

Modelo de Negocio empresa de seguridad electrónica en Santander (Colombia)

Andrés Felipe Giraldo Otero

Trabajo de Grado para Optar el Título de Magister en Gerencia de Negocios

Director

Edna Rocío Bravo

Doctora en administración de empresas

Universidad Industrial de Santander

Facultad de Ingeniería Físico Mecánicas

Escuela de Estudios Industriales y Empresariales

Maestría en Gerencia de Negocios

Bucaramanga

2026

Dedicatoria

A mi familia, el motor y la razón de este esfuerzo.

A mi amada esposa, por su incondicional amor, y el apoyo constante que me brindó durante todo el proceso. Tu creencia en mí, mi mayor impulso para alcanzar esta meta.

A mi querido hijo, eres mi inspiración diaria y el recordatorio más hermoso del futuro que construimos. Espero que este esfuerzo sea un ejemplo de perseverancia y dedicación para que sigas tus sueños con el mismo rigor y pasión.

Ustedes son el verdadero sentido de este MBA.

Agradecimientos

Mi gratitud se extiende a todos los profesores del MBA, cuya excelencia académica y experiencia profesional enriquecieron profundamente mi formación. En particular, agradezco la orientación, el rigor y la pasión transmitida en cada asignatura, elementos fundamentales que hoy me permiten abordar los desafíos empresariales con una visión estratégica.

Un reconocimiento especial a mi directora de trabajo de grado, por su valioso acompañamiento, paciencia y profesionalismo. Su guía experta y sus constructivas observaciones fueron esenciales para poder completar este trabajo de grado. Le agradezco profundamente el tiempo y la dedicación invertida.

Finalmente, agradezco a mis compañeros y amigos del MBA. Compartir este viaje con ustedes fue una experiencia inigualable. Gracias por el compañerismo y el apoyo mutuo. El networking creado es un valor invaluable que atesoraré.

Tabla de Contenido

	Pág.
Generalidades del trabajo de aplicación	13
Introducción	15
1. Objetivos	18
1.1 Objetivo General	18
1.2 Objetivos Específicos.....	18
2. Marco referencial	19
2.1 Antecedentes	19
2.2 Componentes sistema de Automatización Residencial.....	20
3. Marco Teórico.....	24
3.1 Estrategia competitiva según Michael Porter.....	25
3.2 Modelo canvas de Osterwalder	26
3.3 Producto mínimo viable de Bill Aulet	27
3.4 Tensores clave de estrategia organizacional	28
4. Desarrollo del proyecto.....	31
4.1 Vigilancia Tecnológica	31
4.1.1 Patente US_10885734_B2.	33
4.1.2 Patente US_10798244_B2.	36
4.1.3 Empresas que ofrecen el servicio.	38
4.1.4 Selección de empresas destacadas.	41
4.1.5 Patrones de competitividad de Carson Living.	45
4.1.5.1 Propuesta de valor.	47

4.1.5.2 Cadena de Abastecimiento.....	49
5. Modelo de negocio.....	50
5.1 Cliente Objetivo	51
5.2 Como el producto satisface esa necesidad específica.	56
5.3 Diseño del Producto	59
5.4 Estructuración de los canales de Venta y distribución.....	66
5.5 Estrategia para capturar valor a través de la venta	72
5.6 Modelo de Escalabilidad a Futuro	81
6. Conclusiones.....	85
Referencias bibliográficas.....	88

Lista de Tablas

Pág.

Tabla 1. Formato Canvas para la empresa de automatización en seguridad residencial. . 80

Lista de Figuras

	Pág.
Figura 1. Componentes principales de sistemas de seguridad electrónica residencial	23
Figura 2. Diseño del producto de automatización residencial.	72
Figura 3. Formato gráfico Canvas de la empresa de automatización en seguridad residencial	81

Glosario

Acuerdos de Nivel de Servicio (SLA): es un contrato formal y vinculante entre un proveedor de servicios y un cliente. Define el nivel de calidad, la disponibilidad y las expectativas de rendimiento acordadas, incluyendo métricas clave (KPIs) y consecuencias por incumplimiento, asegurando la transparencia y la calidad del servicio.

API (Application Programming Interface): interfaz de programación que permite la comunicación e integración entre diferentes sistemas o aplicaciones de software mediante protocolos y estructuras de datos estandarizadas.

Arquitectura abierta: enfoque de diseño de sistemas tecnológicos que permite la integración con múltiples dispositivos o plataformas mediante estándares interoperables.

Automatización residencial: conjunto de tecnologías que permiten controlar y gestionar de forma automática o remota los sistemas y servicios de un edificio o vivienda, tales como Seguridad y accesos.

Cadena de abastecimiento tecnológica: conjunto de actores, procesos y relaciones estratégicas involucradas en el suministro, integración y soporte de soluciones tecnológicas que respaldan el modelo de negocio.

Capacidades distintivas: conjunto de habilidades organizacionales y recursos estratégicos que permiten a una empresa diferenciarse de sus competidores y generar ventajas competitivas sostenibles.

Central de monitoreo: instalación desde la cual se supervisan, gestionan y responden los eventos generados por sistemas de seguridad electrónica mediante operadores especializados.

Control de accesos: sistema tecnológico que regula y registra el ingreso y salida de personas o vehículos a un espacio determinado mediante mecanismos de autenticación.

Dashboard: interfaz visual que presenta indicadores de desempeño y datos relevantes de manera gráfica para facilitar el monitoreo y la toma de decisiones.

Ecosistema digital: conjunto interconectado de plataformas, aplicaciones, dispositivos y servicios que operan de manera integrada para generar valor a los usuarios.

Enrolamiento: proceso de registrar o inscribir a una persona en un sistema o programa específico. Este registro suele implicar la recopilación de información personal y biométrica, como huellas dactilares, fotografías y datos personales, para crear un registro único e identificable de la persona.

Indicadores de desempeño (KPIs): métricas cuantificables utilizadas para evaluar la eficiencia, efectividad y cumplimiento de objetivos dentro de una organización o sistema.

Integración tecnológica: proceso mediante el cual diferentes sistemas, dispositivos o plataformas se conectan para operar de manera coordinada dentro de una misma solución.

Inteligencia artificial (IA): conjunto de técnicas computacionales que permiten a los sistemas analizar datos, reconocer patrones y generar predicciones o recomendaciones para apoyar la toma de decisiones.

Modelo CANVAS: herramienta estratégica utilizada para describir y analizar modelos de negocio mediante nueve bloques fundamentales que representan sus componentes clave.

Modelo de negocio: representación conceptual que describe la forma en que una organización crea, entrega y captura valor.

Plataforma central: sistema digital que integra y administra la información generada por los diferentes dispositivos y servicios del edificio.

Portería remota: modelo operativo en el cual la supervisión de accesos y eventos del edificio se realiza desde una central de monitoreo externa mediante tecnologías de comunicación y seguridad electrónica.

Producto Mínimo Viable (PMV): versión inicial de un producto que incluye únicamente las funcionalidades esenciales necesarias para validar una propuesta de valor con clientes reales.

Propiedad horizontal: régimen jurídico que regula la coexistencia de bienes privados y bienes comunes dentro de un mismo inmueble o conjunto residencial.

Propuesta de valor: conjunto de beneficios que una organización ofrece a sus clientes para resolver un problema o satisfacer una necesidad específica.

Seguridad electrónica: conjunto de sistemas tecnológicos destinados a la prevención, detección y gestión de riesgos mediante dispositivos electrónicos como alarmas, cámaras y sensores.

Tensor estratégico: dimensión estructural dentro del diseño de la estrategia organizacional que orienta la alineación entre recursos, capacidades y objetivos de la empresa.

Resumen

Título: Modelo de Negocio empresa de seguridad electrónica en Santander (Colombia)*

Autor: Andrés Felipe Giraldo Otero**

Palabras Clave: Modelo de negocio, automatización residencial, portería remota, conserjería remota, seguridad electrónica

Descripción: Este trabajo de aplicación presenta los pasos que se siguieron para desarrollar un modelo de negocio para una empresa de seguridad electrónica en el departamento de Santander, Colombia, más específicamente en una empresa que comercializa servicios de Automatización Residencial. La Automatización Residencial es un servicio que permite asegurar un edificio a través de la instalación de dispositivos de seguridad electrónica, pudiendo disminuir las horas de los servicios de vigilancia física y por ende disminuir los costos de seguridad. La propuesta surge como respuesta a la necesidad de optimizar los esquemas tradicionales de seguridad, caracterizados por una alta dependencia de vigilancia física y elevados costos operativos para las copropiedades. Como insumo para la construcción de este modelo de negocio se siguió un plan de trabajo que contempla la vigilancia tecnológica, en donde se establecieron patentes de tecnología relacionadas con el negocio y tendencias innovadoras de Automatización Residencial con base en patrones de competitividad. Finalmente, y teniendo en cuenta lo anterior, se desarrolló el modelo de negocio mediante la definición del cliente objetivo, la identificación de cómo el producto satisface sus necesidades, el diseño del producto, la estructuración de los canales de venta y distribución, la determinación de la estrategia para capturar valor a través de la venta y la formulación de un plan de escalabilidad a futuro.

Como resultado, se formuló una propuesta de negocio que trasciende la prestación tradicional de servicios de seguridad, integrando sistemas de alarma, control de acceso, videoporteros y una plataforma tecnológica central capaz de consolidar la información operativa del edificio transformando la información generada por los sistemas electrónicos en herramientas de gestión para la administración.

* Trabajo de Grado

** Facultad de Ingeniería Físico mecánicas. Escuela de estudios industriales y empresariales. Director: Edna Rocío Bravo. Doctora en administración de empresas.

Abstract

Title: Business Model of an electronic security company in Santander (Colombia)*

Author: Andrés Felipe Giraldo Otero**

Key Words: Business model, home automation, remote concierge, electronic security

Description: This applied research project presents the steps followed to develop a business model for an electronic security company in the department of Santander, Colombia, specifically for a company that markets residential automation services. Residential automation is a service that allows for the security of a building through the installation of electronic security devices, potentially reducing the hours of physical security personnel and, consequently, lowering security costs. The proposal arises as a response to the need to optimize traditional security systems, characterized by a high dependence on physical security and high operating costs for co-owned properties. As input for the construction of this business model, a work plan was followed that included technological monitoring, identifying technology patents related to the business and innovative trends in residential automation based on competitiveness patterns. Finally, taking the above into account, the business model was developed by defining the target customer, identifying how the product meets their needs, designing the product, structuring the sales and distribution channels, determining the strategy for capturing value through sales, and formulating a future scalability plan.

As a result, a business proposal was formulated that transcends the traditional provision of security services, integrating alarm systems, access control, video intercoms, and a central technological platform capable of consolidating the building's operational information, transforming the data generated by electronic systems into management tools for administration.

* Master Business Administration

** Faculty of Physical-Mechanical Engineering. School of Industrial and Business Studies. Director: Edna Rocío Bravo. Doctor of Business Administration

Generalidades del Trabajo de Aplicación

El presente trabajo de aplicación está basado en un modelo de negocio, el cual se define como una aplicación que atiende necesidades del mercado para crear valor y generar ingresos. El modelo de negocio debe establecer de forma clara como una empresa genera valor para el cliente y beneficios para sí misma. Pero antes de la construcción del modelo, es necesario identificar qué problema, necesidad u oportunidad existe en el mercado y definir claramente que segmento del mercado experimenta esa necesidad. Esta segmentación del mercado implica identificar grupos de clientes homogéneos en cuanto a necesidades, características y comportamientos. El cliente objetivo debe tener características demográficas, geográficas, psicográficas y conductuales comunes que reflejen una misma necesidad o problema que el producto puede resolver.

Una vez definido el mercado, se debe profundizar en la necesidad concreta y en como la propuesta resolverá el problema específico del cliente. Para esto es importante definir con precisión el perfil del cliente, identificando sus motivaciones, prioridades, necesidades y expectativas. El poder identificar ese estado deseado del cliente al estar su necesidad perfectamente satisfecha, permite diseñar el producto o servicio con una oferta atractiva y diferenciada. Lo anterior permite describir el estado actual del cliente y el estado futuro, beneficiando así la comunicación de valor, la toma de decisiones y la validación de la propuesta de negocio y del producto o servicio.

El trabajo de aplicación se centra en un producto de seguridad con base en tecnología electrónica. Esta orientación es una extensión natural de mi formación en ingeniería electrónica y mi experiencia consolidada en el sector de la seguridad. La madurez y versatilidad de la tecnología de dispositivos electrónicos permite hoy soluciones innovadoras a las necesidades de seguridad de

los usuarios. En consecuencia, un modelo de negocio bien estructurado alrededor de estos dispositivos no solo es viable, sino que constituye una inmensa oportunidad para generar, ofrecer y capturar un alto valor en el mercado.

Una vez definido el producto, se debe construir el modelo de generación de ingresos teniendo en cuenta en cómo la empresa entrega y captura valor. Principalmente se deben establecer las actividades y recursos clave que soportarán el funcionamiento del negocio, como el producto llegará al cliente y cuál será el modelo de ingresos adecuado. Esquematizar el cómo un cliente adquiere el producto, es un proceso esencial para diseñar el cómo se entrega el producto, y este proceso implica identificar quien es la persona que toma la decisión de adquirirlo, así como la persona que influye en esa decisión. La relación con el cliente es esencial por lo que se debe asegurar un flujo que construya confianza y reduzca fricciones en la compra, asegurando un proceso eficiente y atractivo que facilite la decisión de compra y maximice el ingreso para la empresa, lo que permite capturar valor a través de la venta. La vigilancia tecnológica permite tener un panorama global de empresas que ya están ofreciendo productos similares, para así determinar cuáles son las fortalezas de estas empresas y construir desde ahí ventajas competitivas.

