UNIVERSITARIO RUMIÑAHUI

Pregrado

Carrera: **ADMINISTRACIÓN Y GESTIÓN COMERCIAL**

Asignatura (UIC): **Gestión de la Innovación Administrativa**

Trabajo de titulación previo a la obtención del Título en:

Tecnólogo Superior Universitario en Administración y Gestión Comercial.

Tema: **"Plan de negocios para la comercialización de una plataforma de simulación de ciberataques orientada a la concientización del personal en MIPYMES de Pichincha - Caso Attack Simulator"**

Autor/s: **Brayan Alexander Iglesias Alcivar**

Tutor 1: **Ing. Hilberth Villalba B.**

Tutor 2: **Mg. Verónica Arevalo**

Fecha: **Marzo 2025**

Autor: BRAYAN ALEXANDER IGLESIAS ALCIVAR

Título a obtener: Tecnólogo superior universitario en administración y gestión comercial

Matriz: Sangolquí -Ecuador

Correo electrónico: brayan.iglesias2003@gmail.com

Dirigido por: VILLALBA BEJARANO HILBERTH ALEXIS

Título: Ingeniero en Finanzas

Matriz: Sangolquí -Ecuador

Correo electrónico: hilberth.villalba@ister.edu.ec

BRAYAN ALEXANDER IGLESIAS ALCIVAR

"PLAN DE NEGOCIOS PARA LA COMERCIALIZACIÓN DE UNA PLATAFORMA DE SIMULACIÓN DE CIBERATAQUES ORIENTADA A LA CONCIENTIZACIÓN DEL PERSONAL EN MIPYMES DE PICHINCHA - CASO ATTACK SIMULATOR"

CARTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

CT-ANX-2025-ISTER-2-2.3

Sangolquí, 04 de septiembre del 2025

MSc. Elizabeth Ordoñez
DIRECTORA DE DOCENCIA

MSc. Mónica Loachamín
COORDINADORA DE TITULACIÓN

INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

Presente

Por medio de la presente, yo, Brayan Alexander Iglesias Alcivar declaro y acepto en forma expresa lo siguiente: Ser autor del trabajo de titulación denominado PLAN DE NEGOCIOS PARA LA COMERCIALIZACIÓN DE UNA PLATAFORMA DE SIMULACIÓN DE CIBERATAQUES ORIENTADA A LA CONCIENTIZACIÓN DEL PERSONAL EN MIPYMES DE PICHINCHA - CASO ATTACK SIMULATOR, de la Tecnología Superior Universitaria en ADMINISTRACIÓN Y GESTIÓN COMERCIAL; y a su vez manifiesto mi voluntad de ceder al Instituto Superior Tecnológico Rumiñahui con condición de Universitario los derechos de reproducción, distribución y publicación de dicho trabajo de titulación, en cualquier formato y medio, con fines académicos y de investigación.

Esta cesión se otorga de manera no exclusiva y por un periodo indeterminado. Sin embargo, conservo los derechos morales sobre mi obra.

En fe de lo cual, firmo la presente.

Atentamente,

Firmado electrónicamente por:
BRAYAN ALEXANDER IGLESIAS ALCIVAR
Validar únicamente con FirmaEC

BRAYAN ALEXANDER IGLESIAS ALCIVAR
C.I.: 1726915927

FORMULARIO PARA ENTREGA DE PROYECTOS EN BIBLIOTECA INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

CT-ANX-2025-ISTER-3

CARRERA:

TECNOLOGÍA UNIVERSITARIA EN ADMINISTRACIÓN Y GESTIÓN COMERCIAL

AUTOR /ES:

BRAYAN ALEXANDER IGLESIAS ALCIVAR

TUTOR (METODOLÓGICO Y ACADÉMICO):

ING. HILBERTH VILLALBA E ING. PATRICIA AREVALO

CONTACTO ESTUDIANTE:

0998603692

CORREO ELECTRÓNICO:

BRAYAN.IGLESIAS2003@GMAIL.COM

TEMA:

PLAN DE NEGOCIOS PARA LA COMERCIALIZACIÓN DE UNA PLATAFORMA DE SIMULACIÓN DE CIBERATAQUES ORIENTADA A LA CONCIENTIZACIÓN DEL PERSONAL EN MIPYMES DE PICHINCHA - CASO ATTACK SIMULATOR

OPCIÓN DE TITULACIÓN:

RESUMEN EN ESPAÑOL:

Attack Simulator se plantea como una respuesta pragmática al eslabón más débil de la ciberseguridad en las MIPYMES de Pichincha: la conducta humana. El proyecto no se limita a la tecnología; combina simulaciones realistas con capacitación personalizada para instaurar una cultura preventiva y duradera, proponiendo un giro desde lo puramente técnico hacia un enfoque pedagógico. El diagnóstico inicial identifica dos cuellos de botella —desconocimiento y ausencia de protocolos— que afectan directamente la resiliencia y la competitividad. En el frente de mercado, a partir de encuestas a 83 representantes, se observa que más del 95% de los incidentes exitosos nace de errores humanos; aun así, existe apertura a invertir en soluciones accesibles, medibles y adaptadas al contexto local. La competencia deja un nicho disponible para propuestas con sello educativo y escalables, donde Attack Simulator puede posicionarse como pionero en Ecuador. En lo técnico, la plataforma se concibe web/cloud, usable desde cualquier navegador, con módulos para seleccionar ataques, ajustar parámetros, auditar historiales y emitir reportes visuales; se apoya en Design Thinking, propuesta de valor y prototipado para alinear funcionalidades con necesidades reales. En lo administrativo, define misión, visión, valores y estructura, se articula con los ODS —innovación, empleo calificado e infraestructura digital— y, vía FODA, reconoce fortalezas (adaptación local) y retos (posicionamiento inicial), orientando estrategias de crecimiento, actualización continua y cercanía con el cliente. Finalmente, la evaluación financiera resulta favorable: VAN de $8.876,57, TIR de 26,42% y relación costo-beneficio de 1,66 (por encima del 12% de tasa de descuento), lo que sugiere factibilidad económica y aporte social.

PALABRAS CLAVE:

Ciberseguridad, MIPYMES, Attack Simulator, Concientización, Viabilidad

ABSTRACT:

Attack Simulator is conceived as a pragmatic response to the weakest link in cybersecurity for MSMEs in Pichincha: human behavior. The project goes beyond technology; it

combines realistic simulations with personalized training to establish a lasting culture of prevention, proposing a shift from a purely technical focus toward a pedagogical approach. The initial diagnosis identifies two main bottlenecks —lack of knowledge and absence of protocols— that directly impact resilience and competitiveness. From a market perspective, based on surveys of 83 representatives, it is observed that more than 95% of successful incidents stem from human errors; nevertheless, there is openness to invest in accessible, measurable, and locally adapted solutions. Competition leaves a niche open for educational and scalable proposals, where Attack Simulator can position itself as a pioneer in Ecuador. Technically, the platform is designed as a web/cloud solution, accessible from any browser, with modules to select attacks, adjust parameters, audit histories, and generate visual reports. It relies on Design Thinking, value proposition, and prototyping to align features with real needs. Administratively, it defines mission, vision, values, and structure; aligns with the SDGs (innovation, qualified employment, and digital infrastructure); and, through a SWOT analysis, recognizes strengths (local adaptation) and challenges (initial market positioning), guiding strategies for growth, continuous updates, and customer engagement. Finally, the financial evaluation is favorable: an NPV of $8,876.57, an IRR of 26.42%, and a cost-benefit ratio of 1.66 (above the 12% discount rate), suggesting both economic feasibility and social contribution.

PALABRAS CLAVE:

Cybersecurity, MSMEs, Attack Simulator, Awareness, Feasibility

Firmado electrónicamente por:
BRAYAN ALEXANDER IGLESIAS ALCIVAR
Validar únicamente con FirmaEC

_____

Firma del Estudiante (AUTOR)

Brayan Alexander Iglesias Alcivar

C.I.: 1726915927

SOLICITUD DE PUBLICACIÓN DEL TRABAJO DE TITULACIÓN

CT-ANX-2025-ISTER-4

Sangolquí, 04 de septiembre del 2025

Sres.-
INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO

Presente

Yo Brayan Alexander Iglesias Alcivar, con C.I.:1726915927 alumno de la Carrera de ADMINISTRACIÓN Y GESTIÓN COMERCIAL, cedo al INSTITUTO SUPERIOR TECNOLÓGICO RUMIÑAHUI CON CONDICIÓN DE UNIVERSITARIO, los derechos de publicaciones del presente trabajo de Titulación en el Repositorio Institucional para hacer uso de todos los contenidos con fines estrictamente académico o de investigación.

Atentamente,

Firmado electrónicamente por:
BRAYAN ALEXANDER IGLESIAS ALCIVAR
Validar únicamente con FirmaEC

_____
Firma del Estudiante
Brayan Alexander Iglesias Alcivar
C.I.: 1726915927

Dedicatoria:

Dedico este trabajo de investigación a mi querido padre, Luis Iglesias, cuya vida se ha caracterizado por un amor profundo, un apoyo incondicional y un sacrificio constante. Gracias por transmitirme los valores más fundamentales desde mi infancia, los cuales me han guiado en cada paso de mi camino.

A mi prometida, Marilyn Quiroz, quien ha sido un pilar fundamental en la consecución de mis metas y en el impulso de mis sueños. Su presencia, apoyo y amor han sido determinantes en cada etapa de mi carrera, y este logro también es suyo, pues juntos hemos construido este triunfo, fruto de años de esfuerzo compartido.

Agradecimientos:

Extiendo también mi gratitud a todas las personas que, con su presencia, contribuyeron a mi proceso de formación y crecimiento durante este viaje académico. Cada uno de ustedes ha dejado una huella imborrable en mi camino, y su apoyo ha sido invaluable.

Resumen:

Attack Simulator se plantea como una respuesta pragmática al eslabón más débil de la ciberseguridad en las MIPYMES de Pichincha: la conducta humana. El proyecto no se limita a la tecnología; combina simulaciones realistas con capacitación personalizada para instaurar una cultura preventiva y duradera, proponiendo un giro desde lo puramente técnico hacia un enfoque pedagógico. El diagnóstico inicial identifica dos cuellos de botella —desconocimiento y ausencia de protocolos— que afectan directamente la resiliencia y la competitividad. En el frente de mercado, a partir de encuestas a 83 representantes, se observa que más del 95% de los incidentes exitosos nace de errores humanos; aun así, existe apertura a invertir en soluciones accesibles, medibles y adaptadas al contexto local. La competencia deja un nicho disponible para propuestas con sello educativo y escalables, donde Attack Simulator puede posicionarse como pionero en Ecuador. En lo técnico, la plataforma se concibe web/cloud, usable desde cualquier navegador, con módulos para seleccionar ataques, ajustar parámetros, auditar historiales y emitir reportes visuales; se apoya en Design Thinking, propuesta de valor y prototipado para alinear funcionalidades con necesidades reales. En lo administrativo, define misión, visión, valores y estructura, se articula con los ODS —innovación, empleo calificado e infraestructura digital— y, vía FODA, reconoce fortalezas (adaptación local) y retos (posicionamiento inicial), orientando estrategias de crecimiento, actualización continua y cercanía con el cliente. Finalmente, la evaluación financiera resulta favorable: VAN de $8.876,57, TIR de 26,42% y relación costo-beneficio de 1,66 (por encima del 12% de tasa de descuento), lo que sugiere factibilidad económica y aporte social.

Palabras claves:

Ciberseguridad, MIPYMES, Attack Simulator, Concientización, Viabilidad

Abstract:

Attack Simulator is conceived as a pragmatic response to the weakest link in cybersecurity for MSMEs in Pichincha: human behavior. The project goes beyond technology; it combines realistic simulations with personalized training to establish a lasting culture of prevention, proposing a shift from a purely technical focus toward a pedagogical approach. The initial diagnosis identifies two main bottlenecks —lack of knowledge and absence of protocols— that directly impact resilience and competitiveness. From a market perspective, based on surveys of 83 representatives, it is observed that more than 95% of successful incidents stem from human errors; nevertheless, there is openness to invest in accessible, measurable, and locally adapted solutions. Competition leaves a niche open for educational and scalable proposals, where **Attack Simulator** can position itself as a pioneer in Ecuador. Technically, the platform is designed as a **web/cloud solution**, accessible from any browser, with modules to select attacks, adjust parameters, audit histories, and generate visual reports. It relies on **Design Thinking, value proposition, and prototyping** to align features with real needs. Administratively, it defines mission, vision, values, and structure; aligns with the **SDGs** (innovation, qualified employment, and digital infrastructure); and, through a **SWOT analysis**, recognizes strengths (local adaptation) and challenges (initial market positioning), guiding strategies for growth, continuous updates, and customer engagement. Finally, the financial evaluation is favorable: an **NPV of $8,876.57**, an **IRR of 26.42%**, and a **cost-benefit ratio of 1.66** (above the 12% discount rate), suggesting both economic feasibility and social contribution.

Keywords:

Cybersecurity, MSMEs, Attack Simulator, Awareness, Feasibility

Tabla de contenido

Tabla de Ilustraciones

CAPÍTULO I: INFORMACIÓN GENERAL DEL PROYECTO

1.1. Identificación del proyecto y problema

Desde mi punto de vista, una de las grandes ironías de la era digital es que, aunque las herramientas tecnológicas han avanzado a pasos agigantados, muchos usuarios —sobre todo en las MIPYMES— siguen siendo el "punto ciego" de la seguridad digital (Institute, 2022). Justamente por eso decidí enfocar este plan de negocios en la implementación de Attack Simulator, una plataforma europea que no solo simula ciberataques, sino que también permite medir y fortalecer el nivel de conciencia del personal ante amenazas reales como el phishing, el ransomware o los fraudes tipo.

¿Y por qué hacerlo en Pichincha? Porque esta provincia, al ser una de las más activas empresarialmente, concentra una gran cantidad de pequeñas y medianas empresas que dependen de la tecnología pero no siempre entienden sus riesgos. Es evidente que muchas de estas organizaciones han subestimado la importancia del comportamiento humano como un factor de vulnerabilidad. A pesar de que usan herramientas digitales diariamente, son pocas las que cuentan con verdaderas políticas de ciberseguridad o con sistemas para evaluar internamente su preparación frente a un ataque.

