de *cibersoporte* para pymes en Lima
Autor(es):	Borowiec, Paula Anabella Jaramillo Calvo, Kassandra Georgina Mendoza Butrón, Jaime Gabriel Pérez Solis, Christian Américo

Resumen:

Las pymes, columna vertebral de la economía peruana, en los últimos tres años están adaptándose con rapidez, introduciendo canales digitales innovadores y migrando hacia infraestructuras en la nube para servir mejor a sus clientes y mantenerse a la vanguardia del mercado. Sin embargo, aquí yace una oportunidad dorada. A pesar de este avance tecnológico, muchas de estas pymes no han considerado plenamente las implicancias de la *ciberseguridad*, y la mayoría carece de un área especializada en este crucial aspecto. Razón por la cual, según un artículo de Mapfre, "Cada segundo se producen sólo en América Latina y el Caribe alrededor de 1.600 *ciberataques* a empresas" (Hernández, 2022).

La problemática tiene aristas interesantes por analizar como el desconocimiento de que las pymes son foco de *ciberataques*, puesto que la cifra creció en 152% en el 2022 en comparación con el 2021 (Gestión, 2022), y que al no invertir en *ciberseguridad* se encuentran más expuestas a incidentes (Conexión ESAN, 2023). Otro factor determinante es la complejidad, agresividad y sofisticación continua de los *ciberataques* con repercusiones financieras, sociales y reputacionales (Editorial Comercio, 2022). A su vez, no existe una variedad de opciones de servicios de c*iberseguridad* asequible que esté enfocada a la necesidad de las pymes.

Bajo la propuesta de valor: "*Tu Negocio, tu Pasión. La Ciberseguridad, nuestra Razón*", se propone un paquete asequible y enfocado a las necesidades de *ciberseguridad* de las pymes de Lima Metropolitana. Identificada la oportunidad y

definido el segmento al que se orientaran los esfuerzos de este plan de negocios mismo que se centra como *early adopters* en el sector construcción. Por consiguiente, se define como *MVP* un paquete de servicios de suscripción anual que constará de 49 licencias de una solución *endpoint* de *Bitdefender* diseñada para pymes, un servicio de respaldo y restauración en *Microsoft Azure* de 5TB para la seguridad de los datos, un programa de concientización para colaboradores y 10 horas mensuales de monitoreo y *cibersoporte* que incluye la atención de requerimientos e incidentes.

Como parte del análisis financiero, cuya proyección se realizó con un horizonte de 5 años, se obtiene un VAN (Valor actual neto) de S/ 450,628.00 y una TIR (Tasa interna de retorno) aproximada del 62%, respaldada por un plan estratégico robusto que considera un periodo preoperativo denominado año 0 donde se contempla realizar una inversión inicial de S/ 282,295.00. Estas consideraciones en conjunto demuestran que la propuesta planteada es viable al mismo tiempo que logra resolver una necesidad latente y un problema actual relevante para el segmento considerado.

Hoy se les presenta una oportunidad única para invertir en un futuro digital más seguro para las pymes del Perú. Juntos, hoy se pueden sentar las bases hacia la promoción de una cultura de *ciberseguridad* y crear un ecosistema digital resiliente para el corazón económico de la nación.

Resumen elaborado por los autores

CAPITULO 1 . INTRODUCCIÓN

En este primer capítulo se presentarán los antecedentes, el detalle de la problemática de la *ciberseguridad* en las pymes, así como también los objetivos generales y específicos del plan de negocios que se han considerado.

1.1. Antecedentes

El año 2021 representó un reto para el mundo entero debido a las medidas de confinamiento, sanidad y protección que se establecieron a raíz del COVID-19, así como por el abrupto cambio de trabajar de manera presencial a remota, y tener que adaptar los modelos de negocio a la nueva normalidad para abrazar lo digital. El esfuerzo de los equipos de tecnología detrás de estas medidas fue impresionante y en algunos casos incluyó el apoyo del equipo de *ciberseguridad* en empresas grandes; no obstante, para las pymes el escenario fue otro. Según el informe de la OEA: "[…] especialmente las pymes de la región […] carecen de una cultura digital tanto a nivel estratégico como operacional donde los beneficios de la digitalización a menudo se desconocen o no se comprenden completamente" (OEA, 2023).

Adicional a ello, durante el año 2022 el mundo ha sido testigo de una serie de *ciberincidentes*, uno más devastador que el otro, a empresas que forman parte de diferentes tipos de sectores. Empresas como Uber, Facebook, LinkedIn han sufrido *ciberincidentes* en los que sus datos confidenciales han sido expuestos; asimismo, la infraestructura crítica de países se ha visto afectada como es el caso del *ciberataque* al mayor oleoducto de Estados Unidos (Bing & Kelly, 2021) y el perpetrado contra redes de energía de Ucrania por parte de Rusia (BBC News Mundo, 2023).

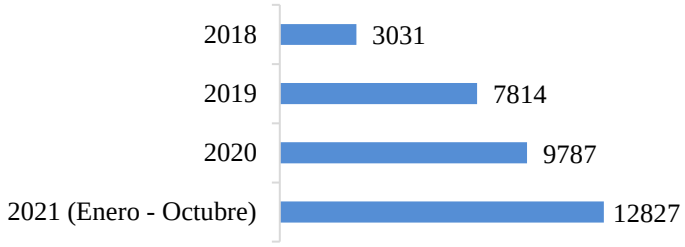
Incluso, las empresas que han sido víctimas de un *ciberataque* exitoso y han sobrevivido para contarlo han brindado luces sobre los resultados que recoge un reporte de IBM (2022), donde se afirma que: "El coste medio de una vulneración de datos fue de 4,35 millones de dólares en 2022, un récord histórico. [...] El 83 % de las organizaciones estudiadas han sufrido más de una vulneración de datos".

En ese sentido, resulta evidente que una pyme en Lima no puede asumir la cifra récord de 4,35 millones de dólares de costo promedio de un *ciberataque* exitoso, ni

siquiera un octavo de ello y seguir operando en el mercado peruano. Además, esto resulta preocupante si se observa que el Perú no ha sido ajeno a la ciberdelincuencia, dado que, según un informe de FortiGuard Labs de Fortinet: "Perú recibió 15 mil millones de intentos de *ciberataques* en 2022 [...]. Esto es un crecimiento del 35% frente a 2021" (El Comercio, 2023). Este crecimiento exponencial coloca en evidencia de que el país está convirtiéndose en un blanco atractivo para los ciberdelincuentes, y que lo mejor que puede efectuar una empresa grande, pequeña o mediana actualmente es adoptar medidas que la protejan de estos temidos *ciberataques*.

Cabe destacar que en los últimos cinco años se ha dado un crecimiento considerable en las denuncias por ciberdelitos, tal como lo muestra el gráfico debajo. El reporte de la Defensoría del Pueblo indica al respecto: "[…] las denuncias se cuadruplicaron entre los años 2018 y 2021, pasando de 3031 a 12,827. Si consideramos la tasa de ciberdelitos por cada 100 mil habitantes, esta pasó de 10% a 39%". Incluso, el mismo reporte afirma: "[…] Lima Metropolitana y Lima Provincias registraron un poco más de la mitad de las denuncias por ciberdelitos formuladas ante la Policía Nacional durante el 2021, con el 53% del total". (Castillo, 2023).

Ilustración 1.1 Denuncias de ciberdelitos ante la PNP



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP, 2023.
Elaboración: Defensoría del Pueblo.

1.2. Problemática

Las pymes desempeñan un papel crucial en la economía peruana, aportando significativamente al Producto Bruto Interno (PBI), generando empleo y fomentando el espíritu emprendedor. Según la CONFIEP: "[...] las pymes [...] generan empleo a más de 7 millones de compatriotas, es decir, el 45% de la PEA, lo que representa el 21% del

PBI nacional" (CONFIEP, 2021). Su aporte a la sociedad lo planteó el director general de Kaspersky América Latina: "Las pymes tienen un papel muy relevante en la economía de la región. Estas empresas administran datos, mueven dinero e información sensible que los *cibercriminales* pueden monetizar. Por ello, ha crecido el número de ataques contra este sector" (Comunidaria, 2023).

La situación actual de las pymes las tiene en una encrucijada, puesto que han migrado parte o toda su operación al ámbito digital, enfocándose solo en la actividad central de sus negocios y dejando de lado a la *ciberseguridad*. Tal como se planteó en un artículo de Conexión ESAN: "[…] la digitalización de sus procesos ha migrado la información física a medios informáticos y gran parte circula en el ciberespacio. Ello representa un riesgo operativo, comercial y económico" (Conexión ESAN, 2022).

Impulsadas inicialmente por la pandemia, cientos de miles de pymes han optado por emprender el camino hacia la digitalización incorporando algunas tecnologías. Según un estudio de Edelman para Microsoft, las pymes han invertido principalmente en tecnologías como: "[…] equipos de cómputo portátiles (85%), almacenamiento / computación en la nube (52%), software para videollamadas (46%) y software para trabajo colaborativo (41%)" (Microsoft, 2022).

Por ello, se definen tres problemas principales en relación con las pymes que están en proceso de transformación digital. En primer lugar, está el desconocimiento de las pymes que no han sufrido *ciberataques* y que creen erróneamente que eso solo les ocurre a las empresas grandes. Sin embargo, no han quedado relegadas del objetivo de los ciberdelincuentes: "El número de *ciberataques* a pymes este año creció en 152%, respecto al 2021" (Gestión, 2022). Esto deja a las pymes peruanas en una posición de riesgo, siendo potenciales blancos para este tipo de ataques que pueden llevar al robo de información, pérdida de ingresos y, en el peor de los casos, al cierre del negocio. Adicional a ello, también existe el desconocimiento de entender que basta con que un colaborador cuente con un celular, tableta, computadora y/o maquinaria conectada a internet, para que esta se convierta en un punto de entrada de amenazas como un *malware*, y de vulnerabilidades como la falta de una solución antivirus eficiente. Por lo

tanto, este desconocimiento de los riesgos asociados conlleva a no invertir en un responsable a tiempo completo para *ciberseguridad* o tercerizar el rol.

Por consiguiente, muchas de las pymes no cuentan con infraestructura de *ciberseguridad* básica, por lo que se convierten en un blanco fácil (Grange, 2023). Incluso, según un artículo de Conexión ESAN: "Este tipo de negocios se consideraba un blanco fácil por su poca inversión en […] herramientas de *ciberseguridad*, sin considerar su mayor exposición por el uso de equipamiento informático poco protegido, así como de software con sistemas operativos obsoletos y sin soporte *cibernético* (Conexión ESAN, 2022). En la misma línea, no se miden los riesgos ante un posible ciberincidente, como lo indica Gestión: "Muchas veces las pymes, en su afán por vender, reciben todo tipo de archivos y estos pueden contener links que terminan afectando su sistema informático" (Gestión, 2022).

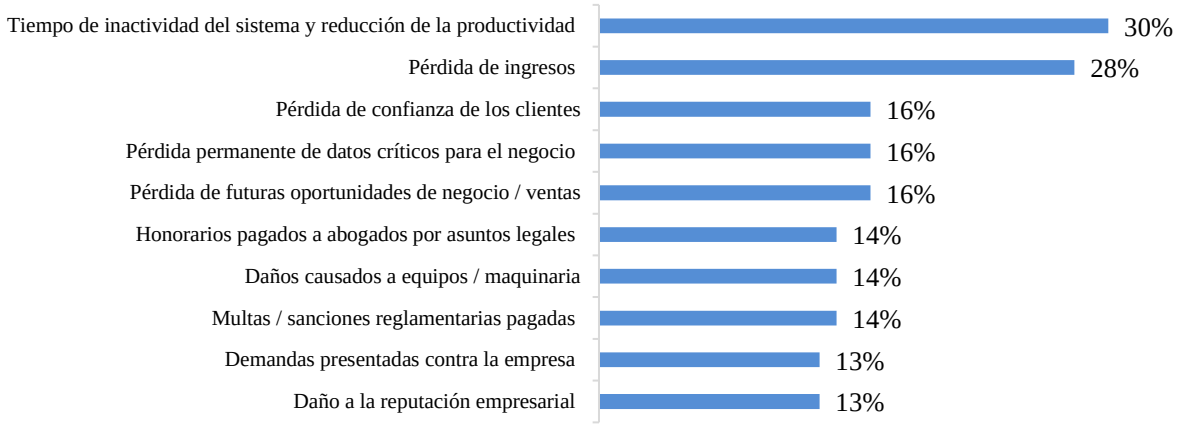
En segundo lugar, los *ciberataques* son más complejos y hasta mejor direccionados, como lo manifiesta un artículo: "[…] Se ha detectado un alto incremento de ataques direccionados a webs, e-mails, y sistemas" (Pymeseguros, 2022). Adicional a ello, de acuerdo con el diario El Comercio (2022): "Ahora los *ciberataques* son cada vez más agresivos, numerosos, sofisticados, específicos y dirigidos a los empleados, lo que está provocando un mayor daño financiero, social o reputacional". Entre los principales tipos de *ciberataques* se encuentra el *malware*, y sobre todo su variante más peligrosa, el *ransomware*; el *phishing* o la suplantación de identidad y los ataques de denegación de servicios (*DDoS*) (*Cloud* Security, 2022). Por lo tanto, las pymes al no contar con los especialistas ni herramientas necesarios no pueden hacer frente adecuadamente a este escenario de ataques continuos.

En tercer lugar, las pymes consideran que muchos de los servicios de *ciberseguridad* ofrecidos actualmente no los buscan captar como clientes, sino a empresas grandes. Por lo tanto, son servicios que no se ajustan a las necesidades y recursos que posee una empresa más pequeña y representan precios poco asequibles. Según un artículo: "Los precios de las soluciones de los proveedores de *ciberseguridad* superan sus bolsillos y se identifican como un desafío clave" (IT Digital Security, 2022). Además, cabe resaltar lo siguiente: "[…] no se identifica dentro de la cadena productiva

la necesidad de incorporar a los costos de la operación de los negocios la *ciberseguridad* como un factor estratégico" (MisiónPyme, 2023).

Asimismo, los impactos tangibles e intangibles de que se materialice un incidente de *ciberseguridad* dependen de la gravedad y la cantidad de activos de información críticos afectados de la pyme. Sin embargo, de acuerdo con un informe de Analysys Mason sobre retos de *ciberseguridad* para las pymes resaltan algunos impactos representados en la ilustración debajo. (Rebbeck, 2022).

Ilustración 1.2 Impactos en pymes que sufrieron un ciberataque



Fuente: Rebbeck, 2022
Elaboración: Autores de esta tesis.

Cabe resaltar que entre los principales impactos tangibles se encuentra la pérdida de ingresos, los costos asociados a la pérdida permanente de datos críticos para la pyme, los honorarios pagados a abogados por asuntos legales, las multas / sanciones reglamentarias pagadas y los costos asociados con demandas presentadas contra la pyme, los costos asociados a la recuperación de sistemas y redes, los costos de consultoría y concientización en ciberseguridad para los colaboradores, los costos asociados a la contratación de una empresa de seguridad forense, entre otros. Por otro lado, los principales impactos intangibles se encuentra el daño a la reputación empresarial, la pérdida de confianza en los clientes, las obligaciones legales y regulatorias más allá de multas y sanciones como enfrentar litigios e investigaciones, la interrupción de las operaciones de la pyme, la afectación al colaborador puesto que

afecta su productividad al ocasionar retrabajos para recuperar información perdida y genera desconfianza y miedo.

En base a la identificación de estas posibles consecuencias se verifica que las pymes necesitan del mejor servicio acotado que cubra sus condiciones mínimas, básicas y escalables de *ciberseguridad*. Por eso la solución está destinada al grupo empresarial que conforman las pymes, pero dado su masivo alcance se está partiendo de una primera fase, *MVP* (*minimum viable product*) por sector y su posterior escalamiento a otros sectores.

Por lo tanto, como parte de este *MVP*, se ha decidido acotar la solución a un sector en particular, siendo el sector de construcción e inmobiliaria la elección del estudio por dos razones principales y que serán desarrolladas a profundidad en los siguientes capítulos. La primera es que, según un informe de EY, el sector construcción e inmobiliaria ha acelerado su proceso de transformación digital en un 11%, empatando en el segundo puesto con el sector banca y seguros, lo cual lo lleva a invertir en *ciberseguridad*, como aliado estratégico. (Escudero, 2022). Mientras, que la segunda razón es que, según un informe de *ReliaQuest*, el sector construcción fue el más atacado por los *cibercriminales* con un promedio de 226 *ciberincidentes* anuales entre febrero del 2022 y 2023. Este mismo informe concluye al respecto:

"Es probable que la falta percibida de madurez, controles y herramientas de *ciberseguridad* junto con los impactos significativos de las interrupciones hayan colocado a […] construcción […] en el punto de mira de los actores de amenazas. Cada uno de estos sectores depende cada vez más de TI para impulsar la eficiencia, lo que los hace susceptibles a los ataques cibernéticos" (ReliaQuest, 2023).

De este modo, se requiere desarrollar un plan de negocios que ofrezca servicios de *ciberseguridad* para las pymes del sector construcción e inmobiliaria en Lima Metropolitana, generando una solución asequible y acorde a sus necesidades, que les permita elevar su nivel de *ciberseguridad* interno de manera confiable, escalable y sencilla, convirtiéndose en la empresa de referencia para este segmento y llegando a ser competitivos en el mercado.

1.3. Objetivos

1.3.1. Objetivo general

Evaluar la viabilidad de un plan de negocios para ofrecer servicios de *ciberseguridad* para las pymes en Lima Metropolitana, generando un paquete asequible y acorde a sus necesidades que les permita incrementar su nivel de *ciberseguridad* para hacer frente a posibles *ciberincidentes*.

1.3.2. Objetivos específicos

- Analizar la problemática que tienen las pymes en el sector construcción e inmobiliaria en términos de *ciberseguridad*, como parte del *MVP*, buscando conocer y entender las necesidades de los clientes potenciales.
- Desarrollar un modelo de negocio que ofrezca una cartera de servicios de *ciberseguridad* necesarios, asequibles y confiables para las pymes.
- Desarrollar las estrategias necesarias que respalden la propuesta de valor ofrecida a las pymes y sea sostenible en el tiempo.
- Diseñar un plan de marketing para promover y posicionar el servicio de *ciberseguridad* en el mercado.
- Elaborar el plan de operaciones que describa cómo se ejecutarán las tareas y los procesos de manera eficiente.
- Elaborar el plan organizacional que sea una guía clara y estructurada para el funcionamiento y desarrollo de la organización.
- Determinar si el plan de negocios es económicamente viable y si tiene el potencial de generar ganancias y retornar la inversión.

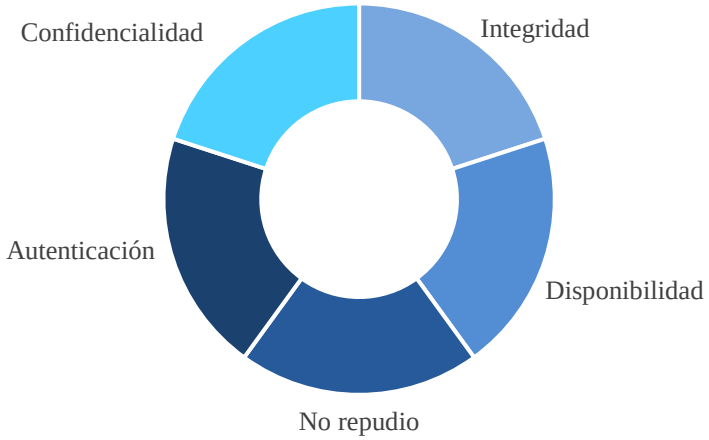
CAPITULO 2 . MARCO CONCEPTUAL

En el presente capítulo se exhibe la terminología propia de la *ciberseguridad*, vital para que el lector posea una base sólida que le permita apreciar los temas y argumentos a desarrollarse en los próximos capítulos.

2.1. La seguridad de la información y la *Ciberseguridad*

La seguridad de la información nació bajo la premisa de proteger la información de riesgos que puedan afectarla en sus diferentes formas y estados, ya sea que esté en modo físico, virtual, almacenado o en tránsito. Con este fin, la seguridad de la información se basa en la confidencialidad, integridad, disponibilidad, no repudio y autentificación de la información (ISO, 2022).

Ilustración 2.1 Principios de seguridad de la información



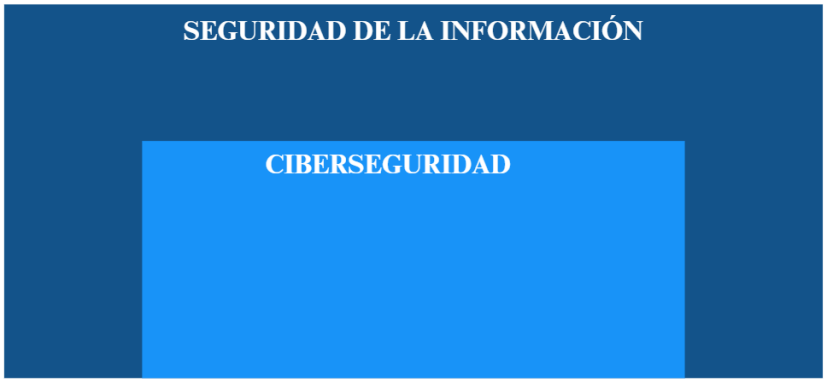
Fuente: ISO/IEC 27001, 2022.
Elaboración: Autores de esta tesis.

La confidencialidad es la propiedad de que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados. (ISO, 2020). En ese sentido, la confidencialidad busca prevenir principalmente el acceso no autorizado a datos sensibles, la divulgación de información a partes no autorizadas y las filtraciones de información, ya sean intencionales o accidentales, entre otros. Mientras que la integridad vela porque la información sea exacta y completa sin alteraciones con o sin intención. Por ello, la integridad busca prevenir principalmente que los datos no sean

modificados intencional o accidentalmente, y que los datos que se envían o reciben permanezcan sin cambios y lleguen a su destino como fueron enviados, entre otros. Asimismo, la disponibilidad es la propiedad de la información de ser accesible y utilizable a pedido por una entidad autorizada (ISO, 2020). Por lo tanto, la disponibilidad busca prevenir principalmente las interrupciones de acceso a sistemas o uso de la información, la recuperación rápida ante interrupciones por eventos inesperados, entre otros. Por otro lado, el no repudio busca demostrar la participación de las partes involucradas dentro de una comunicación o intercambio de información. La autentificación, por su parte, permite identificar a la persona, entidad o proceso que genera determinada información para evitar una suplantación de identidad (ISO, 2022).

Mientras que la *ciberseguridad* nació como parte de la seguridad de la información, ésta cada vez ha ido cobrando más fuerza y desarrollándose más con la migración hacia entornos digitales en el denominado ciberespacio. Las personas hacen uso diario del ciberespacio ya sea para enviar y recibir correos electrónicos, al usar el almacenamiento en nube, al hablar con amigos a través de plataformas de videollamadas, al estudiar *online* desde casa, descargar millones de aplicaciones en el celular, usar la *VPN*, *virtual private network*, para conectarnos a una red corporativa desde casa para trabajar en *laptops*, tabletas y celulares, al realizar compras por páginas web como Amazon, Mercado Libre, entre otros. Todas estas actividades cotidianas se hacen a través del ciberespacio, el cual se define como una red de infraestructuras de tecnología como el internet, redes, sistemas, procesadores y controladores integrados (NIST, 2021).

Ilustración 2.2 Relación entre la seguridad de la información y la *Ciberseguridad*



Fuente: ISO/IEC 27001, 2022.
Elaboración: Autores de esta tesis.

Según la ISO/IEC 27032:2023, la *ciberseguridad* se define como la protección de este ambiente del ciberespacio de *ciberriesgos* que pueden afectar a personas, sociedades, organizaciones y hasta naciones. (ISO, 2023). La *ciberseguridad* se ha visto beneficiada con el proceso de transformación digital que millones de empresas en el mundo han comenzado a emprender en los últimos años, en muchos casos debido a la pandemia del COVID-19. Asimismo, la transformación digital se define como un proceso a través del cual una empresa busca integrar la tecnología progresivamente en cada una de sus áreas, alterando por completo el modelo de negocio bajo el que ofrece valor a sus clientes y la cultura organizacional (McKinsey & Company, 2023). Las empresas pequeñas y medianas del país no han podido afrontar en sí una transformación digital, pero sí una digitalización acelerada, que se podría definir como la simple incorporación de tecnología en algún área de la empresa (Accenture, 2023). Como parte de esta digitalización, muchas pymes han mirado hacia los servicios de computación en la nube, es decir, servicios, aplicaciones y procesos que residen en la nube y a los que se puede conectar uno remotamente.

2.2. El *cibercrimen*

La aparición del ciberespacio y la digitalización acelerada, si bien han traído consigo que se cuente con información en segundos y han interconectado al mundo entero entre sí, también han originado la aparición de un nuevo tipo de crimen denominado *cibercrimen* o *ciberdelito*.

El *cibercrimen* es toda actividad de tipo criminal que está relacionada con servicios y aplicaciones del ciberespacio que se usen o sean blanco de un crimen, ya sea utilizando una computadora o el Internet («Glossary | NIST», 2019). Al ciberdelincuente que comete un *cibercrimen* se le denomina hacker, quien intenta tener acceso a sistemas y redes sin autorización a través de *ciberataques* para obtener dinero o datos confidenciales para vender («Glossary | NIST», 2019). Los *ciberataques* pueden ser de diversos tipos y buscan explotar diferentes componentes de un sistema y/o aplicación.

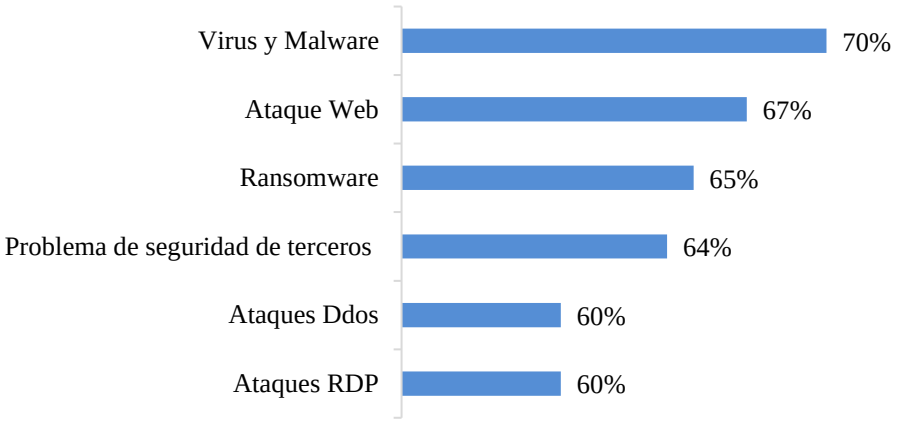
Si los *ciberataques* son exitosos se convierten en *ciberincidentes* que pueden perjudicar a las empresas de diversas formas. Un tipo de *ciberincidente* común es el

denominado brecha de datos, el cual IBM (2022) lo define como: “todo incidente de seguridad que resulta en el acceso no autorizado a información confidencial”.

2.3. Los *ciberataques* más comunes

De acuerdo con el reporte de ESET sobre la *ciberseguridad* y las empresas pequeñas y medianas en el 2022, se evidenció que los fundadores y ejecutivos son conscientes de las amenazas y riesgos que trae consigo la *ciberseguridad*, sin embargo, no cuentan con las suficientes capacidades para poder hacerles frente. Entre los principales *ciberataques* que enfrentan está el virus y *malware*, los ataques web en sus diferentes variantes, el *ransomware*, los problemas de seguridad que derivan de proveedores, los ataques *DDoS*, entre otros. (ESET, 2022).

Ilustración 2.3 Reporte – *Ciberataques* más comunes hacia las pymes



Fuente: ESET, 2022.
Elaboración: Autores de esta tesis.

El *ciberataque* que más aqueja a las pymes es el *malware*, el cual es un término utilizado para describir software malicioso diseñado para dañar o comprometer sistemas informáticos, redes o dispositivos (ISO, 2023). El *malware* puede ser utilizado para distintos propósitos maliciosos, como robo de información, espionaje, secuestro de datos, daño a sistemas informáticos, fraudes financieros, entre otros. Mientras que el virus busca dañar archivos, corromper datos o causar errores en el funcionamiento de un sistema, suele adjuntarse a un archivo o programa legítimo existente. El *malware* se diferencia del virus porque pueden distribuirse a través de diferentes medios como sitios

web, correos electrónicos, anuncios maliciosos, dispositivos USB infectados y vulnerabilidades propias de un software.

El segundo *ciberataque* son los ataques web, entre los cuales resaltan el *phishing*, ataques de inyección de código *SQL* y ataques de fuerza bruta. El *phishing*, el cual es un correo electrónico o mensaje engañoso vía mensaje de texto, redes sociales, código *QR* que parece legítimo y que busca que la víctima tome medidas que podrían comprometer tanto su computadora como la red de la empresa y revelar o robar información confidencial («Glossary | NIST», 2019). Los ataques de inyección de código *SQL* busca la inserción de código *SQL* a través de los datos de entrada del cliente a la aplicación que puede leer datos confidenciales de la base de datos, modificar datos, ejecutar operaciones, recuperar el contenido de un archivo, entre otros. (OWASP, 2023). Los ataques de fuerza bruta son: "[…] Un intento de descifrar una contraseña o nombre de usuario, de buscar una página web oculta o de descubrir la clave utilizada para cifrar un mensaje, que consiste en aplicar el método de prueba y error con la esperanza de dar con la combinación correcta finalmente" (Kaspersky, 2023).

En tercer lugar, una de las variantes más peligrosas y comunes del *malware* es el *ransomware*, el cual secuestra la información almacenada en un dispositivo como computadora, tableta o celular, la cifra (volverla indescifrable) y amenaza con destruirla si es que no se realiza un pago a cambio en bitcoins («Glossary | NIST», 2019). El *ransomware* ha ido perfeccionándose cada vez más y ahora es desarrollado por organizaciones de ciberdelincuentes que lo pueden crear al gusto del hacker.

El cuarto *ciberataque* son los problemas que derivan de la seguridad de los proveedores, dado que puede ocurrir que a través de terceros que cuentan con acceso no autorizado a uno o más activos o la red y se aprovechan de eso de manera accidental o adrede. Incluso, los proveedores pueden ser víctimas de *ciberataques* y brechas de datos que pueden afectar la información y servicios de la empresa cliente exponiendo datos confidenciales.

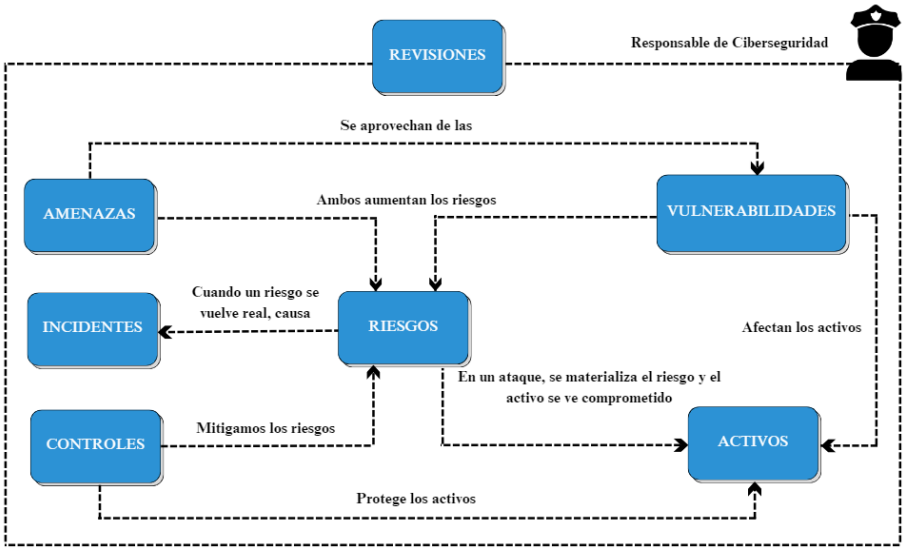
El quinto *ciberataque* es el ataque *DDoS*, el cual busca enviar varias solicitudes en segundos a una plataforma o página web para desbordar su capacidad y evitar que funcione correctamente o hacer que deje de funcionar (Spiceworks, 2022). Por lo que

su objetivo es agotar los recursos del servidor o la red objetivo hasta el punto en que no pueda atender solicitudes legítimas de usuarios reales. Esto ocasiona que los servicios en línea se vuelvan lentos o inaccesibles, ocasionando pérdidas económicas y afectando la reputación de las pymes.

2.4. La gestión de la *Ciberseguridad*

De acuerdo con la ISO/IEC 27000:2018, con el fin de evitar ser presa de *ciberataques*, la *ciberseguridad* inicia con la identificación de activos digitales, los cuales aportan valor a la empresa como la información, software, hardware, servicios, entre otros. Las partes interesadas de la empresa son responsables de valorar los activos en base a la disponibilidad, integridad y confidencialidad. Los activos cuentan con vulnerabilidades que son debilidades inherentes que pueden ser explotadas por una o más amenazas, las cuales constituyen una causa potencial de un incidente que puede dañar un sistema o hasta una empresa. Por lo que la probabilidad de que una amenaza explote una vulnerabilidad de un activo y perjudique a una empresa es un riesgo. A continuación, se obtiene el nivel del riesgo para cada activo si se multiplica la probabilidad de que ocurra con el nivel de impacto que tendría para la empresa. Los riesgos, si es que se llegan a materializar, pueden comprometer un activo y ocasionar incidentes que afecten a la empresa. Sin embargo, si se implementan controles, conjunto de acciones priorizadas que son efectivas para mitigar la materialización de un riesgo, debidamente sobre los activos identificados se mitiga también la ocurrencia de incidentes. El responsable de *ciberseguridad* es quien efectúa periódicamente las revisiones necesarias para validar que los controles son efectivos y mitigan que los riesgos se conviertan en incidentes. (ISO, 2022).

Ilustración 2.4 Diagrama resumen de las relaciones entre conceptos en la gestión de *Ciberseguridad*



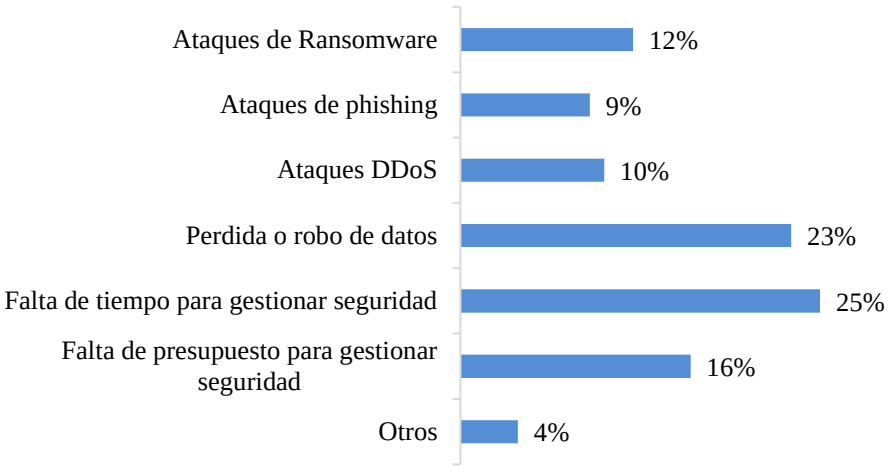
Fuente: ISO/IEC 27001, 2022.
Elaboración: Autores de esta tesis.

Por ello, la gestión de riesgos de *ciberseguridad* es vital y debe ser transversal a todas las áreas del negocio porque permite identificar, evaluar el nivel y aplicar controles para mitigar los riesgos que se identifiquen por activo.

2.5. La *Ciberseguridad* en las pymes

A nivel mundial, las empresas pequeñas y medianas están orientando sus esfuerzos a transformar sus negocios a través de integrar progresivamente lo digital a su operativa diaria. Según un reporte de Digital Ocean sobre la *ciberseguridad* de las pymes en el 2023, las cuatro principales preocupaciones de los fundadores y ejecutivos de empresas que pertenecen a este estrato son la falta de tiempo para gestionar la seguridad, el robo o pérdida de datos y la falta de presupuesto para gestionar la seguridad y los ataques de *ransomware*, tal como se aprecia en la ilustración debajo. (Digital Ocean, 2023).

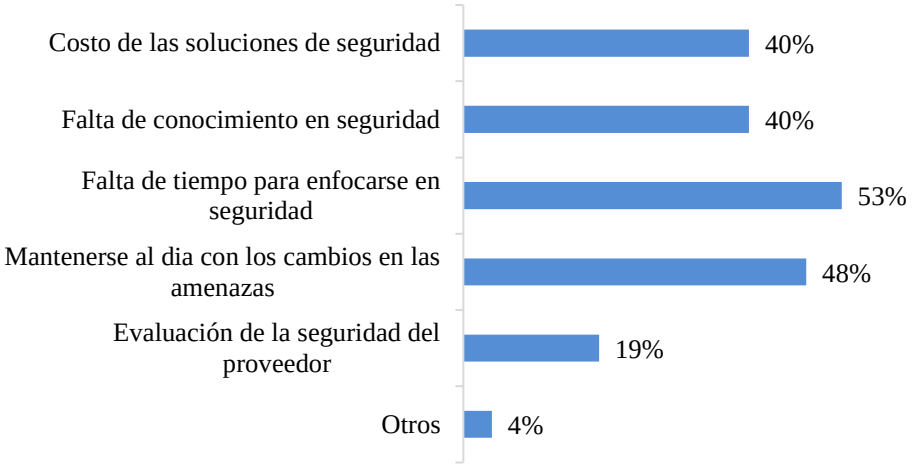
Ilustración 2.5 Encuesta – Preocupaciones relacionadas con seguridad



Fuente: Digital Ocean, 2023.
Elaboración: Autores de esta tesis.

Este mismo reporte evidenció que las pymes enfrentan grandes retos para lograr asegurarse mínimamente, entre ellos los fundadores y ejecutivos resaltaron cuatro razones principales como la falta de tiempo para concentrarse en la seguridad, el mantenerse al día con los cambios continuos en las amenazas, el costo de las soluciones de seguridad y la falta de conocimiento de seguridad. (Digital Ocean, 2023). La *ciberseguridad* es un tema en el que las pymes del mundo, y en este caso de Lima Metropolitana, deben comenzar a prestar atención, puesto que puede comprometer seriamente su futuro.

Ilustración 2.6 Encuesta – Retos para asegurar una pyme



Fuente: Digital Ocean, 2023.

Elaboración: Autores de esta tesis.

2.6. Conclusiones del capítulo

Este segundo capítulo abordó los conceptos necesarios para profundizar en la presente investigación, se partió desde la diferencia entre la seguridad de la información y la *ciberseguridad* delimitada por el ciberespacio, siendo esta última fundamental para proteger los activos digitales. El *cibercrimen* continúa evolucionando y si es exitoso se convierte en un *ciberataque* como un virus, *malware*, *ransomware*, ataques web que incluyen el *phishing*, ataques de inyección de código *SQL* y ataques de fuerza bruta, y problemas de seguridad que emanan de proveedores potenciando las vulnerabilidades existentes. Para hacer frente a estas amenazas se analiza el riesgo considerando la probabilidad de ocurrencia y el impacto con las partes interesadas a través de una gestión de *ciberseguridad* efectiva estableciendo controles apropiados y evaluándolos. El responsable de *ciberseguridad* juega un papel crucial al establecer las estrategias necesarias para prevenir y mitigar la materialización de un incidente.

La *ciberseguridad* es un aspecto importante que es una preocupación constante en las pymes del mundo, muchas de ellas han sufrido las consecuencias de un incidente, las pymes de Lima no deberían esperar a convertirse en víctimas para invertir en ella.

CAPITULO 3 . ANÁLISIS DEL MARCO CONTEXTUAL

En el presente capítulo se presenta el análisis del macroentorno para las pymes y el análisis de la industria de la *ciberseguridad* para este sector.

3.1. Análisis del Macroentorno

El análisis del macroentorno se llevó a cabo empleando el análisis PESTEL, el cual permitió evaluar los factores que afectan a las pymes, abarcando aspectos políticos, económicos, socioculturales, tecnológicos y legales.

3.1.1. Factor político

En los últimos 6 años, el Perú ha experimentado una gran agitación política, con cambios frecuentes en la presidencia y el Congreso. El entorno político del país ha presentado etapas continuas de inestabilidad, desde cambios en el gabinete ministerial como una serie de presidentes (Infobae, 2022).

Esta situación ha llevado a una gran incertidumbre política y económica, que puede y ha afectado negativamente a las pymes. “[…] una crisis política provoca que crezca la angustia entre los ciudadanos ante la problemática no de saber qué va a ocurrir, y reducen su consumo. De este modo, se afecta la economía, al reducir las ventas y los beneficios de las empresas” (Tiempo Minero, 2022).

Además, la inestabilidad política compromete la capacidad de anticipar la dirección del país, lo que a su vez disminuye la claridad para tomar decisiones de inversión. Esta claridad es crucial para generar empleos de alta calidad (Castillo, 2020).

La incertidumbre política también conlleva a un empeoramiento de los recursos económicos internos. A medida que la situación se torna más incierta, los inversores extranjeros reaccionan con mayor ansiedad, lo que impacta negativamente en los gastos relacionados con la financiación, tanto en el ámbito público como en el privado (Castillo, 2020).

Se puede deducir que, si el entorno político del país no logra alcanzar una estabilidad adecuada, las pymes, las cuales dependen de un flujo constante de ventas locales, se verán afectadas si sus clientes deciden recortar sus gastos de compra.

Asimismo, las huelgas, protestas o bloqueos como producto de la inestabilidad, pueden interrumpir las cadenas de suministro, dado que las pymes no tienen capacidad de almacenar mucho inventario de materiales y afectan la seguridad de los trabajadores que se desplazan.

3.1.2. Factor económico

La inestabilidad política de fines del año 2022 hasta fines de enero del año 2023 afectó la economía. De acuerdo con el Informe Macroeconómico del I Trimestre de 2023: "[…] La actividad económica se contrajo 0,4 por ciento en el primer trimestre de 2023, tras dos años de crecimiento continuo". En el periodo se observó: (i) caída de la inversión privada en un contexto de conflictos sociales y ausencia de nuevos megaproyectos mineros; (ii) menor dinamismo del consumo privado, afectado por la aún elevada inflación y el cierre temporal de mercados y restricciones al tránsito de personas y a la circulación de bienes en algunas áreas del territorio nacional; (iii) caída del gasto público tras el retiro del gasto asociado a la emergencia sanitaria y el impacto en la ejecución del primer año de mandato de las nuevas autoridades subnacionales; y (iv) caída de las exportaciones tradicionales, principalmente de los sectores minería y agropecuario" (BCRP, 2023).

Ante un escenario de inestabilidad económica, las pymes podrían verse afectadas por la falta de capital para operar y crecer de parte de las instituciones financieras, dado que estas estarían reacias a ofrecer préstamos o refinanciar deudas existentes. También, ocasiona aumentos en los precios de los bienes y servicios por la inflación o a la escasez, y esto perjudica a las pymes que no pueden absorber estos costos adicionales o ni trasladarlos a sus clientes. Muchas pymes dependen de la importación y exportación de materiales y acabados, que ante una devaluación de la moneda local puede afectar sus costos e ingresos al volverlos más volátiles. Además, son altamente sensibles a las fluctuaciones económicas porque al ser pequeñas y medianas empresas suelen tener menos reservas financieras.

Adicionalmente, aparte de la mencionada situación de inestabilidad, el acceso al financiamiento ha constituido una persistente dificultad para las pymes en el Perú. Este factor tiene el potencial de incidir en la sostenibilidad a largo plazo de estas empresas, ya que, con el fin de mantener su competitividad, deben cumplir ciertos requisitos. La disponibilidad de capital resulta esencial para poder invertir en áreas cruciales como tecnología, estrategias de marketing y el crecimiento del negocio (Gestión, 2023).

En relación con este desafío, durante el periodo de la pandemia se aplicó el programa Reactiva Perú, el cual buscaba asegurar la continuidad en la cadena de pagos. Este programa ofrecía garantías a las micro, pequeñas, medianas y grandes empresas, permitiéndoles que puedan acceder a préstamos de capital, y de esta manera, puedan cumplir sus compromisos con sus empleados y proveedores.

En este contexto, Guardia Gallegos pone de relieve la situación de las pymes que formaron parte del programa Reactiva. "Estas empresas tendrán la responsabilidad de concluir el reembolso de los préstamos para el año 2023, con la expectativa de acceder a financiamiento sin restricciones. Sin embargo, aquellas que tuvieron que reestructurar su deuda verán reducida su capacidad para obtener financiamiento, ya que deberán cumplir primero con los pagos pendientes y posteriormente, al solicitar nuevos fondos, se les exigirá más información y garantías. Por el contrario, las empresas que no logren cumplir con los pagos enfrentarán un inminente riesgo de insolvencia" (Gestión, 2023).

Por otro lado, desde el 2014 entró en vigor la ley N° 30056, cuyo contenido se detalla en el factor legal. Esta ley puede traer oportunidades interesantes para las pymes en el aspecto del acceso a créditos por parte de instituciones financieras y fondos del Estado destinados para apoyarlas, así como ahorros considerables por gastos de capacitación en su personal.

3.1.3. Factor sociocultural

Dentro del factor sociocultural se abordan los aspectos culturales, demográficos y sociales que pueden afectar a las pymes.

En cuanto al factor socio-cultural para las pymes, destaca la significativa adopción de la transformación digital y la digitalización de operaciones, así como el impulso del comercio electrónico por parte de las pymes, el cual no estaba muy desarrollado previo a la pandemia en el país. De acuerdo al Comercio (2022) "[…]Este cambio se pone de manifiesto al observar que 76% de las pymes consideran que la tecnología será importante sin importar el modelo de trabajo que apliquen, ya sea presencial, remoto o híbrido".

En este contexto, cabe destacar que las pymes consideran en la actualidad la tecnología como una ventaja competitiva. Según el Comercio (2022) "[…]se observa un cambio cultural, donde la tecnología se convierte en una ventaja competitiva con excelentes oportunidades como la reducción de costos o el desarrollo de aplicaciones '*in-house*' para agilizar procesos".

En este sentido, otro cambio sociocultural en las pymes es el incremento de la adopción del trabajo remoto e híbrido. El Ministerio de Trabajo y Promoción del Empleo (MTPE) precisó que, "en el sector formal privado, un total de 12,766 empresas declararon al menos un teletrabajador en su planilla, según cifras registradas a noviembre del 2022" (Gestión, 2023).

Resalta también el potencial que tiene el Perú debido al bajo nivel de bancarización de la población, como un mercado propicio para el crecimiento del comercio electrónico y canales digitales. Según El Comercio (2022): "[…] el Perú es un mercado promisorio para el comercio electrónico pues cuenta con más de 33 millones de habitantes y un 47% de estos están sub bancarizados, por lo que hay mucho espacio para continuar creciendo".

Finalmente, este interés por la tecnología ha generado que aumente también la relevancia de la cyberseguridad para las pymes. Según el comercio (2022): "[…] En un estudio realizado por Microsoft, el 88% de las pymes peruanas sitúan a la seguridad cibernética como una prioridad, mientras que 78% planea invertir en tecnologías de

ciberseguridad en sus empresas y el 68% afirmó haber cambiado las políticas con esta herramienta para adaptarse al trabajo remoto".

3.1.4. Factor tecnológico

El continuo avance tecnológico es avasallador e imparable en la actualidad. Las tecnologías en su auge en estos últimos años son el internet de las cosas (*IOT*), la realidad extendida (*AR*), la impresión 3D, la inteligencia artificial con el *machine learning*, entre otros. Cabe resaltar que las pymes ya han iniciado un proceso de transformación digital a través de la implementación de muchas de estas nuevas tecnologías abriéndose así el camino hacia el comercio electrónico y digitalización de sus operaciones.

Ante esta situación, resulta esencial que las pequeñas y medianas empresas se encuentren en posición de ajustarse a las tendencias emergentes y afrontar los retos que se presenten. La habilidad para fomentar la innovación y la capacidad de adaptación cobran un rol fundamental a la hora de preservar la competitividad en sus respectivos mercados (Gestión, 2023).

Esta importancia se pone en evidencia a través de la mayor inversión que las Pymes están realizando en tecnología. "Según un informe emitido por Microsoft en 2022, se reveló que el 94% de las compañías en el Perú han destinado recursos a tecnología, mientras que el 96% ha incorporado la toma de decisiones basada en datos. Por tanto, numerosas pymes están en la búsqueda de digitalizar principalmente sus procesos de pedidos y ventas en plataformas digitales" (Gestión, 2023).

Al referirse a este tema, Jorge Merzthal, director del programa de MBA de ESAN, resalta que "la adopción de soluciones digitales otorga a las empresas peruanas la capacidad de mejorar la eficiencia, reducir costos y elevar la satisfacción del cliente". Además, "Las organizaciones deben ser versátiles y capaces de adaptarse rápidamente a estas cambiantes condiciones del mercado. Deben prepararse para adoptar nuevas tecnologías y procesos de trabajo, así como tener capacidades distintivas, las cuales puedan aprovechar luego en diferentes negocios y productos" (Gestión, 2023).

De este análisis, se puede concluir que las pymes que consigan adaptarse velozmente a estas novedosas tecnologías digitales lograrán establecer una ventaja competitiva en sus respectivos mercados.

3.1.5. Factor legal

En el aspecto legal, desde el 2014 entró en vigor la ley N° 30056, que establece lo siguiente: "[…] cambia los criterios de clasificación para las micro, pequeñas y medianas empresas. […] gozarán de amnistía en sanciones tributarias y laborales durante los primeros años contados a partir de su inscripción (en REMYPE) y siempre que cumplan con subsanar la infracción" (Escalante, 2016). De esta forma se busca incentivar a la formalidad y hasta luchar contra la falta de capital humano debidamente capacitado: "Las pequeñas, medianas y microempresas que capaciten a su personal podrán deducir este gasto del pago del Impuesto a la Renta por un monto máximo similar al 1% del costo de su planilla anual" (El Comercio, 2014).

Esta ley puede traer consigo oportunidades de crecimiento para las pymes que busquen formalizarse porque les permite acceder a créditos, participar en licitaciones públicas, acceder al financiamiento de fondos enfocados a las pymes, reforzar la formación de los trabajadores para mejorar su productividad y competitividad, conformar consorcios o asociaciones que ayuden a que se una más de una pyme para participar en concursos públicos o proyectos privados más grandes al compartir recursos y conocimientos, entre otros.