Finalmente, el modelo de negocio debe establecer un plan de escalabilidad a futuro, cuya finalidad es crecer eficientemente, manteniendo o aumentando la rentabilidad. Para esto se deben diseñar estrategias claras de crecimiento que pueden incluir cobertura geográfica, mayor número de clientes e incremento del portafolio. Este trabajo de aplicación contempla el poder definir una estrategia de crecimiento basados en la tecnología y operatividad.

Introducción

Existe la oportunidad de crear una nueva compañía que comercialice productos y proyectos de seguridad electrónica en el departamento de Santander, Colombia. Lo anterior teniendo en cuenta un mercado en crecimiento que requiere de tecnología para poder fortalecer su seguridad. Este trabajo de aplicación está orientado en poder construir un modelo de negocio para esta nueva empresa, teniendo en cuenta el servicio que se va a comercializar se denomina automatización en seguridad residencial. Tradicionalmente, el modelo predominante ha estado basado en esquemas de vigilancia física, caracterizados por una alta dependencia de personal, costos recurrentes elevados y limitaciones en términos de cobertura, trazabilidad y eficiencia operativa. Paralelamente, el avance de las tecnologías digitales, la automatización y la conectividad han generado nuevas alternativas basadas en seguridad electrónica y vigilancia remota, las cuales prometen mejorar la eficiencia y reducir costos, aunque su adopción en el contexto regional aún es incipiente. En este contexto, se identifica una brecha significativa entre el modelo tradicional de vigilancia física y las soluciones tecnológicas disponibles. Dicha brecha no solo es tecnológica, sino también estratégica y de modelo de negocio, ya que las copropiedades y organizaciones enfrentan dificultades para evaluar, adoptar e integrar soluciones de automatización que realmente generen valor sostenible. Esta desconexión limita la modernización del sector y mantiene estructuras de costos ineficientes. Frente a esta problemática, surge la necesidad de formular una decisión estratégica orientada a evaluar la viabilidad de un modelo de negocio basado en soluciones de automatización residencial, que permita cerrar la brecha identificada y generar valor tanto económico como operativo para los usuarios. El presente trabajo se enfoca en el diseño y estructuración de un modelo de negocio que responda a estas necesidades, alineando capacidades

tecnológicas con una propuesta de valor diferenciada. En este sentido, la investigación se orienta a responder la siguiente pregunta: Es viable, desde una perspectiva estratégica y de creación de valor, el desarrollo de un modelo de negocio basado en soluciones de automatización residencial en el departamento de Santander?

La automatización de seguridad residencial es un producto o servicio que se basa en poder asegurar edificios residenciales con equipos electrónicos que incluyen control de acceso, cámaras y sistemas de alarma. El sistema es supervisado a través de un operador en una central de monitoreo, lo que permite poder disminuir las horas de vigilancia física dentro del edificio, y por ende disminuir el costo del valor de administración en lo que respecta a seguridad. En los últimos años el valor de la seguridad física ha venido incrementando, por lo que el potencial de demanda para este servicio se basa en la tendencia de reducción de costos, incremento en la conciencia de seguridad, la disponibilidad de infraestructura tecnológica, el crecimiento urbano y una creciente cultura tecnológica.

Inicialmente y para poder establecer el modelo de negocio, se utilizó la vigilancia tecnológica, herramienta clave para la toma de decisiones estratégicas, ya que esto permite tener información relevante y actualizada del entorno tecnológico y competitivo del sector de la seguridad electrónica y la automatización residencial. Adicional, la herramienta permite anticiparse a las necesidades futuras del mercado y diseñar productos y servicios diferenciados.

Teniendo como base la información recolectada a través de la vigilancia tecnológica, se seleccionaron diez empresas que actualmente ofrecen el servicio pudiendo definir el modelo de negocio de manera general con base en el modelo CANVAS. De allí se filtraron tres empresas, destacadas por su servicio diferenciado e innovador, lo que llevó a vislumbrar patrones de

competitividad que permiten establecer estrategias claras para empezar a construir un nuevo modelo de negocio para la nueva empresa.

El alcance de este trabajo se enmarca en un enfoque de estructuración estratégica y conceptual, bajo la lógica de desarrollo de un Producto Mínimo Viable (PMV), conforme a la metodología propuesta por Bill Aulet. En consecuencia, el trabajo prioriza la validación de la lógica de creación de valor, la coherencia estratégica del modelo y la identificación de sus componentes clave, por encima de una profundización financiera exhaustiva. Este enfoque permite sentar las bases para futuras etapas de validación de mercado, análisis financiero detallado y escalabilidad del modelo.

El nuevo modelo de negocio se construye con las bases de lo extraído a través de la herramienta de vigilancia tecnológica y definiendo como la empresa generará valor sostenible y escalable, definiendo el cliente, el producto, los canales de venta y distribución y los modelos de suscripción o venta del sistema.

1. Objetivos

Inicialmente el objetivo general propuesto fue el “Formular modelo de negocio para la creación de una empresa que comercialice productos de seguridad electrónica”. Con base en las reuniones con la directora y las mismas recomendaciones de los calificadores, el objetivo general y los objetivos específicos cambiaron y evolucionaron. El nuevo conjunto de objetivos responde a una maduración del planteamiento inicial, pasando de un enfoque amplio y operativo a uno más específico, segmentado y metodológicamente robusto, lo cual aumenta la calidad del proyecto, su pertinencia en el mercado actual y su posibilidad de implementación exitosa.

1.1 Objetivo General

Formular modelo de negocio para la creación de una empresa de seguridad electrónica que comercialice proyectos de Automatización Residencial.

1.2 Objetivos Específicos

1. Desarrollar un ejercicio de vigilancia tecnológica para identificar tendencias competitivas en el mercado de Automatización Residencial.
2. Desarrollo de los modelos de negocio de tres organizaciones en el negocio de Automatización Residencial con el propósito de identificar patrones de competitividad.
3. Construir el modelo de negocio mediante la definición del cliente objetivo, la identificación de cómo el producto satisface sus necesidades, el diseño del producto, la estructuración de los canales de venta y distribución, la determinación de la estrategia para capturar valor a través de la venta y la formulación de un plan de escalabilidad a futuro.

2. Marco Referencial

2.1 Antecedentes

Las tarifas de seguridad privada han experimentado incrementos acumulados superiores al 25% entre 2023 y 2024, con previsión de incrementos adicionales durante 2025 y 2026. Estos incrementos son resultado de factores como la reforma laboral, el alza del salario mínimo y la reducción de la jornada laboral, lo que ha elevado el costo de la mano de obra, influyendo directamente sobre la estructura de precios del sector. La propia Superintendencia de Vigilancia y Seguridad Privada (Supervigilancia) ha alertado sobre el impacto de la reforma laboral en Colombia, que desde julio de 2025 ha incrementado el salario de los vigilantes, elevando aún más el costo del servicio en todo el país. El costo mensual mínimo de un servicio de vigilancia física 24 horas en Colombia ha pasado de \$11 millones COP en 2023 a más de \$15 millones COP en el segundo semestre de 2025, evidenciando un fuerte incremento. La principal normativa que explica el alza es la Ley 2101 de 2021, que reduce gradualmente la jornada laboral, desde julio de 2025 la jornada baja a 44 horas semanales y a partir de julio 2026 será de 42 horas. Esta reforma implica que para cubrir turnos completos, las empresas de seguridad privada necesitan contratar más personal o aumentar recargos y suplencias, elevando así los costos. Además, la reforma laboral 2466 de 2025 ha intensificado este ajuste, aumentando salarios, formalización y recargos nocturnos y dominicales para proteger los derechos de los trabajadores. La presión sobre el presupuesto está impulsando a administradores y residentes a optar por soluciones automatizadas y remotas. La automatización permite a los conjuntos residenciales y edificios reducir significativamente el gasto mensual en seguridad, al disminuir o eliminar la necesidad de vigilantes presenciales. El costo de la automatización requiere una inversión inicial (equipos e instalación) y mantenimientos periódicos, pero el gasto recurrente mensual suele ser significativamente menor

cuando se compara con el servicio de vigilancia física. Típicamente, el retorno total de la inversión llega en un plazo de 1 a 3 años, dependiendo del grado de automatización. La automatización implica una inversión inicial considerable, pero los ahorros sostenibles en costos laborales y operativos suelen superar la inversión en el corto y mediano plazo. La modernización y la presión del mercado han llevado a que la automatización sea vista como estándar deseado en la administración de propiedades, incentivando a otras copropiedades a adoptar la misma tendencia para no quedarse rezagadas.

2.2 Componentes sistema de Automatización Residencial

El servicio de Automatización Residencial se basa en la instalación de tres tipos de sistemas de seguridad electrónica. El primer sistema hace referencia al control de acceso. Este sistema es el encargado de controlar el acceso de los residentes, visitantes, mensajeros, personal de servicio y domiciliarios al edificio. Normalmente el sistema de control de acceso se compone de un equipo electrónico que se instala en la entrada principal del edificio, el cual puede abarcar el ingreso peatonal y vehicular. El dispositivo de control de acceso puede incorporar varios componentes, como teclado, micrófono, altavoz y cámara al cual se le denomina video portero por su capacidad de transmitir video a través de la cámara que tiene instalada. El dispositivo se comunica mediante diferentes tipos de redes, incluyendo redes de área local, redes celulares, ethernet, wifi o internet. El acceso de las personas puede otorgarse mediante credenciales de identificación, como códigos numéricos o datos biométricos como por ejemplo rostro o huella dactilar. El proceso de registro y captura de información de los usuarios se denomina enrolamiento, y para los residentes se hace necesario que realicen este proceso que permite su ingreso al edificio cuando se autentiquen frente al dispositivo o video portero. Para permitir el acceso a las personas que no residen en el edificio,

el sistema normalmente permite dos tipos de control. En la primera opción el visitante puede llamar al residente a través del video portero y este le permite el ingreso al edificio de manera remota, ya sea a través de una aplicación de su celular o a través de un dispositivo tipo Tablet instalado en su apartamento. Una segunda opción contempla un servicio más completo en donde el visitante llama a través del video portero a una central de monitoreo, para que el operador otorgue o niegue el acceso del visitante de acuerdo con una previa autorización que ha transmitido el residente o administrador del edificio.

El segundo sistema hace referencia al circuito cerrado de televisión o CCTV, el cual se compone de cámaras de seguridad y video grabadores. Las cámaras funcionan como sensores diseñados para recibir datos visuales. Estas cámaras pueden capturar una imagen o una señal de vídeo en directo. Se utilizan para monitorizar detalles del entorno o movimientos de personas. Los video grabadores permiten almacenar la información del video en diferentes discos duros que tienen en su interior y su grabación permite realizar análisis de lo ocurrido en un evento determinado. Adicional, estos video grabadores pueden conectarse a una red de internet y transmitir el video a centrales de monitoreo o aplicaciones celulares, lo que le permite a un operador o residente poder observar las áreas perimetrales, accesos y zonas sociales de un edificio residencial en tiempo real. En los últimos años las cámaras han venido optimizando su tecnología y ahora tienen la capacidad para detectar movimiento o intrusión a zonas determinadas a través de lo que se denomina analítica de video. La inteligencia artificial también ha optimizado el funcionamiento de las cámaras para poder diferenciar si estas intrusiones son realizadas por humanos o por animales. Esta nueva tecnología permite generar eventos de intrusión a la central de monitoreo en donde rápidamente el operador puede observar la cámara que ha detectado el

evento y poder reaccionar frente al mismo, pudiendo ofrecer un mejor servicio de seguridad al edificio residencial.

El tercer sistema es el que se denomina sistema de alarma. Este sistema se basa en la instalación de un panel de alarma, teclado y sensores en el edificio residencial. Los sensores incluyen dispositivos que permiten identificar movimiento en determinadas áreas, apertura de puertas o ventanas, sensores de rotura de vidrio, sensores de humo, sensores de gas, sensores de vibración o golpe, sensores de fugas de agua, sensores de temperatura y humedad. Estos sensores se conectan al panel de alarma y este se encarga de identificar la novedad y transmitir la información a través de internet o red celular a un software de monitoreo de alarmas. El teclado le permite al usuario a través de un código numérico armar o desarmar el sistema de alarma. Cuando el usuario arma el sistema y los sensores detectan una activación, el panel de alarma transmite el evento; pero cuando el sistema está desarmado, los eventos no se transmiten y el usuario puede trasladarse a través del edificio sin activar los sensores. Las señales de alarma son atendidas en una central por un operador a través del software de monitoreo. Si el caso lo amerita, el operador puede reaccionar frente al evento con apoyo de personal de reacción o con la policía nacional.

