Diseñar un modelo de negocio sostenible que comercializa planes de capacitación en ciberseguridad para pymes a través de una plataforma de e-learning.

Alejandro Álvarez Alonso

Eumir Pulido de la Pava

Freddy Orlando Martínez Bernal

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá D.C., Colombia

2/10/2023

Diseñar un modelo de negocio sostenible que comercializa planes de capacitación en ciberseguridad para pymes a través de una plataforma de e-learning.

Alejandro Álvarez Alonso

Eumir Pulido de la Pava

Freddy Orlando Martínez Bernal

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director:

Juan Camilo Machado Ferrucho

Modalidad:

Creación de Empresa

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá D.C., Colombia

2/10/2023

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

A nuestras familias, cuya inagotable fe nos ha sostenido en los momentos más difíciles, y a los profesores, cuyas enseñanzas nos han guiado no solo en el conocimiento académico sino en el aprendizaje de la vida. Este trabajo de grado es el fruto de su amor, paciencia y sabiduría.

Resumen

El presente trabajo de grado desarrolla un plan de negocio integral para "GAMSECURE", una plataforma de aprendizaje en línea centrada en la ciberseguridad para pequeñas y medianas empresas en Colombia. El enfoque gamificado busca mejorar la cultura de Ciberseguridad en las empresas para identificar riesgos y responder eficazmente a los crecientes ciberataques. El documento aborda el análisis del mercado, la propuesta de valor innovadora de GAMSECURE, y las estrategias para posicionarse y expandirse en el sector. Se enfoca en cómo esta plataforma interactiva puede cambiar el comportamiento y la actitud hacia la ciberseguridad, con metas a corto, mediano y largo plazo para el crecimiento y posicionamiento de la empresa.

Los resultados destacan la viabilidad y efectividad de GAMSECURE en el mercado de ciberseguridad. Las conclusiones sugieren que GAMSECURE representa una solución prometedora para fortalecer la ciberseguridad en PYMES, ofreciendo una experiencia educativa

Palabras clave: Plataforma de aprendizaje en línea, Ciberseguridad, PYMES (pequeñas y medianas empresas), Enfoque gamificado, Cultura de ciberseguridad, Riesgos cibernéticos, Ciberataques, Comportamiento y actitud, Experiencia educativa

Abstract

This document presents a comprehensive business plan for "GAMSECURE," an online learning platform focusing on cybersecurity for small and medium-sized enterprises in Colombia. Leveraging gamification, GAMSECURE aims to enhance cybersecurity culture within businesses, equipping them to effectively identify and respond to escalating cyber threats. The study includes a market analysis, GAMSECURE's innovative value proposition, and strategies for market positioning and expansion. It emphasizes how this interactive platform can transform attitudes and behaviors towards cybersecurity. The results underscore GAMSECURE's market viability and effectiveness, concluding that it stands as a promising solution to bolster cybersecurity in SMEs through an engaging educational experience.

Keywords: Online learning platform, Cybersecurity, Gamification, Cybersecurity culture, Cyber threats, Interactive platform, Attitudes towards cybersecurity, Behavioral change, educational experience.

Contenido

Pág.

Lista de Figuras

Pág.

Lista de Tablas

Pág.

Introducción

Hoy en día existe una gran preocupación por resguardar la integridad, confidencialidad y disponibilidad de la información en las empresas, debido al incremento de ciberataques cada vez más avanzados, que afectan indistintamente las pequeñas, medianas y grandes empresas que tratan de emerger en un mundo cambiante, y que se convierten en el blanco perfecto al tener empleados sin el suficiente entrenamiento en el reconocimiento de este tipo de amenazas, los que los hace el eslabón más débil en el ecosistema de Ciberseguridad (Fonte, 2022, enero 24).

En el reciente estudio X-Force Threat Intelligence Index 2022 (X-Force®, 2022), que monitorea tendencias y patrones en ciberataques, los ataques cibernéticos están aumentando con preocupación en Latinoamérica, posicionando el ataque de Ransomware como el número uno durante el 2022, y a algunos actores como REvil como los responsables del 37% de todos los ataques de ransomware. El estudio resalta que el principal control y el más efectivo para prevenir ataques de phishing es la sensibilización de usuarios, y su educación es la clave, acompañada con ejemplos reales del mundo en temas de ciberseguridad.

Por su parte, el Centro de Cibernética de la Policía Nacional indica que en 2022 se registraron 54.121 denuncias por delitos informáticos, frente a las 11.223 de 2021 (República L. , 2022). Esta cifra representa un incremento importante, lo que actualmente está motivando a las empresas a buscar nuevas alternativas y estrategias en Ciberseguridad.

En Colombia empresas como EPM, Sanitas, INVIMA - Instituto Nacional de Vigilancia de Medicamentos y Alimentos, como la entidad encargada de legalizar alimentos y medicinas, DANE, Universidad de los Andes, Universidad Javeriana, Canal Caracol,

Famisanar y Audifarma, son algunas de las afectadas por los atacantes que aprovecharon fallos de seguridad en algunos casos de vulnerabilidades no conocidas de plataformas Fortinet, dejándolas a la merced de controles de backup deficientes, ausencia de monitoreo en la red y buenas prácticas de seguridad de la información (Jeimy Cano, 2022).

Los efectos de estos ataques han llevado a muchas empresas a reconocer la importancia de contar con estrategias de Ciberseguridad para responder a este tipo de amenazas. En este contexto, las plataformas de educación con técnicas de gamificación resultan ser una opción atractiva y muy importante, con las cuales pueden aumentar la conciencia y las habilidades que los empleados deben tener sobre los problemas de seguridad. En el artículo hacia la gamificación educativa de (Ricardo Acosta-Díaz, 2016), los autores afirman que: “la gamificación puede ser una estrategia de gran alcance que promueva la educación entre las personas y un cambio de comportamiento”. La gamificación utiliza elementos de los juegos, como la competencia, la recompensa y el reconocimiento, para motivar a las personas a realizar ciertas tareas (Itmadrid, 2023).

En el ámbito de la seguridad informática, la gamificación se está empezando a utilizar con el propósito de aumentar o fortalecer el conocimiento de los empleados sobre los riesgos de seguridad y mejorar su postura de seguridad. Existen dinámicas basadas en juegos que son un 77% más efectivas que el aprendizaje tradicional y, además, se pueden utilizar en casi cualquier contexto (Security, 2017). De esta forma entonces, las estrategias tradicionales de Ciberseguridad se pueden apoyar en “la aplicación de estrategias de juegos (pensamiento o la lógica del juego) a un entorno o tarea ajena al mismo con el objetivo de alentar la participación; convirtiendo una capacitación o un curso en un juego (ESET, 2020).

Este trabajo expone un plan de negocio completo para la creación de "GAMSECURE", que no solo busca el desarrollo de una plataforma de aprendizaje interactiva y divertida,

sino apoyar las necesidades de las empresas, incorporando el conocimiento adquirido en la Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos, así como prácticas de Ciberseguridad a los procesos y cultura organizacional, lo que les permitirá responder ante los posibles riesgos a los que están expuestos en el Ciberespacio. Uno de los principales retos y desafíos de este trabajo, será el de definir los contenidos con técnicas gamificación que serán diseñados para apoyar la estrategia de Ciberseguridad de las pequeñas empresas.

La plataforma permitirá aprender y jugar a los empleados, y a su vez permitirá a los empleadores identificar los niveles de adopción del conocimiento, así como la frecuencia y calidad de la participación por parte de los empleados, en donde se espera lograr una reducción en la cantidad de incidentes o riesgos de ciberseguridad como resultado de la apropiación y creación de conciencia en estos temas.

Objetivo General

Crear un modelo de negocio sostenible que permita la comercialización viable de planes de formación en Ciberseguridad para pequeñas y medianas empresas mediante una plataforma de aprendizaje en línea.

Objetivos Específicos

Realizar un análisis del entorno, considerando tanto las amenazas como las oportunidades de negocio, con el fin de ofrecer soluciones que satisfagan las necesidades del mercado y del cliente.

Desarrollar un modelo de negocio que responda de manera eficaz a las necesidades identificadas en el segmento de clientes, asegurando su coherencia con los aspectos financieros, técnicos y legales, que permitan su viabilidad.

Naturaleza del Proyecto

Las aplicaciones que son utilizadas por las empresas para el desarrollo de sus procesos y actividades tienen vulnerabilidades que en algunos casos no cuentan con actualizaciones o parches con las que se puedan remediar. Cada vulnerabilidad se convierte en un vector de ataque, que fácilmente es aprovechado por actores organizados que buscan desde el robo de información sensible hasta la afectación del servicio, con el propósito de obtener un beneficio económico o dañar la Figura y reputación de la entidad.

Adicional a lo anterior, se suma la ausencia del personal adecuado en las áreas de seguridad, y una falta de conciencia y entrenamiento de los empleados en conocimientos que les permitan identificar dichas amenazas, y así de esta forma reaccionar y responder de forma adecuada en cada ataque (Intelligence, 2023).

Esto representa un nivel bajo de cultura de seguridad informática en el entorno empresarial en general, lo que refleja una preocupación y necesidad de abordar la ciberseguridad de manera efectiva. Estos problemas y desafíos evidenciaron una oportunidad de abordar la ciberseguridad desde una perspectiva educativa y preventiva.

Esto motivó a que surgiera la idea de crear una empresa con servicios que suplan esta necesidad y permita convertirse en un aliado con el que se pueda abordar proactivamente los desafíos de ciberseguridad en el ámbito empresarial, con educación basada en la gamificación, y una plataforma innovadora y adaptada a la realidad de las empresas.

Descripción del modelo de negocio.

GAMSECURE es una empresa que se enfoca en brindar planes de capacitación a través de una plataforma de aprendizaje en línea e-learning, que utiliza técnicas de

gamificación, y una estrategia pedagógica para hacer que el aprendizaje en ciberseguridad sea más atractivo, retentivo y significativo para los usuarios, buscando un cambio real en el comportamiento y actitud hacia la ciberseguridad, dirigida inicialmente a las pequeñas y medianas empresas PYMES.

Propuesta de Valor

GAMSECURE ofrece la mejor formación en ciberseguridad con una propuesta de valor innovadora y vanguardista para las empresas contemporáneas. La plataforma de e-learning transformará la educación de Ciberseguridad, en una aventura interactiva, donde los conceptos y contenidos se convierten en emocionantes misiones, juegos y desafíos, mediante el uso estratégico de la gamificación, capturando de esta forma la atención de los usuarios y asegurando la retención del conocimiento. Las empresas y usuarios podrán acceder al contenido formativo desde cualquier lugar al instante, con contenido actualizado, proporcionando herramientas para el seguimiento al avance de la capacitación, maximizando el retorno de la inversión.

Además, se tendrá un soporte técnico dedicado, y disponible para asegurar una mejor experiencia de aprendizaje integral que impulsa la seguridad de la información y fortalece la resiliencia cibernética en las organizaciones.

Objetivos empresariales a corto plazo

Posicionar la marca GAMSECURE en el mercado de plataformas e-learning.

Desarrollar una estrategia comercial efectiva para el crecimiento de clientes.

Objetivos empresariales a mediano plazo

Diversificar productos y servicios, mediante la creación de nuevos contenidos personalizados de formación.

Publicar al menos tres cursos nuevos gamificados al año, manteniendo el contenido actualizado con las últimas tendencias y amenazas en Ciberseguridad.

Objetivos empresariales a largo plazo

Convertirse en un líder reconocido en la industria de la ciberseguridad en las pymes. Evaluar la posibilidad de expandirse a mercados internacionales con un enfoque en países de habla hispana.

Mantener un crecimiento sostenible y rentable, asegurando la satisfacción continua de los clientes y la fidelización.

Estado actual del negocio

Actualmente, la iniciativa de creación de empresa se encuentra en la fase de diseño, una etapa crítica en el ciclo de vida empresarial, tal como se describe en el libro "Emprendimiento: conceptos y plan de negocios" de Carlos Prieto Sierra (Sierra, 2014). Como parte de esta fase, se ha desarrollado un prototipo de la plataforma, en el que se incluye un curso introductorio de ciberseguridad, que sirve para demostrar las funcionalidades de los distintos módulos de la plataforma y facilita la validación del modelo de negocio propuesto por Gamsecure. Este enfoque práctico y progresivo es esencial para asegurar la eficacia y viabilidad de la propuesta empresarial.

Descripción de productos o servicios

Los productos o servicios que ofrece GAMSECURE son los siguientes:

Desafíos

El primer producto por desarrollar son los desafíos o actividades. el sitio web está relacionado con actividades de ciberseguridad, por lo cual es necesario crear desafíos,

actividades o escenarios de simulación. Cada desafío o actividad puede tener su propia página con descripciones, objetivos y niveles de dificultad.

Cursos de formación

El segundo producto está relacionado con cursos de formación, en los que se ofrecerán contenido relacionado con temas de ciberseguridad, partiendo del nivel básico y nivel medio, al nivel avanzado.

Planes por suscripción.

Esta alternativa ofrece una variedad de cursos de capacitación en ciberseguridad que se pueden comprar por separado. Cada curso podría centrarse en un aspecto específico de la Ciberseguridad. Ofrece un modelo de suscripción mensual o anual para acceder a la plataforma. Las tarifas pueden variar según el curso y su contenido.

Planes personalizados.

Proporciona la flexibilidad de ofrecer planes personalizados según las necesidades específicas de cada empresa. Puede incluir servicios adicionales como asesoramiento en ciberseguridad, contenido e informes personalizados.

Las tarifas pueden variar según el tamaño de la empresa y la cantidad de usuarios que deseen utilizar la plataforma.

Nombre, tamaño y ubicación de la empresa.

La empresa se llamará GAMSECURE, e inicialmente tendrá menos de 10 empleados y se ubicará en la ciudad de Bogotá, bajo la modalidad de teletrabajo, por la dinámica del negocio.

Potencial del Mercado en Cifras

Según el informe de Sophos, en lo corrido del 2023 el 66% de las organizaciones fueron atacadas por ransomware (Republica, 2023).

Durante 2022, el Centro de Cibernética de la Policía Nacional anticipaba el registro de 54.121 denuncias por delitos informáticos, un considerable aumento en comparación con las 11.223 reportadas en 2021 (República L. , 2022).

Conforme a datos de la Cámara Colombiana de Informática y Telecomunicaciones - CCIT, los ciberataques en Colombia el número de ataques cibernéticos aumentó en un 30%, y se registraron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia en el 2021 (Cámara Colombiana de Informática y Telecomunicaciones, 2022). Así mismo “a nivel mundial el promedio del pago por rescate en sectores como la manufactura estuvo en 2.036.189 dólares, mientras que en Latinoamérica fue de 1.5 millones de dólares y en Colombia puede rondar los 900.000 dólares, incluyendo el pago a los ciberdelincuentes, el tiempo de trabajo adicional de los ingenieros, multas, recuperación del sistema y otros aspectos” (INFOBAE, 2022)

Las pequeñas y medianas empresas emergen como el segmento más propenso a sufrir ciberataques debido a la frecuente insuficiencia de recursos para invertir en seguridad informática. Fortalecer la formación y entrenamiento de los ciudadanos en los temas de ciberseguridad y protección de la información personal es una necesidad (Jeimy Cano, 2022).

Las principales tendencias siguen siendo la exfiltración y venta de información sensible de personas, el robo de información sensible de organizaciones y estados, y el patrocinio de ataques cibernéticos con fines económicos y de extorsión, según el documento de Prospectiva de ciberseguridad nacional para Colombia a 2030 (José, 2022).

Perspectivas de crecimiento en el sector de ciberseguridad.

De acuerdo con la 'Guía de Gasto Mundial en Seguridad' de IDC, se estima que el gasto mundial en soluciones y servicios de seguridad sea de 219.000 millones de dólares en 2023, un 12,1% más respecto a 2022 (IDC, 2023).

De acuerdo con Asociación Colombiana de Ingenieros de Sistemas (ACIS), los ataques de phishing y la escasa conciencia cibernética entre los usuarios figuran como las principales amenazas en el país. En el informe de ESET Security Report (ESR) que evalúa el estado de la seguridad de la información en las empresas de América Latina arrojó que una de cada dos organizaciones aseguró haber sufrido un incidente de seguridad informática, y el 24 % de estos incidentes fueron provocados por malware, siendo las principales vías de ataque el phishing y la explotación de vulnerabilidades (ACIS, 2022).

El aumento de las amenazas cibernéticas, y la necesidad de mejorar las capacidades de ciberseguridad han crecido sustancialmente en la región, sin embargo el panorama de fuerza laboral entrenada en ciberseguridad es desalentador, el reciente reporte de "El desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades" (OEA, 2022) confirma que existe una escasez de personal capacitado y calificado en el mercado laboral para trabajar en roles de ciberseguridad que pueda abordar estas amenazas y sus riesgos relacionados.

Evolución del E-Learning.

Según Infobae (Infobae, 2022), la pandemia impulsó notablemente la industria del e-learning a escala global, aunque su desarrollo venía gestándose desde años anteriores. Esta adaptación forzada resultó en la consolidación acelerada de plataformas tecnológicas y en la creación de contenidos adecuados para la educación online.

Un estudio de la Universidad Internacional de La Rioja (UNIR) ((UNIR), 2022) revela que, desde el año 2000, la educación online ha experimentado un crecimiento impresionante del 900% a nivel global.

Se identifica una creciente demanda de cursos especializados, dada la dinámica cambiante del mundo digital. Sectores como e-commerce, trading, finanzas personales, desarrollo personal y bienestar, requieren ofertas educativas adaptadas y actualizadas.

Panorama empresarial en Colombia.

Según el boletín directorio estadístico de empresas 2019-2021 del DANE (DANE, s.f.), Colombia registró en 2021 un total de 5.704.308 empresas. De estas, el 15,2% son jurídicas y el 84,8% son naturales. Se identificó un incremento del 13,1% en la creación de empresas en comparación con años anteriores. A su vez, del universo empresarial, 5.597.316 son microempresas, 81.725 pequeñas, 19.100 medianas y 6.167 grandes, según lo establecido en la Ley 905 de 2004. Así mismo la Cámara de Comercio de Bogotá confirmo para el 2023, 480.441 empresas constituidas, de las cuales hay 24.786 pequeñas y 7311 medianas. (Bogotá C. d., 2023)

Las cifras y tendencias actuales destacan, de manera indiscutible, una urgencia creciente en materia de ciberseguridad, con un enfoque especial hacia las PYMES en Colombia y América Latina. El aumento sostenido de los ciberataques, junto con el aumento de vulnerabilidades en las PYMES, en gran parte por la falta de recursos y conocimiento en seguridad informática, configura un escenario que demanda soluciones efectivas, adaptadas y accesibles.

En este panorama, una propuesta innovadora como GAMSECURE no solo encuentra un mercado potencial significativo, sino también la oportunidad de tener un impacto positivo, al mejorar la protección de los activos de información y operaciones de estas empresas, contribuyendo al fortalecimiento del tejido empresarial, garantizando su

resiliencia frente a amenazas cibernéticas y asegurando su continuidad y crecimiento en un mundo cada vez más digitalizado.

Al ofrecer cursos en áreas clave como ciberseguridad, se está abordando una amplia gama de necesidades en el campo de la seguridad digital. Esto atraerá a un público diverso. Para aquellos que desean sumergirse en un área particular durante un período prolongado, el acceso ilimitado a contenidos específicos brinda una ventaja competitiva al proporcionar un aprendizaje continuo y profundo.

La innovación y la adaptación de técnicas de gamificación a las nuevas tecnologías y contenidos de Ciberseguridad, puede ser una ventaja competitiva importante a medida que el mercado de las plataformas de e-learning continúa evolucionando.

Resumen de las inversiones requeridas.

El análisis preliminar que forma parte del plan de negocio de GAMSECURE, estima una inversión inicial en el primer año (año cero) de $312.000.000. Esta inversión se distribuye, en gran parte, en costos operativos, nómina, marketing, gastos fijos, propiedad planta y equipo, y otros gastos para la puesta en marcha. En la estimación de la inversión requerida a partir del análisis de los posibles costos, y de acuerdo con la cantidad de suscripciones o cursos que se deben vender de cada uno en la plataforma de gamificación con temas de ciberseguridad para generar utilidad.

Costos Operativos - $95.000.000 (12 meses): Estos son los gastos generales asociados con el desarrollo de los seis cursos con su contenido.

Nóminas - $138.000.000 (12 meses): Salarios y compensaciones para los empleados y colaboradores de la empresa, incluyendo beneficios y cargas sociales.

Marketing - $20.000.000 (12 meses): Gastos asociados con la promoción y marketing de la plataforma. Esto podría incluir publicidad online, creación de contenido, eventos promocionales, y otros gastos relacionados con la adquisición y retención de clientes.

Propiedad planta y equipo - $5.000.000: Inversión en infraestructura física, como la compra o alquiler de instalaciones, maquinaria, vehículos y otros bienes de capital.

Equipo de oficina - $5.000.000: Compra de computadoras, mobiliario, impresoras, teléfonos y otros equipos esenciales para la operación de una oficina.

Gastos de puesta en marcha - $10.000.000: Costos iniciales asociados con el lanzamiento del negocio. Estos pueden incluir investigaciones de mercado, diseño de logo y branding, creación del sitio web, y otros gastos al iniciar el negocio.

Tabla 1.

Presupuesto inversión inicial

ÍTEM		**COSTO ASOCIADO**	
	MESES		**VALOR**
COSTOS OPERATIVOS	12	$	95.000.000
NÓMINAS	12	$	138.000.000
MARKETING MIX	12	$	20.000.000
GASTOS FIJOS	12	$	39.000.000
TOTAL INVERSIÓN		$	292.000.000
APORTE DE LOS EMPRENDEDORES		$	30.000.000
PRÉSTAMO A SOLICITAR		$	282.000.000

Nota. Elaboración Propia.

Total Inversión - $312.000.000: Suma total de todos los gastos y costos asociados con el inicio y operación de la empresa durante el primer año. De acuerdo con lo anterior para la inversión inicial en el año cero, se requiere de un préstamo de $282.000.000, y un aporte de los emprendedores de $30.000.000. Los costos operativos, corresponden a los desarrollos necesarios para la creación de los cursos, esto incluye diseño y creación de contenido con técnicas de gamificación, los cuales se distribuyen de la siguiente forma:

Tabla 2.

Costos operativos

NOMBRE DEL PRODUCTO SERVICIO	CANTIDADES	COSTO UNITARIO PDTO O SERVICIO	COSTOS TOTALES
Desafíos Ilimitado	2000	10000	$ 20.000.000
Desafíos Limitado Acceso 3 meses	2000	10000	$ 20.000.000
Curso Fundamentos de Ciberseguridad	1500	10000	$ 15.000.000
Seguridad de la Información	1000	15000	$ 15.000.000
Seguridad de Aplicaciones	1000	15000	$ 15.000.000
Gestión de Riesgos de Seguridad	1000	10000	$ 10.000.000

Nota. Elaboración Propia.

Proyecciones de ventas y rentabilidad

Como se destacó en la descripción de GAMSECURE, la estrategia de monetización gira en torno a la oferta de varios productos y servicios relacionados con la gamificación y la ciberseguridad. Estos han sido meticulosamente diseñados para abordar las demandas y preocupaciones en materia de Ciberseguridad de los posibles clientes, maximizando el valor y la educación. Mediante esta estrategia, no solo se busca diversificar las fuentes de ingresos con productos como "Desafíos Ilimitado" y cursos especializados, sino también garantizar la viabilidad y sostenibilidad financiera de GAMSECURE en el futuro.

La proyección de ventas detalla la cantidad prevista de unidades que se espera vender de cada producto o servicio, el precio de venta unitario sin incluir el IVA (Impuesto al Valor Agregado) y el ingreso total que se generaría de esas ventas. A continuación, se presenta el detalle de la proyección de ventas:

Tabla 3.

Proyección de Ventas

NOMBRE DEL PRODUCTO O SERVICIO	CANTIDADES	PRECIO DE VENTA UNITARIO SIN IVA	INGRESOS TOTALES
Desafíos Ilimitado	2000	$ 58.823	$ 117.647.059
Desafíos Limitado Acceso 3 meses	2000	$ 29.411	$ 58.823.529
Curso Fundamentos de Ciberseguridad	1.500	$ 42.016	$ 63.025.210
Seguridad de la Información	1.000	$ 126.050	$ 126.050.420
Seguridad de Aplicaciones	1.000	$ 50.420	$ 50.420.168
Gestión de Riesgos de Seguridad	1.000	$ 58.823	$ 58.823.529
		TOTAL	$ 474.789.916

Nota. Elaboración Propia.