Lo preocupante es que esta falta de conciencia genera una especie de "tranquilidad falsa" dentro de las organizaciones. Los directivos creen que con un antivirus o un firewall ya están protegidos, sin considerar que el error humano sigue siendo la causa número uno de los ciberataques exitosos. Según varios estudios (y no solo uno aislado), más del 85% de los

incidentes de seguridad están relacionados con acciones humanas (Verizon, 2023) —algo que, sinceramente, no podemos seguir ignorando.

Por eso considero que una herramienta como Attack Simulator es más que una solución tecnológica; es una propuesta educativa, proactiva y adaptada a la realidad local. Su capacidad de identificar qué tan preparados están los colaboradores y luego guiarlos con capacitación personalizada según sus debilidades, la convierte en una herramienta valiosa no solo para reducir riesgos, sino para crear una cultura digital más responsable. En resumen, si las MIPYMES quieren seguir creciendo y ser sostenibles en un mundo cada vez más conectado, deben empezar a fortalecer a su gente, porque al final, la seguridad digital empieza por la conciencia.

1.2. Tema

CIIU: G465102

Plan de negocios para la comercialización de una plataforma de simulación de ciberataques orientada a la concientización del personal en MIPYMES de Pichincha - Caso Attack Simulator

1.3. Antecedentes y contexto

1.3.1. Contexto Histórico

A lo largo de la última década, he notado cómo el discurso de “transformación digital” ha invadido todos los sectores en Ecuador. Y sí, es cierto que muchas empresas han modernizado sus operaciones, se han conectado a la nube o han empezado a usar software de gestión, pero... ¿qué tan segura ha sido esa transición? Desde mi experiencia y observación, puedo decir que el

entusiasmo por digitalizarse no ha ido acompañado por una preocupación real por la ciberseguridad.

En provincias como Pichincha, donde se concentra una parte vital del tejido empresarial del país, las MIPYMES son el motor económico. Pero también, lamentablemente, representan una de las capas más vulnerables ante ataques cibernéticos. ¿La razón? No es solo la falta de inversión en tecnología, sino sobre todo la ausencia de conciencia en el personal.

Phishing, ransomware, suplantación de identidad... estos términos deberían sonar alarmantes para cualquier gerente, pero en muchos casos ni siquiera se conocen con claridad. Y esa desconexión entre el uso de tecnología y la preparación humana es, desde mi punto de vista, el mayor riesgo que enfrentan las pequeñas y medianas empresas hoy.

Una observación importante aquí es que el problema no es únicamente técnico: es cultural, es educativo. Por eso la solución no puede limitarse a instalar software, sino que debe involucrar a las personas. Y justamente allí es donde Attack Simulator puede marcar una diferencia real.

El error humano se ha consolidado como uno de los principales vectores de ataques cibernéticos. La falta de capacitación del personal y el desconocimiento de las amenazas digitales ha llevado a que muchas empresas sufran pérdidas económicas, fuga de información y afectación a la reputación, sin contar con estrategias preventivas claras.

1.3.2. Estudios o Investigaciones Previas

Diversos informes internacionales y locales han evidenciado que entre el 85% y 95% de los ciberataques exitosos tienen como origen un descuido o error del usuario final. En Ecuador, el Informe Nacional de Ciberseguridad 2023 elaborado por la Asociación Ecuatoriana de Seguridad Informática, destacó que más del 70% de las MIPYMES no han realizado capacitaciones formales en seguridad digital. (Informática, Informe Nacional de Ciberseguridad 2023, 2023)

A nivel internacional, estudios como el de Verizon Data Breach Investigations Report 2023 refuerzan que el phishing sigue siendo la técnica más utilizada por los ciberdelincuentes (Verizon, 2023), con un crecimiento sostenido en correos dirigidos a empleados de empresas pequeñas. Asimismo, instituciones como el NIST (National Institute of Standards and Technology) y la ISO/IEC 27001 promueven la concientización y simulación como prácticas fundamentales para mitigar el riesgo interno (Standardization, 2022).

En el ámbito académico, universidades ecuatorianas como la Escuela Politécnica Nacional y la Pontificia Universidad Católica del Ecuador han realizado investigaciones que demuestran la efectividad de las simulaciones de ataque como herramienta educativa y preventiva en entornos corporativos.

1.3.3. Beneficios Esperados

La implementación de una plataforma como Attack Simulator permitirá a las MIPYMES de Pichincha contar con una herramienta de diagnóstico y formación que transformará al

personal operativo y administrativo en un elemento clave dentro de las estrategias de defensa digital. Entre los beneficios más relevantes se espera:

- Identificación del nivel de riesgo humano en la empresa frente a ciberataques.
- Reducción del porcentaje de errores humanos ante ataques informáticos mediante entrenamiento personalizado.
- Disminución del impacto económico y operativo ocasionado por incidentes de seguridad.
- Cumplimiento progresivo de estándares internacionales de ciberseguridad.
- Mejora de la cultura digital organizacional, fomentando la responsabilidad individual frente a la seguridad de la información.

1.4. Justificación

A criterio del autor, uno de los grandes desafíos que enfrentan las MIPYMES en Pichincha no es simplemente "subirse al tren" de la digitalización, sino hacerlo de forma segura. El problema es que, aunque muchas ya han adoptado tecnología, siguen dejando una puerta abierta en un punto crítico: el factor humano. Es decir, esas personas dentro de la organización que, sin mala intención, pueden caer en un engaño digital y abrirle la puerta a un ciberataque.

La experiencia y los datos coinciden en un punto incómodo: la mayoría de los incidentes informáticos en pequeñas y medianas empresas no se originan por fallas técnicas, sino por errores humanos. De hecho, más del 95 % de los ataques exitosos tienen esta causa. Y sí, es un número que asusta. Aun así, muchas empresas siguen sin aplicar programas formales de

concientización o sin medir realmente qué tan preparados están sus colaboradores. Surge una pregunta inevitable: ¿cómo se puede combatir una amenaza que ni siquiera se sabe reconocer?

Bajo esa lógica, la solución no puede quedarse únicamente en lo tecnológico; tiene que ser también pedagógica y estratégica. Aquí es donde entra este proyecto con Attack Simulator, una plataforma que no solo recrea ataques reales para medir la reacción de los usuarios, sino que personaliza la capacitación en función de las fallas detectadas. Eso marca la diferencia: no es un curso genérico, sino una intervención específica basada en evidencia real.

No se trata solo de evitar pérdidas económicas o cumplir con la Ley Orgánica de Protección de Datos Personales (Ecuador, 2021) —aunque eso ya es un gran incentivo—. Es, sobre todo, un cambio de mentalidad: que cada empleado pase de ser el eslabón débil a convertirse en un punto fuerte de defensa. Y en un contexto como el nuestro, eso es clave para construir una cultura de ciberseguridad sólida y duradera.

Finalmente, este tipo de iniciativas también aporta un valor reputacional: las empresas que adopten este modelo no solo serán más seguras, sino que podrán presentarse como pioneras y responsables frente a sus clientes y socios. En definitiva, proteger la información hoy es asegurar la continuidad y credibilidad de los negocios mañana.

1.5. Objetivos de la Investigación

1.5.1. Objetivo General

Analizar la viabilidad de comercializar una solución basada en Attack Simulator que ayude a las MIPYMES de Pichincha a identificar vulnerabilidades humanas frente a

ciberamenazas reales, capacitar a su personal de forma práctica y personalizada, y, con ello, fomentar una cultura organizacional centrada en la ciberseguridad. La intención no es solo reducir el riesgo inmediato, sino impulsar un cambio sostenido en la forma en que las empresas conciben y gestionan su seguridad digital.

1.5.2. Objetivos Específicos

- Estimar la viabilidad económica y operativa de la comercialización del Attack Simulator, proyectando costos, posibles precios de venta, márgenes de ganancia y modelos de implementación que aseguren su sostenibilidad a largo plazo.
- Evaluar el nivel actual de vulnerabilidad digital en las MIPYMES de Pichincha mediante el análisis de prácticas, conocimientos y percepciones del personal, con el fin de identificar brechas que el Attack Simulator podría cubrir de forma efectiva.
- Determinar la percepción y disposición de las MIPYMES a invertir en soluciones de concientización y simulación de ciberataques, considerando factores como presupuesto, prioridades organizacionales y experiencias previas en seguridad digital.
- Analizar la propuesta de valor del Attack Simulator frente a soluciones similares disponibles en el mercado ecuatoriano e internacional, evaluando su diferenciación en términos de funcionalidad, escalabilidad y adaptación al contexto local.

1.6. Impactos

1.6.1. Social

En el ecosistema empresarial de Pichincha, muchas MIPYMES siguen viendo la ciberseguridad como un asunto puramente técnico, cuando en realidad el factor humano es el que marca la diferencia. La implementación de Attack Simulator representa una inversión social tanto como tecnológica, porque empodera a cada empleado para convertirse en un eslabón de protección y no de vulnerabilidad.

El aprendizaje que se genera no se queda encerrado en la oficina: viaja al hogar, a las interacciones familiares y a la comunidad. Este efecto multiplicador de buenas prácticas es especialmente valioso en un contexto donde las brechas digitales siguen siendo una realidad. Además, la herramienta tiene un carácter inclusivo: no distingue entre rangos jerárquicos, todos participan y todos mejoran, contribuyendo a una cultura organizacional más sólida y equitativa en materia de seguridad digital.

1.6.2. Económico

En la práctica, muchas empresas pequeñas y medianas reaccionan a la ciberseguridad solo después de un ataque, cuando las pérdidas ya son inevitables. El costo no es únicamente monetario: implica tiempo, clientes, reputación y, en algunos casos, sanciones legales. Attack Simulator propone romper ese ciclo reactivo y migrar hacia una estrategia preventiva que disminuya la probabilidad de interrupciones y reduzca gastos de recuperación.

Pero la viabilidad económica de esta solución no está únicamente en el ahorro que genera. Una empresa que demuestra responsabilidad digital gana también un valor reputacional

que puede abrirle puertas a nuevos clientes, licitaciones y alianzas estratégicas. En consecuencia, la inversión en esta herramienta no solo protege lo que ya se tiene, sino que también potencia oportunidades de crecimiento a mediano y largo plazo.

1.7. Beneficiarios

1.7.1. Directos

- Colaboradores de las MIPYMES: Son el eje central del cambio. Al participar en simulaciones y recibir formación personalizada, no solo fortalecen su capacidad de respuesta ante ataques, sino que también se empoderan como el primer nivel de defensa digital dentro de la organización.
- Líderes empresariales y equipos de TI: Requieren información clara para decidir. Attack Simulator les proporciona diagnósticos precisos, comparativas de riesgo y planes de mejora, permitiéndoles actuar con datos reales y no con suposiciones.
- Empresa implementadora: Colocar en el mercado un producto que responde a una necesidad urgente y poco atendida representa una ventaja competitiva clara, abriendo el camino hacia un posicionamiento sólido y crecimiento sostenido en el sector tecnológico ecuatoriano.

1.7.2. Indirectos

- Clientes, proveedores y socios: Una empresa más segura genera relaciones comerciales más confiables, reduce riesgos compartidos y refuerza la cadena de valor, construyendo un entorno empresarial más sólido.

- Ecosistema empresarial de Pichincha: La adopción masiva de soluciones como Attack Simulator eleva el estándar de ciberseguridad a nivel provincial, mejorando la competitividad frente a otras regiones.
- Familias y entorno personal de los empleados: El conocimiento adquirido se traslada al hogar, fortaleciendo la seguridad digital de sus familias y multiplicando el impacto positivo fuera del ámbito laboral.

CAPÍTULO II: ESTUDIO DE MERCADO

2.1. Resultados esperados del estudio de mercado

Desde mi punto de vista, todo estudio de mercado debe ser más que una recopilación de datos; debe ofrecer respuestas útiles que nos ayuden a tomar decisiones reales. En este caso, lo que buscamos con esta investigación es entender hasta qué punto las MIPYMES de Pichincha están conscientes de los riesgos digitales que enfrentan, y si están listas —o al menos interesadas— en adoptar una solución como Attack Simulator.

Considero que los principales logros esperados de este estudio son:

- Reconocer qué tan vulnerables se sienten las empresas ante los ciberataques.
- Evaluar el nivel de preparación de su personal ante amenazas digitales, lo que en muchos casos es una "caja negra" que nunca se revisa.
- Medir si existe una disposición real a invertir en herramientas preventivas, más allá del discurso.
- Entender si ya existen soluciones parecidas en el mercado, qué ofrecen, y qué no están logrando.
- Y, algo clave: reunir la información suficiente para diseñar estrategias de mercado que conecten con lo que realmente preocupa a estas empresas.

2.2. Demanda

En lo personal, me preocupa que muchas MIPYMES ecuatorianas no dimensionen la magnitud del riesgo digital que enfrentan. Y no lo digo desde la teoría, sino porque los datos son

contundentes. Según el informe de Kaspersky (Kaspersky, s.f.), Ecuador no solo está en la lista de países más afectados por ciberataques en América Latina... es el primero.

Este dato por sí solo ya justifica la necesidad urgente de soluciones como la que proponemos. Pero si miramos más de cerca, encontramos razones aún más preocupantes:

- Un 13,3% de usuarios en Ecuador ha sido víctima de phishing (Tapia, 2025). Esa cifra nos coloca entre los países con mayor número de afectados a nivel mundial. ¿Y aún creemos que no nos va a pasar?
- El uso de software pirata y el trabajo remoto (Alliance, 2022) (Interpol, s.f.) (muy común en MIPYMES) abren la puerta a amenazas silenciosas que comprometen la información sensible sin que nadie se dé cuenta.
- Los dispositivos móviles también se han vuelto blancos de ataques: troyanos, adware, accesos remotos... Es decir, la amenaza no está solo en la computadora de la oficina.
- Y lo más preocupante: la mayoría de los ataques son posibles por errores humanos (Verizon, 2023). No basta con tener un antivirus. Si un colaborador cae en una trampa, todo el sistema se viene abajo.

En este contexto, lo lógico —y necesario— es impulsar herramientas como Attack Simulator, que no solo muestran el nivel real de vulnerabilidad, sino que permiten educar y corregir desde adentro. Las empresas no solo buscan protegerse, también necesitan cumplir con leyes como la LOPDP (Ecuador, 2021), cuidar su reputación y asegurar su operación. La demanda ya está ahí; lo que hace falta es que las soluciones sean accesibles, útiles y enfocadas en las personas.