Teniendo lo anterior en cuenta, al instalar un servicio de Automatización Residencial que conste de los tres sistemas expuestos, se está brindando seguridad a un edificio a través de la supervisión y monitorización desde una central de monitoreo, pudiendo reducir o eliminar la vigilancia física. Para el modelo de Automatización Residencial, la central de monitoreo juega un papel fundamental en la seguridad del edificio. La central opera de manera ininterrumpida, con equipos de operadores altamente capacitados que supervisan constantemente el sistema de seguridad electrónico. Ante cualquier actividad sospechosa o situación de riesgo, los operadores

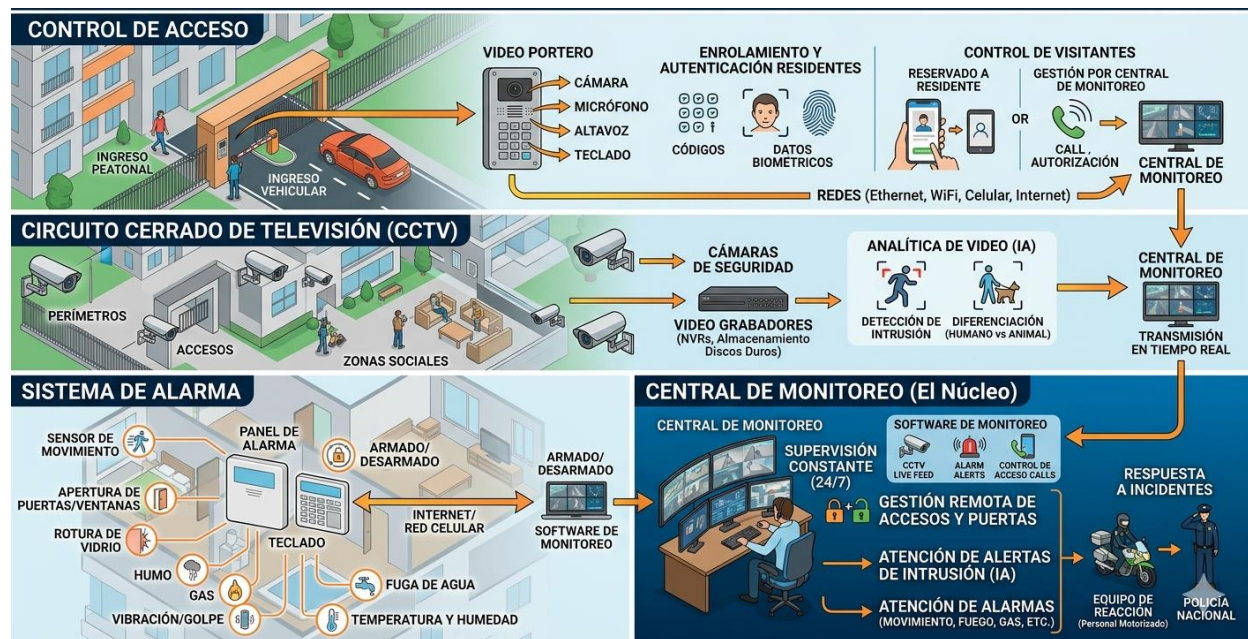
alertan al equipo de reacción, el cual puede estar compuesto por personal motorizado, para que analice la situación y tome medidas disuasivas o de seguridad.

La central de monitoreo también puede asumir funciones de control de acceso y gestión de visitantes para el edificio. Los operadores pueden de manera remota controlar y gestionar las aperturas y cierres de puertas peatonales y vehiculares, eliminando la necesidad de una portería física presencial y garantizando que no queden abiertas por descuido, incluso con sensores que alertan si una puerta queda abierta.

En la siguiente figura se puede observar los componentes principales que integran el sistema de seguridad electrónica enfocado al servicio de seguridad residencial.

Figura 1.

Componentes principales de sistemas de seguridad electrónica residencial



Nota: Generada mediante IA (Gemini)

3. Marco Teórico

La estrategia empresarial puede entenderse como el conjunto de decisiones y acciones que permiten a una organización definir cómo competirá, cómo creará valor y cómo sostendrá su desempeño en el tiempo. La estrategia no se limita a elegir un mercado o fijar metas financieras, también implica articular una propuesta de valor y un sistema operativo para traducirse en decisiones concretas sobre clientes, recursos y actividades.

En la literatura contemporánea, tres enfoques resultan especialmente útiles para construir esa visión integral. El primero es el de las estrategias competitivas genéricas de Michael Porter, que explica cómo una empresa puede alcanzar ventaja competitiva mediante liderazgo en costos, diferenciación o enfoque. El segundo es el Business Model Canvas de Alexander Osterwalder y Yves Pigneur, que ofrece una representación visual del negocio a través de nueve bloques interdependientes. El tercero es la perspectiva de Bill Aulet en *La Disciplina de emprender*, particularmente su desarrollo del Producto Mínimo Viable, como herramienta para validar que el cliente recibe valor y que además está dispuesto a pagar por la solución. A estos tres marcos se suman los tensores de estrategia, entendidos como factores transversales que condicionan la capacidad real de ejecución. Se proponen indicadores de capacidades distintivas, medición, talento, estructura, y asignación de poder factores críticos de éxito, que orientan recursos y prioridades hacia los elementos que más influyen en el logro estratégico. La tesis central es que Porter ayuda a decidir cómo competir, Osterwalder ayuda a visualizar cómo funciona el negocio, Aulet ayuda a validar qué debe probarse primero en el mercado, y los tensores estratégicos ayudan a asegurar qué condiciones organizacionales deben alinearse para que la estrategia se convierta en resultados sostenibles.

3.1 Estrategia competitiva según Michael Porter

Michael Porter plantea que la ventaja competitiva puede construirse a partir de dos tipos básicos de ventaja: costo o diferenciación, y de dos alcances competitivos: amplio o segmentado. Este marco resulta útil porque permite evitar estrategias ambiguas y obliga a que la organización defina con claridad la lógica central de su propuesta. Uno de los aportes más influyentes de Porter es la idea de que intentar perseguir simultáneamente liderazgo en costos y diferenciación sin una arquitectura organizacional coherente puede dejar a la empresa “atrapada en la mitad”. Ese estado implica costos relativamente altos sin una diferenciación suficiente, o promesas de valor sofisticadas que no se reflejan en disposición a pago.

El liderazgo en costos supone que la empresa organiza sus actividades para operar con el menor costo relativo de la industria. Esto puede apoyarse en estandarización, economías de escala, eficiencia operativa, automatización, compras favorables y control disciplinado de recursos. El trabajo de grado no propone un liderazgo puro en costos al estilo de un operador masivo de bajo precio, sin embargo, sí incorpora una dimensión costo-eficiente muy importante, la automatización en seguridad residencial se plantea como alternativa al aumento sostenido del costo de la vigilancia física. La diferenciación ocurre cuando la empresa ofrece atributos que el cliente percibe como únicos y valiosos, de forma que la comparación con alternativas rivales deja de basarse solo en precio. Esa singularidad puede provenir del diseño, la experiencia del usuario, la personalización, la marca, el servicio, la innovación o la integración de soluciones. La diferenciación es sostenible cuando el valor creado es relevante para el cliente y difícil de imitar por competidores. La estrategia para este modelo de negocio debe basarse en la diferenciación, ya que no tiene una propuesta robusta para mantener precios mínimos de mercado. El valor no debe verse solo como

la protección o seguridad del edificio, debe construirse un valor agregado que determine esa diferenciación.

La estrategia de enfoque se orienta a atender un segmento específico del mercado con mayor profundidad que los competidores generalistas. Esa focalización puede basarse en tipo de cliente, geografía, uso, necesidad o capacidad de pago. Su fortaleza es que permite adaptar la propuesta de valor y los procesos a necesidades concretas, reduciendo la dispersión estratégica. Porter entiende que el enfoque no es una estrategia menor, sino una elección deliberada de alcance competitivo. Al restringir su mercado objetivo, la empresa puede comprender mejor a su cliente, adaptar la oferta con mayor precisión y evitar enfrentamientos frontales con competidores generalistas. El trabajo de grado debe tener un enfoque definido y no verlo como un mercado general de seguridad para poder mejorar el diseño del producto, el discurso comercial y la estandarización técnica, permitiendo construir una venta consultiva alineada con las motivaciones reales del comprador.

3.2 Modelo CANVAS de Osterwalder

El Modelo Canvas describe la lógica mediante la cual una organización crea, entrega y captura valor por medio de nueve bloques: segmentos de clientes, propuesta de valor, canales, relaciones con clientes, fuentes de ingresos, recursos clave, actividades clave, socios clave y estructura de costos. Su utilidad principal radica en ofrecer una visión sistémica del negocio, donde cada decisión debe guardar coherencia con las demás. El Canvas es especialmente útil para traducir una estrategia general en hipótesis operativas. Si una empresa declara que competirá por diferenciación, el lienzo permite verificar si esa diferenciación realmente aparece en la propuesta de valor, si los canales refuerzan la experiencia, si las relaciones generan fidelización y si la

estructura de costos soporta la promesa hecha al cliente. Entre las fortalezas del Canvas está su capacidad de síntesis, comunicación transversal y diseño colaborativo. Permite que equipos de estrategia, operaciones, finanzas, tecnología y mercadeo hablen un mismo lenguaje visual y detecten inconsistencias tempranas. Su limitación principal es que, por sí solo, no define prioridades competitivas ni secuencia de validación. El lienzo muestra la arquitectura del negocio, pero no resuelve automáticamente qué posición competitiva conviene ni cuál hipótesis debe probarse primero. Por eso su integración con Porter y Aulet resulta especialmente poderosa.

La tesis utiliza explícitamente el modelo CANVAS como herramienta para estructurar la propuesta empresarial, e incluso presenta tanto una tabla como una representación gráfica del modelo de negocio para la empresa de automatización en seguridad residencial. Esta adopción no es casual, porque el caso exige visualizar cómo se conectan cliente objetivo, propuesta de valor, canal consultivo, ingresos recurrentes, aliados instaladores y plataforma tecnológica.

3.3 Producto mínimo viable de Bill Aulet

Bill Aulet desarrolla en el libro la disciplina de emprender un enfoque sistemático de 24 pasos para construir empresas de base innovadora. Dentro de esa secuencia, el paso 22 define el Producto Mínimo Viable de negocio o PMV. El PMV debe integrar las hipótesis críticas del producto, generar valor para el cliente y demostrar disposición de pago por parte del comprador, aunque todavía no sea una solución totalmente desarrollada. Esta diferencia es crucial desde la estrategia. Un prototipo técnico puede confirmar que algo funciona, un PMV de negocio confirma si existe una transacción creíble y una base inicial para aprendizaje comercial. En otras palabras, no basta con que el usuario diga que le gusta la solución, debe haber evidencia de uso valioso, adopción y pago. Una contribución importante de Aulet es recordar que la validación no debe

limitarse al funcionamiento técnico. El PMV exige que el cliente reciba valor y que exista una forma verificable de monetización. La tesis debe alinearse con este criterio al concebir el PMV como una combinación mínima entre producto, operación y servicio que permita al cliente percibir valor, justificar la inversión y sostener una contratación recurrente. Esa lectura es más madura que la noción clásica de PMV como simple prototipo y se aproxima mucho más al pensamiento de Aulet.

3.4 Tensores clave de estrategia organizacional

La estrategia organizacional no se agota en la formulación de objetivos o en la definición de una propuesta de valor. Su efectividad depende, sobre todo, de la capacidad de la organización para convertir la intención estratégica en resultados concretos y sostenibles. En ese tránsito entre el diseño y la ejecución aparecen los llamados tensores estratégicos, es decir, factores transversales que tensionan, condicionan y orientan la implementación de la estrategia dentro de la empresa. Los tensores clave de estrategia organizacional constituyen la base real sobre la que se sostiene la ejecución. Los indicadores permiten observar el avance en las capacidades distintivas que hacen posible la ventaja, la medición convierte los datos en aprendizaje, el talento ejecuta y adapta, la estructura coordina y la asignación de poder habilita la decisión oportuna. Desde esta perspectiva, la estrategia debe comprenderse como una arquitectura viva compuesta por decisiones, recursos, capacidades y mecanismos de coordinación. Una organización puede formular una estrategia sólida en el papel, pero fracasar si no cuenta con indicadores adecuados, talento alineado, estructura coherente, capacidades distintivas claramente desarrolladas y una distribución del poder compatible con la velocidad de decisión requerida. Por ello, el estudio de los tensores estratégicos

resulta indispensable para explicar por qué unas organizaciones ejecutan con éxito mientras otras permanecen atrapadas en la formulación.

Las capacidades distintivas son el conjunto de habilidades, rutinas, conocimientos y recursos que permiten a una organización desempeñarse mejor que sus competidores en aquellas actividades que son estratégicamente relevantes. No se trata simplemente de fortalezas genéricas, sino de capacidades que generan valor, son difíciles de imitar y resultan coherentes con la propuesta estratégica de la empresa. No basta con declarar una intención competitiva, se requiere dominar procesos, tecnologías, relaciones o métodos que hagan posible la diferenciación o la eficiencia esperada. Las capacidades distintivas no son estáticas. Se construyen, aprenden y refinan con el tiempo. Por eso, la organización debe identificarlas con precisión, protegerlas y convertirlas en parte de su sistema operativo. Cuando una empresa reconoce cuáles son sus capacidades realmente distintivas, puede enfocar mejor sus inversiones, su talento y sus prioridades de mejora. De lo contrario, corre el riesgo de dispersarse en actividades que no fortalecen su ventaja real.

La medición constituye el sistema mediante el cual la organización recoge, procesa, interpreta y utiliza la información. En otras palabras, medir no es solo registrar datos, sino construir un mecanismo de aprendizaje y control. Una buena medición estratégica debe permitir comparar metas con resultados, identificar tendencias, priorizar acciones correctivas y evaluar la consistencia entre planificación y ejecución.