Conclusiones financieras y evaluación de viabilidad

Para hacer una proyección precisa, se tomaron en cuenta los indicadores financieros macroeconómicos esperados en Colombia, como el Índice de Precios del Productor (IPP) y la inflación estimada para el próximo quinquenio, como se muestra en la siguiente tabla.

Tabla 4.

Proyección Indicadores Inflación e IPP.

AÑO	**2025**	**2026**	**2027**
INFLACIÓN	3,9%	3,0%	3,0%
IPP	8,0%	6,0%	6,0%

Nota. Elaboración Propia

En resumen, los siguientes son los indicadores de evaluación financiera para GAMSECURE, los cuales lo hacen ser un proyecto viable:

Ingresos totales del primer año: $474.789.916

Costos anuales: $95.000.000

Aporte Emprendedores: $30.000.000

Total de inversión: $312.000.000

Valor presente neto del proyecto VPN= $ 187.759.492,40 que corresponde al valor máximo que se va a recibir luego de recuperar la inversión.

Periodo de recuperación de la Inversión: El periodo se estima en 3,12 años, tiempo en el cual se habrá recuperado la inversión realizada.

TIR: 41,34% que corresponde al valor máximo que se recibe de utilidad por la inversión.

El punto de equilibrio requiere de la venta de accesos a los diferentes cursos por 3.393 usuarios en el mes.

En el proceso de evaluación de la rentabilidad del negocio de GAMSECURE, se examinaron los costos, la frecuencia anual y el porcentaje de participación de cada servicio que se busca monetizar.

Equipo de trabajo.

El equipo definido para la constitución de GAMSECURE se compone de los siguientes profesionales, los cuales aportarán su conocimiento en diferentes áreas, y quienes tendrán los roles que se describen a continuación:

Eumir Pulido de la Pava, Ingeniero de Sistemas, especialista en Administración de la Informática Educativa y especialista en Gerencia de Tecnología, con más de 18 años de experiencia como docente en programas de formación como lógica de programación,

desarrollo de software, análisis de datos y redes de datos estructurados. Afinidad como experto en docencia y desarrollo de software.

Alejandro Álvarez Alonso es Profesional en Administración Informática, especialista en Gerencia de Proyectos Informáticos, especialista en Seguridad Informática, con habilidades para la administración, dirección, desarrollo, asesoría y gestión de recursos de TI. Afinidad como experto en Ciberseguridad.

Freddy Orlando Martínez Bernal, profesional en Ingeniería de sistemas, cuenta con amplios conocimientos en la ingeniería de software, diseño y programación de sistemas electrónicos, especialista en telecomunicaciones y seguridad de la información, certificado como consultor internacional en la Norma ISO 27001. Afinidad como experto proyectos y robótica, desarrollo y auditor.

La formación de este equipo no sólo garantizará la operación diaria y el crecimiento sostenido de GAMSECURE, sino que también se asegurará de que se mantenga a la vanguardia en las áreas clave de gamificación y ciberseguridad. Es esencial que este equipo tenga una cultura de aprendizaje continuo, dado el rápido cambio en el mundo de la ciberseguridad.

Análisis del Sector

Características del sector.

El sector de la ciberseguridad está en constante evolución debido a las constantes amenazas y ataques cibernéticos. Como resultado, cada vez más empresas están buscando soluciones efectivas para proteger sus activos digitales y garantizar la privacidad de los datos de sus clientes. El tamaño del mercado de ciberseguridad se estima en USD 182.86 mil millones en 2023, y se espera que alcance los USD 314.28 mil millones para 2028, creciendo a una tasa compuesta anual de 11.44% durante el período de pronóstico (2023-2028) (Intelligence, 2023).

Colombia es uno de los países más afectados por ciberataques en América Latina, lo que ha llevado a un aumento en la demanda de soluciones de ciberseguridad y la necesidad de una educación en línea efectiva y accesible en este campo. Cuando se investiga la causa raíz de los incidentes de ciberseguridad, el porcentaje de ataques en su fase inicial utilizan técnicas de phishing, técnica que emerge al top de las técnicas y operaciones para el compromiso, llegando a en 2021 a ser el 41% de los incidentes. Es decir que la mayor parte de los ataques buscan debilidades que tienen origen en la preparación de las personas para el uso de la tecnología, ya sea por falta de reconocimiento de un email engañosos o por el uso de contraseñas débiles o iguales en múltiples sitios (X-Force®, 2022).

En este contexto, la educación en línea con técnicas de gamificación puede ser una herramienta efectiva para aumentar la conciencia y mejorar las habilidades en ciberseguridad. La gamificación puede hacer que el aprendizaje sea más atractivo e interactivo, lo que puede resultar en una mejor retención de la información y un aumento en la motivación de los estudiantes.

De acuerdo con el benchmark (EMIS, 2023) del sector de servicios profesionales, científicos y técnicos, se logra identificar un crecimiento de las empresas entre el 2017 y el 2021, en donde las ventas incrementaron un 38.37%, los activos 12.17%, la utilidad 166% y patrimonio un 10,24%, frente a un año 2020 en el que no hubo mayor diferencia frente a años anteriores.

Figura 1.

Benchmark - Servicios Profesionales, Científicos y Técnicos.

Año	2021	2020	2019	2018	2017
Empresas en industria	11919	11592	11016	10742	10075
Tamaño	**2021**	**2020**	**2019**	**2018**	**2017**
Ventas	68,235,242	49,311,889	44,861,405	44,582,951	35,434,209
Activos	115,642,495	103,091,263	77,213,710	65,847,253	59,417,720
Utilidad	7,549,789	2,828,822	3,703,297	5,545,358	2,417,943
Patrimonio	52,724,416	47,826,591	39,308,104	32,189,238	32,209,787
Crecimiento	**2021**	**2020**	**2019**	**2018**	**2017**
Crecimiento en Ventas %	38.37%	9.92%	0.62%	25.79%	2.69%
Crecimiento / Disminución en Activos	12.17%	33.51%	17.26%	10.82%	23.34%
Crecimiento / Disminución en Utilidad Neta	166.89%	-23.61%	-33.22%	129.33%	-8.75%
Crecimiento (Disminución) del Patrimonio	10.24%	21.67%	22.12%	-0.06%	45.10%

Nota: Base de Datos de Compañía de EMIS

Al realizar el mismo análisis, pero con el sector de Servicios Educativos, se identifica de igual forma un incremento en las ventas del 25%, los activos 25%, y utilidad neta del 50,62% y patrimonio del 4,67%.

Figura 2.

Benchmark - Servicios Educativos.

Año	2021	2020	2019
Empresas en industria	1569	1563	1665

Tamaño	2021	2020	2019
Ventas	10,362,680	8,265,630	7,334,019
Activos	72,051,781	57,460,980	42,183,419
Utilidad	1,602,309	1,063,776	1,082,530
Patrimonio	34,897,830	33,501,689	25,064,546

Crecimiento	2021	2020	2019
Crecimiento en Ventas %	25.37%	12.70%	19.56%
Crecimiento / Disminución en Activos	25.39%	36.22%	6.19%
Crecimiento / Disminución en Utilidad Neta	50.62%	-1.73%	51.23%
Crecimiento (Disminución) del Patrimonio	4.17%	33.66%	10.39%

Nota: Base de Datos de Compañía de EMIS

GAMSECURE también enfrenta la competencia de otros proveedores de soluciones de seguridad cibernética. La empresa deberá destacarse en un mercado saturado mediante la oferta de un enfoque innovador y centrado en el usuario para la educación de seguridad cibernética.

A continuación se hace un análisis del entorno y del mercado por medio de la herramienta PESTEL (Anexo 1. PESTEL), en la que se estudian los factores político, económico, social, tecnológico, ecológico y legal, para poder posibles oportunidades y amenazas externas:

Análisis político

El emprendimiento y la creación de empresa en Colombia se ve influenciado por las diferentes políticas de Gobierno, como lo son la consolidación de la paz, las políticas de justicia social, las políticas de justicia ambiental y las políticas de cambio para las mujeres, en donde su objetivo apunta a reducir las desigualdades de ingresos y de género, crecimiento verde, y una mayor protección de la biodiversidad y la consolidación

de una transición energética baja en carbono de acuerdo con el análisis del panorama en Colombia que hace el Banco Mundial (Mundial, 2023).

Reducir la pobreza es tal vez una de las metas para el Gobierno Colombiano más ambiciosa, en donde no solo se tiene que ampliar la cobertura y adaptación de un sistema de seguridad social, sino que debe flexibilizar el acceso a otros programas sociales, con el objetivo de mejorar los indicadores de desempleo, la calidad de la educación, la salud y la infraestructura.

Según el estudio de Corazones Productivos de la Secretaría de Desarrollo Económico, se evidencia que el 38 % de los propietarios de emprendimientos fueron creadas con objetivos de supervivencia (carencia de alternativas de ingresos y de habilidades para encontrar empleo), lo que traduce en una debilidad en las políticas sociales y de empleo. Bogotá es el principal centro económico de Colombia, con un aporte del 26 % al PIB nacional y del 27 % al empleo formal del país. La economía de la ciudad es movilizada por una población en edad de trabajar de 6,4 millones de habitantes (Bogotá F. C., 2023).

En un contexto político, la implementación de regulaciones proactivas de ciberseguridad, así como las políticas de puede crear oportunidades significativas para GAMSECURE. Los cambios repentinos así mismo pueden representar una amenaza.

Análisis económico

De acuerdo con el Dane, las actividades económicas que más contribuyen a la dinámica del valor agregado son (Dane, 2023), actividades financieras y de seguros con un crecimiento del 22,8%, actividades artísticas, de entretenimiento y recreación y otras actividades de servicios con un crecimiento del 18,7%.

En el segundo trimestre de 2023pr, el valor agregado de las actividades profesionales, científicas y técnicas; y actividades de servicios administrativos y de apoyo decrece 0,2% en su serie original, respecto al mismo periodo de 2022pr. Esta dinámica se da

principalmente por los siguientes cambios (Dane, 2023), actividades profesionales, científicas y técnicas decrecen 1,3%, y las actividades de servicios administrativos y de apoyo crecen 0,6%.

De la misma forma el DANE en su Encuesta Mensual de Servicios (EMS) de agosto de 2023, en donde se muestra la variación anual de los ingresos nominales, confirma un aumento del 12,7% preliminar para el sector de desarrollo de sistemas informáticos y procesamiento de datos (Dane, 2023). Este aumento es una señal positiva para las empresas emergentes en el sector tecnológico, como GAMSECURE, indicando un mercado en crecimiento y una oportunidad para el desarrollo y expansión en este ámbito.

En un entorno económico favorable a la inversión en ciberseguridad, GAMSECURE podría beneficiarse de la creciente demanda de servicios educativos. Empresas y organizaciones que refuercen sus medidas de seguridad podrían ser clientes potenciales, lo que acelera el crecimiento de la empresa.

Análisis social cultural

Las reformas sociales que se intentan promover por el Gobierno actual buscan responder a las necesidades que los ciudadanos han manifestado desde el estallido social antes de la pandemia, y en donde se quiere mejorar las condiciones de salud, pensión, trabajo y educación (República P. d., 2023).

Las características demográficas de los usuarios, como la edad, el nivel educativo y el acceso a la tecnología, pueden influir en el diseño y la estrategia de implementación de la plataforma. La digitalización y el acceso a nuevas tecnologías puede facilitar a los usuarios el proceso, satisfaciendo las necesidades de los diferentes grupos de usuarios.

Adicionalmente y de acuerdo con las metas del plan nacional de desarrollo 2022 – 2026 del Gobierno de Colombia (DNP, 2023), las metas relacionadas con el Derecho

Humano a la Alimentación y la Pobreza extrema, existe una oportunidad para GAMSECURE de ofrecer soluciones de empleo o contribuir a iniciativas que empoderen a los más vulnerables, tal vez a través de programas de capacitación.

El meta y objetivo de duplicar el acceso a internet (DNP, 2023) puede conducir a una creciente necesidad de soluciones de seguridad cibernética, un área en la que GAMSECURE puede desempeñar un papel crucial.

Las metas del PND 2022-2026 (DNP, 2023) de Colombia muestran un claro énfasis en el bienestar social, la infraestructura, la sostenibilidad y la digitalización. Para GAMSECURE, esto significa una serie de oportunidades para expandir sus servicios, adaptarse a las necesidades cambiantes del país y contribuir activamente al desarrollo sostenible de Colombia.

La creciente conciencia de la sociedad sobre los riesgos cibernéticos es una gran oportunidad para GAMSECURE. A medida que la sociedad se dé cuenta de la importancia de la ciberseguridad, la plataforma de aprendizaje podría posicionarse como un recurso importante para satisfacer esta creciente demanda de conocimiento especializado.

Análisis tecnológico

El desarrollo y éxito de una plataforma web depende de la disponibilidad, soporte y el acceso a la tecnología adecuada. Es importante estar al tanto de las últimas tendencias tecnológicas, como la Ciberseguridad, la inteligencia artificial y el desarrollo de juegos, para aprovecharlas en la plataforma y mantenerla actualizada.

El Ministerio TIC de Colombia ha identificado la educación (MINTIC, 2023) como un factor crítico en su estrategia de ciberseguridad. GAMSECURE podría alinear sus estrategias de formación o concienciación con esta iniciativa, ofreciendo programas educativos o capacitaciones en alianza con entidades gubernamentales.

La formación de la Agencia Nacional de Ciberseguridad demuestra un compromiso gubernamental con la ciberseguridad (MINTIC, 2023). GAMSECURE podría buscar oportunidades para colaborar con esta nueva agencia, ya sea como proveedor de soluciones tecnológicas, consultor o socio estratégico.

Con la intención del gobierno de posicionar a Colombia como un centro de referencia en ciberseguridad, GAMSECURE podría considerar ampliar su presencia en el país, invertir en innovación local y buscar alianzas estratégicas. Esto podría incluir asociaciones con centros de investigación, universidades y otras empresas del sector.

GAMSECURE podría considerar alianzas con el Colcert, ofreciendo soluciones tecnológicas avanzadas, formación o servicios de consultoría.

El enfoque renovado de Colombia en la ciberseguridad, apoyado por inversiones significativas y la creación de nuevas entidades, presenta numerosas oportunidades para GAMSECURE. La empresa podría alinear sus objetivos y estrategias con las del gobierno colombiano, buscando alianzas estratégicas, participando en iniciativas educativas y ofreciendo soluciones tecnológicas avanzadas. Es esencial que GAMSECURE esté al tanto de estos desarrollos y actúe proactivamente para maximizar las oportunidades en este mercado en crecimiento.

Análisis ecológico

El impacto ambiental de la plataforma web y las estrategias de gamificación es importante. Se deben adoptar medidas para minimizar la huella ecológica, como el uso eficiente de los recursos, la gestión adecuada de los desechos electrónicos y el fomento de prácticas sostenibles.

Aunque la ciberseguridad y el ámbito ecológico parecen estar en diferentes esferas, en el contexto del Plan Nacional de Desarrollo de Colombia, existen puntos de intersección que GAMSECURE podría considerar: El plan nacional destaca una

transición hacia fuentes de energía renovable y el impulso hacia una economía verde (DNP, 2023). GAMSECURE podría adoptar y promover prácticas ecológicamente sostenibles en sus operaciones, como el uso de energías renovables en sus centros de datos o la optimización de sus sistemas para reducir el consumo de energía.

Mientras que GAMSECURE opera en el ámbito digital, podría asumir un compromiso social y ecológico apoyando proyectos de reforestación o restauración ecológica en Colombia.

Por otra parte, el ministro TIC menciona la intención de hacer de Colombia un 'HUB de ciberseguridad' (MINTIC, 2023), GAMSECURE podría diferenciarse al ser una empresa de ciberseguridad con un fuerte compromiso ecológico, promoviendo prácticas sostenibles no solo en sus operaciones, sino también en el diseño y promoción de sus productos.

GAMSECURE podría desarrollar y ofrecer soluciones y servicios que no solo protejan la infraestructura digital de las empresas y entidades, sino que también promuevan la sostenibilidad y reducción del impacto ambiental, como sistemas optimizados para menor consumo de energía o software diseñado con principios de economía circular.

Análisis legal

De acuerdo con lo requerido por la Superintendencia Financiera de Colombia Circular Externa 042 de 2012 y la 007 de 2018, y las directrices de Gobierno Digital, las entidades financieras deben contar con controles y medidas para evaluar y defender los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).

De acuerdo con MINTIC el gobierno colombiano tiene la intención de crear una Agencia Nacional de Ciberseguridad. Esto probablemente llevará a la implementación de nuevas normativas y regulaciones que las empresas de ciberseguridad deberán

cumplir. GAMSECURE deberá mantenerse informado sobre las directrices de esta nueva entidad para asegurarse de que sus servicios y operaciones estén en conformidad con cualquier nueva regulación.

GAMSECURE deberá estar al tanto de las directrices de Gobierno Digital para asegurarse de que sus soluciones se adapten a los estándares y requerimientos del gobierno colombiano en términos de ciberseguridad y protección de datos.

Dado el énfasis actual en la preparación y respuesta a amenazas de ciberseguridad, GAMSECURE debe asegurarse de tener productos y servicios efectivos para ayudar a las organizaciones a responder rápidamente a cualquier amenaza o vulnerabilidad, en conformidad con las normativas locales.

Es fundamental que GAMSECURE se adhiera a las leyes de protección de datos en Colombia. Estas leyes tienen como objetivo proteger la información personal de los ciudadanos y garantizar que las empresas que manejan datos personales lo hagan de forma segura y responsable.

Dada la naturaleza cambiante de la ciberseguridad y las regulaciones asociadas, es esencial que GAMSECURE mantenga una formación continua para su equipo y actualice regularmente sus soluciones para cumplir con las regulaciones más recientes y brindar la mejor protección posible.

Para operar de forma efectiva, GAMSECURE deberá mantenerse al tanto de las regulaciones y directrices relacionadas con la ciberseguridad, especialmente aquellas emitidas por entidades gubernamentales como el MinTIC y la Superintendencia Financiera de Colombia. Esto no solo garantizará la conformidad legal de GAMSECURE, sino que también le proporcionará una ventaja competitiva al ofrecer soluciones que están alineadas con las necesidades específicas y los requisitos legales del mercado colombiano.

Matriz de Perfil Competitivo

La Matriz de Perfil Competitivo (MPC), tiene en cuenta los factores clave de éxito en la industria de e-learning enfocada en ciberseguridad con técnicas de gamificación, en la que se asigna un peso a cada factor, dependiendo de su importancia en la industria, y luego se califica a cada empresa en esos factores, registrando 1 si es Gran Debilidad, 2 Debilidad menor, 3 Fuerza menor, y 4 Gran fortaleza. El resultado se obtiene de multiplicar los pesos para obtener puntuaciones ponderadas y que al sumar permiten obtener un total que refleja la fuerza competitiva de cada empresa. Los siguientes son los factores clave de éxito para la Industria de e-learning en Colombia y el peso asignado, en done la suma debe ser igual o menor a 1:

1. Innovación (0.30)
2. Calidad en el Contenido (0.15)
3. Acompañamiento en el Proceso (0.10)
4. Productos y servicios de e-learning a la medida (0.25)
5. Calidad del Servicio (0.20)

De acuerdo con el análisis, la empresa Cátedra e-learning es el competidor más fuerte con una puntuación total de 3.70, indicando que tiene un perfil competitivo robusto en la industria. Esto se contrasta con sus estados financieros, ya que en el 2020 tuvo ingresos netos por ventas de 2.063 millones de pesos y una ganancia neta de 372 millones, y en 2022 de 1.429 millones. Cibernos Colombia S.A.S. tiene una posición financiera sólida y competitividad de precios, pero necesita trabajar en innovación y calidad de servicio, en el 2022 tuvo Ingresos netos por ventas de 2050 y ganancia neta de 239 millones (EMIS, 2023). Gestionet Colombia S.A.S. debe trabajar en casi todos los aspectos para mejorar su posición competitiva, quien a su vez en 2022 tuvo unos ingresos netos de 3.134

millones y una ganancia neta negativa de -331 millones de pesos. GAMSECURE, debe centrarse en la innovación y en la calidad de contenido.

Tabla 5.

Matriz de perfil competitivo MPC.

Empresa	Cátedra e-learning		Cibernos Colombia S.A.S.		GAMSECURE		Gestionet Colombia S.A.S.	
Criterio	**Calificación**	**Calificación Ponderada**	**Calificación**	**Calificación Ponderada**	**Calificación**	**Calificación Ponderada**	**Calificación**	**Calificación Ponderada**
Innovación (0.30)	3	0,90	2	0,60	3	0,90	2	0,60
Calidad en el contenido (0.15)	4	0,60	3	0,45	3	0,45	3	0,45
Acompañamiento en el proceso (0.10)	3	0,60	4	0,40	4	0,40	3	0,30
Productos y servicios de e-learning a la medida (0.25)	4	1,00	3	0,75	4	1,00	2	0,50
Calidad del Servicio (0.20)	3	0,60	2	0,4	3	0,60	2	0,40
Puntuación Total		**3,70**		**2,60**		**3,35**		**2,25**

Nota: Elaboración propia.

Como conclusión, se encontró que GAMSECURE tiene un valor agregado frente a las demás empresas principalmente por su innovación en el uso de técnicas de gamificación personalizables y el acompañamiento en el proceso de acompañamiento.

Validación e Investigación de Mercado

Análisis del cliente frente a la propuesta de valor

Se implementará un instrumento de medición efectivo que valorará la aceptación de los clientes hacia las funcionalidades innovadoras y especificaciones técnicas del servicio propuesto, corroborando así la demanda potencial necesaria para la formulación de un plan de negocio sólido.

En este contexto, se tomará en cuenta la perspectiva de profesionales de variados niveles de conocimiento en ciberseguridad, desde principiantes hasta expertos, y de diferentes trasfondos educativos que pueden incluir estudios técnicos, licenciaturas, maestrías y doctorados, enfocándonos en un espectro de edad amplio que va de los 21 a los 56 años. Esta amplitud asegura que GAMSECURE pueda adaptarse a un mercado diverso y en constante cambio. La información recopilada será decisiva para descifrar las necesidades específicas del mercado y las oportunidades para ofrecer un servicio altamente diferenciado y competitivo. Este servicio no solo cumplirá con las expectativas de aprendizaje interactivo y dinámico en Ciberseguridad sino que también propiciará una experiencia de usuario inmersiva y atractiva.

Los datos obtenidos permitirán diseñar estrategias de marketing y comunicación altamente focalizadas y efectivas, que resonarán con nuestro público objetivo y fomentarán la percepción de valor en nuestros clientes, garantizando que GAMSECURE no solo sea reconocido como un producto líder en el campo educativo de la ciberseguridad, sino también como una experiencia innovadora en aprendizaje gamificado.

Necesidades y Oportunidades del Cliente

Necesidad del empleado: Búsqueda de métodos de aprendizaje innovadores que mejoren la retención de la información y sean más comprometedores, así como la necesidad de contar con soluciones de aprendizaje que se ajusten a horarios personales y profesionales. Todo esto soportado en el interés en adquirir habilidades en áreas emergentes como ciberseguridad.

Necesidad de la empresa: Tener personal entrenado en temas de ciberseguridad, con el propósito de reducir el riesgo de sufrir perdida de información o afectaciones a los servicios.

Justificación

El aprendizaje gamificado permite a los empleados y empresarios, capacitarse con técnicas más atractivas y efectivas que los métodos tradicionales. Los posibles clientes estarán dispuestos a pagar por acceso a plataformas gamificadas que ofrezcan contenido de calidad, y que les facilite desarrollar habilidades técnicas en ciberseguridad.

Propuesta de Valor

GAMSECURE ofrece capacitación en Ciberseguridad con contenido personalizado y de calidad, para las pequeñas y medianas empresas, a través de una plataforma e-learning con un diseño amigable, fácil de usar, con técnicas de gamificación y un soporte y acompañamiento virtual constante, para crear una experiencia única. Mejorando el proceso de sensibilización de los empleados en las empresas, y reduciendo el nivel de riesgo.

Objetivos del Estudio de mercado

Recolectar y analizar información del mercado asociado a la propuesta de GAMSECURE.

Determinar el grado de aceptación de las plataformas de aprendizaje basadas en gamificación.