Adicional a ello, el Perú no cuenta con una estrategia nacional de *ciberseguridad* coordinada ni iniciativas, sin embargo, se han efectuado algunos pasos. Desde el año 2015 entró en vigor la Ley de Protección de Datos Personales que regula el consentimiento y tratamiento de los datos personales a toda empresa (El Comercio, 2015). En el año 2019 se aprobó la Ley de Ciberdefensa que lucha por combatir amenazas y la materialización de riesgos en el ciberespacio que puedan afectar la seguridad nacional (El Peruano, 2019). El Perú firmó el Convenio de Budapest para cooperar con la Ley de Delitos Informáticos (Ministerio Público Fiscalía de la Nación, 2020). El 28 de julio del 2023, se aprobó la Política Nacional de Transformación Digital al 2030 para el incremento del ejercicio de la ciudadanía digital (Silva, 2023).

En el caso de las pymes, la ley de protección de datos personales es de obligatorio cumplimiento y abarca la declaración de sus Bancos de Datos ante la Autoridad Nacional de Protección de Datos Personales (ANPD), clasificarlos e implementar los controles de seguridad de la información necesarios para protegerlos y atender las solicitudes de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Las auditorías bajo el ente rector están sujetas a multas si se encuentran incumplimientos a la Ley. En el peor escenario que se detecte una sanción muy grave, según EY se sancionan: "con multas que oscilan entre las 50 UIT (S/ 247,500) y 100 UIT (S/ 495,000), y son consecuencia de la recopilación datos personales a través de medios fraudulentos, desleales o ilícitos, o el suministro de información falsa a la ANPD" (Mishima, 2023). Asimismo, toda pyme que desee contratar con el Estado debe estar preparada para brindar servicios en pro de la transformación digital que los entes del Estado estarían buscando en los próximos años.

Dentro del ámbito legal, es importante mencionar que la Nueva Ley de Teletrabajo, en efecto desde febrero de 2023, establece que los gastos relacionados con servicios básicos y equipos deben ser asumidos por el empleador, a menos que exista un acuerdo mutuo en contrario. Esto da lugar a tres posibles escenarios. En el primer escenario, el empleador proporciona al trabajador tanto mobiliario como computadora o portátil, acceso a internet y cubre los costos de electricidad. La segunda opción involucra al trabajador aportando todo el equipo necesario y, a cambio, el empleador compensa su uso de la infraestructura. Por último, el tercer escenario surge cuando el trabajador aporta todos los elementos y el empleador no realiza ninguna compensación al respecto (Cárdenas, 2022).

La nueva Ley del teletrabajo también prohíbe que el teletrabajador subcontrate a terceros para realizar su labor, siendo esto positivo ya que el contrato laboral se basa en una prestación personal de servicios (Cárdenas, 2022). Esta nueva ley debe ser considerada por las pymes para que valoricen las ventajas de mantener o contratar a trabajadores virtuales o *teletrabajadores,* asumiendo los gastos que esto implica dada la normativa, eligiendo el escenario más beneficioso para ambas partes, tanto la pyme y el trabajador. Asimismo, la norma beneficia a la pyme ya que asegura que el

teletrabajador no subcontrate y realice el trabajo el mismo, aunque la dificultad radica en la supervisión de la pyme para esta condición.

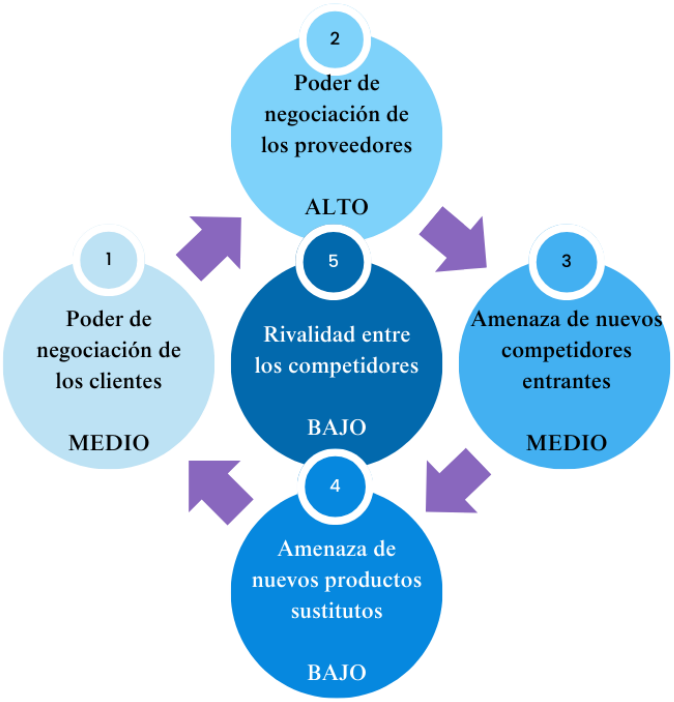
3.1.6. Conclusiones del Macroentorno

Al analizar los diversos aspectos del macroentorno, se puede concluir que, en términos generales, la pandemia en el Perú ha generado incertidumbre política y económica, afectando la perspectiva, la toma de decisiones, el aumento de costos de importación y los problemas de financiamiento para las pymes. Sin embargo, también ha impulsado un cambio en la mentalidad hacia la tecnología y una ola de digitalización. Las pymes han aumentado su presupuesto en este ámbito y lo han adoptado como un elemento estratégico para sus operaciones. Este cambio es beneficioso para la planificación empresarial, ya que la *ciberseguridad* se posiciona como una aliada de la digitalización, garantizando la reducción de pérdidas asociadas a los riesgos de *ciberseguridad* para las pymes.

3.2. Análisis de la industria de servicios de *Ciberseguridad*

El análisis de la industria de servicios de *ciberseguridad* para el mercado de pymes de Lima se llevó a cabo empleando el análisis de las 5 fuerzas de competitividad de Michael Porter. El resumen del análisis en cuestión se presenta en la ilustración debajo.

Ilustración 3.1 Resumen del análisis de las 5 fuerzas de competitividad de Porter



Fuente: Autores de esta tesis.

Elaboración: Autores de esta tesis.

3.2.1. Poder de negociación del cliente

El análisis del poder de negociación de los clientes se ha situado en un nivel intermedio. Actualmente, se observa una tendencia al alza en la demanda del sector de *ciberseguridad* enfocada en las pymes, impulsada por el crecimiento exponencial de los ciberataques en línea con el acelerado proceso de transformación digital.

Esta tendencia se ve reforzada por la limitada competencia en el mercado de *ciberseguridad*, específicamente diseñada para pymes. Este escenario confiere a los clientes cierta capacidad para influir en las condiciones de negociación, especialmente al elegir entre las opciones disponibles, aunque estas alternativas suelen ser escasas. A pesar de contar con empresas transnacionales como opción, su enfoque suele ser más costoso y no se ajusta de manera óptima a las necesidades de las pymes.

Es relevante considerar que los clientes mantienen el poder de no reconocer el problema de *ciberseguridad* o subestimarlo, lo que puede influir en su decisión de contratar servicios o soluciones en este ámbito.

3.2.2. Poder de negociación del proveedor

El poder de negociación de los proveedores es alto, porque la oferta de proveedores especializados en soluciones de *ciberseguridad* con excelente reputación, experiencia sólida y conocimientos técnicos se limita a grandes transnacionales. Al trabajar con grandes marcas tecnológicas y sus soluciones es necesario cumplir con sus requisitos para convertirse y mantenerse como aliado estratégico o *partner*.

Asimismo, existen costos asociados al cambio de proveedor de *ciberseguridad* en términos de tiempo, recursos y posibles interrupciones que afectarían la actividad central de la empresa. Finalmente, al ser la *ciberseguridad* un campo muy técnico y complejo para las pymes, les cuesta entender la diferenciación entre los servicios prestados por los proveedores, no pudiendo exigir mejoras en el mismo.

3.2.3. Amenaza de entrada de nuevos competidores

La amenaza de entrada de nuevos competidores es media, dado que existen cuatro barreras de entrada para el mercado de *ciberseguridad*, lo que constituye un problema para toda nueva empresa que desee incursionar en este mercado.

La primera barrera consiste, en que se requiere contar con personal con conocimientos especializados en el sector de *ciberseguridad* y en diversas soluciones que comercializan marcas como Microsoft, IBM, Cisco, Fortinet, Palo Alto, entre otros, y con experiencia comprobada. Por consiguiente, la naturaleza dinámica de la *ciberseguridad* implica un compromiso continuo con la investigación y desarrollo de servicios y estrategias que puedan responder rápidamente ante el cambiante entorno. Sin embargo, no hay suficientes profesionales en esta rama, por lo que existe una alta rotación entre las empresas que ofrecen servicios de *ciberseguridad*. De acuerdo con un informe de Fortinet, existen problemas para tanto reclutar como retener talento

ocasionando escasez de habilidades que permitan a las empresas hacer frente a las *ciberamenazas* (Fortinet, 2023).

La segunda implica que se requiere una inversión significativa en diversos componentes como la infraestructura tecnológica, herramientas de *ciberseguridad* y el marketing necesario. Incluso, es importante considerar una inversión continua en capacitación al personal, como lo confirma el informe de Fortinet (2023) indicando que los programas de certificación bien diseñados aportan al aprendizaje técnico, pero también a cómo aplicar ese conocimiento.

La tercera es que requieren establecer confianza y construir una reputación ante sus clientes que les asegure que esta nueva empresa puede ofrecer servicios de *ciberseguridad* de calidad protegiendo los activos de manera efectiva. Finalmente, la cuarta es que el mercado de empresas que ofrecen servicios de *ciberseguridad* enfocados únicamente para las necesidades de las pymes es bastante reducido, y hay más empresas grandes o transnacionales que ofrecen servicios mutilados para empresas pequeñas.

3.2.4. Amenaza de productos y servicios sustitutos

La amenaza de productos sustitutos es baja, dado que existen pocos sustitutos que satisfagan las necesidades específicas en *ciberseguridad* de las pymes.

Dentro de la categoría de productos sustitutos, es esencial mencionar a los fabricantes de herramientas digitales de *ciberseguridad*, así como a los proveedores de nube pública que ofrecen sus soluciones de respaldo y restauración en el mercado. Estos servicios, aunque disponibles para las pymes, a menudo plantean un desafío: la carencia de personal especializado capaz de llevar a cabo el monitoreo y análisis necesarios para su implementación. Esto crea un escenario en el que, aunque estas soluciones son accesibles, su verdadera eficacia puede quedar limitada por la falta de recursos internos para administrarlas de manera adecuada.

De igual manera, es relevante mencionar a las empresas consultoras internacionales previamente citadas, que ofrecen soluciones de *ciberseguridad*. Aunque las pymes no tienden a elegir estos servicios debido a su coste significativo y la falta de adaptación a

sus necesidades específicas, estas empresas foráneas constituyen una opción actual y disponible en el mercado, en caso de que surja la necesidad en las pymes para contratar un servicio de *ciberseguridad*.

3.2.5. Rivalidad entre competidores existentes

La rivalidad entre competidores en el mercado peruano es baja, ya que existen muy pocos servicios de *ciberseguridad* específicamente diseñados y enfocados en atender las necesidades que presentan las pymes. Al respecto, se identificó la presencia de un competidor, al que se llamará "Alpha Guard", una empresa latinoamericana establecida en México desde 2019, que se enfoca en ofrecer servicios especializados a las pymes en varios países de la región latinoamericana, incluido el mercado de *ciberseguridad* peruano.

Asimismo, existen profesionales independientes que brindan servicios muy específicos y altamente especializados en el campo de la *ciberseguridad*. Estos profesionales pueden abordar necesidades particulares y entregar soluciones personalizadas a las pymes que buscan fortalecer su seguridad digital.

También es importante destacar la presencia de consultoras transnacionales que han desarrollado servicios especialmente orientados a empresas de gran envergadura en sectores altamente regulados, como banca, seguros, reaseguros y aduanas, entre otros. Estas firmas multinacionales tienen la capacidad de invertir en tecnología de punta y herramientas eficaces, contando con profesionales en *ciberseguridad* con amplia experiencia, profundos conocimientos técnicos y una sólida reputación. Esto les permite distinguirse mutuamente y diferenciar sus servicios, marcando una notable diferencia en el mercado.

3.3. Benchmarking

Se inició con un análisis de los principales fabricantes transnacionales de soluciones de *ciberseguridad* que ofrecen alguna plataforma enfocada a las necesidades de las pymes, y se identificó tres opciones: *Small Office Security* de *Kaspersky*, *CyberCision* de *FirstWave* y *GravityZone Small Business Security* de *Bitdefender*. A

continuación, se presenta el cuadro comparativo y el resultado obtenido a partir de comparar sus principales características entre sí.

Tabla 3.1 Comparación entre plataformas de *Ciberseguridad* para pymes

	Small Office Security		***CyberCision***		***GravityZone Small Business Security***	
Fabricante	*Kaspersky*		*FirstWave*		*Bitdefender*	
Precio	S/ 55.00		S/ 145.00		S/ 77.66	
Certificaciones	No está certificado en ISO 27001.	0	Certificado en ISO 27001.	1	No está certificado en ISO 27001.	0
Seguridad de correo electrónico	No incluye.	0	Seguridad del correo electrónico con aprovisionamiento automatizado en cuentas Microsoft 365.	1	Permite bloquear los correos de tipo spam, phishing y adjuntos maliciosos como *malware*.	1
Aplicación móvil	No cuenta con aplicación móvil.	0	Aplicación móvil para monitoreo en tiempo real de las amenazas.	1	A través de su consola web se puede monitorear en tiempo real las amenazas.	1
Firewall	No incluye.	0	Controla el acceso de las aplicaciones a la red y a Internet.	0.5	Controla el acceso de las aplicaciones a la red e internet y protege el sistema contra escaneos de puertos, restringe ICS y advierte cuando nuevos nodos se unen a una conexión Wi-Fi.	1
Protección contra *malware* y *ransomware*	Protección avanzada contra *ransomware* y reversión para evitar bloqueo de su equipo en caso de un click accidental. Ante un intento de cifrado de los archivos se crea una copia de seguridad del archivo sin cifrar automáticamente para que se restaure.	1	No incluye.	0	Detecta y bloquea el *malware* sin archivos en la fase previa a la ejecución, el tráfico malicioso, el análisis del búfer de memoria antes de la inserción de código y el proceso de inserción de código. También, protege contra el *malware* dinámico. Crea una copia de seguridad de los archivos en tiempo real para enfrentar ataques de *ransomware*.	1
Protección de información confidencial	Cifra datos almacenados en las computadoras y servidores para evitar el acceso de ciberdelincuentes, crea copias de seguridad de datos en línea en caso de emergencia, destruye archivos de forma permanente y detecta y elimina archivos no usados.	1	No incluye.	0	No incluye.	0

	Small Office Security		***CyberCision***		***GravityZone Small Business Security***	
Monitoreo en *Dark Web*	No incluye.	0	Detección y respuesta avanzada con inclusión de monitoreo avanzado en la *Dark Web*, puntuación de riesgos y corrección automatizada.	1	No incluye.	0
Antisploit	No incluye.	0	No incluye.	0	Descubre *exploits* en tiempo real protegiendo navegadores y aplicaciones, así como mitiga las vulnerabilidades de corrupción de memoria.	1
Administrador de contraseñas	Administrador de contraseñas que protege todas las contraseñas del usuario y solo tiene que recordar una.	1	No incluye.	0	No incluye.	0
Seguridad en la web	Al acceder a servicios de pagos o banca en línea determina si el sitio web es seguro, bloquea sitios web maliciosos y descargas sospechosas, impide que sitios web rastreen y espíen las actividades en línea del usuario.	1	Escanea las páginas web antes de que el usuario acceda a ellas bloqueando las inseguras o de tipo phishing.	0.5	Analiza el tráfico web entrante, incluido el tráfico SSL, HTTP y HTTPS para evitar la descarga de *malware* en el *endpoint*. Bloquea automáticamente las páginas web fraudulentas y de *phishing*.	1
VPN	Cifrado y enmascaramiento de IP para evitar rastreo de datos, dispositivos ni ubicación geográfica. Tunelización dividida para configurar qué aplicaciones requieren VPN, e impide la filtración de datos.	1	No incluye.	0	No incluye.	0
Compatibilidad	Compatible con computadoras y servidores Windows, macOS y Android.	0.5	Compatible con computadoras y servidores Windows, macOS y Android.	0.5	Compatible con computadoras y servidores Windows, Linux y macOS, iOS y Android.	1
Resultado	**5.5**		**5.5**		**7**	

Fuente: *Bitdefender*, 2023. *FirstWave*, 2023. *Kaspersky*, 2023.
Elaboración: Autores de esta tesis.

Asimismo, se presenta el cuadro comparativo y los resultados obtenidos de la evaluación a los tres principales proveedores de nube pública en el mercado y sus respectivas soluciones para respaldo y restauración: *AWS Backup* de *Amazon Web Services*, *Azure Backup* de *Microsoft Azure* y *Cloud Storage* de *Google Cloud Platforms*.

Tabla 3.2 Comparación entre Servicio de *Backup* para pymes

	AWS Backup		***Azure Backup***		***Cloud Storage***	
Proveedor	*Amazon Web Services*		*Microsoft Azure*		*Google Cloud Platform*	
Objetivo	Respaldo y restauración de información.	1	Respaldo y restauración de información.	1	Almacenamiento de objetos escalable y duradero.	0.5
Integración	Integrado con la mayoría de los servicios de AWS.	1	Integrado con servicios de Azure y sistemas on-premises.	1	No está diseñado para respaldos, pero puede usarse para tal fin.	0.5
Durabilidad	99.999999999% (11 9's) en general.	1	99.9% en general.	0.5	99.999999999% (11 9's) para clases *Coldline* y *Standard*.	0.5
Tipo de *Backup*	Full y incremental para algunos recursos.	0.5	Full, incremental, y diferencial según la carga de trabajo.	1	No es específico, pero puede ser manejado con soluciones de terceros.	0
Retención de datos	Políticas de retención configurables.	1	Políticas de retención configurables.	1	Según ciclo de vida configurado.	1
Restauración	Restauraciones en el servicio original o diferente.	1	Soporte para restauración en ubicación original o alternativa.	1	Depende de la implementación y las herramientas de terceros utilizadas.	0.5
Pruebas de Restauración	Se pueden hacer restauraciones en ambientes aislados.		Soporta verificaciones de restauración.		Depende de herramientas y procesos de terceros.	0.5
Versión del respaldo	Sí, permite versionado.	1	Sí, gestiona múltiples versiones.	1	Versionado de objetos disponible.	1
Cifrado	Cifrado en tránsito y en reposo.	1	Cifrado en tránsito y en reposo.	1	Cifrado en tránsito y en reposo.	1
Respaldo	Planes de respaldo automatizados.	1	Políticas de respaldo configurables.	1	Depende de soluciones de terceros.	0

SLA	99.99999999999% en múltiples zonas.	1	99.9% para operaciones de *backup* y restauración.	1	99.95% para multirregional y 99.9% para regional.	1
Presencia	Segundo proveedor más usado.	0.8	Proveedor *cloud* más usado debido a la suite de Microsoft.	1	Tercer proveedor más usado.	0.5
Resultado	**10.25**		**10.5**		**7**	

Fuente: *AWS*, 2023. *GCP*, 2023. *Azure*, 2023.
Elaboración: Autores de esta tesis.

Por otro lado, se investigó y se encontró a una empresa latinoamericana que ofrece servicios enfocados para pymes desde el 2019 en países de la región, Alpha Guard. La compañía mexicana proporciona la herramienta propia "Apolo", diseñada para identificar fallos críticos en sitios web, *APIs*, nube y correo, y también para evaluar el nivel de riesgo de la organización al señalar a los colaboradores que deben mejorar sus habilidades en *ciberseguridad*. Además, tienen disponibles servicios como "*CISO as a Service*" que ayuda en la creación y aplicación del marco documentario de *ciberseguridad*, un servicio de "*pentesting*" para hallar y corregir fallos graves en sistemas y aplicaciones, y un servicio de monitoreo en la *Dark* y *Deep Web*.

3.4. Conclusiones del capítulo

El análisis PESTEL del entorno de las pymes en el mercado de las pymes en Perú destacan diversos factores. Respecto al factor político, la inestabilidad política genera incertidumbre económica y dificulta la toma de decisiones de inversión, afectando negativamente a las pymes al reducir el consumo y las ventas. Respecto al factor económico, la reciente contracción económica influye en áreas como inversión, consumo y acceso a financiamiento para las pymes. Aunque programas como Reactiva Perú han ayudado, la reestructuración de deudas puede obstaculizar el acceso a financiamiento. La ley N° 30056 ofrece oportunidades, pero es esencial su comprensión y aprovechamiento por parte de las pymes para impulsar su crecimiento. En términos socioculturales, la digitalización y el comercio electrónico están en aumento, lo que requiere que las pymes se adapten para mantener su competitividad. Las empresas familiares desempeñan un papel importante, pero la transición a generaciones futuras puede ser un desafío. Desde la perspectiva tecnológica, la rápida evolución tecnológica

demanda que las pymes adopten nuevas tecnologías y fomenten la innovación para mantenerse competitivas. Por último, en el ámbito legal, la ley N° 30056 ofrece oportunidades para las pymes al facilitar el acceso a créditos y la formación, promoviendo la formalización. Además, las regulaciones en protección de datos personales y la nueva Ley de Teletrabajo impactan en las operaciones de las pymes, requiriendo su atención y cumplimiento.

Por otro lado, el análisis de la industria de servicios de *ciberseguridad* para el mercado de pymes en Lima se basó en el marco de las 5 fuerzas de competitividad de Porter. La amenaza de entrada de nuevos competidores es moderada debido a barreras como la necesidad de personal especializado, inversiones en infraestructura y marketing, establecimiento de confianza y reputación, y la limitada oferta de servicios enfocados en pymes. La amenaza de productos y servicios sustitutos es baja, dada la falta de soluciones específicas para las necesidades de *ciberseguridad* de las pymes. El poder de negociación de los proveedores es alto debido a la limitada oferta de proveedores especializados y a los costos asociados al cambio. El poder de negociación de los clientes es bajo debido al crecimiento de la demanda en el sector y la escasa competencia para pymes. La rivalidad entre competidores existentes es baja, ya que hay pocos servicios específicos para pymes, aunque se destacan algunas empresas latinoamericanas y profesionales independientes.

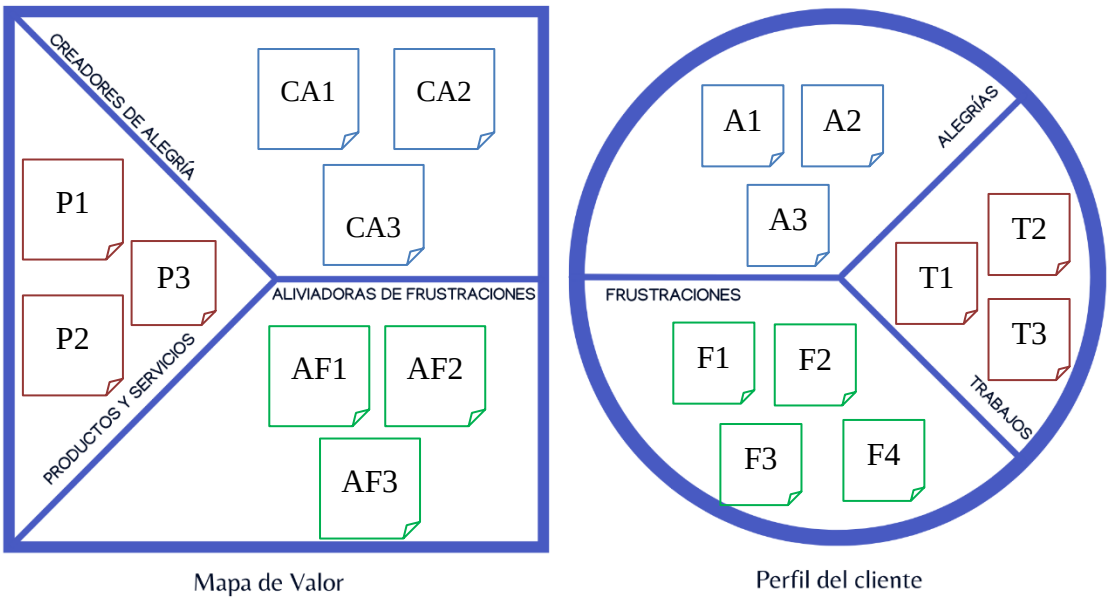
CAPITULO 4 . MODELO DE NEGOCIO

Después de haber definido las preguntas a resolver, los objetivos generales y específicos, así como analizar los marcos conceptuales y contextuales, se ha procedido a seleccionar y definir la metodología y estructura de presentación que seguirá el modelo de negocio para la solución.

En este sentido se comienza por desarrollar el *Value Proposition Lean Canvas*, analizando el **perfil del cliente** desde la definición de sus principales creadores de alegrías, trabajos y las frustraciones que los aquejan. Preliminarmente, se consideró como clientes objetivo a las pymes de Lima Metropolitana.

Para la sección de los **trabajos**, se formulan las preguntas: ¿Cuáles son las necesidades que tiene el público objetivo? ¿Cuáles son los problemas por resolver y qué espera conseguir con el servicio?, entre otros cuestionamientos que se han graficado en la siguiente matriz y concentrado en las siguientes actividades asociadas:

Ilustración 4.1 *Value Proposition Lean Canvas*



Fuente: Strategyzer, 2017.
Elaboración: Autores de esta tesis.

- **Trabajos:**
    - **T1:** Desconocimiento sobre los riesgos de *ciberseguridad* que genera falta de inversión en infraestructura básica.
    - **T2:** Complejidad y sofisticación continua de los ciberataques que dificulta la gestión de *ciberseguridad*.
    - **T3:** Falta de servicios de *ciberseguridad* que se ajusten a sus necesidades y recursos.

Por otro lado, se complementa el desarrollo del perfil del cliente con las secciones de **alegrías** y **frustraciones**, que hacen referencia a los beneficios esperados que se obtendrían por la nueva solución y los riesgos, barreras y/o preocupaciones que se pueden resolver con la solución, respectivamente.

- **Alegrías:**
    - **A1:** Ahorro de costos en el respaldo de datos y recuperación de los sistemas afectados.
    - **A2:** Mejor nivel de seguridad de los datos y sistemas en la organización.
    - **A3:** Apoyo a la continuidad operativa ante un *ciberincidente*.
    - **A4**: Incremento del nivel de conciencia de los colaboradores.
- **Frustraciones:**
    - **F1:** Indisponibilidad de sistemas y datos de la empresa.
    - **F2:** Altos costos para recuperación tras un *ciberincidente*.
    - **F3:** Daños reputacionales y pérdida de confianza de los clientes de las pymes.
    - **F4:** Pérdidas económicas por paralización de las operaciones por un *ciberincidente*.

Una vez concluida una parte del Lean Canvas, se procede con el mapa de valor que está divido en tres secciones: **productos y servicios**, **creadores de alegrías** y **aliviadores de frustraciones**.

- **Productos y Servicios:**
    - **P1:** Monitoreo y gestión de eventos y *ciberincidentes*.

- **P2:** Protección contra *malware*, *ransomware*, ataques web como phishing y ataques *DDoS*.
- **P3:** Gestión, respaldo y restauración de datos ante *ciberincidentes*.
- **P4:** Programa de concientización para los colaboradores.

- **Creadores de alegrías y aliviadores de frustraciones:**
  - **CA1:** Mejora de la seguridad del *endpoint* y el correo electrónico.
  - **CA2:** Mitigación de riesgos asociados a la confidencialidad, disponibilidad e integridad de la información.
  - **CA3:** Sentirse adecuadamente informado acerca de las amenazas y vulnerabilidades más peligrosas.
  - **AF1:** Servicio de copias de seguridad y respaldo de información sensible.
  - **AF2:** Soluciones *endpoint* de seguridad que ofrecen protección ante ciberataques y otras amenazas digitales.
  - **AF3:** Plan de capacitación y material didáctico que asegure una cultura de protección para identificar amenazas, vulnerabilidades y generar conciencia.

Por último, se realizó un cruce entre los **creadores de alegrías** y **alegrías**, así como de los **aliviadores de frustraciones** y **frustraciones**:

Tabla 4.1 Relación entre creadores de alegrías y alegrías

CREADORES DE ALEGRIAS		ALEGRÍAS	
CA1	Mejora de la seguridad del *endpoint* y el correo electrónico.	**A2**	Mejor seguridad de los datos y sistemas en la organización.
CA2	Mitigación de riesgos asociados a la confidencialidad, disponibilidad e integridad de la información.	**A1** **A3**	Ahorro de costos en la recuperación de datos y reparación de los sistemas afectados. Apoyo a la continuidad operativa ante un *ciberincidente*.
CA3	Sentirse adecuadamente informado acerca de las amenazas y vulnerabilidades más peligrosas.	**A4**	Incremento del nivel de conciencia de los colaboradores.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Tabla 4.2 Relación entre aliviadores de frustraciones y frustraciones

ALIVIADORES DE FRUSTRACIONES		FRUSTRACIONES	
AF1	Servicio de copias de seguridad y respaldo de información sensible.	**F1**	Indisponibilidad de sistemas y datos de la empresa.
AF2	Soluciones endpoint de seguridad que ofrecen protección ante ciberataques y otras amenazas digitales.	**F1** **F2** **F4**	Indisponibilidad de sistemas y datos de la empresa. Altos costos para recuperación tras un *ciberincidente*. Pérdida económica por paralización de las operaciones por un *ciberincidente*.
AF3	Plan de capacitación y material didáctico que asegure una cultura de protección para identificar amenazas, vulnerabilidades y generar conciencia.	**F3**	Daños reputacionales y pérdida de confianza de los clientes de las pymes.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

4.1. Lean Canvas

La herramienta seleccionada para desarrollar y presentar el modelo de negocio fue el *Lean Canvas Model*. Se sostiene que el *Lean Canvas* fue creado por Maurya (2012) bajo el fundamento de que un modelo de negocio no está limitado a desarrollar un producto/servicio en términos de la solución, sino que busca relacionar los diferentes componentes que forman parte del plan. De igual manera, Maurya (2012) refuerza la idea de que lo primero es identificar un problema que valga la pena resolver antes de

empeñarse en encontrar la solución. Su propuesta se compone de tres preguntas clave: ¿Es algo que los clientes quieren? ¿Pagarían por ello? ¿Es factible que pueda ser resuelto? Estas preguntas estarán modeladas en una encuesta (Ver Anexo 7), desarrollada en el siguiente capítulo que permitirá la definición del producto mínimo viable (*MVP*).

Asimismo, se efectuó un sondeo inicial que contempló un cuestionario a un público en general de 100 personas, 66 correspondientes a pymes (Ver Anexo 6). Este se realizó con la finalidad de aterrizar mejor el problema a resolver, afinar la propuesta del modelo de negocio y, por consiguiente, modelar el *MVP*. Por último, de acuerdo con Flores-Aguilar (2019), durante el desarrollo del *Lean Canvas* será importante sintetizar el propósito de cada módulo de modo que se pueda precisar qué se está buscando.

El siguiente gráfico consolida la información desarrollada de cada módulo del Lean Canvas:

Tabla 4.3 Lean Canvas

<table>
<tr>
<td rowspan="2">PROBLEMA
→ El desconocimiento sobre los principales riesgos de ciberseguridad asociados al proceso de digitalización, que conlleva a una falta de inversión en infraestructura básica de ciberseguridad.
→ La complejidad y sofisticación continua de los ciberataques, como el malware, ataques web y ransomware; conlleva a que las pymes no puedan afrontar este escenario sin los especialistas o herramientas necesarias.
→ Los servicios de ciberseguridad ofrecidos actualmente están dirigidos a empresas grandes, no se ajustan a las necesidades de las pymes y tienen un costo elevado.</td>
<td>SOLUCIÓN
→ Monitoreo y gestión de eventos y ciberincidentes.
→ Protección contra malware, ransomware, ataques web como phishing y ataques DDoS.
→ Gestión, respaldo y recuperación de datos ante ciberincidentes.
→ Programa de concientización para los colaboradores.</td>
<td rowspan="2">PROPUESTA DE VALOR
→ “Tu Negocio, tu Pasión. La Ciberseguridad, nuestra razón”</td>
<td>VENTAJA COMPETITIVA
→ Servicio end-to-end adaptable
→ Servicio Completo y Rentable
→ Servicio Escalable</td>
<td rowspan="2">SEGMENTO DE CLIENTES
→ Pequeñas & Medianas Empresas (pymes) de Lima Metropolitana
→ Early adopters: Pequeñas & Medianas Empresas (pymes) del sector construcción de Lima Metropolitana que se encuentran transformadas o en proceso de transformación digital.</td>
</tr>
<tr>
<td>MÉTRICAS CLAVE
→ Tasa de Retención
→ Tasa de Conversión
→ Costo de Adquisición
→ Tasa de adopción/conversión
→ Satisfacción del cliente
→ Tasa de retención de clientes
→ Margen de beneficio bruto:
→ Costo de adquisición de clientes (CAC)
→ Tiempo de respuesta ante incidentes
→ Nivel de atención de ciberincidentes
→ Tiempo de recuperación de datos.</td>
<td>CANALES
→ Ventas directas
→ Plan de referidos
→ Redes sociales (Marketing digital)
→ Canal audiovisual (Marketing de contenidos)
→ Alianzas estratégicas
→ Eventos & ferias</td>
</tr>
<tr>
<td colspan="2">ESTRUCTURA DE COSTOS
→ Talento humano
→ Componente tecnológico
→ Infraestructura y hosting
→ Costos operativos
→ Marketing</td>
<td colspan="3">FLUJO DE INGRESOS
→ Suscripción de la solución
→ Productos/Servicios adicionales</td>
</tr>
</table>

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

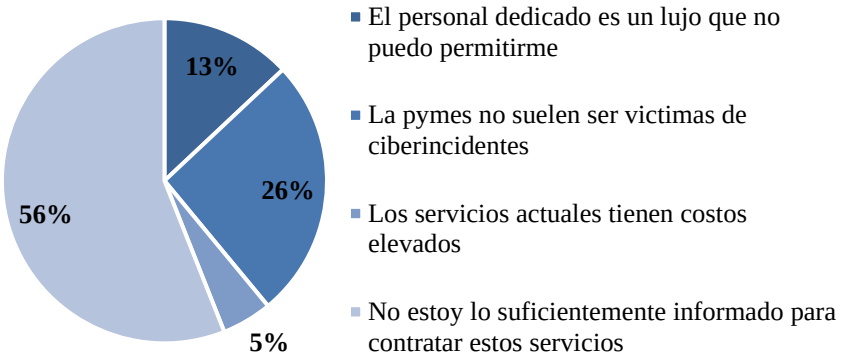
4.2. Problema

El propósito de este módulo es el de precisar los principales problemas que tiene el público objetivo, las pymes de Lima Metropolitana, y posteriormente sobre el malestar identificado se desarrollará la propuesta de valor.

Al recapitular la problemática planteada en el capítulo, cabe resaltar que la situación actual que atraviesan las pymes se ha tornado complicada, dado que muchas se vieron obligadas a transformarse digitalmente sin estar los suficientemente preparadas. Adicional a ello, la realidad descrita por ENISA (2021), es que la mayoría de las pymes tienen un alto riesgo de quebrar ante un *ciberataque*. Bustamante et al (2021), hacen una reflexión sobre cómo las pymes peruanas son el foco más vulnerable ante estos ataques y se justifica a través de Porras et al. (2018), quiénes resaltan que la mayoría de estas empresas tienen altas probabilidades de no detectar *ciberataques* y sus principales motivos son las limitaciones presupuestales, la carencia de recursos y alternativas especializadas. Cabe resaltar que según un reporte de Mapfre: “Cada segundo se producen sólo en América Latina y el Caribe alrededor de 1.600 ciberataques a empresas” (Hernández, 2022).

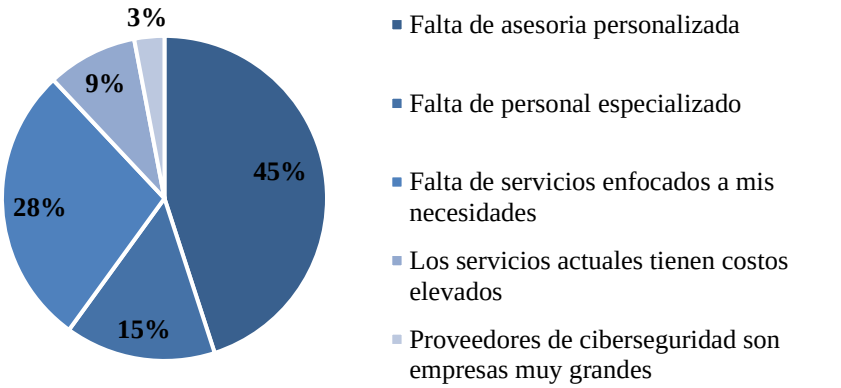
Adicionalmente, para validar los problemas identificados en capítulos iniciales, se efectuó el sondeo inicial mencionado (ver Anexo 6), donde se evidencian que las principales razones por las que las pymes no contratan servicios son la carencia de información sobre en qué consisten los servicios, así como la percepción de que los *ciberataques* no son un problema frecuente de las pymes, sino que es la realidad de grandes empresas. Asimismo, este último factor está expresado y relacionado con la razón principal por la que las empresas no consideran como una opción el contratar los servicios: falta de asesoría personalizada. Finalmente, del sondeo, se rescató los principales tipos de ataques que han sufrido las empresas: *phishing*, virus y *malware*.

Ilustración 4.2 Sondeo Inicial – Razones para no contratar los servicios de *Ciberseguridad*



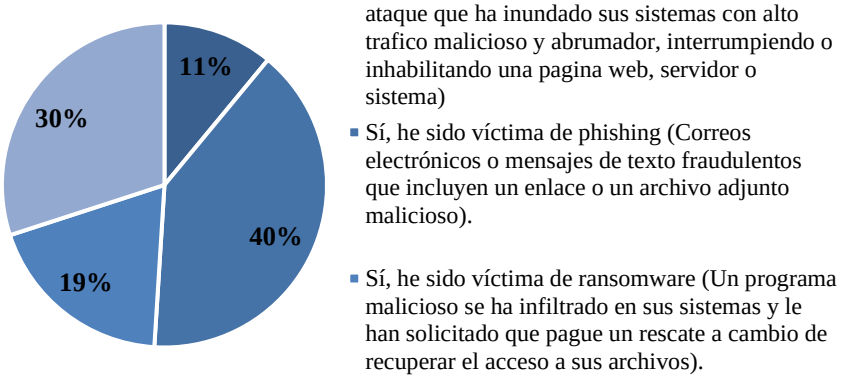
Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Ilustración 4.3 Sondeo Inicial – Problemas identificados con servicios de *Ciberseguridad*



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

lustración 4.4 Sondeo Inicial – Tipos de ciberataques en las pymes



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Por lo tanto, y de acuerdo con el análisis de las respuestas se ratificaron los siguientes problemas:

1) El desconocimiento sobre los principales riesgos de *ciberseguridad* asociados al proceso de digitalización, que conlleva a una falta de inversión en infraestructura básica de *ciberseguridad*.

2) La complejidad y sofisticación continua de los *ciberataques*, como el *malware*, ataques web y *ransomware*, conlleva a que las pymes no puedan afrontar este escenario sin los especialistas o herramientas necesarias.

3) Los servicios de *ciberseguridad* ofrecidos actualmente están dirigidos a empresas grandes, no se ajustan a las necesidades de las pymes y tienen un costo elevado.

4.3. Propuesta de Valor

El propósito de este módulo es el de sintetizar y describir cómo el servicio desarrollado en este plan de negocios brinda una solución a los problemas del público objetivo y cuál es su valor asociado.

La propuesta de valor de la solución tomó en consideración los resultados obtenidos del sondeo inicial (Ver anexo 6). La propuesta consistirá en un paquete de servicios que garantice el incremento del nivel de *ciberseguridad*, mitigando los *ciberataques* y sus severas consecuencias y generando conciencia sobre esta problemática.

La propuesta de valor busca resaltar tres puntos. El primero es democratizar la *ciberseguridad*, dado que en los últimos años ha estado reservada para grandes empresas con presupuestos enormes, pero los avances tecnológicos actuales permiten desarrollar soluciones y servicios para las pymes. El segundo es las pymes se están transformando digitalmente cada vez más para atender a sus clientes y las pymes necesitan servicios accesibles de *ciberseguridad* que las acompañen en este proceso. El tercero es que se desea que las pymes se enfoquen en su *core business*, es decir en su negocio en sí, mientras pueden confiar que el paquete de servicios ofrecidos va a enfocarse en proteger su negocio en el mundo digital.

Después de desarrollar el lienzo de la propuesta de valor, se concluye con la siguiente frase: "*Tu Negocio, tu Pasión. La Ciberseguridad, nuestra razón"*.

4.4. Segmento de Clientes

El objetivo del siguiente modulo es poder analizar, determinar, explicar, confirmar y justificar la elección del cliente objetivo al cual se está destinando el servicio desarrollado en el presente plan de negocios. En este sentido se aplicará un enfoque TAM, SAM, SOM. Esta herramienta de análisis permite hacer una estimación inicial de la oportunidad de mercado que tiene la propuesta y delimitar el segmento al cual será orientado. (Santander, 2021).

Para desarrollar este análisis se utilizó como fuente de información el sondeo inicial realizado a 66 empresas de elaboración propia, la encuesta de madurez digital en el país que realizó EY en el 2022 y el documento desarrollado por el INEI en el 2022, "Perú Estructura empresarial 2020".

Se inició por determinar el mercado total o TAM (*Total Addressable Market*) con una estrategia *Top-Down*, de tal manera que se empieza de lo global a lo particular. De esta manera, el mercado total o TAM de este plan de negocios son las pymes. Para finales del año 2020, de acuerdo con el INEI (2022), en el Perú se tienen identificadas cerca de 2.8 millones de empresas formales, siendo aproximadamente 106 mil las que corresponden a las pequeñas y medianas empresas (hasta 2300 UIT de facturación anual).

La clasificación utilizada para las pymes se presenta en la tabla continuación:

Tabla 4.4: Clasificación de empresas formales en función a ventas anuales en UIT.

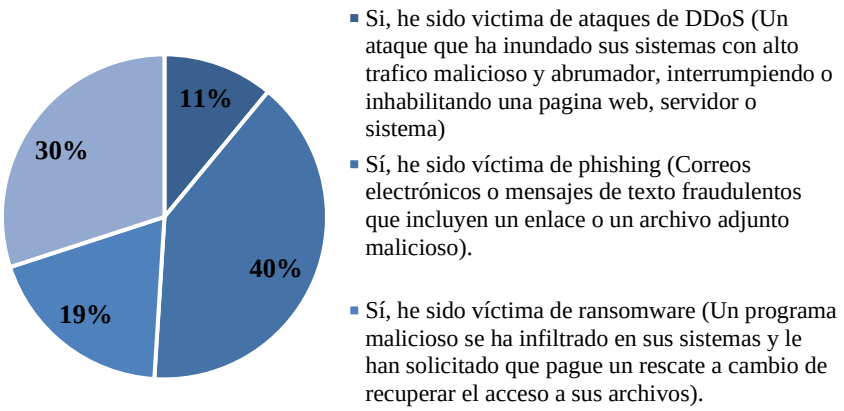
ESTRATO EMPRESARIAL	PROMEDIO DE VENTAS ANUALES (EN UIT)
Microempresa	Ventas anuales hasta el monto máximo de 150 UIT
Pequeña empresa	Ventas anuales superiores a 150 UIT y hasta por el monto máximo de 1.700 UIT
Mediana empresa	Ventas anuales superiores a 1,700 UIT y hasta por el monto máximo de 2.300 UIT

Fuente: MEF, 2023.
Elaboración: Autores de esta tesis.

Luego, con la determinación del mercado disponible o SAM (*Service Addressable Market*), para efectos de este plan de negocios y según lo indicado por el INEI (2022), a finales del año 2020 hay 43% (1.2 millones) aproximadamente de pymes que se concentran en Lima Metropolitana. Y a su vez, las empresas pequeñas (de 10 a 49 colaboradores) y medianas (de 50 a 199 colaboradores) aproximadamente el 5% (63 mil).

En última instancia se acotó el mercado disponible o SAM para definir el mercado obtenible y útil o SOM (*Service Obtainable Market*) en base al sondeo inicial que se realizó a 66 personas que laboraban en pequeñas y medianas empresas. Identificándose que el más alto porcentaje a nivel del sector era el de construcción e inmobiliaria, secundado por manufactura y otros servicios (educación, salud, turismo, sociales).

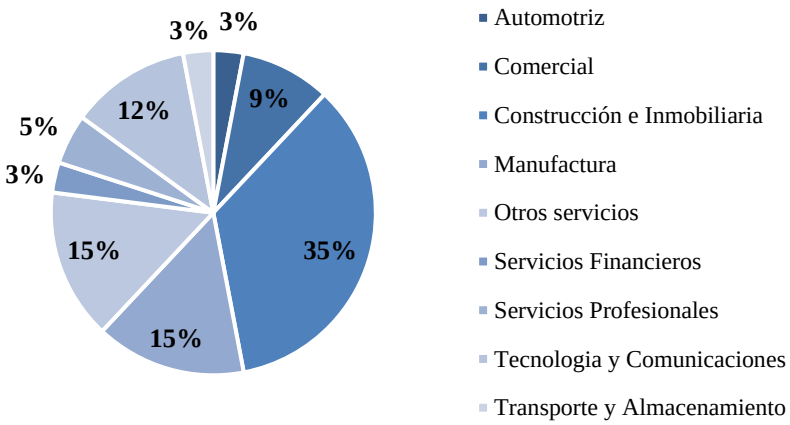
Ilustración 4.5 Sondeo Inicial – Sectores



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Asimismo, se aprovechó para verificar cuáles eran los sectores que más *ciberataques* habían recibido y se tuvo una proporción bastante similar al del gráfico anterior, siendo la más aquejada la de Construcción e Inmobiliaria. El orden lo continúa manufactura y comparten el mismo porcentaje: Otros Servicios y Tecnología y Comunicaciones.

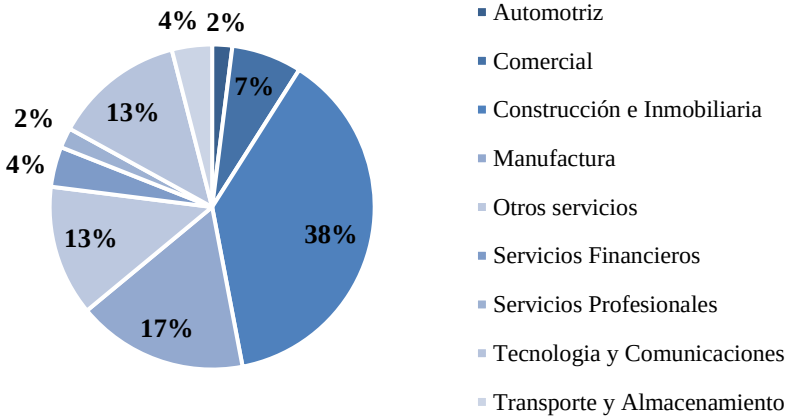
Ilustración 4.6 Sondeo Inicial – *Ciberataques* por Sectores



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Asimismo, del sondeo sobre la disposición a adquirir un servicio de *ciberseguridad*, se rescata la predilección de compra del sector Construcción e Inmobiliaria.

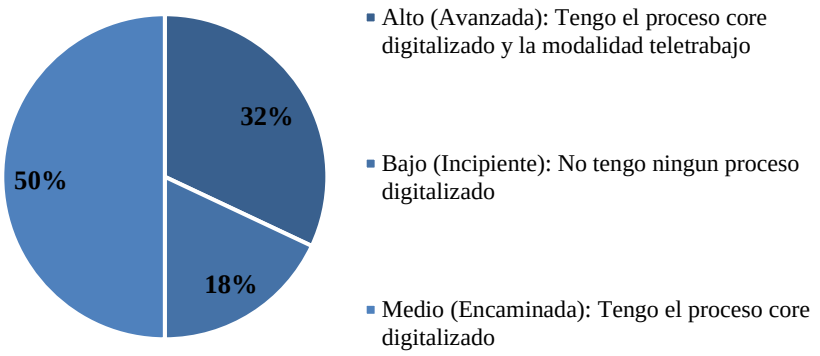
Ilustración 4.7 Sondeo Inicial – Predisposición de comprar servicios de *Ciberseguridad* por Sectores



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Por otro lado, se procedió a evaluar el estado de transformación digital para constatar la madurez que consideran presenta las empresas encuestadas, consideran que tienen, tomando la clasificación de índice de madurez del estudio de EY que también se analizó:

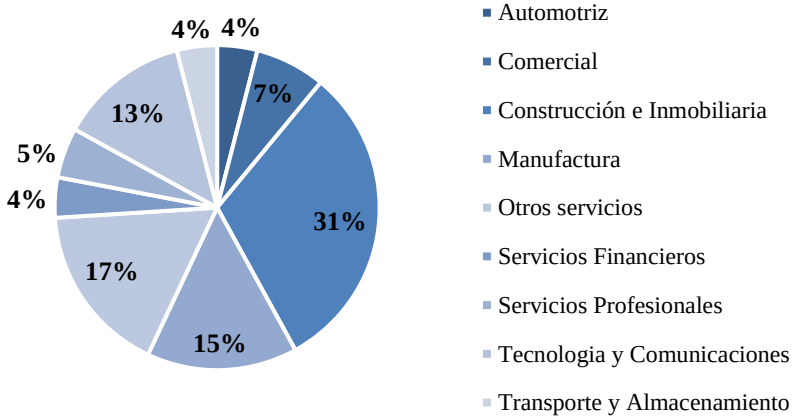
Ilustración 4.8 Sondeo Inicial – Estado de transformación digital



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Se pudo validar que la mitad de los encuestados consideran que están en un nivel medio, seguido de un porcentaje cercano al 30% de las empresas que están ya están transformadas. De esta manera, se realizó nuevamente el filtro por sectores, pero considerando los niveles de madurez medios y altos:

Ilustración 4.9 Sondeo Inicial – Nivel de madurez Medio & Alto por Sectores



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Para complementar la información ya analizada en el sondeo inicial, se analizó la encuesta de madurez digital en el país que realizó EY en el 2022 y sobre esta destacan

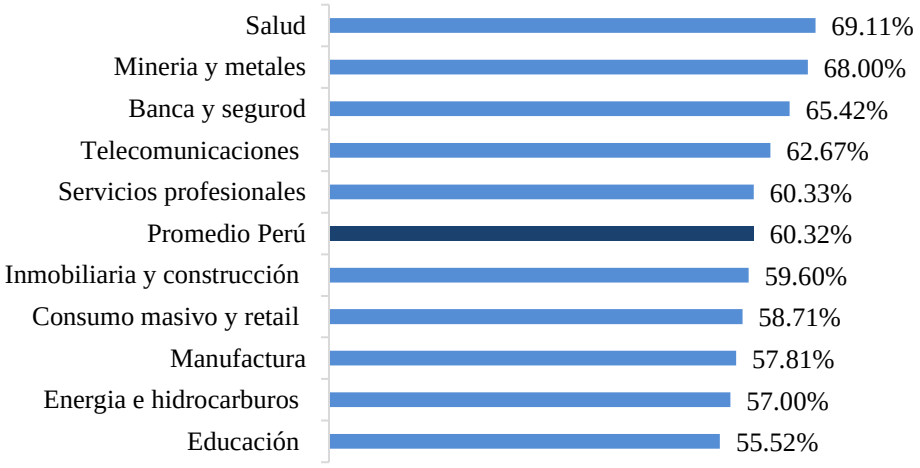
los ámbitos evaluados: estrategia e innovación, experiencia del cliente, información y tecnología, operaciones y cadena de suministro, riesgo y seguridad cibernética, cultura y organización y áreas administrativas (finanzas, legal, recursos humanos y marketing).