El talento es uno de los factores más decisivos de la estrategia porque ninguna estructura ni sistema de indicadores puede compensar la ausencia de personas capaces de ejecutar con criterio, compromiso y adaptabilidad. El talento no debe entenderse solo como capacitación técnica, sino como la combinación de conocimientos, habilidades, actitud, juicio y capacidad de aprendizaje aplicada al cumplimiento de la estrategia. En una organización estratégicamente

alineada, el talento cumple dos funciones esenciales. La primera es operativa: ejecutar procesos con calidad, disciplina y consistencia. La segunda es adaptativa: identificar oportunidades, resolver problemas y contribuir al ajuste continuo de la estrategia. Una empresa puede invertir en tecnología o en expansión, pero si no desarrolla talento interno suficiente, su ejecución quedará limitada. En consecuencia, el talento es un tensor que conecta la visión estratégica con la capacidad real de implementación.

La estructura organizacional define cómo se distribuyen funciones, responsabilidades, flujos de información y mecanismos de coordinación dentro de la empresa. Es uno de los tensores más visibles de la estrategia, porque determina la forma en que la organización actúa, decide y responde al entorno. La relación entre estructura y estrategia es bidireccional. Por un lado, la estrategia debe diseñarse considerando las posibilidades y límites de la estructura existente. Por otro, la estructura debe ajustarse para no obstaculizar la ejecución estratégica. Cuando existe desalineación entre ambas, aparecen problemas como duplicidad de funciones, lentitud decisoria, conflictos internos o falta de coordinación. La estructura se convierte así en un soporte invisible de la estrategia: si funciona bien permite fluidez, si funciona mal genera inercia organizacional.

La asignación de poder es un tensor estratégico fundamental porque determina quién decide, sobre qué decide y con qué nivel de autonomía. En toda organización, la estrategia requiere decisiones oportunas sobre recursos, prioridades, alianzas, inversiones, cambios operativos y respuesta al mercado. Si el poder está mal distribuido, la estrategia se vuelve lenta, fragmentada o excesivamente dependiente de pocas personas. Una asignación de poder adecuada debe equilibrar control y autonomía. Demasiada centralización puede generar rigidez y retrasos, demasiada descentralización puede producir dispersión y pérdida de coherencia. El reto consiste en ubicar las decisiones al nivel donde existan mejor información, responsabilidad y capacidad de acción. En

este sentido, la estrategia se ejecuta mejor cuando el poder está alineado con la información y con los objetivos del negocio.

Desde esta perspectiva, el trabajo de grado debe entender la estrategia como una construcción organizacional integral, no como una declaración aislada de objetivos. La verdadera pregunta no es solo qué quiere lograr la empresa, sino si cuenta con los recursos internos necesarios para hacerlo realidad.

4. Desarrollo del proyecto

4.1 Vigilancia Tecnológica

Basados en el concepto de Vigilancia Tecnológica, el cual se constituye como un proceso que consiste en recopilar y analizar información relevante sobre avances tecnológicos y de mercado para transformar los datos en conocimiento estratégico con el fin de innovar, competir e identificar oportunidades, se inició con este proceso sobre el servicio o producto de Automatización Residencial. La vigilancia tecnológica se estructuró como un proceso sistemático orientado a identificar tecnologías, soluciones y modelos operativos relevantes para el servicio de automatización en seguridad residencial y portería remota. El punto de partida fue la definición de las necesidades de información de la empresa objetivo: comprender el estado del arte en control de accesos, monitoreo remoto de edificios y plataformas integradas para copropiedades bajo propiedad horizontal. Sobre esta base se definieron factores críticos de vigilancia, tales como tecnologías de control de acceso, integración de plataformas residenciales, automatización de conserjería y modelos de portería remota.

Lo primero que se pudo identificar a medida que se profundizaba en el concepto de Automatización Residencial, es que dicho producto era mejor conocido en el mundo como “Remote Concierge” o “Conserjería Remota”. En Colombia se especifica el servicio como “Portería Remota”. A partir de estos factores se construyeron ecuaciones de búsqueda utilizando combinaciones de palabras clave en inglés y español (por ejemplo, "remote concierge", "remote doorman", "residential access control platform", "smart building security", "portero remoto", "automatización residencial"), así como términos asociados a control de accesos, videoporteros, plataformas de gestión de edificios y monitoreo remoto 24/7. Las búsquedas se realizaron en bases de datos públicas de patentes recomendadas internacionalmente, tales como Google Patents, y Lens.org, con el fin de garantizar amplitud y comparabilidad de resultados. Para asegurar la pertinencia de las búsquedas, se definieron criterios explícitos de inclusión y exclusión, alineados con el foco estratégico del modelo de negocio

- **Ámbito tecnológico:** se incluyeron búsquedas relacionadas con sistemas de control de acceso electrónico, videoporteros, plataformas de administración de edificios, integración con servicios de pago y soluciones de portería remota o conserjería digital
- **Aplicación residencial:** se priorizaron las invenciones orientadas a edificios residenciales o multifamiliares, excluyendo desarrollos puramente industriales o de infraestructura crítica.
- **Nivel de integración:** se favorecieron tecnologías que integraran hardware (controladores de acceso, cerraduras, cámaras) con software (plataformas en la nube, aplicaciones móviles, paneles de administración) por su cercanía con el concepto de automatización residencial integral.

- Vigencia y actualidad: se seleccionaron patentes con fechas de prioridad y publicación recientes, de forma que reflejaran las tendencias tecnológicas vigentes en el sector.
- Alcance geográfico: se dio prioridad a búsquedas con protección en mercados de referencia (Estados Unidos, Europa) que suelen marcar estándares tecnológicos y de modelo de negocio en automatización residencial.
- Funcionalidad principal: descripción sintética de la solución propuesta (por ejemplo, sistema de control de acceso basado en nube, plataforma de gestión integral de edificios, sistema de portería remota con video y audio bidireccional)
- Arquitectura tecnológica: identificación de la relación entre hardware, software y servicios en la nube, así como el grado de modularidad e interoperabilidad de la solución.
- Nivel de automatización: grado en el cual la solución permite sustituir tareas presenciales (portería física) por supervisión remota.
- Modelo de generación de datos: tipo de información capturada (eventos de acceso, video, registros de visitantes, integraciones con pagos) y su potencial para habilitar servicios de valor agregado.
- Elementos del modelo de negocio implícitos: indicios sobre fuentes de ingresos (suscripción, licenciamiento de software, venta de hardware), tipo de relación con el cliente (servicio gestionado, autoservicio digital) y alianzas tecnológicas.

4.1.1 Patente US_10885734_B2.

A través de la plataforma LENS.ORG se pudo evidenciar que existe una patente en Estados Unidos con fecha del cinco de enero de 2021 bajo el concepto de Conserjería Remota identificada con el número “US_10885734_B2”. Este documento describe una patente para sistemas y métodos

escalables de monitoreo y conserjería, centrándose en el uso de dispositivos y sensores de control de acceso inteligentes para mejorar la seguridad. El concepto principal consiste en un servidor de monitoreo dinámico que recibe y analiza datos de estos sensores para identificar eventos y generar alertas. Estas alertas se transmiten a un operador o sistema automatizado que puede proporcionar acceso, responder a eventos de seguridad o actuar como conserje remoto, gestionando eficazmente el acceso al edificio y abordando diversas situaciones en tiempo real con base en la información de los sensores.

La patente presenta figuras que representan la arquitectura, los flujos de procesos, las interfaces de usuario y los escenarios específicos de un sistema de seguridad que utiliza sensores y dispositivos inteligentes de control de acceso para monitorear un área, generar alertas y gestionar el acceso, lo que a menudo implica monitoreo remoto e interacción con un operador. Adicional, la patente abarca el modelo para el control de acceso de personas desconocidas, la respuesta a eventos y la participación de servidores de monitoreo y operadores humanos.

Para organizar un modelo de negocio de conserjería remota basándose en la patente US_10885734_B2, se deben considerar los aspectos tecnológicos específicos del sistema descrito en la patente.

A continuación, se detallan los puntos más importantes a tener en cuenta:

Dispositivo de Control de Acceso Inteligente: Este dispositivo es el punto central de la interacción en el lugar del cliente y debe estar configurado para recibir datos de sensores y analizarlos. Debe ser capaz de proporcionar alertas visuales y/o audibles y permitir la comunicación e interacción con un visitante. La patente menciona que incluye micrófono y altavoz, lo que implica capacidades bidireccionales de audio y posiblemente video para la interacción remota.

Sensores Integrados: El sistema se apoya en uno o más sensores que proporcionan datos sobre seguridad, eficiencia y estado de salud. Estos sensores pueden detectar la llegada de un visitante, así como situaciones de emergencia como incendios, humo, inundaciones, fugas de gas o emergencias médicas. La integración de diversos tipos de sensores es crucial para la amplitud del servicio.

Servidor de Monitoreo Dinámico: Este servidor es el cerebro de su operación remota. Es el responsable de recibir las alertas y señales del dispositivo de control de acceso inteligente. La patente especifica que el servidor puede realizar la validación de credenciales numéricas e identificación por voz. Esto es vital para la autenticación y seguridad del acceso.

Operador Humano: A pesar de la tecnología, la patente subraya la intervención del operador humano. El operador debe poder ver e interactuar con el visitante a través del dispositivo inteligente. El operador tiene la capacidad de autorizar o denegar el acceso de forma remota a un edificio. Es fundamental que el operador pueda manejar situaciones inesperadas y, si es necesario, derivar la comunicación a las autoridades o servicios de emergencia si la persona en el lugar no responde o no puede manejar la situación.

Registro Digital de Interacciones: El sistema debe registrar y almacenar un historial digital de la interacción, incluyendo información visual y auditiva. Esto es esencial para auditorías, resolución de disputas y mejora continua del servicio.

Conectividad y Escalabilidad: La comunicación entre el dispositivo de acceso y el servidor de monitoreo debe ser fiable a través de una red. El sistema se describe como escalable, lo que le permitirá expandir su servicio a más propiedades o diferentes tipos de edificios, desde residenciales hasta comerciales.

Soporte y Control de Dispositivos de Consumo: El dispositivo de conserjería puede configurarse para registrar, controlar y ofrecer soporte a otros dispositivos de consumo en el hogar, como interruptores y lámparas. Puede facilitar llamadas de soporte de voz o video para solucionar problemas.

4.1.2 Patente US_10798244_B2.

A través de la plataforma LENS.ORG se pudo evidenciar que existe una patente con fecha del seis de Octubre de 2020 y con número “US_10798244_B2”, relacionada con la patente “US_10885734_B2”, mencionada en el anterior apartado. La patente describe un dispositivo de conserjería para el registro, control y soporte de dispositivos electrónicos de consumo, entre ellos lámparas inteligentes, interruptores, electrodomésticos, dispositivos electrónicos de entretenimiento, ventilación y aires acondicionados. El dispositivo de conserjería puede adoptar diversas formas físicas, como una varita, un dispositivo con teclado de pulgar y controles de navegación, pantalla táctil, o también puede ser una aplicación que se ejecuta en un teléfono inteligente, tableta o PC.

El sistema puede conectarse a un "home management bridge" (puente de gestión del hogar) y/o a servidores de gestión basados en la nube. Este puente es una entidad física que puede ser separada del dispositivo de conserjería, o estar integrada en el mismo, o en otro dispositivo de consumo como una TV o un electrodoméstico principal. Su función es gestionar la comunicación y el registro de dispositivos electrónicos de consumo.

El dispositivo de conserjería puede configurarse para realizar llamadas de soporte por voz o video, durante la videollamada, el dispositivo puede mostrar imágenes de la persona de soporte. El dispositivo de conserjería puede almacenar y enviar información de identificación del

dispositivo de consumo (como número de serie, fabricante, modelo) y del usuario al centro de soporte. Esto puede personalizar la experiencia del usuario y ofrecer resolución automatizada de problemas.

La patente US10798244 B2 se puede complementar de manera significativa con la patente US_10885734_B2 al integrar las funcionalidades de soporte, control y registro de dispositivos de consumo del primero con las capacidades de monitoreo y seguridad del segundo. Ambas patentes, aunque relacionadas con servicios de conserjería o monitoreo, se enfocan en aspectos ligeramente diferentes, lo que permite una fusión sinérgica para crear un sistema de hogar inteligente más robusto y completo. Al combinar ambas, el dispositivo de conserjería de US10798244 B2 podría actuar como la interfaz central para la visualización y gestión de alertas y datos de sensores del sistema de seguridad de US_10885734_B2. Esto permitiría a los usuarios no solo controlar sus luces y electrodomésticos, sino también recibir información en tiempo real sobre la seguridad de su hogar a través de una única plataforma.

La patente US10798244 B2 destaca la capacidad del dispositivo de conserjería para iniciar una sesión de soporte con una sola acción, identificando automáticamente el dispositivo de consumo y permitiendo llamadas de voz o video para soporte. Cuando el sistema de seguridad de US_10885734_B2 detecte un evento y genere una alerta, el dispositivo de conserjería podría ser programado para iniciar automáticamente una sesión de soporte o una videollamada con el centro de monitoreo o los servicios de emergencia. Esta llamada incluiría la identificación automática del sensor o dispositivo de seguridad que activó la alerta, agilizando la respuesta y proporcionando información crítica.