2.3. Oferta

En el contexto actual, la oferta de soluciones de ciberseguridad en Ecuador —especialmente dirigidas a las MIPYMES— sigue siendo limitada, poco especializada y, en muchos casos, basada en enfoques cualitativos o genéricos que no consideran el verdadero costo de una violación de seguridad. A pesar de que el país enfrenta amenazas cibernéticas crecientes, la mayoría de las organizaciones carece de herramientas eficaces para gestionar el riesgo con base en métricas reales y análisis cuantitativo.

Los costos derivados de un ciberataque —como pérdida de productividad, incumplimientos legales, pérdida de reputación y daño financiero (Security, 2023)— demuestran que las empresas necesitan soluciones preventivas, escalables y medibles. Sin embargo, la oferta local sigue centrada en medidas técnicas reactivas (antivirus, firewalls, respaldos), dejando de lado el factor humano, que representa uno de los eslabones más débiles de la seguridad.

El proyecto Attack Simulator se posiciona como una oferta innovadora en este contexto limitado. A diferencia de las soluciones tradicionales, Attack Simulator se centra en la simulación realista de ciberataques vía correo electrónico (como phishing, ransomware, suplantación de identidad, etc.), y permite:

- Medir el comportamiento real de los empleados ante un ataque simulado, identificando los eslabones más débiles.
- Aplicar programas de concientización personalizados para reducir los errores humanos que facilitan las brechas de seguridad.

- Presentar reportes cuantitativos del nivel de riesgo humano, lo cual alinea esta solución con los principios del Valor al Riesgo (CyVaR) (Forum, 2022).
- Cumplir con lo dispuesto en la Ley Orgánica de Protección de Datos Personales, que exige medidas organizativas y técnicas de seguridad.

Por tanto, Attack Simulator no solo cubre una brecha de mercado desatendida, sino que ofrece una herramienta preventiva, medible y rentable frente a las pérdidas que generan los ciberataques. Además, al estar orientada a MIPYMES, ofrece un modelo asequible, con resultados tangibles y de rápida implementación.

2.4. Ficha de observación

La ficha de observación es una herramienta metodológica utilizada para evaluar y comparar (Hernández, 2014) de forma sistemática a la competencia directa en el mercado de soluciones digitales de ciberseguridad. Esta ficha permite recoger información clave sobre características, funcionalidades, precios, canales de comunicación, atención al cliente, y propuesta de valor de al menos cuatro competidores relevantes del sector.

Tabla 1. *Ficha de observación, competencia Attack Simulator*

Parámetro / Producto	Attack Simulator	ITSEGUINFO KnowBe4	IMPUTONE PhishingBox	GMS Hook Security (Hook+)	NGS SECURITY AttackIQ Flex – BAS
Simulación de ataques variados	Sí	Sí	Sí	Sí	Sí
Enfoque en el factor humano	Alto	Alto	Alto	Bajo	Alto
Contenido educativo personalizado	Sí	Sí	Limitado	No	Sí
Reportes automatizados	Detallados	Sí	Sí	Parcial	Sí

Soporte local y en español	Regional	Parcial	Parcial	Parcial	Sí
Precio o escalabilidad	Asequible	Elevado	Alto	Intermedio	Alto
Cumplimiento normativo	Ley Datos EC	GDPR	GDPR	Limitado	GDPR
Facilidad de uso	Alta	Media	Media	Alta	Media
Actualización y mantenimiento	Constante	Sí	Sí	Sí	Sí
Precio Estimado Mensual	$ 180,00	$ 215,00	$ 244,00	$ 350,00	$ 110,00

Autor: *Elaboración propia*

El análisis comparativo realizado entre Attack Simulator y cuatro plataformas líderes en el mercado evidencia que, si bien existen soluciones robustas a nivel internacional, muchas de ellas presentan limitaciones en cuanto a accesibilidad, personalización, soporte regional y costos, especialmente cuando se pretende aplicar en el contexto de las MIPYMES de Pichincha – Ecuador.

Attack Simulator destaca por ofrecer una solución equilibrada, con un enfoque fuerte en la concientización del factor humano, generación de reportes detallados, soporte en idioma local y una estructura de costos accesible. Esta combinación permite que el producto sea especialmente viable para pequeñas y medianas empresas que buscan fortalecer su resiliencia cibernética sin realizar grandes inversiones.

Además, el cumplimiento con normativas locales como la Ley Orgánica de Protección de Datos Personales del Ecuador representa un valor agregado frente a competidores extranjeros que aún no contemplan este marco normativo.

Attack Simulator se posiciona como una alternativa eficaz, adaptable y competitiva, con claras ventajas diferenciales frente a las soluciones tradicionales disponibles en el mercado.

2.5. Encuestas y presentación de resultados

2.5.1. Encuesta

La encuesta representa una herramienta que se ubica entre la observación y la experimentación (Kerlinger, 2002). Su función principal es recopilar información sobre hechos observables y, cuando no es posible llevar a cabo un experimento, se recurre a interrogar directamente a los participantes sobre dichos hechos. Por ello, la encuesta se considera un método descriptivo eficaz para explorar ideas, detectar necesidades, conocer preferencias y analizar hábitos de uso. Generalmente se emplean preguntas cerradas, ya que facilitan tanto el análisis de datos como la comparación entre respuestas.

2.5.2. Población y muestra

En el Distrito Metropolitano de Quito (DMQ) existen 301.173 empresas registradas (Quito, 2024), de las cuales aproximadamente el 93% corresponden a microempresas. Además, estas representan el 89% del total empresarial de la provincia de Pichincha, según datos del Instituto Nacional de Estadística y Censos (INEC, 2023a) (Censos, 2023). Para los fines de esta investigación, la población objetivo estará compuesta por las pequeñas y medianas empresas (MIPYMES) ubicadas en el DMQ, con un total de 19.602 unidades. Este segmento ha sido seleccionado por su mayor grado de formalización y porque permite evidenciar con mayor claridad el impacto de la transformación digital, como el comercio electrónico, en el desarrollo económico de la región.

$$n = \frac{N * Z^2 * p * q}{e^2(N-1) + z^2 * p * q}$$

Tabla 2. *Datos del cálculo de la muestra*

Parámetro	Insertar Valor	Significado
N	19,602	Tamaño de la población o Universo
Z	2,33	Parámetro estadístico que depende el nivel de confianza (NC)
p	96,00%	Probabilidad de que no ocurra el evento estudiado
q	4,00%	Probabilidad de que no ocurra el evento estudiado
e	5,00%	Error de estimación máximo aceptado.

Autor: *Elaboración propia*

- Tamaño de muestra
- "n" =
- **83**

2.5.3. Análisis Y Difusión De Resultados

Este capítulo, más que un simple apartado de datos y gráficas, se siente como ponerle un espejo a una realidad que, curiosamente, muchos prefieren no mirar: la fragilidad humana frente a las amenazas digitales en las MIPYMES. La encuesta se aplicó a 83 representantes de empresas del Distrito Metropolitano de Quito, entre gerentes, jefes de área y responsables de TI. Es decir, personas que conviven a diario con la tensión entre sacar adelante el negocio y, al mismo tiempo, protegerlo de un mundo digital cada vez más hostil.

Pero aquí está el detalle: la intención no fue llenar tablas por llenar, sino escuchar. Escuchar lo que estas personas piensan, lo que sienten, y lo que a veces no dicen directamente, pero se lee entre líneas. Y lo que encontramos es inquietante: muchas amenazas digitales siguen viéndose como algo lejano, casi hipotético, cuando en realidad están a la vuelta de la esquina. ¿No es paradójico que se invierta en nuevas tecnologías, pero se descuide preparar a quienes las usan?

Los resultados se organizaron en ejes temáticos, con gráficos y tablas que facilitan la lectura, pero el verdadero valor no está en las figuras, sino en lo que revelan. La mayoría de las empresas aún carece de una estrategia clara de concientización. Y aquí surge la pregunta que incomoda: si hoy no están listas, ¿qué pasará cuando las amenazas sean más sofisticadas y frecuentes?

Este análisis también permitió ver que soluciones como Attack Simulator no solo serían bien recibidas, sino que podrían llenar un vacío evidente: pasar de la reacción al ataque, a la prevención y la capacitación estratégica. La viabilidad no se limita a lo técnico o económico; hay

un terreno emocional y cultural que necesita ser trabajado. Porque, al final, la ciberseguridad no es un software que se instala y ya, sino un cambio de mentalidad que debe ser cultivado.

Pregunta 1: Nombre de su Empresa

Se logró un total de 96 empresas encuestadas

Pregunta 2: ¿A qué sector pertenece su empresa?

Figura 1.

Resultados de encuesta, pregunta 2

Autor: *Elaboración propia*

Análisis e interpretación

El 34% de empresas encuestadas, fueron empresas de “servicios”

Pregunta 3: ¿Cuántos empleados tiene su empresa actualmente?

Figura 2.

Resultados de encuesta, pregunta 3

Autor: *Elaboración propia*

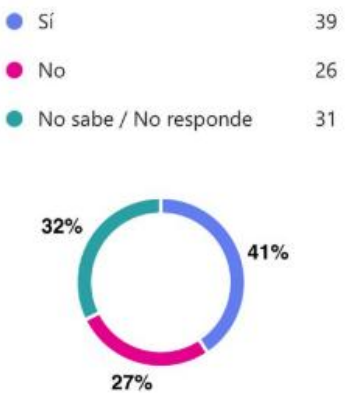
Análisis e interpretación

Del total de encuestados el 36% tiene de 26 a 50 empleados, lo que representa a pequeñas empresas.

Pregunta 4: ¿Ha sufrido su empresa algún intento o ataque cibernético en los últimos 12 meses?

Figura 3.

Resultados de encuesta, pregunta 4



Autor: *Elaboración propia*

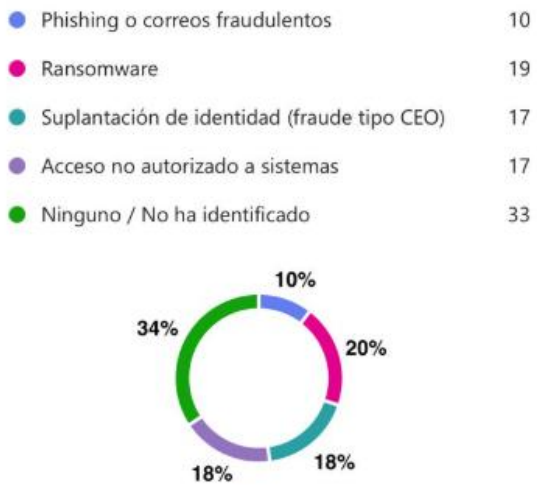
Análisis e interpretación

Del total de empresas encuestadas el 41% a sufrido ataques cibernéticos en los últimos 12 meses

Pregunta 5: ¿Qué tipo de ataques ha identificado en su organización?

Figura 4.

Resultados de encuesta, pregunta 5



Autor: *Elaboración propia*

Análisis e interpretación

Del total de encuestados el 34% no ha logrado identificar que tipo de ataque informático a sufrido.

Pregunta 6: ¿Considera que el comportamiento del personal representa un riesgo para la seguridad digital de la empresa?

Figura 5.

Resultados de encuesta, pregunta 6

Autor: *Elaboración propia*

Análisis e interpretación

Por lo menos el 45% de los encuestados admiten o reconocen que el comportamiento del personal representa un riesgo de seguridad informática.

Pregunta 7: ¿Su empresa realiza capacitaciones en ciberseguridad para su personal?

Figura 6.

Resultados de encuesta, pregunta 7

Autor: *Elaboración propia*

Análisis e interpretación

El 33% de los encuestados realiza capacitaciones en ciberseguridad esporadicamente

Pregunta 8: ¿Con qué frecuencia los empleados reciben alertas o recomendaciones sobre buenas prácticas de ciberseguridad?

Figura 7.

Resultados de encuesta, pregunta 8

Autor: *Elaboración propia*

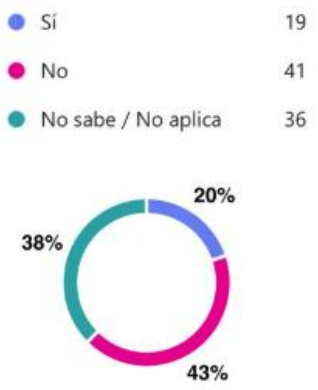
Análisis e interpretación

El 44% de los encuestados tienen campañas de alertas o recomendaciones sobre buenas prácticas de ciberseguridad.

Pregunta 9: ¿Cuenta su empresa con algún sistema para evaluar el nivel de conciencia en ciberseguridad del personal?

Figura 8.

Resultados de encuesta, pregunta 9



Autor: *Elaboración propia*

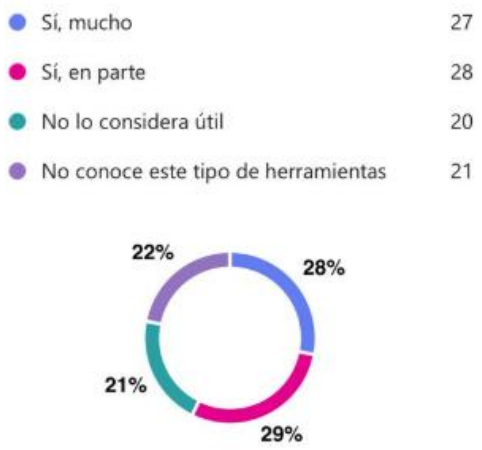
Análisis e interpretación

El 43% de los encuestados no sabe de sistemas para evaluar el nivel de conciencia en ciberseguridad.

Pregunta 10: ¿Considera que una plataforma de simulación de ataques informáticos ayudaría a mejorar la preparación de su equipo?

Figura 9.

Resultados de encuesta, pregunta 10



Autor: *Elaboración propia*

Análisis e interpretación

El 29% de las empresas encuestadas consideran que es importante una plataforma de simulación de ataques informáticos para mejorar la preparación de los colaboradores.

Pregunta 11: ¿Estaría dispuesto a implementar una solución de simulación y capacitación en ciberseguridad si el costo es accesible y se adapta al tamaño de su empresa?

Figura 10.

Resultados de encuesta, pregunta 11

Autor: *Elaboración propia*

Análisis e interpretación

El 42% de los encuestados esta dispuesto a implementar una solución de simulación y capacitación en ciberseguridad siempre y cuando el costo sea accesible y se le presente información mucho mejor.

Pregunta 12: ¿Cuánto estaría dispuesto a invertir mensualmente por una herramienta que ayude a reducir los riesgos humanos en ciberseguridad?

Figura 11.