Determinar la disposición a pagar por cursos gamificados.

Estimar la demanda potencial y la proyección de ventas para cursos de gamificación en línea.

Cálculo de la Muestra

De acuerdo con el análisis (DANE, s.f.), la población de empresas pequeñas y medianas es de 100.825. Con esta información y con la siguiente formula, se realiza el cálculo del tamaño de la muestra:

$$n = \frac{K^2 qpN}{e^2(N-1) + K^2 pq}$$

n = Tamaño de muestra buscado

N = Población o Universo. El número total de personas que podían ser encuestados.

K = Nivel de Confianza, probabilidad de que las respuestas sean ciertas y se sustituye de la siguiente manera. Valor de K cuando el nivel de confianza es 95%, es 1,96.

z = Parámetro estadístico que depende del Nivel de Confianza (NC)

e = Margen de Error, Diferencia entre las respuestas de la muestra y del total de la población.

p = Probabilidad de éxito, proporción de individuos en la población que poseen una característica especifica, que para este caso es 0,5.

q = Probabilidad de fracaso, proporción de individuos que no poseen una característica especifica, e para este caso es 0,5.

De acuerdo con el valor de cada variable, K = 1,96, q = 0,5, p = 0,5, N = 365, e = 5%, se obtiene como resultado la cantidad de empresas que deben participar en la encuesta, el cual es un mundo de n = 188 empresas.

Dado que la muestra de 188 pequeñas y medianas empresas representa un esfuerzo significativo en términos de tiempo y recursos para aplicar la encuesta, y considerando que el objetivo principal es validar la viabilidad del modelo de negocio de GAMSECURE, el siguiente análisis se enfocó en dos grandes entidades como lo son el SENA y las Fuerzas Militares de Colombia, quienes apoyaron el desarrollo y aplicación de la herramienta diseñada con un grupo representativo de empleados, y que fue soportada por la entrevista de diferentes empresarios, con lo cual se tiene una mezcla que busca complementar y representar ese universo.

Estas instituciones, debido a su alcance y tamaño, ofrecen una representación significativa del mercado y permiten obtener aportes valiosos sobre la viabilidad del modelo de negocio de GAMSECURE. Particularmente, el SENA tiene una red extensa de conexiones con empresas de diversos sectores, lo que facilita la evaluación de la plataforma y las técnicas de gamificación en un contexto real de aplicación. Asimismo, las Fuerzas Militares de Colombia representan un entorno crítico que requiere altos estándares de seguridad y formación en ciberseguridad, lo que proporciona una perspectiva importante para la validación del modelo.

Al colaborar con estas dos instituciones, se logra obtener un detalle relevante sobre la funcionalidad y efectividad de la plataforma GAMSECURE, así como sobre la aplicación práctica de las técnicas de gamificación en el ámbito de la Ciberseguridad, permitiendo demostrar que la plataforma es capaz de adaptarse y ser útil para cualquier tipo de

empresa, independientemente de su tamaño o sector, lo que respalda la conclusión de que GAMSECURE puede ser comercializado con éxito en el mercado empresarial.

Diseño de las Herramientas de Investigación

Para el desarrollo de la investigación, se aplicó una herramienta tipo entrevista (Anexo 5. Ficha Técnica Entrevistas) con preguntas abiertas y dirigida a personas que por su experiencia profesional permiten validar el modelo de negocio sostenible, y a su vez se aplicó una herramienta tipo encuesta (Anexo 2. Herramienta Encuesta) por medio de un cuestionario con 20 preguntas relacionadas con los productos de la plataforma de GAMSECURE, para lo cual necesitaron tener acceso y realizar un mini curso en el prototipo de plataforma de GAMSECURE, en el que no solo se muestra contenido relacionado con la ciberseguridad sino que se utilizan técnicas de gamificación. El cuestionario fue dividido en preguntas que permiten caracterizar la persona encuestada, definir su nivel de escolaridad, conocer su necesidad de mejorar su habilidad profesional, e identificas los factores decisivos para tomar los cursos por medio de la plataforma.

Análisis de resultados entrevistas

Se llevaron a cabo entrevistas dirigidas a un grupo dirigido de posibles aliados estratégicos, clientes potenciales, empresarios, emprendedores, expertos técnicos y expertos en sostenibilidad. Este enfoque permitió obtener información valiosa y perspectivas diversas sobre las necesidades y expectativas del mercado para asegurar un modelo de negocio robusto y una plataforma de e-learning efectiva que responda a las demandas del sector empresarial y con el cual se pueda contrastar con el resultado de la herramienta de encuestas, para validar el modelo de negocio sostenible propuesto por GAMESECURE.

Entrevistas Aliados Estratégicos

El ingeniero Víctor Aguirre (Anexo 6. Validación Entrevistas) que una forma de colaborar con GAMSECURE es utilizar la plataforma para estimular las empresas e incentivarlas, lo que fortalece este proyecto de formación en ciberseguridad online dirigido a las PYMES. Su experiencia en diseño de sistemas y gestión de proyectos, respaldada por una Maestría en Tecnología Innovadora, lo convierte en un aliado clave. Reconoce la importancia de aumentar la seguridad cibernética en las PYME y le interesa ofrecer una plataforma interactiva como la propuesta para promover salvaguardar la infraestructura tecnológica de las organizaciones. Destaca la necesidad de recursos actualizados y apoyo técnico, financiero y humano para garantizar el éxito. Enfatiza la importancia de establecer el retorno de la inversión y acuerdos contractuales claros. Recalca lo importante del aporte de esta clase de soluciones a universidades y otras Pymes. Anexo 5. Ficha Técnica Entrevistas y Formato Entrevista

El ingeniero Luis Fernando Tamayo Bustamante (Anexo 6. Validación Entrevistas) manifiesta interés en colaborar con GAMSECURE en el proyecto mencionado. Su vasta experiencia en alta dirección, gestión financiera, gestión de proyectos y economía empresarial lo posiciona como un aliado clave para impartir formación y promover mejores prácticas en ciberseguridad. Respecto a los recursos necesarios, enfatiza la importancia de contar con personal calificado, recursos financieros y técnicos adecuados. Sugiere que GAMSECURE se enfoque en la gestión y control de datos para generar confianza entre los clientes, garantizando así la integridad y seguridad de la información. Destaca la confianza como valor clave para establecer una relación de trabajo duradera y mutuamente beneficiosa. Propone el uso de una plataforma de formación en Ciberseguridad y la implementación de mecanismos de seguimiento y control periódicos, así como la adopción de métodos ágiles como Scrum para un desarrollo efectivo del proyecto. En cuanto a socios clave, sugiere la posibilidad de establecer alianzas con

organismos gubernamentales a través de organismos oficiales para implementar modelos de capacitación en ciberseguridad. Señala la importancia de minimizar los riesgos informáticos y garantizar la confiabilidad del alojamiento de datos con servidores adecuados.

En ambas entrevistas se puede destacar que ambos profesionales se encuentran interesados como aliados estratégicos, lo que genera una buena percepción y aceptación del proyecto mencionado. Frente a la percepción del ingeniero Víctor Aguirre, él se centra en las implicaciones de la transformación digital para las PYME y cómo una plataforma educativa puede contribuir a la seguridad de los datos y la infraestructura técnica de sus organizaciones. Por su parte, el ingeniero Luis Fernando Tamayo destaca la importancia de considerar las medidas de ciberseguridad y las buenas prácticas que deben tener las PYME para garantizar la confianza de los clientes.

Entrevistas Clientes Potenciales

La principal preocupación de la cooperativa COOMPER, encabezada por el ingeniero Cesar Augusto (Anexo 6. Validación Entrevistas), es la ciberseguridad en la empresa. Reconoce la importancia de capacitar a los usuarios y mejorar las prácticas de seguridad. Actualmente tienen servidores físicos y máquinas virtuales, pero hay problemas de gestión de datos con los usuarios. Buscan recursos de formación breves y específicos con un modelo de precios atractivo. Para él una plataforma de formación debe ser intuitiva y fácil de usar. Es evidente que los colaboradores no conocen las normas de seguridad o no cuentan con certificaciones de seguridad, dado que, los perfiles y manuales de funciones no exigen contar con este tipo de experiencia o conocimiento académico. COOMPER no cuenta con un plan de respaldo sólido. La seguridad de los datos se considera importante, pero puede ser difícil priorizarla sobre otras inversiones, al igual que no tienen una política de capacitación establecida y comparten información

aleatoriamente a través de grupos de WhatsApp y obviamente no han tenido la oportunidad de que se haya utilizado antes plataformas de formación en ciberseguridad.

La Compañía de Seguros POSITIVA a través de su Gerente Regional Jorge Pérez (Anexo 6. Validación Entrevistas) se ocupa de la protección de los datos de los clientes y de la confidencialidad de estos. Para el Gerente hay un referente muy positivo frente al nivel de ciberseguridad en su empresa, pero busca mejorar la practicidad de los procesos de seguridad con todos sus colaboradores. Considera esencial la capacitación en antivirus y aplicaciones de escritorio y por esta razón es tan valiosa la propuesta de una plataforma de formación en ciberseguridad, pero destaca la importancia que desde este medio se genere la concienciación de la importancia del uso adecuado y responsable de la información entre el equipo de trabajo de POSITIVA. No existe una política de formación en ciberseguridad establecida, pero se organizan campañas de formación, por esta razón el Doctor Jorge Pérez considera factible la propuesta y se suma a revisar propuestas que permitan un vínculo comercial entre GAMSECURE SAS y la Compañía de Seguros POSITIVA.

Tanto la Cooperativa del Municipio de Pereira y Departamento de Risaralda “COOMPER” como la compañía de Seguros POSITIVA, tienen preocupaciones similares sobre la protección de los datos de sus clientes y la confidencialidad de dicha información. Ambos reconocen la importancia de implementar medidas de seguridad ciberseguridad para garantizar transacciones seguras e integridad de datos. Ambos clientes enfrentan desafíos para mejorar la seguridad cibernética, por un lado, el ingeniero César Augusto se enfoca en asegurar el conocimiento y cumplimiento de las políticas de seguridad por parte de su equipo de trabajo, mientras que el Gerente Jorge Pérez trabaja para que los procesos de seguridad sean prácticos y efectivos para sus empleados. En cuanto a la formación en ciberseguridad, ambos consideran importante obtener información y recursos para reforzar la seguridad de su empresa. El ingeniero

César Augusto busca capacitaciones en prácticas seguras como la detección de ataques de phishing, mientras que desde POSITIVA enfatiza el uso adecuado de antivirus y aplicaciones de escritorio. Finalmente, ambos clientes consideran que la plataforma de capacitación es útil para su negocio y consideran la viabilidad de generar vínculos comerciales.

Entrevistas Emprendedores - Empresarios

El empresario Santiago Londoño Gerente (Anexo 6. Validación Entrevistas) Comercial de la empresa Dotación Integral, reconoce la necesidad de formar a las PYME en ciberseguridad debido a los frecuentes ataques informáticos y la falta de departamentos de tecnología en dichas empresas, además, cree que existe una demanda real de formación en ciberseguridad en el mercado actual. En cuanto a preocupaciones y desafíos, Santiago destaca la necesidad de proteger los datos de la empresa, incluida la información contable y financiera, las cuentas bancarias y los datos técnicos digitales propios de la empresa. Estas consideraciones son importantes para garantizar la seguridad de los datos y evitar posibles pérdidas o violaciones de la privacidad. Enfatiza que es importante adaptar la capacitación a las necesidades específicas de la empresa y garantizar su facilidad de uso. Esto demuestra su interés en crear una relación comercial justa y mutuamente beneficiosa. Santiago estimó que, en términos de beneficios para su empresa, el uso de una plataforma de capacitación en seguridad cibernética aumentaría la capacidad de la empresa para prevenir y responder a los ataques cibernéticos. A largo plazo, esto tendría un impacto positivo en el negocio, garantizando la seguridad de los datos y protegiendo la reputación de la empresa.

El emprendedor Rodolfo Vega (Anexo 6. Validación Entrevistas) de No Rules Sport reconoce la necesidad de formar a las PYME en ciberseguridad y cree que existe una demanda real de este tipo de formación en el mercado actual. Su empresa, que se

enfoca en el desarrollo, la fabricación y la venta de ropa y equipos deportivos, se dio cuenta de la importancia de la seguridad cibernética al digitalizar la cantidad de información manejada por y a través de los canales de mercadeo. Una de las preocupaciones o desafíos que enfrenta la empresa es la falta de entendimiento entre la fuerza laboral sobre la importancia y sensibilidad del manejo de contraseñas e información. El empresario destaca casos concretos en los que el desconocimiento de la ciberseguridad ha provocado la pérdida de información y la necesidad de proteger las plataformas utilizadas, como Instagram, donde tienen un número importante de seguidores y donde se realizan transacciones. En cuanto a la cooperación, el empresario recomienda adaptar la formación de la plataforma a las necesidades de su empresa. Además, señala que la plataforma puede ayudar a aumentar la capacidad de su empresa para anticipar y responder a los ataques de seguridad, lo cual es esencial para proteger los datos y prevenir posibles daños.

Ambos empresarios coinciden en la necesidad de formar a las PYME en temas de ciberseguridad y reconocen la demanda real de formación en este ámbito en el mercado actual. Ambos entienden que la mayoría de los canales de marketing son digitales, es importante proteger los datos y comprender la importancia de la seguridad en línea. En general, hay una falta de herramientas disponibles para los vendedores y empresarios para gestionar esta información, al igual que la sensibilización en el uso de contraseñas y el manejo de la información que se da de forma administrativa y empresarial. Ambos enfatizan en la necesidad de capacitar a sus empleados en ciberseguridad y proteger las plataformas que utilizan, como las redes sociales, donde tienen una importante base de seguidores y constantemente se hacen negocios. Se enfatiza en la importancia de construir una relación comercial justa y sostenible a largo plazo entre las partes.

Entrevista Experto Técnico

El experto técnico Sandra Milena Villa (Anexo 6. Validación Entrevistas) introdujo varios aspectos relevantes para el desarrollo de una plataforma en línea de capacitación en Ciberseguridad para PYMES y enfatizó la importancia de entender el grupo objetivo de la plataforma, sus necesidades, gustos y expectativas. Esto incluye la identificación de los proveedores y desarrolladores de los materiales y los métodos utilizados. También se menciona que es importante conocer las expectativas que tiene el cliente frente al uso de la plataforma. Resalta la importancia de según los niveles del curso, manejar temas de firewall, seguridad de tipos de conexiones, VPN y tipos de ataques. Además, enfatiza la necesidad de brindar información práctica, ya que solo la teoría no es suficiente. Recomienda involucrar laboratorios para que los usuarios puedan aplicar los conocimientos en escenarios reales y estar preparados para situaciones de seguridad. También menciona que el desafío es la escalabilidad de la plataforma, ya que las necesidades y requerimientos de los usuarios pueden cambiar con el tiempo. Por último destaca que es importante adaptarse a las necesidades de los usuarios y mantener la plataforma actualizada y disponible.

Entrevista Experto Sostenibilidad

La profesora María Cristina (Anexo 6. Validación Entrevistas) muestra gran interés por mejorar los procesos de las PYME desde el punto de vista de la seguridad de la información y el desarrollo sostenible. Reconoce la importancia de llegar a tiempo a estas empresas y organizaciones para mejorar sus operaciones y cumplir con la normativa vigente. En cuanto a las mejores prácticas para el desarrollo sostenible en la industria de la ciberseguridad, la Magister María Cristina destaca la eficiencia energética y la gestión responsable de los recursos necesarios para el mantenimiento de la plataforma. Integrar estas prácticas en la plataforma requiere tomar medidas para optimizar el uso de los

recursos electrónicos y asegurar la correcta gestión de los residuos generados, además, considera importante crear alianzas estratégicas para minimizar costos y maximizar el impacto social. En cuanto al involucramiento de los stakeholders y comunidades locales, la docente María Cristina recomienda crear alianzas con empresas involucradas en el cambio tecnológico y entidades de apoyo como las cámaras de comercio. Estas alianzas facilitarían la participación comunitaria y asegurarían un apoyo sostenible para la creación de la plataforma. Por último, destaca que es importante buscar sinergias con otras iniciativas de desarrollo sostenible en el ámbito de la ciberseguridad.

Análisis de los resultados encuesta

A continuación, se hace un análisis de resultados de la encuesta aplicada, la cual se puede consultar en el Anexo 2. Herramienta Encuesta:

Cerca de la mitad (48.4%) están familiarizados con plataformas que utilizan gamificación, o tienen conocimiento previo de gamificación.

La mitad de los entrevistados (50.5%) no han utilizado plataformas de aprendizaje basadas en gamificación antes.

Existe un interés significativo en aprender ciberseguridad (28.7%) a través de plataformas gamificadas.

Existe una alta disposición para pagar por cursos gamificados de alta calidad (87%).

Una mayoría está de acuerdo en que los cursos gamificados retienen más su atención (62.8%) y pasarían entre 1 y 2 horas semanales en la plataforma de aprendizaje en línea (39.4%).

Los encuestados prefieren las redes sociales (47.9%) y los correos electrónicos (45.2%) para recibir información acerca de nuevos contenidos.

La calidad del contenido es el más importante al elegir una plataforma de aprendizaje (64.9%).

Así mismo y de acuerdo con su nivel educativo, se identificaron 4 participantes con maestría (2.1%), 15 con postgrado (8%), 26 con título profesional (13.8%), 93 con estudios técnico/tecnólogos (49.5%), y 50 bachilleres (26.6%). Los directivos que participaron tienen un nivel de educación entre maestría y postgrado.

En general los resultados obtenidos en las entrevistas y de las encuestas, convergen en una percepción positiva y una buena disposición hacia las plataformas de aprendizaje gamificadas, así como una voluntad de parte de los usuarios y empresarios de pagar por este tipo de contenido, especialmente en áreas como la ciberseguridad. La calidad del contenido es primordial, y los elementos de gamificación más apreciados pueden ser clave para el diseño de futuras plataformas. De la misma forma, el diseño amigable y la facilidad de uso son muy importantes para los ambos. La comunicación efectiva a través de redes sociales y correos electrónicos puede ser vital para la adopción y la vinculación de los usuarios con este tipo de plataformas.

La mayoría no está utilizando actualmente estas plataformas, lo que indica un mercado no saturado con potencial de crecimiento.

El interés en ciberseguridad podría estar vinculado a la creciente importancia de la seguridad informática en las empresas y todos los sectores.

El resultado también confirma que existe el interés por esta clase de servicios propuestos por GAMESECURE, lo que hace de esta propuesta viable desde el punto de vista de usuarios y empresario.

Lienzo de modelo de negocio sostenible

De acuerdo con la herramienta deentrevista lienzo de modelo sostenible Anexo 7. Lienzo de Modelo de Negocio Sostenible, la propuesta de valor se debe centrar en la formación en ciberseguridad, y esta debe ser atractiva y efectiva con técnicas de gamificación, enfocando parte de su servicio en el soporte dedicado. Los principales

beneficios sociales serán el promover la Cibersegurdad por medio de una plataforma en línea los productos y servicios, dirigido inicialmente a pequeñas y medianas empresas que busquen fortalecer la conciencia y las habilidades en Ciberseguridad. La idea de negocio es creativa y novedosa en el mercado, con lo cual se puede apoyar en aliados clave que permitan promocionar y referenciar los servicios, tal y como las empresas de tecnología, otras plataformas de educación y las mismas instituciones educativas. Gamesecure es consciente del impacto ambiental y social que se deriva de reducir las emisiones de carbono, incentivando el uso de tecnologías limpias, las políticas de cero papel y el uso de centros de datos que cumplan con condiciones de eficiencia energética. El principal canal es la plataforma web, y el relacionamiento con el cliente debe ser a través de un soporte técnico personalizado. Los principales costos se derivan del desarrollo de contenido con técnicas de gamificación, así como la promoción de la plataforma y su mantenimiento.

Cálculo de la demanda potencial

Utilizando la información proporcionada por el Dane (DANE, s.f.), respecto a la cantidad de empresas Pymes en la ciudad de Bogotá se puede realizar el cálculo la demanda potencial de GAMSECURE, de la siguiente forma:

Total de Empresas en Colombia: 5,704,308

Total de Pequeñas y Medianas Empresas (Pymes): 81,725 (pequeñas) + 19,100 (medianas) = 100,825

Porcentaje de PYMES en Colombia = (Total de PYMES / Total de Empresas) * 100

Porcentaje de PYMES en Colombia = (100,825 / 5,704,308) * 100 ≈ 1.77%

Porcentaje de Empresas en Bogotá = 28.1%

Porcentaje de PYMES en Colombia = 1.77%

Porcentaje de PYMES en Bogotá = (Total de Empresas en Colombia) * (Porcentaje de Empresas en Bogotá) * (Porcentaje de PYMES en Colombia)

Porcentaje de PYMES en Bogotá = 5,704,308 * 0.281 * 0.0177 ≈ 28,371

Porcentaje de PYMES en Bogotá: 28,371 * 28.7% (% de posibles interesados resultado de la pregunta 5 Anexo 2. Herramienta Encuesta)

Demanda Potencial en Bogotá = 8,131

De esta forma se estable la demanda potencial de GAMSECURE para las PYMES en Bogotá de aproximadamente 8,131 empresas, basada en el interés en aprender ciberseguridad a través de plataformas gamificadas.

Proyección de ventas

La siguiente proyección se hace a partir de la identificación de las empresas potenciales en Bogotá (8,131 empresas) y en donde se estima que tengan en promedio 100 empleados, y suponiendo que cada uno tome como mínimo un curso en promedio de $70.000, y capturando el 10% de ese mercado potencial.

Primer escenario: La proyección de ventas sería igual a: 8,131 empresas x 100 empleados x $70.000 COP x 10% participación de mercado = $ 569.170.000. En este escenario todos los empleados tomaran el curso ilimitado.

Segundo escenario: La proyección de ventas sería igual a: 8,131 empresas x 100 empleados x $35.000 COP x 10% participación de mercado = $284.585.000. En este escenario todos los empleados tomaran el curso limitado al acceso por tres meses.

Participación del mercado

Bajo la suposición de una tasa de cambio de $4.000 pesos colombianos por 1 USD, la participación en el mercado mundial de seguridad para los escenarios proporcionados sería aproximadamente la siguiente:

En comparación con el gasto mundial estimado en soluciones y servicios de seguridad de $219,000 millones de dólares en 2023, la proyección de ventas del primer escenario representaría aproximadamente el 0.0065% del mercado global, y en el segundo escenario, representaría aproximadamente el 0.0032% del mercado global. Es de aclarar que el informe de (Expertos, 2023) indica que el mercado se divide en Solución y Servicios, los servicios se subdividen en seguridad gestionada y profesionales, y los profesionales incluyen los servicios profesionales en donde entraría lo que ofrece GAMESECURE. Aunque no se cuantifica el gasto por componente es claro que si los incluye y hacen parte del gasto en las empresas.

Ahora si se hace el análisis del mercado de ciberseguridad en Colombia para el primer escenario representaría aproximadamente el 0.058%, y para el segundo escenario, la participación sería aproximadamente el 0.029%, respecto a el tamaño del mercado de la ciberseguridad en Colombia, que alcanzó un valor de 243.86 millones de dólares en 2022 (Expertos, 2023).

Conclusiones sobre oportunidades y riesgos de mercado

De acuerdo con el análisis realizado, existe una clara oportunidad de mercado en el sector de ciberseguridad para cursos gamificados, así como una alta disposición a pagar por cursos como los que ofrece GAMSECURE, lo que sugiere un modelo de negocio sólido con potencial de crecimiento.

La importancia dada al diseño amigable y a la calidad del contenido señala áreas clave para la diferenciación y la satisfacción del cliente.

El desarrollo del prototipo permite la validación de ideas y conceptos antes de la inversión completa en el desarrollo del producto, reduciendo así el riesgo de fracaso del mercado. También ofrece la oportunidad de obtener retroalimentación de los usuarios

potenciales y hacer ajustes necesarios, lo que puede mejorar significativamente la calidad y aceptación del producto final.

Un prototipo funcional como el que se ha desarrollado puede ser una herramienta poderosa para atraer inversionistas, demostrando el potencial real del producto y la seriedad del equipo detrás del proyecto.

Si el prototipo no cumple con las expectativas o no funciona como se planeó, puede afectar negativamente la percepción y concepción de la idea de negocio.

Existe una diversidad de plataformas de e-learning que se convierten en una competencia existente que ya ha capturado una parte del mercado.