Es así como Escudero (2022), recalca que de una escala de 0 a 100 y de acuerdo con las clasificaciones de nivel de transformación digital: incipiente, encaminada y avanzada; el índice de madurez digital a nivel Perú es de 60.32, lo que la catalogaría con un estado de encaminada (de 50 a 80 puntos). Esto se traduce en organizaciones en movimiento, en ruta hacia la madurez digital, pero que aún presentan oportunidades de mejora para la integración digital de sus procesos se vuelva uniforme.

De igual manera, cabe mencionar que este índice, 60.32, es inferior al índice del año anterior, sin embargo, se explicaría por la desaceleración propia de la pandemia del COVID-19, dado que este decremento también se dio en toda la región.

En el territorio nacional, la madurez digital por sectores evidenció que salud, minería, banca, telecomunicaciones y servicios profesionales están por encima del promedio, mientras que inmobiliaria y construcción es el primer sector por debajo del promedio:

Ilustración 4.10 Madurez Digital por Sectores – Perú



Fuente: Escudero, 2022.
Elaboración: Autores de esta tesis.

De igual manera, cuando se asocian los ámbitos evaluados por sector, Escudero (2022), menciona que se tienen hallazgos como que la minería y metales tiene alta madurez en operaciones y cadena de suministros e información y tecnología, por el contrario, tienen menos desarrollo en estrategia e innovación.

Con respecto a banca y seguros, este sector presenta mayor avance en los ámbitos de información y tecnología, y riesgo y seguridad cibernética. Sin embargo, de todo el análisis, existen dos sectores que presentan desigualdad en avance en dos ámbitos que debieran ser complementarios: educación e inmobiliaria y construcción. De esta manera, en ambos sectores se tiene un gran avance en información y tecnología, mas no es el caso de riesgo y seguridad cibernética, lo que podría interpretarse que las organizaciones en estos sectores son blanco fácil ante ciberataques externos.

Por consiguiente, las pymes evaluadas en el análisis de transformación digital son alrededor de la mitad de la muestra total, y tal como menciona Escudero (2022), el índice de madurez digital promedio en este sector empresarial está aún por debajo de las grandes empresas y a nivel del promedio nacional, teniendo desde el 2020 una evolución de 58.53 a 60.38 en 2021 y 58.56 en 2022. En consecuencia, para el modelo de negocio se decidió tomar en consideración tanto los resultados del sondeo inicial, donde los sectores que están predispuestos a adquirir servicios de *ciberseguridad* son: construcción, tecnología y comunicaciones, servicios financieros y seguros y otros servicios.

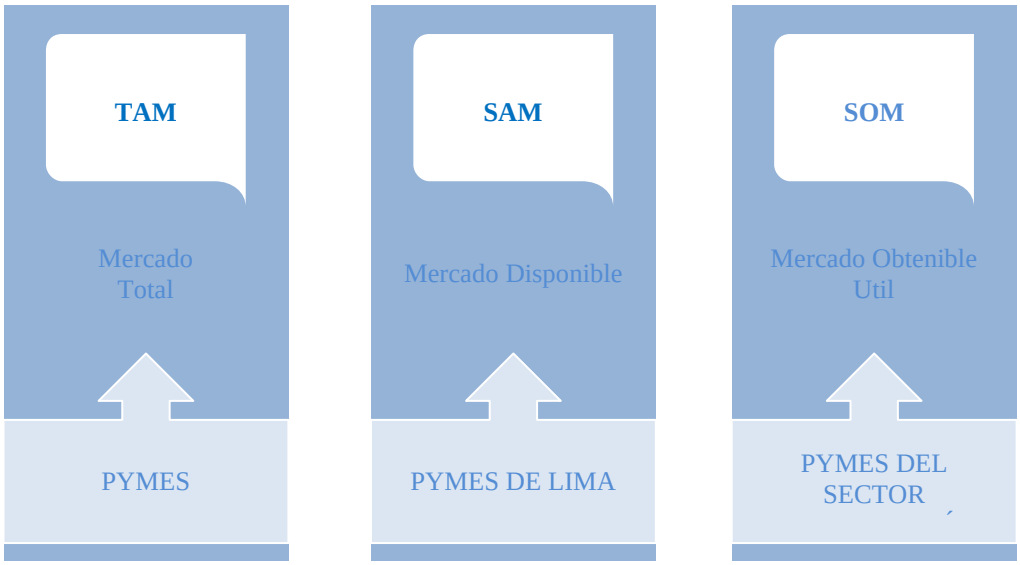
Por otro lado, en la encuesta de transformación con sentido digital se rescata la información asociada a los niveles promedio de madurez digital donde había algunos sectores por encima del promedio nacional de 60.32 y al mismo tiempo dado el enfoque de *ciberseguridad* de la investigación, se considera importante la evaluación a nivel de los ámbitos de riesgos y seguridad cibernética, e información y tecnología.

De esta manera, después de conocer que el sector de educación y el de inmobiliaria y construcción tienen una dificultad en el avance de riesgo y *ciberseguridad* por lo que son organizaciones donde existe potencial para reforzarse, se selecciona como *MVP* al público objetivo a las pymes de Lima Metropolitana del sector de construcción e inmobiliaria que están en proceso o ya transformadas digitalmente, de modo que se

puede profundizar en un sector dada la complejidad de analizar a todos los sectores de que comprenden al grupo económico.

Según el informe “Perú: Estructura Empresarial, 2020” (INEI, 2022), el universo de las pymes del sector construcción en Lima es de 3895.

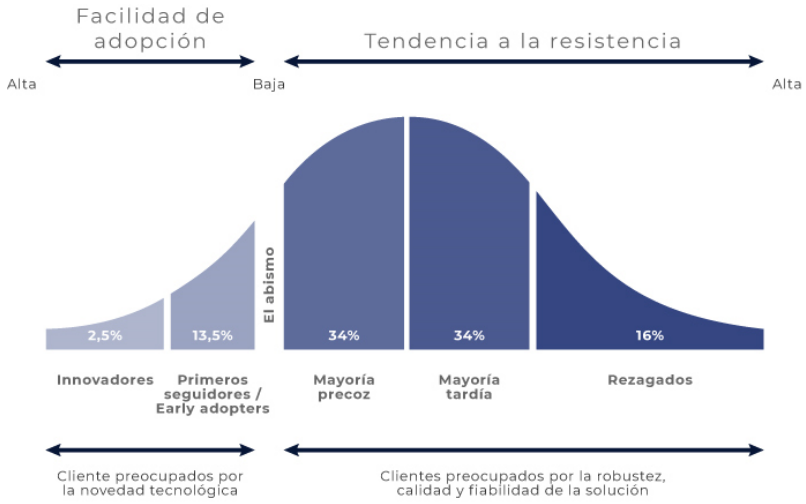
Ilustración 4.11 TAM, SAM, SOM



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Como parte del proceso de definición del segmento objetivo mediante el TAM, SAM y SOM se ha determinado los *Early Adopters* o como lo indica Rogers (2003) primeros adoptantes. Rogers (2003) definió las categorías de adopción como “las clasificaciones de los miembros de un sistema social sobre la base de su capacidad de innovación”. Esta clasificación incluye innovadores, primeros adoptantes, mayoría temprana, mayoría tardía y rezagados, según se muestra en el siguiente gráfico:

Ilustración 4.12 Categorización de adoptantes



Fuente: CEEI Valencia, 2023.
Elaboración: Autores de esta tesis.

Según el CEEI Valencia (2023) los principales adoptantes son consumidores o usuarios que tienen una necesidad por satisfacer y que se atreven o son definidos como los primeros en probar la solución. Aunque no es una regla, suelen ser perfiles innovadores o que no le tienen miedo al cambio, en general comprenden las necesidades que la innovación demanda y pueden adoptar soluciones o propuestas más arriesgadas.

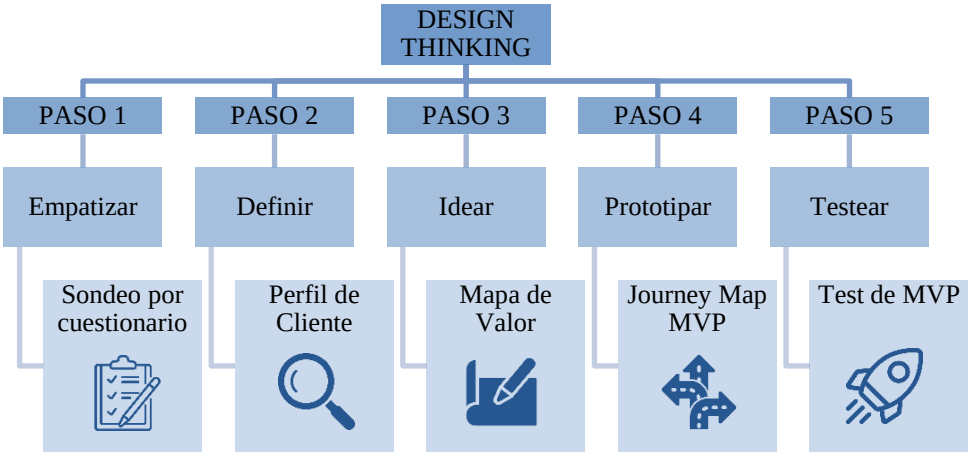
En este sentido y después del análisis de segmentación se ha definido como e*arly adopter* a las pymes del sector construcción de Lima Metropolitana, que se encuentren transformadas o en proceso de transformación.

4.5. Solución

El propósito de este módulo es el de precisar las características principales del servicio que se propone para ayudar a resolver el problema identificado del cliente. De las metodologías existentes para la resolución de problemas y para el planteamiento de soluciones, se ha definido el empleo del *Design Thinking*.

La metodología de *Design Thinking* permite generar ideas innovadoras, centrando su eficacia en entender y dar solución a las necesidades reales, a través de cinco pasos: empatizar, definir, idear, prototipar y testear, según lo mencionan Ramos y Wert (2015).

Ilustración 4.13 Metodología de *Design Thinking* aplicada para definir la solución



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

A lo largo de las distintas etapas, se logró una comprensión profunda de las necesidades de los usuarios y se diseñó una solución que responde de manera efectiva a sus desafíos y deseos. A continuación, se detalla cómo se aplicaron las diferentes fases del *Design Thinking*.

Para la etapa de **Empatizar**, se llevó a cabo un sondeo por cuestionario para comprender a fondo las necesidades de los usuarios. Esto permitió recopilar información valiosa de los clientes potenciales y sus perspectivas; además permitió aterrizar mejor el problema a resolver. Este enfoque permitirá que el servicio desarrollado esté centrado en el usuario.

Durante la etapa de **Definir**, se consolidó la información recopilada en la fase anterior. Se creó el perfil del cliente desde la definición de sus trabajos, identificando sus frustraciones y alegrías. Este proceso sirvió como brújula para guiar las decisiones en las etapas posteriores y se diagramo mediante el *Value Proposition Canvas*

En la etapa de **Idear**, se utilizó la herramienta “Mapa de Valor”, con el objetivo de identificar los creadores de alegrías y aliviadores de frustraciones, y poder generar ideas innovadoras, para definir los Productos/Servicios necesarios para el *MVP* del servicio de *ciberseguridad* que se ofrecerá a las pymes del sector construcción. Esto permitió

identificar oportunidades para agregar valor en cada etapa de su experiencia y generar soluciones que fueran relevantes y significativas.

La etapa de **Prototipar** fue crucial para transformar los servicios identificados en una solución más tangible y prototipo más visual. Esto se realizó a través de la creación de un *Journey Map* detallado que trazó la experiencia del cliente desde el punto de inicio hasta la meta final. Este mapa ayudó a visualizar los puntos de contacto clave a lo largo del *journey*, a fin de poder identificar áreas de mejora y perfeccionar la experiencia antes de su implementación.

Tabla 4.5 *Customer Journey Map* del Servicio

	CONCIENCIA	CONSIDERACIÓN	COMPRA	SERVICIO	RETENCIÓN
Acciones del Cliente	→ Se entera de la empresa → Solicita información/ Demo	→ Recibe información de servicios → Participa en Demo → Recibe cotización	→ Se Afilia → Firma Contrato → Realiza Pago → Recibe Comprobante	→ Instalación → Reporte Mensual → Atención de Req. De Incidentes → Recibe boletines → Encuesta de Satisfacción	→ Membresía VIP → Programas de Referidos
Puntos de contacto	→ Redes Sociales → whatsapp → Web	→ Correo → Videollamada	→ Correo	→ Videollamada (instalación, reuniones) → Correo (boletines, reportes, req.) → whatsapp (incidentes)	→ Correo → Whatsapp
Resultados Esperados	→ Publicidad Atractiva que capte el interés → Respuesta clara y rápida a solicitudes	→ Información clara y detallada → Demo profesional y genera confianza → Cotización clara y detallada	→ Afiliación sencilla → Envío oportuno del contrato → Medios de pago variados → Envío oportuno de Comprobante	→ Instalación en plazo y sin errores → Envío oportuno del reporte. → Atención eficaz de Incidentes	→ Información clara sobre los programas → Entrega Oportuna de beneficios

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

En la etapa de **Testear**, se realizó la presentación de el *journey map* a algunos usuarios. Esto se realizó a través presentaciones por videollamadas y se recopiló *feedback* y comentarios valiosos sobre el funcionamiento y efectividad de la experiencia

diseñada. Estos comentarios proporcionaron información esencial para iterar y ajustar la solución, asegurando que estuviera alineada con las expectativas y necesidades de los usuarios.

En conclusión, tomando en cuenta la metodología de *Design Thinking*, y los resultados obtenidos del análisis del *benchmark* se determinó que la solución debe cumplir con las siguientes características más resaltantes:

Finalmente, se articula la solución y se define el *MVP*, como un paquete de *ciberseguridad* para pymes, empezando por uno de los sectores más representativos y con un atractivo potencial en Lima (construcción e inmobiliaria) según lo revisado en el numeral 4.4 Segmento de Clientes, que constará de:

- La solución *endpoint GravityZone Small Business Security* de *Bitdefender* con protección *anti-malware*, *anti-exploit*, *anti-phishing*, *anti-ransomware*, prevención de fraude y ataques basados en *scripts*, protección de navegación web y correo electrónico, y *firewall* (49 licencias por paquete),
- El servicio de *Azure Backup* que ofrece respaldo y restauración de la información ante un *ciberincidente* (5TB por paquete), y
- Un programa de concientización para los colaboradores.
- El servicio incluye el monitoreo centralizado y el *cibersoporte* ante la atención de requerimientos de configuración de reglas y accesos y de incidentes en ambas soluciones bajo un esquema de 10 horas mensuales.
- El nombre comercial para ofertar este plan base será "*Cyber Plus*".

Adicional a ello, se ha definido que las pymes interesadas en adquirir una mejora en las prestaciones actuales del paquete del plan base "*Cyber Plus*" podrían optar por estoss *upgrades*:

- *Support Plus*: Incluye 10 horas mensuales adicionales de monitoreo y *cibersoporte* ante la atención de requerimientos e incidentes, así como 20 licencias adicionales de la solución *endpoint GravityZone Small Business Security* de *Bitdefender*.

- *Backup Plus*: El segundo incluye 5 TB adicionales para almacenamiento de respaldo y restauración de información en *Azure Backup*, así como 20 licencias adicionales de la solución *endpoint GravityZone Small Business Security* de *Bitdefender*.

4.6. Métricas Clave

El propósito de este módulo es el de identificar las actividades/acciones clave para la toma de decisiones y para futuro monitoreo.

Se empleó la metodología de Dave McClure (2010), el cual se conoce como las métricas piratas. Este propone que las métricas acompañen la estructura de un embudo de conversión: adquisición (¿cómo te encuentran los clientes?) / activación (¿tienen los clientes una primera buena experiencia?) / retención (¿los clientes vuelven?) / ingresos (¿cómo se gana dinero?) / referencias (¿te recomiendan los usuarios?). De esta manera, se toma como fuente la información previamente detallada y, se definen las siguientes métricas:

- **Tasa de adopción/conversión:** Número de pymes del sector activas que han adoptado el paquete de *ciberseguridad*.
- **Satisfacción del cliente (Net Promoter Score - NPS):** Satisfacción general de los clientes con la solución adquirida, a través de la evaluación de su recomendación.
- **Tasa de retención de clientes:** Número de clientes que se mantienen con la solución durante un período determinado.
- **Margen de beneficio bruto:** Beneficio bruto en relación con los ingresos totales, de modo que se pueda evaluar la rentabilidad de la solución.
- **Costo de adquisición de clientes (CAC):** Costo promedio que se asume/incurre por adquirir un nuevo cliente.
- **Tiempo de respuesta ante incidentes:** Tiempo promedio que toma la solución en resolver los incidentes reportados por los clientes.
- **Nivel de atención de *ciberincidentes*:** *Ciberincidentes* que se han detectado y mitigado con éxito dentro del SLA del servicio brindado al cliente.

- **Tiempo de recuperación de datos:** Tiempo necesario para que se restauren los datos de respaldo en caso de un incidente de seguridad.

4.7. Ventaja Competitiva

El propósito de este módulo es reflejar lo que distingue a la solución frente a otras alternativas y competidores.

Después de haber delimitado el problema, la propuesta de valor, el segmento de cliente objetivo, así como detallar la solución y las métricas clave de medición, se ha determinado que la ventaja competitiva del modelo de negocio radica en 3 aspectos. El primero busca brindar un servicio *e2e* (*end-to-end)* garantizando el contacto con las pymes y una adaptabilidad para integrarse sin mayor inconveniente con la infraestructura que soporta el *core business* de la pyme.

Asimismo, se ofrece un servicio completo y rentable al proporcionar una serie de componentes que por separado son más caros, como la solución *endpoint*, el espacio cloud, especialistas en *ciberseguridad* y un programa de concientización personalizado; los cuales en conjunto permiten establecer un nivel base de *ciberseguridad* que acompañe el éxito de la pyme.

Por último, se resalta la escalabilidad del servicio en sí, puesto que a medida que las pymes crezcan, el paquete de servicios es lo suficientemente flexible para adaptarse a sus necesidades cambiantes sin requerir grandes inversiones adicionales o cambios muy drásticos en la integración y configuración de la operación. Esto fortalece la inversión de parte de las pymes en optar por un servicio a largo plazo.

4.8. Canales

El propósito de este módulo es el de definir cuál será el medio adecuado para hacer llegar la solución (paquete de servicios) a los clientes.

Si bien existen canales tradicionales de distribución y contacto con el cliente, hace unos años la tendencia se ha volcado hacia la *virtualización*, tal como menciona Lewandowski (2016). En ese punto, se hace referencia a que los negocios deben tener

la capacidad de contar con canales donde virtualmente pueden vender y comunicar la propuesta de valor y el producto/servicio. Es por eso por lo que para la solución propuesta se han seleccionado el siguiente *mix* de canales:

- **Ventas directas:** Disponer de la posibilidad de ofrecer y adquirir la solución a través de un Ejecutivo Comercial que se contacte y pueda ser contactado por las pymes interesadas.

- **Plan de referidos:** Apoyarse de un programa de referencias para incentivar a los clientes actuales para que recomienden la solución a otras pymes.

- **Redes sociales (Marketing digital):** Utilizar los medios actualmente populares para tener contacto con los clientes interesados de las pymes. En el portal de *Facebook*, *Instagram* y *TikTok* podrán tener infografía de la empresa y números de contacto. La comunicación por *whatsapp* también estará habilitada.

- **Canal audiovisual (Marketing de contenidos):** Mediante un canal de *YouTube* los clientes actuales tendrán la posibilidad de acceder a material informativo y audiovisual (tutoriales, *webinars*, guías, etc.) que les permitirá estar actualizados sobre lo último en *ciberseguridad* y algunos conceptos importantes que los ayudará a crear conciencia y adoptar mejores prácticas.

- **Alianzas estratégicas:** Asociaciones con otras empresas y/o canales que tenga una relación establecida con el público objetivo, pymes de Lima Metropolitana del sector construcción e inmobiliaria, de modo que se pueda ampliar el alcance actual.

- **Eventos & ferias:** Presencia en eventos y ferias comerciales que tengan relación con el segmento de las pymes y tópicos tecnológicos para poder establecer contactos con clientes interesados.

4.9. Estructura de Costos

El propósito de este módulo es el de determinar y analizar cuáles serán los principales gastos en los que se incurrirá.

La estructura de costos propuesta tiene en consideración el alcance de la solución, el cual es el de un paquete de servicios de *ciberseguridad* conformado por la plataforma *endpoint GravityZone Small Business Security* de *Bitdefender*, el servicio de *Azure Backup* y un programa de concientización en *ciberseguridad* para los colaboradores.

- **Talento humano:** Costos del personal contratado y encargado de la operación del negocio (desarrollos, implementaciones, soporte y servicio al cliente).

- **Componente tecnológico:** Costos asociados a la adquisición, integración e implementación de la solución (antivirus, *firewall* y seguridad empresarial para protección de correo).

- **Infraestructura y *hosting*:** Costos de hardware y software que soporten la solución (almacenamiento, servidores, licencias de software y servicio de *hosting* en nube).

- **Costos operativos:** Gastos generales asociados a la operación del negocio (alquiler del espacio físico, servicios de agua, luz, entre otros).

- **Marketing:** Costos para comercializar, promocionar y publicitar el paquete diseñado de *ciberseguridad*.

4.10. Flujo de Ingresos

El propósito de este módulo es el de precisar la razón detrás del por qué y cómo los clientes pagarían por la solución determinada.

Dado la propuesta de valor antes descrita y también las consideraciones del costo, se están tomando en cuenta los siguientes aspectos para el flujo de ingresos esperados:

- **Suscripción de la solución:** Pago de una tarifa recurrente (frecuencia puede ser mensual, trimestral o anual) para disponer del paquete *Cyber Plus*.

- **Productos/Servicios adicionales:** Pago por servicios adicionales y que forman parte del catálogo del negocio, los planes *Support Plus* y *Backup Plus*.

4.11. Fundamento teórico de la generación de valor

En esta sección se justifica cómo se genera valor a través de la solución, la cual es un ejemplo de *re-packing* de recursos y capacidades porque combina una solución endpoint de *Bitdefender*, espacio de respaldo y restauración en *Azure Backup*, monitoreo y gestión de requerimientos e incidentes, y un programa de concientización. Cabe mencionar que estos recursos y capacidades provienen de diferentes fuentes, como proveedores de software y servicios de nube. De esta manera, la generación de valor se gesta a partir de:

- **Reducción de costos:** El *re-packing* permite ofrecer una solución integral a un precio más competitivo que las soluciones de seguridad tradicionales.
- **Mejora de la eficiencia:** El *re-packing* facilita a las pymes la implementación y el uso de una solución de seguridad integral.
- **Mejora de la innovación:** El *re-packing* permitirá ofrecer una solución de seguridad que se adapta a las necesidades cambiantes de las pymes.

Por lo tanto, se esperaría que las pymes se beneficien de la solución dado que:

- No poseen los recursos necesarios para implementar una solución de seguridad integral puede beneficiarse de una solución de seguridad que combina recursos de diferentes proveedores.
- Necesitan una solución de seguridad que se adapte a sus necesidades específicas por lo que valorarían una solución que se puede personalizar.
- Quieren mantenerse al día con las últimas amenazas cibernéticas lo que destaca que se proponga una solución de seguridad que se actualiza regularmente.

Se tiene el compromiso no solo con la protección digital de las pymes, sino también con el fortalecimiento del tejido social y económico de Lima, y del país, más adelante. Se sabe que las pequeñas y medianas empresas son el motor económico del país y, al brindarles servicios integrales de *ciberseguridad*, se les permite operar con confianza y seguridad en el mundo digital. Además, el programa de concientización ofrecido garantiza que los colaboradores, quienes son a la vez ciudadanos del país, estén

informados y preparados para enfrentar *ciberamenazas*, elevando así el nivel general de conocimiento y preparación en esta área vital. Al ir más allá de lo que ofrece la competencia, se reafirma el compromiso con una visión más amplia: una sociedad donde la *ciberseguridad* y el conocimiento empoderen a las pymes para crecer, innovar y contribuir al bienestar colectivo.

4.12. Conclusiones del capítulo

El capítulo se ha centrado en desarrollar la propuesta del modelo de negocio, considerando todos los elementos clave bajo el modelo del *Lean Canvas*. Se buscará validar y justificar esta hipótesis en el siguiente capítulo de metodología de investigación, a través del uso de herramientas que ayudarán a estimar la demanda y perfilar aún más la solución propuesta.

CAPITULO 5 . METODOLOGÍA DE LA INVESTIGACIÓN

En el presente capítulo se va a desarrollar la metodología de la investigación para el estudio y evaluación de la viabilidad del plan de negocios para la oferta de servicios de *ciberseguridad* para las pymes en Lima, acotado bajo el *MVP* enfocado en el sector de construcción e inmobiliaria.

5.1. Diseño de la Investigación

Considerando la complejidad de la temática elegida, se ha considerado optar por metodologías de análisis cuantitativo.

Para llevar a cabo esta investigación, se han utilizado diversas fuentes de información, como libros, artículos académicos, informes especializados y normativas relacionadas con la problemática de análisis. Estas fuentes ayudan a establecer las bases teóricas académicas necesarias para comprender los aspectos fundamentales de la *ciberseguridad* y su aplicación en el contexto de las pymes.

El estudio realizado busca analizar e investigar a través de una encuesta a una muestra de colaboradores (gerentes, responsables de TI, etc.) de pymes del sector priorizado en Lima Metropolitana, con el fin de validar las premisas sobre las necesidades y soluciones propias del modelo de negocio en materia de *ciberseguridad*.

Asimismo, esto permitirá identificar y estimar la demanda, así como revisar las brechas existentes y las áreas de mejora en relación con las condiciones mínimas, básicas y escalables de *ciberseguridad* requeridas por las pymes del sector y de la región, sobre todo considerando que no se cuenta con información estadística previa lo suficientemente relevante como para tomarla de referencia.

5.2. Objetivos de la Investigación

Esta investigación se propone para validar la solución planteada en el modelo de negocio de modo que se pueda mejorar el servicio cumpliendo con las condiciones básicas y escalables de *ciberseguridad* para las pymes de Lima.

Los objetivos principales de la presente investigación de carácter cuantitativo serán:

- Comprender el panorama actual de las pymes de Lima y constatar el nivel de digitalización en la que se encuentran.

- Recopilar datos y estadísticas sobre la percepción y el nivel de conocimiento de las pymes de Lima en relación con la problemática.

- Obtener información relevante sobre las necesidades y expectativas de las pymes del sector construcción de Lima que permita definir los criterios fundamentales del plan de negocios.

- Identificar si la propuesta de plan de negocio desarrollada en esta investigación tendrá aceptación en el mercado de las pymes del sector construcción de Lima.

- Definir la herramienta a utilizar para realizar el estudio de mercado que permita validar el plan de negocio.

5.3. Fuentes de Información

A continuación, se presentan las fuentes de información utilizadas en la investigación para el plan de negocios, de acuerdo con la metodología desarrollada.

5.3.1. Fuentes Secundarias

Para obtener información económica, tendencias de mercado y calcular el mercado objetivo, se han utilizado fuentes secundarias tales como reportes y estadísticas obtenidas del INEI, SUNAT, Ministerio de Producción, BCRP, entre otros.

Asimismo, para obtener información sobre el panorama de *ciberseguridad*, se ha recurrido a diarios de renombre, reportes de marcas de soluciones de *ciberseguridad* y blogs dedicados a *ciberseguridad*, encuestas y estudios previos de temas relacionados.

5.3.2. Fuentes Primarias

Considerando que la problemática planteada no tiene una base de datos y/o algún estudio específico a fin de obtener datos relevantes y confiables que sustenten la presente investigación, ha sido necesario generar estos datos a través de un sondeo (Ver anexo 6) y una encuesta (Ver anexo 7).

Para la elaboración del cuestionario para la encuesta aplicada, se partió de la definición de objetivos específicos, para posteriormente elaborar las preguntas que respondan a estos objetivos. Se aplicará la encuesta a representantes de las empresas del sector construcción, lo que permitirá obtener una base de datos y tendencias que permitirán validar el modelo de negocio y posteriormente construir las distintas estrategias del plan de negocios.

5.4. Metodologías de Análisis Cuantitativo

Como parte del enfoque cuantitativo se han recolectado datos estadísticos del informe "Perú: Estructura Empresarial, 2020" (INEI, 2022), adicionalmente se realizó un sondeo inicial que permitió identificar el universo de pymes en Lima, complementándolo con información relevante del informe "Transformación con sentido digital 2022: Madurez digital de las organizaciones en Perú" (EY, 2022).

Considerando lo limitado de la información disponible sobre la problemática, la carencia de normativa que regule estas prácticas en los distintos sectores, pese a que se están haciendo algunos esfuerzos por generar conciencia respecto de esta necesidad creciente, sumándole a la realidad de las pymes en general, sin discriminación de sectores en el Perú, la gran informalidad, las constantes bajas de pymes, la poca vida que muchas de ellas llegan a tener, la realidad de que no se cuenta con un censo que permita identificarlas rápidamente o contar con información precisa de sus necesidades; se logró definir como técnica de selección de muestra, el método de muestreo no probabilístico por conveniencia.

"El muestreo no probabilístico por conveniencia es un tipo de técnica de muestreo en la que las muestras se seleccionan según la conveniencia del investigador, lo que le permite elegir arbitrariamente cuántos participantes puede haber en el estudio. Esta técnica se basa en un juicio subjetivo en lugar de hacer la selección al azar" (Ortega, 2023).

En este sentido se decidió realizar una encuesta priorizando el público objetivo del sector y que permita validar la problemática definida en esta investigación y el modelo de negocio desarrollado en el capítulo anterior, identificando información relevante para complementar este modelo. Se revisaron fuentes secundarias para acotar y estructurar

las preguntas que se incluyeron en la encuesta. Para este levantamiento de información se usó la aplicación *Google Forms*. El detalle de estas preguntas se encuentra planteado en el Anexo 7 – Estructura de la Encuesta para validación del Modelo de Negocio enfocado al segmento de construcción de las pymes.

El universo de las pymes del sector construcción en Lima es de 3995 según el informe "Perú: Estructura Empresarial, 2020" (INEI, 2022).

Tabla 5.1 Cantidad de pymes del sector construcción en Lima en 2020

ACTIVIDAD ECONÓMICA	TOTAL		MICROEMPRESA		PEQUEÑA EMPRESA		GRAN EMPRESA		MEDIANA EMPRESA	
	ABS	%	ABS	%	ABS	%	ABS	%	ABS	%
TOTAL	1,281,871.00	100	1,208,678.00	100	60,799.00	100	10,146.60	100	1,127.40	100
Agricultura, ganadería, sil. y pesca	5,256.00	0.4	4,051.00	0.3	926.00	1.5	250.2	1.5	27.8	2.5
Exploración de minas	4,777.00	0.4	4,091.00	0.3	407.00	0.7	251.1	0.7	27.9	2.5
Industrias manufactureras	112,012.00	8.7	102,925.00	8.5	7,524.00	12	1402.2	12	155.8	13.8
Electricidad, gas y agua	3,273.00	0.3	2,847.00	0.2	322.00	0.5	93.6	0.5	10.4	0.9
Construcción	33,111.00	2.6	28,218.00	2.3	3,895.00	6.4	896.4	6.4	99.6	8.8
Comercio y rep. de vehículos y moto	559,041.00	43.5	532,796.00	44.2	22,215.00	37	3624.3	37	402.7	35.7
Transporte y almacenamiento	78,173.00	6.1	72,322.00	6	5,006.00	8.2	759.6	8.2	84.4	7.5
Actividades de alojamiento	5,957.00	0.5	5,511.00	0.5	387.00	0.6	52.2	0.6	5.8	0.5
Actividades de servicio de comida y bebidas	80,186.00	6.3	77,846.00	6.4	2,170.00	3.6	152.1	3.6	16.9	1.5
Información y comunicaciones	30,536.00	2.4	28,211.00	2.3	1,940.00	3.2	342.9	3.2	38.1	3.4
Servicios prof,, técnicos y de apoyo empresarial	136,552.00	10.6	126,589.00	10.5	8,678.00	14	1125.9	14	125.1	11.1
Otros servicios 1/	232,997.00	18.2	223,271.00	18.5	7,329.00	12	1196.1	12	132.9	11.8

Fuente: Perú Estructura Empresarial, INEI, 2022.
Elaboración: Autores de esta tesis.

5.5. Objetivos de la Encuesta

- Obtener información necesaria sobre el segmento elegido identificando su posición dentro de la empresa y su nivel de influencia para la toma de decisiones.

- Identificar el grado de experiencia con otros productos y/o servicios similares que tiene el público objetivo.

- Conocer el grado de digitalización en el que se encuentran las empresas pymes del sector construcción.

- Tener una primera aproximación al monto que el público objetivo estaría dispuesto a invertir por el servicio.

- Definir el paquete de servicios a ofrecer y los servicios adicionales que se evaluarían para ampliar la gama de servicios.

- Definir canales de comunicación para el soporte del servicio.

5.6. Criterio de segmentación

El desarrollo de este análisis se enfocó en las pymes de Lima Metropolitana, que se encuentren en proceso de transformación o que hayan pasado por un proceso de transformación digital que no cuenten con un área de *ciberseguridad*.

Esta definición toma en consideración el análisis del segmento de clientes en el capítulo anterior, modelo de negocio. De igual manera, se incluye en esta definición el sondeo inicial y la complejidad de abordar a todos los sectores de las pymes y enfocarse inicialmente en uno de los sectores con mayor oportunidad dado su nivel de madurez digital.

Se utilizo el método TAM, SAM, SOM, para segmentar el mercado en diferentes niveles, mediante el cual con una estrategia *Top-Down* para segmentar desde lo global a lo particular.

Producto del análisis, se han determinado y formalizado los siguientes criterios de segmentación, que acompañará la estructura de la herramienta cuantitativa seleccionada, la encuesta:

- **Tamaño de la empresa:** Se definirá el mercado total o TAM (*Total Addressable Market*) para acotar en primera instancia el mercado a las pymes. Dado que el presente análisis se centra en las pymes, es necesario indicar las características de cada una de ellas en función de la cantidad de empleados y definir la estrategia adoptada considerando sus necesidades específicas.

- **Pequeñas empresas:** Aquellas con entre 10 y 50 empleados, un mayor nivel de operaciones y hasta 1700 UIT de facturación anual.

- **Medianas empresas:** Aquellas con entre 50 y 250 empleados, una estructura organizativa más compleja y hasta 2300 UIT de facturación anual.

- **Ubicación geográfica:** Se determinará el mercado disponible o SAM *(Service Addressable Market*), acotando el segmento a su ubicación geográfica, en este caso las pymes en Lima Metropolitana.

- **Sector empresarial:** Se acotará el mercado disponible o SAM para definir el mercado obtenible y útil o SOM (*Service Obtainable Market*), en este nivel de segmentación se buscará justificar el sector elegido para el análisis desarrollado en el presente plan de negocios. Considerando la complejidad de buscar representatividad en todos los sectores del público objetivo que son las pymes, se priorizó al sector que mayor afinidad y predisposición demostró en el sondeo inicial, tanto como el cruce de la información asociada a la madurez digital. Para el *MVP* el sector seleccionado es: construcción e inmobiliaria, tal como se sustentó en el capítulo anterior.

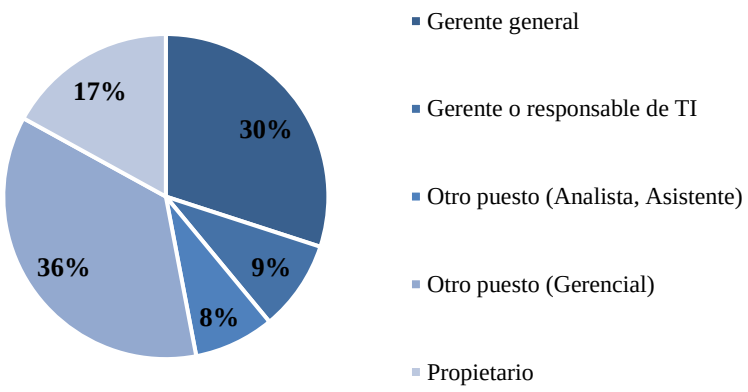
- **Madurez digital:** El segmento objetivo apunta a aquellas pymes que están aún en proceso de transformarse digitalmente y aquellas que ya están más consolidadas en cuestión de transformación digital. Considerando que el sector construcción es uno de los sectores que mayores esfuerzos está haciendo en materia de transformación digital y adicionalmente cuenta con ciertas condicionantes propias de la disciplina.

5.7. Resultados del Análisis Cuantitativo

Dado el público objetivo definido y las preguntas seleccionadas (Anexo 7: Encuesta para validación de Modelo de Negocio) para estimar la demanda y afinar el modelo de negocio se tienen las siguientes respuestas a las encuestas a 100 representantes de pymes limeñas que corresponden al sector construcción e inmobiliario:

- Puestos que ocupan los representantes que participaron de cada empresa. Se muestra resultado en Ilustración 5.1:

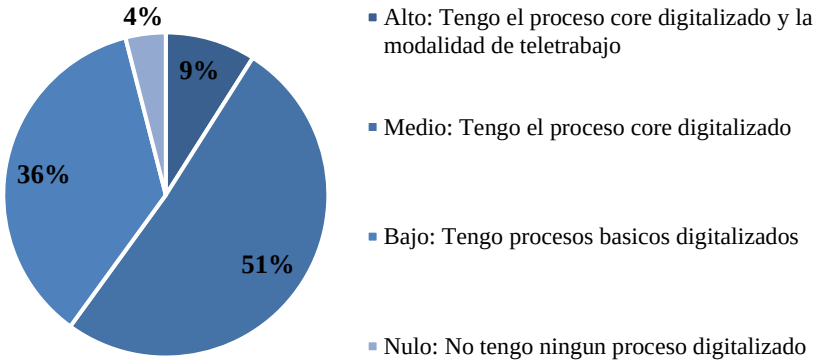
Ilustración 5.1 Puestos por empresas en pymes



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Nivel de transformación digital en el que se encuentran las empresas según representantes encuestados. Se muestra resultado en Ilustración 5.2:

Ilustración 5.2 Nivel de Transformación Digital en pymes del sector Construcción

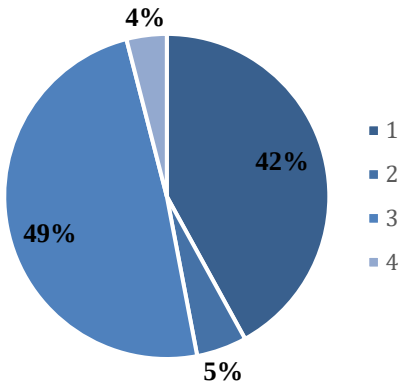


Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Calificación del servicio de *ciberseguridad* previamente ofrecido por otras empresas, tomando como escala del 1 al 5, donde 1 es "Muy insatisfecho" y 5 es "Muy satisfecho". En caso no se haya contratado, se deberá colocar 3. El resultado de esta pregunta se muestra en la Ilustración 5.3:

-

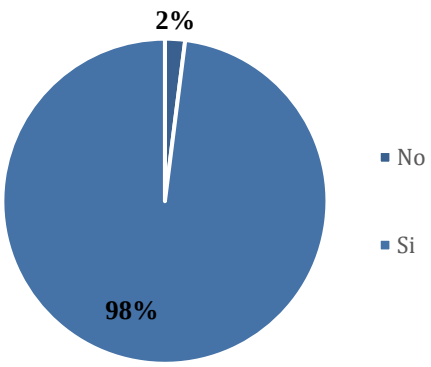
Ilustración 5.3 Clasificación de experiencia con servicios de *Ciberseguridad* o empresas que han brindado estos servicios anteriormente



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Cantidad de interesados y dispuestos a adquirir la solución propuesta de: Monitoreo y *cibersoporte* centralizado de eventos e incidentes a través del licenciamiento y configuración de una solución *endpoint* con módulos *anti-malware*, *anti-exploit*, *anti-phishing*, prevención de fraude y ataques basados en *scripts* y *firewall* (*partner* estratégico de marca líder), configuración de seguridad y accesos para navegación web contra amenazas de descarga de *malware* y páginas fraudulentas, configuración de seguridad y accesos para proteger tus correos e información en la nube contra el *phishing*, *malware* y *ransomware*, almacenamiento en la nube para respaldo y restauración ante un ciberincidente, y programa de concientización para los colaboradores. Se muestra el resultado en la Ilustración 5.4:

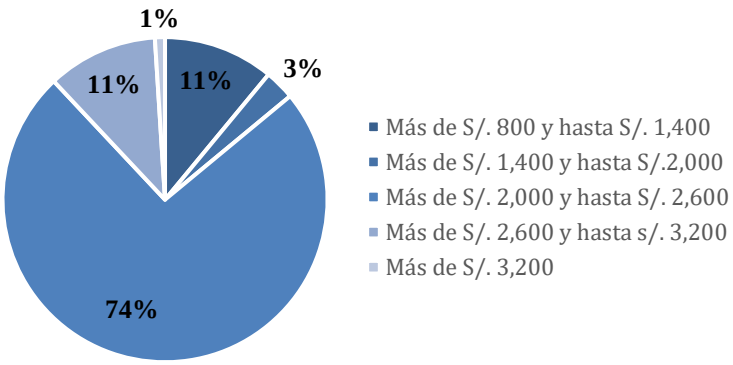
Ilustración 5.4 Interés por tomar el paquete de *Ciberseguridad* propuesto



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Rango de precios para el pago mensual que estarían dispuestos a asumir por el paquete de *ciberseguridad*. Se muestra el resultado en la Ilustración 5.5:

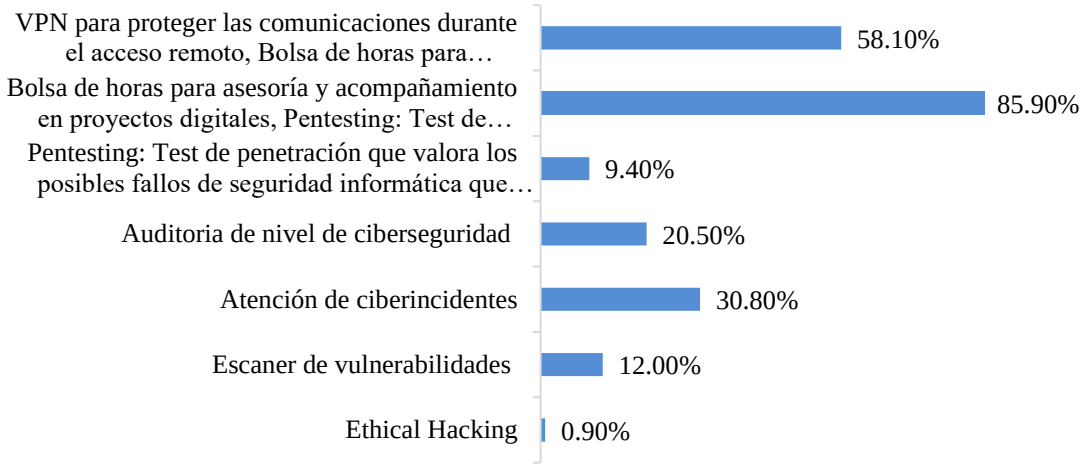
Ilustración 5.5 Pago que estarían dispuesto a pagar mensualmente por el servicio descrito



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Servicios adicionales que le gustaría añadir al paquete: *VPN* para proteger las comunicaciones durante el acceso remoto y/o bolsa de horas para asesoría y acompañamiento en proyectos digitales y/o *pentesting* (test de penetración que valora los posibles fallos de seguridad informática que puede tener un sistema y qué alcance tienen dichos fallos) y/o auditoría de nivel de *ciberseguridad* y/o atención de *ciberincidentes* y/o escáner de vulnerabilidades. Se muestra el resultado en la Ilustración 5.6:

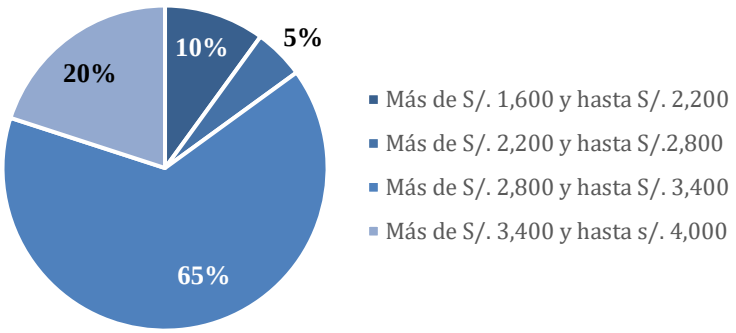
Ilustración 5.6 Servicios adicionales para el paquete de *Ciberseguridad*



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Rango de precios para el pago mensual que estarían dispuestos a asumir por el paquete de *ciberseguridad* si se le añadiera los servicios adicionales. Se muestra resultado en Ilustración 5.7:

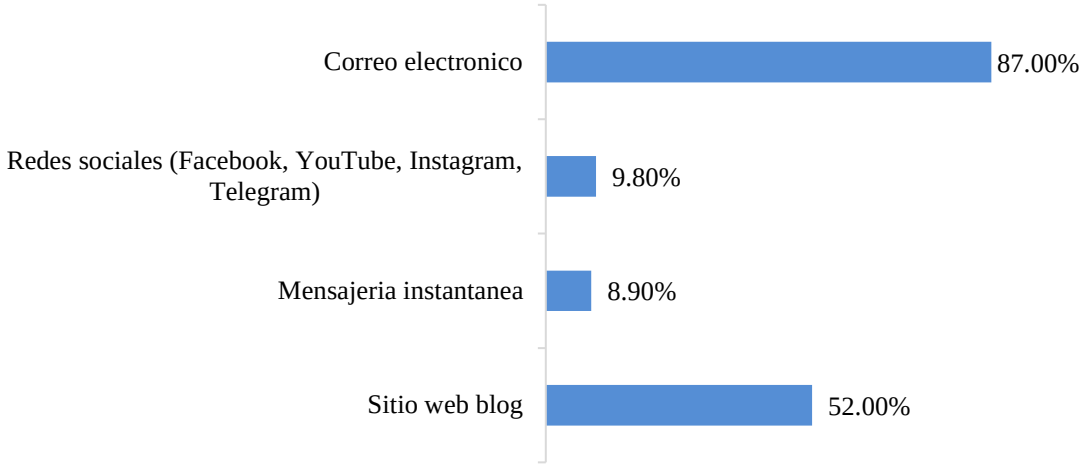
Ilustración 5.7 Pago que estarían dispuesto a pagar mensualmente si se añadieran servicios adicionales al paquete definido



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Canales de comunicación que prefieren para contactarse, concretar informarse sobre amenazas de *ciberseguridad*, charlas online y promociones en servicios. Se muestra resultado en Ilustración 5.8:

Ilustración 5.8 Preferencia de canales de comunicación



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

5.8. Evidencias preliminares de la Investigación

Después de organizar, revisar y analizar los resultados del análisis cuantitativo aplicado a la muestra seleccionada, se tienen los siguientes *insights*, evidencias preliminares de la investigación:

- Se tuvo un alto grado de aceptación respecto a la propuesta de negocio para el público objetivo; dado que el 97% de la muestra estaría dispuesto a tomar el paquete de servicio de *ciberseguridad*.

- El 91% de los encuestados tienen puestos gerenciales y/o son propietarios de las pymes del sector de construcción e inmobiliarias por lo que su opinión e influencia en la empresa es altamente considerada.

- La mitad de los representantes de las pymes encuestadas, consideran que su empresa se encuentra en un nivel intermedio de transformación digital, es decir cuentan con al menos el proceso central de su actividad digitalizado y sólo el 10% de la muestra posee un nivel alto por lo que ya dispone regularmente de la modalidad de teletrabajo.

- El precio mensual que la mayoría, 73%, de la muestra estaría dispuesta a pagar por el paquete inicial de *ciberseguridad* oscila entre los S/ 2,000 y S/ 2,600. En el caso de querer adicionar algún servicio al paquete definido, la selección más popular, 59%, incluye al *VPN* para proteger las comunicaciones durante el acceso remoto. De esta manera, la combinación que más se demandó sería la del *VPN* más la bolsa de horas para asesoría y acompañamiento en proyectos digitales. Por otro lado, estos adicionales suponen un incremento en el rango inicial de S/ 800.

- El 70% de los encuestados no han contratado servicios de *ciberseguridad* en el pasado. Adicionalmente, ninguno calificó su experiencia como muy satisfactoria.

- El canal de comunicación único que tienen la predilección de la muestra es el correo electrónico con un 39% de selección. Sin embargo, el mix de canales que más destaca, 43%, es adicionarle al correo las comunicaciones a través de un sitio web y/o blog.