La recolección de datos de ambos sistemas (información de registro y estado de dispositivos de consumo, y datos de sensores), podría alimentar análisis más complejos en la nube.

Esto permitiría al sistema aprender patrones de comportamiento del usuario y diferenciar entre actividad normal y posibles amenazas, mejorando la inteligencia y la capacidad de respuesta proactiva del hogar inteligente.

En resumen, la integración de las dos patentes transformaría un dispositivo de conserjería general en un centro de comando integral para el hogar inteligente, combinando comodidad, soporte y gestión con capacidades avanzadas de monitoreo y seguridad.

4.1.3 Empresas que ofrecen el servicio.

Se pudieron establecer diferentes empresas a nivel mundial que ofrecen el servicio de Automatización Residencial de las cuales se escogieron diez. Las empresas seleccionadas fueron identificadas a partir de un proceso de análisis comparativo a nivel internacional, considerando proveedores con experiencia comprobada en automatización residencial y monitoreo inteligente, presencia activa en diferentes mercados y capacidad de ofrecer soluciones integrales adaptables a distintos contextos normativos y operativos. Se incluyeron empresas de Colombia, Perú, Estados Unidos, Canadá y el Reino Unido con el fin de garantizar una visión amplia del mercado, incorporando tanto proveedores locales como referentes internacionales en el sector. Se consideró la capacidad de las soluciones para ser implementadas o adaptadas a las condiciones técnicas, regulatorias y operativas del entorno objetivo del proyecto. A continuación, se relacionan las diferentes empresas:

- a. Empresas en Colombia: Intelligate, Domosis, Alarmar, Guardacol
- b. Empresas en Perú: Portero Seguro
- c. Empresas en Estados Unidos y Canada: Spotter, Live Patrol, Stealth Monitoring, Carson Living, Inc

d. Empresas en el Reino Unido: Alert Monitoring

Estas empresas describen diversas soluciones remotas de seguridad y control de acceso para propiedades residenciales y comerciales. Varias empresas ofrecen sistemas que combinan tecnología como cámaras e intercomunicadores con monitorización humana para gestionar tareas que tradicionalmente realiza el personal in situ, como la gestión del acceso de visitantes y entregas, la vigilancia de actividades sospechosas y la respuesta a emergencias. Las empresas promocionan el servicio como una forma de aumentar la seguridad y reducir los costos asociados a los porteros o guardias tradicionales.

Con base en lo anterior, es posible definir un modelo de negocio general que abarca los aspectos más importantes de las empresas seleccionadas.

Basado en el modelo CANVAS se propone el modelo de negocio general para estas 10 empresas:

Segmentos de Clientes: Administradores. Residentes (inquilinos). Propietarios de edificios, copropiedades, negocios y almacenes. Edificios/propiedades residenciales.

Propuestas de Valor: Reducir significativamente los costos en comparación con el servicio tradicional de portero/personal. Aumenta y optimiza la seguridad. Realiza un monitoreo de seguridad proactivo. Garantiza un monitoreo continuo y permanente sin pausas ni distracciones. Gestiona el acceso al edificio de forma remota. Ofrece un registro detallado de entradas y salidas del edificio. Puede rastrear cuándo se ha desbloqueado una puerta del sistema. Ofrece respuesta inmediata a emergencias o intrusiones. Envía una respuesta motorizada cuando es necesario. Envía personal al edificio o llama a la policía. Facilita la colaboración y la comunicación con la policía y las autoridades. Brinda tranquilidad y seguridad a los ocupantes. Permite el acceso a los invitados preaprobados y los recibe. Ofrece atención de emergencia 24/7.

Canales: Ventas y consultas directas: Los proveedores interactúan directamente con clientes potenciales, como administradores de propiedades, juntas de condominios, propietarios de edificios y empresas. Presencia en línea y puntos de contacto: Los sitios web y portales en línea sirven como puntos principales para que los clientes potenciales conozcan los servicios y soliciten información.

Recursos Clave: Equipo de operadores de medios y central de monitoreo. Equipo de servicio técnico. Tecnología y sistemas integrados: Plataformas de software, hardware (intercomunicadores, cámaras, CCTV, dispositivos/lectores de control de acceso, cerraduras inteligentes, sensores, motores de portones, alarmas, barreras físicas, servidores, equipos de red). Personal físico para respuesta (supervisor/equipo motorizado, personal de seguridad). Inventario de equipos y repuestos.

Actividades clave: Operación de un servicio de monitoreo remoto 24/7. Gestión remota de entradas y accesos. Control de acceso en todos los edificios. Monitoreo (alarmas, videovigilancia, eventos de seguridad, cámaras, actividades diarias, detección de incendios). Monitoreo proactivo. Respuesta a emergencias e incidentes. Activación de protocolos de reacción. Envío de equipos de respuesta motorizados. Evaluación de riesgos. Diseño de sistemas a medida.

Colaboradores Clave: Autoridades como la Policía Nacional. Empresas de administración de propiedades que son clientes y socios de integración.

Proveedores/fabricantes de tecnología y hardware para control de acceso, intercomunicadores, cerraduras inteligentes, cámaras, sensores y alarma. Técnicos instaladores de seguridad electrónica.

Estructura de Costo: Costos asociados con la dotación de personal para la operación (operadores de medios, equipos de respuesta, personal de soporte técnico). Costos de

infraestructura tecnológica, incluyendo hardware (intercomunicadores, cámaras, servidores, etc.), desarrollo y licencias de software, alojamiento, servicios en la nube, sistemas de respaldo y conexiones a internet. Costos relacionados con la instalación y el mantenimiento de sistemas y equipos de seguridad. Costos de respuesta física, como el mantenimiento de equipos motorizados. Costos de marketing y ventas, incluyendo la generación de leads, la elaboración de presupuestos, las consultas, las visitas a las instalaciones y las sesiones de diseño en línea. Costos administrativos, que cubren operaciones generales. Costos como el seguro contra robo e incendio.

Ingresos: Tarifas de servicio para Conserjería Remota o Portero Virtual. Suelen estructurarse en función de diferentes planes que incluyen el servicio mensual de monitorización, de video, alarmas y otros eventos de seguridad. Venta de sistemas, productos y equipos de seguridad, incluyendo cámaras, sistemas de control de acceso y alarmas. Tarifas de instalación de los equipos de seguridad electrónica. Tarifas de mantenimiento y servicio técnico.

4.1.4 Selección de empresas destacadas.

Las siguientes empresas, Carson Living, Inc, Guardacol y Portero Seguro, presentan propuestas de valor robustas y bien descritas para sus servicios de conserjería remota, abarcando aspectos como ahorro de costos, alcance de servicios, uso de tecnología, capacidades de respuesta y beneficios para residentes y la administración.

Carson Living Inc, empresa de Estados Unidos, ofrece un servicio de lujo a una fracción del costo de un portero de tiempo completo. Su equipo opera 24/7 a través del intercomunicador del edificio. La propuesta de valor incluye:

Gestión de entregas: Vetan a los mensajeros, seleccionan entregas, otorgan acceso a la sala de paquetes y deniegan el acceso si el mensajero está en la dirección incorrecta o si la entrega no está aprobada.

Gestión de acceso para visitantes: Otorgan acceso a vendedores programados, huéspedes preaprobados (saludándolos y alertando al residente)

Captura de potenciales clientes: Capturan información de potenciales clientes en la puerta y la reenvían al equipo de arrendamiento o ventas.

Equipo humano 24/7: Un ser humano atiende el intercomunicador en un promedio de 10 segundos o menos.

Experiencia "One-app Resident Experience": Integra funciones como solicitudes de servicio, reserva de amenidades, tablón de mensajes y se integra con software para pagos de alquiler (como Clickpay).

Integración tecnológica: Soporta hardware como control de acceso (Brivo), intercomunicadores y cerraduras inteligentes.

Seguridad mejorada: Se integra con cámaras en la nube para video (con hasta 30 días de grabación descargable), rastrea puertas desbloqueadas, alerta a residentes sobre visitantes denegados y a administradores sobre vendedores denegados.

Guardacol GUVI (Guarda Virtual Inteligente), empresa de Colombia, se presenta como un sistema integral de seguridad para edificios residenciales y empresariales. Su guarda virtual combina tecnología con un Centro de Operaciones disponible las 24 horas. Su propuesta de valor se centra en:

Reducción de costos: Permite reducir hasta un 70% los costos de administración y vigilancia.

Control de acceso seguro y eficiente: Anuncia y autoriza visitas, gestiona el acceso a parqueaderos y registra entradas y salidas.

Monitoreo especializado: Cuenta con monitoreo constante por operadores especializados.

Respuesta inmediata: Actúa ante emergencias o intrusiones. Incluye disuasión activa contra delincuentes, respuesta motorizada y alerta a las autoridades.

Gestión de servicios: Gestiona correspondencia, domicilios y entregas. Botón de asistencia a través de una aplicación celular.

Planes flexibles: Ofrece diferentes planes (Autónomo, Híbrido, GUVI 360) para adaptarse a diversas necesidades y presupuestos.

Portero Seguro (Portería Remota Inteligente), empresa de Perú, ofrece una portería remota inteligente que busca revolucionar la seguridad residencial combinando la calidez humana con la eficiencia tecnológica. Su propuesta de valor destaca por:

Reducción significativa de costos: Permite un ahorro de hasta el 50% en los costos de portería tradicional.

Realización de todas las tareas de un portero tradicional: Atiende visitas, recibe entregas, abre/cierra puertas peatonales y de cochera, se comunica con residentes, enciende/apaga luces y recibe paquetes en casilleros electrónicos.

Monitoreo 24/7 sin interrupciones: La vigilancia remota nunca se detiene, garantizando seguridad continua con tecnología avanzada y un equipo capacitado. Utiliza Inteligencia Artificial en video para monitoreo permanente y alerta ante actividad sospechosa.

Atención rápida: Atiende el intercomunicador en menos de 10 segundos.

Respuesta proactiva: Actúa de manera preventiva ante eventos sospechosos. Incluye ahuyentar delincuentes con sirenas, enviar un motorizado para emergencias y comunicarse con la Policía Nacional.

Tecnología avanzada: Utiliza tecnología con plataforma de video management system y diseño de cobertura basado en análisis estadístico. Ofrece sensores en puertas peatonales para evitar que queden abiertas.

Confiabilidad: El servicio continúa funcionando incluso sin luz (con respaldo de energía) o internet (con opción de línea de contingencia).

Tranquilidad adicional: Incluye seguro contra robos e incendios, rondas nocturnas y exención de responsabilidad legal.

Flexibilidad y prueba: Ofrece un periodo de prueba de 2 meses y permite cancelar el servicio sin penalización después del contrato inicial de 3 meses.

Énfasis en el equipo humano: Aclara que la vigilancia es realizada por un equipo humano capacitado que administra la tecnología, no por una máquina.

Dentro de los servicios ofrecidos por estas tres empresas, se destaca el concepto de una "experiencia para residentes en una sola aplicación" o soluciones integradas como un elemento clave para la comodidad. Esta plataforma sirve como centro neurálgico para que los residentes y los administradores de propiedades interactúen con el servicio de portero remoto/conserje virtual y accedan a otras funciones relacionadas con el edificio.

Solicitudes de servicio: Carson Living, Inc ofrece explícitamente "Solicitudes de servicio" como un complemento de software dentro de su experiencia para residentes en una sola aplicación. También incluye "Solicitudes de mantenimiento y reserva de citas" y "Solicitudes de servicio" como servicios gestionables. Los residentes pueden enviar una solicitud de mantenimiento a través

de la aplicación, y el equipo remoto puede coordinar el acceso del proveedor, aprovechando su capacidad para facilitar el acceso al edificio de los proveedores.

Gestión de Proveedores y Contratistas: Los sistemas están diseñados para filtrar y otorgar acceso a proveedores y contratistas programados. Esta funcionalidad ya cuenta con la infraestructura y los procesos necesarios para evaluar y permitir el acceso a proveedores de servicios externos.

Capacidades de Integración: Carson Living, Inc se describe como una empresa de software especializada en la integración de software de administración de propiedades, hardware de edificios y el equipo de portero remoto. También se integra con programas específicos como Clickpay. Esto indica que los sistemas están diseñados con la integración en mente, lo que facilita la conexión con plataformas o proveedores para servicios como la programación de mantenimiento, o incluso con sistemas de reservas de terceros para otros servicios.

4.1.5 Patrones de competitividad de Carson Living.

La estrategia y el enfoque de integrar las diversas operaciones del edificio y servicios para residentes en una única plataforma móvil parece ser un factor diferenciador clave, que genera valor, y para la empresa Carson Living, Inc esto es una de sus fortalezas. Carson se describe como una empresa de software, no solo un fabricante de hardware. Este enfoque les permite personalizar la experiencia para cada edificio según sus preferencias específicas para la gestión de visitantes y proveedores. Pueden integrarse con el hardware existente del edificio, como intercomunicadores, sistemas de control de acceso y cámaras conectadas a una plataforma de vídeo en la nube. Esta flexibilidad y el énfasis en la personalización de la experiencia de software y la integración de diversos sistemas en una sola plataforma distinguen aún más a Carson Living, Inc. El énfasis del

modelo que incluye una experiencia integrada del residente en una sola aplicación, la gestión del acceso de proveedores/contratistas, la oferta de funciones de "Solicitudes de Servicio" y la capacidad de adaptar e integrar soluciones proporciona una base sólida para añadir servicios como el mantenimiento de viviendas y reservas de servicios, mejorando así la personalización y la comodidad para los usuarios.