Las plataformas como la propuesta por GAMSECURE, tienen una alta dependencia de canales digitales, lo que puede representar un riesgo para la prestación del servicio.

Estrategia y Plan de Introducción de Mercado

Objetivos de Mercadeo

Incrementar la base de usuarios en un 10% en el próximo año.

Establecer a GAMSECURE como la principal referencia en cursos gamificados de ciberseguridad en el mercado.

Mejorar la retención de usuarios en un 10% mediante mejoras en el contenido y la experiencia del usuario.

Uso de Google Ads, página web y redes sociales, para captar el 40% de clientes nuevos.

Estrategias de Mercadeo

Segmentación del mercado enfocándose pequeñas y medianas empresas que busquen capacitación para sus empleados en ciberseguridad.

Diferenciación a través de la gamificación, ofreciendo una experiencia única y atractiva, y un soporte diferencial.

Lograr convenios con empresas que usen la plataforma gratis, con el propósito de tener posibles prospectos referenciados, o inclusive contratos.

Penetración en el mercado ofreciendo promociones y descuentos iniciales para empresas de más de 100 usuarios.

Estrategias de Producto/Servicio

Diseñar cursos de ciberseguridad de alta calidad, actualizados y adaptados a las últimas tendencias y amenazas.

Una plataforma amigable, intuitiva y con soporte técnico eficiente.

Estrategias de Distribución

Venta directa a través de la plataforma web de GAMSECURE.

Alianzas con instituciones educativas y empresas para ofrecer licencias grupales o empresariales.

Establecer asociaciones clave para maximizar las ventas, esto incluye colaborar con empresas aliadas que patrocinen a sus empleados en nuestros cursos, incentivando el aprendizaje y el desarrollo profesional. Además, se implementa un programa de referidos donde las recomendaciones personales juegan un papel crucial en atraer nuevos usuarios. También ofrecemos descuentos especiales en inscripciones grupales, fomentando así la participación colectiva en nuestros cursos gamificados de ciberseguridad.

Estrategias de Precios

Establecer un modelo de suscripción limitada por tres meses e ilimitada por seis meses al contenido de los cursos.

Ofrecer descuentos por volumen para empresas o instituciones.

Implementar promociones temporales para atraer nuevos usuarios.

Análisis detallado del mercado y las tendencias de precios de la competencia, en comparación con los costos internos de sus servicios. Este enfoque permite establecer precios que no solo cubran los costos, sino que también generen el margen de rentabilidad deseado.

Estrategias de Comunicación y Promoción

Reforzar la marca y sus valores a través de una comunicación clara y coherente en todos los canales.

Uso de testimonios y casos de éxito para demostrar la eficacia de los cursos.

Organizar webinars o eventos virtuales sobre ciberseguridad para posicionar a GAMSECURE como líder en el sector.

Crear y distribuir contenido que no solo promocione los cursos, sino que también eduque al público sobre la importancia de la ciberseguridad.

Implementar campañas dinámicas y participativas en redes sociales, utilizando hashtags relevantes, desafíos o concursos para aumentar el engagement con la audiencia.

Desarrollar un programa de referencias o afiliados donde los clientes actuales puedan recomendar los cursos de GAMSECURE a sus contactos, incentivando con descuentos o beneficios tanto para el referente como para el nuevo cliente.

Optimizar el sitio web y el contenido para motores de búsqueda, asegurando que GAMSECURE aparezca en las búsquedas relacionadas con ciberseguridad.

Mantener una comunicación regular con los suscriptores a través de correos electrónicos y boletines informativos, compartiendo actualizaciones, ofertas exclusivas y contenido de valor agregado.

Establecer alianzas con empresas reconocidas en el sector de la tecnología y la ciberseguridad.

Presupuesto de la Estrategia de mercadeo

Se destino un presupuesto de mercadeo de 20 millones de pesos, para cubrir los gastos de publicidad digital y tradicional. Este incluye una asignación mensual para servicios de publicidad en diversas redes sociales, así como los costos asociados a la publicidad impresa, que abarca tanto la producción como la impresión de materiales. Este enfoque presupuestario garantiza una amplia cobertura publicitaria, aprovechando tanto los medios digitales como los tradicionales para maximizar el alcance y la efectividad de las campañas de mercadeo.

Aspectos Técnicos

Objetivos de prestación de servicio

Proporcionar una formación robusta en ciberseguridad, asegurando que los empleados de las empresas adquieran conocimientos y habilidades esenciales.

Alcanzar altas tasas de finalización para que los estudiantes completen los cursos y refuercen su competencia en ciberseguridad.

Mejorar la oferta educativa basándonos en el análisis de retroalimentación de participantes y empresarios.

Mantener la plataforma de aprendizaje operativa y segura, actualizando constantemente el contenido para reflejar nuevas tendencias y amenazas en ciberseguridad.

Ficha técnica del producto o servicio

La ficha técnica constituye una herramienta fundamental para GAMSECURE, la cual se diseña para estandarizar los servicios ofrecidos. Su propósito, facilita la gestión interna de estos productos y asegura su entrega al cliente con un nivel de calidad sobresaliente.

Esta herramienta es clave para mantener la consistencia y la excelencia en todos los servicios proporcionados. La ficha técnica para cada uno de los productos y servicios que GAMSECURE ofrecerá, se relacionan en el Anexo 3. Ficha Técnica Productos o Servicios.:

- Curso: “Fundamentos en Ciberseguridad” - Código: FCE
- Curso: “Introducción a la Ciberseguridad” - Código: ICE
- Curso: “Higiene Digital y Seguridad en el Uso de Internet” - Código: HDSUI
- Curso: “Protección de Datos Personales” - Código: PDP
- Curso: “Prácticas de Contraseñas Seguras” - Código: PCS

- Curso: “Seguridad en el Correo Electrónico y Protección contra el Phishing” - Código: CEPP
- Curso: “Seguridad en el Trabajo Remoto” - Código: STR
- Curso: “Responsabilidad Legal y Ética en Ciberseguridad” - Código: RLEC

Descripción del proceso

A continuación, se describe el proceso para cada uno de los productos y servicios que GAMSECURE busca ofrecer, los cuales pueden adaptarse o personalizarse según las necesidades específicas de cada curso y audiencia:

Desarrollo: Creación de actividades o escenarios de simulación de ciberseguridad.

Implementación: Cada desafío se aloja en una página web propia con detalles, objetivos y niveles de dificultad específicos.

Actualización: Revisión periódica para mantener los desafíos relevantes y desafiantes.

Publicación: Puesta en marcha de los cursos en la plataforma para acceso de usuarios.

Evaluación y Mejora: Recopilación de feedback para mejorar y actualizar el contenido de los cursos.

Suscripción: Implementación de un modelo de suscripción mensual o anual para acceder a los cursos.

Gestión: Administración y ajuste de tarifas según el contenido y la demanda del curso.

Soporte: Brindar soporte constante a los usuarios, acompañando cada experiencia para resolver en el menor tiempo posible, preguntas, respuestas o inclusive incidencias.

Personalización: Creación de planes que incluyen cursos, asesoramiento y contenidos a medida.

Cada cliente podrá entonces, realizar el proceso de autenticación con su cuenta para iniciar el curso, consultar manuales de operación, evaluar su progreso, realizar pruebas de conocimiento, y descargar un certificado que acredita la realización del curso.

Necesidad y Requerimientos

Los productos y servicios que ofrece GAMSECURE requieren de la implementación exitosa de una plataforma LMS de formación en ciberseguridad. Esta plataforma a su vez requiere los siguientes aspectos técnicos:

Tabla 6.

Necesidad o Requerimiento

Necesidad o Requerimiento	Descripción
Equipos de cómputo	5 computadores
Talento Humano	Director ejecutivo Director técnico Desarrollador Analista marketing y Ventas
Hosting, correo electrónico	Servicio de hosting por tres años, con pasarela de pagos.
Servicio de Internet	Plan de Internet para el desarrollador

Nota: Elaboración propia.

Tabla 7.

Plataforma requerida para la operación.

Plataforma requerida para la operación	Costo
Servidores y Alojamiento Web	$ 136.550 COP/mes
Conexión a Internet	$ 125.000 COP/mes
Software LMS (Licencia GPL – GNU)	$ 0
Respaldos de Datos (Incluido en el plan VPS del servidor y alojamiento web)	$ 0
Soporte Técnico y Mantenimiento	$ 0
Escalabilidad	$ 0
Monitoreo y Supervisión	$ 0

Nota: Elaboración propia.

El servicio está orientado a contratar con un proveedor de alojamiento web dedicado, de un servidor privado virtual, que tenga presencia y acceso mundial, y en el cual se incluya el hardware, la seguridad, la continuidad y disponibilidad necesaria para soportar los productos y servicios que ofrece GAMSECURE. Este servicio adicionalmente debe apoyar el cuidado del medio ambiente y contar con certificaciones que lo acrediten.

Tabla 8.

Características VPS Virtual Privaste Server.

Hardware	Características
vCPU	8 Cores Xeon Gold, 2 Cores por cada 1000 estudiantes conectados simultáneamente.
RAM	32GB
Almacenamiento	240GB SSD
Ancho de banda	Se requiere que el ancho de banda no sea medido, lo que significa que no se le cobra según la cantidad de ancho de banda.
IP dedicada	2 IPs
Sistema Operativo	CentOS 8
SSL	Certificado digital.
Cuenta email	10
MySQL	Aplica
Soporte	24/7/365 support

Nota: Elaboración propia

En la figura 3, se muestra una arquitectura de tres capas para la arquitectura requerida para la prestación de los servicios, en el cual se tiene muestra la infraestructura:

Arquitectura de la aplicación: La arquitectura se basaría en una estructura de tres capas, que consta de una capa de presentación (front-end), una capa de lógica de negocios (back-end) y una capa de almacenamiento de datos (base de datos).

Figura 3.

Diagrama de arquitectura.

Fuente: Elaboración propia

Tecnologías front-end: Para el desarrollo del front-end, se utilizarían tecnologías web modernas de LMS como Moodle.

Tecnologías back-end: Servidor Centos con base de datos Mysql.

Seguridad: Se requiere una medida adicional de firewall de aplicación WAF como control para la detección de posibles ataques o amenazas, como inyección de código o XSS (cross-site scripting).

Plan de producción

Análisis de Necesidades y Planificación

- Identificación de las necesidades actuales del mercado en ciberseguridad.

- Definición de los objetivos de producción y planificación del desarrollo de la plataforma y los cursos.

Desarrollo de Contenidos y Plataforma

- Diseño y desarrollo de cursos interactivos gamificados, en el que se incluya las necesidades identificadas en el punto anterior.

- Creación de la plataforma online con herramientas y tecnología avanzadas.

- Contratación de expertos en ciberseguridad para desarrollo de contenido.

Pruebas y Calidad

- Realización de pruebas beta con usuarios objetivo para recopilar feedback.

- Ajustes en la plataforma y los contenidos basados en las pruebas.

Lanzamiento y Producción

- Lanzamiento oficial de la plataforma y los cursos.

- Monitoreo constante y actualizaciones regulares de contenido.

Evaluación y Mejora Continua

- Análisis continuo de feedback de usuarios y rendimiento de la plataforma.

- Actualizaciones y mejoras periódicas para mantener relevancia y eficacia.

Escalabilidad y Expansión

- Planificación para expansión y adaptación a nuevas necesidades y tecnologías.

- Estrategias para escalar la producción y alcanzar más segmentos del mercado.

Capacidad de Producción

Se estima que la plataforma dimensionada tenga una capacidad máxima de 1000 usuarios concurrentes, de forma tal que entren de forma simultánea 10 empresas cada una con 100 empleados.

Para la salida en producción la plataforma debe tener como mínimo un curso por cada servicio con una gran variedad de horas de contenido.

Se estima que un usuario se aprovisione de forma automática una vez el administrador valide el registro de conformidad en la plataforma.

Costos de Producción

En la siguiente tabla se relaciona los costos de producción de cada producto o servicio con su valor unitario y la cantidad de unidades de cada uno que se estiman vender.

Tabla 9.

Costos de cada producto o servicio.

	NOMBRE PRODUCTO SERVICIO	CANTIDADES	COSTO UNITARIO	COSTOS TOTALES
1	Desafíos Ilimitado	2000	$ 10.000,00	$ 20.000.000
2	Desafíos Limitado Acceso 3 meses	2000	$ 10.000,00	$ 20.000.000
3	Curso Fundamentos de Ciberseguridad	1500	$ 10.000,00	$ 15.000.000
4	Seguridad de la Información	1000	$ 15.000,00	$ 15.000.000
5	Seguridad de Aplicaciones	1000	$ 15.000,00	$ 15.000.000
6	Gestión de Riesgos de Seguridad	1000	$ 10.000,00	$ 10.000.000
			TOTAL	**$ 95.000.000**

Nota: Elaboración propia

Aspectos Organizacionales y Legales

Misión

Empoderar y educar a las PYMES en ciberseguridad a través de nuestra plataforma web interactiva, combinando técnicas de gamificación y contenidos de vanguardia para garantizar un aprendizaje efectivo y un entorno digital más seguro.

Visión

Ser la plataforma web de referencia a nivel global en formación de ciberseguridad para PYMES, transformando la educación digital a través de la gamificación y construyendo una comunidad comprometida con la seguridad en el ciberespacio.

Estructura organizacional

La siguiente imagen resume la estructura organizacional de GAMSECURE con los cargos que inicialmente se requieren para la constitución de la empresa y la puesta en marcha:

Figura 4.
Organigrama.

Nota: Elaboración propia

En esta estructura, el Director lidera la jerarquía y reporta directamente al director técnico, al analista de mercado y al desarrollador principal. Cada uno de estos roles es responsable de áreas específicas, el director técnico supervisa el equipo de contenido y la gestión de datos; el analista de marketing es responsable de la estrategia de mercado y publicidad digital; El desarrollador principal lidera el equipo de desarrollo web/aplicaciones, así como las pruebas y la calidad del producto.

Perfiles y funciones

Los perfiles y funciones para los cargos de director ejecutivo, director técnico, analista de marketing y ventas, así como el desarrollador, se encuentran en el anexo 4 personal requerido.

Factores clave de la gestión del talento humano

Los factores clave en la gestión del talento humano incluyen, Identificar y atraer el talento adecuado que se alinee con los valores y objetivos de la organización.

Fomentar el crecimiento continuo del personal a través de la formación y el desarrollo de habilidades, e implementar sistemas efectivos para evaluar y mejorar el rendimiento de los empleados.

Crear y mantener una cultura laboral positiva que promueva la satisfacción y la productividad, fomentando un entorno de trabajo diverso e inclusivo.

Asegurar el bienestar y la salud mental de los empleados.

Mantener una comunicación abierta y transparente dentro de la organización.

Esquema de gobierno corporativo

Para GAMSECURE, es esencial adoptar un esquema de gobierno corporativo que respalde su misión de proveer educación en ciberseguridad innovadora y efectiva. Este esquema debe estar centrado en la transparencia, la responsabilidad y la sostenibilidad. Sería ideal implementar un consejo directivo compuesto por expertos en tecnología, educación y ciberseguridad, así como representantes de los stakeholders clave. Este consejo debería enfocarse en garantizar que las decisiones empresariales estén alineadas con los mejores intereses de los clientes, empleados y la comunidad en general. Además, deberían establecerse políticas claras sobre ética, privacidad de datos

y seguridad cibernética, así como mecanismos de supervisión y reporte que aseguren el cumplimiento de estas normas y la adaptación a las regulaciones vigentes. Este enfoque ayudará a GAMSECURE a mantener la confianza de sus usuarios y a posicionarse como un líder responsable en el campo de la ciberseguridad.

Estructura jurídica y tipo de sociedad

GAMSECURE será una Sociedad por Acciones Simplificada (S.A.S.), ya que este tipo de sociedad permite una gran flexibilidad en su estructura administrativa y en la toma de decisiones, no hay un mínimo exigido por ley para el capital social, y puede ser pagado de manera gradual, puede tener uno o varios accionistas (personas naturales o jurídicas), y la responsabilidad de cada uno está limitada a su aporte en acciones.

Su constitución y registro pueden realizarse de forma ágil y sencilla, incluso mediante documento privado. Puede definir libremente su estructura de gobierno corporativo, incluyendo la distribución de roles entre los accionistas, la administración y los órganos de control.

Aspectos Financieros

Objetivos Financieros

Alcanzar un margen operativo de al menos $380.000.000 en 2024.

Incrementar las ventas anuales en un 10% mínimo durante los próximos 5 años.

Generar ventas el primer año de $475’000.000

Supuestos Económicos para la Simulación

Crecimiento anual del mercado de la ciberseguridad en torno al 10%.

Tasa de interés del préstamo constante al 20,12% anual.

Inversión continua en innovación y desarrollo del personal.

Para la tasa de evaluación del proyecto, se toma la tasa de los CDT a 360 días de acuerdo con la proyección del banco de la república sobre las Tasas de captación semanales y mensuales, se toma la proyección del IPC promedio hasta 2028 conforme a la publicación de la encuesta de expectativas del banco de la república encuesta mensual de expectativas de analistas económicos (EME) y se aplica la siguiente formula: +(1+tasa CDts 360 días)*(1+proyeccion IPC a 5 años)-1, dando como resultado 20,05%. El resultado de 20,05% representa una tasa de rendimiento anual ajustada por inflación, que se utiliza para evaluar si la inversión en el proyecto es financieramente viable y atractiva en comparación con otras opciones de inversión. A esta tasa de rendimiento se le suma una prima de riesgo utilizando las betas de riesgo de Damodaran (University, 2024) para el sector de education 1.07. Para agregar la tasa de riesgo del sector, adicionalmente se utilizó la siguiente formula bajo el modelo CAPM (Capital Asset Pricing Model) o Modelo Principal de Valoración de Activos:

$$E(ri)= rf + \beta\ [E(rm)– rf]$$

E(ri)=tasa de evaluación del proyecto 20,05%

rf = tasa libre de riesgo Tasa del banco de la república 12,75% (Colombia, 2024)

rm= rendimiento de mercado (Tasa de tesoros americanos a 10 años Nov30-2023, 4,33%) (DatosMacro, 2024)

$$=4,33\%+1,07*(20,05\%-4,33\%) = 21,15\%$$

Es importante tener en cuenta que esta tasa de evaluación refleja tanto el costo de oportunidad del capital (a través de la tasa de CDT) como el efecto de la inflación en el valor del dinero a lo largo del tiempo, más la tasa de riesgo del sector, lo cual es crucial para cualquier análisis de inversión a largo plazo.

Proyección de Ventas

Ingresos del Primer Año (2024) de $474.789.916.

Proyección de crecimiento de ventas del 10% anual.

Proyección de Gastos de Mercadeo

Presupuesto inicial de $20.000.000 en 2024.

Aumento del presupuesto de marketing en línea con el crecimiento de los ingresos.

Proyección de Costos de Producción

Costos de ventas de $95.000.000 en 2024.

Incremento anual del 5% en los costos de producción.

Proyección de Gastos Administrativos

Gastos administrativos de $138.000.000 en 2024.

Aumento anual del 8% en gastos administrativos.

Presupuesto de Inversión

Inversión inicial: $20.000.000.

Capital de trabajo inicial: $292.000.000.

Estados Financieros (Escenario Probable)

Proyección de estados financieros para 2024-2028 incluyendo balance general, estado de resultados y flujo de caja.

Estado de Resultados

Utilidad neta en 2024: $75.297.853,03.

Incremento constante en utilidades en los años siguientes.

Ingresos

En 2024, la empresa generara un total de $474.789.916, en ingresos por concepto de sus servicios.

Se visualizan los ingresos que resultan de la ejecución de los servicios que se ofertaran en la empresa, el precio de venta unitario sin IVA los cuales tienen unos ingresos totales de $474.789.916, los costos de cada servicio están definidos de la siguiente manera:

Inversión inicial

Un análisis de la inversión inicial y los costos/gastos fijos del primer año resalta varios puntos clave. La inversión inicial de $20,000,000 indica el importante capital requerido para iniciar y operar el negocio. Esto incluye la adquisición de bienes inmuebles, activos fijos, equipo de oficina y la depreciación anual de dichos activos, teniendo en cuenta los costos iniciales.

Los costos salariales constituyen una parte importante de los costos fijos del primer año, por un total de $138.000.000.

Se asigna un presupuesto inicial de marketing de $20.000.000, para el primer año, indicando la importancia de la promoción y comercialización del negocio desde su inicio para atraer a potenciales clientes.

Se tendrán gastos fijos por $39.000.000 del primer año, para lo siguiente, arriendo $24.000.000 servicios públicos $ 12.000.000 y telefonía celular $3.000.000.

En el marco de las inversiones y considerando todos y cada uno de los factores en los que se deben desarrollar los parámetros, son los mismos que se establecen para la puesta en marcha de la empresa GAMSECURE.

Podemos analizar la inversión total y las necesidades de financiación para el negocio, es de $20.000.000. A continuación, se detallan los cálculos

Inversión total

La inversión total requerida para el negocio asciende a $20.000.000.

Cálculo del capital de trabajo inicial

Se presenta un desglose mensual de los costos operativos, nóminas y gastos fijos durante los primeros 12 meses. El cálculo del capital de trabajo inicial se realiza sumando estos gastos mensuales durante el período de un año.

Cálculo del préstamo

Se solicita un préstamo para financiar las necesidades de capital de trabajo. La tasa de interés anual del préstamo es del 20,16% efectivo anual. El préstamo se otorga por un período de 5 años.

Resultados

Las necesidades de capital de trabajo inicial ascienden a $292.000.000.

El aporte de los emprendedores es de $30.000.000.

La cantidad de préstamo a solicitar para cubrir las necesidades de financiación es de $282.000.000.

Estos cálculos sugieren que se necesita un préstamo de $82.000.000, para financiar la inversión inicial y las necesidades de capital de trabajo del negocio. El aporte de los emprendedores contribuye con $30.000.000, al financiamiento inicial.

Es importante llevar a cabo un análisis detallado de las condiciones del préstamo, incluyendo los términos y la capacidad de pago del negocio, para garantizar una gestión financiera sólida y sostenible a lo largo de los años.

Figura 5.

Estado de Resultados.

ESTADO DE RESULTADOS

	2024	2025	2026	2027	2028
VENTAS	$ 474.789.916,0	$ 542.637.395,0	$ 614.808.168,5	$ 696.577.654,9	$ 789.222.483,0
COSTO VENTAS	$ 95.000.000,0	$ 112.860.000,0	$ 131.594.760,0	$ 154.887.032,5	$ 180.598.279,9
UTILIDAD BRUTA	$ 379.789.916,0	$ 429.777.395,0	$ 483.213.408,5	$ 541.690.622,4	$ 608.624.203,1
GASTOS ADTIVOS Y VTAS	$ 138.000.000,0	$ 143.382.000,0	$ 147.683.460,0	$ 152.113.963,8	$ 156.677.382,7
GASTOS FIJOS DEL PERIODO	$ 39.000.000,0	$ 40.521.000,0	$ 41.736.630,0	$ 42.988.728,9	$ 44.278.390,8
OTROS GASTOS	$ 20.000.000,0	$ 20.000.000,0	$ 20.000.000,0	$ 15.000.000,0	$ 10.000.000,0
DEPRECIACIÓN	$ 3.500.000,0	$ 3.500.000,0	$ 3.500.000,0	$ 3.500.000,0	$ 3.500.000,0
UTILIDAD OPERATIVA	$ 179.289.916,0	$ 222.374.395,0	$ 270.293.318,5	$ 328.087.929,7	$ 394.168.429,6
GASTOS FINACIEROS	$ 56.851.200,0	$ 49.235.546,1	$ 40.084.576,4	$ 29.088.771,1	$ 15.876.211,6
UTILIDAD ANTES DE IMPTOS	$ 122.438.716,0	$ 173.138.848,9	$ 230.208.742,1	$ 298.999.158,5	$ 378.292.218,0
IMPUESTOS	$ 41.629.163,4	$ 58.867.208,6	$ 78.270.972,3	$ 101.659.713,9	$ 128.619.354,1
UTILIDAD NETA	**$ 80.809.552,5**	**$ 114.271.640,2**	**$ 151.937.769,8**	**$ 197.339.444,6**	**$ 249.672.863,9**

Nota: Elaboración propia

En 2024, GAMSECURE generara ventas por un total de $474.789.916, con costos de ventas de $95.000.000, lo que representara una utilidad bruta de $379.789.916.