5.9. Concept Testing

El *concept test* es una herramienta de evaluación durante la investigación de mercado para validar la aceptación de un producto antes de su lanzamiento, debido a que ayuda a comprender cómo los potenciales clientes perciben una idea o diseño inicial y a obtener información valiosa sobre su utilidad y posibles mejoras antes de producirlo y llevarlo al mercado.

En el caso de la solución desarrollada en el capítulo de modelo de negocio, se hubieran complementado los resultados de la encuesta con el siguiente planteamiento del concepto que se realizaría al público objetivo priorizado y hubiera sido moderado por el equipo de trabajo:

Ilustración 5.9 *Concept Test* de la solución

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Este concepto gráfico estaría acompañado de un par de preguntas bajo enfoque de escala de Likert y otros que hubieran permitido certificar cierta información:

- Después de leer la descripción del servicio propuesto, ¿estaría interesado en adquirirlo? (Desinteresado / No muy interesado / Indiferente / Interesado / Muy interesado)
- ¿Qué características son los más valiosos para usted? (Pregunta abierta)
- Después de leer la descripción, ¿qué precio esperaría pagar mensualmente por el servicio? Favor de registrar un número, no rango. (Pregunta abierta)

5.10. Conclusiones del capítulo

De esta manera, dada la metodología de investigación seleccionada para recoger información a través de encuestas dirigidas a representantes del segmento objetivo, se pudo validar preliminarmente la intención de compra en base a la solución propuesta en el modelo de negocio. Sin embargo, se reconoce la limitación de no haber realizado la pregunta de intención de compra bajo una escala de Likert o bajo el modelo del *Concept Testing* que se definió en el inciso anterior pero no fue probado. Por otro lado, se pudo conocer cuáles serían las características (precio y servicios adicionales) que esperarían los clientes. Por lo tanto, ya definida y mejor perfilada la solución, se procederá a definir los planes estratégicos en los siguientes capítulos, empezando por el plan de marketing.

CAPITULO 6 . PLAN DE MARKETING

6.1. Objetivos del plan de Marketing

El objetivo central del presente plan de marketing es incrementar la visibilidad, generar confianza y captar nuevos clientes que busquen adquirir el paquete de servicios de *ciberseguridad* especializada en pymes.

6.1.1. Objetivos específicos

Dentro del marco de análisis *SMART (Specific, Mesurable, Achivable, Relevant and Time)* del presente plan de marketing, se definen los siguientes objetivos específicos:

- Obtener por lo menos una cuota de mercado del 3.5% del público objetivo en el primer año.
- Mantener una Tasa de Abandono del servicio menor al 25% al término de la suscripción.
- Conseguir al menos 2000 seguidores en las redes sociales en el primer año de operación, y apuntar a un crecimiento de 15% anual.
- Conseguir una tasa de solicitud de Demos por la web en un 20% en el primer año.
- Conseguir una tasa de conversión de ventas en un 15% en el primer año.
- Obtener al menos un 65% de clientes satisfechos tras el primer año de operación.
- Obtener al menos 30% de referidos por cada cliente, tras el primer año de operación.

6.1.2. Indicadores claves de desempeño

Para medir el cumplimiento de los objetivos específicos planteados se utilizarán los siguientes criterios de desempeño:

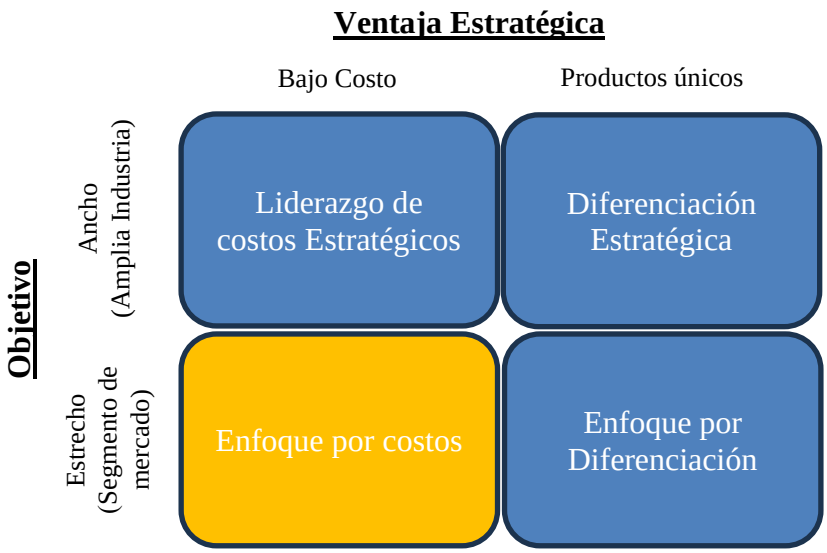
- Cuota de Mercado
    - Métrica: Cuota de Mercado
    - Cálculo: Ventas de *CyberWave* / Total de Mercado * 100%
- Tasa de Abandono del servicio
    - Métrica: Tasa de Abandono

    - Cálculo: (Número de Clientes que abandonaron el servicio / Total de Clientes) * 100%
- Crecimiento de Seguidores en Redes Sociales:
    - Métrica: Crecimiento de Seguidores
    - Cálculo: (Número de Seguidores al final del año - Número de Seguidores al inicio del año) / Número de Seguidores al inicio del año) * 100%
- Tasa de Solicitud de *Demos* por la Web:
    - Métrica: Tasa de Solicitud de *Demos*
    - Cálculo: (Número de Solicitudes de *Demo* / Total de Visitas a la Web) * 100%
- Tasa de Conversión de Ventas:
    - Métrica: Tasa de Conversión de Ventas
    - Cálculo: (Número de Ventas / Número de Visitantes) * 100%
- Porcentaje de Clientes Satisfechos:
    - Métrica: Porcentaje de Clientes Satisfechos
    - Cálculo: (Número de Clientes Satisfechos / Total de Clientes) * 100%
- Porcentaje de Referidos:
    - Métrica: Porcentaje de Referidos
    - Cálculo: (Número de Referidos / Total de Clientes) * 100%

6.2. Estrategia Genérica de Enfoque

Según lo planteado por Michael Porter, las estrategias genéricas representan herramientas empresariales cuyo propósito radica en que una compañía logre ventajas competitivas dentro del mercado en el que se desenvuelve (*HubSpot*, 2023).

Ilustración 6.1 Estrategias Genéricas de Porter



Fuente: *Hubspot*.
Elaboración: Autores de esta tesis

Para el plan de negocios desarrollado, se ha optado por la estrategia genérica de "Enfoque" por costos. Esta se orienta hacia un segmento específico del mercado en lugar de buscar abarcarlo en su totalidad y ofrece el precio más bajo posible. Usualmente se dirige hacia un nicho particular en el que la empresa puede sobresalir, ya que se busca aumentar la participación de mercado al satisfacer las necesidades y demandas específicas de un grupo de clientes relevante o menos atendido" (*HubSpot*, 2023).

Considerando lo detallado en el del capítulo 4 sección 4.4, el segmento en el cual se está enfocando la solución de *ciberseguridad* corresponde a las pymes en Lima del sector de construcción. El servicio diseñado se enfoca en cubrir las necesidades específicas y mínimas de las pymes en materia de *ciberseguridad* y a un costo bajo y atractivo, considerando que la competencia es mínima en este segmento para el rubro de *ciberseguridad*.

Esta decisión se respalda en análisis del macroentorno y de las fuerzas de la industria, analizadas en el capítulo 3, así como en la definición del modelo de negocio en el capítulo 4.

6.2.1. Factores Críticos para el éxito

Los factores críticos del éxito se definen como aquellos elementos que permiten a una empresa crear y mantener una ventaja competitiva sostenible en el mercado, basándose en el desarrollo y la explotación de sus competencias básicas (*hubspot*, 2021)

En ese sentido, para el plan de negocios desarrollado se están considerando los siguientes ámbitos para los factores críticos de éxito (EAFIT, 2005):

- El ambiente económico y sociopolítico que contiene a la empresa.
- El sector industrial en que se compite
- La empresa (a nivel de áreas administrativas formalmente constituidas, de funciones específicas de negocio y de individuos clave para el éxito de la estrategia).

En referencia al análisis del macroentorno socioeconómico y sociopolítico del capítulo 3, es importante destacar como factores críticos la "Adaptabilidad", "establecimiento de Alianzas Estratégicas" y "Alineación con la Transformación Digital".

En relación con el análisis de las fuerzas competitivas del sector industrial del mismo capítulo 3, surgen como factores críticos la "Innovación Continua" y la prestación de un "Servicio enfocado".

Considerando que la empresa aún no está constituida, se están evaluando los atributos clave para su establecimiento y operación. Entre los aspectos más relevantes se encuentran el "conocimiento del mercado", la "Educación y Sensibilización" adecuada de los clientes, así como contar con un "Equipo Altamente Capacitado y Especializado".

Tabla 6.1 Factores Críticos de éxito para el plan de negocios de *Cibersoporte*

Ámbito	Factor Crítico
Ambiente Económico y socio político	• Adaptabilidad • Alianzas Estratégicas • Alineación con metas de transformación Digital
Sector de *Ciberseguridad*	• Innovación Continua • Servicio enfocado
Interno de la Empresa	• Conocimiento del mercado. • Nivel de educación y sensibilización de clientes. • Equipo Capacitado y Especializado:

Fuente: Propia.
Elaboración: Autores de esta tesis.

6.3. Segmentación

De acuerdo con el modelo de negocio se ha definido que el segmento de clientes hacia quienes está enfocada la solución de *ciberseguridad* desarrollada, son las pymes.

Asimismo, en la segmentación realizada en el capítulo 4 numeral 4.4, se ha realizado un análisis a partir de la data de INEI (2022), identificando a 63 mil empresas pequeñas y medianas en Lima.

6.4. Selección del Mercado Meta

Dentro del segmento elegido, el mercado meta considerado para el lanzamiento del servicio, a las pymes del sector construcción e inmobiliaria. El motivo es debido a la creciente innovación tecnología en la que se encuentra el sector y el potencial para reforzar su *ciberseguridad* debido a la dificultades y riesgos que han presentado. Esto se detalla en el capítulo 4 numeral 4.4.

6.5. Posicionamiento

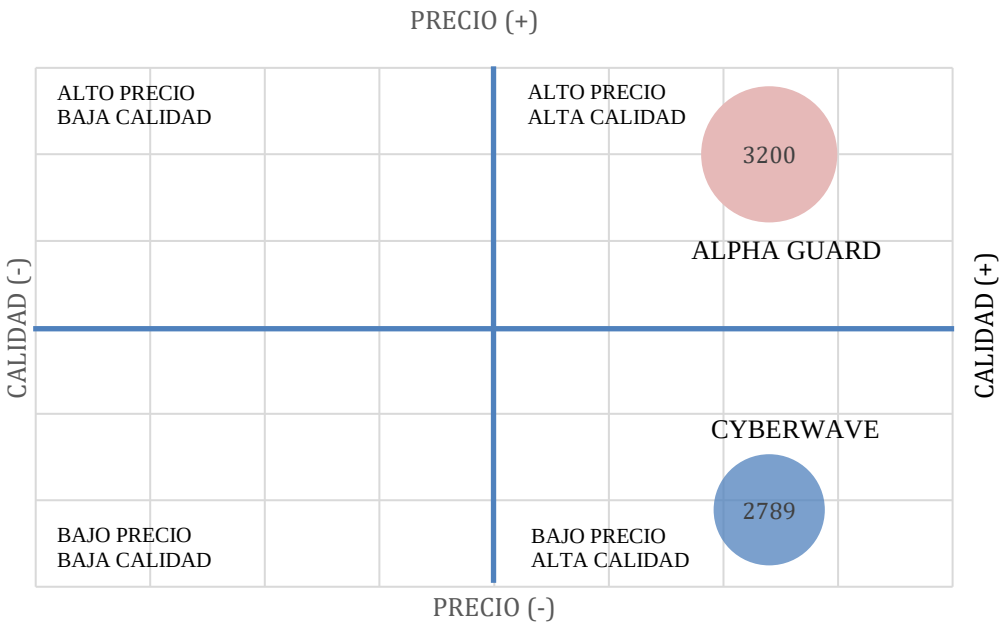
"De acuerdo con la perspectiva de Kotler, el posicionamiento de una empresa se refiere a cómo desea ubicarse en la mente de su audiencia objetivo. La posición de un producto, en este sentido, es cómo los consumidores lo perciben (Armstrong y Kotler, Fundamentos de Marketing, 2013).

La estrategia de posicionamiento que *CyberWave* ha adoptado tiene como objetivo establecer su marca y así ser percibido como una opción confiable, innovadora y

accesible, de acuerdo con las necesidades de las pymes del sector construcción e inmobiliaria. Es esencial mantener un enfoque en la educación del mercado y en la creación de conciencia y una cultura de prevención en el mercado objetivo en relación con los riesgos de *ciberseguridad* y la importancia de salvaguardar los activos digitales de las pymes.

Según lo indicado por Kotler, cada empresa debe diferenciar su oferta mediante la creación de un paquete único de beneficios que atraiga a un grupo sustancial dentro del segmento (Armstrong y Kotler, Fundamentos de Marketing, 2013) y dado a que el posicionamiento de una marca debe atender a las necesidades y preferencias del mercado meta definimos el uso de una matriz de posicionamiento para indicar la posición en el mercado.

Ilustración 6.2 Matriz de posicionamiento



Fuente: Propia.
Elaboración: Autores de esta tesis.

6.5.1 Diferenciadores de Marca

Es importante que los clientes reconozcan a *CyberWave* por los siguientes aspectos clave:

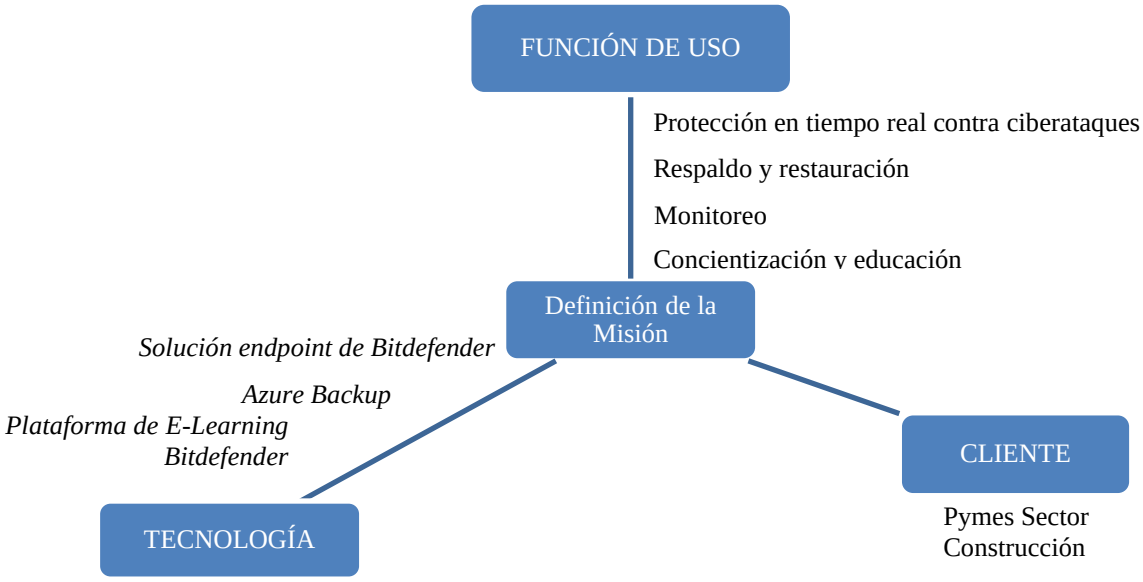
- Enfoque en el valor: Se ofrece una solución integral conformada por componentes integrados entre sí, dado que *CyberWave* es la única empresa que ofrece una combinación de servicios que suelen ofrecerse por separado y a un precio más alto. Se ofrece una solución *endpoint* muy completa a través de *Bitdefender*, un servicio de respaldo y restauración a través de *Azure Backup*, un servicio de monitoreo y gestión de requerimientos e incidentes y un programa de concientización para colaboradores. Esto se logra a través del equipo de marketing y ventas que busca resaltar este punto en la publicidad en redes sociales, puntos de contacto con clientes, demos, entre otros canales.
- Enfoque en el servicio al cliente: No solo busca proteger a través de la prevención, sino brindar un acompañamiento a través de su servicio de soporte y atención al cliente ofreciendo un servicio de postventa acorde a las necesidades particulares de cada pyme. Esto se logra a través de la asignación de un *Key Account Manager* que gestione los requerimientos de la pyme y habilitando un canal directo ante posibles incidentes manteniendo un buen nivel de comunicación, asegurando las respuestas oportunas a través de los distintos canales de comunicación, a fin de mantener un buen nivel de experiencia. También, mediante la encuesta de satisfacción enviada periódicamente se va midiendo el nivel de satisfacción y se obtiene retroalimentación valiosa para mantener actualizada la oferta de servicios y mejorar las prestaciones actuales.

6.5.2 Imagen de marca

La imagen de marca representa la propuesta de valor única, estableciendo un diferenciador significativo y que busca generar un impacto profundo en el público objetivo. De acuerdo con Jeff Bezos (2012), “La marca es lo que la gente dice de ti cuando no estás en la sala”. Para la creación de la imagen de marca, a continuación, se definen los elementos necesarios tales como la misión, la visión y valores, la misma que definimos a partir de la matriz o Modelo de Abell, que busca definir estos conceptos a partir del análisis de tres dimensiones:

- **Función de Uso:** Se refiere a las necesidades específicas del público objetivo, respondiendo a preguntas como ¿Qué es necesario? y ¿Cuáles son los requisitos que deben cumplirse?
- **Tecnología:** Hace referencia a las diferentes formas en que se pueden satisfacer estas necesidades, abordando la cuestión de ¿Cómo pueden ser satisfechas las necesidades de los clientes?
- **Cliente:** Se focaliza en el segmento al que nos dirigimos, respondiendo a preguntas como ¿Quién es nuestro público objetivo? y ¿Quiénes son los clientes a los que atendemos?

Ilustración 6.3 Matriz de las 3 dimensiones de Abell



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

De esta manera podemos delinear nuestra misión la misma que es la interacción de la Fusión de Uso, la Tecnología y el Cliente.

Asimismo, se ha desarrollado el logo, así como los elementos visuales de la marca considerando un escudo como ícono que refuerza la idea de seguridad dentro de un círculo que representa un perímetro seguro. Además, se ha optado por emplear colores neutros como el negro y un trazo de color celeste asociado a la sabiduría y confianza que se busca transmitir a los clientes con el servicio.

Además, se ha planteado el nombre de marca *CyberWave*, el cual refleja una poderosa fusión que consta de dos componentes. Por un lado, "*cyber*" representa el entorno digital y la tecnología asociada a *ciberseguridad*; mientras que "*wave*" evoca la imagen de una ola con su flujo constante y energía expansiva. Este nombre posiciona a la marca como una fuerza que se mueve en sintonía con el dinámico y cambiante mundo digital.

Ilustración 6.4 Logo de la marca

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Además, se busca garantizar una experiencia fluida y segura a lo largo de la relación con el cliente. Por ende, se ha definido el eslogan: "Tu Negocio, tu Pasión. La ciberseguridad, nuestra razón", el cual busca influir en la forma en la que los clientes perciben y se relacionan con *CyberWave*.

A través del modelo *Big Five Personality Dimensions*, se ha definido la identidad de marca:

- Apertura a la experiencia: *CyberWave* se mantiene a la vanguardia en *ciberseguridad* adoptando las últimas tendencias y tecnologías para garantizar la protección integral. Su enfoque no solo se limita a ofrecer herramientas de

protección, sino también a educar y concientizar, mostrando una perspectiva holística de los riesgos en el mundo digital.

- Responsabilidad: *CyberWave* se caracteriza por su compromiso inquebrantable con la protección de las pymes. Cada componente de su servicio garantiza que las empresas estén seguras, y este sentido de deber se refleja en cada interacción con el cliente.
- Extraversión: A pesar de operar en un ámbito técnico, *CyberWave* busca activamente el diálogo con sus clientes, buscando ofrecer un servicio de calidad y estando siempre dispuesta a escuchar y adaptarse a las necesidades cambiantes de las pymes gracias a la retroalimentación continua.
- Amabilidad: *CyberWave* trabaja constantemente para construir y mantener relaciones sólidas con las pymes. Su enfoque en la educación y concientización muestra un genuino interés en el bienestar y éxito a largo plazo de sus clientes.
- Estabilidad emocional: En un mundo digital lleno de amenazas, *CyberWave* se presenta como un pilar de estabilidad y confianza. Las pymes pueden confiar en que sus activos digitales están protegidos y concentrarse en lo que mejor saben hacer, seguir enfocándose en el desarrollo de su negocio.

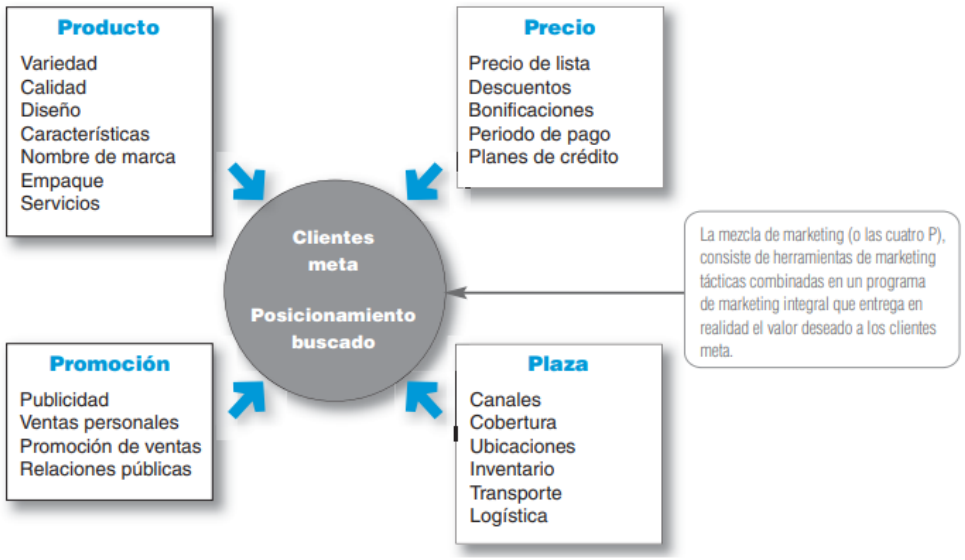
6.5.3 Misión, Visión y Valores

- **Misión:** Brindar servicios de *ciberseguridad* innovadores, eficientes, seguros y de alta calidad que contribuyan al éxito de las pymes.
- **Visión:** Ser el aliado estratégico de las pymes peruanas en su camino hacia una transformación digital *cibersegura* a través de servicios adaptados a sus necesidades.
- **Valores:** confiable, adaptable y colaborativo. El ser confiable en demostrar capacidad para proteger y salvaguardar la seguridad digital de los clientes. El ser adaptable para hacer frente a las nuevas *ciberamenazas* del entorno tecnológico en constante cambio. El ser colaborativo para mostrar disposición a cooperar con los clientes y trabajar en conjunto para garantizar su *ciberseguridad*.

6.6. Marketing Mix

De acuerdo con un artículo de IEBS *School* respecto a la definición de Philip Kotler sobre el marketing mix, indica: "[…] es una herramienta clásica para ayudar a planificar qué ofrecer a los consumidores y cómo ofrecérselo" (Estaún, 2023).

Ilustración 6.5 Variables del Marketing Mix



Fuente: Marketing, Philip Kotler / Gary Armstrong (2012)
Elaboración: Marketing, Philip Kotler / Gary Armstrong (2012)

6.6.1. Producto o servicio

Según el artículo de IEBS *School*: "El producto es una de las variables más importantes ya que es el bien o servicio que satisface una necesidad" (Estaún, 2023). Por ello, el paquete de servicios propuesto incluye el siguiente detalle:

- Seguridad *Endpoint*: Incluye la instalación y configuración base, la gestión de requerimientos como creaciones y modificaciones a reglas y perfiles, el monitoreo, la gestión de eventos y *ciberincidentes* y la elaboración de reportes.
- Seguridad de correo: Incluye la instalación y configuración base, la gestión de requerimientos como creaciones y modificaciones a reglas y listas blancas y negras de correos, el monitoreo, la gestión de eventos y *ciberincidentes* y la elaboración de reportes.

- Seguridad de navegación web: Incluye la instalación y configuración base y de accesos, la gestión de requerimientos como creaciones y modificaciones a perfiles, el monitoreo, la gestión de eventos y *ciberincidentes* y la elaboración de reportes.
- *Firewall*: Incluye la instalación, la configuración base y de accesos, la gestión de requerimientos como creaciones y modificaciones a reglas y perfiles, el monitoreo, la gestión de eventos y *ciberincidentes* y la elaboración de reportes.
- *Anti-exploit*: Incluye la instalación y configuración base, la gestión de requerimientos como creaciones y modificaciones a bloqueos y alertas, así como de listas blancas y negras de aplicaciones, el monitoreo, la gestión de eventos y *ciberincidentes* y la elaboración de reportes.
- Respaldo y restauración: Incluye el respaldo periódico de la información en la nube y *cibersoporte* para la restauración de esta ante un *ciberincidente*.
- Programa de concientización: Incluye el desarrollo de un plan de concientización acorde al cliente y los eventos y *ciberincidentes*, así como el envío del material didáctico disponible como contenido educativo y sesiones de capacitación al personal.

Como servicios adicionales se plantean los siguientes:

- Bolsa de horas para proyectos digitales: incluye el acompañamiento para proyectos digitales que la pyme esté emprendiendo y que desea alinear con los riesgos y controles de *ciberseguridad* mínimos y necesarios.
- Asesorías: incluye el alineamiento a mejores prácticas como la ISO 27001 de seguridad de la información, el *framework* del NIST CSF, la ISO 27017 de seguridad *cloud*, la ISO 27018 de protección de información de identificación personal, entre otros.
- Capacitaciones especializadas: incluye capacitaciones sobre temas especializados de *ciberseguridad* para equipos tecnológicos, tales como los estándares para el desarrollo seguro, gestión de riesgos, protección de datos personales bajo la Ley N° 29733, entre otros.

Cabe destacar que el competidor que se ha analizado, Alpha Guard, no ofrece una solución integral que se encuentre conformada por componentes integrados entre sí como *CyberWave*. Su servicio principal gira en torno a una plataforma desarrollada por ellos mismos para identificar fallos críticos en sitios web, APIs, nube y correo y brinda una calificación del nivel del riesgo de la empresa en base a los hallazgos efectuados, y un servicio de "*CISO as a Service"* que incluye gestión documentaria, un servicio de *pentesting* que no aplica para pymes de todos los sectores, y el servicio de monitoreo en la *Dark Web* y *Deep Web*. Estos servicios no se asemejan al plan *Cyber Plus* ni sus *upgrades*, ni brinda acompañamiento en la implementación de las medidas pertinentes para mitigar los riesgos detectados. Finalmente, tampoco su servicio está planteado bajo un plan de suscripción como el de *CyberWave*, sino esquematiza sus servicios como proyectos con una duración determinada.

6.6.2. Precio

Según el artículo de IEBS *School*: "Debemos establecer un precio para el producto, lo suficientemente amplio para generar ingresos para cubrir gastos y que, además, genere un beneficio" (Estaún, 2023). Por ello, es vital contar con una estrategia eficiente, acorde a los servicios y a la estrategia general de la empresa.

Se ha definido la estrategia de fijación de precios basada en los costos. Esta estrategia garantiza que el precio establecido cubrirá tanto los gastos y costos fijos, como los variables asociados al servicio. Según los resultados de la encuesta analizada en el capítulo anterior, se determinó que, para el paquete descrito, los potenciales clientes estarían dispuestos a pagar un precio dentro del rango de S/ 2000 a S/ 2600. En consecuencia, se propone lanzar al mercado de Lima Metropolitana con un precio inicial de S/ 2363 (sin IGV) para el primer año. Posteriormente, y dependiendo de la aceptación y respuesta positiva del mercado, se contempla la posibilidad de incrementar progresivamente el precio.

Parte de la estrategia de fijación de precios es considerar este precio como precio de entrada, lo que permitirá medirlo respecto del mercado y la competencia, el mismo que se irá ajustando en los siguientes periodos a medida que el resto de las estrategias, como la de posicionamiento y fidelización, empiecen a dar resultados.

Cabe destacar que el competidor que se ha analizado, *Alpha Guard*, cobra alrededor de los 3200 soles (con IGV) al mes por una duración de 4 meses como máximo por el servicio principal que ofrece de la plataforma de identificación de fallos críticos, mientras que el plan *Cyber Plus,* más completo y conformado por los 4 componentes descritos anteriormente, tiene un costo mensual de alrededor 2789 soles (con IGV).

6.6.3. Plaza (Distribución)

La estrategia de marketing *mix* para la plaza o distribución en este caso, se enfoca en asegurar que el servicio de *ciberseguridad* de *CyberWave* esté disponible y accesible para los clientes en cada etapa del proceso de venta. Se está considerando lo siguiente:

- Canales de Comunicación Accesibles: Establecimiento de canales efectivos y multicanalidad, tales como redes sociales, *WhatsApp*, formulario web y correo electrónico para que los clientes puedan solicitar información y comunicarse con la empresa fácilmente.
- Presentación del Servicio a través de Demos Virtuales: Organización de *Demos* virtuales para presentar de manera detallada el servicio, sus funciones, herramientas, planes y beneficios a los clientes.
- Facilitación del Proceso de Afiliación y Contratación: Utilización de formularios web y correos electrónicos para permitir a los clientes completar formularios de afiliación, recibir el contrato del servicio, así como información para el pago y el envío del comprobante de pago.
- Asegurar Acceso Rápido a la Información Relevante: Garantizar que toda la información necesaria sobre el servicio esté disponible en el sitio web de la empresa y sea fácilmente accesible para los clientes durante todo el proceso.

6.6.4. Promoción

La promoción, según el artículo de IEBS *School*: “Consiste en todos los esfuerzos que la empresa lleva a cabo para que ese producto alcance un mayor éxito y notoriedad” (Estaún, 2023).

En la estrategia de Promoción de *CyberWave*, se establecen dos etapas fundamentales: inicialmente, se ejecutarán actividades promocionales enfocadas en el lanzamiento del servicio para captar la atención del mercado y comunicar los beneficios clave. Posteriormente, se implementarán acciones promocionales recurrentes para mantener la visibilidad de la marca, fomentar la lealtad de los clientes y fortalecer la presencia continua en el mercado.

Para el lanzamiento del nuevo servicio, se llevarán a cabo actividades específicas para el lanzamiento inicial, enfocadas en captar la atención y generar interés en el mercado. Estas acciones promocionales estarán diseñadas para establecer una sólida presencia inicial y comunicar los beneficios y propuestas de valor de manera impactante:

- Publicidad Tradicional:
  - Para maximizar la visibilidad, se utilizarán medios tradicionales como anuncios en periódicos, revistas locales y estaciones de radio pertinentes a la audiencia.
- Campaña de Lanzamiento:
  - Una agencia especializada será contratada para diseñar una campaña integral de lanzamiento, que incluirá material gráfico atractivo y estrategias publicitarias impactantes.
  - La campaña se promocionará tanto en medios tradicionales como digitales para maximizar su alcance y efectividad.
- Redes Sociales y Marketing Digital:
  - Se diseñará y publicará contenido relevante y atractivo en redes sociales, destacando los beneficios del servicio.
  - Implementación de pautas publicitarias segmentadas en plataformas clave para llegar a la audiencia específica de pymes.
  - Promoción activa del sitio web en desarrollo e incentivo a la suscripción a través de ofertas exclusivas.
- Evento de Lanzamiento:
  - Organización de un evento de lanzamiento para las pymes del público objetivo, reforzando la relación y fomentando la participación activa.

    - Durante estos eventos, se resaltará la importancia de la *ciberseguridad* y se presentará el servicio de forma detallada.
- *Partnerships* Estratégicos:
    - Búsqueda de colaboraciones con figuras públicas y/o *influencers* relevantes en el ámbito de la tecnología, para promocionar la marca en distintos medios, incluyendo *reels* y otros canales digitales.

Posterior al lanzamiento, se implementarán actividades de promoción recurrentes que buscan mantener la visibilidad de la marca y fomentar la lealtad de los clientes. Estas acciones tendrán un enfoque tanto *pull* como *push*.

Con respecto a las estrategias de tipo *pull* se han considerado las siguientes:

- Contenido para generar conciencia de *ciberseguridad* a través de redes sociales, siendo contenido digital de carácter más liviano pero impactante, busca aumentar la conciencia sobre la relevancia de la *ciberseguridad* en el día a día empresarial. A través del uso de afiches virtuales, videos informativos y publicaciones de fácil asimilación, se busca resaltar las amenazas cibernéticas comunes, brindar consejos prácticos y promover comportamientos seguros en línea. Estas campañas se difundirán mediante redes sociales como *LinkedIn, Facebook, YouTube, Instagram, TikTok*. Asimismo, se busca que el público objetivo pueda adquirir conocimientos sobre *ciberseguridad* en un formato accesible y comprensible. La meta central es impulsar un cambio positivo en los comportamientos y cultivar una cultura de seguridad en línea.
- Publicaciones regulares como boletines y contenido educativo especializado en la página web notificado vía correo para generar contenido de *ciberseguridad* valioso y relevante con el fin de atraer e involucrar al público objetivo. Esta iniciativa se llevará a cabo mediante la distribución de boletines mensuales. Además, se complementará con la formación en temas de actualidad de *ciberseguridad* para el segmento de clientes, que guarden estrecha relación con los servicios proporcionados. Se ofrecerá *webinars* como medio para impartir esta formación, con el objetivo de brindar un valor agregado y fortalecer las relaciones con la comunidad de pymes del sector elegido.

- Participación en eventos, conferencias y ferias profesionales siendo presentador o panelista en estas conferencias. Esto permitirá la difusión de las experiencia, conocimientos y perspectivas sobre temas relevantes en *ciberseguridad*. Se debe contemplar también, la preparación de presentaciones, charlas y talleres que ofrezcan contenido valioso y relevante para la audiencia. Incluyendo tendencias de *ciberseguridad*, mejores prácticas, realizar demostraciones prácticas, virtuales o presenciales para dar a conocer como las *ciberamenazas* pueden afectar a las pymes, y cómo el paquete de servicios es efectivo ante un ciberataque, en un entorno en vivo controlado.

Asimismo, respecto a las actividades de promoción de tipo *push* se han considerado la siguientes:

- Creación de una lista de potenciales clientes a partir del resultado de los *webinars*, comentarios de publicaciones en redes sociales, contactos en ferias, eventos profesionales y de comunidades de pymes.
- Contratación a ejecutivos comerciales con una cartera de potenciales clientes.
- Definición de un plan de comunicaciones a clientes potenciales, que incluya un mix de canales apropiado empleando email marketing, mensajes vía LinkedIn y comunidades.

Respecto a las acciones de fidelización de *CyberWave*, se han definido 2 programas de fidelización, el primero dirigido a los clientes definidos como VIP y el segundo orientado a los clientes definidos como referidos, así como un programa de retención.

- Membresías VIP: Es un programa orientado a aquellos clientes leales que compran frecuentemente servicios adicionales o renuevan sus suscripciones al año de servicio, el cual contará con los siguientes beneficios:
  - Acceso a información especial y diferenciada a través de boletines de *ciberseguridad*.
  - Acceso exclusivo a *webinars* de *ciberseguridad*.
  - Descuentos en servicios adicionales como capacitaciones especializadas, asesorías, bolsas de horas para proyectos digitales, implementación de soluciones adicionales, entre otros.

- Programa de referidos: Programa orientado a todos los clientes que quieran recibir un beneficio por recomendar el servicio de la propuesta. El beneficio ofrecido será un descuento por cada referido, sobre el paquete de servicio facturado en el siguiente mes. Cabe resaltar que el referido no debe ser parte de la base de clientes actual ni histórica y debe contratar el servicio.
- Programa de retención: Programa orientado a todos los clientes con el fin de asegurar que los clientes sigan utilizando el servicio y decidan mantenerse con nosotros sin buscar alternativas. El beneficio ofrecido será un descuento inmediato sobre el paquete de servicio facturado por decidir quedarse en la cartera.

6.7. Presupuesto de marketing

Se ha elaborado el presupuesto de marketing considerando las estrategias descritas y los componentes necesarios para poder desarrollarlas en el cuadro líneas abajo. Los costos asociados a producto y distribución del marketing mix, se están considerando en el presupuesto operativo del capítulo 7.

Cabe resaltar en lo que concierne a la proyección de ventas, se tendrá en cuenta la demanda proyectada. Este aspecto será abordado con mayor detalle en el capítulo 9 del Plan Financiero, específicamente en los numerales 9.4 y 9.5.

Tabla 6.2 Presupuesto de Marketing y Ventas

PLAN DE MARKETING	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
LANZAMIENTO						
NOTAS DE PRENSA	S/ 1,667					
EVENTO DE LANZAMIENTO	S/ 25,000					
IMÁGENES CORPORATIVAS	S/ 333					
PUB. ESPECIAL (LANZAMIENTO EN REDES)	S/ 3,000					
AGENCIA DE MARKETING	S/ 12,000					
CREACIÓN DE MARCA	S/ 8,358	S/ 16,000	S/ 16,800	S/ 17,640	S/ 18,522	S/ 19,448
COPYWRITING	S/ 1,600					
REGISTRO DE MARCA	S/ 54					
IMÁGENES CORPORATIVAS		S/ 4,000	S/ 4,200	S/ 4,410	S/ 4,631	S/ 4,862
DESARROLLO DE PÁGINA WEB	S/ 3,000					
CERTIFICADO SSL	S/ 204					
SERVICIOS LEGALES	S/ 500					
COMMUNITY MANAGER / DISEÑADOR		S/ 12,000	S/ 12,600	S/ 13,230	S/ 13,892	S/ 14,586
INFLUENCER	S/ 3,000					

PLAN DE MARKETING	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
PROMOCION						
PROGRAMA DE CONCIENTIZACIÓN		S/ 93,460	S/ 98,133	S/ 103,040	S/ 108,192	S/ 113,601
DISEÑO DE LA SECUENCIA DE E-MAILS		S/ 960	S/ 1,008	S/ 1,058	S/ 1,111	S/ 1,167
MAQUETA DE NEWSLETTER		S/ 9,600	S/ 10,080	S/ 10,584	S/ 11,113	S/ 11,669
HERRAMIENTA DE E-MAIL MARKETING		S/ 960	S/ 1,008	S/ 1,058	S/ 1,111	S/ 1,167
HERRAMIENTAS DE DISEÑO		S/ 900	S/ 945	S/ 992	S/ 1,042	S/ 1,094
HERRAMIENTAS SEO		S/ 72,000	S/ 75,600	S/ 79,380	S/ 83,349	S/ 87,516
DESARROLLO WEBINARS		S/ 3,040	S/ 3,192	S/ 3,352	S/ 3,519	S/ 3,695
CREACIÓN DE VIDEOS EXPLICATIVOS		S/ 6,000	S/ 6,300	S/ 6,615	S/ 6,946	S/ 7,293
RELACIONES PÚBLICAS Y EVENTOS		S/ 66,667	S/ 70,000	S/ 73,500	S/ 77,175	S/ 81,034
PARTICIPACIÓN EN FERIAS		S/ 30,000	S/ 31,500	S/ 33,075	S/ 34,729	S/ 36,465
ASISTENCIA A EVENTOS Y EXPOSICIONES		S/ 16,667	S/ 17,500	S/ 18,375	S/ 19,294	S/ 20,258
NOTAS DE PRENSA		S/ 20,000	S/ 21,000	S/ 22,050	S/ 23,153	S/ 24,310
PERSONAL VENTAS DIRECTAS / KAM		S/ 86,111	S/ 166,667	S/ 166,667	S/ 166,667	S/ 166,667
PERSONAL VENTAS DIRECTAS (COMISIONES)		S/ 14,160	S/ 11,077	S/ 10,468	S/ 11,689	S/ 11,998
DESARROLLO WEBINARS (MEMBRESÍAS VIP)		S/ 0	S/ 1,596	S/ 1,676	S/ 1,760	S/ 1,848
MEMBRESIAS VIP		S/ 0	S/ 33,137	S/ 55,762	S/ 52,493	S/ 56,329
PROGRAMA DE REFERIDOS		S/ 1,305	S/ 436	S/ 458	S/ 824	S/ 865
DSCTO. RETENCIÓN		S/ 1,246	S/ 1,275	S/ 1,219	S/ 1,532	S/ 1,246
CONTINGENCIA	**S/ 0**	**S/ 5,748**	**S/ 6,973**	**S/ 7,915**	**S/ 8,156**	**S/ 8,600**
TOTAL, PLAN DE MARKETING	**S/ 50,358**	**S/ 283,451**	**S/ 406,064**	**S/ 438,400**	**S/ 446,696**	**S/ 461,922**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

6.8. Conclusión del capítulo

En este capítulo se definieron los objetivos del plan de marketing, los principales indicadores, así como las principales estrategias genéricas y de marketing, y finalmente el marketing *mix*.

Como objetivo central se definió aumentar la visibilidad, generar confianza y adquirir nuevos clientes a través de la aplicación de las estrategias definidas en este plan y se establecieron los recursos necesarios para poder lograrlo. Además, se definió la imagen corporativa de la marca, se detalló el servicio, precio, y medios de promoción y distribución, definiendo las estrategias que se aplicarán para lograr justificar la viabilidad del plan.

Considerando que es una propuesta que tiene muy poca competencia en el mercado peruano y adicionalmente se está condicionado por el poco conocimiento general sobre

la materia, se ha definido realizar una inversión necesaria en marketing que permitirá alcanzar el público objetivo y sentar las bases para ampliar el segmento en los próximos años.

CAPITULO 7 . PLAN DE OPERACIONES

En este capítulo se abordará la estructura de los procesos que soportarán las operaciones, así como los recursos asignados, los planes de acción operativos, las actividades de seguimiento e indicadores clave, y finalmente el presupuesto necesario para implementar el modelo de negocio propuesto, a fin de poder ofrecer los servicios de *ciberseguridad* propuesto a las pymes.

7.1. Objetivo General

Definir los procesos, acciones y recursos necesarios para poder brindar el servicio propuesto de *ciberseguridad*, aterrizando el modelo de negocio propuesto, y soportar las estrategias propuestas en los capítulos anteriores, a fin de conseguir los objetivos y metas planteados.

Detallar los procesos, acciones y recursos requeridos para implementar el servicio de *ciberseguridad* propuesto, a fin de materializar el modelo de negocio y soportar la ejecución de las estrategias definidas en los capítulos previos.

7.2. Objetivos Específicos

- Diseñar el plan Preoperativo identificando las tareas y actividades necesarias a considerar antes del inicio de la operación.
- Identificar los procesos estratégicos, los procesos de la cadena de valor e identificar los procesos de soporte y apoyo relacionados con el servicio.
- Diseñar el proceso de Afiliación y de Operación del servicio prestado por la empresa.
- Definir los recursos tecnológicos y materiales necesarios para realizar el proceso operativo, garantizando la disponibilidad y capacidad operativa suficiente para atender la demanda de los servicios.
- Establecer indicadores que permitan evaluar la calidad y rendimiento de las operaciones, asegurando una medición efectiva del desempeño y la mejora continua en la prestación de los servicios de *ciberseguridad*.

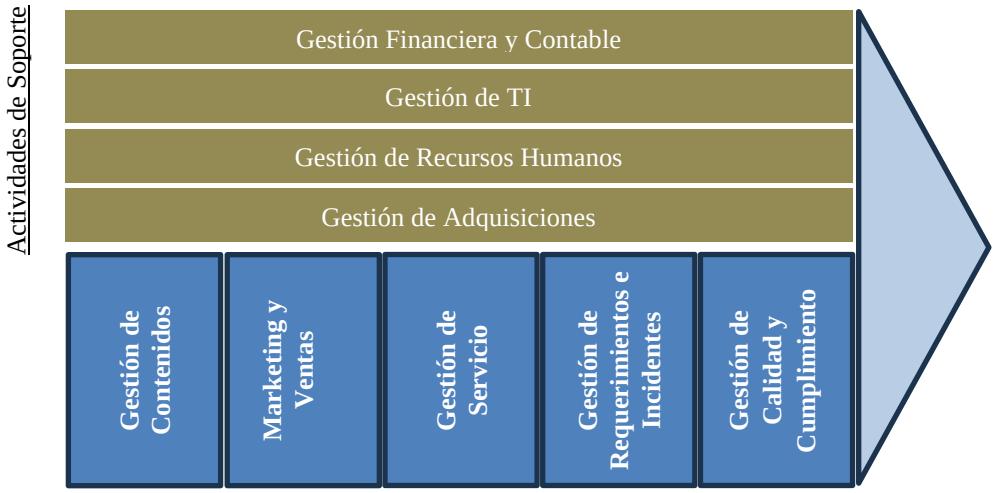
- Establecer el presupuesto para la inversión y la operación, definiendo los recursos financieros necesarios para llevar a cabo las actividades planificadas y sostener las operaciones del negocio.

7.3. Cadena de Valor

La cadena de valor es una herramienta estratégica usada para analizar las actividades de una empresa y así identificar sus fuentes de ventaja competitiva (Gestiopolis, 2021).

Basándonos en el modelo de negocio, hemos empleado la cadena de valor para el sector de servicios. Dentro de las actividades primarias, se destaca la Gestión de Contenidos. Esta etapa comienza con un análisis inicial de ventas y marketing, donde la gestión de contenidos juega un papel crucial para implementar estrategias educativas en el mercado. Luego, se procede con la gestión de marketing y ventas, donde se promociona el servicio y se cierran las ventas de suscripción. A continuación, se concentra en la gestión del servicio, que comienza con el proceso de instalación, monitoreo de la seguridad y programas de concientización. Posteriormente, se aborda la gestión de requerimientos e incidentes que puedan surgir durante la prestación del servicio. Por último, se considera la Gestión de Calidad y el cumplimiento del servicio, en la cual la organización se asegura de cumplir con las políticas, condiciones y plazos ofrecidos.

Ilustración 7.1 Proceso de Registro y Afiliación



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

7.4. Recursos y capacidades

La finalidad de examinar los recursos y capacidades consiste en reconocer el potencial de la compañía para obtener ventajas competitivas a través de la evaluación de los recursos y competencias que posee o puede adquirir. (Instituto Consorcio Clavijero, 2019)

Se analizarán los siguientes tipos de recursos:

- **Recursos Financieros**: Se están considerando a los recursos financieros propios, los cuales están conformados por los aportes de capital de los 4 fundadores. Esto se detalla en el capítulo 8, sección 8.4.2. Además, se considera el capital de trabajo necesario para las actividades y la prestación del servicio, incluyendo costos de licencias de software, el incremento de espacio en el servicio *cloud* y la contratación y pago a especialistas y analistas que brindaran el servicio.

  Asimismo, se consideran las utilidades previstas luego de cada periodo, necesarias para y pagar los dividendos a los aportantes.

- **Recursos Humanos**: Se está considerando la estructura organizacional desarrollada en el capítulo 8. Para mencionar en nivel de jerarquía se contará con un Gerente General y 4 *Heads* para las áreas clave: Operaciones, Marketing y Ventas, Administración y Finanzas y Recursos Humanos. Dentro del área de Operaciones, se ha considerado dos roles para brindar los servicios: especialistas y analistas de *ciberseguridad*. Dentro del área de Marketing y ventas, se contará con un rol mixto de *Key Account Manager* y Ejecutivo de Ventas. Dentro del área de Recursos Humanos se contará con un Analista de Recursos Humanos.
- **Recursos materiales**: Los principales recursos para brindar los servicios son los recursos tecnológicos. En primer lugar, se está considerando la solución tecnológica de *ciberseguridad* (*GravityZone Small Business Security* de *Bitdefender*) y las licencias para los usuarios. En segundo lugar, se está considerando la Infraestructura Tecnológica *Cloud* (*Microsoft Azure).* En tercer lugar, se está considerando la página web, que permitirá la oferta de servicios, la afiliación y la gestión de contenidos.

  Asimismo, la empresa no contará con otros recursos materiales, dado que la estrategia planificada es de alquiler y tercerización de todos los servicios no claves. En este caso se ha considerado una organización del trabajo híbrida, dada la naturaleza de los servicios brindados, para lo cual se contará con un servicio de coworking que permitirá acceder y utilizar sus instalaciones compartidas, como escritorios, salas de reuniones y áreas comunes. La zona donde se ha cotizado y se ubicará el *coworking* será en Lince. Los costos asociados se indican en el capítulo 9.

  Finalmente, respecto al equipo necesario para brindar los servicios se está considerando un servicio de alquiler de laptops para los colaboradores, El servicio comprende el alquiler del equipo, recambio inmediato de equipo similar, el mantenimiento preventivo y *Help Desk* remoto en 5 minutos. Los costos asociados se indican en el capítulo 7.
- **Recursos Técnicos**: Se está considerando en primer lugar el *partnership* con el proveedor de la solución tecnológica elegida, en este caso *Bitdefender*. En segundo lugar, se está considerando, la capacitación continua ya actualizada del personal operativo en materia de *ciberseguridad*, así como también en el uso de las herramientas tecnológicas: la solución tecnológica de *ciberseguridad*

(*GravityZone*), la gestión y uso de las herramientas de monitoreo de Microsoft Azure.

Finalmente, otro recurso importante son las certificaciones que se están considerando, en la norma ISO 27001 que asegura la confidencialidad, integridad y disponibilidad de la información, y en la norma ISO 22301 para establecer un sistema de gestión de continuidad del negocio.

7.5. Fase Preoperativa

En esta esta fase se han definido las actividades necesarias y previas al inicio de la actividad operativa de la empresa, considerando un plazo de duración de tres meses. Asimismo, se está considerando un Plan Preoperativo y un Plan de Lanzamiento para *CyberWave*.

Durante la fase Preoperativa, se llevan a cabo actividades de registro y constitución de la empresa, la adquisición de recursos necesarios, la contratación y formación de personal. Además, se considera el costo para el proceso de certificación de la norma ISO 27001 para la seguridad de la Información, y de la norma ISO 22301, para la continuidad del negocio; Ambas necesarias para la para el rubro del negocio de la *ciberseguridad*. Asimismo, se encuentra el *partnertship* con *Bitdefender* para poder distribuir las licencias de *GravityZone*.