Plataformas como ClickPay ofrecen una "Experiencia Moderna para Residentes" con un solo inicio de sesión para pagos, comunicaciones, seguimiento de paquetes y solicitudes de mantenimiento. Esto incluye la posibilidad de consultar saldos y configurar pagos automáticos. La integración de un servicio de portero remoto con plataformas de pago como ClickPay permite a los residentes pagar el alquiler desde una única aplicación que también gestiona otros servicios.

La Suite de Seguridad de Brivo, presente también en la solución de Carson, unifica el control de acceso con dispositivos de hardware como intercomunicadores y cerraduras inteligentes. Entre sus características principales se incluyen un control de acceso simplificado, mayor seguridad para los residentes que incluye la capacidad de gestionar y supervisar remotamente cada puerta, portón y ascensor, como proporcionar acceso a los residentes e invitados.

Guy Blachman es el fundador y presidente ejecutivo de Carson Living, Inc. A lo largo de su carrera, Blachman ha demostrado un fuerte interés en tecnología para propiedades residenciales, ha fundado y liderado empresas como MyBuilding y ActiveBuilding, enfocadas en software para la gestión de comunidades residenciales e innovación en servicios para residentes. Blachman también ha compartido su experiencia en eventos y medios especializados, discutiendo temas y oportunidades de integración tecnológica en edificios residenciales. Guy Blachman está profundamente involucrado en la intersección de la tecnología y la gestión de propiedades

residenciales, buscando constantemente innovar y mejorar la experiencia de los residentes a través de soluciones tecnológicas avanzadas. La colaboración con ClickPay y Brivo es un ejemplo de cómo Blachman busca integrar servicios complementarios para ofrecer una solución integral en el sector inmobiliario. En abril de 2019, Carson y Brivo anunciaron una integración que permite a los usuarios de la aplicación controlar el acceso a puertas mediante las funcionalidades de Brivo. Esta integración también permite al centro de llamadas 24/7 de Carson conectarse con las puertas de entrada de los edificios, y a los residentes y al personal utilizar la aplicación de Carson para abrir puertas y enviar llaves digitales geolocalizadas a los invitados. Además, los nombres del directorio de Brivo se actualizan continuamente a través de Carson, basándose en las actualizaciones de mudanzas de los residentes en el sistema contable principal del administrador de la propiedad, logrando una integración fluida en la gestión de propiedades. Los usuarios de Carson también pueden enviar llaves temporales a visitantes sin necesidad de que estos descarguen una aplicación, una característica adicional construida sobre la infraestructura de Brivo.

Esta colaboración refleja la visión de Blachman de ofrecer una experiencia integral a los residentes, integrando múltiples servicios en una sola aplicación para mejorar la eficiencia operativa y la calidad de vida en comunidades residenciales.

4.1.5.1 Propuesta de valor. El modelo de los "tensores clave" en el diseño de la estrategia organizacional está influido por diversas corrientes y autores reconocidos en el campo de la administración estratégica. Estos tensores como indicadores de medición, talento, estructura, capacidades distintivas y asignación de poder o derechos de decisión representan dimensiones fundamentales que aseguran la coherencia y efectividad de la estrategia en cualquier organización. Definir una estrategia con base en estos tensores permiten establecer patrones de competitividad

que fortalecen las condiciones de la organización en el mercado. Consultores organizacionales y equipos directivos suelen adoptar y adaptar estos modelos para diseñar la arquitectura estratégica específica de cada organización.

Con base en lo anterior, la estrategia de Carson Living, Inc. basada en la integración de servicios y operaciones del edificio en una única plataforma móvil para residentes y administradores corresponde principalmente al tensor de "Capacidades distintivas". Esta integración, así como la capacidad de adaptación y personalización para cada edificio, configuran una ventaja competitiva central, al diferenciar claramente a Carson respecto a soluciones tradicionales y a otros competidores.

Aunque el énfasis principal está en las capacidades distintivas, la estrategia de Carson Living también abarca otros tensores del modelo:

Estrategia: Carson tiene bien definida su meta ("dónde jugar y cómo ganar"): ser el centro operativo digital en la vida del residente, optimizando la gestión y experiencia de servicios residenciales.

Indicadores: Se apoya en la experiencia del usuario, la eficiencia operativa y la satisfacción del residente como indicadores de éxito e impacto.

Talento: El personal, especialmente la visión de liderazgo de Guy Blachman, impulsa la innovación y la orientación tecnológica.

Estructura y Asignación de poder: Carson facilita la toma de decisiones centralizada y eficiente, dando autonomía tanto a residentes como a administradores mediante la plataforma.

Teniendo en cuenta lo anterior, se puede establecer que la propuesta de valor de Carson Living se fundamenta en ofrecer a edificios residenciales y a sus comunidades una plataforma digital integral que centraliza, automatiza y personaliza la gestión de servicios, operaciones y

experiencias del residente, mejorando simultáneamente la eficiencia administrativa, la calidad de vida y la toma de decisiones, elevando la experiencia de vida en comunidad mediante capacidades tecnológicas distintivas y escalables.

4.1.5.2 Cadena de Abastecimiento. Carson Living establece su estrategia en la cadena de abastecimiento sobre la base de la integración digital y la colaboración directa con proveedores clave de tecnología, lo que le permite operar e innovar en el sector de la conserjería remota. Esta estrategia se orienta a maximizar la eficiencia operativa, ofrecer soluciones diferenciadas y asegurar la escalabilidad del modelo. Carson integra hardware y software de aliados estratégicos como Brivo (control de acceso), ClickPay (pagos y gestión de residentes), unificando estos sistemas en una sola plataforma para administradores y residentes. Estas alianzas permiten personalizar la solución para cada edificio. Carson selecciona socios tecnológicos que aportan valor agregado, no solo en suministro, sino en soporte posventa, adaptabilidad y presencia local en mercados clave como Europa y EE.UU. La colaboración se basa en acuerdos donde el proveedor no solo suministra tecnología, sino que también apoya el despliegue, instalación y atención continua de la solución, fortaleciendo la experiencia final del usuario. Carson establece alianzas con distribuidores regionales (como CIE en Reino Unido) que tienen conocimiento del mercado, red de instaladores y canales de soporte, facilitando la expansión internacional y adaptación a normativas locales. Esta relación con proveedores transforma a los socios en extensiones directas del modelo de negocio de Carson, asegurando la consistencia y calidad en cada implementación. Utilizando la integración de diferentes servicios, Carson optimiza procesos internos como la gestión y recepción de paquetes, control de visitantes, y acceso remoto, asegurando la trazabilidad y seguridad de cada operación. El modelo de “portero remoto”,

habilitado por la colaboración con proveedores de hardware, permite reducir la dependencia de personal físico, ahorrar costos y mejorar la atención 24/7. El relacionamiento estratégico con proveedores permite a Carson responder rápidamente a nuevas demandas de funcionalidad y seguridad, se obtienen sinergias con especialistas que facilitan la evolución tecnológica sin la carga de desarrollos propios complejos y garantiza continuidad operativa con soporte local/global para clientes finales.

La estrategia de Carson respecto a la cadena de abastecimiento se basa en una relación estratégica de colaboración con proveedores clave, que actúan como socios tecnológicos y comerciales. Esta integración otorga flexibilidad, optimización de procesos, diferenciación competitiva y una plataforma sólida para la innovación y expansión. Carson actúa como un integrador de múltiples soluciones en una sola plataforma, teniendo en cuenta la experiencia del usuario final.

5. Modelo de Negocio

Un producto solo existe cuando responde a una necesidad real, y solo un negocio existe si alguien está dispuesto a pagar por ese producto. El objetivo global de este trabajo de aplicación es la construcción de un modelo de negocio para una empresa de seguridad electrónica, más específicamente en una empresa que comercializa servicios de automatización en seguridad residencial. Lo anterior con base en una necesidad que se identificó en el mercado y que tiene una alta probabilidad de que alguien la adquiere. A través de este capítulo se va a definir el cliente objetivo, se va a identificar el cómo el producto satisface esa necesidad específica, se va a diseñar el producto y se estructurarán los canales de venta y distribución con base en las ventajas competitivas que se pudieron vislumbrar en el capítulo anterior, se determinarán las estrategias

para capturar valor a través de la venta y se formulará un plan de escalabilidad a futuro teniendo en cuenta la tecnología y operatividad. Esto permitirá definir el modelo de negocio para la nueva empresa.

5.1 Cliente Objetivo

Existe la necesidad en el mercado residencial de poder disminuir los costos de seguridad por el incremento que ha tenido la vigilancia física en los últimos años y por las nuevas condiciones laborales que fueron ya expuestas en los anteriores capítulos. A nivel residencial existen varios tipos de conjuntos o edificios, pero se requiere limitar el mercado a edificios residenciales bajo el régimen de propiedad horizontal que tengan entre 20 a máximo 80 unidades residenciales, red eléctrica estable, conectividad a internet y de estratos 4, 5 y 6. Se excluyen los conjuntos residenciales de casas como segmento del cliente objetivo debido a criterios técnicos, económicos y operativos. Los conjuntos residenciales de casas presentan una distribución espacial dispersa, caracterizada por amplias extensiones de terreno, múltiples accesos, y una mayor separación entre las unidades habitacionales. Esta configuración incrementa significativamente los costos de instalación de los sistemas de seguridad electrónica, debido a la necesidad de un mayor número de dispositivos, infraestructura de comunicación y puntos de control. Los conjuntos de casas demandan soluciones altamente personalizadas, dado que presentan múltiples variables en términos de accesos peatonales y vehiculares, zonas comunes extensas y perímetros de difícil control. Esta complejidad incrementa los riesgos operativos, por el contrario, los edificios residenciales, al concentrar los flujos de personas y vehículos en puntos de acceso definidos, permiten implementar sistemas de automatización más controlables y eficientes. Los edificios de propiedad horizontal se caracterizan por una configuración vertical que permite diseñar sistemas

de seguridad más eficientes, al focalizar la instalación de dispositivos tecnológicos en áreas críticas como porterías, accesos vehiculares, zonas comunes y núcleos de circulación. La similitud en la tipología de accesos y áreas comunes permite desarrollar paquetes tecnológicos homogéneos, lo que simplifica los procesos de diseño, instalación, mantenimiento y soporte técnico para los diferentes edificios. Esta estandarización reduce la complejidad operativa, mejorando la eficiencia en la prestación del servicio y su respectivo costo.

Desde una perspectiva económica, los edificios pertenecientes a los estratos 4, 5 y 6 presentan una mayor capacidad de pago por parte de los copropietarios, lo que facilita la implementación de soluciones tecnológicas avanzadas bajo esquemas de pago recurrente. En estos estratos, las cuotas de administración suelen contemplar rubros asociados a seguridad, mantenimiento y modernización, permitiendo absorber el costo del servicio sin afectar de manera significativa la estabilidad financiera de la copropiedad. En contraste, los edificios de estratos 1, 2 y 3 enfrentan mayores restricciones presupuestales. Para estos estratos se encuentra algún tipo de informalidad con el costo del servicio de vigilancia física, en donde se puede observar que estos no están acordes a lo exigido por la Super Intendencia de Vigilancia y Seguridad Privada, por lo que en los estratos 1, 2 y 3 se observa una menor penetración tecnológica y una preferencia por esquemas tradicionales de vigilancia, lo que incrementa la resistencia al cambio y dificulta la adopción de soluciones automatizadas. Desde el análisis del retorno sobre la inversión, los estratos 4, 5 y 6 ofrecen un entorno más favorable para la sostenibilidad del modelo de negocio, desde el punto de vista estratégico. La focalización en los estratos 4,5 y 6 permite alinear la propuesta de valor del servicio de automatización en seguridad con un segmento que valora la diferenciación, la calidad del servicio y la valorización del inmueble.

El proceso de adquisición de soluciones de automatización en seguridad residencial no recae en un consumidor individual, sino en una figura administrativa y organizacional propia del régimen de propiedad horizontal. En este sentido, el administrador del edificio y, de manera complementaria, el consejo de administración, se definen como las personas responsables de la evaluación, aprobación y contratación del servicio. El administrador del edificio constituye el buyer principal, en la medida en que es el encargado de la gestión operativa, financiera y contractual de la copropiedad. El administrador es responsable de garantizar la seguridad de los residentes y de las áreas comunes, optimizar los costos operativos del edificio, ejecutar las decisiones aprobadas por el consejo y la asamblea, contratar y supervisar proveedores de servicios. El consejo de administración constituye un buyer colectivo, con capacidad decisoria sobre la aprobación o rechazo de la inversión. Este órgano está conformado por copropietarios elegidos por la asamblea y representa los intereses financieros y patrimoniales del edificio. En el proceso de compra, el consejo actúa como decisor final, validando la propuesta presentada por el administrador y asegurando su alineación con los objetivos estratégicos de la copropiedad. Esta dinámica implica que el modelo de negocio debe comunicar beneficios técnicos claros para el administrador, presentar argumentos financieros sólidos para el consejo y ofrecer transparencia, soporte y continuidad del servicio.