Resultados de encuesta, pregunta 12

Autor: *Elaboración propia*

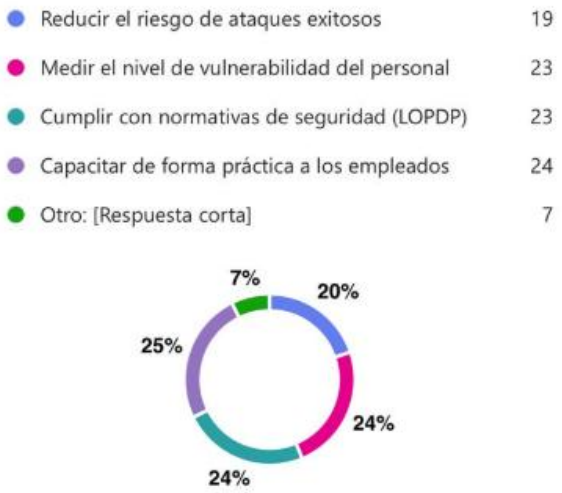
Análisis e interpretación

Hablando de un servicio mensual, el 41% de los encuestados invertiría entre $30 y $100 dólares mensuales por un sistema de simulación de ataques

Pregunta 13: ¿Qué beneficio considera más importante de una solución como Attack Simulator?

Figura 12.

Resultados de encuesta, pregunta 13



Autor: *Elaboración propia*

Análisis e interpretación

El 25% de las empresas encuestadas considera que es muy importante capacitar a los empleados de formas practicas y aprecian este punto como clave para contratar herramientas como Attack Simulator

2.6. Estrategias de mercado

A medida que fui analizando las principales plataformas que existen actualmente en el mercado de la concientización en ciberseguridad, me di cuenta de que muchas de ellas no están realmente pensadas para las necesidades ni las posibilidades de las MIPYMES ecuatorianas. Desde mi punto de vista, ahí radica precisamente la oportunidad: ofrecer una solución que no solo sea funcional, sino también realista y contextualizada. A partir de ese análisis, se definieron varias estrategias para posicionar Attack Simulator en Pichincha con fuerza, coherencia y propósito.

Estrategia de diferenciación por valor

Considero que el mayor activo de Attack Simulator no es su tecnología en sí, sino el enfoque que propone: educativo, personalizado y alineado a la normativa nacional. No se trata solo de simular ataques, sino de transformar la cultura digital dentro de las empresas. En este sentido, su valor diferencial es que está hecha pensando en el usuario final —los empleados— y no solo en cumplir con requisitos técnicos.

Estrategia de penetración en el mercado local

Una observación importante que no podemos ignorar es que muchas de las plataformas competidoras son costosas y, en la práctica, inaccesibles para la mayoría de las MIPYMES. Por eso, proponemos un modelo de precios justo, flexible y escalable, que se adapte al tamaño y posibilidades reales de estas empresas. No se trata de abaratar por competir, sino de democratizar el acceso a una solución efectiva.

Estrategia de alianzas estratégicas

Desde mi experiencia, los gremios empresariales, cámaras de comercio y universidades tecnológicas son aliados naturales para este tipo de iniciativas. Por eso, planteamos generar convenios que nos permitan multiplicar el alcance, construir credibilidad y acceder a bases de datos de tomadores de decisión que ya confían en estas instituciones.

Estrategia de concientización y educación

Mucho antes de vender una herramienta, hay que sembrar conciencia. ¿Cómo pretendemos que las empresas inviertan en ciberseguridad si no entienden la magnitud del

riesgo? Por eso, diseñaremos campañas informativas con un enfoque pedagógico: webinars, infografías, contenidos en redes y casos reales locales. Queremos que Attack Simulator sea reconocido no solo como una plataforma, sino como una fuente confiable de aprendizaje continuo.

Estrategia digital multicanal

Hoy más que nunca, la presencia digital define la reputación. Por eso, creemos que es clave estar donde están los tomadores de decisiones: en LinkedIn, en Google, en su bandeja de entrada. Usaremos herramientas como SEO, Google Ads, email marketing y redes sociales para posicionar la solución de forma estratégica y directa.

Estrategia de prueba gratuita y resultados tangibles

Finalmente, y esto lo aprendí en carne propia con otros productos tecnológicos, nada convence más que ver los resultados por uno mismo. Por eso, ofreceremos pruebas gratuitas con reportes inmediatos. Cuando una empresa ve en pocos días las vulnerabilidades de su equipo, la decisión de invertir ya no es un gasto: se vuelve una necesidad urgente.

2.7. Propuesta de valor digital

En un entorno digital cada vez más amenazado por ataques cibernéticos y en el que las MIPYMES de Pichincha enfrentan retos crecientes en términos de seguridad digital y preparación del personal, se hace evidente la necesidad de soluciones accesibles, efectivas y adaptadas al tamaño y capacidad operativa de estas empresas. Los resultados de la investigación revelan que:

- Más del 47% de las empresas han sufrido algún intento o ataque cibernético en los últimos 12 meses.
- El 83% de los encuestados considera que el comportamiento del personal representa un riesgo medio a alto para la seguridad digital.
- El 74% no cuenta con un sistema para evaluar el nivel de conciencia en ciberseguridad del personal.
- Más del 80% está dispuesto a implementar soluciones de capacitación si el costo es accesible.
- El 57% considera que capacitar de forma práctica, medir vulnerabilidades humanas y cumplir normativas son los principales beneficios esperados de una solución.

En este contexto, nuestra propuesta de valor digital se construye sobre los siguientes pilares:

- Capacitación práctica basada en simulaciones reales

Attack Simulator ofrece una plataforma digital interactiva que permite a los colaboradores de las MIPYMES aprender mediante escenarios reales de ciberataques como phishing, ransomware y suplantación de identidad. Esta metodología activa y basada en errores controlados permite aprender haciendo, reduciendo la curva de aprendizaje y mejorando la retención del conocimiento.

- Evaluación continua del nivel de conciencia en ciberseguridad

La herramienta incluye módulos de evaluación continua que permiten medir el nivel de exposición al riesgo humano en cada organización. Los responsables pueden acceder a reportes visuales que identifican las principales debilidades del personal y tomar decisiones preventivas más informadas.

- Adaptabilidad a la estructura y tamaño de la empresa

A diferencia de soluciones robustas y costosas dirigidas a grandes corporaciones, nuestra plataforma ha sido diseñada exclusivamente para pequeñas y medianas empresas, permitiendo planes flexibles y escalables. Los costos se ajustan al tamaño de cada empresa y garantizan un retorno de inversión mediante la reducción del riesgo de incidentes.

- Cumplimiento normativo y respaldo legal

Attack Simulator ayuda a las MIPYMES a cumplir con la Ley Orgánica de Protección de Datos Personales (LOPDP) (Ecuador, 2021) mediante la implementación de medidas organizativas y técnicas exigidas por la normativa, lo que contribuye a evitar sanciones y mejorar la reputación institucional.

- Concientización organizacional a largo plazo

El enfoque de nuestra solución no es solo técnico, sino cultural. Buscamos que las organizaciones desarrollen una cultura de ciberseguridad desde el liderazgo hasta el personal operativo, promoviendo prácticas seguras de manera sistemática y sostenida.

- Plataforma amigable y de fácil implementación

A través de un entorno digital intuitivo y completamente en español, cualquier empresa puede comenzar a utilizar la plataforma con mínima asistencia técnica. Esto garantiza una implementación rápida y eficiente, incluso sin departamentos especializados en tecnología.

Conoce más sobre nuestra propuesta visual y conceptual a través de nuestro sitio web interactivo:

Tabla 3. *Redes Sociales y links de acceso*

	https://www.gisfal.com/attack-simulator
	https://www.facebook.com/share/19CGnvS4pm/?mibextid=wwXIfr
	https://www.canva.com/design/DAGfYTde14Q/Vq3ZJHPOLukUN11GOialYg/view?utm_content=DAGfYTde14Q&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=had023f7b8b
	https://www.instagram.com/gisfalec?utm_source=ig_web_button_share_sheet&igsh=MWRscDRybGtvaDJpMw==

CAPÍTULO III: ESTUDIO TÉCNICO

3.1. Localización

Una buena localización puede facilitar el acceso a nuestros clientes, mejorar la percepción de nuestra marca (Kotler, 2016), optimizar tiempos de respuesta y conectividad, e incluso fortalecer alianzas estratégicas. Si bien gran parte de nuestra operación puede gestionarse virtualmente, tener una oficina en una zona adecuada nos permite construir confianza, agendar reuniones presenciales efectivas y mantener una presencia cercana a los tomadores de decisiones empresariales.

Además, elegir una zona bien conectada, con infraestructura tecnológica, cercanía a polos de desarrollo económico y acceso a talento humano, potencia la eficiencia operativa y la escalabilidad del proyecto.

Tabla 4. *Factor de localización*

FACTORES DE LOCALIZACION	PONDERACION DE FACTORES	ALTERNATIVAS					
		QUITO NORTE (Isla Seymour y Rio Coca)		SANGOLQUI (Parque Turismo)		CONOCOTO	
		VALOR	CALIFICACION	VALOR	CALIFICACION	VALOR	CALIFICACION
Accesibilidad y transporte (movilidad, rutas, tráfico)	15	5	75	5	75	5	75
Cercanía a clústeres empresariales y tecnológicos	15	4	60	3	45	5	75
Infraestructura tecnológica y servicios básicos	15	5	75	3	45	4	60
Disponibilidad de talento humano especializado	10	5	50	5	50	5	50

Imagen y posicionamiento estratégico	12	5	60	4	48	4	48
TOTAL	100		320		263		308

Autor: *Elaboración propia*

Análisis e interpretación

Después de haber realizado un análisis detallado sobre las posibles ubicaciones para establecer la sede operativa de nuestra empresa, considero que la zona de Quito Norte, específicamente en la Av. Isla Seymour y Río Coca, representa la opción más estratégica y coherente con los objetivos de nuestro proyecto. Esta conclusión no es fruto del azar, sino del cruce de múltiples factores clave que, desde mi perspectiva, inciden directamente en el posicionamiento, la eficiencia y la proyección del negocio a mediano y largo plazo.

3.2. Tamaño óptimo

Cuando hablamos de capacidad instalada o lo que algunos llaman tamaño óptimo (Heizer, 2017), nos estamos refiriendo básicamente al límite máximo que una empresa puede alcanzar en su producción de bienes o servicios dentro de un periodo específico, usando todo lo que tiene a su disposición: máquinas, instalaciones, personal, infraestructura, etc. Es como preguntarse: "¿Hasta dónde puedo llegar si aprovecho al máximo mis recursos?". Este concepto, más allá de ser técnico, me parece fundamental porque nos ayuda a entender cuán eficiente puede llegar a ser una organización y hasta qué punto tiene potencial para crecer o responder a una mayor demanda sin necesidad de hacer inversiones adicionales de inmediato.

Tabla 5. *Cálculo del tamaño optimo*

PROCESO		NÚMERO DE TRABAJADORES	HORAS POR DÍA	DÍAS LABORABLES AL AÑO	
Tiempo de Procesos (Minutos)	60	4	8	52	semanas
Unidades Producidas	1		75%	5	días a la semana
Resultado (1 hora)	**1**	**4**	**6,00**	**260**	
					6240

Autor: *Elaboración propia*

Análisis he interpretación

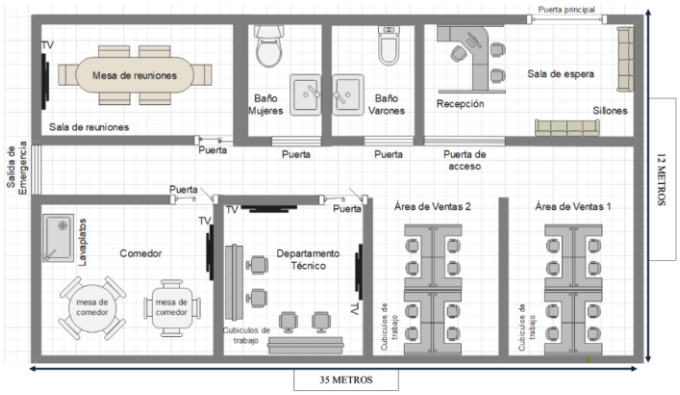
Dado nuestra actual situación operativa, la empresa cuenta con un número total de 4 empleados, la ejecución del proceso comercial de Attack Simulator lleva 1 hora, con el análisis realizado hemos descifrado que nuestra capacidad operativa con la cantidad de empleados actuales es de 6240 “servicios producidos al año”

3.3. Distribución

Se trata de cómo vamos a ordenar y distribuir todos los elementos dentro de nuestra oficina (Slack, 2013) o centro de operaciones, de manera que se aproveche eficientemente el espacio, se reduzcan los tiempos de ejecución, se facilite la comunicación entre los equipos y se garantice un entorno de trabajo cómodo, seguro y productivo.

Figura 13

Distribución operativa optima



Autor: *Elaboración propia*

3.4. Ingeniería del Proyecto

Este apartado representa el "cómo" del proyecto. Es decir, cómo se va a poner en marcha todo lo que hemos venido planeando. No se trata solo de tener una buena idea (como implementar un sistema de simulación de ciberataques en las MIPYMES), sino de definir de manera concreta y ordenada los procesos, herramientas, personas y recursos (Kerzner, 2017) que se necesitan para que esa idea funcione en la práctica.

3.4.1. Identificación de Recursos Humanos

Aquí nos enfocamos en las personas. Y no solo en cuántas se necesitan, sino en qué perfiles profesionales o técnicos son clave para ejecutar y sostener el proyecto. Desde mi experiencia, no basta con tener "personal suficiente", sino que es necesario contar con talento humano especializado y con roles bien definidos (Dessler, 2020).