Tabla 7.1 Actividades para la Fase Preoperativa

PREOPERATIVO	DETALLE
Registro como persona jurídica	Presentar documentos ante SUNARP, para establecer legalmente a la entidad, permitiéndole operar, firmar contratos y adquirir derechos
Derechos y patentes registral	Costo de Registros ante INDECOPI, para brindar protección legal sobre invenciones, diseños o marcas, asegurando exclusividad en el uso y comercialización.
Gastos notariales	Pago de honorarios notariales por la elaboración y revisión de escrituras y documentos legales.
TOTAL, CONSTITUCIÓN	
Cumplimiento normativo (SST)	Capacitación para empleados, adquisición de equipos de protección personal, evaluaciones de riesgos, exámenes médicos ocupacionales y otros costos relacionados.

PREOPERATIVO	DETALLE
Registro como persona jurídica	Presentar documentos ante SUNARP, para establecer legalmente a la entidad, permitiéndole operar, firmar contratos y adquirir derechos
Derechos y patentes registral	Costo de Registros ante INDECOPI, para brindar protección legal sobre invenciones, diseños o marcas, asegurando exclusividad en el uso y comercialización.
Gastos notariales	Pago de honorarios notariales por la elaboración y revisión de escrituras y documentos legales.
Coworking	Costo del espacio de coworking para acceder y utilizar sus instalaciones compartidas, como escritorios, salas de reuniones y áreas comunes.
plataformas web de reclutamiento	Uso de Plataformas líderes tales como *LinkedIn, Bumeran, Laborum, Computrabajo.*
Servicio de reclutamiento y selección	Contratación de un tercero para los procesos de reclutamiento y selección del personal para la empresa
Exámenes psicométricos	Exámenes para contratación
Verificación de antecedentes	Validación de personal a contratar
Capacitaciones	Entrenamiento básico para eventos previos de lanzamiento
Servicios legales abogado laboralista	Asesoría en pagos a colaboradores y elaboración de contratos para operación
Compensaciones preoperativas	Pago por concepto de personal en actividades preoperativas
Certificación de ISO 22301	Proceso de certificación de ISO 27001 para la empresa
Certificación de ISO 22301	Proceso de certificación de ISO 22301 para la empresa
Costo anual del *partnership* con *Bitdefender*	Pago anual para ser miembro del programa de *partnership* con *Bitdefender*

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

De manera similar, para el Plan de Lanzamiento se han evaluado los costos necesarios para el registro de la marca y la creación de la estrategia de marketing y promoción, según se indica en el capítulo 6. Se está considerando la contratación de una agencia de marketing para diseñar y llevar a cabo una campaña publicitaria de lanzamiento en plataformas digitales. Además, se planifica la realización de un evento

de lanzamiento dirigido a representantes de pymes del sector de Construcción e Inmobiliaria, y se están contemplando los gastos asociados al desarrollo de un sitio web que desempeñará un papel crucial en la promoción del contenido y la captación de clientes.

Tabla 7.2 Actividades para el Lanzamiento

PLAN DE LANZAMIENTO (MKT)	DETALLE
Registro de marca	Registro de la marca con INDECOPI
Notas de prensa	Publicaciones en medios de publicidad tradicionales
Evento de lanzamiento	Incluye el alquiler de local, catering, búsqueda e invitación a representantes de pymes.
Imágenes corporativas	Material gráfico corporativo
Agencia de marketing	Pago a la agencia para diseño y despliegue de campaña de lanzamiento
Publicidad especial de lanzamiento en redes	Diseños y publicaciones en redes sociales, pautas, publicaciones, etc.
Copywriting	Patentar la marca para evitar copias
Desarrollo de página web	Desarrollo de la página web en *stagging*, pruebas y pase a producción dentro del entorno *Azure*
Certificado SSL	Certificado digital que verifica la identidad de la página web y permite habilitar una conexión cifrada
Servicios legales	Pago a abogados por asesoría en contratos y/o pagos asociados a la campaña
Influencer	Pago a figura pública para que promocione la marca en *reels* u otro medio

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.6. Identificación de los Procesos

A continuación, se detallan los procesos con los que contará el servicio propuesto, a partir de la consideración de tres niveles: estratégicos, de negocio y de soporte.

7.6.1. Procesos Estratégicos

Los procesos estratégicos propuestos que apoyaran la guía de la dirección y la toma de decisiones de la empresa son los siguientes:

Tabla 7.3 Procesos Estratégicos

TIPO DE PROCESO	PROCESO
Nivel Estratégico	Definición de Alianzas Estratégicas
	Investigación y Desarrollo
	Gestión de Experiencia del Cliente

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- **Proceso de Definición de Alianzas Estratégicas**

Este proceso busca forjar colaboraciones estratégicas con marcas que brindan soluciones tecnológicas de *ciberseguridad* a fin de obtener precios más competitivos en licenciamiento, así como descuentos en cursos y certificaciones. Inicialmente se está optando por un *partnership* con *Bitdefender*, pero se podrían explorar otras opciones para pymes.

También, se busca forjar alianzas con comunidades de pymes del sector construcción para ampliar la capacidad y alcance de los servicios, así como entablar relaciones con comunidades de pymes de otros sectores.

- **Proceso de Investigación y Desarrollo**

Este proceso es importante ante el continuo dinamismo que demanda la innovación tecnológica para la gestión de riesgos, controles e incidentes de *ciberseguridad*. Por ende, esto implica mantenerse al tanto sobre las últimas tendencias, amenazas y

vulnerabilidades emergentes, evitando ser reactivos y, por el contrario, ser pioneros en el diseño e innovaciones de soluciones.

El proceso de Investigación y Desarrollo (I+D) para la empresa se inicia identificando las tendencias y amenazas emergentes en el panorama digital. Luego, se evalúan con el fin de identificar si las soluciones tecnológicas actuales pueden abordar estas amenazas, y en caso contrario poder identificar en el mercado posibles nuevas soluciones tecnológicas. Además, se colabora estrechamente con expertos en seguridad cibernética para diseñar y mejorar continuamente el programa de concientización y formación integral. El responsable de este proceso es el Especialista de *ciberseguridad*.

- **Gestión de Experiencia del Cliente**

Este proceso busca identificar nuevas necesidades de *ciberseguridad* a partir de la retroalimentación de los clientes, para no solo brindar seguridad técnica, sino también construir relaciones de confianza y satisfacción a largo plazo al adaptar constantemente las medidas de protección en función de la evolución de las amenazas y las necesidades del cliente.

Para ejecutar este proceso es vital escuchar activamente y absorber la retroalimentación brindada por los clientes para atender mejor sus necesidades y diseñar servicios que se centren en el cliente, por tanto, se implementará una encuesta de satisfacción general de los clientes sobre los servicios y la atención recibida. El responsable de este Proceso es el Head de Recursos Humanos.

7.6.2. Procesos de Negocio

Los procesos de negocio propuestos sirven para identificar y coordinar las operaciones necesarias para brindar el servicio, garantizando su calidad, y asegurando la ejecución eficiente y efectiva de las tareas.

Tabla 7.4 Procesos de Negocios

TIPO DE PROCESO	PROCESO
Nivel de Negocio	Gestión de Contenidos
	Gestión de Ventas y Marketing
	Gestión de Servicio
	Gestión de Requerimientos e Incidentes
	Gestión de Calidad y Cumplimiento

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- **Gestión de Contenidos**

Este proceso se enfoca en la ideación, diseño y publicación del contenido educativo, relevante y especializado en materia de *ciberseguridad* para los clientes suscritos.

De esta manera, el Especialista de *ciberseguridad* es el encargado la elaboración del contenido de fondo para los boletines mensuales especializados y la generación del material para los *webinars* y capacitaciones. Además, también es responsable de generar el contenido para el material de concientización en temas de *ciberseguridad*.

Por otro lado, el diseño y publicación de los contenidos se realizará a través Servicio de *Community Manager* / Diseñador contratado. Este servicio está bajo la responsabilidad del Head de Recursos Humanos.

El objetivo de este proceso es concientizar a potenciales clientes y posicionar la marca de la empresa en el mundo digital, a través de la generación contenido en redes sociales y en la web empresarial.

- **Gestión de Ventas y Marketing**

Este proceso es importante porque se enfoca en la ejecución de las estrategias de marketing, desarrolladas en el capítulo 6, así como la medición del resultado de las campañas y contenido publicado.

También prioriza la búsqueda e identificación de nuevas oportunidades de mercado para crear nuevas estrategias, con el objetivo de atraer nuevos clientes.
Fomentar la prospección activa, el seguimiento efectivo y la comunicación estratégica con clientes potenciales y gestionar el cierre de las ventas.

Además, comprende la gestión proactiva de las relaciones con los clientes existentes, por parte de los Ejecutivos de Ventas/ *Key Account Managers,* para fomentar la fidelización y la colaboración a largo plazo.

- **Reclutamiento, Selección y Capacitación**

Este proceso se enfoca en Identificar el talento adecuado sobre todo para los recursos críticos para la prestación del servicio que vienen a ser los Especialistas y Analistas. A fin de asegurar que los candidatos cuenten con habilidades técnicas y éticas esenciales, seguida de una selección basada en competencias técnicas en las mejores prácticas de *ciberseguridad* y habilidades blandas necesarias para brindar un servicio que satisfaga a los clientes.

Asimismo, contempla el diseño e implementación de un programa de capacitaciones para los Analistas y Especialistas en materias de *ciberseguridad* tanto a nivel de normas técnicas, *frameworks* y en el uso de las herramientas para la prestación del servicio a los clientes.

Este proceso es responsabilidad del Head de Recursos Humanos, apoyado en el Analista de Recursos Humanos.

- **Gestión de Servicio**

EL objetivo del proceso es gestionar la entrega de los servicios de *ciberseguridad* en los paquetes contratados por los clientes durante su periodo de suscripción. Gestionando efectivamente desde la instalación, hasta la entrega del reporte del Servicio.

Además, incluye el monitoreo activo de las amenazas de *ciberseguridad* a fin de responder oportunamente ante incidentes, atender los requerimientos de los clientes eficazmente y emitir los informes mensuales y detallados con recomendaciones de las

amenazas detectadas. El detalle de las actividades necesarias para este proceso se indica en el numeral 7.5

- **Gestión de Requerimientos e Incidentes**

El objetivo del proceso es la atención y solución de los incidentes reportados por los clientes o detectados durante el monitoreo, a fin de asegurar una gestión ágil y oportuna. Asimismo, se enfoca en la atención de los requerimientos que el cliente solicite brindando asesoría y/o efectuando las configuraciones necesarias para asegurar su satisfacción. El Detalle de las actividades necesarias para este proceso se indica en el numeral 7.5.

- **Gestión de Calidad y Cumplimiento**

Este proceso busca garantizar que los servicios prestados cumplan con los acuerdos de nivel de servicio y las regulaciones en *ciberseguridad* para el servicio contratado por el cliente. Además, hace foco en la identificación de oportunidades de mejora en la prestación de servicios y la generación de planes de acción para su solución.

7.6.3. Procesos de Soporte

Los procesos de soporte propuestos para la empresa abarcan aquellas actividades que respaldan las funciones principales, comprendiendo áreas como recursos humanos, tecnología y administración financiera. Estos procesos aseguran un funcionamiento fluido y eficiente de *CyberWave* en su conjunto.

Tabla 7.5 Procesos de Soporte

TIPO DE PROCESO	PROCESO
Nivel de Soporte	Gestión de Recursos Humanos
	Gestión Financiera y Contable
	Gestión de Adquisiciones
	Gestión de TI

Fuente: Autores de esta tesis.

Elaboración: Autores de esta tesis

- **Gestión de Adquisiciones**

El objetivo de este proceso es Adquirir y gestionar los recursos necesarios para la prestación de los servicios de *ciberseguridad*.

En este sentido, el Head de Operaciones será el responsable de solicitar a inicios de cada mes, la adquisición de nuevas licencias de *GravityZone* al Gerente de Cuentas del proveedor tecnológico de *Bitdefender*, de acuerdo con la demanda proyectada, la cual se detalla en el capítulo 9.

De igual manera, para el incremento de espacio contratado de almacenamiento *cloud*, el Head de Operaciones autoriza al Especialista de *ciberseguridad* para que aprovisione el espacio a través del portal de Azure y realice el pago correspondiente utilizando una tarjeta empresarial configurada en la cuenta para este propósito.

- **Gestión de Finanzas y Contabilidad**

El objetivo de este proceso es asegurar una administración financiera efectiva que respalde las operaciones y crecimiento de la empresa. Esto incluye controlar costos relacionados con licencias del software, infraestructura *cloud*, recursos humanos y equipos informáticos. Comprende también la gestión de la facturación y cobranza, para lo cual se utilizará la plataforma de facturación electrónica de TeFacturo. Además, contempla la elaboración de los presupuestos mensuales y anuales en base a la demanda proyectada, la evaluación de la rentabilidad de nuevos proyectos y servicios, la realización de análisis financieros, la gestión de riesgos financieros, y la generación de informes claros sobre la salud financiera de la empresa.

Asimismo, respecto a la gestión contable, se utilizará un servicio tercerizado que realizará la labor de llevar el registro preciso de todas las transacciones financieras y contables, asegurando la conformidad con las regulaciones pertinentes. Además, el servicio incluye el uso de un software eficiente y adecuado para la gestión de libros electrónicos y contabilidad.

- **Gestión de TI**

El proceso se enfoca en gestionar y preservar la tecnología complementaria necesaria para la operatividad de la empresa, en términos de aplicaciones,

infraestructura, licenciamiento y *cibersoporte* para la empresa, asegurándose de que esté en condiciones óptimas y protegida. Esto involucra supervisar su funcionamiento, resolver problemas y adoptar nuevas tecnologías para mejorar constantemente el rendimiento y respaldar los objetivos de la empresa. El responsable de este proceso es el Head de Operaciones soportado en un servicio tercerizado de tecnología. El detalle de los Recurso tecnológicos se detalla en el numeral 7.6

- **Gestión de Recursos Humanos**

El proceso contempla la evaluación de desempeño de los colaboradores a través de revisiones regulares y orientado al cumplimiento de metas. La planificación y ejecución del Plan de Carrera para los colaboradores. También se enfoca en Identificar el talento adecuado sobre todo para los recursos críticos para la prestación del servicio (Especialistas y Analistas), a fin de asegurar que los candidatos cuenten con habilidades técnicas y éticas esenciales, seguida de una selección basada en competencias técnicas en las mejores prácticas de *ciberseguridad* y habilidades blandas.

Además, contempla el diseño e implementación de un programa de capacitaciones para los Analistas y Especialistas en materias de *ciberseguridad* tanto a nivel de normas técnicas, *frameworks* y en el uso de las herramientas para la prestación del servicio a los clientes.

Incluye también la administración del servicio de pago de nómina y la Compensación y Beneficios. También se considera el promover actividades y eventos que mejoren el clima organizacional y fortalezcan el trabajo en equipo. El responsable de este proceso es el Head de Recursos Humanos, soportado en un Analista de Recursos humanos, así como una serie de servicios tercerizados necesarios para la ejecución de las actividades y responsabilidades correspondientes. El detalle de las estrategias y presupuestos para este propósito se describe en el capítulo 8.

7.7. Diseño de Servicio

7.7.1. Políticas del Servicio

Se han definido las siguientes políticas para el servicio planteado:

- Para llevar a cabo la instalación de la plataforma de *ciberseguridad*, el cliente deberá proporcionar información relevante, incluyendo el número de *endpoints* a proteger, detalles sobre la infraestructura de red y las carpetas que serán respaldadas. Este proceso debe completarse en un plazo de 7 días para que se pueda diseñar el plan de instalación.
- La instalación de la plataforma tecnológica se llevará a cabo después de recibir y procesar la información solicitada del cliente, y esto se realizará en un plazo máximo de 7 días.
- El cliente debe cumplir con el pago mensual por el servicio, y la duración mínima del contrato es de 12 meses. En caso de que el cliente decida cancelar el contrato antes de su término, se aplicará una penalidad del 15% por cada mes restante.
- Si el pago no se efectúa en los 7 días siguientes a la fecha de vencimiento, el servicio se desconectará hasta que se realice el pago mensual correspondiente.
- Los datos respaldados estarán disponibles durante el período de contrato del servicio. Después de este período, *CyberWave* se reserva el derecho de eliminar de forma segura los datos respaldados.
- El plan *Cyber Plus* incluye un total de 10 horas mensuales de atención de requerimientos e incidentes por parte de personal especializado.
- Se busca que el plan *Cyber Plus* ayude a proteger activos críticos para una pyme del sector construcción como los mencionados a continuación:
    - Bases de datos que contienen información financiera que incluyen datos como detalles de costos, presupuestos, pagos, cuentas bancarias, entre otros.
    - Bases de datos de planos y especificaciones que son documentos esenciales para la pyme.
    - Base de datos de colaboradores que incluyen datos como nombres, direcciones, detalles bancarios, datos de salud, entre otros.

- Base de datos de clientes que incluyen datos como nombres, direcciones, detalles bancarios, entre otros.
- Base de datos de proveedores que incluyen datos como nombres, direcciones, acuerdos de precios, términos y condiciones, detalles bancarios, entre otros.
- Contratos y acuerdos con proveedores, clientes, y otras entidades.
- Base de datos de historiales de proyectos que incluyen datos como información sobre proyectos pasados, errores, aprendizajes, fotografías, planos, entre otros.
- Software específico de la industria de construcción como programas de diseño asistido por computadora, software de gestión de proyectos, entre otros.

- Se busca que el plan *Cyber Plus* cubra a los principales actores de la cadena de suministro del sector construcción como algunos de los siguientes:
  - Proveedores de materiales como empresas que producen materiales de construcción como cemento, acero, madera, distribuidores que compran materiales a los fabricantes y lo distribuyen a pymes constructoras, y tiendas de construcción donde las empresas adquieren materiales en menor cantidad o de forma urgente.
  - Proveedores de equipamiento como empresas que arriendan maquinaria pesada o equipos especializados, proveedores de equipos y herramientas que las empresas constructoras pueden comprar.
  - Proveedores de transporte como empresas encargadas de trasladar materiales y maquinaria al lugar de la construcción, servicios logísticos, entre otros.
  - Subcontratistas como empresas o individuos especializados en áreas como construcción, fontanería, electricidad, ventilación y aire acondicionado, entre otros.
  - Personal tercerizado como arquitectos, ingenieros, consultores en gestión de proyectos, seguridad laboral, evaluación ambiental, topógrafos, entre otros.
  - Proveedores de software especializado para empresas de construcción desde software de diseño hasta sistemas de gestión de proyectos.

- La comunicación oficial sobre la atención de incidentes y requerimientos resueltos se llevará a cabo mediante correo electrónico.
- Los informes mensuales del servicio se enviarán una vez al mes, de acuerdo con las fechas acordadas en el contrato.
- El servicio no incluye acompañamiento ni soporte legal, ni investigaciones o servicios dentro del espectro de la seguridad forense.

7.7.2. Actividades del Servicio

En el capítulo 4, específicamente en la sección 4.5 titulada "Solución", se ha proporcionado una descripción detallada del contenido y alcance del paquete de servicios propuesto, concebido como un Producto Mínimo Viable (MVP) para el presente plan de negocios, el cual se detalla en la siguiente tabla:

Tabla 7.6 Detalle del Servicio

SERVICIO	DESCRIPCIÓN	OBJETIVO
Protección activa contra amenazas cibernéticas para dispositivos finales.	*GravityZone Small Business Security* de *Bitdefender*, proporciona una protección integral contra *malware*, *exploits*, *phishing*, *ransomware*, fraudes y ataques basados en scripts. También incluye protección de navegación web, correo electrónico y *firewall*. Cada paquete contiene 49 licencias.	Garantizar la seguridad de los dispositivos de los clientes y prevenir posibles ataques y violaciones de seguridad.
Respaldo seguro y recuperación de datos en caso de pérdida o ataque	*Azure Backup* ofrece respaldo y restauración de datos en caso de *ciberincidentes*. Cada paquete incluye capacidad de almacenamiento de hasta 5TB.	Asegurar la disponibilidad y recuperación de datos críticos en situaciones de *ciberemergencia*.
Monitoreo continuo y respuesta rápida a incidentes de seguridad	El servicio incluye monitoreo centralizado y *cibersoporte* para configuración de reglas y accesos, así como atención de incidentes en ambas soluciones. Se proporciona un total de 10 horas mensuales para la atención de incidentes.	Detectar y mitigar de manera eficiente cualquier amenaza o actividad sospechosa en las soluciones implementadas.
Educación y formación de empleados en prácticas de seguridad cibernética	Implementación de un programa de concientización para los colaboradores con el objetivo de promover prácticas seguras en línea y prevenir posibles amenazas cibernéticas.	Crear una cultura de *ciberseguridad* en *CyberWave* y reducir la vulnerabilidad humana ante ciberataques.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Asimismo, se plantean los servicios que complementan al plan *Cyber Plus* o *upgrades*, los cuales podrán ser solicitados por los clientes en caso superen la capacidad propuesta en el plan definido.

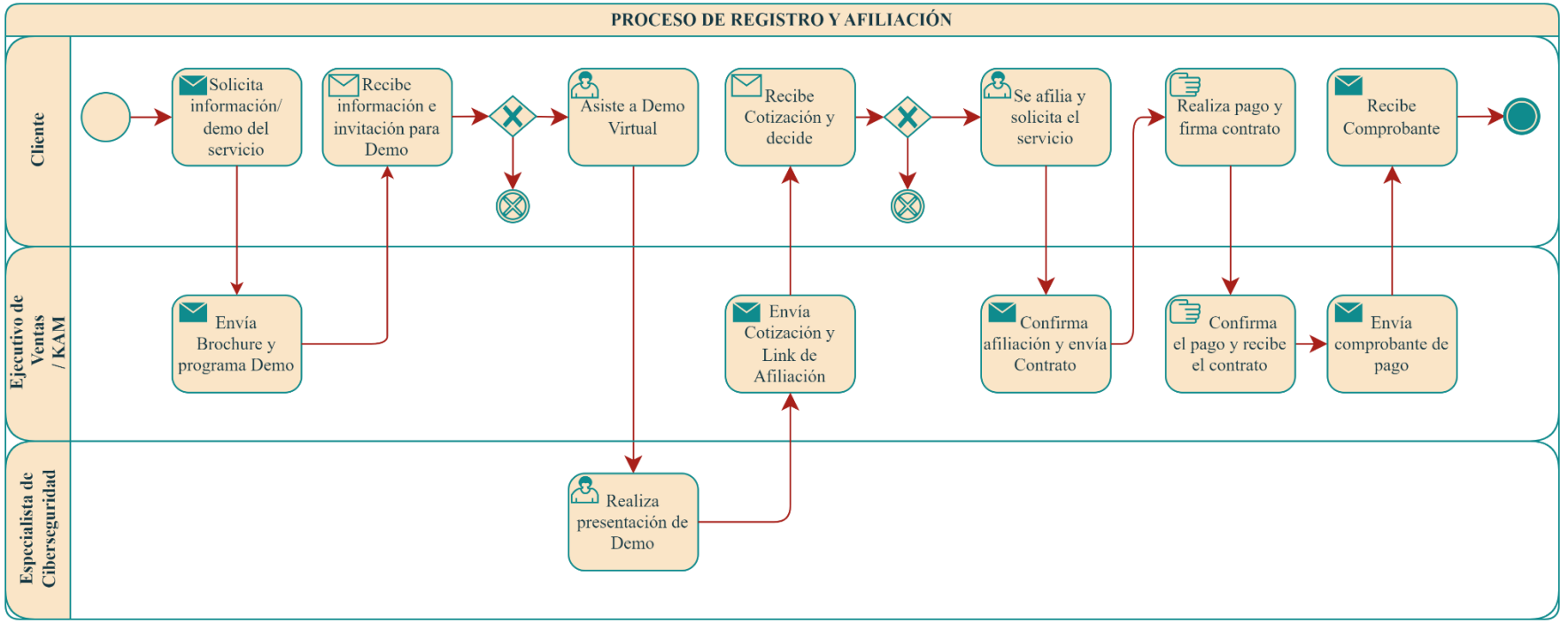
Tabla 7.7 Planes Adicionales

SERVICIO	DESCRIPCIÓN
Support Plus	Incluye 10 horas mensuales adicionales de monitoreo y atención de requerimientos e incidentes, así como adquirir 20 licencias adicionales de la solución *endpoint GravityZone Small Business Security de Bitdefender*.
Backup Plus	Incluye 5 TB adicionales para almacenamiento de respaldo y restauración de información en *Azure Backup*, así como adquirir 20 licencias adicionales de la solución *endpoint GravityZone Small Business Security de Bitdefender*.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Basándonos en esta delimitación y descripción de los servicios, se ha desarrollado el procedimiento y las acciones con el propósito de ofrecer el servicio previsto a los clientes. Dicho proceso se ha estructurado en dos fases distintas: inicialmente, se encuentra el proceso de Inscripción y Afiliación de clientes, seguido por el proceso operativo para el servicio de *ciberseguridad*.

Ilustración 7.2 Proceso de Registro y Afiliación



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

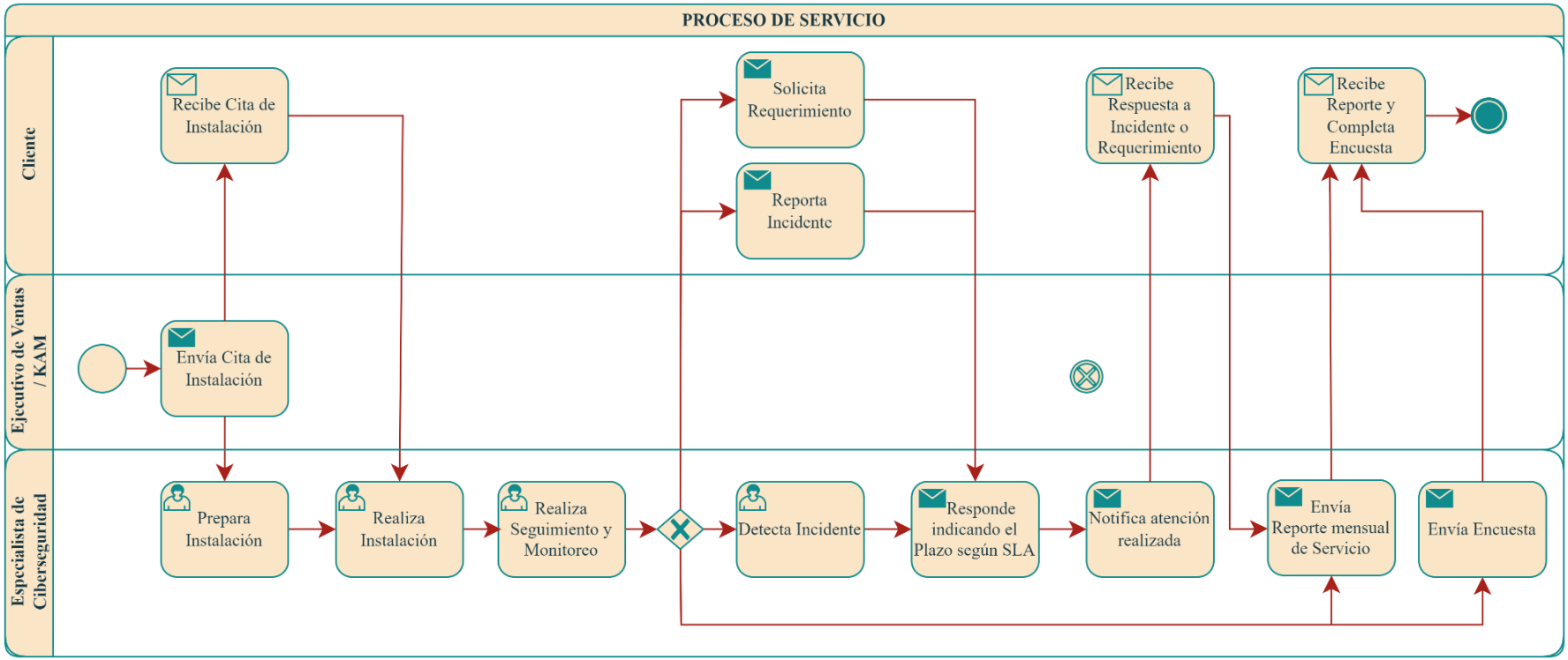
La descripción del servicio ofrecido, parte del contacto inicial del cliente con la empresa, el cliente solicita información a través de los diferentes canales habilitados, como las redes sociales: *whatsapp*, formulario de la web de la empresa y correo electrónico. El cliente recibirá información del servicio y se programará una demo virtual para darle más información y presentarle el servicio. El cliente recibirá una invitación para la demo a través de su correo electrónico.

En un segundo contacto el cliente asistirá a la demo programada virtualmente y recibirá la presentación del servicio, incluyendo las funciones, herramientas, detalle del plan y beneficios. Como resultado de la demo y tras su visto bueno, recibirá una cotización del servicio junto con el formulario de afiliación a través del correo.

Posterior a esto, el cliente ingresará a su correo y completará el formulario web, el cual notificará su solicitud de afiliación a *CyberWave*. En respuesta recibirá un correo electrónico con el contrato detallado de acuerdo con el plan elegido, así como la información para el pago.

El cliente firmará el contrato y realizará el pago respectivo y finalmente recibirá la confirmación de la afiliación al servicio, y el comprobante de pago enviado a su correo electrónico.

Ilustración 7.3 Operación del Servicio de *Ciberseguridad*



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Una vez que el cliente ha sido afiliado al servicio, el siguiente paso consistirá en realizar la instalación de los módulos de protección como parte del paquete ofrecido. Para esto se coordinará y se enviará por correo la cita para la instalación.

Cabe resaltar que previo a la instalación se dispondrá de un periodo corto de preparación durante el cual se levantarán los requerimientos del cliente. Además, al interno la empresa evaluará si cuenta con las licencias y almacenamiento necesarios para atender al cliente, y se solicitaran de ser el caso. Posterior a esto, el especialista de *ciberseguridad* elaborará el plan de instalación que comprende la instalación, las pruebas y el pase a producción.

La instalación se realizará de manera remota sobre la infraestructura brindada por el cliente. Una vez instalados los servicios, como parte de las prestaciones se notificará al cliente sobre la periodicidad de envío del reporte del servicio, que se hará de manera mensual, que comprende el análisis de los eventos e incidentes y las recomendaciones de configuración acorde a las necesidades del cliente.

Posterior a la instalación, el servicio estará activo y se monitoreará la actividad de los usuarios y los eventos que puedan surgir durante el mes. A fin de mes se consolidará el resumen del análisis realizado en un Reporte Mensual del servicio, que será recibido por el cliente a la dirección de correo registrada. Este reporte Mensual reunirá el análisis de eventos, actividad, y recomendaciones para el servicio.

Durante el uso del servicio, el cliente podrá comunicar si necesita algún requerimiento. En este caso la atención es a través de correo electrónico. El cliente recibirá un correo indicando el plazo de atención. La siguiente comunicación será para coordinar y resolver el requerimiento. Finalmente, el cliente recibirá la respuesta de la atención al correo electrónico desde donde se realizó la solicitud.

De manera similar, durante el uso del servicio el cliente podrá comunicarse ante incidentes de *ciberseguridad*. En este caso la atención se realiza a través de *whatsapp*. El cliente recibirá respuesta en el chat de *whatsapp*, indicando el plazo de atención de acuerdo con la clasificación del incidente. Las siguientes comunicaciones se realizarán para coordinar, obtener más información y resolver el requerimiento. Finalmente, el

cliente recibirá la respuesta al chat de *whatsapp*, confirmando la atención del incidente. Asimismo, recibirá un reporte de la incidencia al electrónico registrado.

Para la medición de satisfacción del servicio, el cliente recibirá una encuesta cada 3 meses, a fin de obtener *feedback* oportuno del cliente con respecto al servicio prestado. El cliente deberá completar la encuesta y enviarla por correo. Finalmente, se analizará el *feedback* y se evaluarán mejoras o ajustes a los servicios para asegurar la satisfacción y experiencia del cliente.

7.8. Protocolo de atención frente a un *ransomware*

El enfoque del plan *Cyber Plus* y sus *upgrades* es de carácter más preventivo, sin embargo, en el caso la pyme sea víctima de un *ransomware* se establece el siguiente protocolo de atención, ya sea si se recibe una alerta a través de la solución endpoint o es reportada vía *whatsapp* o correo por parte de la pyme:

- Establecer un canal de comunicación directo y seguro con el cliente para los *updates* constantes.
- Brindar al responsable de TI de la pyme su apoyo para la ejecución de las siguientes tareas:
    - Desconectar los equipos infectados de la red para evitar la propagación.
    - Los equipos infectados deben ser reiniciados en modo seguro para restringir la ejecución de programas y servicios innecesarios.
    - Las credenciales de acceso de los usuarios de los equipos comprometidos deben ser bloqueados en todos los sistemas, carpetas compartidas y plataformas a los que tienen acceso.
- El analista de *ciberseguridad* asignado para la atención del incidente en paralelo debe ejecutar las siguientes tareas:
    - Emplear el módulo antimalware de la solución endpoint para escanear y eliminar el *ransomware*.
    - Escanear y obtener el listado de los equipos infectados para enviar al responsable de TI.
    - Reescanear todos los equipos infectados para validar que el *ransomware* fue erradicado.

- En caso el *ransomware* siga presente en uno o más equipos infectados se debe indicar al responsable de TI de la pyme que restaure a punto de fábrica, reconfigure y notifique cuando haya concluido. El analista de *ciberseguridad* debe volver a ser escanear para comprobar que se ha eliminado todo rastro del *ransomware*.
- El analista de *ciberseguridad* en coordinación con el responsable de TI de la pyme valida la actividad de los usuarios en las últimas horas para encontrar alguna actividad sospechosa a través de la cuenta de algún colaborador.
- El analista de ciberseguridad coordina con el responsable de TI de la pyme la aprobación y el levantamiento de otra instancia en la nube de *Microsoft Azure* en el que se pueda efectuar el proceso de *backup* y *restore* de la información que respalda continuamente *CyberWave* a través del plan *Cyber Plus*.
- El responsable de TI de la pyme gestiona el cambio de contraseña obligatorio para todas las cuentas de acceso de los colaboradores en sistemas, plataformas y la nube.
- El analista de *ciberseguridad* recolecta evidencia, logs, el listado de acciones tomadas y demás datos útiles para la elaboración del respectivo informe que se enviará a la pyme.
- El analista de *ciberseguridad* continúa con el monitoreo a través de la solución endpoint.

7.9. Recursos Tecnológicos necesarios

Con el fin de que la empresa pueda prestar los servicios diseñados, se están considerando los siguientes componentes tecnológicos:

7.9.1. Solución integral de *Ciberseguridad*

Como bien se ha mencionado en los capítulos anteriores, la solución tecnológica de *ciberseguridad* elegida ha sido *GravityZone* Small Business Security de *Bitdefender*, la cual es una solución completa de *ciberseguridad*, diseñada para proteger a las pequeñas empresas de diversas amenazas cibernéticas.

De manera que, con el fin de que la empresa pueda gestionar las licencias y controlar la instalación de *GravityZone*, de manera efectiva, se debe considerar las siguientes actividades clave:

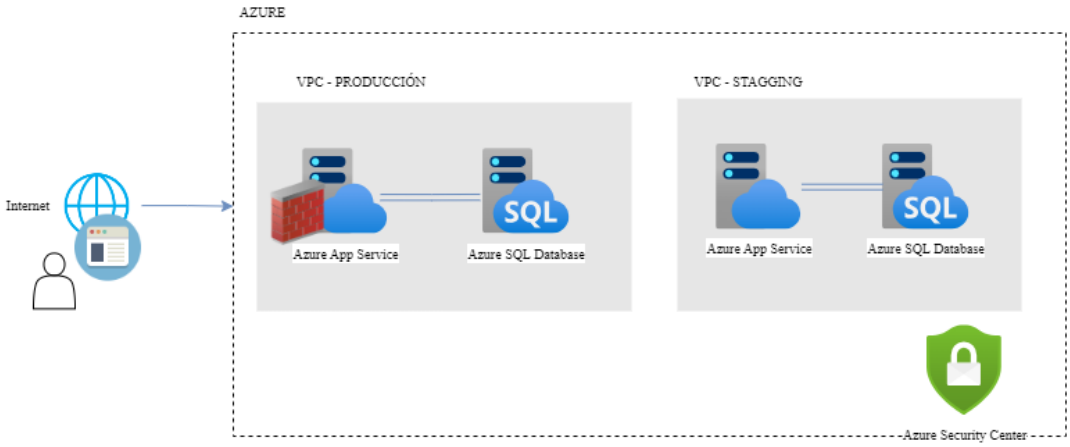
- *Partnership* anual con *Bitdefender*: Esto implica un costo anual del *partnership* asociado con la colaboración continua con *Bitdefender*, que puede incluye un precio más bajo para las licencias, además del *cibersoporte* y acceso a recursos exclusivos educativos y para capacitación.
- Adquisición de Licencias: *CyberWave* debe adquirir las licencias necesarias según el número de dispositivos o usuarios que desean proteger de sus clientes. La adquisición que se empleará será mensual y en función a la demanda proyectada, que se detalla en el capítulo 9.
- Registro en la Consola de *GravityZone:* Después de adquirir las licencias, se registra la empresa en la consola de administración de *GravityZone* provista por *Bitdefender*. Esto implicará la creación de una cuenta y el acceso a la consola en línea que será administrada por los Especialistas y Analistas de *ciberseguridad*.
- Asignación de Licencias: Dentro de la consola de administración, se asignan las licencias adquiridas a los dispositivos o usuarios que se desean proteger. Esto se utilizando el sistema de gestión de políticas definido por los Especialistas de *ciberseguridad* a fin de agrupar dispositivos y aplicar políticas de seguridad específicas en los clientes.
- Implementación en Dispositivos: Los Especialistas y Analistas de *ciberseguridad* instalan el software de seguridad de *Bitdefender* en los dispositivos que requieren protección. Esto puede hacerse de forma manual o mediante herramientas de implementación remota, dependiendo de la escala y la infraestructura de la empresa.
- Gestión de Políticas: Los Especialistas y Analistas de *ciberseguridad* configuran y gestionan las políticas de seguridad desde la consola central. Esto incluye la configuración de reglas de *firewall*, la programación de análisis de *malware* y la definición de políticas de uso de aplicaciones.
- Monitorización Continua: La consola de administración proporciona información en tiempo real sobre el estado de la seguridad en todos los dispositivos protegidos. Los Especialistas y Analistas de *ciberseguridad* pueden detectar y responder a amenazas de seguridad desde esta consola.

- Actualizaciones y Mantenimiento: *Bitdefender* suele proporcionar actualizaciones periódicas de sus definiciones de virus y software para mantener la protección al día. Estas actualizaciones se gestionan desde la consola de administración.
- Informe y Auditoría: La solución de seguridad *Bitdefender* ofrece la capacidad de generar informes detallados sobre la seguridad de la red y los dispositivos, lo que permite una auditoría efectiva.
- Auditoría y Cumplimiento: La empresa realizará auditorías periódicas para asegurarse de que todas las licencias se estén utilizando adecuadamente y que no haya instalaciones no autorizadas.
- Renovación de Licencias: Cuando se acerca la fecha de vencimiento de las licencias, la empresa debe renovarlas para garantizar una protección continua.

7.9.2. Infraestructura Tecnológica *Cloud* para el servicio

La infraestructura tecnológica que soporta a *CyberWave* se ha levantado en la nube pública de *Microsoft Azure* configurándose inicialmente 2 redes virtuales privadas, una de producción y otra de *stagging*. Los permisos y roles se restringirán desde *Azure Active Directory*. En cada red virtual privada se configurará el rango de direcciones IP y subredes necesario y diferente del otro. Empleando el servicio de *Azure App Service* en alta disponibilidad, el cual integra las funciones de servidor web y de aplicaciones para alojar los recursos necesarios como la página web, *landings* por campañas y sistemas. Asimismo, se está empleando *Azure SQL Database* en alta disponibilidad para el almacenamiento de la información a recabarse. Finalmente, se habilita el registro y monitoreo de los recursos usando el servicio de *Azure Security Center*.

Ilustración 7.4 Diagrama de la arquitectura configurada en la nube de Azure



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Para la solución propuesta se están considerando los siguientes recursos relacionados con infraestructura, tecnología y licencias necesarias para brindar el paquete de servicios:

Tabla 7.8 Recursos tecnológicos necesarios

RECURSOS TECNOLÓGICOS	DESCRIPCIÓN
Licencias de GravityZone Small Business Security de *Bitdefender*	Licencia por equipo que incluye protección del *endpoint, firewall, anti-exploit* y seguridad de navegación web.
Infraestructura de Microsoft Azure	Levantamiento de los servidores, repositorios de datos, base de datos por ambiente de desarrollo, pruebas y producción en la nube de *Azure*.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

7.9.3. Página Web

Para el proceso de Atención se ha planteado el desarrollo de una página web que tendrá las siguientes funcionalidades:

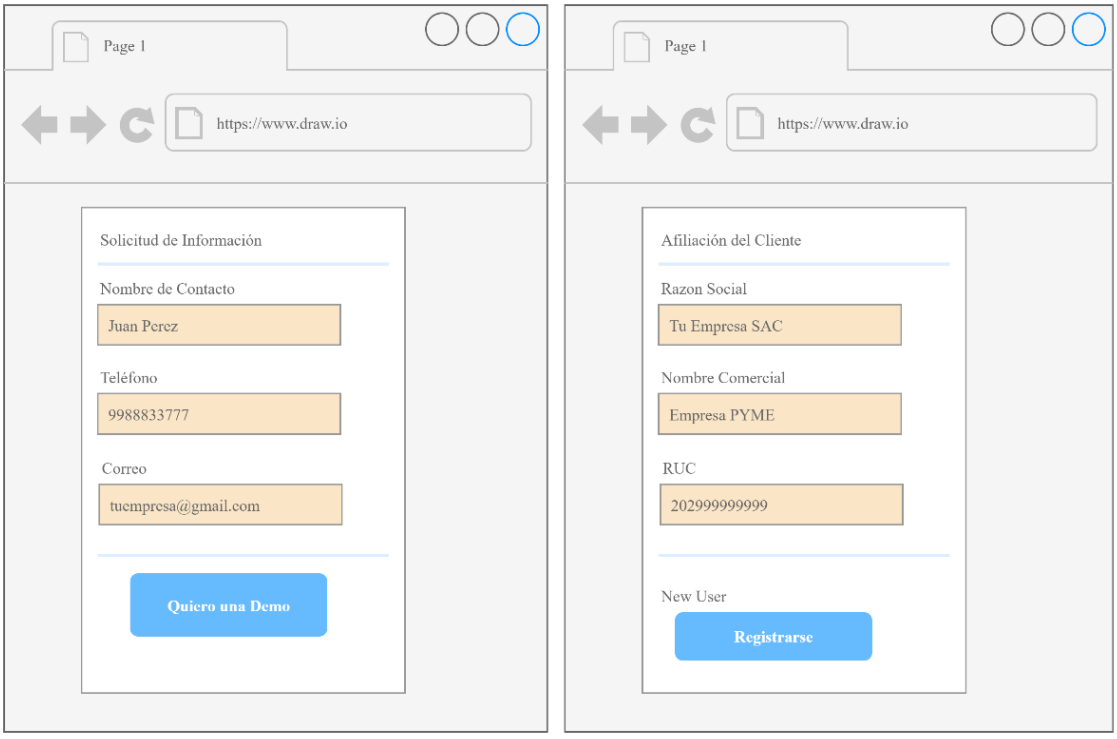
En primer lugar, se utilizará como punto de partida para establecer la presencia y visibilidad en línea de la empresa. Esto permitirá a los usuarios conocer la gama de

servicios disponibles y, si están interesados, registrar sus datos para solicitar información adicional o una demostración.

En segundo lugar, la página web facilitará que aquellos usuarios que hayan recibido una demostración y una cotización puedan afiliarse al servicio mediante un enlace enviado a su correo electrónico. Para este propósito, la página web estará conectada a una base de datos en la nube que registrará a los clientes que elijan afiliarse al servicio.

Por último, la página web actuará como un sistema de gestión de contenidos, permitiendo que *CyberWave* publique regularmente contenido educativo como boletines especializados, publicaciones y videos informativos. Esto contribuirá a la educación del público y fortalecerá la presencia de la empresa en el sector de la *ciberseguridad*.

Ilustración 7.5 Diseño de la Página Web



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.9.4. Otros recursos tecnológicos

En el contexto de la operación de la empresa, se deben considerar también una serie de recursos tecnológicos que desempeñan un papel fundamental y soportan la operación y los procesos previamente mencionados. Estos recursos incluyen licencias de Microsoft 365 para la comunicación y colaboración de los trabajadores. El *GravityZone Small Business Security* para la defensa propia contra amenazas cibernéticas de la empresa. Una infraestructura en la nube de Microsoft *Azure* para escalabilidad y disponibilidad tanto de la web como para contar con espacio para gestionar la propia información. El alquiler de equipos informáticos para brindar equipamiento adecuado al personal administrativo y operativo de la empresa. *TeFacturo El* Plan Emprendedor para la gestión eficiente de la facturación electrónica. Cada uno de estos recursos puede desempeñar un papel crucial en fortalecer la postura de *ciberseguridad* de la empresa.

Tabla 7.9 Listado de Recursos Tecnológicos

RECURSOS
Licencias de Microsoft 365 – Empresa Básico
Licencias de Microsoft 365 – Empresa Premium
Licencias de GravityZone Small Business Security
Infraestructura *cloud* en Microsoft Azure
Alquiler de Equipo Informático (Laptop) Operaciones
Alquiler de Equipo Informático (Laptop) Administrativos
TeFacturo Plan Emprendedor

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.10. Otros requisitos necesarios para el Servicio

En el caso de las marcas de soluciones de *ciberseguridad*, estas establecen ciertos requisitos que deben cumplir las empresas que buscan convertirse en sus *partners*, con el fin de ofrecer sus soluciones en el mercado, tales como:

- Cursar las formaciones técnicas y comerciales que brinde la marca y obtener los niveles de certificación necesarios en sus productos.
- Demostrar experiencia y competencia técnica a través de casos de estudio, referencias de clientes.
- Establecer metas de ventas mínimas que cada partner en consenso con la marca debe alcanzar.
- Pago de una cuota anual y tras cada renovación anual como parte del programa de *partners.*
- Acuerdo de *partner* para establecer los términos y condiciones de la asociación para acordar el manejo de las ventas, el soporte, el marketing, entre otros.

Asimismo, se considera necesario en una empresa del rubro de *ciberseguridad* contar con la implementación tanto de la norma ISO 27001 y de la norma ISO 22301. En primer lugar, la norma ISO 27001 proporciona un marco sólido para establecer un sistema de gestión de seguridad de la información eficaz, ayudando a identificar y gestionar los riesgos relacionados con la *ciberseguridad* de manera sistemática y estructurada.

Además, la ISO 27001 asegura la confidencialidad, integridad y disponibilidad de la información. Al implementar esta norma, *CyberWave* puede demostrar a sus clientes y socios comerciales su compromiso con la protección de la información sensible y la mitigación de riesgos cibernéticos. La norma también fomenta la mejora continua al requerir evaluaciones periódicas de riesgos y auditorías internas, lo que permite a la empresa adaptarse a las amenazas cambiantes y evolucionar sus medidas de seguridad de manera constante.

La implementación de la norma ISO 22301 en una empresa de *ciberseguridad* es crucial para establecer un sistema de gestión de continuidad del negocio. Esto asegura la preparación y recuperación ante interrupciones, como ciberataques, garantizando la operación continua de los servicios. Además, la norma promueve la identificación de riesgos, planificación de respuestas a incidentes y pruebas de recuperación, fortaleciendo la resiliencia y demostrando compromiso con la disponibilidad y fiabilidad de los servicios de *ciberseguridad*.

7.11. Monitoreo e Indicadores

Para poder monitorear los resultados y el desempeño que se obtendrán de los procesos y servicios definidos en el plan operativo, es necesario realizar la definición de las métricas clave.

Los *KPIs* (indicadores clave de rendimiento) sirven para realizar mediciones objetivas que permitan determinar los procesos que están funcionando o no, dentro de *CyberWave*. El análisis a través de los resultados numéricos obtenidos permitirá identificar brechas y realizar ajustes para asegurar el éxito de las estrategias definidas (Martos, 2022).

A continuación, se describirán los indicadores más importantes para la medición del progreso que se han identificado para el plan, y que servirán como guía para la toma de decisiones.

Tabla 7.10 Indicadores Clave de Operación

INDICADOR	DESCRIPCIÓN
Número de Demostraciones realizadas en plazo	Evalúa el porcentaje de Demostraciones de servicio agendadas con los clientes prospectos y realizadas dentro del plazo establecido.
Número de Instalaciones realizadas en plazo	Evalúa el porcentaje de instalaciones de servicio planificadas y realizadas dentro del plazo establecido.
Ratio de Conversión de Ventas	Evalúa la proporción de clientes a los cuales se les presentó una Demo y adquirieron el servicio.
Nivel de atención de incidencias y requerimientos	Evalúa el porcentaje de atención de las incidencias y requerimientos solicitados por el cliente y que fueron atendidos dentro del plazo establecido.
Tiempo Medio de Respuesta ante Incidentes y Requerimientos	Evalúa el promedio del tiempo de Respuesta ante incidentes y Requerimientos, de acuerdo con su categorización.
Nivel de Atención de Envío de Reportes mensuales de Servicio	Evalúa el porcentaje del envío los Reportes de Servicio mensuales que fueron enviados dentro del plazo establecido.
Nivel de Satisfacción del Cliente	Evalúa la calidad percibida por los clientes del servicio, obtenido en la encuesta.
Net Promoter Score	Evalúa el nivel de satisfacción y lealtad de los clientes, obtenido en la encuesta.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.12. Presupuesto de Operaciones

7.12.1. Plan de Producción

Para poder estimar las horas hombre necesarias para brindar el servicio, es necesario establecer los tipos de atención y los tiempos promedio necesarios para estas atenciones. Esta información se obtuvo a partir de la estimación vía juicio de experto para atenciones similares en otras empresas.