El perfil del administrador del edificio corresponde a una persona que normalmente suele contar con estudios en áreas administrativas, contables, jurídicas, técnicas o afines, así como con experiencia previa en la gestión de propiedades horizontales. Posee conocimientos básicos de normatividad asociada a la propiedad horizontal, contratación de servicios, presupuestos y manejo de proveedores, lo que le permite evaluar propuestas técnicas y económicas con un enfoque pragmático orientado a resultados. El administrador enfrenta permanentemente restricciones

presupuestales, presión por parte de los copropietarios para mantener o reducir las cuotas de administración y una alta responsabilidad frente a la ocurrencia de incidentes de seguridad. En este contexto, muestra una marcada orientación hacia soluciones que reduzcan riesgos, optimicen costos y mejoren la eficiencia de los procesos, privilegiando esquemas de servicio confiables, estables y de fácil implementación. El administrador presenta una alta sensibilidad frente a soluciones que permitan mejorar la eficiencia operativa, reducir riesgos y minimizar contingencias legales y financieras. El administrador valora la continuidad del servicio, el soporte técnico oportuno y la claridad contractual, dado que cualquier falla o incumplimiento impacta directamente su gestión y su relación con los copropietarios. Por esta razón, privilegia proveedores que ofrezcan respaldo, experiencia comprobada y acompañamiento permanente. Aunque no siempre ostenta la decisión final, su criterio técnico y operativo tiene un peso significativo en la aprobación de soluciones, especialmente cuando estas demuestran beneficios claros en términos de seguridad, eficiencia y sostenibilidad financiera.

El consejo de administración está conformado por copropietarios elegidos por la asamblea general, quienes, en la mayoría de los casos, no ejercen funciones operativas directas, pero sí cumplen un rol fundamental en la evaluación y aprobación de propuestas presentadas por el administrador. En términos de perfil socioeconómico y profesional, los miembros del consejo suelen presentar una alta heterogeneidad, incluyendo profesionales de distintas áreas, empresarios, empleados y residentes con experiencia previa en gestión, finanzas o administración. Esta diversidad genera un enfoque plural en el análisis de las decisiones, donde convergen criterios técnicos, financieros y sociales. Desde el punto de vista financiero, el consejo de administración prioriza la estabilidad presupuestal del edificio y el uso eficiente de los recursos comunes. El consejo evalúa las propuestas de inversión con base en la relación costo–beneficio, el impacto en

las cuotas de administración y el retorno esperado en términos de reducción de costos operativos, mitigación de riesgos y valorización del activo inmobiliario. El consejo exige que las soluciones propuestas cuenten con respaldo técnico, viabilidad legal y aceptación social por parte de la comunidad. La minimización del riesgo reputacional y legal constituye un elemento central en su proceso de decisión. Por ello, privilegia proveedores con experiencia demostrada, soporte local y capacidad de acompañamiento a largo plazo.

En resumen, el cliente objetivo del servicio de automatización residencial en seguridad corresponde a edificios residenciales bajo el régimen de propiedad horizontal en Colombia, ubicados principalmente en zonas urbanas, con una estructura administrativa formal y una población de copropietarios que demanda mayores niveles de seguridad, control y eficiencia operativa. Los edificios de estratos 4, 5 y 6 suelen contar con estructuras administrativas más consolidadas, con administradores profesionalizados y consejos de administración activos, lo que facilita la evaluación, aprobación y seguimiento de proyectos tecnológicos. La decisión de compra del servicio recae en un cliente organizacional, conformado por el administrador del edificio, quien actúa como iniciador y evaluador técnico de la solución, y el consejo de administración, que desempeña el rol de órgano decisor colectivo encargado de aprobar la inversión y la contratación del servicio. Ambos actores comparten el interés por soluciones que contribuyan a la reducción de riesgos, la optimización de los costos operativos y la valorización del inmueble. Desde una perspectiva funcional, el cliente objetivo presenta necesidades claras asociadas a la gestión de la seguridad, tales como el control de accesos, la trazabilidad de eventos, la disminución de la dependencia de vigilancia presencial y la mejora en la eficiencia de los procesos administrativos. Estas necesidades se ven reforzadas por restricciones presupuestales y por la obligación de garantizar la continuidad y sostenibilidad del servicio.

5.2 Como el producto satisface esa necesidad específica.

La seguridad residencial es vista en Colombia como una necesidad imperiosa, no como un lujo. En el mercado inmobiliario colombiano un edificio con fallas de seguridad sufre una desvalorización inmediata. Los edificios deben protegerse contra modalidades específicas del país, como robo a residencias o fleteo en las entradas vehiculares. El residente en Colombia paga su cuota de administración buscando ante todo el “poder dormir tranquilo”. Si ocurre un incidente por negligencia en los protocolos (ej. un guardia que no estaba en su puesto o cámaras dañadas), el edificio y su administrador pueden enfrentar demandas civiles millonarias. Actualmente en la mayoría de los edificios el responsable de la seguridad es la empresa de vigilancia privada quien es supervisada por la Superintendencia de Vigilancia y Seguridad privada. Solo las empresas que cuenten con una licencia vigente pueden operar y estas deben contar con pólizas de responsabilidad civil para responder por posibles daños o hurtos. Los guardas de seguridad que la empresa contrata deben estar certificados por escuelas de capacitación autorizadas y deben renovar anualmente su certificado. El servicio de vigilancia que se presta al edificio se adapta según la necesidad, pero normalmente consta de un vigilante fijo que permanece en un puesto fijo, la portería principal, controlando accesos de personas y vehículos, recibiendo y registrando la correspondencia y monitoreando las cámaras del edificio. Adicional, dentro del servicio de vigilancia física, se incluye un supervisor. El supervisor conecta la empresa de vigilancia con el edificio, garantizando que el contrato de seguridad se cumpla con los estándares de calidad. El supervisor realiza visitas aleatorias al edificio para verificar el estado del vigilante, los registros en minuta, coordina que los cambios de turno se realicen a tiempo y realiza inspección a la infraestructura de tecnología (Sistema de cámaras y radios de comunicación). Cuando ocurre una emergencia, el supervisor apoya al vigilante y coordina con la Policía Nacional y los servicios de emergencia cualquier

reacción, y finalmente genera el informe de la novedad correspondiente. Normalmente los turnos del vigilante obedecen a una configuración denominada 2X2X2 para cubrir las 24 horas del día, la cual funciona de la siguiente manera: Dos días de turno diurno (6:00a.m a 6:00p.m 12 horas), dos días de turno nocturno (6:00p.m a 6:00a.m 12 horas) y dos días de descanso. Para esta configuración se requieren cuatro guardias. El servicio de vigilancia física depende en su mayoría de los costos de mano de obra los cuales en los últimos años se han visto afectados por el incremento del salario mínimo, la disminución de la jornada laboral y el recargo nocturno y dominical.

El aumento constante en los costos de vigilancia física debido a factores legales genera en el administrador una necesidad de poder encontrar un equilibrio entre la sostenibilidad financiera del edificio y la integridad de sus residentes. Existe una presión por optimizar los costos de vigilancia sin reducir los niveles de seguridad y una solicitud explícita de los copropietarios para modernizar la seguridad disminuyendo las horas activas del vigilante físico. Este desencadenante genera la búsqueda activa de una solución viable por parte del administrador, en donde solicita una solución que permita gestionar accesos al edificio de forma automática y trazable y automatizar la seguridad. El proveedor debe diseñar e implementar un sistema de automatización en seguridad que integre: control de accesos digital, videovigilancia con monitoreo remoto y registro y evidencia de eventos. El administrador valora modelos de negocio basados en esquemas de pago predecibles, preferiblemente bajo modalidades de servicio recurrente, que faciliten la planeación financiera y reduzcan la inversión inicial. Asimismo, privilegia proveedores que ofrezcan respaldo técnico, cumplimiento normativo y acompañamiento permanente, minimizando los riesgos operativos y legales asociados a la implementación de nuevas tecnologías. El administrador solicita que el sistema permita gestión desde una plataforma centralizada, para el

proceso de enrolamiento de los residentes y visitantes, como también la generación de reportes de acceso y novedades cuando lo requiera. El edificio debe operar con mayor control, menor riesgo y costos optimizados.

El administrador enfrenta una creciente complejidad operativa derivada del manejo simultáneo de la seguridad, la logística interna y la relación con múltiples actores, tales como residentes, visitantes, proveedores y personal de apoyo. En este escenario, la necesidad de contar con una plataforma centralizada de gestión se convierte en un elemento crítico para garantizar el control, la trazabilidad y la eficiencia en la operación del edificio. Desde la perspectiva del administrador, la seguridad no puede ser gestionada como un sistema aislado, sino como parte integral de la operación diaria del inmueble. La ausencia de una plataforma unificada genera fragmentación de la información, dependencia de registros manuales, pérdida de trazabilidad y mayores riesgos operativos y legales. En consecuencia, surge la necesidad de una solución tecnológica que permita centralizar la operación, el monitoreo y la generación de reportes, tanto para fines de seguridad como para la gestión logística. La plataforma centralizada se concibe como el núcleo operativo desde el cual el administrador puede supervisar y coordinar los procesos críticos del edificio. Esta plataforma integra los sistemas de automatización en seguridad con funcionalidades orientadas a la logística, permitiendo una visión unificada de la operación. Esta centralización reduce la carga operativa del administrador y mejora su capacidad de control y toma de decisiones. La plataforma debe permitir registrar y controlar el ingreso de proveedores de servicios como aseo, mantenimiento, jardinería y mensajería, asociando horarios y responsables. Esta funcionalidad facilita la supervisión del cumplimiento contractual y la verificación de la presencia del personal autorizado. El sistema debe gestionar la recepción y entrega de paquetes, generando registros automáticos que incluyen fecha, hora, destinatario y responsable. Esta

trazabilidad reduce pérdidas, reclamos y conflictos entre residentes y administración. La plataforma debe permitirle al administrador el poder controlar el uso de zonas comunes (salones sociales, parqueaderos de visitantes, áreas recreativas), asociando accesos, reservas y horarios. Adicionalmente, la plataforma debe permitir generar reportes sobre flujo de accesos, uso de recursos comunes, frecuencia de proveedores, incidentes y eventos relevantes. Estos reportes fortalecen la capacidad del administrador para justificar decisiones, optimizar procesos y presentar resultados ante el consejo de administración. Desde la perspectiva del administrador, la plataforma centralizada transforma la seguridad en un componente integrado de la logística y la operación del edificio, fortaleciendo el rol del administrador como gestor integral.

La necesidad se considera cubierta cuando se reduzca la dependencia de la vigilancia presencial, se mejora el control y la trazabilidad de accesos, se disminuyen los eventos de seguridad, se reducen los costos operativos, se incrementa la percepción de seguridad de los residentes, y el administrador puede demostrar gestión eficiente ante el consejo.

5.3 Diseño del Producto

El diseño del producto constituye el nexo crítico entre la visión estratégica de un modelo de negocio y su ejecución operativa en el mercado. El producto se concibe como la materialización de la propuesta de valor diseñada para resolver una problemática específica o satisfacer una necesidad identificada en los capítulos anteriores. El objetivo central de este apartado es detallar el proceso de configuración técnica y conceptual del producto. De acuerdo con Bill Aulet en el libro *La Disciplina de emprender*, el producto mínimo viable debe entenderse como la solución más simple y funcional que permite resolver la necesidad prioritaria del cliente objetivo, validando que este está dispuesto a utilizarla y pagar por ella. En este sentido, el producto mínimo viable

debe enfocarse en una necesidad crítica y frecuente, evitando funcionalidades extras que no sean esenciales para la validación del producto. Para el servicio de automatización residencial en seguridad, el producto se define a partir de la necesidad principal del administrador el cual incluye reducir o suprimir las horas de vigilancia física, controlar los accesos y asegurar el edificio, contar con una plataforma centralizada que le permita operar el sistema y generar trazabilidad verificable.

La principal necesidad se enfoca en poder disminuir las horas de vigilancia física, pero sin afectar la seguridad del edificio. El diseño del producto se debe centrar en el despliegue de un sistema de seguridad que permita ser monitoreado a través de una central de monitoreo en donde un operador de medios reaccione frente a este evento de seguridad. Para esta necesidad existen ya en el mercado diversas soluciones denominadas sistemas de alarma que permiten a través de sensores identificar cualquier tipo de intrusión al edificio. El producto debe contener esta solución como sistema principal, desde donde allí se desplieguen las demás soluciones que cubran las necesidades del administrador. Marcas reconocidas en Latinoamérica como Hikvision, Johnson Controls, e Intelbras, ofrecen dentro de su portafolio productos diseñados para proteger el edificio. Siguiendo el patrón de la empresa Carson Living, en donde su servicio integra productos de marcas existentes, el modelo de negocio planteado en este proyecto debe basarse en esta misma idea y no depender de un diseño y fabricación propios de un nuevo producto de seguridad, sino en integrar elementos ya existentes de diferentes marcas que permitan construir el nuevo producto. Normalmente un edificio de las características expuestas en el mercado objetivo consta de un acceso peatonal, uno vehicular, y un perímetro. Justamente para poder proteger un edificio y dotarlo de seguridad, se deben cubrir estas áreas vulnerables con sistemas de alarma. El sistema de alarma debe proteger solo estos accesos mencionados y no abarcar zonas internas en donde el tránsito de residentes genere falsas alarmas que confundan o induzcan al error al operador de

medios que monitorea el sistema. De acuerdo con lo anterior, el primer subproducto del servicio a ofrecer debe contener el diseño del sistema de alarma para cubrir solo los accesos descritos con sensores de movimiento, contactos magnéticos y cámaras de seguridad para la puerta principal y puerta vehicular, y con cámaras con detección de analítica para el perímetro. Estos sensores y cámaras envían su señal a un panel de alarma, y cuando es detectada una intrusión se envía una señal de alerta a la central de monitoreo para que el operador de medios la atienda a través de un software de monitoreo, verifique el evento, lo confirme a través de las cámaras, y reaccione con personal motorizado cuando se ratifique la intrusión. Las marcas mencionadas como Hikvision, Johnson Controls, e Intelbras, cuentan con esta solución por lo que el producto de este trabajo de aplicación debe integrarla dentro de su diseño.