Los gastos administrativos y de ventas serán de $138.000.000, con otros gastos de $20.000.000 y una depreciación de $3.500.000. La utilidad operativa para 2024 será de $179.289.916.

Los gastos financieros totalizados son de $56.851.200, lo que lleva a una utilidad antes de impuestos de $122.438.716, y una utilidad neta de $80.809.552.

Los valores proyectados para los años subsiguientes (2025-2028) muestran un crecimiento constante en las ventas, los costos y las utilidades netas. Esto indica que GAMSECURE mantiene una tendencia positiva de crecimiento y rentabilidad a medida que avanza en su negocio de servicios de ciberseguridad.

Estados financieros

La previsión de informes financieros juega un papel clave en la planificación estratégica y la toma de decisiones de cualquier empresa. Al respecto, presentamos un cuadro detallado de los estados financieros anticipados de GAMSECURE para los años 2024-2028.

Figura 6.
Balance

BALANCE

	ANO 0	2024	2025	2026	2027	2028
			ACTIVO			
CAJA/BANCOS	$ 292.000.000,00	$ 380.162.654,93	$ 388.971.072,89	$ 394.998.281,48	$ 401.750.208,00	$ 405.792.218,03
FIJO NO DEPRECIABLE	$ -	$ -	$ -	$ -	$ -	$ -
FIJO DEPRECIABLE	$ 20.000.000,00	$ 20.000.000,00	$ 20.000.000,00	$ 20.000.000,00	$ 20.000.000,00	$ 20.000.000,00
DEPRECIACIÓN ACUMULADA	$ -	$ 3.500.000,00	$ 7.000.000,00	$ 10.500.000,00	$ 14.000.000,00	$ 17.500.000,00
ACTIVO FIJO NETO	$ 20.000.000,00	$ 16.500.000,00	$ 13.000.000,00	$ 9.500.000,00	$ 6.000.000,00	$ 2.500.000,00
TOTAL ACTIVO	**$ 312.000.000,00**	**$ 396.662.654,93**	**$ 401.971.072,89**	**$ 404.498.281,48**	**$ 407.750.208,00**	**$ 408.292.218,03**
			PASIVO			
Impuestos X Pagar	0	$ 41.629.163,4	$ 58.867.208,6	$ 78.270.972,3	$ 101.659.713,9	$ 128.619.354,1
TOTAL PASIVO CORRIENTE	$ -	$ 41.629.163,4	$ 58.867.208,6	$ 78.270.972,3	$ 101.659.713,9	$ 128.619.354,1
Obligaciones Financieras	$ 282.000.000,00	$ 244.223.938,97	$ 198.832.224,03	$ 144.289.539,36	$ 78.751.049,46	$ -
PASIVO	**$ 282.000.000,00**	**$ 285.853.102,40**	**$ 257.699.432,64**	**$ 222.560.511,68**	**$ 180.410.763,37**	**$ 128.619.354,13**
			PATRIMONIO			
Capital Social	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00
Utilidades del Ejercicio	0	$ 80.809.552,5	$ 114.271.640,2	$ 151.937.769,8	$ 197.339.444,6	$ 249.672.863,9
TOTAL PATRIMONIO	**$ 30.000.000,00**	**$ 110.809.552,54**	**$ 144.271.640,25**	**$ 181.937.769,80**	**$ 227.339.444,64**	**$ 279.672.863,90**
TOTAL PAS + PAT	**$ 312.000.000,00**	**$ 396.662.654,93**	**$ 401.971.072,89**	**$ 404.498.281,48**	**$ 407.750.208,00**	**$ 408.292.218,03**
CUADRE (ACT = PAS+PAT)	$ -	$ -	$ -	$ -	$ -	$ -

Nota: Elaboración propia

Este análisis se centrará en el estado de resultados y el balance, examinando los números clave que reflejan el rendimiento, la solidez financiera y el crecimiento continuo de GAMSECURE a lo largo de los años proyectados. Los detalles específicos y las tendencias identificadas en estos estados financieros permitirán una comprensión más profunda de la situación financiera de la empresa y su potencial para el futuro.

El aumento en las utilidades del ejercicio indica que la empresa será rentable y estará en constante crecimiento.

Activo

El saldo en efectivo y cuentas bancarias aumenta de $ 292.000.000, en el año 0 a $ 405.792.218, en 2028. Esto puede indicar una gestión eficiente de los recursos financieros.

Este activo muestra la inversión en activos fijos de la empresa. Se mantiene constante en $ 20.000.000, durante el período de proyección.

Pasivo

Los impuestos aumentan significativamente a lo largo del período proyectado, pasando de $0,00 en el año 0 a $ 128.619.354, en 2028. Esto puede deberse a un aumento en las operaciones de la empresa.

Las obligaciones financieras disminuyen a lo largo del tiempo, llegando a $0,00 en 2028. Esto será debido a la liquidación de deudas.

Patrimonio

El capital social permanece constante en $ 30.000.000, a lo largo de los años.

Las utilidades del ejercicio aumentan con el tiempo, indicando que la empresa estará generando ganancias consistentes.

Flujo de Caja

El balance proyectado muestra una empresa con una sólida base financiera y un enfoque en la liquidez. A medida que pasa el tiempo, GAMSECURE acumula ganancias que sustentan el crecimiento de su patrimonio neto. La gestión de los activos fijos y pasivos a corto plazo es clave para garantizar la estabilidad financiera de la empresa.

Este análisis se centra en los flujos de caja del proyecto GAMSECURE en el periodo 2024-2028. Examina el capital empleado y los cálculos del flujo de caja libre y analiza de cerca cómo una empresa gestiona sus activos y pasivos y su capacidad para generar efectivo neto. El flujo de caja libre del proyecto varía positivamente a lo largo de los años, lo que sugiere un aumento en la generación

de efectivo después de impuestos y gastos de inversión. Esto es una señal positiva de que el proyecto está generando valor.

En el año base (Año 0), GAMSECURE cuenta con activos corrientes por valor de $ 292.000.000, compuestos principalmente por caja/bancos. Esta cifra experimenta un crecimiento significativo en los años subsiguientes, llegando a $405.792.218 en 2028. Esto refleja la generación de efectivo por las operaciones de la empresa y la acumulación de recursos financieros.

Por otro lado, los pasivos corrientes, inicialmente nulos, aumentan progresivamente a lo largo del período, principalmente debido a los impuestos por pagar. Este incremento muestra una responsabilidad financiera creciente a medida que la empresa expande sus operaciones.

El total de Capital Operativo Neto (KTNO) representa el capital necesario para financiar las operaciones de GAMSECURE. En el año base, es de $ 312.000.000 y disminuye gradualmente a medida que avanza el tiempo, llegando a $279.672.864 en 2028. Esta disminución indica una gestión eficiente de los activos y pasivos de la empresa.

Cálculo del Flujo de Caja Libre. El EBIT (Beneficio Antes de Intereses e Impuestos) es una medida de la rentabilidad operativa. A lo largo de los años, el EBIT muestra un crecimiento constante, lo que refleja el éxito en la generación de beneficios. En 2028, el EBIT alcanza los $ 394.168.429.

Los impuestos sobre la renta aumentan a medida que los ingresos y las utilidades crecen. GAMSECURE paga impuestos por un total de $134.017.266 en 2028.

El NOPLAT (Beneficio Neto Operativo Después de Impuestos) refleja la utilidad neta después de impuestos. Experimenta un aumento constante a lo largo de los años debido al crecimiento de las utilidades y la eficiencia fiscal. En 2028, el NOPLAT es de $260.151.163.

La inversión neta se refiere a las inversiones en activos fijos netos y disminuye debido a una menor inversión en activos a lo largo del tiempo. En 2028, la inversión neta es de $26.417.630.

El Flujo de Caja Libre del período muestra un crecimiento constante a medida que avanza el tiempo, lo que indica la capacidad de la empresa para generar efectivo después de cubrir gastos e inversiones. En 2028, GAMSECURE genera un Flujo de Caja Libre de $286.568.794.

El análisis del flujo de caja del proyecto de GAMSECURE demuestra una gestión financiera sólida y sostenible. La empresa es capaz de generar efectivo positivo a medida que crece, lo que le permite respaldar sus operaciones continuas, financiar inversiones futuras y mantener una posición financiera saludable en el competitivo mercado de la ciberseguridad.

Evaluación financiera y punto de equilibrio

El punto de equilibrio es un indicador clave para cualquier empresa porque indica el nivel de ventas en el que los ingresos son iguales a los costos, lo que significa que la empresa no obtiene ni pierde dinero. En el caso de GAMSECURE, se realiza un análisis de beneficios sobre los distintos productos o servicios que ofrece la empresa.

Desafíos Ilimitado: Para alcanzar el punto de equilibrio en este producto, la empresa necesita vender 841 unidades.

Desafíos Limitado Acceso 3 meses: Se requieren 421 unidades vendidas para alcanzar el punto de equilibrio en este producto.

Curso Fundamentos de Ciberseguridad: El punto de equilibrio para este curso se alcanza con la venta de 451 unidades.

Seguridad de la Información: Para este servicio, se necesitan 901 unidades vendidas para llegar al punto de equilibrio.

Seguridad de Aplicaciones: El punto de equilibrio se logra con la venta de 360 unidades de este servicio.

Gestión de Riesgos de Seguridad: Se requieren 420 unidades vendidas para alcanzar el punto de equilibrio en este servicio.

En total, se necesitan 3.393 unidades en ventas para que la empresa alcance su punto de equilibrio.

Total Margen de Contribución Promedio Ponderado: $49.259. La siguiente tabla muestra la participación en las ventas totales por cada producto o servicio, siendo los desafíos ilimitados % los más representativos con un 25%.

Tabla 10.
Margen de contribución

NOMBRE DEL PRODUCTO O SERVICIO	MARGEN DE CONTRIBUCION UNITARIO		PARTICIPACION % EN VENTAS TOTALES
Desafíos Ilimitado	$	48.823,53	25%
Desafíos Limitado Acceso 3 meses	$	19.411,76	12%
Curso Fundamentos de Ciberseguridad	$	32.016,81	13%
Seguridad de la Información	$	111.050,42	27%
Seguridad de Aplicaciones	$	35.420,17	11%

NOMBRE DEL PRODUCTO O SERVICIO	MARGEN DE CONTRIBUCION UNITARIO		PARTICIPACION % EN VENTAS TOTALES
Gestión de Riesgos de Seguridad	$	48.823,53	12%

Nota: Elaboración propia

Punto de Equilibrio = Costos y Gastos Fijos / Margen de Contribución Promedio Ponderado (MCPP): 3.393 unidades.

El análisis financiero muestra que el proyecto GAMSECURE es muy rentable, con un valor presente neto (VPN) positivo de $187.759.492 y una tasa interna de retorno (TIR) de 41,34% superior a la tasa de evaluación del proyecto de 21,15%. Además, el punto de equilibrio se alcanza con la venta de 3.393 unidades en los distintos servicios que ofrece GAMSECURE, y un periodo de recuperación de 3.12 años, lo que sugiere que la empresa tiene un amplio margen de rentabilidad. Estos resultados sugieren que el proyecto es financieramente estable y prometedor.

Enfoque hacia la Sostenibilidad

GAMSECURE adopta un enfoque holístico y sostenible alineado con los Objetivos de Desarrollo Sostenible (ODS) propuestos por las Naciones Unidas, apuntando a ser un catalizador de cambio social y económico a través de la educación especializada en ciberseguridad. Nuestra misión se entrelaza estrechamente con el ODS 4, Educación de Calidad, reconociendo que la formación en habilidades digitales avanzadas es fundamental para el empoderamiento socioeconómico y la erradicación de la pobreza.

Desde otra perspectiva como el ODS 1, Fin de la Pobreza, GAMSECURE buscará ofrecer acceso equitativo a la capacitación en ciberseguridad, una habilidad cada vez más demandada, que puede ser el diferenciador en la vida de muchas personas al mejorar su empleabilidad y posibilidades de obtener un trabajo digno y bien remunerado.

Con el ODS 8, Trabajo Decente y Crecimiento Económico, GAMSECURE aspira a fomentar un ecosistema donde el crecimiento profesional individual se traduzca en beneficios tangibles para las comunidades, mediante la creación de empleos que no solo sean decentes sino también impulsores de un progreso económico sostenible y de largo alcance.

GAMSECURE se compromete a trabajar en consonancia con el ODS 10, Reducción de las Desigualdades, y el ODS 17, Alianzas para lograr los Objetivos, para forjar alianzas estratégicas con entidades gubernamentales, organizaciones no gubernamentales y el sector privado. Buscamos patrocinio para aquellos en situaciones vulnerables, garantizando que la capacitación en ciberseguridad trascienda las barreras económicas y contribuya a cerrar la brecha digital.

La visión de GAMSECURE es democratizar la educación en ciberseguridad, proporcionando herramientas de aprendizaje que no solo educan, sino que también empoderan a individuos y comunidades para proteger su información y recursos digitales.

Al hacerlo, no solo impulsamos el desarrollo económico, sino que también fortalecemos la infraestructura de seguridad de información de las pequeñas y medianas empresas, crucial para la sostenibilidad del progreso tecnológico.

En términos sociales, el modelo de negocio puede contribuir a la seguridad y protección de datos tanto de las empresas como de los clientes, lo cual es fundamental en la era digital. Esto ayuda a crear confianza en el uso de la tecnología y puede promover una cultura de seguridad cibernética tanto a nivel empresarial como a nivel de los individuos.

Desde el punto de vista económico, la implementación de medidas de ciberseguridad puede prevenir pérdidas financieras significativas asociadas con violaciones de datos, ataques cibernéticos y robo de información confidencial. Esto puede traducirse en ahorros económicos a largo plazo para las empresas, ya que evitarán costosos incidentes de seguridad cibernética y las consiguientes consecuencias legales y de reputación.

Aunque puede parecer menos evidente, la sostenibilidad también puede abordarse desde la eficiencia energética y la reducción de la huella de carbono asociada con la tecnología utilizada en la plataforma web. La optimización de los servidores, el uso de energía renovable para alimentar los centros de datos y la minimización del consumo de recursos digitales pueden ser aspectos que contribuyan a la sostenibilidad ambiental del negocio.

Se pueden desarrollar indicadores específicos de sostenibilidad para medir y monitorear el desempeño ambiental, social y económico del negocio a lo largo del tiempo. Estos indicadores pueden incluir métricas como la reducción de emisiones de carbono, la satisfacción del cliente, la retención de empleados y el crecimiento económico sostenible.

Conclusiones

GAMSECURE, ha creado un sólido modelo de negocio que combina innovación, calidad de la educación, orientación al cliente y valores éticos para brindar soluciones de ciberseguridad para la educación. Su compromiso con la innovación continua, la excelencia educativa y el servicio al cliente demuestra un compromiso integral con las necesidades cambiantes del mercado de la ciberseguridad.

La compañía muestra un claro compromiso con la responsabilidad social al priorizar la educación de comunidades vulnerables y promover prácticas comerciales sostenibles. Además, su visión de expansión global y alianzas estratégicas con gobiernos e instituciones educativas subrayan su intención de cruzar fronteras y colaborar activamente para promover la ciberseguridad a nivel internacional.

La situación actual revela una brecha significativa en la concientización y capacitación en ciberseguridad entre las pequeñas y medianas empresas (PYMES). La explosión de ciberataques, especialmente en América Latina, y la falta de recursos y seguridad en estas organizaciones ponen de relieve la urgente necesidad de formación en este ámbito.

La propuesta de GAMSECURE responde a este desafío con una innovadora plataforma basada en juegos dirigida principalmente a las PYMES. La empresa tiene como objetivo cerrar esta brecha proporcionando contenido interactivo y actualizado que se centra en la prevención y la educación continua en ciberseguridad.

La implementación de GAMSECURE en el mercado colombiano requiere un enfoque holístico que incluye aspectos legales, desarrollo de productos, estrategias de marketing y un profundo conocimiento de los clientes. En el ámbito de la ciberseguridad y el e-learning, es fundamental una combinación de estricto cumplimiento de la normativa, desarrollo de contenidos de alta calidad y estrategias de marketing centradas en las

necesidades del cliente. Además, las colaboraciones con instituciones educativas y asociaciones industriales pueden fortalecer la credibilidad y el alcance de la marca.

Es esencial una comprensión profunda de las necesidades específicas de seguridad cibernética de las PYMES colombianas. Gracias a un análisis exhaustivo del mercado local y una segmentación detallada, tanto el producto como la estrategia de marketing se pueden adaptar a sus necesidades específicas. Esta comprensión detallada es la base para desarrollar una plataforma atractiva y relevante y guía las tácticas de marketing para llegar de manera efectiva a este público objetivo.

GAMSECURE, ha trazado un camino estratégico integral que va más allá de simplemente proporcionar una plataforma tecnológica. Su enfoque holístico incluye un profundo conocimiento del mercado, el desarrollo de una plataforma técnica avanzada y la creación de contenido de capacitación especializado. Esta combinación tiene como objetivo no solo llenar un vacío en la capacitación en ciberseguridad para las PYMES, sino también cambiar las percepciones sobre el aprendizaje técnico a través del juego y la accesibilidad.

Referencias

(UNIR), U. I. (2022). *La educación 'online' ha crecido un 900% en todo el mundo desde el año 2000*. Obtenido de https://alfabetizaciondigital.redem.org/la-educacion-online-ha-crecido-un-900-en-todo-el-mundo-desde-el-ano-2000/

ACIS. (octubre de 2022). *Ataques de ciberseguridad efectivos crecen un 400% en el último trimestre de 2022*. Obtenido de https://acis.org.co/portal/content/ataques-de-ciberseguridad-efectivos-crecen-un-400-en-el-%C3%BAltimo-trimestre-de-2022

Bogotá, C. d. (2023). *Cámara de Comercio de Bogotá*. Obtenido de https://www.ccb.org.co/informacion-especializada/observatorio/dinamica-empresarial/empresas-activas/tamano

Bogotá, F. C. (2023). *Flexibilizar acceso y educación pertinente, ejes para la creación de más empleos*. Obtenido de Bogotá es el principal centro económico de Colombia, con un aporte del 26 % al PIB nacional y del 27 % al empleo formal del país. La economía de la ciudad es movilizada por una población en edad de trabajar de 6,4 millones de habitantes.

Cámara Colombiana de Informática y Telecomunicaciones, C. (abril de 2022). *Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno*. Obtenido de https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/#:~:text=De%20acuerdo%20con%20el%20%C3%BAltimo,comparado%20con%20el%20a%C3%B1o%20anterior.

Colombia, B. d. (enero de 2024). *Tasas de captación semanales DTF, CDT y TCC*. Obtenido de https://totoro.banrep.gov.co/analytics/saw.dll?Go

CONGRESO, D. L. (2012). *LEY ESTATUTARIA 1581 DE 2012.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Dane. (agosto de 2023). *Producto Interno Bruto (PIB) nacional trimestral*. Obtenido de https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

DANE. (s.f.). *Boletín Directorio Estadístico de Empresas 2019-2021*. Obtenido de https://www.dane.gov.co/files/investigaciones/boletines/registro-estadistico/boletin-directorio-estadistico-empresas-2019-2021.pdf

DatosMacro. (enero de 2024). *Bono de Estados Unidos a 10 años*. Obtenido de https://datosmacro.expansion.com/bono/usa?dr=2023-12

DNP, D. N. (agosto de 2023). *Metas del Plan Nacional de Desarrollo 2022-2026*. Obtenido de https://colaboracion.dnp.gov.co/CDT/portalDNP/PND-2023/2023-02-23-METAS.pdf

EMIS. (2023). Obtenido de https://www-emis-com.bdbiblioteca.universidadean.edu.co/php/companies?pc=CO&cmpy=12801160

ESET, W. b. (abril de 2020). *Cómo la gamificación puede potenciar la capacitación en ciberseguridad*. Obtenido de https://www.welivesecurity.com/la-es/2020/04/21/como-gamificacion-puede-potenciar-capacitacion-ciberseguridad/

Expertos, I. d. (2023). *Análisis de la Industria de la Ciberseguridad en Colombia*. Obtenido de https://www.informesdeexpertos.com/informes/mercado-de-la-ciberseguridad-en-colombia

Fonte, A. (2022, enero 24). Técnicas de ingeniería social: Así atacan al eslabón más débil de la ciberseguridad. *Derecho de la red. https://derechodelared.com/tecnicas-de-ingenieria-social/*.

IDC. (2023). *Dealerworld*. Obtenido de https://www.dealerworld.es/seguridad/una-nueva-prevision-de-idc-eleva-al-121-el-crecimiento-de-las-inversiones-mundiales-en-seguridad-en-2023

Infobae. (2022). *Como será la evolución del e-learning en los proximos años*. Obtenido de https://www.infobae.com/america/opinion/2022/10/18/como-sera-la-evolucion-del-e-learning-en-los-proximos-anos-tras-su-crecimiento-durante-la-pandemia/

INFOBAE. (03 de 12 de 2022). *infobae*. Obtenido de https://www.infobae.com/america/tecno/2022/12/03/cuanto-dinero-pagan-las-empresas-para-rescatar-los-datos-de-ataques-ciberneticos/#:~:text=La%20empresa%20prestadora%20de%20salud,atenci%C3%B3n%20de%20miles%20de%20usuarios&text=Las%20empresas%20en%20el%20mu

Intelligence, M. (2023). *ANÁLISIS DEL TAMAÑO Y LA PARTICIPACIÓN DEL MERCADO DE CIBERSEGURIDAD TENDENCIAS Y PRONÓSTICOS DE CRECIMIENTO (2023 - 2028)*. Obtenido de https://www.mordorintelligence.com/es/industry-reports/cyber-security-market

Itmadrid. (septiembre de 2023). *Itmadrid*. Obtenido de https://www.itmadrid.com/que-es-la-gamificacion-educativa/

Jeimy Cano, P. C. (diciembre de 2022). *Ciberseguridad en Colombia 2022. Cinco ataques y algunas lecciones aprendidas*. Obtenido de https://www.linkedin.com/pulse/ciberseguridad-en-colombia-2022-cinco-ataques-y-jeimy-cano-ph-d-cfe/?trackingId=ZegYz1YuR1amTEHKscVTqg%3D%3D

José, C. M. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, 19.

Ministerio de Educación Nacional, M. (2021). *Guía de Política de protección sobre la propiedad intelectual: eje derechos de autor.* Obtenido de https://www.mineducacion.gov.co/1780/articles-336187_recurso_3.pdf

MINTIC, M. d. (19 de octubre de 2023). *MinTIC resaltó la importancia de que la formación en ciberseguridad se haga desde las regiones*. Obtenido de https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/281055:MinTIC-resalto-la-importancia-de-que-la-formacion-en-ciberseguridad-se-haga-desde-las-regiones

Mundial, B. (junio de 2023). *El Banco Mundial en Colombia*. Obtenido de https://www.bancomundial.org/es/country/colombia/overview#1

OEA, O. d. (2022). *Organization of American States*. Obtenido de https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

República, L. (14 de diciembre de 2022). Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles.

Republica, L. (23 de agosto de 2023). *Diario La Republica*. Obtenido de https://www.larepublica.co/empresas/cerca-de-66-de-las-organizaciones-han-sido-objeto-de-ataques-ciberneticos-3686618

República, P. d. (agosto de 2023). *Plan Nacional de Desarrollo 2022 - 2026*. Obtenido de https://colaboracion.dnp.gov.co/CDT/portalDNP/PND-2023/2023-05-04-bases-plan-nacional-de-inversiones-2022-2026.pdf

Ricardo Acosta-Díaz, S. B.-F. (enero de 2016). *ResearchGate.* Obtenido de In book: Abordajes metodológicos para problemas educativos (pp.65-80)Publisher: Printego-Universidad Autónoma de San Luis Potos'i. ISBN: 978-607-8062-63-8:

https://www.researchgate.net/publication/303784776_Hacia_la_gamificacion_educativa

Security, P. (noviembre de 2017). *Panda Media Center*. Obtenido de Gamificación para mejorar la seguridad de tu empresa: https://www.pandasecurity.com/es/mediacenter/seguridad/gamificacion/

Sierra, C. P. (2014). *Emprendimiento: conceptos y plan de negocios.* Pearson Educación.

University, N. Y. (enero de 2024). *Betas by Sector (US)*. Obtenido de https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/Betas.html

X-Force®, I. S. (2022). *IBM Security X-Force Threat Intelligence Index 2022 Full Report.* Obtenido de https://www.ibm.com/downloads/cas/ADLMYLAZ

A. Anexo 1. PESTEL

Tabla 11.