Tabla 7.11 Estimación de Horas de Analista y Especialista

TIPO DE ATENCIÓN	ACTIVIDAD	HORAS AL MES	RECURSO
Coordinación de Ventas	Coordinación con Clientes durante el proceso de Venta	4	*key account manager*
Demo	Presentación de Demo	1	Analista
Instalación	Instalación y Configuración	3	Analista
	Instalación y Configuración	1	Especialista
Capacitación a Clientes	Capacitación clientes VIP	0.33	Especialista
Capacitación a Clientes	Capacitación clientes Regular	0.08	Especialista
Reporte Mensual	Elaboración del Reporte	2	Analista
	Validación del Reporte	1	Especialista
Gestión de Contenido	Boletines mensuales	4	Especialista
	Webinars posicionamiento	1	Especialista
	Contenido para Programa de Concientización	4	Especialista
Requerimientos e Incidentes	Atención de Requerimientos e Incidentes	6.19	Analista hrs
	Atención de Requerimientos e Incidentes	3.81	Especialista hrs
	Seguimiento de Requerimientos e Incidentes	4	*key account manager*
Atención a Clientes	Gestión de Comunicaciones con Clientes	4	*key account manager*

TIPO DE ATENCIÓN	ACTIVIDAD	HORAS AL MES	RECURSO
Investigación y Desarrollo	Investigación y Desarrollo	10	Especialista

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

De este cálculo se obtiene que la media de tiempos tanto del Analista y del Especialista de *ciberseguridad*, así como para el *key Account Manager*. Estos tiempos se aplicarán para estimar el plan de producción, el cual se presenta en la tabla a continuación. En el plan de producción, partiendo de la estimación de la demanda, que se indica en el capítulo 9, se calcula la cantidad de horas hombre por cada recurso operativo, de acuerdo con los tiempos que se han determinado para cada tarea.

Tabla 7.12 Estimación de Horas de Analista y Especialista

	AÑO 1	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Días laborables	264	264	264	264	264
Demanda	**57**	**23**	**28**	**32**	**28**
Demanda acumulada	**357**	**677**	**844**	**956**	**1048**
Deserción	**0**	**9**	**12**	**16**	**21**
Horas analista	3,703.21	6,512.07	8,114.40	9,192.90	10,035.09
Horas especialistas	2,490.94	4,123.92	5,122.07	5,795.63	6,302.17
Horas *key account manager*	3,084.00	5,508.00	6,864.00	7,776.00	8,496.00
Suplemento analista (15%)	555.48	976.81	1,217.16	1,378.93	1,505.26
Suplemento especialista (15%)	373.64	618.59	768.31	869.35	945.33
Suplemento *key account manager* (15%)	462.60	826.20	1,029.60	1,166.40	1,274.40
Total, horas analista	**4,258.70**	**7,488.88**	**9,331.56**	**10,571.83**	**11,540.36**
Total, horas especialista	**2,864.58**	**4,742.50**	**5,890.38**	**6,664.98**	**7,247.50**
Total de horas K*ey Account Manager*	**3,546.60**	**6,334.20**	**7,893.60**	**8,942.40**	**9,770.40**
Cantidad de *key account manager*	**3.00**	**4.00**	**5.00**	**5.00**	**6.00**
Cantidad especialistas	**3.00**	**3.00**	**3.00**	**4.00**	**4.00**
Cantidad analistas	**4.00**	**5.00**	**5.00**	**6.00**	**7.00**
Costo de analista	**S/ 111,111**	**S/ 217,778**	**S/ 266,667**	**S/ 284,444**	**S/ 328,889**
Costo de especialista	**S/ 126,667**	**S/ 240,000**	**S/ 240,000**	**S/ 266,667**	**S/ 320,000**
Costo de *key account manager*	**S/ 61,111**	**S/ 105,556**	**S/ 138,889**	**S/ 166,667**	**S/ 172,222**
Costo de horas extra de analista	**S/ 6,778**	**S/ 0**	**S/ 1,241**	**S/ 1,718**	**S/ 0**
Costo de horas extra de especialista	**S/ 4,184**	**S/ 0**	**S/ 5,055**	**S/ 5,129**	**S/ 0**

Costo de horas extra *key account manager*	**S/ 7,333**	**S/ 4,439**	**S/ 2,567**	**S/ 634**	**S/ 634**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.12.2 Presupuesto Operativo

Los costos de los recursos necesarios, que hacen posible la prestación del servicio se estan considerando como costos directos e indirectos de operación.

Respecto a los costos directos de operación, se está considerando al costo de las licencias de la plataforma e*ndpoint* de *Bitdefender* y el Servicio *cloud* de *Microsoft Azure*.

Respecto al costo de la plataforma endpoint, *GravityZone Small Business Security*, esta tiene un costo anual por cada usuario de acuerdo a lo indicado en la tabla líneas abajo. Asimismo, se está considerando un número máximo de 49 licencias para el plan *Cyber Plus*. Esta decisión corresponde a la cantidad máxima de trabajadores que tienen las empresas pequeñas, considerando que estas tienen la mayor proporción para nuestro mercado, según se analizó en el segmento de clientes del capítulo 4.

Respecto al costo del almacenamiento cloud, *Azure*, este tiene un costo mensual de indicado en la tabla líneas abajo. La capacidad considerada para cada cliente es de 5TB como máximo para el plan *Cyber Plus.* Este es un supuesto considerado a partir de las entrevistas realizadas a expertos.

Tabla 7.13 Tabla de Costos Unitarios

Recurso	**Cantidad máxima de licencias por cada paquete**	**Costo anual por usuario ($)**	**Costo anual por paquete ($)**	**Costo anual por paquete (S/.)**	**Descripción**
Licencia de Plataforma *Endpoint*	49	$ 15.74	$ 771.26	S/ 2,854	*GravityZone Small Business Security*

Recurso	Costo mensual por 5 TB	Costo mensual por paquete ($)	Costo mensual por paquete (S/.)	Descripción
Espacio Cloud necesario, *Azure (Microsoft)*	$ 152.49	$ 152.49	S/ 564	Servicio de *Azure Backup.*

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Por otro lado, se están considerando también costos indirectos de operación. Entre los cuales cabe resaltar a las licencias de *Microsoft* 365 necesarias para que los colaboradores puedan realizar sus tareas del día a día. Las Licencias de *Gravity Zone,* necesarias para que los colabores de la empresa puedan estar protegidos. La infraestructura *cloud* necesaria para el almacenamiento de toda la información generada por los componentes de la solución, y la información generada por analistas y especialistas. También se considera el alquiler de equipos informáticos, instrumento principal de trabajo de los colaboradores. Muy importante tambien considerar el costo anual del *Partnership* con *Bitdefender.* Finalmente se encuentran los gastos para la recertificación de la ISO 27001 y la ISO 22301.

Tabla 7.14 Tabla de Costos de Indirectos de Operación

Recurso	Costo anual	Descripción
Licencias de Microsoft 365 – Empresa Básico	$ 6	De tipo Empresa Básico para la mayoría de los colaboradores. La suite de Microsoft permitirá contar las herramientas de ofimática necesarias para el día a día.
Licencias de Microsoft 365 – Empresa Premium	$ 22	De tipo E Empresa Premium para configuraciones avanzadas de seguridad para el equipo de *ciberseguridad*. La suite de Microsoft permitirá contar las herramientas de ofimática necesarias para el día a día.
Licencias de GravityZone Small Business Security	$ 16	Licencia por equipo que incluye protección del endpoint, firewall, anti-exploit y seguridad de navegación web.

Recurso	Costo anual	Descripción
Infraestructura cloud en Microsoft Azure	$1,095	El servicio de almacenamiento cloud necesario para el Levantamiento de Azure App Services con WAF y base de datos SQL para ambientes de stagging y producción en la nube de Azure. Asimismo, para el almacenamiento de toda la información generada por los componentes de la solución, y la información generada por analistas y especialistas.
Alquiler de Equipo Informático (Laptop) Operaciones	$ 977	El servicio comprende el alquiler del Equipo, Recambio inmediato de equipo similar en máximo 24 horas, el Mantenimiento preventivo una vez al año, Help desk remoto en 5 minutos.
Alquiler de Equipo Informático (Laptop) Administrativos	$ 750	El servicio comprende el alquiler del Equipo, Recambio inmediato de equipo similar en máximo 24 horas, el Mantenimiento preventivo una vez al año, *Help desk* remoto en 5 minutos.
Costo anual del *partnership* con *Bitdefender*	$ 5,000	Programa de alianza con la marca *Bitdefender* que se renueva por año.
ISO 22301 Recertificación	S/ 15,000	Implica gastos como la auditoría de certificación, revisión y actualización del sistema de gestión, formación y capacitación del personal, ajustes en la infraestructura y procesos, posible contratación de consultores especializados, revisión continua y mejoras, así como el pago de tasas de certificación.
ISO 27001 Recertificación	S/ 15,000	Implica gastos como la auditoría de certificación, revisión y actualización del sistema de gestión, formación y capacitación del personal, ajustes en la infraestructura y procesos, posible contratación de consultores especializados, revisión continua y mejoras, así como el pago de tasas de certificación

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Finalmente, en base a los costos unitarios mencionados, se anualizan y totalizan acordes a la demanda proyectada, que se indica en el capítulo 8, obteniendo los resultados descritos en la tabla líneas abajo. Cabe resaltar que se está considerando un presupuesto de 5% destinado a la Investigación y Desarrollo, acorde a los procesos

indicados en el numeral 7.4.1. Así como también un margen de contingencia del 3% ante posibles eventualidades.

Tabla 7.15 Tabla de Costos de Operación

Concepto	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Costos directos de operación					
Espacio de almacenamiento en Azure Backup	S/ 288,877	S/ 470,757	S/ 430,863	S/ 452,653	S/ 454,377
Licencia de GravityZone Small Business Security	S/ 121,756	S/ 198,415	S/ 181,601	S/ 190,785	S/ 191,512
Costos del Plan Backup Plus	S/ 101,572	S/ 165,523	S/ 151,496	S/ 151,325	S/ 149,383
Costos del Plan Support Plus	S/ 14,909	S/ 24,296	S/ 22,237	S/ 23,361	S/ 23,450
Subtotal Costos Directos	**S/ 527,114**	**S/ 858,990**	**S/ 786,197**	**S/ 818,124**	**S/ 818,722**
Costos indirectos de operación					
Licencias de *Microsoft 365*	S/ 6,638	S/ 10,723	S/ 11,259	S/ 12,010	S/ 14,787
Licencias de *GravityZone Small Business Security*	S/ 675	S/ 1,040	S/ 1,092	S/ 1,157	S/ 1,345
Infraestructura Cloud en Microsoft Azure	S/ 4,052	S/ 4,255	S/ 4,467	S/ 4,691	S/ 6,533
Alquiler de equipo informático (laptop)	S/ 36,356	S/ 56,607	S/ 59,437	S/ 63,107	S/ 74,318
Costo anual del *Partnership* con *Bitdefender*	S/ 5,000	S/ 5,250	S/ 5,513	S/ 5,788	S/ 6,078
ISO 22301 recertificación	S/ 15,000	S/ 15,750	S/ 16,538	S/ 17,364	S/ 18,233
ISO 27001 recertificación	S/ 15,000	S/ 15,750	S/ 16,538	S/ 17,364	S/ 18,233
Subtotal Costos Indirectos	**S/ 82,720**	**S/ 109,374**	**S/ 114,842**	**S/ 121,482**	**S/ 139,526**
Investigación y desarrollo					
Costos de Investigación y Desarrollo	S/ 30,492	S/ 48,418	S/ 45,052	S/ 46,980	S/ 47,912
Subtotal Investigación y Desarrollo	**S/ 30,492**	**S/ 48,418**	**S/ 45,052**	**S/ 46,980**	**S/ 47,912**
Contingencia					
Contingencias	S/ 18,295	S/ 29,051	S/ 27,031	S/ 28,188	S/ 28,747
Subtotal Contingencia	**S/ 18,295**	**S/ 29,051**	**S/ 27,031**	**S/ 28,188**	**S/ 28,747**
Total (s/.)	**S/ 628,129**	**S/ 997,415**	**S/ 928,070**	**S/ 967,794**	**S/ 986,995**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

7.13. Conclusión del Capítulo

De acuerdo con lo desarrollado en el presente capítulo se inició con la definición de los procesos en sus tres niveles, estratégicos, de negocio y de soporte. Identificando los objetivos correspondientes.

Asimismo, se define el servicio partiendo de la solución diseñada en el capítulo 4, ofreciendo una Protección activa contra amenazas cibernéticas para dispositivos finales, Respaldo seguro y recuperación de datos en caso de pérdida o ataque, monitoreo continuo y respuesta rápida a incidentes de seguridad y educación y formación de empleados en prácticas de seguridad cibernética. También, se han definido las políticas del servicio, y sobre el diseño del mismo se plantean dos procesos principales: Inscripción y afiliación de clientes; Operación del servicio de *ciberseguridad.*

A continuación, se definen como recursos tecnológicos necesarios para brindar el servicio, tales como la solución integral de *ciberseguridad*, la infraestructura *cloud*, la página web entre otros recursos necesarios para asegurar la operación.

En este orden, se definieron los requisitos necesarios para el servicio, tales como las alianzas o el *partnership* con las marcas tecnológicas de *ciberseguridad*, y la implementación de las normas ISO 27001 y ISO 22301.

Finalmente se definió el Plan de Producción, los costos recurrentes (tanto variables como fijos) y finalmente se armó un presupuesto operativo, el cual hace posible la prestación del servicio.

CAPITULO 8 . PLAN ORGANIZACIONAL

En el presente plan se definirán las consideraciones para la estructura organizacional de la empresa, de modo que le permita desarrollar las estrategias planteadas en el plan de marketing y plan de operaciones.

Se procederá a detallar los puestos claves y organigrama organizacional y los perfiles necesarios para cada puesto.

8.1. Objetivo general

El principal objetivo que plantea el Plan Organizacional descrito es el establecimiento de la dirección de la empresa, definiendo los roles, responsabilidades, estructura de comunicación interna de la compañía y sentar las bases para el crecimiento y desarrollo de su cultura.

8.2. Objetivos específicos:

- Definir la constitución de la organización
- Definir el organigrama de la organización
- Definir y detallar los perfiles para cada puesto

8.3. Constitución de la Empresa

Para la constitución de la empresa del presente plan de negocios, se tomará como base legal el marco regulatorio actual para la constitución de una empresa en Perú.

Estos son los principales tipos de empresas y sus características, según lo expresa (Gobierno Nacional, 2023):

Tabla 8.1 Tipos de empresas

	CANTIDAD ACCIONISTAS / SOCIOS	ORGANIZACIÓN	CAPITAL Y ACCIONES	EJEMPLO
SOCIEDAD ANÓNIMA (S.A.)	Mínimo: 2	Se debe establecer	Capital definido por aportes de cada socio.	Cassinelli S.A.
	Máximo: ilimitado	-Junta general de accionistas.	Se deben registrar las acciones en el Registro de Matrícula de Acciones.	Socosani S. A. Banco Ripley Peru S.A.
		-Gerencia.	-	-
		-Directorio.	-	-
SOCIEDAD ANÓNIMA CERRADA (S.A.C.)	Mínimo: 2	Se debe establecer	Capital definido por aportes de cada socio.	Montalvo Spa Peluqueria S.A.C.
	Máximo: 20	-Junta general de accionistas.	Se deben registrar las acciones en el Registro de Matrícula de Acciones.	Pisopak Peru S.A.C. Distribuidora Concordia S.A.C.
		-Gerencia.	-	-
		-Directorio. (Opcional)	-	-
SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA (S.R.L.)	Mínimo: 2	Normalmente empresas familiares pequeñas.	Capital definido por aportes de cada socio.	Clinica Cayetano Heredia S.R.L.
	Máximo: 20		Se debe inscribir en Registros Públicos.	Corporacion Inca Kola Peru S.R.L. Directv Peru S.R.L.
EMPRESARIO INDIVIDUAL DE RESPONSABILIDAD LIMITADA (E.I.R.L.)	Máximo: 1	Una sola persona figura como Gerente General y socio.	Capital definido por aportes del único aportante.	G.L.P. Distribuciones E.I.R.L.
				Global Solutions Peru E.I.R.L. Plastitodo E.I.R.L.
SOCIEDAD ANÓNIMA ABIERTA (S.A.A.)	Mínimo: 750	Se debe establecer	Más del 35% del capital pertenece a 175 o más accionistas.	Alicorp S.A.A.

		-Junta general de accionistas.	Debe haber hecho una oferta pública primaria de acciones u obligaciones convertibles en acciones. Deben registrar las acciones en el Registro de Matrícula de Acciones.	Luz del Sur S.A.A. Creditex S.A.A.
		-Gerencia.		
		-Directorio.		

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

A efectos de este plan de negocios y considerando las características del servicio que se prestará, se ha definido trabajar bajo la creación de una Sociedad Anónima Cerrada (S.A.C.). Este tipo de empresas son creadas por personas naturales o jurídicas, con un mínimo de 2 accionistas y un máximo de 20, el capital de la sociedad será definido por el aporte de cada uno de los miembros.

En ese sentido, la empresa se constituirá bajo el nombre de la sociedad *CYBERWAVE* S.A.C., bajo la forma societaria de Sociedad Anónima Cerrada (S.A.C.), cuyo capital será conformado por los aportes de sus accionistas, y que se constituye como persona jurídica. Se contará con la participación de 4 socios mayoritarios, con domicilio fiscal registrado en San Borja, con una duración indefinida.

Tabla 8.2 Resumen de datos de constitución de la empresa

NOMBRE DE LA SOCIEDAD	***CYBERWAVE* S.A.C.**
FORMA SOCIETARIA	SOCIEDAD ANONIMA CERRADA
CAPITAL SOCIAL	APORTE DE ACCIONISTAS
TIPO DE SOCIEDAD	PERSONA JURIDICA
CANTIDAD DE SOCIOS	4
DOMICILIO FISCAL	SAN BORJA
DURACIÓN DE LA SOCIEDAD	INDEFINIDA

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Según lo publicado por el portal del gobierno peruano, para poder registrar o constituir una empresa se deben seguir los siguientes pasos:

- Buscar y reservar el nombre elegido
- Elaboración del acto constitutivo (Minuta)
- Abono de capital y bienes
- Elaboración de la escritura pública
- Inscripción en registros públicos (SUNARP)
- Inscripción al RUC para persona jurídica

El presupuesto para la constitución de la empresa es el que se detalla a continuación:

Tabla 8.3 Presupuesto de constitución de la empresa

CONCEPTO	**IMPORTE (S/.)**
REGISTRO COMO PERSONA JURÍDICA	S/ 1,000
DERECHOS Y PATENTES REGISTRAL	S/ 30
GASTOS NOTARIALES	S/ 400
TOTAL CONSTITUCIÓN	**S/ 1,430**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

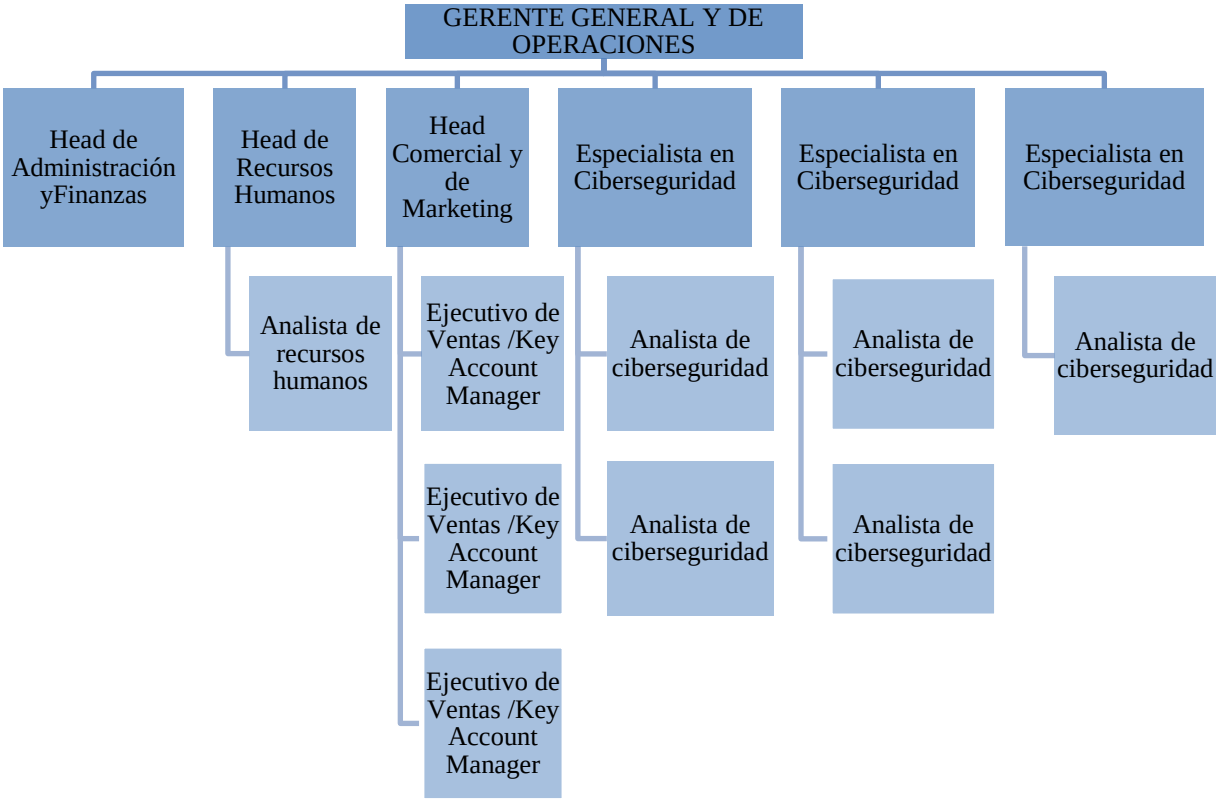
8.4. Estructura Organizacional

En el escenario de crecimiento digital exponencial se puede encontrar que la mayoría de las industrias, economías y sociedades están migrando a organizaciones ágiles, según McKinsey&Company (2018) “Agilidad rima con estabilidad”, por lo que solo las organizaciones verdaderamente ágiles pueden dominar el arte de ser dinámicas y estables al mismo tiempo.

Dado que la *ciberseguridad* se dedica a salvaguardar los activos empresariales ante ataques impredecibles en diversos escenarios, se considera que una organización ágil es esencial para complementar la propuesta de valor en el plan de negocios. Esta propuesta asegura que, en momentos críticos, la organización responda con agilidad a la situación y los riesgos, brindando estabilidad y una capacidad de adaptación más sólida ante posibles cambios.

Para lograr esto, es crucial establecer una cultura organizativa sólida, con valores coherentes y enfocados, así como definir una visión y un propósito compartidos. El objetivo es que todo el equipo se sienta profundamente comprometido a nivel personal y emocional. En este sentido, se plantea una estructura organizacional tradicional de manera inicial, que se irá transformando en ágil a medida que se complejice los servicios y aumente la cartera de clientes:

Tabla 8.4 Estructura Organizacional al cierre del 1er año



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

8.4.1. Descripción de los Puestos

Tabla 8.5 Descripción de puesto Gerente General y de Operaciones

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Gerente General y de Operaciones
Supervisado por:	Junta Directiva
Jefe Inmediato:	Presidente de la Junta Directiva
Personas a cargo:	Head de Administración y Finanzas, Head de Recursos Humanos, Head comercial y de MKT, Especialistas en *Ciberseguridad*
Objetivo del Cargo o Puesto de Laboral	

Tiene como objetivo liderar la dirección estratégica de *CyberWave* y ser el representante. Además, lidera y supervisa todas las actividades operativas relacionadas con la *Ciberseguridad* y la protección de activos digitales de la empresa y sus clientes. Su enfoque está en garantizar la integridad, confidencialidad y disponibilidad de la información, así como en prevenir y responder eficazmente a las amenazas cibernéticas.

Funciones Generales	
a)	**Planificación Estratégica:** Definir y establecer la dirección estratégica de la empresa a corto, medio y largo plazo identificando oportunidades de negocio, establecer objetivos y determinar cómo alcanzar los objetivos. Ser el representante de la empresa ante medios, la comunidad, instituciones gubernamentales, entre otros.
b)	**Gestión de *Ciberseguridad*:** Planificar y supervisar la ejecución de estrategias para mitigar riesgos cibernéticos, establecer objetivos operativos y alinearlos con la visión y misión de la empresa.
c)	**Gestión de Equipos:** Supervisar y liderar el equipo de operaciones de *Ciberseguridad*, incluyendo la formación, desarrollo y evaluación del desempeño de los miembros del equipo.
d)	**Monitoreo y Respuesta a Incidentes:** Supervisar las actividades de monitoreo de *Ciberseguridad* en tiempo real, apoyar en el seguimiento y análisis de posibles *ciberincidentes* críticos, y coordinar respuestas efectivas para mitigar los impactos.
e)	**Seguimiento a la implementación de medidas de *Ciberseguridad*:** Liderar el seguimiento a la implementación de controles de *Ciberseguridad*, políticas y procedimientos, así como garantizar la aplicación de estándares reconocidos.

Relación con otros Departamentos
El Gerente General y de Operaciones de *Ciberseguridad* colabora estrechamente con el equipo ejecutivo, el departamento legal, el equipo de desarrollo de software, el equipo de TI, el equipo de recursos humanos y el equipo de comunicaciones para garantizar una estrategia integral de *Ciberseguridad* en toda la empresa.

Habilidades y Conocimientos
Conocimientos en gestión de equipos, comunicación efectiva, planificación estratégica, gestión de incidentes, conocimiento legal y normativo, tecnologías de *Ciberseguridad*, resolución de problemas, gestión de proyectos, visión empresarial. Certificaciones en *Ciberseguridad* como el *CISM, CISSP y/o CRISC, y un MBA.*

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.6 Descripción de puesto Head de Administración y Finanzas

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Head de Administración y Finanzas
Supervisado por:	Gerente General y de Operaciones
Jefe Inmediato:	Gerente General y de Operaciones
Personas a cargo:	Servicio tercerizado

Objetivo del Cargo o Puesto de Laboral

Tiene como objetivo principal gestionar eficientemente los recursos financieros y administrativos de la empresa de *Ciberseguridad*, asegurando la salud financiera de *CyberWave*, el cumplimiento de regulaciones fiscales y la optimización de los procesos administrativos.

Funciones Generales	
a)	**Gestión Financiera:** Supervisar la planificación y gestión financiera, incluyendo presupuestos, proyecciones, análisis de costos y beneficios, y flujo de efectivo.
b)	**Cumplimiento Regulatorio:** Asegurar que la empresa cumpla con todas las regulaciones fiscales y normativas relacionadas con las finanzas y la contabilidad.
c)	**Negociaciones Financieras:** Participar en negociaciones con bancos, proveedores y clientes para asegurar condiciones financieras favorables para la empresa.
d)	**Análisis de Riesgos:** Evaluar riesgos financieros y desarrollar estrategias para mitigarlos, incluyendo la gestión de riesgos relacionados con inversiones y financiamiento.
e)	**Gestión de Activos:** Supervisar la gestión de activos, incluyendo equipos tecnológicos y licencias de software, garantizando su adecuado mantenimiento y actualización.

Relación con otros Departamentos
El Head de Administración y Finanzas colabora estrechamente con los equipos ejecutivo, de operaciones, ventas y recursos humanos. También interactúa con el equipo legal para garantizar el cumplimiento normativo y contractual en cuestiones financieras.

Habilidades y conocimientos
Gestión financiera, cumplimiento normativo, habilidades analíticas, liderazgo, comunicación financiera, planificación estratégica, negociación, tecnología financiera, ética profesional, conocimiento de la industria.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.7 Descripción de puesto Head de Recursos Humanos

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Head de Recursos Humanos
Supervisado por:	Gerente General y de Operaciones
Jefe Inmediato:	Gerente General y de Operaciones
Personas a cargo:	Analista de Recursos Humanos

Objetivo del Cargo o Puesto de Laboral
Tiene como objetivo principal liderar las estrategias y actividades relacionadas con el capital humano de *CyberWave*, asegurando la atracción, retención y desarrollo de talento en línea con los objetivos.

Funciones Generales	
a)	**Gestión del Talento:** Diseñar y ejecutar estrategias para atraer, seleccionar y retener a profesionales calificados en el campo de la *Ciberseguridad*.
b)	**Desarrollo Organizacional:** Identificar necesidades de capacitación y desarrollo, diseñar programas de formación, y fomentar un ambiente de aprendizaje continuo.
c)	**Gestión de Desempeño:** Implementar sistemas de evaluación del desempeño, proporcionando retroalimentación constructiva y estableciendo planes de mejora para los empleados.
d)	**Relaciones Laborales:** Gestionar relaciones con empleados, manejar conflictos y colaborar con el cumplimiento de políticas y regulaciones laborales.
e)	**Reclutamiento y Selección:** Supervisar el proceso de reclutamiento, entrevistas y selección de candidatos, considerando las necesidades específicas de la *Ciberseguridad*.

Relación con otros Departamentos
El Head de Recursos Humanos colabora con el equipo ejecutivo, el departamento legal, el departamento de operaciones, el equipo de administración y finanzas, y otros equipos funcionales para garantizar la alineación de estrategias de recursos humanos con los objetivos empresariales.

Habilidades y conocimientos
Gestión del talento, comunicación interpersonal, liderazgo, conocimiento legal, resolución de conflictos, desarrollo organizacional, conocimiento de la industria, tecnología de recursos humanos, ética profesional, empatía y escucha activa.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.8 Descripción de puesto Analista de Recursos Humanos

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Analista de Recursos Humanos
Supervisado por:	Head de Recursos Humanos
Jefe Inmediato:	Head de Recursos Humanos
Personas a cargo:	-

Objetivo del Cargo o Puesto de Laboral
El objetivo principal del Analista de Recursos Humanos es asegurar la atracción, integración y retención de talento especializado en *Ciberseguridad* mediante procesos efectivos de reclutamiento y selección, programas estructurados de inducción, un sistema competitivo y equitativo de beneficios y compensaciones, y evaluaciones de desempeño continuas.

Funciones Generales

a)	Asistir en la administración de procesos de reclutamiento y selección, incluida la revisión de currículums, coordinación de entrevistas y comunicación con candidatos.
b)	Apoyar en la inducción y orientación de nuevos empleados en temas de recursos humanos y culturales.
c)	Mantener y actualizar registros de empleados, incluyendo información personal, historial laboral y documentación legal.
d)	Participar en la gestión de beneficios y compensaciones, asegurando que se cumplan los requisitos legales y las expectativas de los empleados.
e)	Asistir en la gestión de evaluaciones de desempeño y retroalimentación.

Relación con otros Departamentos
El Analista de Recursos Humanos colabora con el equipo de Recursos Humanos, departamento de Finanzas, departamento de Operaciones, departamento de Capacitación.

Habilidades y conocimientos
Gestión del talento, comunicación interpersonal, resolución de conflictos, desarrollo organizacional, conocimientos en la industria de *Ciberseguridad*, tecnología de recursos humanos, ética profesional, empatía y escucha activa, prácticas y regulaciones de recursos humanos.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.9 Descripción de puesto Head Comercial y de Marketing

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Head Comercial y de Marketing
Supervisado por:	Gerente General y de Operaciones
Jefe Inmediato:	Gerente General y de Operaciones
Personas a cargo:	Ejecutivo Comercial / *Key Acount Manager*

Objetivo del Cargo o Puesto de Laboral
Tiene como objetivo principal liderar las estrategias y actividades relacionadas con la promoción, comercialización y venta de los servicios de *Ciberseguridad* de la empresa, impulsando el crecimiento de ingresos y la expansión del mercado.

Funciones Generales	
a)	**Estrategia Comercial y de Marketing:** Diseñar y ejecutar estrategias integrales que impulsen la generación de leads, la conversión de ventas y la mejora de la visibilidad de la marca.
b)	

	Desarrollo de Mercado: Identificar oportunidades de mercado, segmentos de clientes y geografías para el crecimiento de la empresa.
c)	**Generación de Leads:** Supervisar la creación de campañas de marketing digital y estrategias de generación de leads para atraer clientes potenciales.
d)	**Gestión de Ventas:** Dirigir el equipo de ventas en la identificación de oportunidades, el proceso de ventas y el cierre exitoso de acuerdos.
e)	**Desarrollo de Contenido:** Supervisar la creación de contenido de calidad, incluyendo blogs, estudios de caso y materiales de marketing, para respaldar la estrategia de ventas.

Relación con otros Departamentos
El Head Comercial y de Marketing colabora estrechamente con el equipo ejecutivo, el equipo de Operaciones, y el equipo de Recursos Humanos para garantizar la coherencia en la oferta de productos, servicios y mensajes.

Habilidades y conocimientos
Ventas y marketing, liderazgo, comunicación estratégica, análisis de datos, negociación, conocimiento de la industria, gestión de proyectos, marketing digital, comunicación interpersonal, innovación.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.10 Descripción de puesto Ejecutivo de Ventas / *Key Account Manager*

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Ejecutivo de Ventas / *Key Account Manager*
Supervisado por:	Head Comercial y de Marketing
Jefe Inmediato:	Head Comercial y de Marketing
Personas a cargo:	-

Objetivo del Cargo o Puesto de Laboral
Tiene como objetivo principal desarrollar y mantener relaciones sólidas con clientes clave (grandes cuentas) en el sector de la *Ciberseguridad*, identificando sus necesidades y ofreciendo soluciones que resuelvan problemas específicos, contribuyendo así al crecimiento de los ingresos de la empresa.

Funciones Generales	
a)	**Gestión de Cuentas Clave:** Desarrollar relaciones sólidas con clientes clave, comprendiendo sus objetivos, necesidades y desafíos en *Ciberseguridad*.
b)	**Identificación de Oportunidades:** Identificar oportunidades de ventas cruzadas y upselling dentro de las cuentas asignadas.
c)	**Elaboración de Estrategias:** Crear y ejecutar estrategias de ventas personalizadas para cada cliente clave, alineadas con sus necesidades y metas.

d)	**Presentación de la Demostración:** Presentar el paquete de servicios de *Ciberseguridad* de manera persuasiva, destacando los beneficios y el valor que aportan al cliente, con apoyo del Analista de *Ciberseguridad*.
e)	**Seguimiento Postventa:** Asegurar la satisfacción continua del cliente y gestionar cualquier problema que pueda surgir.

Relación con otros Departamentos
El Ejecutivo de Ventas *Key Account Manager* trabaja en estrecha colaboración con el equipo de Operaciones para garantizar la presentación precisa de la demostración del paquete de servicios que garantice una implementación y atención al cliente exitosas.

Habilidades y conocimientos
Ventas y negociación, comunicación efectiva, relaciones interpersonales, enfoque en el cliente, gestión del tiempo, análisis de datos, solución de problemas, tecnología y *Ciberseguridad*, habilidades de presentación.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.11 Descripción de puesto Especialista en *Ciberseguridad*

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Especialista en *Ciberseguridad*
Supervisado por:	Gerente General y de Operaciones
Jefe Inmediato:	Gerente General y de Operaciones
Personas a cargo:	Analista de *Ciberseguridad*

Objetivo del Cargo o Puesto de Laboral
Tiene como objetivo principal asegurar la integridad, confidencialidad y disponibilidad de los activos digitales de los clientes, así como prevenir, detectar y responder a amenazas cibernéticas, garantizando la *Ciberseguridad* y la infraestructura tecnológica.

Funciones Generales	
a)	**Análisis de Vulnerabilidades:** Identificar y evaluar posibles vulnerabilidades en sistemas, redes y aplicaciones, y recomendar medidas de mitigación.
b)	**Gestión de Requerimientos e *Ciberincidentes* clasificados como altos:** Gestionar requerimientos y *ciberincidentes*, clasificados como altos guiando a los analistas de *Ciberseguridad*.
c)	**Capacitación a Clientes:** Llevar a cabo la capacitación anual a clientes regulares y las 4 capacitaciones anuales para los clientes VIP.
d)	**Monitoreo Continuo:** Supervisar la elaboración de los reportes y validarlos previo a su envío a los clientes, y apoyo en la instalación inicial de los componentes de la solución.
e)	

	Investigación de Amenazas: Mantenerse actualizado sobre las últimas tendencias y amenazas en *Ciberseguridad* y adaptar las estrategias en consecuencia, así como elaborar el contenido de los boletines mensuales que se destinan a los clientes.

Relación con otros Departamentos
El Especialista en *Ciberseguridad* colabora con el resto del equipo de Operaciones, el equipo de Comercial y Marketing y cualquier otro departamento que maneje información y tecnología.

Habilidades y conocimientos
Gestión de herramientas de *Ciberseguridad*, redes y sistemas, resolución de problemas, análisis de datos, comunicación técnica, gestión de incidentes, ética y confidencialidad, conciencia de amenazas, y soporte en herramientas. Contar con la certificación ISO 27001 o LCSPC, o alguna especialización en *Ciberseguridad*.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 8.12 Descripción de puesto Analista de *Ciberseguridad*

Identificación del Cargo o Puesto de Laboral	
Nombre del puesto:	Analista en *Ciberseguridad*
Supervisado por:	Especialista en *Ciberseguridad*
Jefe Inmediato:	Especialista en *Ciberseguridad*
Personas a cargo:	-

Objetivo del Cargo o Puesto de Laboral
Tiene como objetivo principal ayudar a garantizar la continuidad del servicio, gestionar los requerimientos e incidentes reportados por el cliente y la infraestructura tecnológica de la empresa, identificando y abordando vulnerabilidades, amenazas y brechas de *Ciberseguridad*.

Funciones Generales	
a)	**Gestión de Requerimientos y *Ciberincidentes*:** Gestionar requerimientos y *ciberincidentes*, reportados o identificados bajo la guía del Especialista de *Ciberseguridad*.
b)	**Monitoreo de *Ciberseguridad*:** Supervisar los componentes del paquete de servicios en busca de actividades sospechosas o anómalas.
c)	**Análisis de Vulnerabilidades:** Identificar y evaluar vulnerabilidades en sistemas y aplicaciones, y proponer medidas de mitigación en el reporte mensual que valida el Especialista.
d)	**Configuración del Paquete de Servicios de *Ciberseguridad*:** Configurar y administrar los componentes del paquete para que pueda funcionar correctamente en los *endpoints* del cliente.
e)	**Presentación de la Demostración:** Preparar la demostración para los clientes bajo la guía del Especialista apoyando al *KEY ACCOUNT MANAGER* en las presentaciones de la demostración.

Relación con otros Departamentos

El Analista en *Ciberseguridad* colabora con el equipo de TI, el equipo de Operaciones, el equipo de Comercial y Marketing y cualquier otro departamento que maneje tecnología y datos sensibles.
Habilidades y conocimientos
Conocimientos en *Ciberseguridad*, conocimiento en gestión de herramientas de *Ciberseguridad*, gestión de entorno *cloud*, redes y sistemas, análisis de datos, resolución de problemas, análisis de datos, comunicación técnica, gestión de *ciberincidentes*, ética, conciencia de amenazas.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

8.4.2. Socios y Capital

Se define en el estatuto de constitución societaria, los socios que integran esta sociedad son los 4 autores del presente plan de negocios.

De igual manera, según se definirá en el estatuto de constitución societaria, el capital social es de **S/ 201,018.00,** dividido en 4 acciones nominativas de un nominal de **S/ 50,225.00** cada una.

8.4.3. Obligaciones Fiscales

Como parte del marco regulatorio que rige a todas las empresas que quieran desarrollar sus actividades comerciales en el país, se debe considerar los requisitos tributarios y contables.

El marco regulatorio actual clasifica a las empresas en base a la cantidad de empleados y en base a los ingresos anuales o ventas en UIT (Unidad de Impuestos), por año, las mismas que se clasifican de la siguiente manera:

Tabla 8.13 Características de los tipos de empresas

Tamaño de la empresa	Cantidad de colaboradores	UIT
Microempresas	2 a 9 empleados	Hasta 150
Empresa pequeña	10 a 49 empleados	Más de 150 hasta 1700
Empresa mediana	50 a 199 empleados	Más de 1700 hasta 2300
Empresa grande	200 a más empleados	Más de 2300

Fuente: Autores de esta tesis.

Elaboración: Autores de esta tesis

En ese sentido, *CyberWave* será registrada en el Registro de Personas Jurídicas de la SUNARP, bajo el régimen de pyme, dado que contará con más de 9 empleados y facturará más de 500 Unidades Impositivas Tributarias por año.

Las obligaciones a las que están sujetas las pymes son las siguientes:

Tabla 8.14 Obligaciones tributarias según pyme

OBLIGACIÓN	PORCENTAJE
IMPUESTO GENERAL A LAS VENTAS (IGV)	18%
IMPUESTO A LA RENTA (IR)	29.5%

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

8.5. Gestión de Recursos Humanos

Ahora que ya se definió los criterios organizacionales para la propuesta en el punto anterior, y el organigrama junto con los perfiles profesionales, es turno de definir los criterios de gestión para los recursos humanos.

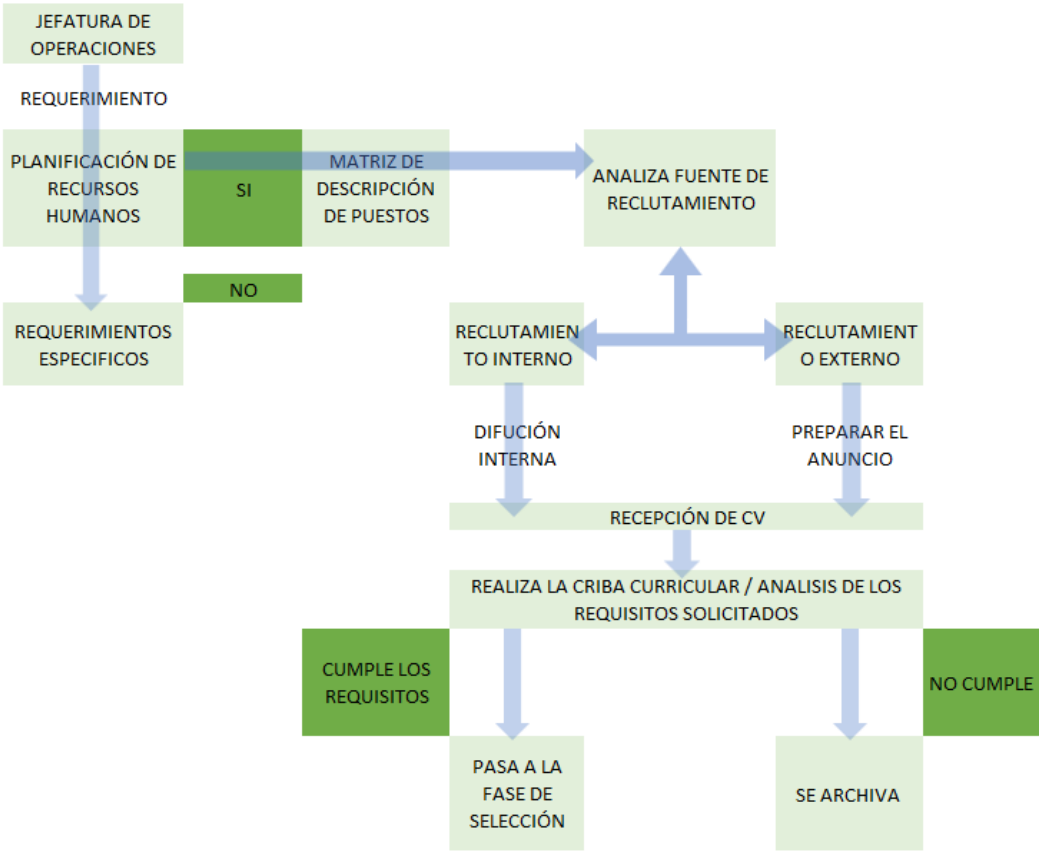
8.5.1. Reclutamiento y selección

Considerando la complejidad y especialización de los puestos requeridos para cada uno de los roles necesarios se definirán los criterios de reclutamiento y selección.

El proceso estará a cargo del área de recursos humanos en coordinación con Gerente General y de Operaciones. Se aplicará una estrategia de reclutamiento Net-hunter que aplicará el Analista de Recursos Humanos para ubicar talentos a través de bolsas de trabajo masivos como CompuTrabajo, Laborum, LinkedIn etc. las que permiten ser gestionadas personalmente. Para los puestos más especializados se podría considerar un reclutador externo o head-hunter evaluando le especialización y certificaciones requeridas para cada puesto.

El flujograma de reclutamiento será el siguiente:

Ilustración 8.1 Flujograma de la fase de Reclutamiento



Fuente: Jáuregui, 2022.
Elaboración: Autores de esta tesis

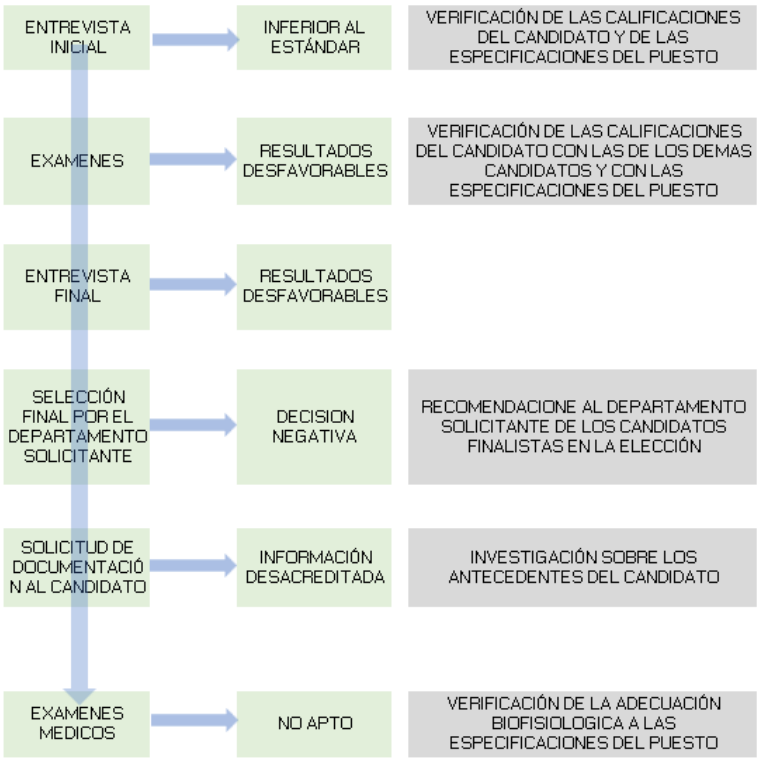
De manera exploratoria, se introducirá el uso de IA, con aplicaciones como Textio para describir de mejor manera los puestos con datos más tangibles. Este programa puede analizar todas las ofertas con los datos de retroalimentación sobre quien aplica y utilizar palabras claves que atraen mejor al talento, y de esta manera automatizar un poco el flujo de trabajo para apoyar al Analista de Recursos Humanos.

De igual manera, y también aplicando IA, se incluirá el reclutamiento predictivo al proceso de reclutamiento de los puestos de Especialista y Head, que a través de algoritmos recogen información y pueden definir cuál de los candidatos es el mejor para el puesto. De esta manera, se podrá reducir con mayor facilidad y precisión la lista de candidatos apoyando al Analista de Recursos Humanos.

Se iniciará la fase de reclutamiento con la llamada inicial para cotejar datos básicos y coordinar la primera entrevista. Tras la entrevista inicial, que verificará que el candidato cumpla con las especificaciones del puesto, se descartarán aquellos perfiles que tengan bajo estándar para el puesto solicitado. A continuación, se aplicarán las pruebas psicométricas y de razonamiento lógico y verbal a los candidatos restantes. Luego, se descartarán los perfiles que no hayan pasado las pruebas y se procederá a la entrevista final con la terna de los 3 finalistas.

Para la fase de selección se seguirá con una entrevista final que valide el conocimiento técnico específico en *ciberseguridad* y la resolución de un caso práctico, liderado por el Gerente General y de Operaciones y el Head de Recursos Humanos. La selección final será realizada por el Head que solicitó el perfil. Se solicitará al candidato seleccionado la documentación necesaria para efectuar la respectiva validación de antecedentes. En caso no se encuentre una tacha, se coordinará el examen médico correspondiente. Se seguirá el siguiente flujograma de procesos:

Ilustración 8.2 Flujograma de la fase de selección



Fuente: Jáuregui, 2022
Elaboración: Autores de esta tesis

Se considerará los siguientes plazos máximos para cubrir las vacantes:

Tabla 8.15 Plazos máximos para cubrir vacantes

PUESTO	TIEMPO MAXIMO
GERENCIA GENERAL	50 DIAS
EJECUTIVOS	45 DIAS
MANDOS MEDIOS	30 DIAS
EMPLEADOS	25 DIAS
OBREROS	15 DIAS

Fuente: *Benchmarking* de gestión de Recursos Humanos PWC (2021)
Elaboración: Autores de esta tesis

8.5.2. Capacitación y desarrollo

El siguiente ámbito de capacitaciones y desarrollo de los colaboradores será definido a través de las cuatro fases del plan de capacitaciones:

Fase 1: Evaluación de las necesidades de la empresa.

- Análisis de la empresa
- Análisis de las tareas
- Análisis de las personas

Fase 2: Diseño del plan de capacitaciones

- Objetivo de las capacitaciones
- Disponibilidad de los colaboradores
- Principios de aprendizaje
- Método en el puesto de trabajo
- Método fuera del puesto de trabajo
- Desarrollo Gerencial

Fase 3: Implementación

- Plan de capacitaciones anual según planilla de desempeño

Fase 4: Evaluación

- Reacciones
- Aprendizaje
- Comportamiento (transferencia)
- Resultado

Se utilizarán los siguientes indicadores de rendimiento para medir la efectividad de las capacitaciones aplicadas:

- Porcentaje de la planilla gastado en capacitaciones = (Monto gastado en capacitación/total de la nómina)
- Dinero de capacitación invertido por empleado = (Monto total de la capacitación/total de empleados capacitados)
- Promedio de horas de capacitación por colaborador = (número de horas de capacitación (horas*personas) /total de colaboradores capacitados)
- % de colaboradores capacitados por año = Total de empleados capacitados / total de empleados
- Costo de capacitación por hora por alumno = Costo total de capacitaciones / número total de horas de capacitación)
- Inversión en formación en relación con compensación = Gastos de capacitación y desarrollo / total de competencia / total de empleados claves * 100

8.5.3. Remuneraciones y Presupuesto

La estrategia principal para la definición de las remuneraciones estará fundamentada en la cultura de la empresa, respetando los principios de esta y teniendo siempre presente los valores, misión y visión.

Se planteará una estrategia de recompensa total, donde se considere no solo la remuneración monetaria sino un enfoque en el bienestar integral de los colaboradores, considerando también las denominadas compensaciones emocionales (PWC, 2021).