Tabla 6. *Matriz de calificación del Recurso Humano*

Cargo	Funciones Principales	Perfil Profesional Recomendado	Nivel de Experiencia (1–5)	Conocimiento en	Habilidades Blandas (1–5)	Adaptación al Cambio (1–5)	Total Evaluación (Suma)

				Ciberseguridad (1–5)			
Líder del Proyecto / Coordinador General	Dirección, planificación, ejecución del proyecto, relaciones con aliados y toma de decisiones.	Ingeniero en Sistemas, Proyectos o afines	5	4	5	5	24
Especialista en Ciberseguridad / Técnico	Configuración de Attack Simulator, ejecución de simulaciones, soporte técnico, análisis de resultados.	Técnico o Ingeniero en Ciberseguridad	4	5	3	4	21
Especialista en Formación / Contenidos	Diseño de materiales de concientización, análisis de comportamiento humano, capacitación personalizada.	Psicólogo Organizacional / Comunicación	3	3	5	5	21
Asesor Comercial / Marketing Digital	Difusión del producto, gestión de clientes, campañas en redes, contacto con MIPYMES y gremios.	Publicidad, Marketing o Administración	4	2	5	5	21

Autor: *Elaboración propia*

3.4.2. Identificación de Recursos Materiales.

Aquí hablamos de los insumos tangibles o tecnológicos que vamos a necesitar para implementar el proyecto. Y ojo: no se trata solo de computadoras o escritorios. Desde mi perspectiva, los recursos materiales incluyen el software principal (Attack Simulator), la infraestructura tecnológica donde se alojará (Turban, 2018), licencias, servidores, equipos de comunicación, mobiliario, y demás herramientas que sostendrán la operación.

Tabla 7. *Matriz de calificación de materiales*

Recurso Material	Uso Específico en el Proyecto	Cantidad Necesaria	Costo Estimado Unitario (USD)	Disponibilidad Local (1–5)	Importancia Operativa (1–5)	Facilidad de Reposición (1–5)	Total Evaluación (Suma)
Computadoras de trabajo (laptops)	Operación del software, comunicación, gestión de simulaciones y reportes.	4	$800	5	5	5	15

Servidor virtual / hosting cloud	Plataforma para pruebas, almacenamiento seguro de datos y gestión de simulaciones.	1	$150 / mes	5	5	4	14
Acceso a licencias Attack Simulator	Uso de la herramienta para simulación, pruebas y capacitación.	Según clientes	$6 / usuario	5	5	5	15
Mobiliario básico (escritorios, sillas ergonómicas)	Espacios adecuados para trabajo diario del equipo.	4 puestos	$250	5	4	4	13
Herramientas de comunicación (Zoom, Google Meet, MS Teams)	Capacitaciones remotas, reuniones con clientes, demos y soporte.	1 cuenta empresarial	$15 / mes	5	5	5	15
Material POP / Publicitario digital	Difusión de la herramienta y sensibilización (PDFs, infografías, anuncios).	Pack inicial	$300	5	3	4	12
	TOTAL		$1521				

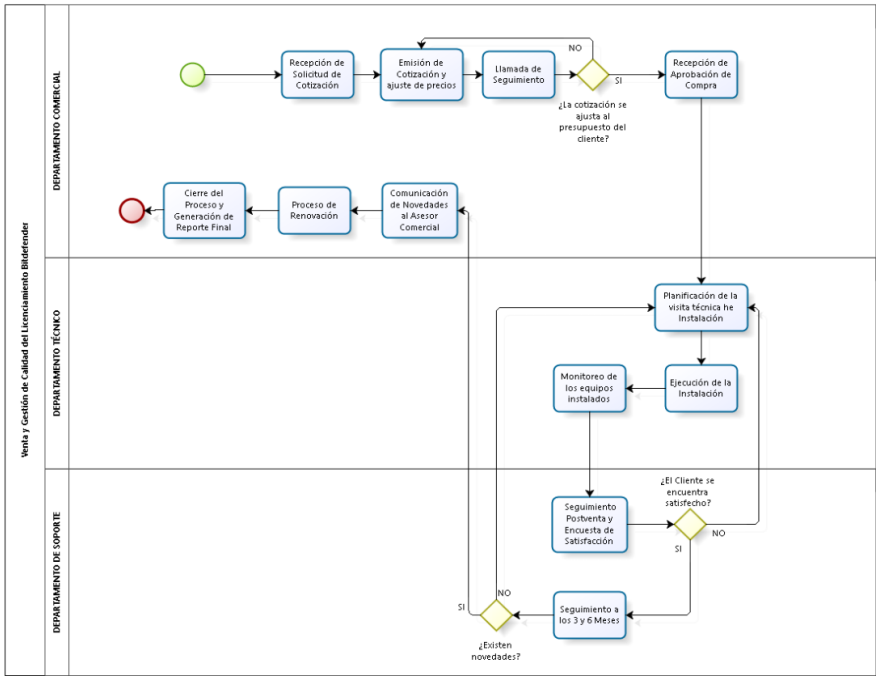
Autor: *Elaboración propia*

3.5. Proceso Productivo

En nuestro caso —la implementación del sistema Attack Simulator como plataforma de concientización y simulación de ciberataques para MIPYMES— el proceso productivo no se refiere a una línea de ensamblaje industrial, sino más bien a un flujo lógico de actividades digitales, técnicas y humanas que nos permiten entregar un servicio funcional, medible y útil para nuestros clientes (Stevenson, 2020).

Figura 14

Planteamiento del proceso productivo aplicado al proceso de ventas



Autor: *Elaboración propia*

3.6. La Casa de la Calidad

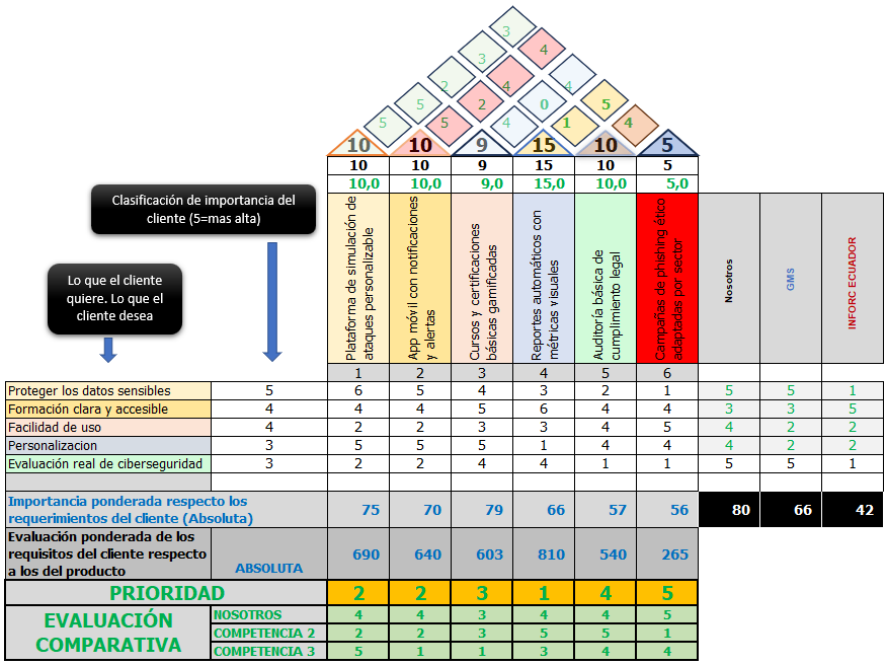
En el diseño de una solución como Attack Simulator, es fácil caer en la tentación de priorizar lo que la empresa quiere mostrar sobre lo que realmente necesita el usuario. Y aquí es donde la Casa de la Calidad se vuelve clave. Esta metodología, también llamada QFD (Akao, 1990), obliga a hacer un ejercicio de empatía con estructura: tomar lo que el cliente valora y traducirlo en decisiones técnicas concretas.

No basta con suponer que se sabe lo que quiere el usuario; hay que comprobarlo y convertirlo en acciones medibles. En este sentido, la herramienta conecta directamente expectativas —como simplicidad, personalización o reportes claros— con especificaciones que las respalden. Así se evita desarrollar funciones bonitas pero inútiles en la práctica.

En resumen, la Casa de la Calidad recuerda que cada característica debe responder a un "¿para qué?" que importe al usuario. Porque al final, una plataforma que no se alinea con la realidad de sus clientes, por muy innovadora que sea, difícilmente logrará el impacto que promete.

Figura 15

Matriz De Relación Entre Necesidades (Qués) Y Soluciones Técnicas (Cómos)



Autor: *Elaboración propia*

Análisis e interpretación

Reportes automáticos con métricas visuales

Los reportes automáticos con métricas visuales no son un simple "extra bonito" para el usuario; en realidad, representan un puente entre la experiencia de la simulación y la toma de

decisiones informadas. Desde una mirada crítica, este tipo de funcionalidad resuelve uno de los vacíos más comunes en programas de capacitación en ciberseguridad: la falta de datos claros y accionables que permitan medir avances o detectar retrocesos.

Plataforma de simulación de ataques personalizable

La idea de contar con una plataforma de simulación de ataques personalizable, como la que propone Attack Simulator, no es simplemente un recurso tecnológico más, sino un cambio de enfoque en la forma en que las MIPYMES abordan la ciberseguridad. Tradicionalmente, muchas herramientas del mercado ofrecen entrenamientos genéricos que repiten escenarios idénticos para todas las empresas, pero eso rara vez refleja la realidad particular de cada organización.

CAPÍTULO IV: ESTUDIO ADMINISTRATIVO

4.1. Dirección Estratégica

La dirección estratégica, en esencia, es ese mapa que orienta a una empresa para decidir hacia dónde quiere ir y cómo va a llegar allí. Implica tomar decisiones con la vista puesta en el largo plazo, pero también con los pies bien plantados en las oportunidades reales del entorno y en las capacidades que la organización ya posee.

En el caso de este proyecto, enfocado en medir la viabilidad de implementar Attack Simulator en MIPYMES de Pichincha, la dirección estratégica no es un formalismo, sino la columna vertebral de la propuesta. Una idea puede ser brillante y la tecnología impecable, pero si no existe una hoja de ruta clara —que conecte las necesidades reales del mercado con un plan coherente— el riesgo de quedarse a mitad de camino es alto.

4.1.1. Misión

Brindar a las MIPYMES de Pichincha una solución práctica y accesible para fortalecer su seguridad digital, enfocándonos en el eslabón más vulnerable pero también más valioso: las personas.

4.1.2. Visión

Ser un referente local en la formulación de estrategias de ciberseguridad centradas en las personas, demostrando que incluso las empresas más pequeñas pueden protegerse con soluciones realistas, educativas y adaptadas a su realidad. Soñamos con un ecosistema MIPYME en el que

la tecnología no sea vista como un lujo, sino como una herramienta cotidiana de protección, aprendizaje y mejora continua.

4.1.3. Valores

- Conciencia digital: Reconocer que la verdadera defensa empieza entendiendo nuestras propias vulnerabilidades.
- Accesibilidad: Ofrecer soluciones que puedan ser adoptadas por cualquier empresa, sin importar su tamaño o presupuesto.
- Empatía: Escuchar y entender el contexto particular de cada organización antes de proponer cambios.
- Responsabilidad ética: Tratar datos y personas con integridad y compromiso.
- Aprendizaje continuo: Acompañar el proceso de transformación digital como un socio, no como un impositor.

4.1.4. Slogan

“Ciberseguridad para personas reales, en empresas reales.”

Más que una frase de marketing, es una declaración de principios. Resume la convicción de que el verdadero cambio se logra con soluciones adaptadas al pulso diario de las MIPYMES, con sus propios tiempos, limitaciones y aspiraciones.

4.1.5. Logotipo

Figura 16

Propuesta de logotipo para software de simulación

Autor: https://attacksimulator.es/

Análisis he interpretación

1. **Elementos gráficos**

Escudo rojo: El escudo es un símbolo universal de protección y defensa. En el contexto de ciberseguridad, transmite inmediatamente la idea de seguridad, resguardo y prevención frente a amenazas.

Diseño minimalista: El escudo no tiene detalles complejos, lo que comunica modernidad, limpieza visual y facilidad de reconocimiento en diferentes tamaños o soportes (web, móvil, impresión).

2. **Tipografía**

"ATTACK":

- Estilo sans serif (sin remates), lo que aporta un carácter moderno, directo y tecnológico.
- Uso de mayúsculas: refuerza la seriedad y contundencia del mensaje.
- Color rojo: ligado a alerta, urgencia, advertencia y acción. En marketing de seguridad, el rojo enfatiza la importancia y el peligro que se busca mitigar.

"SIMULATOR":

- También en sans serif y mayúsculas, pero en color negro: aporta contraste y estabilidad visual.
- El negro transmite profesionalismo, autoridad y solidez.

3. Colores

Rojo (#D32F2F aproximado):

- Asociado a alerta, advertencia, peligro y acción inmediata.
- Genera una respuesta emocional rápida, ideal para captar atención en temas de seguridad.

Negro (#000000):

- Simboliza autoridad, profesionalismo y confianza.
- Crea un contraste fuerte con el rojo, mejorando legibilidad y jerarquía visual.

Blanco de fondo: Transmite limpieza, orden y neutralidad, permitiendo que los otros elementos destaquen con fuerza.

4. Composición

Alineación horizontal: escudo a la izquierda y texto a la derecha.

- Este orden es natural para la lectura de izquierda a derecha, guiando al usuario primero hacia el símbolo (identidad visual) y luego hacia el nombre.

Jerarquía visual:

- El escudo y la palabra ATTACK captan primero la atención por el color rojo.
- "SIMULATOR" funciona como complemento explicativo, en tono más neutro.

5. Interpretación y mensaje

El logotipo comunica:

- Protección y prevención (escudo).
- Urgencia ante amenazas (rojo).
- Tecnología y modernidad (tipografía sans serif).
- Confianza y profesionalismo (negro).

En conjunto, es un diseño claro, directo y fácilmente memorable, alineado con un producto de ciberseguridad que busca alertar y proteger.

Utilizar la forma de escudo con las iniciales de nuestra razón social refuerza el concepto de nuestro trabajo en la ciberseguridad.

4.2. Análisis FODA.

El análisis FODA no es simplemente una matriz para llenar casillas; en realidad, es como ponerle un espejo a un proyecto o empresa y observar, sin filtros, lo que está funcionando y lo que no. Esta herramienta ayuda a distinguir, por un lado, los puntos fuertes que vale la pena mantener y potenciar, y por otro, las debilidades que podrían convertirse en un dolor de cabeza si no se atienden. También obliga a mirar hacia afuera, detectando oportunidades que se pueden aprovechar y amenazas que podrían golpear en el momento menos esperado.

En esencia, su propósito es aterrizar las decisiones, evitar planes ilusorios y diseñar estrategias que tengan sentido con los recursos que realmente se tienen, todo esto en un entorno que —como bien sabemos— no deja de cambiar.