Análisis PESTEL.

FACTORES EXTERNOS	OPORTUNIDADES	AMENAZAS
POLÍTICOS	Políticas gubernamentales de apoyo a la innovación y desarrollo de tecnología Políticas de financiamiento para proyectos tecnológicos Políticas relativas al comercio nacional e internacional Existencia de ayudas, o subvenciones aplicables Grado de fiabilidad o corrupción en las instituciones del país	Legislación nacional vigente que afecte a los negocios considerados Legislación nacional futura o prevista Existencia de órganos legislativos o normativos que afecten a los sectores Políticas gubernamentales desfavorables a la innovación y desarrollo de tecnología Falta de financiamiento para proyectos tecnológicos Cercanía de procesos electorales y su impacto en los mercados Políticas ecológicas y medioambientales
ECONÓMICOS	Creciente demanda de las PYMES de soluciones técnicas de seguridad Crecimiento de las inversiones tecnológicas por parte de las empresas Reducción de los costos de tecnología y aumente la disponibilidad de herramientas de software Tendencias en los mercados y canales de comercialización Tendencias y modas en las motivaciones de compra de los consumidores Índice de confianza de los consumidores en el país	Situación de la economía nacional (análisis de coyuntura) Tendencias económicas del país Situación de la economía y tendencias en el entorno internacional Impuestos y política fiscal en el país Tasas de interés y políticas cambiarias Nivel de liquidez de los consumidores en el país
SOCIALES CULTURALES	Actitudes y opiniones de los consumidores en los mercados Motivaciones de compra, modas y tendencias en los mercados Influencia de los medios de información Importancia de la imagen de marca o de empresa en el país Patrones de compra/consumo de los consumidores	Impacto de la publicidad y sus canales Factores éticos que afectan a los mercados Factores sociales afectados por legislaciones nacionales o internacionales Modelos de comportamiento y modas en el país Principales eventos y su influencia en los mercados

	Poder de compra de los consumidores y tendencias	Niveles de educación y formación en el país y su efecto en los mercados Capacidad y formación de los equipos directivos en el país Estilos de Management preponderantes en el país Cultura organizacional
TECNOLÓCIGOS	Desarrollos tecnológicos relevantes en el entorno Tecnologías aplicables en el entorno Nuevos desarrollos tecnológicos en la enseñanza y el aprendizaje Herramientas de colaboración, trabajo en equipo y autónomo Desarrollos en software informático en el país	Obsolescencia tecnológica en el entorno Legislación aplicable relativa a la tecnología Acceso a la tecnología, licencias y patentes Gestión de la propiedad intelectual en el país Fuentes y usos de la energía en el país Estado de la disposición y tratamiento de residuos en el país
ECOLÓGICOS	Cultura empresarial en el país respecto a los factores medioambientales Manejo de residuos contaminantes en el país Importancia del impacto del desarrollo industrial en el medio ambiente	Consideraciones ecológicas y medioambientales Regulaciones medioambientales aplicables, nacionales e internacionales Impacto de los aspectos medioambientales en los consumidores Concepto de valor medioambiental en el mercado
LEGALES	Legislación vigente aplicable, en los mercados del entorno	Legislación futura aplicable Leyes de protección a los consumidores Regulaciones específicas aplicables a los sectores empresariales Leyes que regulan la competencia en el país Leyes y regulaciones de derechos de autor y propiedad intelectual Violación a la privacidad y la seguridad de los datos en línea pueden amenazar el compromiso del proyecto

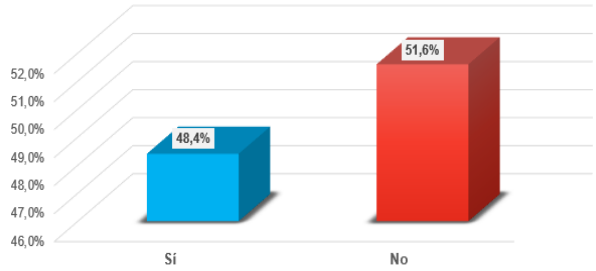
Nota: Elaboración propia

B. Anexo 2. Herramienta Encuesta

De acuerdo con las repuestas el resultado es el siguiente para cada pregunta:

Figura 7.

Pregunta 1. ¿Conoce alguna plataforma que use técnicas de gamificación en sus cursos?

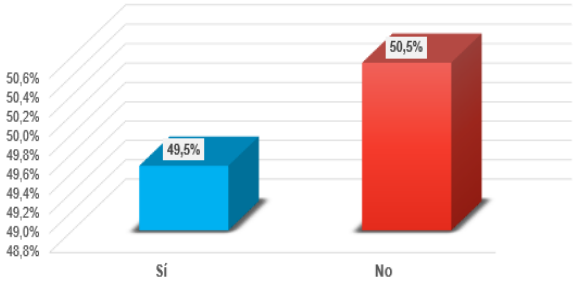


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 51,6% respondió que no conoce y el 48,4% que si. La respuesta está prácticamente dividida, con un ligero predominio del desconocimiento (51,6% no conoce), lo que puede indicar una oportunidad de mercado para aumentar la conciencia y el conocimiento sobre plataformas de gamificación.

Figura 8.

Pregunta 2. ¿ha utilizado anteriormente alguna plataforma de aprendizaje basada en gamificación?

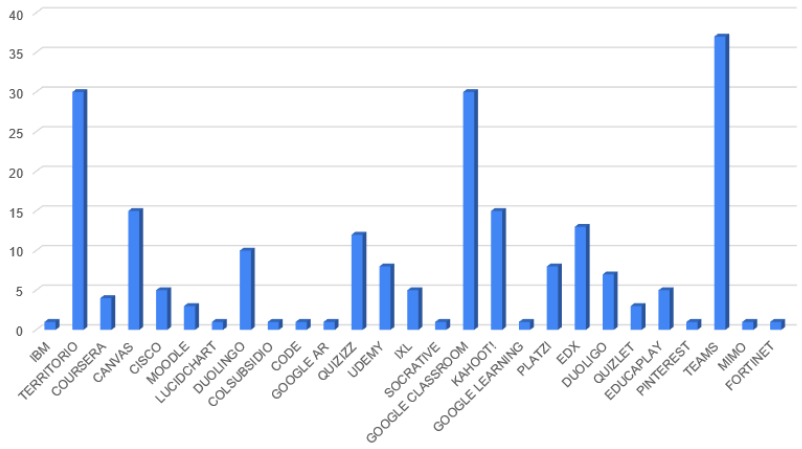


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 50,5 % respondió que no ha utilizado plataformas basadas en gamificación, lo que sugiere que hay espacio para el crecimiento de la adopción de este tipo de aprendizaje.

Figura 9.

Pregunta 3. Si la respuesta anterior es "Sí", ¿cuál/es?

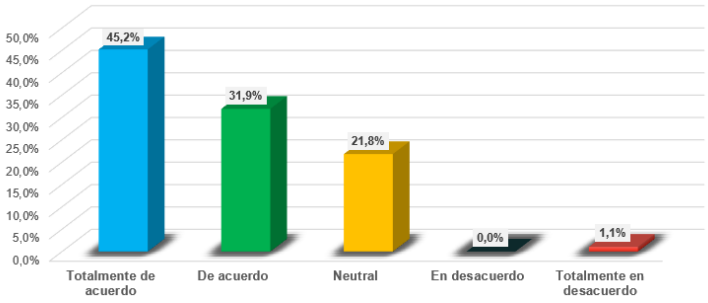


Nota. Elaboración propia a partir de la encuesta.

Resultado: Hay una gran variedad de plataformas conocidas y utilizadas, lo que muestra una diversidad en la oferta de plataformas de aprendizaje gamificadas.

Figura 10.

Pregunta 4. ¿Considera que las técnicas de gamificación mejoran su experiencia de aprendizaje?

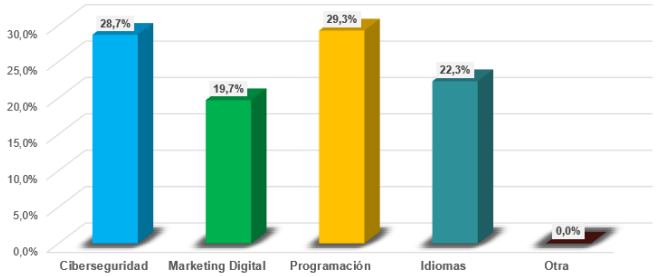


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 46,2 % respondió que está totalmente, confirmando que las técnicas de gamificación mejoran la experiencia. Un 31,9% estuvo de acuerdo y el 21,8% prefirió ser neutral. La mayoría de los encuestados (78,1% sumando 'Totalmente de acuerdo' y 'De acuerdo') cree que la gamificación mejora la experiencia de aprendizaje, lo que refleja una percepción positiva de esta técnica.

Figura 11.

Pregunta 5. ¿Qué temas le gustaría aprender a través de una plataforma gamificada?

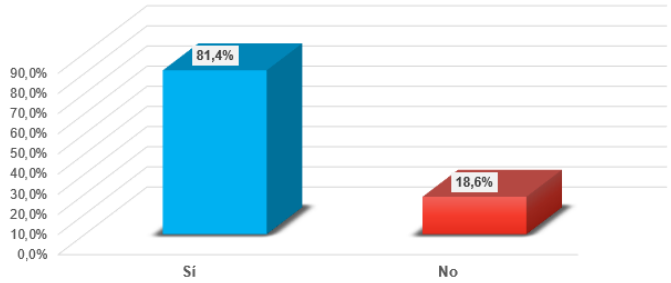


Nota. Elaboración propia a partir de la encuesta.

Resultado: Hay un interés considerable en aprender Ciberseguridad (28,7%) y programación (28,3%), destacando estas áreas como potenciales mercados para plataformas de aprendizaje gamificadas.

Figura 12.

Pregunta 6. ¿Estaría dispuesto a pagar por un curso gamificado de alta calidad?

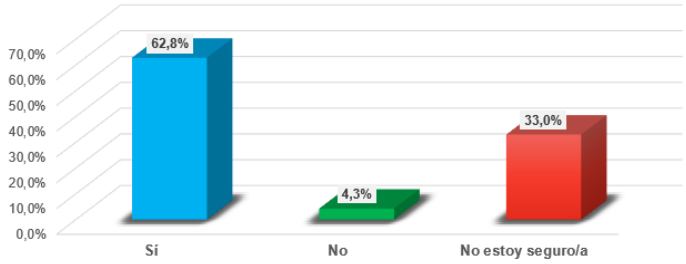


Nota. Elaboración propia a partir de la encuesta.

Resultado: Una gran mayoría (87%) está dispuesta a pagar por cursos gamificados de alta calidad, indicando una buena aceptación de modelo de negocio de pago.

Figura 13.

Pregunta 7. En comparación con los cursos tradicionales, ¿Cree que los cursos gamificados retiene más su atención?

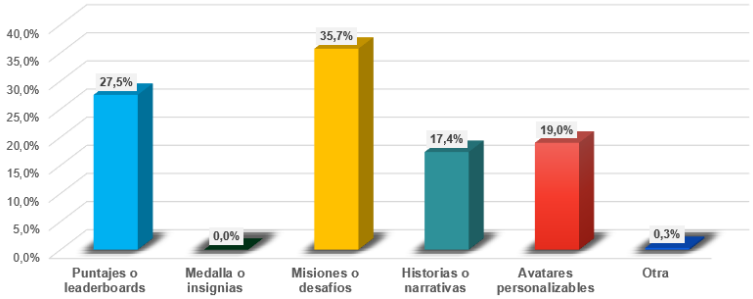


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 33% indica que no está seguro, pero una mayoría significativa (62,8%) siente que los cursos gamificados retienen más su atención en comparación con los cursos tradicionales.

Figura 14.

Pregunta 8. ¿Qué elementos de gamificación considera más atractivos?

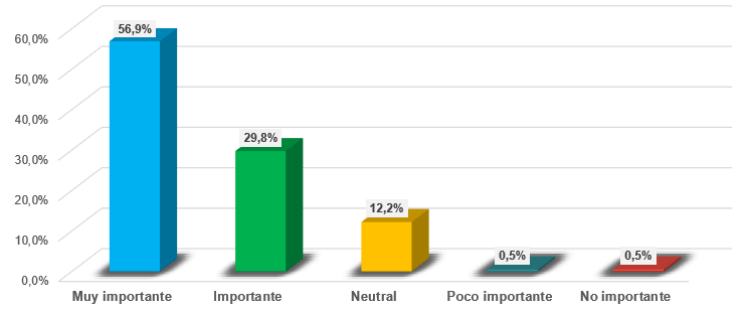


Nota. Elaboración propia a partir de la encuesta.

Resultado: Las misiones o desafíos (35.7%) y los puntajes o leaderboards (27,5%) son los elementos más atractivos, lo que puede guiar el diseño de las plataformas para enfocarse en estos aspectos.

Figura 15.

Pregunta 9.¿Que tan importante es para usted que una plataforma de aprendizaje gamificada tenga un diseño amigable y fácil de usar?

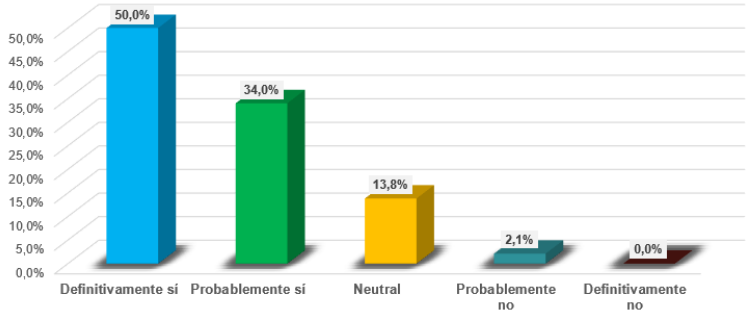


Nota. Elaboración propia a partir de la encuesta.

Resultado: Una mayoría sustancial (56,9%) considera muy importante que una plataforma tenga un diseño amigable y fácil de usar.

Figura 16.

Pregunta 10. ¿Recomendaría una plataforma de aprendizaje basada en gamificación a amigos o colegas?

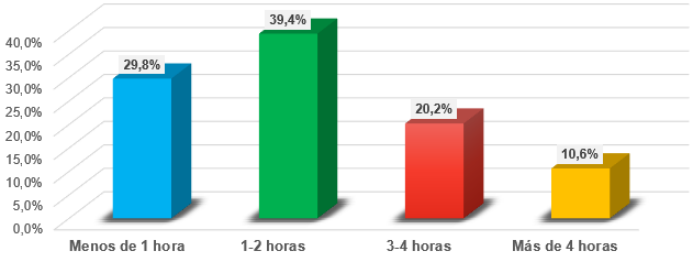


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 84% (sumando 'Definitivamente sí' y 'Probablemente sí') probablemente recomendaría estas plataformas a amigos o colegas, indicando una percepción favorable.

Figura 17.

Pregunta 11. ¿Cuánto tiempo, en promedio, dedica semanalmente a plataformas de aprendizaje en línea?

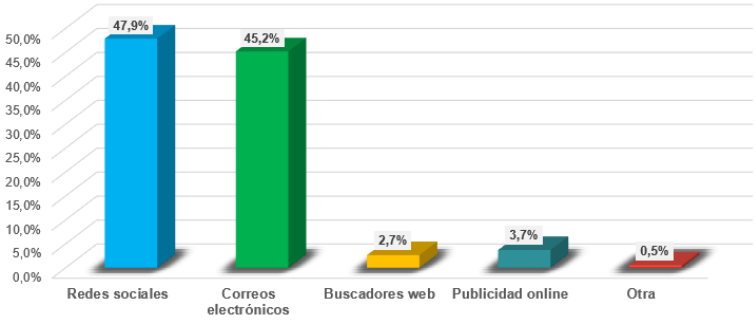


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 39,4% de los encuestados, indica que le dedicarían entre 1 y 2 horas a la plataforma de aprendizaje en línea, lo que proporciona una medida de compromiso con el aprendizaje en línea. 29,8% menos de una hora y 20,2% entre tres y cuatro horas.

Figura 18.

Pregunta 12. ¿Cuál sería el medio de comunicación preferido para recibir información y enterarse de nuevos cursos en la plataforma de GAMSECURE?

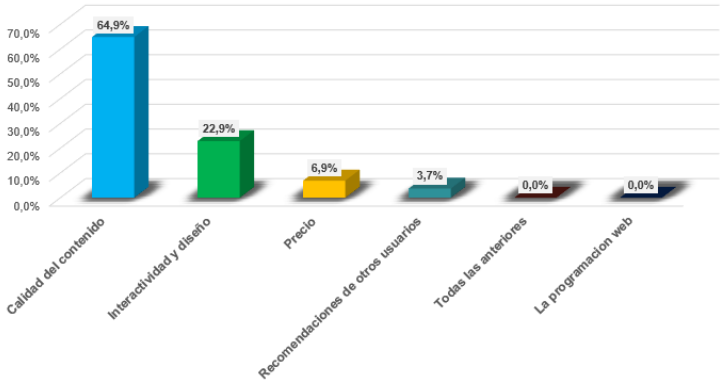


Nota. Elaboración propia a partir de la encuesta.

Resultado: Las redes sociales (47,9%) y los correos electrónicos (45,2%) son los medios preferidos, lo que podría informar estrategias de marketing y comunicación.

Figura 19.

Pregunta 13. ¿Qué factor considera más importante al elegir una plataforma de aprendizaje en línea?

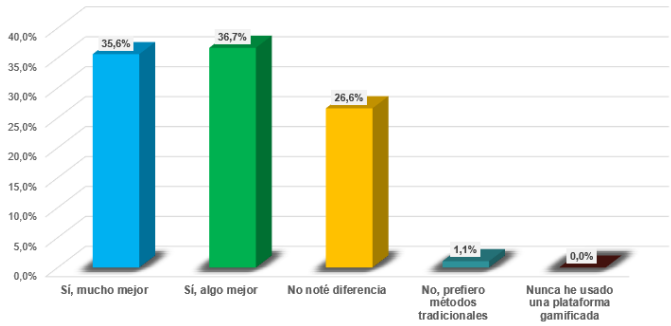


Nota. Elaboración propia a partir de la encuesta.

Resultado: La calidad del contenido (64,9%) es el factor más importante, subrayando la necesidad de un contenido de alta calidad en plataformas de aprendizaje.

Figura 20.

Pregunta 14. Si ha utilizado anteriormente plataformas gamificadas, ¿considera que su rendimiento y retención de la información fue mejor en comparación con métodos tradicionales?

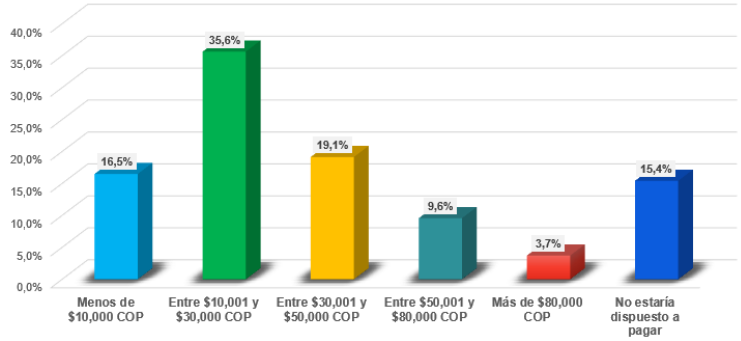


Nota. Elaboración propia a partir de la encuesta.

Resultado: La mayoría siente que las plataformas gamificadas mejoraron su rendimiento y retención de información (sumando 36,7% y 35,6%).

Figura 21.

Pregunta 15. ¿Cuánto estaría dispuesto a pagar mensualmente por el acceso a una plataforma de aprendizaje en línea con técnicas de gamificación de alta calidad como la que propone GAMSECURE?

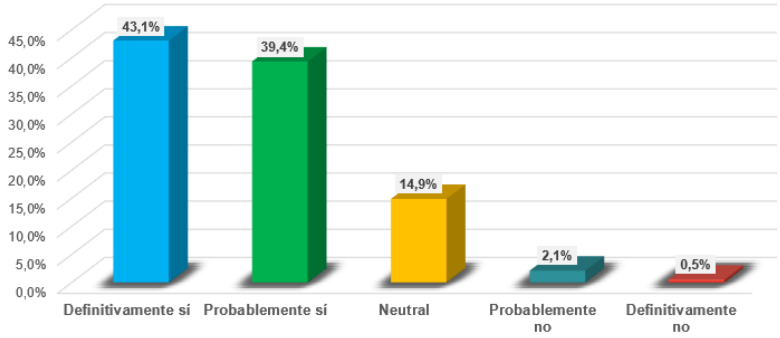


Nota. Elaboración propia a partir de la encuesta.

Resultado: La mayoría está dispuesta a pagar entre 10.000 y 30.000 COP (36,6%), lo que indica una sensibilidad al precio dentro de ese rango.

Figura 22.

Pregunta 16. En relación con el contenido de ciberseguridad ¿Considera que aporta a la creación de conciencia por parte de los empleados?

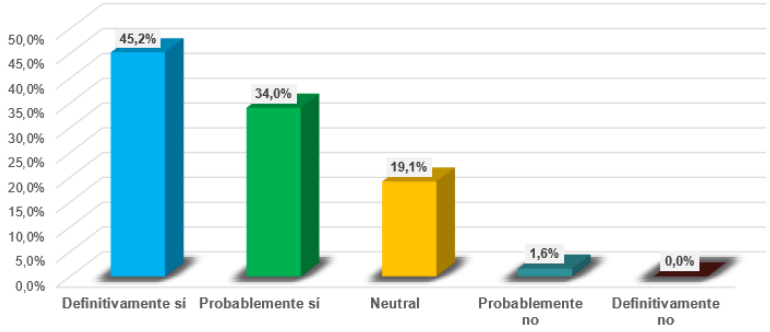


Nota. Elaboración propia a partir de la encuesta.

Resultado: Una gran parte (82,5% sumando 'Definitivamente sí' y 'Probablemente sí') cree que el contenido de ciberseguridad contribuye a la conciencia de los empleados.

Figura 23.

Pregunta 17. Como califica la experiencia contenido de ciberseguridad ¿Considera que aporta a la creación de conciencia por parte de los empleados?

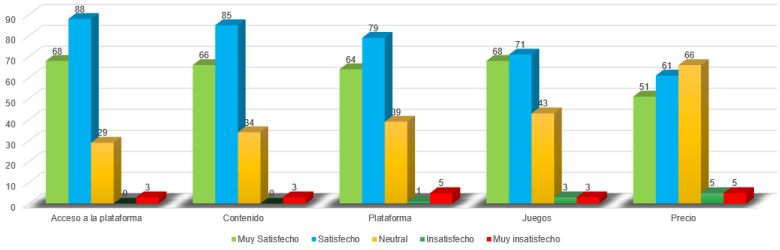


Nota. Elaboración propia a partir de la encuesta.

Resultado: Un 45,2% confirma que definitivamente contribuye a la creación de conciencia, reforzando la respuesta de la pregunta 16.

Figura 24.

Pregunta 18. Por favor, califica tu nivel de satisfacción para los siguientes puntos? (Responde a las opciones: Muy insatisfecho, Insatisfecho, Neutral, Satisfecho, Muy Satisfecho)

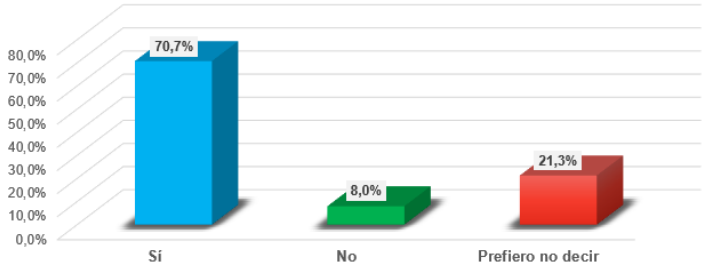


Nota. Elaboración propia a partir de la encuesta.

Resultado: La satisfacción es alta con respecto al acceso y contenido, 64% para la plataforma, juegos con un 68% y un 51% para el precio.

Figura 25.

Pregunta 19. ¿Crees que la duración del programa fue lo suficientemente buena como para satisfacer las expectativas de formación?