Para el proceso de administración de las remuneraciones se tendrá en cuenta el análisis del presupuesto, que se iniciará valorizando los puestos y considerará encuestas salariales, de modo tal que permitan definir la estructura salarial, incluyendo políticas

de pago que debe tomar en cuenta una consistencia interna para evitar las desigualdades. El pago será individual y se modificará según la evaluación de desempeño.

El presupuesto de Recursos Humanos se estructurará de la siguiente manera:

Tabla 8.16 Presupuesto de Recursos Humanos

PRESUPUESTO RRHH					
PLANILLA					
CONCEPTO	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Gerente general y de Operaciones	S/ 100,000	S/ 100,000	S/ 100,000	S/ 100,000	S/ 100,000
Head comercial	S/ 86,667	S/ 86,667	S/ 86,667	S/ 86,667	S/ 86,667
Head administración y finanzas	S/ 88,033	S/ 88,033	S/ 88,033	S/ 88,033	S/ 88,033
Head de Recursos Humanos	S/ 86,667	S/ 86,667	S/ 86,667	S/ 86,667	S/ 86,667
Analista de Recursos Humanos	S/ 40,000	S/ 40,000	S/ 40,000	S/ 40,000	S/ 40,000
Ejecutivo de ventas / *Key Account MGR*	S/ 86,111	S/ 166,667	S/ 166,667	S/ 166,667	S/ 166,667
Especialista *Ciberseguridad*	S/ 160,000	S/ 240,000	S/ 240,000	S/ 246,667	S/ 320,000
Analista de *Ciberseguridad*	S/ 160,000	S/ 266,667	S/ 266,667	S/ 271,111	S/ 320,000
Horas extra	S/ 21,628	S/ 961	S/ 0	S/ 4,196	S/ 0
Total compensaciones y beneficios	**S/ 829,105**	**S/ 1,075,661**	**S/ 1,074,700**	**S/ 1,090,007**	**S/ 1,208,033**
SERVICIOS ADMINISTRATIVOS					
Contabilidad	S/ 4,100	S/ 5,800	S/ 7,000	S/ 7,000	S/ 7,400
Servicios tercerizados de tecnología	S/ 30,000	S/ 31,500	S/ 33,075	S/ 34,729	S/ 36,465
Servicios legales abogado laboralista	S/ 42,000	S/ 44,100	S/ 46,305	S/ 48,620	S/ 51,051
Tefacturo Plan Empredor	S/ 948	S/ 995	S/ 1,045	S/ 1,097	S/ 1,152
Total servicios administrativos	**S/ 77,048**	**S/ 82,395**	**S/ 87,425**	**S/ 91,446**	**S/ 96,069**
GESTIÓN DEL TALENTO					
CONCEPTO	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Capacitaciones	S/ 42,000	S/ 44,100	S/ 46,305	S/ 48,620	S/ 51,051
Evaluación de desempeño	S/ 47,700	S/ 137,025	S/ 174,150	S/ 174,150	S/ 186,075
Plan de carrera	S/ 42,000	S/ 44,100	S/ 46,305	S/ 48,620	S/ 51,051
Total Gestión De Talento	**S/ 131,700**	**S/ 225,225**	**S/ 266,760**	**S/ 271,391**	**S/ 288,178**
RECLUTAMIENTO Y CONTRATACIÓN					
CONCEPTO	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Plataformas web de reclutamiento	S/ 600	S/ 630	S/ 662	S/ 695	S/ 729
Exámenes psicométricos	S/ 2,400	S/ 2,520	S/ 2,646	S/ 2,778	S/ 2,917
Verificación de antecedentes	S/ 600	S/ 630	S/ 662	S/ 695	S/ 729
Total reclutamiento y contratación	**S/ 3,600**	**S/ 3,780**	**S/ 3,969**	**S/ 4,167**	**S/ 4,376**
SEGURIDAD Y BIENESTAR					
CONCEPTO	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Cumplimiento normativo (Salud y Seguridad en el Trabajo)	S/ 10,800	S/ 11,340	S/ 11,907	S/ 12,502	S/ 13,127
Actividades recreativas	S/ 2,400	S/ 2,520	S/ 2,646	S/ 2,778	S/ 2,917
Coworking	S/ 37,750	S/ 56,700	S/ 59,535	S/ 63,091	S/ 72,930
Total seguridad y bienestar	**S/ 50,950**	**S/ 70,560**	**S/ 74,088**	**S/ 78,371**	**S/ 88,975**
Contingencias	**S/ 32,772**	**S/ 43,729**	**S/ 45,208**	**S/ 46,061**	**S/ 50,569**
TOTAL POR AÑO	**S/ 1,125,175**	**S/ 1,501,350**	**S/ 1,552,150**	**S/ 1,581,444**	**S/ 1,736,199**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

El total del sueldo por rol estará conformado por los siguientes conceptos:

- ESSALUD O EPS
- Seguro vida ley
- Gratificación anual
- Bonificación extraordinaria tras los resultados de la evaluación de desempeño
- Vacaciones anuales (15 días al año)
- CTS mensual
- Asignación familiar en caso aplique (10% de la remuneración mínima vital)

8.6. Conclusión del capítulo

En este apartado, se ha determinado la estructura organizacional que tendrá *CyberWave* no solo a nivel de talento humano sino también de los recursos que se requerirán para la operación, tales como activos tangibles como espacios de trabajo y algunas consideraciones que se enfocan en el desarrollo del colaborador, como el plan de carrera y las evaluaciones de desempeño.

CAPITULO 9 . PLAN ECONÓMICO Y FINANCIERO

En este capítulo se buscará detallar las proyecciones financieras, los recursos necesarios y la estrategia para administrar los aspectos económicos de *CyberWave* tomando de referencia todos los planes anteriormente desarrollados para ofrecer la solución del modelo de negocio propuesto.

Por otro lado, se buscará definir si el plan de negocios es rentable o no financieramente. Para ello se desarrollará el flujo de caja económico, el análisis de sensibilidad y análisis de riesgos que permita evaluar, justificar y sustentar la viabilidad de la propuesta.

9.1. Supuestos y Consideraciones

Para el análisis financiero del presente capitulo se han determinado algunos supuestos, así como también se consideraron algunos valores reales que se han consolidado en la siguiente tabla de parámetros:

Tabla 9.1 Relación de supuestos y parámetros

ASPECTO	INDICADOR	VALOR
Genérico	% inflación	5%
Genérico	Tipo de cambio spot	3.70
Genérico	% IGV	18%
Genérico	% contingencia	3%
Demanda	% suplemento de horas	15%
Demanda	% deserción	25%
Demanda	% personas interesadas en servicios adicionales de horas	65%
Demanda	% clientes con la necesidad del servicio	80%
Producción	% considerado de horas extra	135%
Producción	% clientes que contratarían servicios adicionales	52%
Organizacional	Remuneración mínima vital (*rmv*)	S/ 1,025
Organizacional	Bonificación anual	1.5
Organizacional	% máx. aumento sueldo anual	15%
Ventas	Precio paquete 1 (sin igv.)	S/ 2,373
Ventas	Precio adicional 15 horas + 20 licencias (sin igv.)	S/ 1,000
Ventas	Precio adicional *cloud* (igv.)	S/ 1,000
Ventas	% crecimiento precios de venta año 2	5.0%
Ventas	% crecimiento precios de venta año 3	5.0%
Ventas	% crecimiento precios de venta año 4	5.0%
Ventas	% crecimiento precios de venta año 5	5.0%

Operaciones	% producción adicional espacio en *cloud*	30%
Operaciones	Precio unitario alquiler de equipo informático (laptop) ope.	$69
Operaciones	Precio unitario alquiler de equipo informático (laptop) administ.	$53
Marketing	% comisión de ventas	5.0%
Marketing	% renovación de servicio	75%
Marketing	% descuento vip	3.5%
Marketing	% descuentos referidos	2.5%
Marketing	% descuento retención	2.5%
Marketing	% clientes que refieren	30%
Estado de resultados	Unidad impositiva tributaria (UIT) - 2023	S/ 4,950
Estado de resultados	Impuesto a la renta menor a 15 UIT	10.0%
Estado de resultados	Impuesto a la renta mayor a 15 UIT	29.5%
Estado de resultados	Variación promedio de UIT	S/ 300
Estado de resultados	Devaluación soles	2%

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

9.2. Proyección de la Demanda

Según Kotler, el marketing busca influenciar la demanda, haciendo que el producto o servicio resulte atractivo, esté disponible y sea accesible. Sin embargo, no altera las necesidades, ya que están existen antes de la demanda (Melara, 2020)

De esta manera se definen tres atributos que se utilizarán para proyectar la demanda del presente plan de negocios: la necesidad, el deseo y la demanda.

- Se define como aspiración que durante el primer año se obtenga una cuota aproximada de mercado del 3.5% que equivale a 80 pymes del sector construcción e inmobiliaria. Este valor se estableció a partir de la lógica de un *funnel* de conversión que considera como último factor una estimación extrapolada de la demanda a partir de un cruce de fuentes secundarias y primarias utilizadas en el plan de negocios.

Tabla 9.2 Cálculo de la demanda para pymes del sector construcción

CÁLCULO DE LA DEMANDA				
***Funnel* de Demanda**	**%**	**Cálculo**	**Detalle**	**Fuente**
Población obj.(finita)	100%	3,995	Total de la población de pymes del sector construcción (97.51% son pequeñas empresas)	INEI
Necesidad	80%	3,196	Pymes que sufrieron ciberataques	Sondeo inicial pymes

Deseo	98%	3,132	Pymes dispuestas a tomar el servicio	Encuesta
Demanda	73%	2,286	Pymes que pagarían 2000 a 2600 al mes	Encuesta
Cuota de Mercado	3.5%	80	Supuesto / aspiración	

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- Se tienen como supuestos de proyección de demanda:
  - Año 2: Crecimiento atribuido a la novedad de la propuesta, por lo que se estima un incremento del 25%.
  - Año 3: Probabilidad de que se pueda a imitar la solución por lo que se estima competencia que afecte la intención de un mayor crecimiento, para ese año se mantiene el 20%.
  - Año 4: Se determina que es un buen momento de diversificar y ampliar el mercado hacia otros sectores relevantes, se estima un crecimiento del 40%.
  - Año 5: Se estima el crecimiento conservador del 25%.

Tabla 9.3 Estimación de la demanda ampliación de segmento

CALCULO DE LA DEMANDA				
***Funnel* de Demanda**	**%**	**Cálculo**	**Detalle**	**Fuente**
Población obj.(finita)	100%	61,926	Total, de la población de pymes	INEI
Necesidad	80%	49,541	Pymes que sufrieron ciberataques	Sondeo inicial pymes
Deseo	98%	48,550	Pymes dispuestas a tomar el servicio	Encuesta
Demanda	73%	35,442	Pymes que pagarían 2000 a 2600 al mes	Encuesta

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Tabla 9.4 Proyección de la demanda

Consideraciones	**SECTOR CONSTRUCCION**			**TODOS SECTORES**	
	AÑO 1	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Crecimiento de Demanda		25%	20%	40%	25%
Demanda cada año	80	100	120	168	210
Incremento		20	20	48	42
Deserción		20	25	30	42
Total clientes	**80**	**100**	**115**	**186**	**210**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

9.3. Inversión y capital de trabajo

Para el cálculo de la inversión necesaria y aporte de capital para el inicio de las operaciones, se consolidó el presupuesto preoperativo y la campaña de lanzamiento.

- **Presupuesto Preoperativo:** Considera costos de constitución, seguridad y bienestar, reclutamiento y gestión de personal. (Plazo estimado: 3 meses)

Tabla 9.5 Presupuesto preoperativo

PREOPERATIVO	AÑO 0	DETALLE
Registro como persona jurídica	S/ 1,000	Presentar documentos ante SUNARP, para establecer legalmente a la entidad, permitiéndole operar, firmar contratos y adquirir derechos
Derechos y patentes registral	S/ 30	Costo de Registros ante INDECOPI, para brindar protección legal sobre invenciones, diseños o marcas, asegurando exclusividad en el uso y comercialización.
Gastos notariales	S/ 400	Pago de honorarios notariales por la elaboración y revisión de escrituras y documentos legales.
Total constitución	**S/ 1,430**	
Cumplimiento normativo (SST)	S/ 2,700	Capacitación para empleados, adquisición de equipos de protección personal, evaluaciones de riesgos, exámenes médicos ocupacionales y otros costos relacionados.
Coworking	S/ 5,250	Costo del espacio de coworking para acceder y utilizar sus instalaciones compartidas, como escritorios, salas de reuniones y áreas comunes.
Total seguridad y bienestar	**S/ 7,950**	
Plataformas web de reclutamiento	S/ 150	Uso de Plataformas líderes tales como *Linkedin*, *Bumeran*, *Laborum*, *Computrabajo*.
Servicio de reclutamiento y selección	S/ 13,889	Contratación de un tercero para los procesos de reclutamiento y selección del personal para la empresa
Exámenes psicométricos	S/ 600	exámenes para contratación
Verificación de antecedentes	S/ 150	Validación de personal a contratar
Capacitaciones	S/ 3,600	Entrenamiento básico para eventos previos de lanzamiento
Servicios legales abogado laboralista	S/ 15,000	Asesoría en pagos a colaboradores y elaboración de contratos para operación
Compensaciones preoperativas	S/ 42,892	Pago por concepto de personal en actividades preoperativas
Total reclutamiento y gestión de personal	**S/ 76,281**	
certificación de ISO 22301	S/ 30,000	Proceso de certificación de ISO 27001 para la empresa
Certificación de ISO 22301	S/ 30,000	Proceso de certificación de ISO 22301 para la empresa
Costo anual del *partnership* con *Bitdefender*	S/ 5,000	Pago anual para ser miembro del programa de *partnership* con *Bitdefender*
Total certificaciones y partnership	**S/ 65,000**	
Total inversión preoperativa	**S/ 150,661**	

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- **Presupuesto para plan de lanzamiento:** Este incluye los costos por la asesoría de la agencia de marketing, así como el evento de lanzamiento, desarrollo de marca y todos los esfuerzos necesarios para iniciar el primer mes de operaciones con ventas. La duración de la campaña será de 3 meses y forma parte de la estrategia de posicionamiento de la marca desarrollada en el plan de marketing.

Tabla 9.6 Presupuesto de plan lanzamiento Marketing

PLAN DE LANZAMIENTO	AÑO 0	DETALLE
Registro de marca	S/ 54	Registro de la marca con INDECOPI
Notas de prensa	S/ 1,667	Publicaciones en medios de publicidad tradicionales
Evento de lanzamiento	S/ 25,000	Incluye el alquiler de local, catering, búsqueda e invitación a representantes de pymes.
Imágenes corporativas	S/ 333	Material gráfico corporativo
Agencia de marketing	S/ 12,000	Pago a la agencia para diseño y despliegue de campaña de lanzamiento
Publicidad especial de lanzamiento en redes	S/ 3,000	Diseños y publicaciones en redes sociales, pautas, publicaciones, etc.
Copywriting	S/ 1,600	Patentar la marca para evitar copias
Desarrollo de página web	S/ 3,000	Desarrollo de la página web en *stagging,* pruebas y pase a producción dentro del entorno Azure
Certificado SSL	S/ 204	Certificado digital que verifica la identidad de la página web y permite habilitar una conexión cifrada
Servicios legales	S/ 500	Pago a abogados por asesoría en contratos y/o pagos asociados a la campaña
Influencer	S/ 3,000	Pago a figura pública para que promocione la marca en *reels* u otro medio
Plan de Lanzamiento MKT	**S/ 50,358**	

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

La suma del presupuesto de lanzamiento y el presupuesto preoperativo estimado para un periodo de 3 meses y previo a las operaciones oficiales para el ingreso en el mercado es de S/ 201,018.00 incluyendo IGV (doscientos un mil dieciocho y 00/100 nuevos soles incluido el impuesto general a las ventas).

Por otro lado, para estimar del capital de trabajo se utilizó el modelo de desfase, donde se contabiliza la duración del negocio al momento de adquirir y distribuir la

solución. En este caso, el valor será de 15 días lo cual al momento de anualizar el cálculo se determina como un factor de 24 meses que asciende a los S/ 81,277 en el año 0.

De esta manera, al realizar la adición de conceptos se determina el aporte de capital total que deberá asumir cada socio, mismo que se encuentra detallado en el capítulo del Plan Organizacional.

9.4. Proyección de Ingresos

Dada la demanda estimada para los cinco años del ejercicio se han proyectado ingresos bajo el concepto de venta directa por suscripciones mensuales del paquete de la solución de *ciberseguridad* que ascienden a casi 1 millón de soles. Adicionalmente, se está considerando un incremento anual del precio por efectos de la inflación de 5%.

Por otro lado, se está asumiendo el supuesto probabilístico de que algunos de los usuarios demanden servicios adicionales al paquete ya contratado. Estos servicios adicionales se han separado en una bolsa de 10 horas más 20 licencias, mientras que el otro paquete consiste en mayor capacidad de almacenamiento, 5TB, así como 20 licencias más. Ambos planes se adquieren a 1000 soles cada uno. El supuesto detrás del paquete adicional de horas se construyó con la información de la encuesta, donde se tenía una pregunta asociada a la intención de adquirir algún servicio extra al ya definido.

Tabla 9.7 Ingresos proyectados

CONCEPTO	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Demanda acumulada	**80**	**78**	**71**	**85**	**81**
Paquete *Cyber Plus* (sin IGV)	S/ 2,373	S/ 2,492	S/ 2,616	S/ 2,747	S/ 2,884
Paquete *Support Plus*: horas + licencias	S/ 1,000	S/ 1,050	S/ 1,103	S/ 1,158	S/ 1,216
Paquete *Backup Plus*: *cloud* + licencias	S/ 1,000	S/ 1,050	S/ 1,103	S/ 1,158	S/ 1,216
Ventas (clientes nuevos)	S/ 1,433,600	S/ 2,404,920	S/ 2,265,858	S/ 2,450,461	S/ 2,532,143
Paquete *Support Plus*: horas + licencias	S/ 314,163	S/ 527,021	S/ 496,547	S/ 537,001	S/ 554,901
Paquete *Backup Plus*: *cloud* + licencias	S/ 181,248	S/ 304,051	S/ 286,469	S/ 309,808	S/ 320,135
Ventas Totales	**S/ 1,929,011**	**S/ 3,235,992**	**S/ 3,048,874**	**S/ 3,297,270**	**S/ 3,407,179**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

9.5. Costos y Gastos

En este punto se detallarán los costos que se asumirán durante los primeros 5 años de desarrollo del presente plan de negocios considerando los presupuestos asociados a los planes que se desarrollaron en los capítulos anteriores.

Estos incluyen los gastos operativos, gastos de personal, gastos de ventas, gastos de marketing y gastos administrativos. Los mismos que se agrupan en la siguiente tabla:

Tabla 9.8 Proyección de gastos

	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Gastos operativos	S/ 628,129	S/ 997,415	S/ 928,070	S/ 967,794	S/ 986,995
Gastos de personal	S/ 742,994	S/ 908,994	S/ 908,033	S/ 923,340	S/ 1,041,367
Gastos de ventas	S/ 100,271	S/ 177,743	S/ 177,134	S/ 178,355	S/ 178,665
Gastos de marketing	S/ 183,180	S/ 228,321	S/ 261,265	S/ 268,341	S/ 283,257
Gastos administrativos	S/ 296,070	S/ 425,689	S/ 477,450	S/ 491,437	S/ 528,166
Total de gastos	**S/ 1,950,644**	**S/ 2,738,162**	**S/ 2,751,954**	**S/ 2,829,267**	**S/ 3,018,450**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- **Gastos operativos:** Se consideran los gastos variables, aquellos que se generan producto de los paquetes a ofrecer a los clientes, y los gastos fijos, aquellos que serán recurrentes para garantizar la operación como licencias, infraestructura *Cloud*, alquiler de computadoras, el costo anual del socio estratégico, el costo de las licencias y certificaciones y la plataforma para facturas digitales.

- **Gastos de personal:** Se consideran en este apartado, todos aquellos gastos asociados al personal menos el ejecutivo de ventas / *Key Account Manager (KEY ACCOUNT MANAGER)* que se considera como gasto de ventas junto con las comisiones asociadas a este personal. Se consideran todas las prestaciones de ley, una bonificación anual y un porcentaje de aumento de sueldo anual como parte de la evaluación de rendimiento del personal que no supere el 1.5 sueldo. El porcentaje máximo de aumento de sueldo anual será del 15%.

Tabla 9.9 Remuneraciones y compensaciones

CONCEPTO	BASICO	TOTAL 1
Gerente General y de Operaciones	S/ 7,500	S/ 8,333
Head Comercial	S/ 6,500	S/ 7,222
Head Administración y Finanzas	S/ 6,500	S/ 7,336
Head de Recursos Humanos	S/ 6,500	S/ 7,222
Analista de Recursos Humanos	S/ 3,000	S/ 3,333
Especialista *Ciberseguridad*	S/ 6,000	S/ 6,667
Analista de *Ciberseguridad*	S/ 4,000	S/ 4,444
Total compensaciones y beneficios	**S/ 42,500**	**S/ 47,336**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

- **Gastos de ventas:** En este punto se consideran como los sueldos de los vendedores y sus comisiones por ventas que serán el 5% del valor más alto de ventas en el trimestre. Se considera el inicio de las actividades con 1 solo vendedor, cantidad que se irá incrementando con el paso de los meses.

- **Gastos de marketing:** Se encuentran detallados en el presupuesto de marketing, este presupuesto incluye todas las estrategias que se tomaran para el posicionamiento de la marca, entre los cuales se encuentran la creación de la marca, los programas de concientización, presupuesto para relaciones públicas y eventos, estrategias de diferenciación, fidelización y retención. Se considera un porcentaje de descuento como parte de las estrategias de fidelización para clientes VIP, descuentos para referidos, descuento por retención.

- **Gastos administrativos:** Comprenden todos los gastos asociados al personal descontando sus remuneraciones. Gastos asociados a la seguridad y bienestar, reclutamiento y contratación, gestión del talento, y los servicios administrativos contratados con terceros para poder operar tales como contabilidad, servicios legales etc.

9.6. Amortizaciones

Dado que no se cuenta con activos que estén afectos a la depreciación, se considera en este punto las amortizaciones que se harán por las inversiones. En este sentido corresponde efectuarla sobre la inversión inicial, misma que será amortizada en el

primer año de operaciones tal y como lo indica la Ley del Impuesto a la Renta que señala que la deducción de los gastos preoperativos, a opción del contribuyente, debe realizarse en el primer ejercicio o amortizarse en el plazo máximo de diez años.

Tabla 9.10 Proyección de amortizaciones

	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Amortización	S/ 282,295				

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

9.7. Financiamiento

La presente propuesta no contempla la solicitud de financiamiento de un tercero o entidad bancaria, inicialmente será totalmente financiado por el aporte de los accionistas, los mismos que aportaran el 25% cada uno, respectivamente.

9.8. Balance General Proyectado

El balance general es una representación financiera que consolida los activos, pasivos y el patrimonio de la empresa que se constituirá. De esta manera, se presenta el siguiente balance:

Tabla 9.11 Balance General Proyectado

	Al 31 Dic Año 0	Al 31 Dic Año 1	Al 31 Dic Año 2	Al 31 Dic Año 3	Al 31 Dic Año 4
Activo	**S/ 282,295**	**S/ 114,090**	**S/ 114,665**	**S/ 117,886**	**S/ 125,769**
Pasivo	0	S/ 54,446	0	0	0
Patrimonio	S/ 282,295	S/ 59,644	S/ 114,665	S/ 117,886	S/ 125,769
Pasivo y Patrimonio	**S/ 282,295**	**S/ 114,090**	**S/ 114,665**	**S/ 117,886**	**S/ 125,769**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

La empresa presenta como activos al capital de trabajo y considera el pasivo que representa el préstamo de los accionistas por el primer año de operaciones.

9.9. Estado de Resultados

El estado de resultados consolida todos los conceptos de ingresos y egresos y los modela en un horizonte de cinco años. Se puede distinguir que el primer año no presenta ganancias y acumula pérdidas arrastrables hasta el segundo año y dado que se tributará

bajo el régimen MYPE se tienen pagos de impuesto a la renta a partir del tercer año y se cierran con utilidades netas cercanas al millón de soles en el último año del ejercicio.

Tabla 9.12 Estado de resultados

	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Ventas	S/ 1,929,011	S/ 3,235,992	S/ 3,048,874	S/ 3,297,270	S/ 3,407,179
Gastos operativos	S/ 628,129	S/ 997,415	S/ 928,070	S/ 967,794	S/ 986,995
Gastos de personal	S/ 742,994	S/ 908,994	S/ 908,033	S/ 923,340	S/ 1,041,367
Gastos de ventas	S/ 100,271	S/ 177,743	S/ 177,134	S/ 178,355	S/ 178,665
Gastos de marketing	S/ 183,180	S/ 228,321	S/ 261,265	S/ 268,341	S/ 283,257
Gastos Administrativos	S/ 296,070	S/ 425,689	S/ 477,450	S/ 491,437	S/ 528,166
Amortización	S/ 282,295				
Utilidad operativa	**-S/ 303,928**	**S/ 497,829**	**S/ 296,920**	**S/ 468,002**	**S/ 388,728**
Pérdidas acumuladas	-S/ 303,928	S/ 0	S/ 0	S/ 0	S/ 0
Utilidad impositiva	S/ 0	S/ 193,901	S/ 296,920	S/ 468,002	S/ 388,728
Impuesto a la renta	S/ 0	S/ 40,967	S/ 70,480	S/ 120,072	S/ 95,809
Utilidad neta	**-S/ 303,928**	**S/ 456,862**	**S/ 226,440**	**S/ 347,930**	**S/ 292,920**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

9.10. Flujo de Caja Económico

El flujo económico es una consecuencia del estado de resultados desarrollado en el subcapítulo anterior, donde se han ordenado los principales conceptos de entrada (ingresos) y su contraparte de principales egresos, así como la inversión previamente descrita que considera el plan de lanzamiento y costos incurridos por la preparación.

Tabla 9.13 Flujo de caja económico

	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Ingresos		S/ 1,929,011	S/ 3,235,992	S/ 3,048,874	S/ 3,297,270	S/ 3,407,179
Gastos operativos		-S/ 628,129	-S/ 997,415	-S/ 928,070	-S/ 967,794	-S/ 986,995
Gastos personal		-S/ 742,994	-S/ 908,994	-S/ 908,033	-S/ 923,340	-S/ 1,041,367
Gastos de ventas		-S/ 100,271	-S/ 177,743	-S/ 177,134	-S/ 178,355	-S/ 178,665
Gastos marketing		-S/ 183,180	-S/ 228,321	-S/ 261,265	-S/ 268,341	-S/ 283,257
Gastos administ.		-S/ 296,070	-S/ 425,689	-S/ 477,450	-S/ 491,437	-S/ 528,166
Amortización		-S/ 282,295	S/ 0	S/ 0	S/ 0	S/ 0
Utilidad antes de impuestos		**-S/ 303,928**	**S/ 497,829**	**S/ 296,920**	**S/ 468,002**	**S/ 388,728**
Impuestos		S/ 0	-S/ 40,967	-S/ 70,480	-S/ 120,072	-S/ 95,809
Amortización		S/ 282,295	S/ 0	S/ 0	S/ 0	S/ 0
Flujo operativo		**-S/ 21,633**	**S/ 456,862**	**S/ 226,440**	**S/ 347,930**	**S/ 292,920**
Capital de trabajo	-S/ 81,277	-S/ 32,813	-S/ 575	-S/ 3,221	-S/ 7,883	S/ 125,769
Conceptos preop.	-S/ 150,661					
Plan lanzamiento	-S/ 50,358					

Flujo de caja de inversiones	**-S/ 282,295**	**-S/ 32,813**	**-S/ 575**	**-S/ 3,221**	**-S/ 7,883**	**S/ 125,769**
Flujo de caja económico	**-S/ 282,295**	**-S/ 54,446**	**S/ 456,288**	**S/ 223,219**	**S/ 340,048**	**S/ 418,689**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Ahora que se cuenta con el desagregado de conceptos de las salidas y entradas del flujo económico, se puede apreciar un periodo inicial de pérdida, el cual se cubrirá con un aporte o préstamo de los accionistas a cobrar en con las utilidades de los siguientes años. Por otro lado, los años siguientes presentan una tendencia positiva de crecimiento, por lo que se procederá a realizar un análisis de rentabilidad fundamentado en calcular el VAN y TIR del proyecto. No obstante, como paso previo se debe determinar cuál será la tasa de descuento involucrada.

9.11. Tasa de descuento

Para este ejercicio, como accionistas se decidió considerar una tasa de descuento promedio esperada del 20%. Sin embargo, para ver si la tasa seleccionada se encontraba alineada con el estándar matemático se realizó el ejercicio del costo medio ponderado de capital o *WACC (weighted average cost of capital)*, donde el resultado fue de 18%, lo cual indica que la tasa de 20% es adecuada.

9.12. Análisis de Rentabilidad

Una vez que se ha determinado la tasa de descuento, se calculan los indicadores del VAN y TIR en un horizonte de 5 años que considera un periodo inicial, al que se le ha nombrado año 0. Vale mencionar que ambos indicadores son los más usados al momento de evaluar la rentabilidad de un proyecto por lo cual su cálculo permitirá determinar el punto con el cual se puede modelar posteriores escenarios.

Tabla 9.14 Cálculo de rentabilidad

TIR (Tasa interna de retorno)	**62%**
VAN (Valor actual neto)	**S/ 450,628**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Después del cálculo se tiene una tasa interna de retorno de 62% que está por encima de la tasa de descuento del 20%, así como se tienen un VAN de S/ 450,628 que permita que se concluya con que el proyecto es viable.

9.13. Análisis de Escenarios

Dada la volatilidad que presentan siempre los proyectos y los flujos económicos que consideran diferentes variables en su cálculo, se recomienda realizar un análisis de escenarios que visione diferentes probabilidades. De esta manera, para este análisis de riesgos y evaluación de escenarios, se contemplarán cambios porcentuales en las condiciones de las principales variables: ventas, gastos operativos y la inversión inicial.

Se comienza por el umbral de rentabilidad o también conocido como el análisis de punto muerto, donde se espera conocer el momento en el que las ventas y/o ingresos cubren los cargos fijos de la operación. Es así que al partir con una TIR de 62% y un VAN de S/ 451 mil, se simularon cambios anuales en las principales variables, teniendo como resultado:

Tabla 9.15 Análisis de punto muerto

VARIABLE	VALOR ORIGINAL	PUNTO MUERTO	
Ventas	0.00%	-6.94%	
Gastos operativos	0.00%	22.50%	
Inversión inicial	0.00%	202%	

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Por lo tanto, para que el VAN sea cero y se equiparen las ventas a los costos, éstas deberán tener un ritmo decremento del 6.9%. Otro de los efectos debe ser el aumento porcentual del valor de los gastos operativos en aproximadamente un 23% y que las inversiones iniciales se hayan incrementado en un 202%.

Por otro lado, se realizó un análisis de sensibilidad univariado que certifican los cambios en el VAN y TIR por cada uno de los cambios de comportamiento de las variables identificadas:

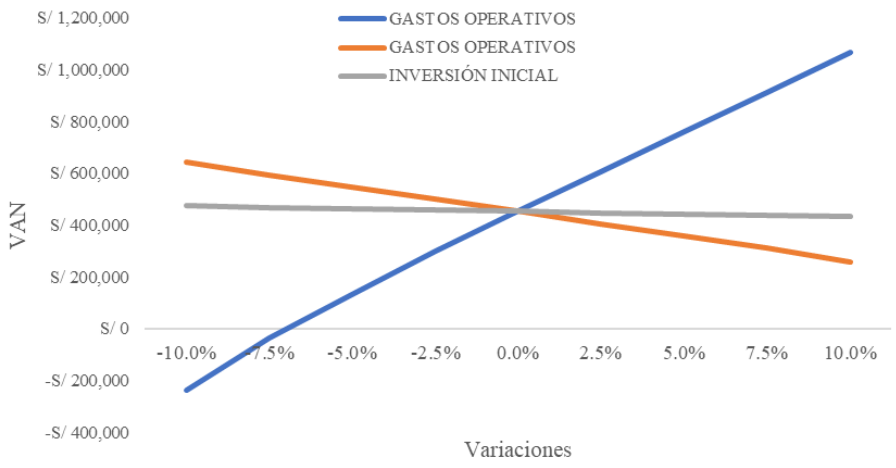
Tabla 9.16 Análisis univariado

VENTAS	VAN	TIR
	S/ 450,628	62%
-10.0%	-S/ 241,578	-4%
-7.5%	-S/ 40,233	16%

-5.0%	S/ 129,953	32%
-2.5%	S/ 294,954	48%
0.0%	S/ 450,628	62%
2.5%	S/ 603,800	75%
5.0%	S/ 756,972	89%
7.5%	S/ 910,144	102%
10.0%	S/ 1,063,316	116%
GASTOS OPERATIVOS	**VAN**	**TIR**
	S/ 450,628	62%
-10.0%	S/ 639,312	79%
-7.5%	S/ 592,141	75%
-5.0%	S/ 544,970	70%
-2.5%	S/ 497,799	66%
0.0%	S/ 450,628	62%
2.5%	S/ 403,457	57%
5.0%	S/ 356,286	53%
7.5%	S/ 307,323	48%
10.0%	S/ 254,561	43%
INVERSIÓN INICIAL	**VAN**	**TIR**
	S/ 450,628	62%
-10.0%	S/ 471,361	67%
-7.5%	S/ 466,177	65%
-5.0%	S/ 460,994	64%
-2.5%	S/ 455,811	63%
0.0%	S/ 450,628	62%
2.5%	S/ 445,444	60%
5.0%	S/ 440,261	59%
7.5%	S/ 435,078	58%
10.0%	S/ 429,895	57%

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Ilustración 9.1 Análisis multidimensional



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Por consiguiente, se puede determinar que la principal variable que tiene impacto directo en el VAN son las ventas dada la pendiente positiva que exhibe. A esta variable

lo secundan los gastos operativos los cuales, si bien tienen una pendiente negativa, ésta se explica por su relación inversa con el VAN dado que éstos deben reducirse para impactar positivamente al indicador de rentabilidad. Finalmente, las inversiones presentan en menor proporción una relación directa con cambios en el VAN.

Si se evalúa el impacto que tienen dos variables en la rentabilidad del negocio, se debe utilizar un análisis bivariado, donde las variables seleccionadas serán las ventas y gastos operativos, los cuales demostraron en el análisis anterior, ser las de mayor impacto. Para este análisis se amplió el rango a una variación de -20% a 20%:

Tabla 9.17 Análisis Multivariado

VENTAS \ GASTOS OPERATIVOS	-20%	-15%	-10%	-5%	0%	5%	10%	15%	20%
-20%	-S/ 571,760	-S/ 703,677	-S/ 835,594	-S/ 967,512	-S/ 1,099,429	-S/ 1,231,346	-S/ 1,363,263	-S/ 1,495,181	-S/ 1,627,098
-15%	-S/ 143,506	-S/ 274,752	-S/ 406,669	-S/ 538,586	-S/ 670,504	-S/ 802,421	-S/ 934,338	-S/ 1,066,255	-S/ 1,198,173
-10%	S/ 205,083	S/ 103,599	-S/ 1,993	-S/ 112,974	-S/ 241,578	-S/ 373,495	-S/ 505,413	-S/ 637,330	-S/ 769,247
-5%	S/ 521,651	S/ 427,309	S/ 332,967	S/ 229,822	S/ 129,953	S/ 22,359	-S/ 84,468	-S/ 208,405	-S/ 340,322
0%	S/ 827,996	S/ 733,654	S/ 639,312	S/ 544,970	S/ 450,628	S/ 356,286	S/ 254,561	S/ 154,489	S/ 46,710
5%	S/ 1,134,340	S/ 1,039,998	S/ 945,656	S/ 851,314	S/ 756,972	S/ 662,630	S/ 568,288	S/ 473,946	S/ 379,604
10%	S/ 1,443,094	S/ 1,346,342	S/ 1,252,000	S/ 1,157,658	S/ 1,063,316	S/ 968,974	S/ 874,632	S/ 780,290	S/ 685,948
15%	S/ 1,755,061	S/ 1,662,059	S/ 1,564,524	S/ 1,466,207	S/ 1,369,660	S/ 1,275,318	S/ 1,180,976	S/ 1,086,634	S/ 992,292
20%	S/ 2,057,453	S/ 1,964,451	S/ 1,871,450	S/ 1,778,448	S/ 1,685,447	S/ 1,587,637	S/ 1,489,319	S/ 1,392,978	S/ 1,298,636

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Mediante este análisis de sensibilidad multidimensional se puede evidenciar que el umbral ideal donde la rentabilidad no se ve perjudicada es hasta el decremento de casi 10% de las ventas y un máximo de 20% en el incremento de los valores asociados a los gastos operativos. No obstante, al tener claro que existen escenarios pesimistas, se procederá a consolidar estos en un último ejercicio donde también se tendrá el efecto acotado de variar en un 10% las principales variables:

Tabla 9.18 Análisis de Escenarios

Escenarios	Pesimista	Moderado	Optimista
Ventas	-10.00%	0.00%	10.00%
Gastos operativos	10.00%	0.00%	-10.00%
Inversión inicial	10.00%	0.00%	-10.00%
TIR	**-35%**	**62%**	**147%**
VAN	**-S/ 527,304**	**S/ 450,628**	**S/ 1,276,010**

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Por lo tanto, se determina que el negocio presenta una buena rentabilidad que únicamente en un escenario pesimista, que se cumplan los factores de disminución a ritmo 10% de las ventas e incremento de 10% en gastos operativos e inversión inicial, podría sugerir que se consideren acciones para contrarrestar estos efectos.

No obstante, se rescata que en un escenario conservador/moderado se tengan valores positivos en VAN y TIR, a pesar de haber dimensionado altos costos de operación y determinar un porcentaje fijo para las contingencias en cada presupuesto.

9.14. Análisis de Riesgos

9.14.1. Identificación de Riesgos

De acuerdo con el análisis financiero realizado, se identificaron los siguientes riesgos en el Plan de Negocios.

Tabla 9.19 Identificación de Riesgos

Riesgo
R1: Financiamiento insuficiente para inversión inicial del proyecto
R2: Demanda real inferior a la proyección
R3: Deserción superior al valor esperado
R4: Aumento de competidores que reduzcan la participación de mercado proyectada
R5: Incremento desmesurado en los costos de las licencias.
R6: Incremento desmesurado en los costos del almacenamiento Cloud

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

9.14.2. Análisis de Riesgos

Se definen los criterios de ponderación por riesgo de acuerdo con las escalas de probabilidad de ocurrencia e impacto definidas para evaluar objetivamente los riesgos identificados en el anterior acápite.

Tabla 9.20 Criterios de ponderación para la probabilidad de ocurrencia

Probabilidad	Escala	Descripción
Muy probable	5	Ha ocurrido al menos 4 veces en el último año.
Probable	4	Ha ocurrido al menos 2 veces en el último año.
Posible	3	Ha ocurrido una vez en el último año.
Improbable	2	No ha ocurrido hace un año.
Raro	1	No ha ocurrido en los últimos dos años.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Tabla 9.21 Criterios de ponderación para el impacto

Impacto	Escala	Descripción
Catastrófico	5	Interrupción total del servicio.
Mayor	4	Interrupción total de un componente del servicio.
Moderado	3	Interrupción parcial del servicio.
Menor	2	Interrupción parcial de un componente del servicio.
Insignificante	1	Interrupción momentánea del servicio hasta 10 minutos.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis

Establecidas las escalas para establecer tanto el nivel de la probabilidad de ocurrencia como el nivel del impacto, se efectúa el análisis del riesgo que permite obtener el nivel del riesgo para cada escenario planteado, multiplicando ambos valores.

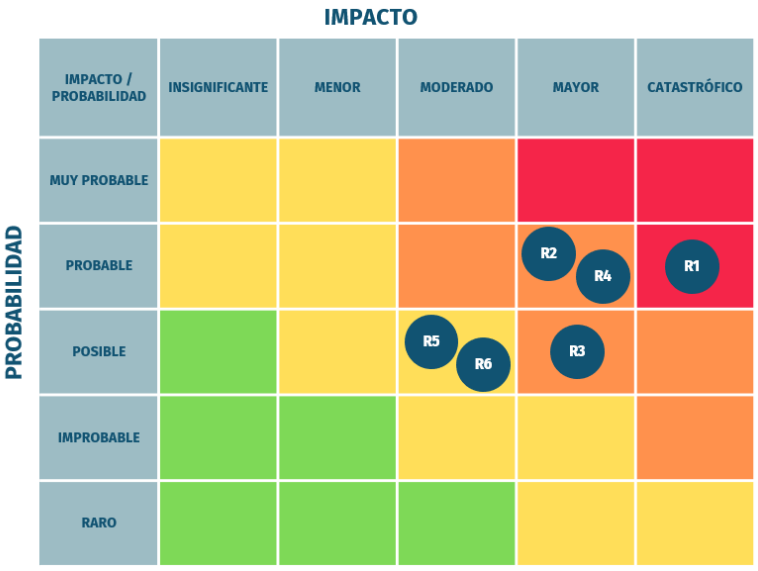
Tabla 9.22 Análisis de los riesgos

Riesgo	Probabilidad	Impacto	Nivel del Riesgo
R1: Financiamiento insuficiente para inversión inicial del proyecto	4	5	4 x 5 = 20
R2: Demanda real inferior a la proyección	4	4	4 x 4 = 16
R3: Deserción superior al valor esperado	3	4	3 x 4= 12
R4: Aumento de competidores que reduzcan la participación de mercado proyectada	4	4	3 x 4 = 16
R5: Incremento desmesurado en los costos de las licencias *endpoint*	3	3	3 x 3 = 9
R6: Incremento desmesurado en los costos del servicio de respaldo y restauración	3	3	3 x 3 = 9

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

Se grafica el resultado del análisis de los riesgos en la matriz debajo.

Ilustración 9.2 Matriz de Probabilidad e Impacto de Riesgos



Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

9.14.3. Plan de Tratamiento del Riesgo

Se establecen controles que ayudarían a mitigar los riesgos identificados, así como el dueño del riesgo o responsable de implementarlo ante la materialización del riesgo.

Tabla 9.23 Plan de Tratamiento de Riesgos

Riesgo	Dueño del Riesgo	Controles
R1	*Head* de Administración y Finanzas	C1: Identificar posibles fuentes de financiamiento adicional al capital propio como ángeles inversores, entidades financieras e incubadoras de emprendimiento.
		C2: Incluir en Plan Preoperativo un monto para tratar contingencias (ej: contratación de expertos ante desafío técnico)
R2	*Head* Comercial y de Marketing	C3: Rediseñar e intensificar la campaña de marketing para aumentar la visibilidad y conocimiento de la marca reforzando los planes de acción para las estrategias de posicionamiento.
	Gerente General y de Operaciones	C4: Evaluar la posibilidad de expansión a pymes de otros sectores antes de lo planificado.
R3	*Head* Comercial y de Marketing	C6: Redefinir el programa de retención para ofrecer un mayor descuento o un beneficio más atractivo.
		C7: Redefinir los programas de referidos y membresías VIP para otorgar beneficios antes de que el cliente decida desertar.
		C8: Monitorear periódicamente los resultados de las encuestas de satisfacción para identificar oportunidades de mejora en el servicio y actuar oportunamente.
	Gerente General y de Operaciones	C9: Aumentar el presupuesto del proceso de investigación y desarrollo a fin de continuar innovando en las funcionalidades y especificaciones de los planes vigentes.
	Head de Administración y Finanzas	C10: Incluir cláusulas de penalidad por deserción antes del período contratado.
R4	*Head* Comercial y de Marketing	C3: Rediseñar e intensificar la campaña de marketing para aumentar la visibilidad y conocimiento de la marca reforzando los planes de acción para las estrategias de posicionamiento.
		C8: Monitorear periódicamente los resultados de las encuestas de satisfacción para identificar oportunidades de mejora en el servicio y actuar oportunamente.
	Gerente General y de Operaciones	C9: Aumentar el presupuesto del proceso de investigación y desarrollo a fin de continuar innovando en las funcionalidades y especificaciones de los planes vigentes.
		C11: Invertir en el desarrollo de una plataforma propia para diversificar la cartera actual de servicios e ingresar al mercado de proveedores tecnológicos de c*iberseguridad*.
R5	Gerente General y de Operaciones	C12: Sostener una buena relación con el proveedor tecnológico y procurar negociar contratos a largo plazo para bloquear tarifas más favorables durante un período de tiempo prolongado.
		C13: Identificar alternativas de proveedores tecnológicos de soluciones para protección *endpoint* a fin de diseñar paquetes de servicios que contemplen otras plataformas de *ciberseguridad*.
R6	Gerente General y de Operaciones	C14: Diversificar proveedores tecnológicos con servicio de respaldo y restauración para poder seleccionar la opción más rentable en el momento dado.

Fuente: Autores de esta tesis.
Elaboración: Autores de esta tesis.

9.15. Conclusión del capítulo

En este último inciso del trabajo de investigación se procedió a evaluar la viabilidad y rentabilidad del modelo de negocio tomando en consideración las estimaciones de cada uno de los presupuestos, lo cual demuestra que el proyecto es viable y rentable con los supuestos y valores determinados. De igual manera, a modo de contramedida se efectuaron análisis de sensibilidad con una y más variables para determinar cuáles de ellas inciden directamente en la rentabilidad de la propuesta.

CAPITULO 10 . CONCLUSIONES Y RECOMENDACIONES

10.1. Conclusiones

En base a los resultados obtenidos, se llega a la conclusión de que el plan de negocio propuesto para la implementación de un servicio de *cibersoporte* para pymes en Lima es financieramente viable. Esta evaluación a 5 años revela un valor presente neto (VAN) positivo de S/ 450,628 junto con una tasa interna de retorno (TIR) del 62%, la cual supera la tasa descuento que se ha establecido como referencia. Además, la inversión inicial requerida para el negocio asciende a S/ 201,018 y será asumida por los socios.

Respecto al análisis de punto muerto, lo más relevante es que, para tener un VAN de cero, las ventas deben decrecer en 6.94%, así como que los gastos operativos deben aumentar en 22.50%. Asimismo, con relación al análisis de sensibilidad multidimensional se evidenció que en un escenario pesimista donde las ventas caen en 10% se observa un VAN de -S/ 527,304 y una TIR de -35%. Se ha prestado especial atención a este escenario a fin de evaluar los riesgos asociados y plantear los planes de mitigación correspondientes.

El aporte social del trabajo realizado es el de mejorar y fortalecer la seguridad informática de las pymes de la región. En la actualidad, la *ciberseguridad* es un tema crítico dado que muchas de las empresas se encuentran expuestas a constantes amenazas cibernéticas que pueden comprometer información sensible y confidencial, dañar la reputación y causar pérdidas económicas considerables. El enfoque de la solución es el de prevenir principales *ciberataques* buscando fortalecer el entorno empresarial en su conjunto, fomentando la confianza y la seguridad en las transacciones digitales. Además, al proteger a las pymes, se protege también a los colaboradores y clientes que confían en ellas, generando un impacto positivo en la comunidad en su conjunto.

Este proyecto también busca contribuir a la comunidad académica generando conocimiento y experiencia en el campo de la *ciberseguridad*. Dicho conocimiento puede ser compartido a través de publicaciones científicas, presentaciones en conferencias o colaboraciones con instituciones educativas. Esto no solo enriquecerá el conocimiento que ya existe en *ciberseguridad*, sino que también incentivará y fomentará la investigación y el desarrollo en este campo. De esta manera el proyecto

tiene el potencial de generar un impacto positivo en la comunidad académica al promover la investigación, el intercambio de conocimientos y la colaboración entre académicos y profesionales del campo de la *ciberseguridad*.

De acuerdo con el análisis del marco conceptual realizado se ha identificado que la *ciberseguridad* es un aspecto importante que es una preocupación constante en las pymes del mundo, y la *ciberseguridad* juega un papel crucial al establecer las estrategias necesarias para prevenir y mitigar la materialización de un incidente.

Respecto al análisis PESTEL del entorno de las pymes en el mercado peruano destaca la inestabilidad política, la contracción económica y la necesidad de adaptación a la digitalización. La ley N° 30056 ofrece oportunidades legales. En cuanto al análisis de la industria, según Porter, la entrada de nuevos competidores es moderada, el poder de negociación de los proveedores es alto, el poder de negociación de los clientes es bajo y la rivalidad entre competidores existentes es baja debido a la falta de servicios específicos para las pymes.

Como consecuencia del análisis, se han identificado las siguientes problemáticas: La falta de conciencia sobre los riesgos de *ciberseguridad* durante la digitalización, lo que resulta en una falta de inversión en medidas básicas de *ciberseguridad*. La creciente sofisticación de los ciberataques hace que las pymes carezcan de la capacidad necesaria para combatirlos sin especialistas o herramientas adecuadas. Los servicios de *ciberseguridad* existentes no se adaptan a las necesidades ni al presupuesto de las pymes, ya que generalmente están orientados hacia empresas más grandes y tienen costos elevados

En base a estas problemáticas se ha generado el modelo de negocio, condensando la propuesta de valor en la frase: *"Tu Negocio, tu Pasión. La Ciberseguridad, nuestra razón"*. Además, se identificaron las características de la solución que contempla el uso de una plataforma de protección *endpoint*, el servicio de *Backup* y recuperación, el monitoreo y respuesta a incidentes y requerimientos, la educación y formación de empleados en prácticas *ciberseguridad*.

Respecto de la metodología de investigación nos planteamos desarrollar los métodos de análisis que nos permitan validar la viabilidad de la propuesta, como

conclusión los resultados de la encuesta muestran un alto grado de aceptación, con un 97% de los encuestados dispuestos a tomar el paquete de servicios que desarrollamos. Además, se observa que la mayoría de los representantes de las pymes tienen puestos gerenciales o son propietarios, lo que sugiere que su opinión es altamente influyente en la toma de decisiones. La transformación digital en estas empresas varía, se evidencia que la mayoría está adoptando procesos tecnológicos e iniciando su camino en la innovación, lo que permitió determinar que se tiene una necesidad latente.

Acerca de las estrategias de marketing definidas, se ha optado por una campaña de Lanzamiento como punto de inicio para dar a conocer a la marca a través de un evento y publicidad en redes, sumado a la definición de la marca *CyberWave*. Respecto a estrategias de posicionamiento, resaltan el desarrollo de un programa de educación del mercado en *ciberseguridad*, y la generación de conciencia a través de redes sociales y conferencias para pymes, sumado a la participación en ferias tecnológicas.