Tabla 8. *Matriz FODA*

Fortalezas (F)	**Oportunidades (O)**
Contamos con un enfoque educativo y personalizado, que permite adaptar la solución a las necesidades reales de las MIPYMES.	La digitalización forzada por la pandemia dejó abierta una puerta para implementar soluciones de ciberseguridad como una necesidad prioritaria.
Nuestra propuesta tiene un costo accesible, escalable y adaptado a presupuestos limitados, sin sacrificar calidad.	Existe un incremento en las políticas públicas, capacitaciones y apoyo de gremios hacia la transformación digital de pequeñas empresas.
Conocemos el contexto local, sus limitaciones técnicas, culturales y económicas. Hablamos el mismo idioma que los negocios a los que queremos llegar.	Hay poco conocimiento práctico sobre ciberseguridad en este segmento, lo que permite posicionarnos como pioneros en el enfoque educativo-simulativo.
Podemos medir resultados de forma rápida y tangible a través de simulaciones y reportes personalizados.	Se abren oportunidades de alianzas con cámaras de comercio, universidades y ONGs enfocadas en el desarrollo tecnológico.

Debilidades (D)	**Amenazas (A)**
Limitado posicionamiento inicial y falta de reconocimiento de marca en comparación con gigantes del sector.	Aumento de ataques cibernéticos sofisticados que pueden generar desconfianza en soluciones "locales" si no se comunican correctamente sus capacidades.
Dependencia de la conciencia y compromiso del personal de las empresas, lo cual puede ralentizar el proceso de adopción.	Inestabilidad económica nacional, alta inflación y reducción del gasto empresarial en innovación o formación.
Requiere un acompañamiento constante, lo que puede limitar el crecimiento rápido sin una estructura adecuada.	Falta de educación general sobre ciberseguridad en el país, lo que puede llevar a subestimar su importancia.
Resistencia al cambio por parte de directivos que ven la ciberseguridad como un gasto y no como una inversión.	Altas tasas de rotación de personal en MIPYMES, lo cual complica mantener una cultura sólida de seguridad digital.

Autor: *Elaboración propia*

Análisis e interpretación

El FODA del proyecto Attack Simulator muestra un balance claro: las fortalezas —enfoque educativo, personalización y costos accesibles— están alineadas con las oportunidades

del mercado postpandemia y el impulso a la transformación digital. Esto le permite posicionarse como una solución pionera y adaptada al contexto local. Sin embargo, el limitado reconocimiento de marca y la dependencia del compromiso del personal pueden frenar la adopción inicial. A esto se suman amenazas como la inestabilidad económica y la sofisticación de los ciberataques. El éxito dependerá de una estrategia de entrada gradual, comunicación clara del valor y alianzas estratégicas que potencien la confianza.

4.3. Estructura Organizacional y funcional

La estructura organizacional y funcional no es solo un organigrama bonito para colgar en la pared; es, en realidad, el mapa que muestra cómo se distribuyen las responsabilidades, cómo fluye la comunicación y quién toma las decisiones en una empresa. Sirve para que cada persona sepa con claridad su rol, a quién reporta y cómo su trabajo encaja en el objetivo general de la organización.

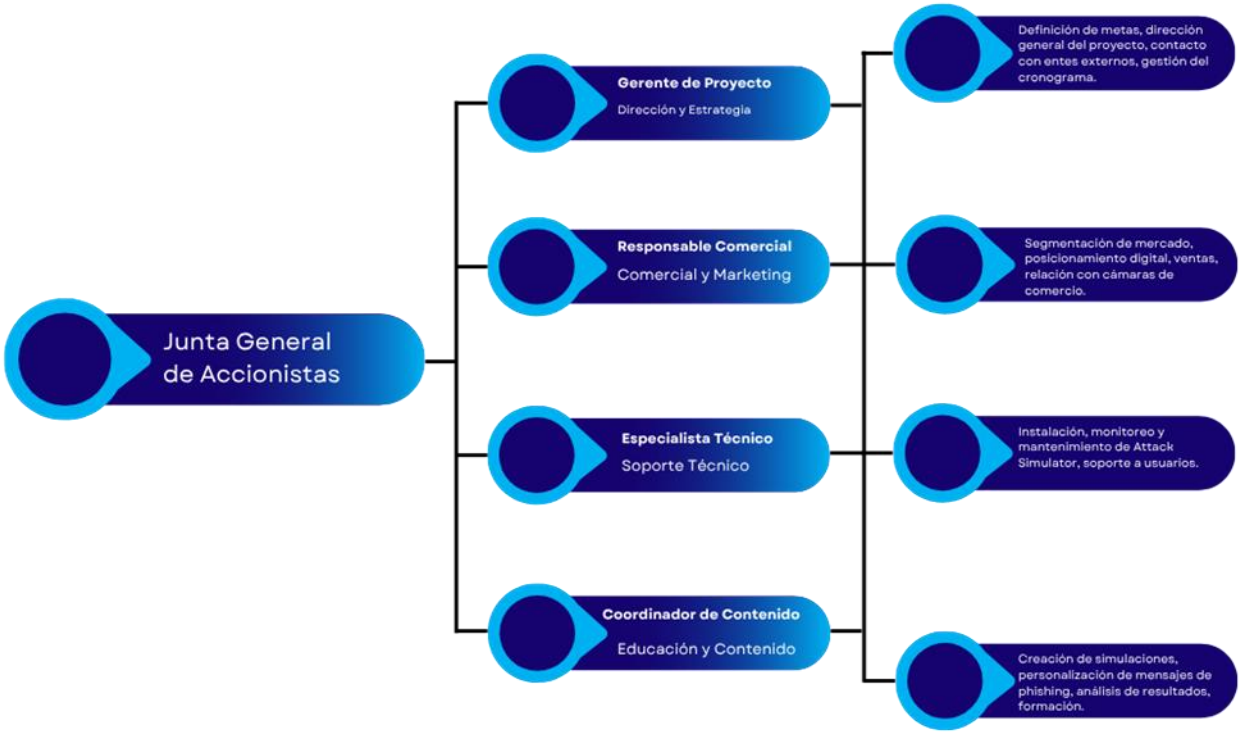
Su importancia radica en que, sin una estructura definida, es fácil caer en duplicidad de tareas, confusión de funciones y pérdida de tiempo en procesos poco claros. En cambio, cuando está bien diseñada, facilita la coordinación, optimiza recursos y ayuda a que todos remen en la misma dirección, especialmente en proyectos innovadores como el nuestro, donde cada área tiene un papel clave para que la propuesta llegue con éxito al mercado.

Figura 17

Estructura Organización y funcional

Autor: *Elaboración propia*

La estructura organizacional y funcional es el esquema que define cómo se organizan y distribuyen las funciones, responsabilidades y jerarquías dentro de una empresa o proyecto. En otras palabras, muestra quién hace qué, cómo se relacionan los equipos y qué canales de



comunicación existen entre ellos.

Sirve como una guía clara para que todos los miembros del equipo conozcan sus roles, a quién deben reportar y con quién deben coordinarse. Esto permite optimizar recursos, evitar duplicación de tareas, mejorar la eficiencia operativa y facilitar la toma de decisiones.

Su importancia radica en que una estructura bien definida reduce la improvisación, mejora el ambiente laboral y favorece el crecimiento ordenado de la empresa, especialmente en etapas iniciales donde cada decisión impacta directamente en el desarrollo del proyecto. Para emprendimientos como el nuestro, tener claridad en esta estructura es clave para mantener el enfoque, escalar adecuadamente y responder con agilidad ante cambios del entorno.

4.4. Estudio Legal

Al constituirse como una Sociedad Anónima (S.A.), IS SOLUTIONS adopta una de las estructuras jurídicas más sólidas y formales dentro del sistema empresarial ecuatoriano. Este tipo de sociedad ofrece una serie de beneficios clave, especialmente para negocios con proyecciones de crecimiento, operaciones tecnológicas y necesidad de financiamiento futuro.

Una Sociedad Anónima es una figura jurídica regulada por la Ley de Compañías del Ecuador, en la que el capital se divide en acciones, permitiendo que la propiedad esté representada por los accionistas, quienes tienen responsabilidad limitada al valor de sus aportes. Es decir, los socios no arriesgan su patrimonio personal más allá del capital invertido en la empresa.

Ventajas estratégicas en el mercado ecuatoriano

- Acceso a inversión y crecimiento sostenible

El formato de sociedad anónima facilita la entrada de nuevos inversionistas, permitiendo ampliar el capital mediante la emisión de nuevas acciones. Para un proyecto tecnológico como el nuestro, esto es esencial para crecer, innovar y escalar.

- Mayor confianza y reputación institucional

En el contexto local, muchas entidades públicas, privadas y organismos internacionales muestran preferencia por contratar con sociedades anónimas, ya que son percibidas como estructuras formales, fiscalizadas y con mayor compromiso de cumplimiento legal y tributario.

- Responsabilidad limitada

En un sector como la ciberseguridad, donde existen riesgos legales asociados al manejo de datos, brechas informáticas o incumplimientos contractuales, el hecho de que los accionistas no respondan con su patrimonio personal reduce considerablemente el riesgo financiero.

- Facilidad para internacionalización

La figura de Sociedad Anónima permite una estructura más profesional y estandarizada, lo cual abre oportunidades para alianzas internacionales, licitaciones regionales, certificaciones ISO, y cooperación con socios tecnológicos del exterior.

- Transparencia y gobernanza corporativa

Al contar con una junta general de accionistas, directorio y auditoría obligatoria, se establece un modelo de gobernanza claro. Esto no solo fortalece la toma de decisiones, sino que también genera confianza ante stakeholders, inversionistas y clientes corporativos.

4.4.1. Tipo de empresa.

Nuestra empresa, se enmarca dentro del sector terciario de la economía, también conocido como el sector de los servicios. Esto significa que no producimos bienes tangibles

como lo haría una industria o el agro, sino que ofrecemos servicios especializados, en este caso: ciberseguridad, simulación de ataques, consultoría digital y protección de datos.

4.5. Estudio Ambiental /Objetivos de desarrollo sostenible

En el contexto de este proyecto, la relación con los Objetivos de Desarrollo Sostenible (ODS) no es un añadido decorativo, sino una consecuencia natural de la propuesta. La iniciativa busca ir más allá de lo técnico, contribuyendo de forma tangible al progreso económico y social del país.

ODS 8: Trabajo decente y crecimiento económico

Meta relacionada: 8.2 – Impulsar la productividad mediante innovación y modernización tecnológica.

Este proyecto no se limita a vender una herramienta, sino que plantea un cambio en la forma en que las MIPYMES gestionan su seguridad digital. Implementar Attack Simulator es, en esencia, modernizar los procesos internos con tecnología accesible, escalable y adaptada a la realidad ecuatoriana. No se trata de imponer soluciones “de laboratorio”, sino de integrar sistemas que funcionen en entornos con recursos limitados, logrando así que las empresas sean más productivas, minimicen pérdidas por incidentes y se concentren en crecer.

Meta relacionada: 8.5 – Alcanzar empleo pleno y decente para hombres y mujeres.

La naturaleza de la propuesta genera oportunidades de empleo calificado en áreas como ciberseguridad, análisis de datos, soporte técnico y formación digital. No hablamos únicamente de trabajo técnico, sino de empleos que exigen criterio, creatividad y actualización constante, lo

que abre espacios para que tanto hombres como mujeres —independientemente de su experiencia previa— puedan desarrollarse en un campo con alta proyección futura. Además, al fortalecer las capacidades digitales de los empleados dentro de las MIPYMES, se mejora su perfil profesional y, con ello, su valor en el mercado laboral.

ODS 9: Industria, innovación e infraestructura

Meta relacionada: 9.5 – Mejorar la capacidad tecnológica e investigativa de los sectores productivos.

La plataforma propuesta no es solo un software; es una herramienta que permite recopilar datos sobre el comportamiento digital real de los colaboradores. Esa información, correctamente analizada, se convierte en insumo para investigación aplicada y para diseñar estrategias de seguridad más precisas. Así, las MIPYMES dejan de reaccionar únicamente cuando hay un problema y pasan a anticiparse a las amenazas, fortaleciendo sus capacidades tecnológicas con base en evidencia.

Meta relacionada: 9.c – Aumentar significativamente el acceso a las tecnologías de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos desarrollados.

Uno de los puntos fuertes de Attack Simulator es que puede implementarse sin requerir infraestructura costosa, lo que facilita que incluso empresas pequeñas, con conexiones de Internet básicas, puedan acceder a simulaciones y capacitaciones de alto nivel. Esto reduce la brecha digital en el sector productivo, especialmente en negocios que tradicionalmente han visto la ciberseguridad como algo “inalcanzable” o reservado para grandes corporaciones. De esta

manera, no solo se amplía el acceso a herramientas tecnológicas, sino que se garantiza que este acceso sea realmente útil y seguro para el crecimiento empresarial.

CAPÍTULO V: ESTUDIO FINANCIERO

5.1. Inversión Inicial

En cualquier proyecto, la inversión inicial es ese primer empujón que lo pone en marcha. En el caso de nuestra plataforma de simulación de ataques, implica destinar recursos a desarrollo tecnológico, licencias, pruebas, marketing inicial y capacitación del equipo. No es un gasto aislado, sino una apuesta a futuro: si se subestima, el proyecto podría nacer débil; si se sobreestima, podría comprometer la sostenibilidad financiera. La clave está en encontrar un equilibrio realista que permita lanzar un producto competitivo sin asfixiar el flujo de caja desde el primer día.

Tabla 9. *Valores involucrados en el monto de inversión inicial*

Detalle	Valores
1.1 Inversión en activos fijos	**$6.340,00**
1.2 Inversión en Intangibles	**$2.480,00**
1.3 Capital de trabajo	**$24.723,00**
(=) Total Inversión	**$33.543,00**
(-) Financiamiento	**$20.125,80**
(=) Inversión Neta	**$13.417,20**

Autor: *Elaboración Propia*

Análisis he interpretación

Una vez finalizado el análisis financiero, hemos detectado que, para garantizar la operatividad de nuestra empresa durante 3 meses, necesitamos una inversión total de $33.543,00. El mismo que recibirá un financiamiento del 60% mediante crédito bancario.

5.2. Capital de trabajo

Aquí no hablamos de una inversión “de una sola vez”, sino del oxígeno diario que mantiene viva la operación. Es el dinero para pagar sueldos, mantener servidores, cubrir licencias de software y gestionar imprevistos. En un servicio digital como Attack Simulator, subestimar el capital de trabajo es como arrancar un carro con el tanque casi vacío: puede encender, pero no llegar muy lejos.