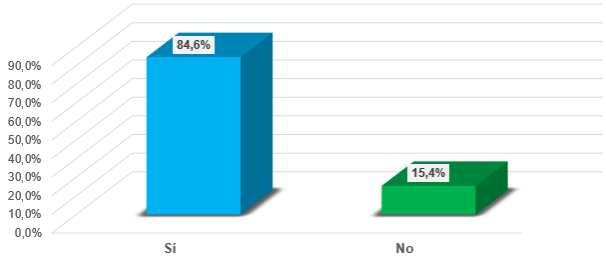


Nota. Elaboración propia a partir de la encuesta.

Resultado: El 70,7% de los encuestados confirma que la duración del curso fue los suficientemente buena para satisfacer las necesidades, con relación a sus expectativas de formación.

Figura 26.

Pregunta 20. ¿Después de realizar el curso se siente con el conocimiento para identificar y reaccionar ante un posible riesgo a la seguridad de la información (ejemplo Phishing)?



Nota. Elaboración propia a partir de la encuesta.

Resultado: La mayoría (84,6%) siente que ahora tiene el conocimiento para identificar y reaccionar ante riesgos de seguridad.

C. Anexo 3. Ficha Técnica Productos o Servicios.

Tabla 12.

Ficha técnica del producto o servicio.

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Fundamentos en Ciberseguridad” **Código: FCE**
Descripción	El curso de "Fundamentos en Ciberseguridad" es una introducción esencial al mundo de la ciberseguridad. Diseñado tanto para individuos como para empresas, este curso proporciona los conocimientos y habilidades fundamentales necesarios para comprender y abordar las amenazas cibernéticas.
Contenido del Curso	Módulo 1: Introducción a la Ciberseguridad Módulo 2: Amenazas y Riesgos Módulo 3: Principios Fundamentales de Seguridad Módulo 4: Prácticas de Seguridad de Contraseñas Módulo 5: Concientización en Ciberseguridad
Objetivos del curso	✓ Comprender los conceptos básicos de la ciberseguridad. ✓ Identificar y mitigar amenazas cibernéticas comunes. ✓ Aprender prácticas de seguridad de datos y contraseñas. ✓ Concientizar sobre la importancia de la ciberseguridad.
Público objetivo	✓ Empresas que desean capacitar a sus empleados en prácticas de ciberseguridad. ✓ Individuos interesados en aprender sobre ciberseguridad.
Modalidad	Curso en línea autoadministrado.
Duración	4 semanas (puede variar según el ritmo de estudio del participante).
Certificación	Certificado de finalización disponible al completar el curso y superar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Adquiere conocimientos fundamentales en ciberseguridad. ✓ Protege tus datos y dispositivos en línea. ✓ Mejora la seguridad de tu empresa y reduce el riesgo de brechas de seguridad. ✓ Capacidad de gestionar situaciones de seguridad en un mundo digital.

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Introducción a la Ciberseguridad” **Código: ICE**
Descripción	El curso "Introducción a la Ciberseguridad" es una formación esencial diseñada para brindar a individuos y organizaciones una comprensión sólida de los principios fundamentales de la ciberseguridad. Este curso proporciona una base sólida para la protección de datos y sistemas en un mundo digital en constante cambio.
Contenido del Curso	Módulo 1: Conceptos Básicos de Ciberseguridad Módulo 2: Amenazas y Ataques Cibernéticos Módulo 3: Seguridad de la Información Módulo 4: Seguridad de Red y Comunicaciones Módulo 5: Seguridad de Sistemas y Software Módulo 6: Prácticas de Seguridad de Contraseñas
Objetivos del curso	✓ Comprender los conceptos fundamentales de ciberseguridad. ✓ Identificar y reconocer amenazas y ataques cibernéticos comunes. ✓ Adquirir habilidades para proteger la información y los sistemas. ✓ Fomentar la conciencia de la importancia de la ciberseguridad.
Público objetivo	✓ Empresas que desean capacitar a sus empleados en ciberseguridad. ✓ Individuos que deseen comprender los principios básicos de ciberseguridad.
Modalidad	Curso en línea autoadministrado.
Duración	6 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Establece una base sólida en ciberseguridad. ✓ Mejora la seguridad de la información personal y empresarial. ✓ Proporciona a los empleados las habilidades necesarias para proteger los datos de la organización. ✓ Fomenta una cultura de seguridad en la empresa.

Nota: Elaboración

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Higiene Digital y Seguridad en el Uso de Internet” **Código: HDSUI**
Descripción	El curso "Higiene Digital y Seguridad en el Uso de Internet" está diseñado para proporcionar conocimientos esenciales sobre la seguridad en línea y prácticas seguras al navegar por Internet. Dirigido tanto a individuos como a empresas, este curso enseña

Ficha Técnica del Producto o Servicio	
	cómo proteger la información personal y corporativa en el mundo digital.
Contenido del Curso	Módulo 1: Introducción a la Higiene Digital Módulo 2: Amenazas en Línea y Ataques Comunes Módulo 3: Seguridad de Correo Electrónico y Redes Sociales Módulo 4: Protección de Datos Personales Módulo 5: Seguridad en Transacciones en Línea Módulo 6: Prácticas de Seguridad en Navegadores Web
Objetivos del curso	✓ Comprender la importancia de la higiene digital y la seguridad en línea. ✓ Identificar amenazas comunes en Internet y cómo evitarlas. ✓ Adquirir habilidades para proteger datos personales y corporativos en línea. ✓ Fomentar una cultura de seguridad en la empresa y entre los individuos.
Público objetivo	✓ Empresas que desean capacitar a sus empleados en seguridad en Internet. ✓ Individuos interesados en aprender prácticas seguras en línea.
Modalidad	Curso en línea autoadministrado.
Duración	6 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Aumenta la conciencia de la importancia de la higiene digital y la seguridad en línea. ✓ Protege la información personal y corporativa de amenazas en línea. ✓ Ayuda a los empleados a navegar de manera segura por Internet y a evitar trampas en línea. ✓ Promueve la seguridad en línea en la empresa y en la vida personal.

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Protección de Datos Personales” **Código: PDP**
Descripción	El curso "Protección de Datos Personales" se enfoca en la importancia de salvaguardar la información personal y sensible. Tanto para individuos como empresas, este curso ofrece pautas claras sobre cómo proteger los datos personales y cumplir con las regulaciones de privacidad.
Contenido del Curso	Módulo 1: Introducción a la Protección de Datos Personales Módulo 2: Regulaciones y Leyes de Privacidad Módulo 3: Prácticas de Protección de Datos

Ficha Técnica del Producto o Servicio	
	Módulo 4: Cumplimiento Legal y Responsabilidad
Objetivos del curso	✓ Comprender la importancia de la protección de datos personales. ✓ Conocer las regulaciones de privacidad relevantes. ✓ Aprender cómo proteger y gestionar datos personales. ✓ Cumplir con las leyes de privacidad y responsabilidad.
Público objetivo	✓ Empresas que buscan cumplir con regulaciones de privacidad ✓ Individuos interesados en proteger datos personales.
Modalidad	Curso en línea autoadministrado.
Duración	4 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Protege datos personales de amenazas y violaciones. ✓ Cumple con las regulaciones de privacidad y protección de datos. ✓ Mejora la conciencia y la responsabilidad en la protección de datos.

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Prácticas de Contraseñas Seguras” **Código: PCS**
Descripción	El curso "Prácticas de Contraseñas Seguras" se centra en la importancia de mantener contraseñas fuertes y seguras. Está diseñado para enseñar a individuos y empresas cómo crear y gestionar contraseñas de forma segura.
Contenido del Curso	Módulo 1: Importancia de Contraseñas Seguras Módulo 2: Creación de Contraseñas Fuertes Módulo 3: Gestión y Almacenamiento Seguro de Contraseñas
Objetivos del curso	✓ Comprender la importancia de las contraseñas seguras. ✓ Aprender a crear contraseñas fuertes y únicas. ✓ Conocer las mejores prácticas para gestionar y almacenar contraseñas.
Público objetivo	✓ Individuos interesados en mejorar la seguridad de sus contraseñas. ✓ Empresas que deseen fortalecer las prácticas de seguridad de contraseñas.
Modalidad	Curso en línea autoadministrado.
Duración	3 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.

Ficha Técnica del Producto o Servicio	
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Refuerza la seguridad en línea a través de contraseñas seguras. ✓ Protege cuentas y datos de ataques de acceso no autorizado. ✓ Facilita la gestión y el almacenamiento seguros de contraseñas

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Seguridad en el Correo Electrónico y Protección contra el Phishing” **Código: CEPP**
Descripción	El curso "Seguridad en el Correo Electrónico y Protección contra el Phishing" se centra en la seguridad de las comunicaciones por correo electrónico y la prevención de ataques de phishing. Está diseñado tanto para individuos como para empresas, brindando conocimientos y habilidades esenciales para protegerse contra amenazas en línea.
Contenido del Curso	Módulo 1: Seguridad en el Correo Electrónico Módulo 2: Identificación de Correos Electrónicos de Phishing Módulo 3: Prevención de Ataques de Phishing Módulo 4: Prácticas de Comunicación Segura
Objetivos del curso	✓ Comprender los riesgos de seguridad en el correo electrónico. ✓ Identificar correos electrónicos de phishing y otras amenazas. ✓ Aprender a prevenir y responder a ataques de phishing. ✓ Mejorar la seguridad de la comunicación por correo electrónico.
Público objetivo	✓ Individuos interesados en protegerse contra el phishing y otras amenazas por correo electrónico. ✓ Empresas que buscan fortalecer la seguridad en la comunicación por correo electrónico.
Modalidad	Curso en línea autoadministrado.
Duración	4 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Protege a los individuos y a la empresa contra ataques de phishing. ✓ Mejora la seguridad en la comunicación por correo electrónico. ✓ Reduce el riesgo de caer en estafas en línea. ✓ Fortalece la conciencia y la respuesta a amenazas por correo electrónico.

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Seguridad en el Trabajo Remoto” **Código: STR**
Descripción	El curso "Seguridad en el Trabajo Remoto" se centra en la seguridad de los empleados que trabajan fuera de la oficina, ya sea de forma ocasional o a tiempo completo. Está diseñado para brindar a individuos y empresas las habilidades necesarias para garantizar la seguridad de los datos y sistemas mientras se trabaja de forma remota.
Contenido del Curso	Módulo 1: Introducción a la Seguridad en el Trabajo Remoto Módulo 2: Seguridad de la Conexión Remota Módulo 3: Protección de Dispositivos Remotos Módulo 4: Prácticas de Seguridad en el Trabajo Remoto
Objetivos del curso	✓ Comprender los riesgos y desafíos de trabajar de forma remota. ✓ Aprender a establecer conexiones seguras y proteger dispositivos remotos. ✓ Adquirir prácticas de seguridad efectivas para el trabajo remoto. ✓ Garantizar la seguridad de los datos y sistemas fuera de la oficina.
Público objetivo	✓ Individuos que trabajan o desean trabajar de forma remota. ✓ Empresas que deseen fortalecer la seguridad de los empleados remotos.
Modalidad	Curso en línea autoadministrado.
Duración	4 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Asegura la seguridad de los empleados que trabajan de forma remota. ✓ Protege los datos y sistemas fuera de la oficina. ✓ Fomenta una cultura de seguridad en el trabajo remoto. ✓ Facilita la transición al trabajo remoto de forma segura.

Nota: Elaboración propia

Ficha Técnica del Producto o Servicio	
Denominación del Producto/Servicio	Curso: “Responsabilidad Legal y Ética en Ciberseguridad” **Código: RLEC**
Descripción	El curso "Responsabilidad Legal y Ética en Ciberseguridad" se enfoca en las cuestiones legales y éticas relacionadas con la ciberseguridad. Está diseñado para individuos y empresas que deseen comprender sus obligaciones legales y éticas en la protección de datos y sistemas.
Contenido del Curso	Módulo 1: Ética en la Ciberseguridad Módulo 2: Cumplimiento Legal en Ciberseguridad

Ficha Técnica del Producto o Servicio	
	Módulo 3: Responsabilidad Legal y Consecuencias Módulo 4: Casos de Estudio y Mejores Prácticas
Objetivos del curso	✓ Comprender la importancia de la ética en la ciberseguridad. ✓ Conocer las regulaciones y leyes de ciberseguridad relevantes. ✓ Identificar la responsabilidad legal y las consecuencias de las violaciones. ✓ Aplicar las mejores prácticas legales y éticas en ciberseguridad.
Público objetivo	✓ Individuos interesados en la ética y la responsabilidad legal en ciberseguridad. ✓ Empresas que buscan cumplir con regulaciones y promover prácticas éticas.
Modalidad	Curso en línea autoadministrado.
Duración	4 semanas (el ritmo de estudio es flexible y se adapta a las necesidades de los participantes).
Certificación	Certificado de finalización disponible al completar el curso y aprobar las evaluaciones.
Requisitos Técnicos	✓ Conexión a Internet. ✓ Dispositivo con capacidad para acceder al contenido en línea.
Beneficios	✓ Fomenta la ética y la responsabilidad en la ciberseguridad. ✓ Ayuda a cumplir con las regulaciones y leyes de ciberseguridad. ✓ Reduce el riesgo legal y mejora la reputación de la empresa. ✓ Proporciona directrices éticas para individuos y organizaciones.

Nota: Elaboración propia

D. Anexo 4. Personal Requerido

Tabla 13.

Personal requerido para la producción o prestación de servicios.

<table>
<tr><th colspan="2">Formato Descripción del Cargo</th></tr>
<tr><td>Nombre: Director Técnico - Experto en Ciberseguridad</td><td>Jefe Inmediato: Director ejecutivo</td></tr>
<tr><td>Nivel del Cargo: Operativo</td><td></td></tr>
<tr><td colspan="2">Misión del Cargo:
Diseñar, crear y ofrecer cursos de ciberseguridad de alta calidad que permitan a los estudiantes adquirir los conocimientos y habilidades necesarios para proteger la información y los sistemas de una organización. Esto implica el desarrollo de contenidos didácticos, la creación de materiales de formación efectivos y la implementación de estrategias de enseñanza innovadoras. La misión se centra en preparar a los estudiantes para comprender, prevenir y mitigar las amenazas cibernéticas, así como en fomentar una cultura de seguridad cibernética. Además, el Experto en Ciberseguridad debe estar al tanto de las últimas tendencias y amenazas en ciberseguridad y asegurarse de que los contenidos de los cursos estén actualizados y reflejen los desafíos actuales en este campo.
Funciones:
➢ Diseñar y desarrollar material didáctico efectivo y relevante para cursos de ciberseguridad, que incluye presentaciones, guías, lecturas y ejercicios.
➢ Desarrollar recursos de aprendizaje, como videos, simulaciones y actividades interactivas, para mejorar la comprensión de los conceptos de ciberseguridad.
➢ Contribuir al diseño curricular de los cursos, identificando los temas clave y secuenciándolos de manera lógica.
➢ Planificar y organizar la estructura de los cursos, estableciendo objetivos de aprendizaje claros y definiendo las estrategias pedagógicas adecuadas.
➢ Diseñar y administrar evaluaciones, exámenes y proyectos para medir el progreso y la comprensión de los estudiantes.
➢ Mantenerse al tanto de las últimas tendencias y amenazas en ciberseguridad y actualizar regularmente el contenido de los cursos.
➢ Brindar asistencia y responder a preguntas de los estudiantes sobre los temas de ciberseguridad.</td></tr>
<tr><th colspan="2">Perfil Requerido</th></tr>
<tr><td>Educación:
Ingeniero de Sistemas, Licenciado en Sistemas o Informática
Especialista en Seguridad Informática, Ciberseguridad</td><td>Experiencia:
24 meses en el campo de la ciberseguridad. Esto puede incluir roles como analista de seguridad, administrador de seguridad de la información o especialista en seguridad de redes.
24 meses en desarrollo de contenidos de cursos y la enseñanza, se valorará la experiencia previa en la creación de material didáctico y la instrucción en ciberseguridad.</td></tr>
</table>

Nota: Elaboración propia.

<table>
<tr><th colspan="2">Formato Descripción del Cargo</th></tr>
<tr><td>Nombre: Desarrollador</td><td>Jefe Inmediato: Director ejecutivo</td></tr>
<tr><td>Nivel del Cargo: Operativo</td><td></td></tr>
<tr><td colspan="2">Misión del Cargo:
Diseñar y producir materiales multimedia de alta calidad que mejoren la comunicación y la formación en la organización. Esto se logra a través de la creación de videos, animaciones, presentaciones interactivas y otros elementos multimedia que transmitan información de manera efectiva y atractiva. La misión se centra en enriquecer la experiencia de aprendizaje, comunicación y marketing, contribuyendo al logro de los objetivos de la organización y al compromiso de sus audiencias.
Funciones:
➢ Crear contenido multimedia, como videos, animaciones, presentaciones interactivas, infografías y otros materiales visuales, que sean atractivos y efectivos.
➢ Guiar el proceso creativo desde la concepción hasta la finalización del proyecto.
➢ Escribir guiones y crear storyboards para planificar y estructurar proyectos multimedia, asegurando que el contenido comunique de manera efectiva el mensaje deseado.
➢ Dirigir y participar en la producción de contenido multimedia, que incluye tareas como la grabación de video, edición de audio, animación, diseño gráfico y otros aspectos técnicos.
➢ Evaluar y seleccionar las herramientas y tecnologías multimedia adecuadas para cada proyecto, teniendo en cuenta las necesidades y los objetivos específicos.
➢ Realizar la edición y postproducción de materiales multimedia, incluyendo la corrección de color, montaje de video, efectos especiales y otros aspectos técnicos.
➢ Mantener altos estándares de calidad visual y sonora en todos los proyectos, asegurando una experiencia multimedia atractiva y efectiva.
➢ Mantener y actualizar los contenidos multimedia existentes según sea necesario para mantener la relevancia y la precisión de la información.</td></tr>
<tr><th colspan="2">Perfil Requerido</th></tr>
<tr><td>Educación:
Diseñador Gráfico
Comunicador Audiovisual y Digital
Familiaridad con herramientas y plataformas multimedia, como Adobe Creative Suite, software de edición de video, herramientas de animación y presentación, y software de diseño gráfico.</td><td>Experiencia:
24 meses en el desarrollo de contenido multimedia, que incluya la creación de videos, animaciones, gráficos y otros elementos visuales interactivos.
12 meses en edición de video, producción de medios y uso de software de edición, como Adobe Premiere, Adobe After Effects, Final Cut Pro u otras herramientas similares, es altamente valorada.</td></tr>
</table>

Nota: Elaboración propia.

<table>
<tr><th colspan="2">Formato Descripción del Cargo</th></tr>
<tr><td>Nombre: Director Ejecutivo</td><td>Jefe Inmediato: N/A</td></tr>
<tr><td>Nivel del Cargo: Estratégico</td><td></td></tr>
<tr><td colspan="2">Misión del Cargo:
Liderar y supervisar un equipo o departamento en la organización para lograr los objetivos y metas establecidos. Esto implica la planificación estratégica, la asignación de recursos, la toma de decisiones efectivas y la gestión de personal para asegurar el éxito de las operaciones. El Gerente trabaja en colaboración con otros líderes y departamentos, comunica la visión de la organización y garantiza que su equipo esté alineado con los valores y la cultura de la empresa. Además, el Gerente es responsable de garantizar un ambiente de trabajo productivo, el desarrollo de su equipo y la rendición de cuentas por los resultados.
Funciones:
➢ Participar en la planificación estratégica de la organización y traducir esa estrategia en objetivos y metas específicas para su departamento o equipo.
➢ Proporcionar liderazgo y dirección a su equipo, estableciendo expectativas claras y alineando a los miembros del equipo con los objetivos organizacionales.
➢ Tomar decisiones clave para el departamento o equipo, abordando desafíos y aprovechando oportunidades para el éxito.
➢ Gestionar y supervisar el desempeño del personal, incluyendo la contratación, la formación, el desarrollo y la evaluación del rendimiento.
➢ Comunicar la visión, los objetivos y las expectativas a los miembros del equipo y otros departamentos, asegurando una comunicación efectiva en toda la organización.
➢ Monitorear y evaluar el progreso hacia los objetivos y metas, y tomar medidas correctivas según sea necesario.
➢ Fomentar y mantener una cultura organizacional positiva y productiva dentro del equipo.
➢ Liderar y gestionar procesos de cambio dentro del departamento, adaptando estrategias y operaciones según sea necesario.
➢ Ser responsable de los resultados y el desempeño del equipo ante la alta dirección y la organización en su conjunto.
➢ Identificar riesgos y oportunidades para el departamento y desarrollar estrategias para mitigar o capitalizar estos aspectos.
➢ Buscar oportunidades de mejora continua en las operaciones, procesos y procedimientos del departamento.</td></tr>
<tr><th colspan="2">Perfil Requerido</th></tr>
<tr><td>Educación:
Profesional o Especialista en áreas de administración de empresas o gerencia de proyectos.</td><td>Experiencia:
48 meses en cargos directivos, gerenciales o similares.</td></tr>
</table>

Nota: Elaboración propia.

Formato Descripción del Cargo	
Nombre: Analista Marketing y ventas	**Jefe Inmediato:** Director Técnico
Nivel del Cargo: Operativo	

Misión del Cargo:

Desarrollar e implementar estrategias de marketing que generen conciencia, interés y demanda por los productos, servicios o la marca de la organización. Esto se logra a través de la planificación de campañas, el uso de diversos canales de marketing, la creación de contenido atractivo y relevante, y la medición del desempeño. La misión se centra en aumentar la visibilidad de la organización en el mercado, generar clientes potenciales, retener a los clientes actuales y contribuir al crecimiento y el éxito de la empresa. Además, el Especialista en Marketing debe mantenerse actualizado con las tendencias y las mejores prácticas de marketing para garantizar un enfoque efectivo y actualizado.

Funciones:

- Realizar investigaciones de mercado para comprender a la audiencia, las tendencias del mercado, la competencia y las oportunidades.
- Desarrollar estrategias de marketing que incluyan objetivos claros, tácticas, presupuesto y plazos.
- Planificar, ejecutar y supervisar campañas de marketing, que pueden incluir publicidad en línea, marketing de contenidos, email marketing, redes sociales, entre otros.
- Crear contenido atractivo y relevante, como blogs, artículos, videos, infografías y otros materiales para atraer y retener a la audiencia.
- Administrar y mantener una presencia activa en las redes sociales, interactuando con seguidores y gestionando la programación de publicaciones.
- Optimizar el contenido y el sitio web para motores de búsqueda (SEO) y gestionar campañas de búsqueda paga (SEM) para aumentar la visibilidad en línea.
- Diseñar y ejecutar campañas de email marketing para llegar a la audiencia y mantener a los suscriptores informados.
- Utilizar herramientas de análisis para evaluar el rendimiento de las campañas y ajustar estrategias según sea necesario.
- Crear y gestionar estrategias para la generación de clientes potenciales y la construcción de listas de contactos.
- Implementar estrategias para convertir clientes potenciales en clientes reales y mantener una base de clientes leales.
- Planificar y coordinar eventos, ferias comerciales y promociones para aumentar la visibilidad de la empresa.
- Mantenerse al tanto de las últimas tendencias y mejores prácticas de marketing, y aplicarlas en las estrategias.

Perfil Requerido	
Educación: Profesional en las áreas de mercadeo, comunicaciones o afines.	**Experiencia:** 24 meses en ventas, mercadeo, comunicaciones.

Nota: Elaboración propia.