Asimismo, para la fidelización, se han definido programas de Membresías VIP, referidos y retención, planteando beneficios hacia los clientes, para asegurar su fidelización y evitar su deserción.

Respecto a las Operaciones se han definido las actividades del Plan Pre-Operativo. Además, se han definido los procesos estratégicos, de negocio y soporte necesarios para brindar el servicio. También se han definido las políticas del servicio y se ha diseñado el servicio para la Inscripción y afiliación de clientes, y para la operación del servicio de *ciberseguridad*. Es importante resaltar los requisitos tecnológicos necesarios para el servicio como la solución integral de *ciberseguridad*, la infraestructura *cloud*, la página web. Además de otros requisitos para el servicio: tales como las alianzas o el *partnership* con las marcas tecnológicas de *ciberseguridad*, y la implementación de las normas ISO 27001 y ISO 22301.

En relación con la organización, se ha definido la constitución de la empresa *CyberWave* como una sociedad anónima cerrada, que será financiada a través del aporte de los accionistas y contará con las obligaciones tributarias de una pyme. Asimismo, se plantea inicialmente una estructura organizacional para definir claramente los perfiles y responsabilidades de los colaboradores y asegurar la prestación del servicio de manera

controlada. Por último, se han definido los procesos asociados a Recursos Humanos, así como las remuneraciones y el presupuesto organizacional necesario.

Cabe resaltar que la decisión inicial de optar por no buscar financiamiento bancario, y decidir invertir con dinero propio de los socios, se basa en que la empresa, al no estar aún operativa, no cumpliría con las condiciones mínimas necesarias para ser sujeta a una evaluación crediticia positiva. De esta manera, no se retrasa la ejecución del presupuesto preoperativo y el presupuesto de lanzamiento, ni se consideran gastos derivados de condiciones adicionales que pueda exigir la entidad bancaria como la contratación de seguros y la solicitud de garantías líquidas como depósitos a plazo por un período fijo, cuentas de ahorro con saldos significativos, acciones o bonos de empresas que se cotizan en la bolsa, entre otros.

10.2. Recomendaciones

Como acciones a realizar para el escalamiento de la solución o a considerar en una nueva versión del producto o servicio, se sugiere integrar a la página web la funcionalidad de una pasarela de pagos para facilitar la contratación del paquete *Cyber Plus*, así como otros servicios complementarios que podrían ofrecerse a futuro. De esta manera, se establecería una interacción más directa con los clientes apalancándose en la tecnología.

En la misma línea de desarrollo de servicios complementarios, se propone considerar el diseño de paquetes bajo el análisis de la necesidad de otros sectores de pymes para acotar y personalizar la solución en base a la lista completa de servicios que se evaluaron en la encuesta (ej: *VPN* y la bolsa de horas para asesoría y acompañamiento en proyectos digitales). Esta estrategia sería una alternativa previa a ampliar el segmento inicial como estrategia de expansión y crecimiento futuro.

Otro servicio complementario interesante sería establecer una alianza con una empresa especializada en ofrecer cobertura de *ciberriesgos*, brindando así a nuestras pymes interesadas la opción de acceder a un plan adicional que brinde como quinto componente un ciberseguro ante una amenaza avanzada como un *ransomware* que podría paralizar la operación de la pyme. La cobertura del ciberseguro debería incluir mínimamente la conducción de una investigación forense de *ciberseguridad*, servicios

de relaciones públicas y de representación legal, así como indemnización de gastos ante gestión de crisis, multas administrativas y honorarios de otros expertos, entre otros.

Por otro lado, se recomienda efectuar alianzas con instituciones educativas como universidades u otros, que ofrezcan cursos o programas especializados en *ciberseguridad* para obtener descuentos. Además, brinda la posibilidad de pertenecer a las bolsas de trabajo universitarias para conectar con estudiantes y egresados con deseos de adentrarse en la *ciberseguridad* como un canal adicional para apoyar el proceso de reclutamiento y selección.

Como alternativa al paquete *Cyber Plus* conceptualizado con el proveedor actual, se sugiere explorar, analizar e invertir en el desarrollo de más alianzas y afiliación a programas de *partnership* con otros proveedores de soluciones de *ciberseguridad* para ampliar el catálogo de plataformas que se puede ofrecer a las pymes y contar con *backups* ante fallo de proveedor.

En relación con la práctica de considerar *backups* y/o planes de contingencia, se sugiere invertir en el desarrollo de una plataforma propia de *ciberseguridad* que no dependa de un proveedor y que constituya una solución más completa que cubra por completo toda la necesidad de las pymes. Esto contribuiría también a la diferenciación del servicio en un mercado que potencialmente se volvería más competitivo, un mejor control del modelo de precios, y diversificar la cartera de servicios en incurriendo en el mercado de proveedores tecnológicos de *ciberseguridad*.

Para optimizar partes del proceso que rigen el servicio actual, se apunta a automatizar el proceso de solicitud de las licencias adicionales a través de la integración con una *API* del proveedor *Bitdefender* y otros en adelante, que permitan la construcción de un proceso más directo, rápido y que reduzca el posible error humano.

De cara a solventar y/o mitigar riesgos en el escalamiento, se propone durante el tercer año y previo a la gran inversión que se destinaría a la incursión al mercado general de las pymes, considerar una fuente adicional de financiamiento proveniente de una entidad bancaria o una incubadora, dado que *CyberWave* contaría con años de operación que le han permitido desarrollar un historial operativo y financiero suficiente como

sustento, así como un flujo de efectivo estable, un plan de negocios sólido y una relación con una o más entidades financieras al abrir cuentas comerciales.

Por último, en pro de conseguir eficiencias en los costos operativos, se recomienda negociar cada año las condiciones del *partnership* con la finalidad de obtener mayores beneficios y descuentos en los procesos de las licencias, conforme aumenta la cartera de clientes que contratan el servicio.

CAPITULO 11 . ANEXOS

Anexo 1. Lista de Expertos entrevistados de *Ciberseguridad*

N°	Edad	Puesto
1	36	Security Officer
2	45	Gerente Corporativo de Seguridad TI
3	28	Subgerente Planeamiento Estratégico TI
4	35	Project Team Leader de Seguridad TI

Anexo 2. Lista de Expertos entrevistados de *Ciberseguridad*

N°	**Puesto**
1	*Security Officer*
2	Gerente Corporativo de Seguridad TI
3	Subgerente Planeamiento Estratégico TI
4	*Project Team Leader* de seguridad TI

Anexo 3. Lista de Potenciales Clientes entrevistados

N°	Puesto	Sector
1	Gerente General	Medios de Pago
2	Gerente	Textil
3	Gerente General	Tecnología
4	Gerente	Textil

Anexo 4. Estructura de la Entrevista a Expertos de *Ciberseguridad*

1) ¿Cómo describiría el panorama actual de la *Ciberseguridad* en las empresas peruanas?

2) ¿Cuáles son los desafíos más comunes que enfrentan las organizaciones en términos de *Ciberseguridad*?

3) ¿Cuáles son los más grandes mitos de la *Ciberseguridad* que has escuchado de parte de empresarios?

4) ¿Qué medidas mínimas debería adoptar una empresa pequeña y mediana para protegerse ante ciberataques?

5) ¿Qué papel juega la concientización en la prevención de *ciberincidentes*?

6) ¿Cuáles son los aspectos clave a tener en cuenta al evaluar un proveedor de *Ciberseguridad* disponible en el mercado?

7) ¿Qué servicios de *Ciberseguridad* consideras los más solicitados por las empresas pequeñas y medianas?

8) ¿Cuáles serían los argumentos para justificar una inversión en *Ciberseguridad* a un empresario de una empresa pequeña y mediana?

Anexo 5. Estructura de la Entrevista a Potenciales Clientes

1) ¿De qué rubro es su empresa y en qué nivel de digitalización considera que se encuentra?

2) ¿Has experimentado alguna vez un incidente de *Ciberseguridad* en tu empresa? ¿Cómo los afrontó? ¿Llegaron a solucionarlo?

3) ¿Qué tanto conoces de *Ciberseguridad*? ¿Consideras que es un aspecto importante para las empresas pequeñas y medianas?

4) ¿Qué tipo de amenazas cibernéticas considera que son las más preocupantes para su empresa?

5) ¿Qué impacto o consecuencias considera que puede generar un incidente de *Ciberseguridad* en su empresa?

6) ¿Cómo evalúa el nivel de conciencia y capacitación de su personal en temas de *Ciberseguridad*?

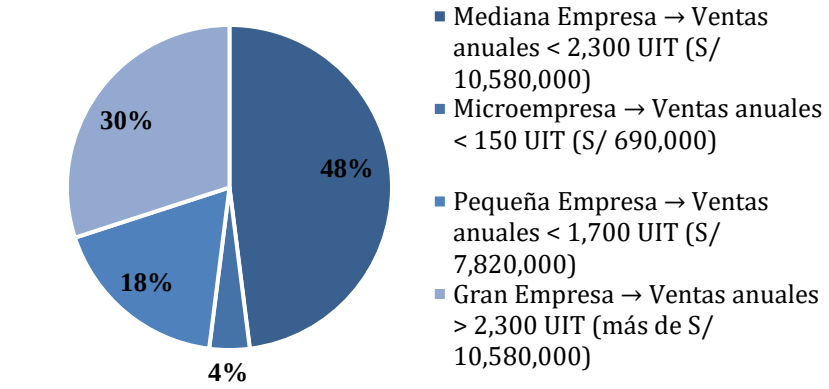
7) ¿Qué tipo de medidas de *Ciberseguridad* tiene actualmente implementadas en su empresa?

8) ¿Considera que sería beneficioso para su empresa contratar un servicio de *Ciberseguridad*? ¿De qué manera?

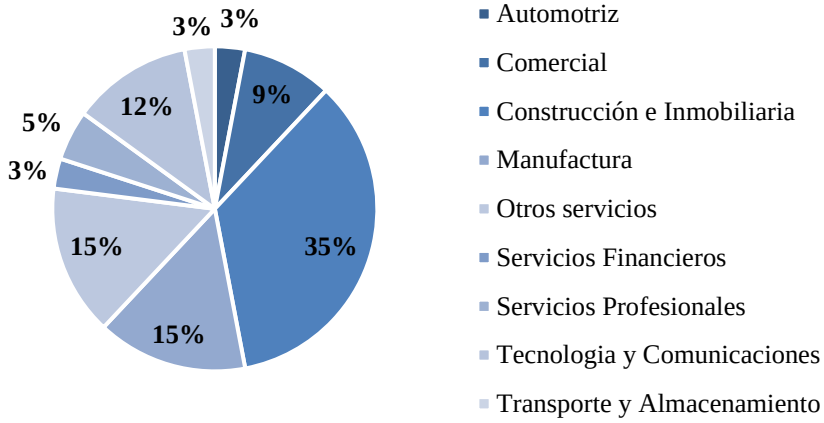
9) ¿Qué criterios y factores consideraría más importantes para la elección de un proveedor de servicios de *Ciberseguridad*?

Anexo 6. Sondeo Inicial

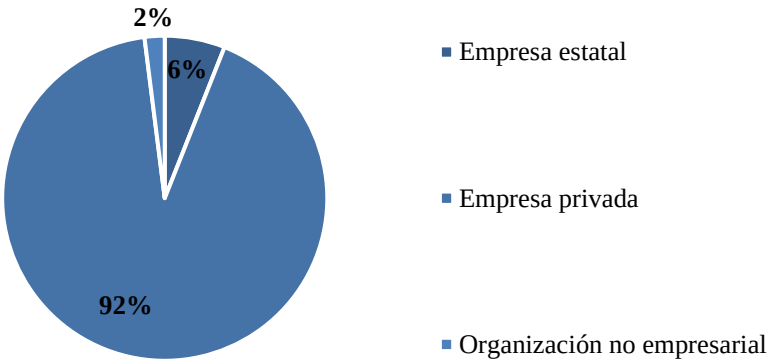
1. ¿Cuál es el segmento de la empresa?



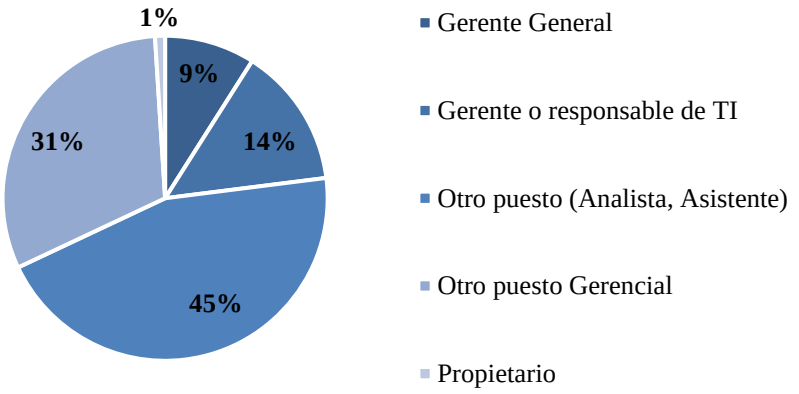
2. Solo pymes en adelante, ¿En qué sector te desempeñas laboralmente?



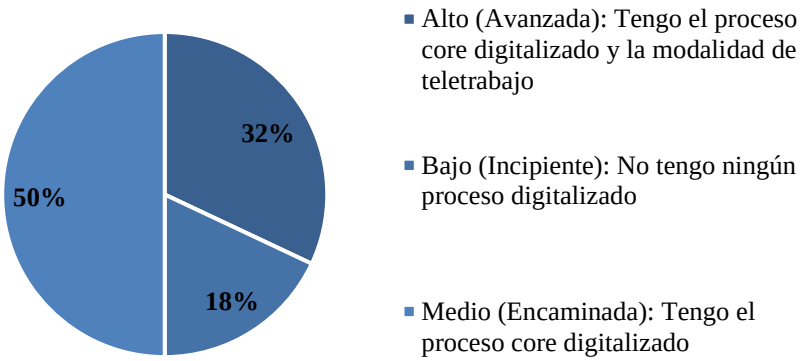
3. ¿Cuál es el tipo de empresa?



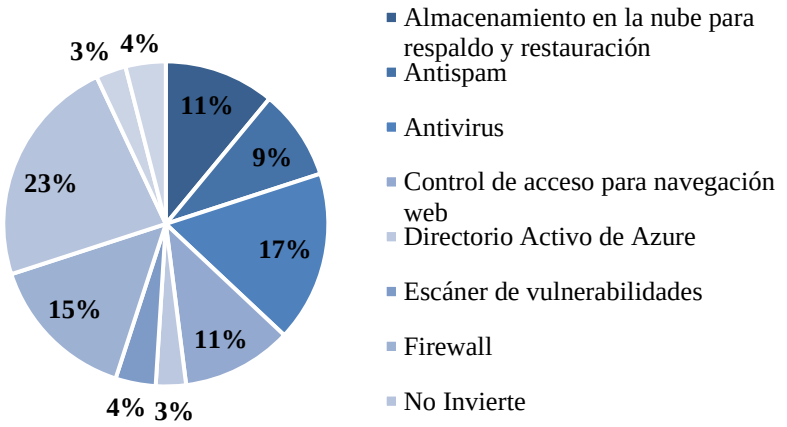
4. ¿Cuál es su cargo en la empresa?



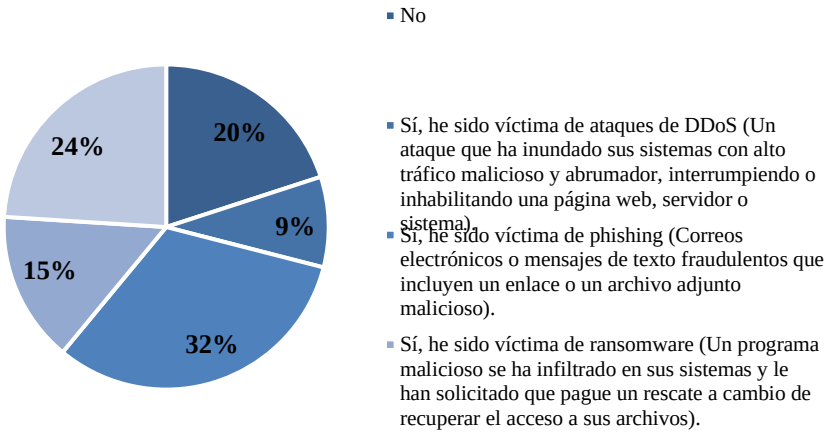
5. ¿En qué estado de transformación digital se encuentra la empresa?



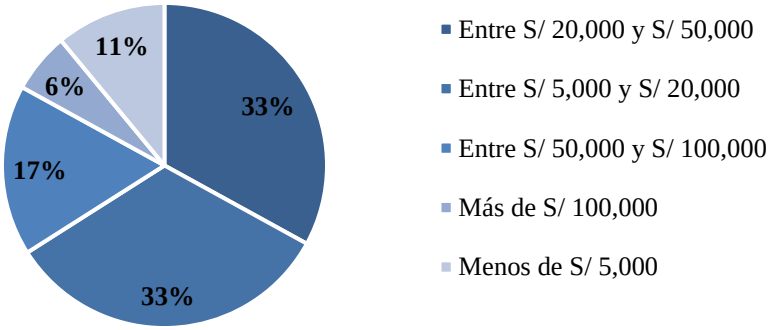
6. ¿En qué componentes de *Ciberseguridad* invierte actualmente tu organización?



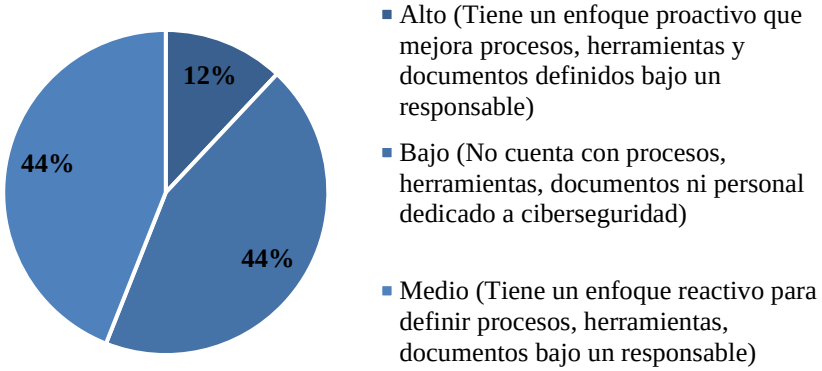
7. ¿Has experimentado alguna vez *ciberataques* en tu empresa? En caso de que sí, ¿De qué tipo fueron?



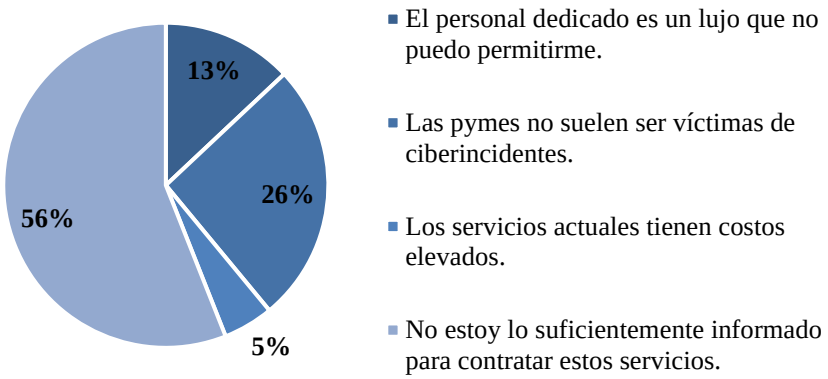
8. ¿Cuánto dinero estimado habrá perdido la empresa como resultado del *ciberataque*?



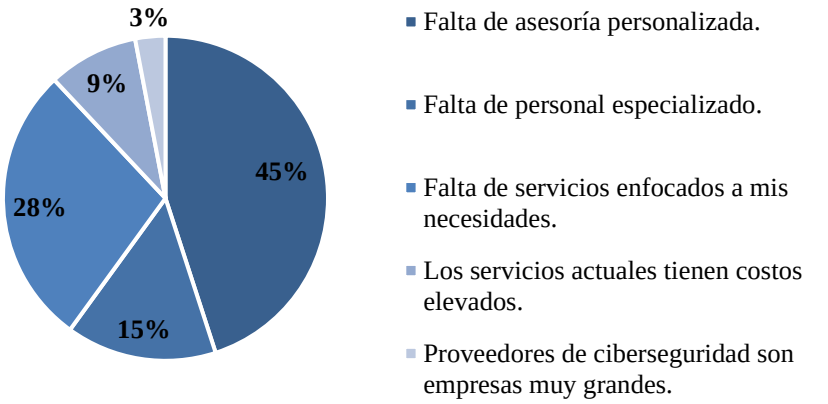
9. ¿Cuál consideras que es el nivel de conocimiento de tu organización para afrontar amenazas de *Ciberseguridad*?



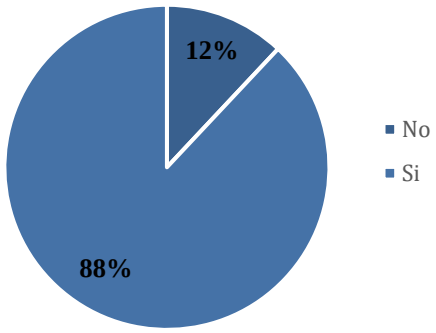
10. ¿Cuál es la principal razón por la cual no has contratado servicios de *Ciberseguridad*?



11. De los servicios que has contratado, o existentes en el mercado de *Ciberseguridad* ¿Qué problemáticas has encontrado?



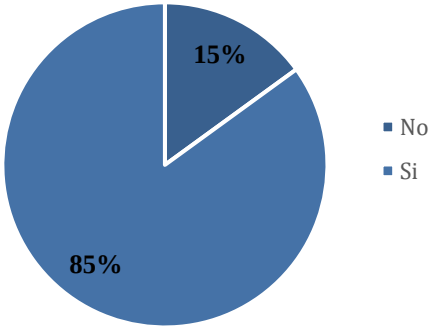
12. Estarías dispuesto a adquirir un servicio de *Ciberseguridad* de calidad enfocado a pymes, a un precio asequible.



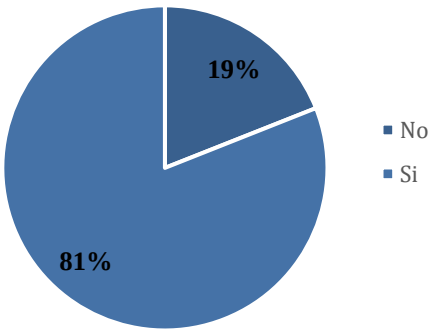
Anexo 7. Encuesta para Validación del Modelo de Negocio

"Estimados, esperamos estén bien. La siguiente encuesta forma parte de nuestro proyecto de tesis para el MBA y tiene como objetivo evaluar la viabilidad y el interés de un paquete de *Ciberseguridad* especialmente diseñado para pymes en el sector construcción/inmobiliaria en Lima. Todas sus respuestas serán tratadas con absoluta confidencialidad, y los resultados obtenidos se utilizarán únicamente con fines académicos. ¡Muchas gracias por su participación y tomarse el tiempo en responder!"

1. ¿Trabajas en una Pequeña y Mediana empresa (PYME) en Lima Metropolitana?

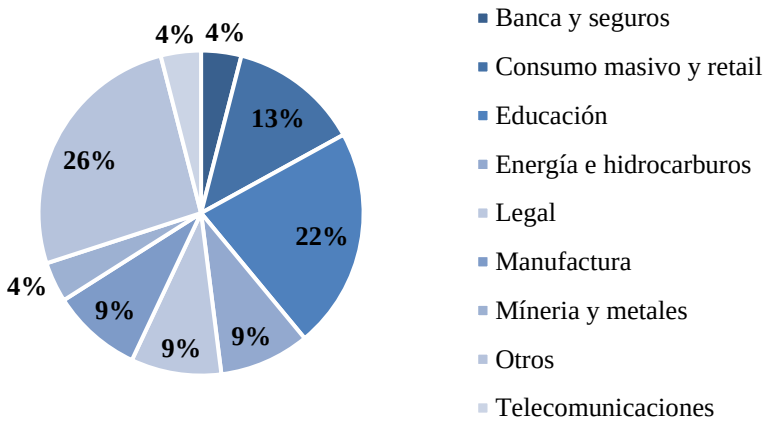


2. <u>Solo pymes en adelante</u>, ¿Trabajas en el sector de Construcción/Inmobiliaria?



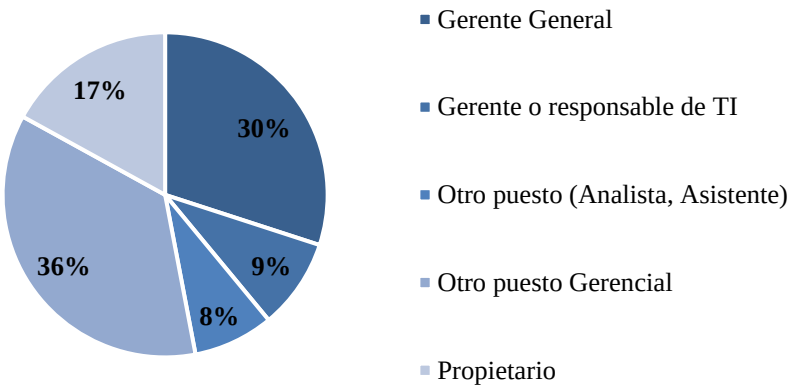
OTROS SECTORES

3. ¿En qué sector te desempeñas?



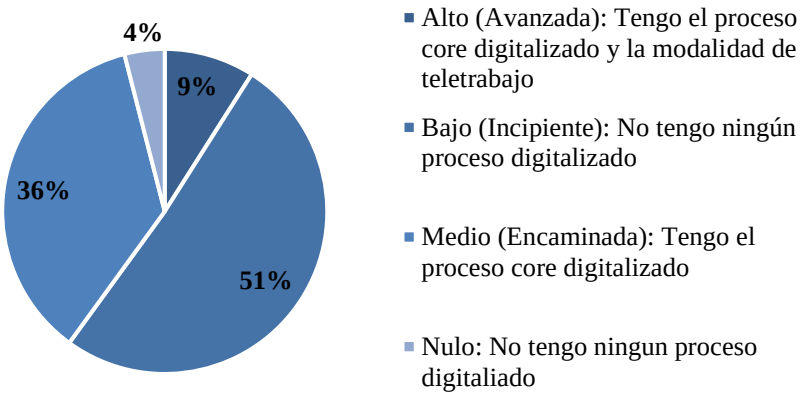
CARGO

4. Sólo Construcción e Inmobiliaria en adelante, ¿Cuál es tu cargo en la empresa?

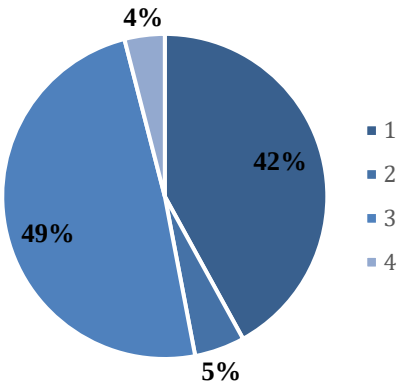


NIVEL DE DIGITALIZACIÓN

5. ¿En qué nivel de transformación digital consideras que se encuentra tu empresa?



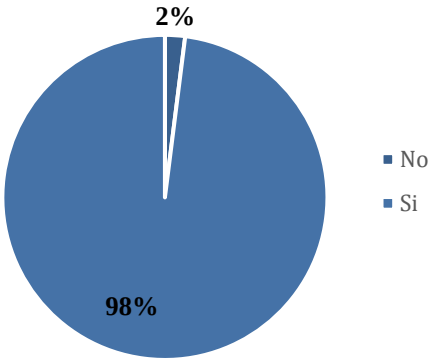
6. En una escala del 1 al 5, donde 1 es "Muy insatisfecho" y 5 es "Muy satisfecho", ¿cómo calificarías tu experiencia con servicios de *Ciberseguridad* o empresas que te han brindado estos servicios anteriormente (si no lo has contratado, coloca neutral (3))?



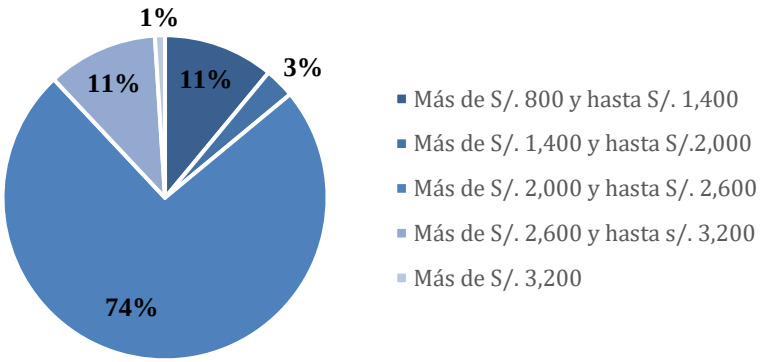
7. Proponemos un paquete de servicios de *Ciberseguridad* enfocado a pymes que incluya:

   - Monitoreo centralizado de eventos e incidentes en Antivirus y *Firewall*,
   - Configuración de seguridad y accesos para proteger tus correos e información en la nube contra el *phishing*, *malware* y *ransomware*,
   - Almacenamiento en la nube para respaldo y restauración ante un ciberincidente, y
   - Programa de concientización para tus trabajadores.

   ¿Estarías dispuesto a tomar sus servicios?

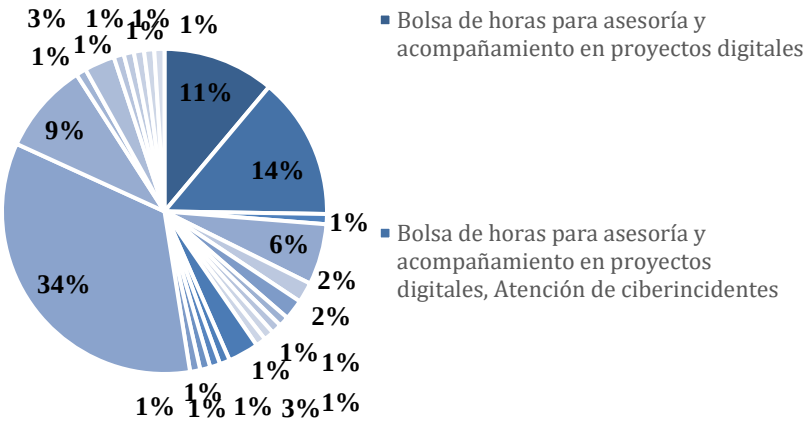


8. ¿Cuánto estarías dispuesto a pagar mensualmente por un paquete de servicios de *Ciberseguridad* como el descrito anteriormente?

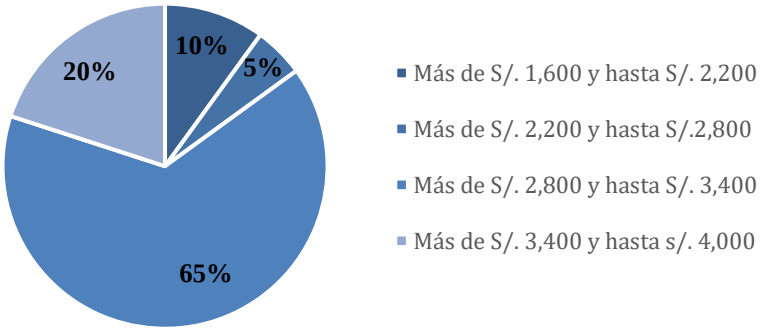


9. ¿Qué servicios adicionales añadirías al paquete mensual? (Opción múltiple)

- *VPN* para proteger las comunicaciones durante el acceso remoto
- Bolsa de horas para asesoría y acompañamiento en proyectos digitales
- *Pentesting*: Test de penetración que valora los posibles fallos de seguridad informática que puede tener un sistema y qué alcance tienen dichos fallos
- Auditoría de nivel de *Ciberseguridad*
- Atención de *ciberincidentes*
- Escáner de vulnerabilidades
- Otras



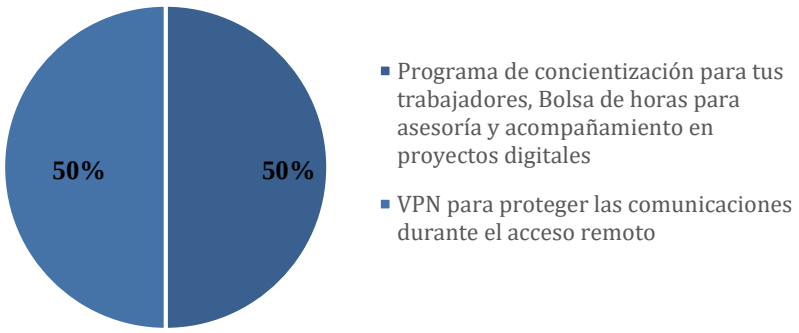
10. ¿Cuánto estarías dispuesto a pagar mensualmente por un paquete de servicios de *Ciberseguridad* que incluyera los servicios que marcaste en la pregunta anterior?



11. ¿Qué servicios de los siguientes mencionados tomarías para armar un paquete de *Ciberseguridad* que se ajuste a tus necesidades?

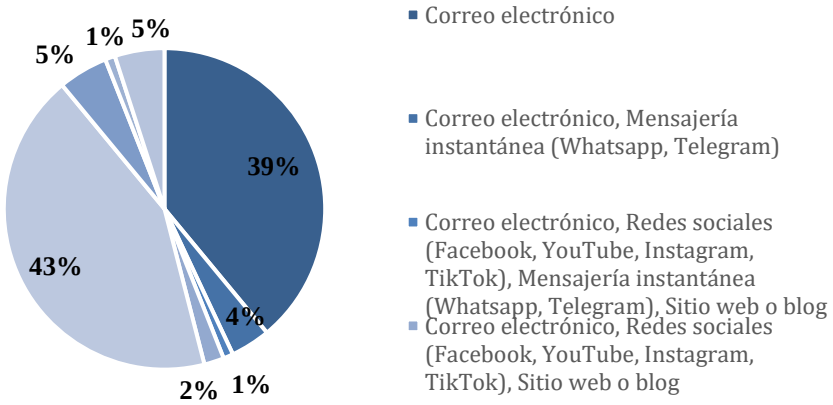
- Monitoreo centralizado de eventos e incidentes en Antivirus y *Firewall*
- Configuración de seguridad y accesos para proteger tus correos e información en la nube contra el *phishing*, *malware* y *ransomware*
- Almacenamiento en la nube para respaldo y restauración ante un ciberincidente
- Programa de concientización para tus trabajadores
- *VPN* para proteger las comunicaciones durante el acceso remoto
- Bolsa de horas para asesoría y acompañamiento en proyectos digitales
- Pentesting: Test de penetración que valora los posibles fallos de seguridad informática que puede tener un sistema y qué alcance tienen dichos fallos

- Auditoría de nivel de *Ciberseguridad*
- Atención de *ciberincidentes*
- Escáner de vulnerabilidades
- Otra



12. ¿Qué canales de comunicación prefiere usted para mantenerse informado sobre las amenazas de *Ciberseguridad*, charlas online y promociones en servicios? (Selecciona todas las opciones que apliquen)

- Correo electrónico
- Redes sociales (LinkedIn, Facebook, YouTube, Instagram, TikTok)
- Mensajería instantánea (Whatsapp, Telegram)
- Sitio web o blog



CAPITULO 12 . BIBLIOGRAFÍA

Accenture. (2023). *Digital Transformation.* https://www.accenture.com/us-en/insights/digital-transformation-index

BBC News Mundo. (2023). *La otra guerra inclemente que libran Ucrania y Rusia.* https://www.bbc.com/mundo/noticias-internacional-65266795

BCRP. (2023). *Informe Macroeconómico: I Trimestre del 2023.* https://www.bcrp.gob.pe/docs/Publicaciones/Notas-Estudios/2023/nota-de-estudios-36-2023.pdf

Bing, C., & Kelly, S. (2021, 9 mayo). *Cyber attack shuts down U.S. fuel pipeline 'Jugular,' Biden briefed. Reuters.* https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Bustamante García, S., Valles Coral, M. Ángel, Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). *Policies based on ISO 27001: 2013 and its influence on information security management in municipalities of Peru.* Enfoque UTE, 12(2), pp. 69 - 79. https://doi.org/10.29019/enfoqueute.743

CEEI Valencia. (2023). *Early Adopters: Quiénes son y cómo identificarlos. Centro Europeo de Empresas e Innovación.* https://ceeivalencia.emprenemjunts.es/?op=8&n=29037

Comunidaria. (2023). *Ciberataques pueden costar más de 100 mil dólares a Pymes de América Latina: Kaspersky.* https://comunidaria.com/ciberataques-pueden-costar-mas-100-mil-dolares-pymes-america-latina-kaspersky/

Conexión ESAN. (2023). *¿Cómo debemos prepararnos ante el aumento de ciberataques en el Perú?* https://www.esan.edu.pe/conexion-esan/como-debemos-prepararnos-ante-el-aumento-de-ciberataques-en-el-peru

CONFIEP. (2021). *PYMES: El motor del crecimiento en el Perú.* https://www.confiep.org.pe/confiep-tv/pymes-el-motor-del-crecimiento-en-el-peru/

Castillo, N. (2020). *Inestabilidad política: ¿cómo está afectando a la reactivación económica? El Comercio Perú.* https://elcomercio.pe/economia/inestabilidad-politica-y-su-impacto-en-la-reactivacion-economica-noticia/

Castillo, P. (2023). *La ciberdelincuencia en el Perú: Estrategias y Retos del Estado. Defensoría del Pueblo.* https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

DeKorte, R. (2019). *Cybersecurity Insurance: Toward a More Effective Marketplace.* https://www.proquest.com/openview/c1aba763e8bfa4b04ab66581a4ec6e91/1?pq-origsite=gscholar&cbl=18750&diss=y

Digital Ocean. (2023). *Small businesses and cybersecurity: How startups and SMBs are viewing security threats in 2023. Digital Ocean.* https://www.digitalocean.com/reports/cybersecurity-smbs-2023#cybersecurity

El Comercio, R. (2023). *Pymes peruanas: el 95% aceleró su transformación digital por la pandemia, según Microsoft*. El Comercio Perú. https://elcomercio.pe/economia/peru/pymes-peruanas-un-95-de-pequenas-y-medianas-empresas-aceleraron-su-transformacion-digital-por-la-pandemia-segun-microsoft-rmmn-noticia/?ref=ecr#google_vignette

El Comercio, R. (2023). *Perú fue el objetivo de más de 15 mil millones de intentos de ciberataques en 2022. Diario El Comercio.* https://elcomercio.pe/tecnologia/actualidad/*Ciberseguridad*-peru-fue-el-objetivo-de-mas-de-15-mil-millones-de-intentos-de-ciberataques-en-2022-hackers-espana-mexico-colombia-noticia/

El Comercio, R. (2022). *E-commerce en Perú: se moverá US$ 20.000 millones y crecerá 53% al cierre de este año, según estudio. Diario El Comercio.* https://elcomercio.pe/economia/peru/ecommerce-en-el-peru-se-movera-20000-millones-de-dolares-y-crecera-53-al-cierre-de-este-2022-rmmn-noticia/

El Comercio, R. (2015). *Ya entró en vigencia la Ley de Protección de Datos Personales. Diario El Comercio.* https://elcomercio.pe/economia/peru/entro-vigencia-ley-proteccion-datos-personales-190244-noticia/

El Comercio, R. (2014). *Siete puntos claves en los cambios de la Ley de MyPes. Diario El Comercio.* https://elcomercio.pe/economia/peru/siete-puntos-claves-cambios-ley-mypes-165266-noticia/

El Peruano. (2019). *Ley Nº 30999 Ley de Ciberdefensa. Diario El Peruano.* https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

ENISA. (2021). *Guía de Ciberseguridad para pymes. The European Union Agency for Cybersecurity.* https://www.enisa.europa.eu/publications/report-files/ smes-leaflettranslations/enisa-cybersecurity-guide-for-smes_es.pdf

Escalante, E. (2016). *Promulgan Ley No 30056 que modifica la actual ley MYPE y otras normas para las micro y pequeñas empresas. MiEmpresaPropia.* https://www.mep.pe/promulgan-ley-no-30056-que-modifica-la-actual-ley-mype-y-otras-normas-para-las-micro-y-pequenas-empresas/

Escudero, F. (2022, August 12). *Transformación con Sentido Digital 2022: Madurez Digital de las Organizaciones en Perú. EY US - Home.* https://www.ey.com/es_pe/consulting/madurez-digital-en-peru

ESET. (2022). *Cyber risks driving SMBs to enterprise solutions. ESET Security.* https://web-assets.esetstatic.com/wls/2022/11/eset_smb_digital_security_sentiment_report.pdf

Estaún, M. (2023). *¿Qué es el marketing mix y cuáles las 9P's del marketing? Thinking for Innovation.* https://www.iebschool.com/blog/marketing-mix-marketing-digital/

Flores-Aguilar, E. (2019). *Design of a Center for Entrepreneurs in an Engineering School applying the Lean Canvas Model.* Formación universitaria, 12(6), 151-166. https://dx.doi.org/10.4067/S0718-50062019000600151

Fortinet. (2023). *Cybersecurity Skills Gap Global Research Report. Fortinet Training Institute.* https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

Gestión, R. (2023). *Cerca de 12,000 empresas en Perú declararon al menos un teletrabajador en 2022. Diario Gestión.* https://gestion.pe/economia/management-empleo/teletrabajo-cerca-de-12000-empresas-en-peru-declararon-al-menos-un-teletrabajador-en-2022-trabajo-remoto-ley-de-teletrabajo-noticia/

Gestión, R. (2023). *B2B: Oportunidades y retos para las Pymes en el Perú este 2023. Diario Gestión.* https://gestion.pe/publirreportaje/empresas-negocios-y-financiamiento-comercio-b2b-oportunidades-y-retos-para-las-pymes-en-el-peru-este-2023-esan-prioridades-de-inversion-noticia/

Gestión, R. (2022). *Educación Financiera: ¿Cuántas pymes son víctimas de ciberataques? Diario Gestión.* https://gestion.pe/economia/empresas/ciberataques-a-pymes-peruanas-la-importancia-de-la-cibersegurad-para-las-pymes-como-evitar-un-ciberataque-noticia/

Gestiopolis (2021). *¿Qué es la cadena de valor?* gestiopolis. https://www.gestiopolis.com/que-es-la-cadena-de-valor/

Grange, T. (2023). *What Are The Effects of Cyber Attacks on Small Businesses? Bionic.* https://bionic.co.uk/business-connectivity/guides/the-effects-of-online-attacks-small-business/

Hernández, J. (2022). *Mil seiscientos ciberataques por segundo en Latam. MAPFRE.* https://www.mapfre.com/actualidad/seguros/ciberataques-en-latam/

Hubspot (2023) Estrategias genéricas de Porter: qué son y cómo aplicarlas. HubSpot. Recuperado de https://blog.hubspot.es/marketing/estrategias-genericas-de-porter

IBM. (2022) *Cost of a Data Breach 2022: Resumen ejecutivo.* https://www.ibm.com/reports/data-breach-action-guide#:~:text=Data%20breach%20costs%20averaged%20USD,Breach%20Report%20has%20been%20published.

IBM. (2022). *What is a data breach? IBM.* https://www.ibm.com/topics/data-breach

Infobae. (2022). *Seis presidentes en seis años: Se abre un nuevo capítulo de inestabilidad en la política peruana.* https://www.infobae.com/america/peru/2022/12/08/seis-presidentes-en-seis-anos-se-abre-un-nuevo-capitulo-de-la-inestabilidad-politica-peruana/

INEI. (2021). *Perú: Estructura Empresarial, 2019. Instituto Nacional de Estadística e Informática.* https://www.inei.gob.pe

INEI. (2022). *Perú: Estructura Empresarial, 2020. Instituto Nacional de Estadística e Informática.* https://www.inei.gob.pe

ISO. (2023). *ISO/IEC 27032:2023. International Organization for Standardization.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en

ISO. (2022). *ISO/IEC 27001:2022. International Organization for Standardization.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

ISO. (2022). *ISO/IEC 27002:2022. International Organization for Standardization.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

ISO. (2020). ISO/IEC 22624:2020. *International Organization for Standardization.* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22624:ed-1:v1:en

ISO. (2019). *ISO/IEC 31000:2019. International Organization for Standardization.* https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

ISO. (2018). *ISO/IEC 27000:2018. International Organization for Standardization.* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en

IT Digital Security. (2022). *Las pymes luchan contra la falta de experiencia y recursos en ciberseguridad.* https://www.itdigitalsecurity.es/endpoint/2022/10/las-pymes-luchan-contra-la-falta-de-experiencia-y-recursos-en-Ciberseguridad

Lewandowski, M. (2016). *Designing the Business Models for Circular Economy—Towards the Conceptual Framework.* Sustainability 8, no. 1: 43. https://doi.org/10.3390/su8010043

Martos, S. (2022). *Indicadores de rendimiento (KPI): Cuáles son, objetivos, ejemplos y cómo definir KPIs para tu empresa.* https://www.cinconoticias.com/indicadores-de-rendimiento/

Maurya, A. (2012). *Running Lean: Iterate from Plan A to a Plan That Works.* Sebastopol: O'Reilly.

McClure. D. (2010). *Startup metrics for pirates.* https://es.slideshare.net/ dmc500hats/Startup-metrics-for-pirates-long-version

McKinsey. (2023). *What is digital transformation? McKinsey & Company.* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation

Melara, M. (2020). *Necesidades, deseos, demanda y el marketing. El Blog de Marlon Melara.* https://marlonmelara.com/necesidades-deseos-demanda-y-el-marketing/

Ministerio Público Fiscalía de la Nación. (2020). *Convenio sobre la ciberdelincuencia permite a jueces y fiscales realizar requerimientos de cooperación internacional. Ministerio Público Fiscalía de la Nación.* https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

Mishima, M. (2023). *Multas por infracciones en materia de protección de datos personales pueden ascender hasta S/ 495,000. Ernst & Young.* https://www.ey.com/es_pe/news/2023/02/multas-infracciones-proteccion-datos-personales

MisiónPyme. (2023). *Pymes, las más afectadas por los ciberataques. MisiónPyme.* https://misionpyme.com/pymes-4-0/pymes-las-mas-afectadas-por-los-ciberataques/

Microsoft. (2022). *Aceleración digital: más del 94% de las pymes peruanas invirtió en tecnología en el último año. News Center Latinoamérica.* https://news.microsoft.com/es-xl/aceleracion-digital-mas-del-94-de-las-pymes-peruanas-invirtio-en-tecnologia-en-el-ultimo-ano/

NIST. (2019). *Glossary. NIST.* https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

NIST. (2021). *Developing Cyber-Resilient Systems: A systems security engineering approach (2 ed., p. 62). NIST Special Publication 800-160.* https://doi.org/10.6028/NIST.SP.800-160v2r1

OEA. (2023). *Reporte sobre el desarrollo de la fuerza laboral de Ciberseguridad en una era de escasez de talento y habilidades. Organización de los Estados Americanos.* https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_Ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

Ortega, C. (2023). *Muestreo no probabilístico: definición, tipos y ejemplos. QuestionPro.* https://www.questionpro.com/blog/es/muestreo-no-probabilistico/

OWASP. (2023). *SQL Injection. Open Web Application Security Project.* https://owasp.org/www-community/attacks/SQL_Injection

Porras, J., Pastor, S., & Alvarado, R. (2018). *Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas.* Revista Peruana de Computación y Sistemas, 1(1), 47–56. http://dx.doi.org/10.15381/rpcs.v1i1.14856

Pymeseguros. (2022). *Correduidea analiza la Ciberseguridad en la actualidad | Pymeseguros.* https://www.pymeseguros.com/%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8Bcorreduidea-analiza-la-Ciberseguridad-en-la-actualidad

Ramos, R. & Wert, A. (2015). *¿Qué es el Design Thinking? Design Thinking en Español.* http://designthinking.es/home/index.php

Rebbeck, T. (2022). *Small and medium-sized business (SMB) cyber-security challenges and solutions. Analysys Mason.* https://app.hushly.com/runtime/view/Analysys%20Mason%20Check%20Point_Paper%20on%20SMB.pdf?guid=sieh2t3235ov65b5vh6517tgvn

ReliaQuest. (2023). *Annual Cyber-Threat Report: ReliaQuest Annual Cyber-Threat Report. ReliaQuest.* https://www.reliaquest.com/wp-content/uploads/2023/06/2023_ReliaQuest_AnnualThreatReport.pdf

Revista EAFIT - 105, Gladis Villegas. (s. f.). http://web.archive.org/web/20030205200444/www.eafit.edu.co/revista/105/villega.html

Santander. (2021). *Tam Sam Som: cómo calcular el tamaño de mercado. Becas Santander.* https://www.becas-santander.com/es/blog/tam-sam-som.html

Silva, C. (2023). *Gobierno publicó su política de transformación digital al 2030: ¿qué se propone? | ANÁLISIS. Diario El Comercio Perú.* https://elcomercio.pe/economia/gobierno-publico-su-politica-de-transformacion-digital-al-2030-que-se-propone-comercio-electronico-servicios-digitales-tramites-documentos-dina-boluarte-noticia/

Spiceworks. (2022). *DDoS Definition, Types, and Prevention Best Practices. Spiceworks.* https://www.spiceworks.com/it-security/network-security/articles/what-is-ddos/

Strategyzer. (2017) *Value Proposition Canvas: a tool to understand what customers really want.* https://www.strategyzer.com/library/value-proposition-canvas-a-tool-to-understand-what-customers-really-want

Tema 2.3 Análisis de los recursos y capacidades - Instituto Consorcio Clavijero. (s. f.). https://cursos.clavijero.edu.mx/cursos/117_deh/modulo2/contenido/tema2.3.html

Tiempo Minero. (2022). *Crisis política en Perú y cómo afecta la industria. Tiempo Minero*. https://camiper.com/tiempominero-noticias-en-mineria-para-el-peru-y-el-mundo/crisis-politica-en-peru-y-como-afecta-la-industria/

Turín, N. (2021). *Impacto de las empresas familiares en la economía peruana. Blogs Universidad Continental.* https://blogs.ucontinental.edu.pe/impacto-de-las-empresas-familiares-en-la-economia-peruana/contiblogger/