Tabla 10. *Valores involucrados en el capital de trabajo*

Detalle	Valor mensual
Costos	**$4.644,00**
Gastos Adm y Ventas	**$3.597,00**
Total costo y gastos (mensuales)	**$8.241,00**
Total Capital de trabajo previsto	**$24.723,00**

Autor: *Elaboración propia*

Análisis he interpretación

Realizando un análisis de los costos y gastos involucrados en nuestro primer trimestre, el resultado dio un flujo de capital de $8.241,00 mensuales, de esta forma podremos garantizar el trabajo optimo en todas las áreas.

5.3. Identificación de Ingresos

No basta con suponer que habrá ventas; es necesario definir de dónde saldrán los ingresos y en qué volumen. Para este proyecto, se debe analizar si la monetización vendrá por licencias mensuales, paquetes por número de usuarios o servicios complementarios como auditorías.

Entender estas fuentes es vital para proyectar la rentabilidad y justificar ante inversores o socios que el negocio tiene un camino claro para generar retorno.

Tabla 11. *Identificación de las fuentes de ingresos con sus respectivos servicios*

#	Detalle	Proyección mensual			Anual
Item	Producto / Servicio	Cantidad	P. Unitario	Mensual	
1	Attack Simulator Basico 1-50	15	$80,00	$1.200,00	$14.400,00
2	Attack Simulator Basico 51-100	10	$128,00	$1.280,00	$15.360,00
3	Attack Simulator Enterprise 1-50	20	$180,00	$3.600,00	$43.200,00
4	Attack Simulator Enterprise 51-100	10	$288,00	$2.880,00	$34.560,00
5	Charla de concientización				
6	Acompañamiento y Buenas Practicas de Seguridad				
	Total ingresos ingresos proyectados			$8.960,00	$107.520,00

Autor: *Elaboración propia*

Análisis he interpretación

Dentro de los servicios de simulación de ataques que proponemos comercializar y después de un amplio análisis del mercado proponemos la comercialización de dos versiones del producto, esto nos da como resultado ingresos mensuales de $8.960,00

5.4. Costos y Gastos Administrativos

En todo emprendimiento, los costos administrativos son como ese ruido de fondo que, si no se controla, termina dominando la conversación. Incluyen desde gastos de oficina hasta

herramientas de gestión, soporte y marketing. En nuestro caso, aunque el servicio es digital, no estamos exentos: la plataforma requiere soporte técnico, actualizaciones y gestión comercial constante.

Tabla 12. *Costos involucrados en el funcionamiento de la empresa*

COSTOS

# Item	Detalle	Costo del producto / Servicio (Costo unitario)				Proyección mensual		Costo Anual
	Productos y/o servicios	Materiales	Mano de obra	Indirectos	Total costo	Cantidad	C. mensual	
1	Attack Simulator Basico 1-50	$44,00			$44,00	$15,00	$660,00	$7.920,00
2	Attack Simulator Basico 51-100	$60,00			$60,00	$10,00	$600,00	$7.200,00
3	Attack Simulator Enterprise 1-50	$90,00			$90,00	$20,00	$1.800,00	$21.600,00
4	Attack Simulator Enterprise 51-100	$158,40			$158,40	$10,00	$1.584,00	$19.008,00
5	Charla de concientización							
6	Acompañamiento y Buenas Practicas de Seguridad							
	Costo Total						$4.644,00	$55.728,00

Autor: *Elaboración propia*

Análisis he interpretación

Los costos relacionados a la distribución del software Attack Simulator en Ecuador tomando en cuenta un volumen de venta de 45 paquetes de simulación tenemos un promedio de costos equivalente a $4.644,00.

Tabla 13. *Gastos involucrados en el funcionamiento de la empresa*

GASTOS			
Item	**Rubro**	**V Mensual**	**Anual**
1	**Sueldo y Salarios**	**$2.800,00**	**$33.600,00**
2	**Servicios Básicos**	**$50,00**	**$600,00**
3	**Internet**	**$40,00**	**$480,00**
4	**Asistente Contable**	**$80,00**	**$960,00**
5	**Publicidad en redes sociales y medios**	**$200,00**	**$2.400,00**
6	**Arriendo**	**$100,00**	**$1.200,00**
7			
8	**Imprevistos (10%)**	**$327,00**	**$3.924,00**
	Totales	**$3.597,00**	**$43.164,00**

Autor: *Elaboración propia*

Análisis he interpretación

Para finalizar este análisis se realizó el calculo de los gastos administrativos los que están relacionados con el optimo funcionamiento de la empresa, estos gastos corresponden a todo el entorno operativo de la misma, dándonos un total mensual de $3.597,00.

5.5. Financiamiento

El financiamiento define de dónde saldrá el dinero para cubrir la inversión inicial y el capital de trabajo. Aquí entra la decisión estratégica: ¿autofinanciamiento, inversionistas, préstamos o una combinación? En un mercado como el ecuatoriano, donde el crédito puede ser

costoso, elegir mal la fuente de financiamiento puede comprometer la viabilidad a largo plazo, incluso más que la competencia.

Tabla 14. *Monto a financiarse por 5 años*

Concepto	Año 01	Año 02	Año 03	Año 04	Año 05	Totales
Pago Capital	$2.665,19	$3.218,08	$3.885,68	$4.691,77	$5.665,08	$20.125,80
Pago Interes	$3.599,70	$3.046,81	$2.379,21	$1.573,12	$599,81	$11.198,66
Dividendo	$6.264,89	$6.264,89	$6.264,89	$6.264,89	$6.264,89	$31.324,46

Autor: *Elaboración propia*

Análisis he interpretación

Una vez analizado los puntos anteriores y realizando la consolidación general de los ingresos, costos y gastos, se requiere una fuente externa de inversión, dándonos como resultado la solicitud de un crédito a 5 años.

5.6. Flujo de caja

Más que un documento contable, el flujo de caja es un termómetro de salud financiera. Permite saber si el proyecto podrá cubrir sus obligaciones mes a mes sin caer en déficit. En una plataforma SaaS, prever la periodicidad de los pagos y las renovaciones de clientes es crucial, ya que un desfase prolongado entre ingresos y gastos puede poner en riesgo la continuidad del servicio.

Tabla 15. *Monto efectivo en el flujo de caja*

Concepto	(+/-)	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	Totales

Flujo de caja Neto	=	-$13.417,20	$1.676,88	$1.903,05	$2.489,67	$2.567,38	$27.978,48	$23.198,26
Flujo de caja acumulado	=	-$13.417,20	-$11.740,32	-$9.837,27	-$7.347,60	-$4.780,21	$23.198,26	

Autor: *Elaboración propia*

Análisis he interpretación

A pesar de iniciar los primeros 4 años con números negativos, la correcta gestión y una proyección real de ventas nos permite recuperar la inversión y tener una ganancia optima a partir del año 5.

5.7. Valor Actual Neto (VAN) y tasa Interna de Retorno (TIR)

El VAN y la TIR no son simples fórmulas financieras: son la traducción matemática de si el proyecto vale la pena o no. En este caso, ayudan a medir si la inversión en Attack Simulator generará un valor superior al costo del capital invertido. Un VAN positivo y una TIR por encima de la tasa de descuento indican que el proyecto no solo es viable, sino atractivo para inversores. Sin embargo, estas métricas dependen mucho de proyecciones realistas; inflarlas artificialmente solo lleva a tomar decisiones equivocadas.

Tabla 16. *Resultados VAN/TIR*

Tasa de descuento =	**12%**
VAN =	**$8.876,57**
TIR =	**26,42%**

Autor: *Elaboración propia*

Análisis he interpretación

Interpretación del VAN ($8.876,57)

El Valor Actual Neto indica cuánto valor adicional generará el proyecto después de recuperar la inversión inicial, descontando el costo del dinero en el tiempo (en este caso, 12%).

- Un VAN positivo como este significa que, proyectando los flujos de caja estimados, el proyecto no solo se paga a sí mismo, sino que dejará una ganancia neta real de casi $8.900.
- Dicho de forma práctica, si la empresa invierte hoy en el desarrollo e implementación, al finalizar el periodo de evaluación habrá recuperado todo lo invertido y obtenido ese valor adicional, sin contar con otros beneficios intangibles como posicionamiento, reputación o impacto social.

Interpretación de la TIR (26,42%)

La Tasa Interna de Retorno refleja la rentabilidad anual esperada del proyecto.

- Una TIR de 26,42% frente a una tasa de descuento del 12% indica que el retorno supera ampliamente el mínimo esperado por los inversionistas o la propia empresa.
- Esto significa que, financieramente, el proyecto no solo es viable, sino atractivo: está generando más del doble del rendimiento mínimo exigido.
- Incluso si hubiera un margen de error en las proyecciones, el proyecto podría absorber cierto nivel de variaciones negativas sin volverse inviable.

Relación entre VAN, TIR y Riesgo

La combinación de VAN alto y TIR superior a la tasa de descuento es señal de fortaleza económica, pero no se debe olvidar que ambos indicadores dependen de las proyecciones de ingresos y costos.

- Si la captación de clientes es más lenta de lo previsto o si los gastos operativos crecen más rápido de lo esperado (por ejemplo, por aumentos en licencias, soporte o marketing), los indicadores podrían ajustarse a la baja.
- No obstante, el margen actual es lo suficientemente amplio para que el proyecto tolere ciertos desvíos y siga siendo rentable.

5.8. Costo beneficio

Este análisis permite poner en la balanza todo lo que se invierte frente a todo lo que se gana, no solo en términos monetarios, sino también en impacto social, reputacional y de posicionamiento. Para nuestro proyecto, el beneficio no se mide únicamente en ingresos, sino también en la reducción de incidentes de seguridad, la confianza de los clientes y la reputación como empresa innovadora en ciberseguridad.

Tabla 17. *Resultados del costo/beneficio a obtener*

COSTO BENEFICIO =	**$1,66**

Autor: *Elaboración propia*

Análisis he interpretación

Al integrar los resultados financieros del proyecto:

- VAN = $8.876,57
- TIR = 26,42%
- Costo-Beneficio = 1,66

Se obtiene un panorama claro: la propuesta no solo es viable, sino que proyecta una rentabilidad atractiva. El Valor Actual Neto positivo confirma que, descontando el valor del dinero en el tiempo con una tasa del 12%, el proyecto generará ganancias reales. La Tasa Interna de Retorno, al superar con holgura la tasa de descuento, refuerza la solidez del retorno esperado y su atractivo para inversionistas. Finalmente, el costo-beneficio indica que por cada dólar invertido se generarían $1,66, lo que equivale a un margen adicional del 66% sobre la inversión inicial. Sin embargo, este potencial debe administrarse con cautela: factores como sobrecostos operativos, variaciones en la captación de clientes o cambios regulatorios podrían afectar las proyecciones. Aun así, bajo las condiciones planteadas, la combinación de estos tres indicadores sitúa al proyecto Attack Simulator como una iniciativa rentable, sostenible y estratégicamente alineada con las necesidades del mercado MIPYME de Pichincha.

Conclusiones

El problema central es humano y la respuesta debe ser pedagógica. Las MIPYMES no fallan por falta de firewalls sofisticados, sino por vacíos de formación y protocolos. Por eso, Attack Simulator resulta pertinente cuando combina simulaciones realistas con capacitación continua y guías claras, para instalar hábitos y reducir errores cotidianos.

Hay encaje de mercado y ventaja competitiva local. Existe disposición a invertir si la solución es accesible, mide resultados y se adapta al contexto. Frente a ofertas externas rígidas y costosas, Attack Simulator destaca por su enfoque educativo, su escalabilidad y su ajuste a la realidad operativa de las MIPYMES ecuatorianas, abriendo espacio para un posicionamiento pionero.

La viabilidad financiera respalda la implementación sostenida. Los indicadores (VAN positivo, TIR superior a la tasa de descuento y relación costo-beneficio favorable) apuntan a factibilidad y rentabilidad de largo plazo. Con gestión prudente y crecimiento coherente, el proyecto puede generar retornos económicos y, además, fortalecer la cultura de ciberseguridad con impacto social.

Recomendaciones

Despliegue por segmentos con pilotos. Iniciar con un grupo piloto de MIPYMES con mayor apertura y presupuesto; convertir esos casos en testimonios locales. Luego escalar por tamaño/sector, ajustando planes y precios para reducir fricciones y acelerar adopción.

Reinversión para sostener ventaja. Destinar una parte de los ingresos a tres frentes: mejora continua de la plataforma, marketing educativo y soporte técnico robusto. Así se mantiene el valor percibido, se acompasa la evolución de las amenazas y se asegura competitividad a largo plazo. con la evolución de las ciberamenazas y las exigencias del mercado ecuatoriano, asegurando su relevancia y competitividad a futuro.