E. Anexo 5. Ficha Técnica Entrevistas y Formato Entrevista

Tabla 14.
Ficha técnica y formato entrevista Experto Técnico

Realizada por	Eumir Pulido de la Pava
Nombre de la encuesta	Encuesta sobre Ciberseguridad: Perspectivas de Expertos Técnicos
Universo	Profesionales con experiencia significativa en el campo de la ciberseguridad
Tipo de muestreo	No probabilístico o de juicio
Técnica de recolección de datos	Entrevista Semiestructurada (si bien se tienen algunas preguntas predefinidas, el entrevistador tiene la libertad de explorar temas adicionales o profundizar en ciertos aspectos según las respuestas del entrevistado).
Fecha de creación	7 de junio de 2023
Objetivo de la encuesta	Obtener información relevante y valiosa sobre las necesidades, expectativas, percepciones, desafíos y oportunidades de cada grupo de interés en relación con la propuesta de valor y el modelo de negocio.
N.º de preguntas formuladas	9
N.º de encuestadores	1
Tipo de preguntas aplicadas	Preguntas abiertas

Formato Entrevista Experto Técnico

Grupo de interés:	Experto Técnico
Objetivo de la entrevista:	Obtener información relevante y valiosa sobre las necesidades, expectativas, percepciones, desafíos y oportunidades de cada grupo de interés en relación con la propuesta de valor y el modelo de negocio.
Hipótesis o dudas para validar (del modelo de negocios):	Entender las necesidades, desafíos, expectativas y posibilidades de los clientes potenciales, los proveedores y socios estratégicos, los empresarios y los expertos en sostenibilidad, así como identificar las oportunidades de mejora en la oferta de la plataforma y su modelo de negocio, así como los recursos y herramientas más

	efectivos para atraer y fidelizar a los clientes potenciales. La información recopilada nos permitirá ajustar y fortalecer nuestra propuesta de valor y nuestra estrategia comercial, maximizando el impacto y la sostenibilidad de la plataforma.
Mensaje (es un mensaje de introducción para romper el hielo):	Hola, somos GAMSECURE SAS. Estamos trabajando en el desarrollo de una plataforma de capacitación en ciberseguridad para PYME y nos interesa conocer su opinión y necesidades como experto técnico. Con esta entrevista, buscamos entender mejor su perspectiva sobre la ciberseguridad en las PYME, los desafíos y oportunidades que enfrentan en este tema, y cómo podemos mejorar nuestra propuesta de valor y nuestra estrategia comercial para satisfacer sus necesidades.

Preguntas para realizar:

1. ¿Qué consideraciones técnicas específicas se deben tener en cuenta para desarrollar una plataforma web de capacitación en ciberseguridad para PYME?
2. ¿Cuáles son las principales tecnologías y herramientas que se deben utilizar para garantizar la seguridad y la confidencialidad de la información de los usuarios?
3. ¿Qué clase de contenido espera encontrar en la plataforma web que sea de interés y utilidad para la sensibilización de colaboradores de la PYME?
4. ¿Cuáles son los principales costos y gastos asociados con la creación y el mantenimiento de una plataforma web de capacitación en ciberseguridad para PYME?
5. ¿Qué desafíos técnicos podrían surgir al ofrecer cursos web de ciberseguridad y cómo se pueden abordar estos desafíos?
6. ¿Cómo se puede garantizar la calidad y relevancia de los cursos en línea de ciberseguridad ofrecidos en la plataforma?
7. ¿Cómo se puede garantizar la escalabilidad de la plataforma web para atender a un número cada vez mayor de usuarios y demanda de cursos?
8. ¿Qué consideraciones técnicas se deben tener en cuenta al establecer alianzas estratégicas con proveedores de seguridad cibernética y otros socios

para mejorar la calidad y la relevancia de los cursos y recursos de capacitación web? 9. ¿Conoce usted plataformas web que ofrezcan los servicios de capacitación utilizando técnicas de gamificación?

Tabla 15.

Ficha técnica y formato entrevista Aliado Estratégico

Realizada por	Eumir Pulido de la Pava
Nombre de la encuesta	Encuesta de Evaluación de Ciberseguridad para Aliados Estratégicos
Universo	Profesionales y empresas con experiencia en ciberseguridad, especialmente aliados estratégicos en la industria de la seguridad informática.
Tipo de muestreo	Muestreo no probabilístico o de juicio. Se seleccionan aliados estratégicos en base a su experiencia y conocimientos en ciberseguridad.
Técnica de recolección de datos	Entrevista semiestructurada. Permite una exploración más profunda de los temas y opiniones del aliado estratégico.
Fecha de creación	1 de junio de 2023
Objetivo de la encuesta	Obtener información relevante y valiosa sobre las necesidades, expectativas, percepciones, desafíos y oportunidades de cada grupo de interés en relación con la propuesta de valor, el modelo de negocio y los costos.
N.º de preguntas formuladas	7
N.º de encuestadores	1
Tipo de preguntas aplicadas	Preguntas abiertas

Formato Entrevista Aliado Clave

Grupo de interés:	Aliado clave (proveedor, socio, distribuidor)

Objetivo de la entrevista:	Obtener información relevante y valiosa sobre las necesidades, expectativas, percepciones, desafíos y oportunidades de cada grupo de interés en relación con la propuesta de valor, el modelo de negocio y los costos.
Hipótesis o dudas para validar (del modelo de negocios):	Entender las necesidades, desafíos, expectativas y posibilidades de los clientes potenciales, los proveedores y socios estratégicos, los empresarios y los expertos en sostenibilidad. Además, queremos identificar las oportunidades de mejora en la oferta de la plataforma y su modelo de negocio, así como los recursos y herramientas más efectivos para atraer y fidelizar a los clientes potenciales. La información recopilada nos permitirá ajustar y fortalecer nuestra propuesta de valor y nuestra estrategia comercial, maximizando el impacto y la sostenibilidad de la plataforma.
Mensaje (es un mensaje de introducción para romper el hielo):	Hola, somos GAMSECURE SAS. Estamos trabajando en el desarrollo de una plataforma de capacitación en ciberseguridad para PYME y nos interesa conocer su opinión y necesidades como Aliado Clave. Con esta entrevista, buscamos entender mejor su perspectiva sobre la ciberseguridad en las PYME, los desafíos y oportunidades que enfrentan en este tema, y cómo podemos mejorar nuestra propuesta de valor y nuestra estrategia comercial para satisfacer sus necesidades.

Preguntas para realizar:

1. ¿Cómo ve la oportunidad de colaborar con nosotros en un proyecto de capacitación web en ciberseguridad para PYME? ¿Cree que esta es una iniciativa valiosa para su empresa?
2. ¿Qué tipo de recursos podría aportar a este proyecto, ya sea financieros, técnicos o humanos? ¿Cómo podría ayudar a asegurar el éxito del proyecto?

3. ¿Cómo podríamos asegurarnos de que nuestra relación de trabajo sea mutuamente beneficiosa y sostenible a largo plazo? ¿Qué medidas de seguimiento o monitoreo podríamos poner en marcha para evaluar nuestro progreso juntos?
4. ¿Cree que hay otros socios clave que podrían ser valiosos para involucrar en este proyecto? ¿Cómo podríamos trabajar juntos para maximizar el impacto de nuestro trabajo?
5. ¿Cuáles son algunas de las preocupaciones o riesgos que ve en cuanto a colaborar con nosotros en este proyecto? ¿Cómo podríamos abordar estas preocupaciones y garantizar una colaboración productiva?
6. ¿Qué tipo de costos podríamos esperar en términos de su colaboración en este proyecto? ¿Cómo podríamos trabajar juntos para garantizar que los costos se mantengan dentro de un presupuesto razonable?
7. ¿Qué tipo de beneficios ve en términos de colaborar con nosotros en este proyecto? ¿Cómo podríamos trabajar juntos para maximizar estos beneficios y asegurarnos de que se logren nuestros objetivos compartidos?

Tabla 16.
Ficha técnica y formato entrevista Emprendedores - Empresarios

Realizada por	Eumir Pulido de la Pava
Nombre de la encuesta	Encuesta de Percepción de Ciberseguridad para Emprendedores - Empresarios
Universo	Emprendedores y empresarios con experiencia en diversos sectores y niveles de negocio, especialmente aquellos interesados en ciberseguridad.
Tipo de muestreo	Muestreo no probabilístico o de juicio. Se seleccionan emprendedores y empresarios con base en su experiencia y conocimientos en ciberseguridad.
Técnica de recolección de datos	Entrevista semiestructurada. Permite una exploración más profunda de los conocimientos y perspectivas de los emprendedores y empresarios en ciberseguridad.
Fecha de creación	2 de junio de 2023

Objetivo de la encuesta	Validar el concepto del negocios, potencial y visión emprendedora, costos y modelo de ingreso
N.º de preguntas formuladas	7
N.º de encuestadores	1
Tipo de preguntas aplicadas	Preguntas abiertas

Formato Entrevista Empresarios

Grupo de interés:	Empresarios
Objetivo de la entrevista:	Validar el concepto del negocios, potencial y visión emprendedora, costos y modelo de ingreso
Hipótesis o dudas para validar (del modelo de negocios):	Buscamos entender las necesidades, desafíos, expectativas y posibilidades de los clientes potenciales, los proveedores y socios estratégicos, los empresarios y los expertos en sostenibilidad. Además, queremos identificar las oportunidades de mejora en la oferta de la plataforma y su modelo de negocio, así como los recursos y herramientas más efectivos para atraer y fidelizar a los clientes potenciales. La información recopilada nos permitirá ajustar y fortalecer nuestra propuesta de valor y nuestra estrategia comercial, maximizando el impacto y la sostenibilidad de la plataforma.
Mensaje (es un mensaje de introducción para romper el hielo):	Hola, somos GAMSECURE SAS. Estamos trabajando en el desarrollo de una plataforma de capacitación en ciberseguridad para PYME y nos interesa conocer su opinión y necesidades como empresario. Con esta entrevista, buscamos entender mejor su perspectiva sobre la ciberseguridad en las PYME, los desafíos y oportunidades que enfrentan en este tema, y cómo podemos mejorar nuestra propuesta de valor y nuestra estrategia comercial para satisfacer sus necesidades.

Preguntas para realizar:

1. ¿Cómo ve la necesidad de capacitar a las PYME en ciberseguridad? ¿Cree que hay una demanda real de este tipo de formación en el mercado actual?
2. ¿Cuáles son algunas de las preocupaciones o desafíos que enfrenta actualmente su empresa en términos de ciberseguridad? ¿Cómo podría nuestra plataforma ayudar a abordar estos desafíos?
3. ¿Cómo podríamos trabajar juntos para asegurarnos de que nuestra plataforma sea accesible y útil para su empresa? ¿Cómo podríamos adaptar nuestra formación a sus necesidades específicas?
4. ¿Qué tipo de costos podríamos esperar en términos de utilizar nuestra plataforma para capacitar a su personal en ciberseguridad? ¿Cómo podríamos trabajar juntos para asegurarnos de que estos costos sean razonables y sostenibles a largo plazo?
5. ¿Cómo podría nuestra plataforma ayudar a su empresa a aumentar su capacidad para prevenir y responder a los ataques de ciberseguridad? ¿Cómo podría esto afectar positivamente su negocio a largo plazo?
6. ¿Cómo ve la oportunidad de generar ingresos adicionales a través de la venta de nuestros cursos de formación en ciberseguridad? ¿Cree que esto podría ser una fuente de ingresos viable para su empresa?
7. ¿Cómo podríamos trabajar juntos para asegurarnos de que nuestra relación comercial sea mutuamente beneficiosa y sostenible a largo plazo? ¿Qué medidas de seguimiento o monitoreo podríamos poner en marcha para evaluar nuestro progreso juntos?

Tabla 17.

Ficha técnica y formato entrevista Experto sostenibilidad

Realizada por	Eumir Pulido de la Pava
Nombre de la encuesta	Encuesta de Evaluación de Ciberseguridad desde la Perspectiva de la Sostenibilidad

Universo	Profesionales y expertos en sostenibilidad y ciberseguridad, con conocimientos específicos en la intersección de ambos campos.
Tipo de muestreo	Muestreo no probabilístico o de juicio. Se seleccionan expertos en sostenibilidad y ciberseguridad en base a su experiencia y conocimientos en ambos ámbitos.
Técnica de recolección de datos	Entrevista semiestructurada. Permite explorar en profundidad las percepciones y conocimientos del experto en sostenibilidad sobre la ciberseguridad.
Fecha de creación	2 de junio de 2023
Objetivo de la encuesta	Validar el concepto del negocios, potencial y visión emprendedora y modelo de ingreso.
N.º de preguntas formuladas	7
N.º de encuestadores	1
Tipo de preguntas aplicadas	Preguntas abiertas

Formato Entrevista Experto en Sostenibilidad

Grupo de interés:	Experto en Sostenibilidad
Objetivo de la entrevista:	Validar el concepto del negocios, potencial y visión emprendedora y modelo de ingreso.
Hipótesis o dudas para validar (del modelo de negocios):	Entender las necesidades, desafíos, expectativas y posibilidades de los clientes potenciales, los proveedores y socios estratégicos, los empresarios y los expertos en sostenibilidad. Además, queremos identificar las oportunidades de mejora en la oferta de la plataforma y su modelo de negocio, así como los recursos y herramientas más efectivos para atraer y fidelizar a los clientes potenciales. La información recopilada nos permitirá ajustar y fortalecer nuestra propuesta de valor y nuestra estrategia comercial, maximizando el impacto y la sostenibilidad de la plataforma.

Mensaje (es un mensaje de introducción para romper el hielo):	Hola, somos GAMSECURE SAS. Estamos trabajando en el desarrollo de una plataforma de capacitación en ciberseguridad para PYME y nos interesa conocer su opinión y necesidades como experto en sostenibilidad. Con esta entrevista, buscamos entender mejor su perspectiva sobre la ciberseguridad en las PYME, los desafíos y oportunidades que enfrentan en este tema, y cómo podemos mejorar nuestra propuesta de valor y nuestra estrategia comercial para satisfacer sus necesidades.

Preguntas para realizar:

1. ¿Cómo podría nuestra plataforma contribuir a una sociedad más sostenible y resiliente desde la perspectiva de la ciberseguridad?
2. ¿Cuáles son algunas de las mejores prácticas actuales en términos de sostenibilidad en la industria de la ciberseguridad? ¿Cómo podríamos integrar estas prácticas en nuestra plataforma?
3. ¿Cómo podríamos medir y reportar el impacto ambiental y social de nuestra plataforma y cursos de formación en ciberseguridad? ¿Qué medidas podríamos tomar para minimizar nuestro impacto ambiental y maximizar nuestro impacto social?
4. ¿Cómo podríamos involucrar a las partes interesadas y comunidades locales en nuestra estrategia de sostenibilidad y en el diseño y desarrollo de nuestra plataforma?
5. ¿Qué tipo de sinergias podría haber entre nuestra plataforma y otras iniciativas de sostenibilidad existentes en el sector de la ciberseguridad? ¿Cómo podríamos colaborar con estas iniciativas para maximizar nuestro impacto y reducir los costos y el riesgo?
6. ¿Cómo podríamos asegurarnos de que nuestra plataforma cumpla con las normas y regulaciones ambientales y sociales relevantes y sea un ejemplo de liderazgo en el sector de la ciberseguridad?
7. ¿Cómo podríamos trabajar juntos para desarrollar y mantener una estrategia de sostenibilidad sólida y creíble para nuestra plataforma y cursos de

formación en ciberseguridad? ¿Cómo podríamos asegurarnos de que esta estrategia esté integrada en nuestra cultura y operaciones diarias?

Tabla 18.

Ficha técnica y formato entrevista Clientes Potenciales

Realizada por	Eumir Pulido de la Pava
Nombre de la encuesta	Encuesta de Evaluación de Necesidades de Ciberseguridad para Clientes Potenciales
Universo	Empresas y organizaciones que podrían convertirse en clientes potenciales de servicios de ciberseguridad, especialmente aquellas que muestran interés en mejorar su seguridad digital.
Tipo de muestreo	Muestreo no probabilístico o de juicio. Se seleccionan clientes potenciales en base a su interés y relevancia en el ámbito de la ciberseguridad.
Técnica de recolección de datos	Entrevista semiestructurada. Permite recopilar información detallada sobre las necesidades y percepciones de los clientes potenciales en relación con la ciberseguridad.
Fecha de creación	2 de junio de 2023
Objetivo de la encuesta	Validar el concepto del negocios, potencial y visión emprendedora y modelo de ingreso.
N.º de preguntas formuladas	15
N.º de encuestadores	1
Tipo de preguntas aplicadas	Preguntas abiertas

Formato Entrevista Clientes Potenciales

Grupo de interés:	Clientes Potenciales
Objetivo de la entrevista:	Validar el concepto del negocios, potencial y visión emprendedora y modelo de ingreso
Hipótesis o dudas para validar (del modelo de negocios):	Entender las necesidades, desafíos, expectativas y posibilidades de los clientes potenciales, los proveedores y socios estratégicos, los empresarios y los expertos en sostenibilidad. Además, queremos identificar las oportunidades de mejora en la oferta de la plataforma y su modelo de negocio, así como los recursos y herramientas más efectivos para atraer y fidelizar a los clientes potenciales. La información recopilada nos permitirá ajustar y fortalecer nuestra propuesta de valor y nuestra estrategia comercial, maximizando el impacto y la sostenibilidad de la plataforma.
Mensaje (es un mensaje de introducción para romper el hielo):	Hola, somos GAMSECURE SAS. Estamos trabajando en el desarrollo de una plataforma de capacitación en ciberseguridad para PYME y nos interesa conocer su opinión y necesidades como cliente potencial. Con esta entrevista, buscamos entender mejor su perspectiva sobre la ciberseguridad en las PYME, los desafíos y oportunidades que enfrentan en este tema, y cómo podemos mejorar nuestra propuesta de valor y nuestra estrategia comercial para satisfacer sus necesidades.

Preguntas para realizar:

1. ¿Cuáles son las principales preocupaciones que tienes con respecto a la ciberseguridad en tu empresa? ¿Qué te gustaría aprender o mejorar en este ámbito?
2. ¿Cómo evalúas actualmente el nivel de ciberseguridad de tu empresa? ¿Qué herramientas o soluciones utilizas actualmente para mejorar la seguridad?
3. ¿Cuáles son los principales desafíos que has enfrentado al intentar mejorar la ciberseguridad en tu empresa? ¿Cómo te gustaría abordar estos desafíos en el futuro?
4. ¿Qué tipo de cursos o recursos de formación en ciberseguridad te resultarían más útiles para ti y tu equipo? ¿Qué aspectos te gustaría que se cubrieran en estos cursos?
5. ¿Cómo valorarías la propuesta de valor de nuestra plataforma de formación en ciberseguridad? ¿Crees que esta plataforma sería útil para ti y tu empresa?
6. ¿Qué tipo de modelo de precios te resultaría más atractivo para acceder a nuestros cursos y recursos de formación en ciberseguridad? ¿Qué aspectos te gustaría que se incluyeran en este modelo de precios?
7. ¿Hay algún otro aspecto que consideres importante para ti al momento de elegir una plataforma de formación en ciberseguridad?
8. ¿Cuál es el tamaño de tu empresa y cuántos empleados tienen acceso a la información crítica de la empresa?
9. ¿Cuáles son los principales riesgos de seguridad que ha enfrentado tu empresa en el pasado? ¿Qué medidas se tomaron para evitar que vuelvan a ocurrir?
10. ¿Estás familiarizado con los estándares de seguridad existentes en el mercado (por ejemplo, ISO 27001)? ¿Tu empresa tiene algún tipo de certificación en seguridad de la información?
11. ¿Tienes algún tipo de plan de contingencia en caso de un ataque cibernético o pérdida de datos? ¿Cuánto tiempo tardaría tu empresa en recuperarse de un incidente de este tipo?

12. ¿Cómo evalúas la importancia de la seguridad de la información en relación con otras prioridades empresariales (por ejemplo, la innovación, la eficiencia, la rentabilidad, etc.)?
13. ¿Tienes algún tipo de política de formación en ciberseguridad para tus empleados? ¿Cómo te aseguras de que tus empleados estén al día en cuanto a las amenazas y riesgos de seguridad?
14. ¿Has utilizado alguna plataforma de formación en ciberseguridad en el pasado? ¿Qué te gustó y qué no te gustó de esa experiencia?
15. ¿Cómo te aseguras de que los proveedores y terceros que trabajan con tu empresa cumplan con los estándares de seguridad necesarios?

F. Anexo 6. Validación Entrevistas

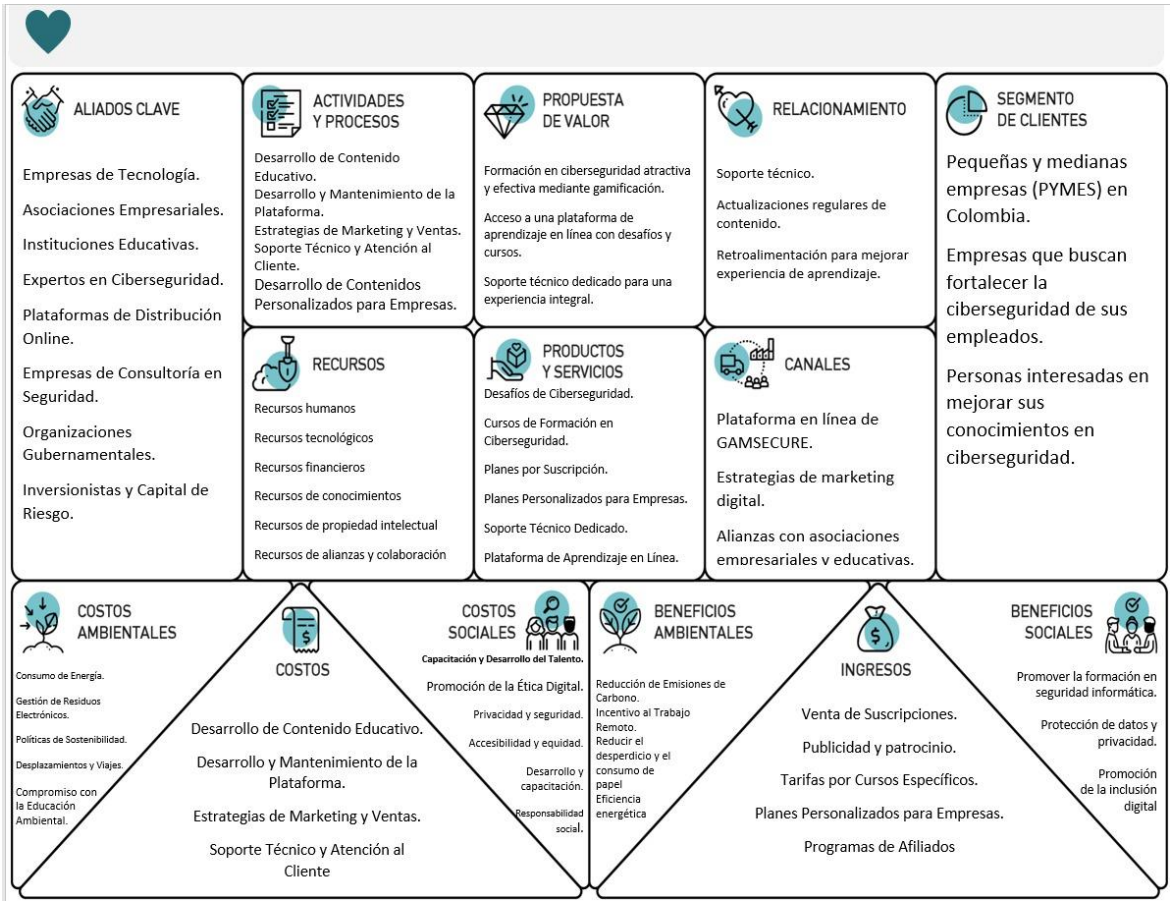
A continuación, se podrán encontrar los links (enlaces) de los videos, grabaciones y medio audiovisual como evidencia de las entrevistas realizadas. Se utilizó la plataforma Google Meet (cuenta de pago) para las entrevistas pues la herramienta permite la grabación.

Tipo de Entrevista	Nombre Entrevistado	Empresa - Cargo	Enlace
Aliados Estratégicos	Víctor Aguirre	Instructor Ingeniero de Sistemas	https://youtu.be/x4FVv5QRnqc
	Luis Fernando Tamayo Bustamante	Asesor MinTIC Ingeniero de Sistemas	https://youtu.be/SZmHklWd-aU
Clientes Potenciales	César Augusto Castaño Obando	COOMPER Director IT	https://youtu.be/81OCKVdPr0U
	Jorge Eduardo Pérez Velásquez	Compañía de Seguros POSITIVA Gerente	https://youtu.be/kBekzhMxRjQ
Empresarios - Emprendedores	Santiago Londoño	Dotación Integral Director Comercial	https://youtu.be/g5LuPHkpy8U
Empresarios - Emprendedores	Rodolfo Vega	No Rules Sport Gerente	https://youtu.be/qu5re1KsW_I
Experto Técnico	Sandra Milena Villa Motato	Asesora Ingeniera de Sistemas	https://youtu.be/wAOS0y3oK7k
Experto Sostenibilidad	María Cristina Rodríguez Villera	Docente – Investigadora Universidad EAN	https://youtu.be/4VQr0Bx8H2o

G. Anexo 7. Lienzo de Modelo de Negocio Sostenible

Figura 27.

Lienzo de Modelo de Negocio Sostenible



Fuente: Nota: Elaboración propia.