Bibliografía

Bibliografía

Akao, Y. (1990). *Quality function deployment: Integrating customer requirements into product design*. Obtenido de Productivity Press.: https://www.sciepub.com/reference/151230

Alliance, B. S. (2022). *Software piracy impact study*. Obtenido de BSA: https://www.bsa.org

Censos, I. N. (2023). *Directorio de empresas y establecimientos*. Obtenido de INEC: https://www.ecuadorencifras.gob.ec

Dessler, G. (2020). *Human resource management (16th ed.)*. Obtenido de Pearson.: https://www.pearson.com/en-us/subject-catalog/p/human-resource-management/P200000005876/9780135637289?srsltid=AfmBOoqynmuOxuseg01pfnXQ_LO_3J8Fn5uLvJ9NpNWOLjuX4mXiNzm6

Ecuador, A. N. (2021). *Ley Orgánica de Protección de Datos Personales*. Obtenido de Registro Oficial Suplemento 459: https://www.registroficial.gob.ec

establecimientos, D. d. (2023). *Instituto Nacional de Estadística y Censos*. Obtenido de INEC: https://www.ecuadorencifras.gob.ec

Forum, W. E. (2022). *WEF*. Obtenido de Cyber Value at Risk framework: https://www.weforum.org

Heizer, J. R. (2017). *Operations management: Sustainability and supply chain management (12th ed.).* Obtenido de Pearson: https://sophora.id/wp-content/uploads/2023/08/operations-management-12ed-jay-heizer-pdfdrive-.pdf

Hernández, R. F. (2014). *Metodología de la investigación (6.ª ed.)*. Obtenido de McGraw-Hill: https://dialnet.unirioja.es/servlet/libro?codigo=775008

Informática, A. E. (2023). *Informe Nacional de Ciberseguridad 2023*. Obtenido de AESI: https://aesi.ec/informe2023

Informática, A. E. (2023). *Informe Nacional de Ciberseguridad 2023*. Obtenido de AESI: https://aesi.ec/informe2023

Institute, P. (2022). *Cost of Insider Threats Global Report*. Obtenido de Proofpoint: https://www.proofpoint.com

Interpol. (s.f.). *Cybercrime: COVID-19 impact*. Obtenido de Interpol: https://www.interpol.int

Kaspersky. (s.f.). *Kaspersky Security Bulletin*. Obtenido de Estadísticas de ciberataques en América Latina: https://latam.kaspersky.com

Kerlinger, F. N. (2002). *Foundations of behavioral research (4th ed.)*. Obtenido de Wadsworth: https://www.scirp.org/reference/referencespapers?referenceid=230631

Kerzner, H. (2017). *Project management: A systems approach to planning, scheduling, and controlling (12th ed.)*. Obtenido de Wiley.: https://www.wiley.com/en-

se/Project+Management%3A+A+Systems+Approach+to+Planning%2C+Scheduling%2C+and+Controlling%2C+12th+Edition-p-9781119165361

Kotler, P. &. (2016). *Marketing management (15th ed.)*. Obtenido de Pearson.: https://www.scirp.org/reference/referencespapers?referenceid=3155681

Quito, D. M. (2024). *Quito Como Vamos* . Obtenido de Entorno Económico y Empresarial 2024 : https://quitocomovamos.org/wp-content/uploads/2025/02/10Factsheet_Economia2025.pdf

Security, I. (2023). *Cost of a Data Breach Report 202*. Obtenido de IBM: https://www.ibm.com/security/data-breach

Slack, N. C. (2013). *Operations management (7th ed.).* Obtenido de Pearson.: https://books.google.com.ec/books?id=8uowDgAAQBAJ&lpg=PA57&ots=cvK8bC5ixn&dq=Slack%2C%20N.%2C%20Chambers%2C%20S.%2C%20%26%20Johnston%2C%20R.%20(2013).%20Operations%20management%20(7th%20ed.).%20Pearson.&lr&hl=es&pg=PA57#v=onepage&q&f=false

Standardization, I. O. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection*. Obtenido de ISO: https://www.iso.org

Stevenson, W. J. (2020). *Operations management (14th ed.)*. Obtenido de McGraw-Hill: https://www.taylorfrancis.com/books/mono/10.4324/9781351034982/operations-management-michael-lewis

Tapia, E. (2025). *Primicias El Periodismo Comprometido*. Obtenido de Primicias : https://www.primicias.ec/economia/tarjetas-credito-delitos-informaticos-estafas-cuentas-bancos-98471/

Turban, E. P. (2018). *Information technology for management: On-demand strategies for performance, growth and sustainability (11th ed.)*. Obtenido de Wiley.: https://www.wiley.com/en-es/Information+Technology+for+Management%3A+On-Demand+Strategies+for+Performance%2C+Growth+and+Sustainability%2C+11th+Edition-p-9781118890868

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. Obtenido de Verizon Enterprise: https://www.verizon.com/business/resources/reports/dbir

Anexos

(Anexo 1. Detalle de Activos)

Anexo Activos Fijos

Detalle de activos fijos

# Item	Cantidad	Detalle	P. Unitario	P. Total	Terrenos	Inmuebles	Maquinaria	Muebles	Vehículos	Eq. Computo	Otros 1	Totales
1	3	Computadoras Operativas	$900,00	$2.700,00						$2.700,00		$2.700,00
2	1	Servidor Local	$1.500,00	$1.500,00						$1.500,00		$1.500,00
3	3	Escritorio	$180,00	$540,00				$540,00				$540,00
4	3	Sillas	$150,00	$450,00				$450,00				$450,00
5	2	Archivador	$120,00	$240,00				$240,00				$240,00
6	1	Pantalla	$180,00	$180,00						$180,00		$180,00
7	1	Mesa de reuniones	$250,00	$250,00				$250,00				$250,00
8	6	Silla de reuniones	$80,00	$480,00				$480,00				$480,00
		Totales		$6.340,00				$1.960,00		$4.380,00		$6.340,00

Detalle de intangibles

# Item	Cantidad	Detalle	P. Unitario	P. Total	G. Constitución	Preoperativos	Software	Otros 1	Otros 2	Otros 3	Otros 4	Totales
1	**1**	**Constitución Legal**	**$600,00**	**$600,00**		**$600,00**						**$600,00**
2	**1**	**Marketing**	**$500,00**	**$500,00**		**$500,00**						**$500,00**
3	**1**	**software complementario**	**$1.000,00**	**$1.000,00**			**$1.000,00**					**$1.000,00**
4	**1**	**CRM**	**$180,00**	**$180,00**			**$180,00**					**$180,00**

5	**1**	**Contabilidad Externa**	**$200,00**	**$200,00**				**$200,00**	**$200,00**
		Totales		**$2.480,00**		**$1.100,00**	**$1.180,00**	**$200,00**	**$2.480,00**

(Anexo2. Tabla de amortización)

Concepto	Año 01	Año 02	Año 03	Año 04	Año 05	Totales
Pago Capital	**$2.665,19**	**$3.218,08**	**$3.885,68**	**$4.691,77**	**$5.665,08**	**$20.125,80**
Pago Interes	**$3.599,70**	**$3.046,81**	**$2.379,21**	**$1.573,12**	**$599,81**	**$11.198,66**
Dividendo	**$6.264,89**	**$6.264,89**	**$6.264,89**	**$6.264,89**	**$6.264,89**	**$31.324,46**

Nro. Cuota	C. Inicial	Interés	Capital	Dividendo	C. Final
0	$ 20.125,80	$ -	$ -	$ -	$ 20.125,80
1	$ 20.125,80	$ 318,66	$ 203,42	$ 522,07	$ 19.922,38
2	$ 19.922,38	$ 315,44	$ 206,64	$ 522,07	$ 19.715,75
3	$ 19.715,75	$ 312,17	$ 209,91	$ 522,07	$ 19.505,84
4	$ 19.505,84	$ 308,84	$ 213,23	$ 522,07	$ 19.292,61
5	$ 19.292,61	$ 305,47	$ 216,61	$ 522,07	$ 19.076,00
6	$ 19.076,00	$ 302,04	$ 220,04	$ 522,07	$ 18.855,96
7	$ 18.855,96	$ 298,55	$ 223,52	$ 522,07	$ 18.632,44
8	$ 18.632,44	$ 295,01	$ 227,06	$ 522,07	$ 18.405,38
9	$ 18.405,38	$ 291,42	$ 230,66	$ 522,07	$ 18.174,72

10	$	18.174,72	$	287,77	$	234,31	$	522,07	$ 17.940,42
11	$	17.940,42	$	284,06	$	238,02	$	522,07	$ 17.702,40
12	$	17.702,40	$	280,29	$	241,79	$	522,07	$ 17.460,61
13	$	17.460,61	$	276,46	$	245,61	$	522,07	$ 17.215,00
14	$	17.215,00	$	272,57	$	249,50	$	522,07	$ 16.965,49
15	$	16.965,49	$	268,62	$	253,45	$	522,07	$ 16.712,04
16	$	16.712,04	$	264,61	$	257,47	$	522,07	$ 16.454,57
17	$	16.454,57	$	260,53	$	261,54	$	522,07	$ 16.193,03
18	$	16.193,03	$	256,39	$	265,68	$	522,07	$ 15.927,34
19	$	15.927,34	$	252,18	$	269,89	$	522,07	$ 15.657,45
20	$	15.657,45	$	247,91	$	274,16	$	522,07	$ 15.383,29
21	$	15.383,29	$	243,57	$	278,51	$	522,07	$ 15.104,78
22	$	15.104,78	$	239,16	$	282,92	$	522,07	$ 14.821,87
23	$	14.821,87	$	234,68	$	287,39	$	522,07	$ 14.534,47
24	$	14.534,47	$	230,13	$	291,95	$	522,07	$ 14.242,53
25	$	14.242,53	$	225,51	$	296,57	$	522,07	$ 13.945,96
26	$	13.945,96	$	220,81	$	301,26	$	522,07	$ 13.644,70
27	$	13.644,70	$	216,04	$	306,03	$	522,07	$ 13.338,66
28	$	13.338,66	$	211,20	$	310,88	$	522,07	$ 13.027,78
29	$	13.027,78	$	206,27	$	315,80	$	522,07	$ 12.711,98
30	$	12.711,98	$	201,27	$	320,80	$	522,07	$ 12.391,18

31	$	12.391,18	$	196,19	$	325,88	$	522,07	$	12.065,30
32	$	12.065,30	$	191,03	$	331,04	$	522,07	$	11.734,26
33	$	11.734,26	$	185,79	$	336,28	$	522,07	$	11.397,98
34	$	11.397,98	$	180,47	$	341,61	$	522,07	$	11.056,37
35	$	11.056,37	$	175,06	$	347,02	$	522,07	$	10.709,36
36	$	10.709,36	$	169,56	$	352,51	$	522,07	$	10.356,85
37	$	10.356,85	$	163,98	$	358,09	$	522,07	$	9.998,76
38	$	9.998,76	$	158,31	$	363,76	$	522,07	$	9.635,00
39	$	9.635,00	$	152,55	$	369,52	$	522,07	$	9.265,48
40	$	9.265,48	$	146,70	$	375,37	$	522,07	$	8.890,10
41	$	8.890,10	$	140,76	$	381,31	$	522,07	$	8.508,79
42	$	8.508,79	$	134,72	$	387,35	$	522,07	$	8.121,44
43	$	8.121,44	$	128,59	$	393,48	$	522,07	$	7.727,95
44	$	7.727,95	$	122,36	$	399,72	$	522,07	$	7.328,24
45	$	7.328,24	$	116,03	$	406,04	$	522,07	$	6.922,19
46	$	6.922,19	$	109,60	$	412,47	$	522,07	$	6.509,72
47	$	6.509,72	$	103,07	$	419,00	$	522,07	$	6.090,72
48	$	6.090,72	$	96,44	$	425,64	$	522,07	$	5.665,08
49	$	5.665,08	$	89,70	$	432,38	$	522,07	$	5.232,70
50	$	5.232,70	$	82,85	$	439,22	$	522,07	$	4.793,48
51	$	4.793,48	$	75,90	$	446,18	$	522,07	$	4.347,30

52	$	4.347,30	$	68,83	$	453,24	$	522,07	$	3.894,06
53	$	3.894,06	$	61,66	$	460,42	$	522,07	$	3.433,64
54	$	3.433,64	$	54,37	$	467,71	$	522,07	$	2.965,93
55	$	2.965,93	$	46,96	$	475,11	$	522,07	$	2.490,82
56	$	2.490,82	$	39,44	$	482,64	$	522,07	$	2.008,18
57	$	2.008,18	$	31,80	$	490,28	$	522,07	$	1.517,90
58	$	1.517,90	$	24,03	$	498,04	$	522,07	$	1.019,86
59	$	1.019,86	$	16,15	$	505,93	$	522,07	$	513,94
60	$	513,94	$	8,14	$	513,94	$	522,07	$	0,00
Totales			**$**	**11.198,66**	**$**	**20.125,80**	**$**	**31.324,46**		

(Anexos 3. Balance General)

	Año 0	**Año 01**	**Año 02**	**Año 03**	**Año 04**	**Año 05**
ACTIVO CORRIENTE	$24.723,00	$26.399,88	$28.302,93	$30.792,60	$33.359,99	$36.615,46
Caja - bancos	$0,00	$1.676,88	$3.579,93	$6.069,60	$8.636,99	$36.615,46
Cuentas por cobrar	0	0	0	0	0	0
INVENTARIOS	0	0	0	0	0	0
Otros activos corrientes	$24.723,00	$24.723,00	$24.723,00	$24.723,00	$24.723,00	
ACTIVO NO CORRIENTE	$8.820,00	$5.828,00	$3.936,00	$2.044,00	$1.612,00	$1.180,00

ACTIVOS FIJOS	$6.340,00	$6.340,00	$6.340,00	$6.340,00	$6.340,00	$6.340,00
ACTIVOS INTANGIBLES	$2.480,00	$2.480,00	$2.480,00	$2.480,00	$2.480,00	$2.480,00
(-) DEPRECIACION Y AMORTIZACIÓN ACUMULADA	$0,00	-$2.992,00	-$4.884,00	-$6.776,00	-$7.208,00	-$7.640,00
OTROS ACTIVOS	0	0	0	0	0	0
TOTAL ACTIVOS	**$33.543,00**	**$32.227,88**	**$32.238,93**	**$32.836,60**	**$34.971,99**	**$37.795,46**
PASIVO CORRIENTE	0	0	0	0	0	0
CUENTAS POR PAGAR PROVEEDORES (HASTA A 1 AÑO)	0	0	0	0	0	0
OBLIGACIONES LABORALES POR PAGAR	0	0	0	0	0	0
OBLIGACIONES FISCALES POR PAGAR	0	0	0	0	0	0
CRÉDITO CON BANCOS O COOPERATIVAS (HASTA 1 AÑO)	0	0	0	0	0	0
OTRAS CUENTAS POR PAGAR (HASTA 1 AÑO)	0	0	0	0	0	0
PASIVO NO CORRIENTE	$20.125,80	$17.460,61	$14.242,53	$10.356,85	$5.665,08	$0,00
CUENTAS POR PAGAR (MÁS DE 1 AÑO)	0	0	0	0	0	0
CRÉDITO CON BANCOS O COOPERATIVAS (MÁS DE 1 AÑO)	$20.125,80	$17.460,61	$14.242,53	$10.356,85	$5.665,08	0
OTRAS CUENTAS POR PAGAR (MÁS DE 1 AÑO)	0	0	0	0	0	0
TOTAL PASIVO	**$20.125,80**	**$17.460,61**	**$14.242,53**	**$10.356,85**	**$5.665,08**	**0**
PATRIMONIO	$13.417,20	$14.767,26	$17.996,40	$22.479,75	$29.306,91	$37.795,46
CAPITAL (APORTES)	$13.417,20	$13.417,20	$13.417,20	$13.417,20	$13.417,20	$13.417,20
RESULTADOS ACUMULADOS	0	0	$1.350,06	$4.579,20	$9.062,55	$15.889,71

RESULTADOS DEL PERÍODO	0	$1.350,06	$3.229,14	$4.483,35	$6.827,15	$8.488,56
TOTAL PASIVO Y PATRIMONIO	**$33.543,00**	**$32.227,88**	**$32.238,93**	**$32.836,60**	**$34.971,99**	**$37.795,46**