La siguiente necesidad hace referencia al poder controlar los accesos de manera remota sin depender de un guarda físico. El producto debe volver a apoyarse en marcas que tienen esta solución para poder integrarlas dentro del proyecto. Marcas como Intelbras tienen dentro de su portafolio dispositivos denominados videoporteros cuya funcionalidad permite establecer comunicación con un operador de medios de la central de monitoreo. Siguiendo el ejemplo del edificio anterior, en donde solo se tiene una puerta peatonal y una puerta vehicular, el producto debe contemplar la instalación de videoporteros en cada una de estas puertas tanto en las salidas como en las entradas. La referencia del videoportero que se escoja para este producto debe tener la capacidad de brindar funciones que se acoplen como identificación facial, para que cuando el residente se acerque al videoportero el sistema reconozca su rostro y le permita el ingreso peatonal o vehicular, automatizando el acceso al residente sin depender de un tercero. El videoportero debe permitir la comunicación con una central de monitoreo para que el operador de medios pueda atender la llamada. Esta función le permite al operador de medios controlar el acceso de los

visitantes y domiciliarios a nivel peatonal y vehicular, controlando de manera remota la apertura de la puerta principal y vehicular a través del software de recepción de llamadas o portería virtual. La gestión de los accesos se centraliza en un dispositivo denominado controladora. Este equipo procesa las señales enviadas por los videoporteros o el software de portería virtual del operador para emitir un pulso eléctrico hacia el portón vehicular o el electroimán de la puerta peatonal, accionando así su apertura.

La tercera necesidad hace referencia a que el administrador del edificio pueda mostrar gestión sobre el sistema, por lo que se hace necesario tener una plataforma que centralice la información y que genere reportes de trazabilidad de todo lo acontecido. Es en esta parte del producto en donde se requiere el desarrollo personalizado de la plataforma para generar ese valor agregado y atractivo tanto para la administración como para el consejo de administración. La plataforma debe ser de entorno Web, en donde a través de un navegador de internet el administrador con un usuario y contraseña pueda ingresar al sistema, controlarlo y generar reportes. Para esto se hace necesario que los productos de las marcas escogidas, como son el sistema de alarma y los videoporteros, tengan la capacidad de integrarse a una plataforma de software sin restricciones. Hoy en día las marcas incluyen dentro de sus dispositivos protocolos API o Application Programming Interface, el cual es un conjunto de reglas y protocolos que permite a dos aplicaciones de software comunicarse e intercambiar datos entre sí. Actúa como un intermediario o puente, permitiendo que una aplicación utilice funciones o información de otra sin conocer su código interno. Es necesario que el sistema de alarma y videoporteros cuenten con esta opción para permitir el desarrollo de la plataforma centralizada, funciones hoy presentes en la marca Intelbras y Hikvision.

Teniendo los equipos reportando a una sola plataforma Web, el administrador puede gestionar de manera centralizada el sistema de seguridad y control de acceso en donde pueda visualizar el estado del sistema de alarma, consultar en tiempo real los eventos de intrusión, visualizar alarmas técnicas, acceder a las transmisiones de video, registrar acciones realizadas por la central de monitoreo, registrar tiempos de atención y respuesta ante alarmas, administrar perfiles de acceso como residentes, proveedores y contratistas, programar accesos por franjas horarias y control de entregas, y registrar de manera digital la recepción de encomiendas. Adicionalmente la plataforma debe permitir generar reportes con fecha y hora para tener indicadores de gestión que permitan medir la frecuencia de los eventos de seguridad, análisis de horarios y puntos críticos de acceso. Lo anterior le permite al administrador mostrar gestión frente al consejo de administración al controlar el desempeño del proveedor de monitoreo, optimizar los procesos diarios y tener información para justificar ajustes operativos o inversiones futuras.

Teniendo en cuenta lo anterior, el producto se compone de tres sistemas: El sistema de alarma, el sistema de control de acceso y la plataforma que centraliza la información y operatividad de los dos sistemas anteriores. Para definir el producto con mayor detalle se requiere establecer el recurso requerido en cada sistema.

El sistema de alarma es monitoreado por un operador de medios que opera desde una central y está atento a un evento de alarma que se genera a un software de monitoreo una vez activados los sensores o las cámaras de analítica. Una vez se genere el evento, el operador debe verificar las cámaras del edificio y de confirmarse la intrusión debe comunicarse con un supervisor motorizado para que se dirija al lugar del edificio y atienda la novedad. El primer sistema requiere de un operador de medios de seguridad, un supervisor motorizado, medios de comunicación,

equipo de cómputo, software de monitoreo de recepción de alarmas, servidores e infraestructura de red, y un lugar físico en donde alojar la infraestructura de tecnología y la central de monitoreo.

Para el sistema de control de acceso se requiere otro operador de medios que se encuentra también en una central, pero con un perfil y función diferente. Este operador recibe una llamada al software de portería virtual desde el videoportero instalado en los accesos del edificio. Esta llamada es realizada por el mensajero, domiciliario o visitante. El perfil que tiene este operador obedece a uno de servicio al cliente, en donde tiene que responder al llamado e interactuar con la persona para confirmar con el residente o administrador la respectiva autorización de acceso. Este segundo sistema requiere de un operador de medios, equipo de cómputo y el software de portería virtual.

El tercer componente del sistema hace referencia a la plataforma central del producto, cuya responsabilidad es de un equipo de ingenieros de sistemas que diseñan, desarrollan, mantienen en operación y prestan soporte a la plataforma que integra y controla el sistema, como también genera los reportes e indicadores respectivos.

El sistema debe ser instalado y mantenido por un equipo de técnicos que se especializan en la instalación de equipos de seguridad electrónica. Los técnicos obedecen al llamado de instalación y se presentan en el edificio para instalar el sistema de alarma y videoporteros. Una vez instalado el sistema, se realizan las pruebas respectivas, probando las activaciones de los sensores y cámaras, generando eventos a la central de monitoreo y estableciendo comunicación bidireccional con el operador de medios de portería virtual. Los técnicos también deben prestar el servicio de mantenimiento preventivo y correctivo garantizando el buen funcionamiento del sistema.

Hasta el momento el producto define componentes que fueron investigados en capítulos anteriores con empresas que ya ofrecen el servicio. Se ha mencionado que el producto contemple

el desarrollo de una plataforma central que puede llegar a ser personalizada con base en las necesidades de la administración, pero por ahora no se puede definir con exactitud en donde radica la diferencia de este producto con lo ofertado por las demás empresas. Bill Aulet habla de la esencia que debe tener cada organización para poder plantear la diferencia competitiva, por lo que la define como la única cosa que la organización debe hacer mejor que nadie y la cual debe ser muy difícil de copiar. Tener una definición clara de la esencia permitirá construir y reforzar esa ventaja competitiva por la cual este producto se diferencie de los demás. Esta esencia no radica en los componentes físicos del sistema de seguridad, los cuales ya existen en el mercado y son ofrecidos por múltiples proveedores, sino en la capacidad de integrar, operar y traducir dichos componentes en valor tangible para la administración del edificio. Las soluciones actuales del mercado se concentran principalmente en la instalación y operación de dispositivos de seguridad, tales como alarmas, cámaras y videoporteros, cuya propuesta de valor se limita a la detección y reacción ante eventos de riesgo. En contraste, el producto propuesto trasciende la seguridad como fin en sí mismo y la integra dentro de un ecosistema de gestión, donde la información generada por los dispositivos se transforma en insumos estratégicos para la administración del edificio. A diferencia de plataformas genéricas de monitoreo o control de accesos, el producto se apoya en la capacidad de integración abierta mediante APIs, lo que permite conectar múltiples marcas y tecnologías sin dependencia de un fabricante específico. Esta arquitectura posibilita la adaptación a las particularidades operativas de cada edificio para la evolución progresiva de la plataforma sin rediseñar el sistema físico. La plataforma convierte eventos operativos en información estructurada, generando reportes, indicadores y evidencia objetiva de gestión. Este enfoque transforma la seguridad en una fuente de valor administrativo, al permitir justificar decisiones ante el consejo de administración, optimizar recursos humanos y financieros, y mejorar la gobernanza

del edificio. Esta orientación permite que el sistema no solo proteja el edificio, sino que también facilite la gestión administrativa, posicionando la plataforma como una herramienta indispensable para el ejercicio del rol del administrador. La esencia del producto se define como la capacidad de convertir sistemas de seguridad existentes en una plataforma integral de gestión administrativa y operativa del edificio, orientada a la toma de decisiones, la trazabilidad y la optimización de recursos, mediante un desarrollo de software profundamente alineado con las necesidades reales del administrador de propiedad horizontal. La experiencia del administrador debe ser tan clara que la plataforma se convierta en su herramienta diaria de trabajo, y no en un sistema adicional de consulta ocasional.

5.4 Estructuración de los canales de Venta y distribución.

En el modelo de negocio propuesto, los canales de venta deben ser coherentes con la naturaleza del producto y con el perfil del cliente objetivo, caracterizado por procesos de decisión racionales, colegiados y orientados a la mitigación de riesgos. El diseño de los canales de venta no se limita a la transacción comercial, sino que debe cubrir el ciclo completo de relación con el cliente, desde la generación de la oportunidad hasta la operación recurrente del servicio. El canal principal de comercialización del producto debe ser la venta directa de tipo consultivo, orientada al segmento B2B, específicamente a administradores de propiedad horizontal y consejos de administración. La naturaleza del producto, caracterizada por su alta complejidad técnica y su impacto crítico en la operatividad y seguridad de la infraestructura, exige un modelo de comercialización especializado. Dado que la decisión de adquisición no recae en un individuo, sino que se gestiona de manera colegiada, y considerando que implica una inversión recurrente a largo plazo, el canal masivo o transaccional resulta insuficiente. En su lugar, se requiere un proceso

de venta consultiva que integre un diagnóstico preciso de las necesidades del edificio, la exposición de beneficios administrativos y una sólida sustentación técnica y económica. Este despliegue es liderado por un equipo comercial experto, apoyado por ingenieros de preventa en el diseño conceptual que aseguran la validez institucional de la propuesta.

El proceso comercial del canal directo se inicia con una fase de prospección dirigida, enfocada estratégicamente en edificios residenciales de estratos 4,5 y 6 que operan bajo esquemas de vigilancia tradicional con altos costos operativos. Una vez establecido el contacto con los administradores, se procede a un diagnóstico técnico-administrativo integral. En esta etapa, se realiza el levantamiento de información sobre accesos y perímetros, permitiendo identificar puntos críticos de riesgo y analizar la estructura de costos asociada a la seguridad física. Este análisis previo es fundamental para construir una propuesta de valor que no solo prometa la reducción de gastos, sino que también posicione a la plataforma como una herramienta de gestión esencial para la trazabilidad y la generación de indicadores operativos.

Finalmente, la consolidación del proceso requiere una etapa de validación ante el consejo de administración, donde se resuelven objeciones sobre confiabilidad y se presentan los beneficios en términos de gobernanza y eficiencia financiera. Al tratarse de una decisión colectiva, el soporte técnico y conceptual brindado en estas sesiones es determinante para el avance hacia el cierre. La fase de formalización contractual concluye el ciclo mediante la firma de acuerdos de prestación de servicios recurrentes, en los cuales se definen con precisión los niveles de servicio (SLA) y los esquemas de mantenimiento. Este enfoque asegura una relación técnica y comercial sostenible que garantiza la continuidad operativa de la solución implementada.

El modelo de negocio propuesto fundamenta su canal de distribución en una tercerización controlada de la instalación y el soporte del hardware, integrando sistemas de alarma y control de

accesos mediante alianzas estratégicas con firmas especializadas en seguridad electrónica. Este mismo enfoque lo aplica la empresa Carson Living en su cadena de abastecimiento, en donde establece alianzas con distribuidores regionales que tienen red de instaladores y canales de soporte, facilitando la expansión internacional y adaptación a normativas locales. Esta decisión estratégica se sustenta en la teoría de las capacidades centrales, la cual sugiere que una organización debe concentrar sus recursos en aquellas actividades que constituyen su esencia competitiva, delegando funciones estandarizadas que no generan una diferenciación sostenible. En este contexto, dado que la instalación y el mantenimiento físico de dispositivos de seguridad son actividades ampliamente normalizadas en el mercado, la ventaja competitiva no reside en el componente tangible, sino en la integración, operación y explotación de datos a través de la plataforma central. Por consiguiente, la externalización del componente físico permite una optimización de la eficiencia operativa sin comprometer la propuesta de valor del producto.

Este canal de distribución se estructura bajo un esquema híbrido donde la empresa matriz conserva la soberanía sobre el diseño de la solución, la administración de la plataforma, la operación de la central de monitoreo y la relación estratégica con el cliente. Paralelamente, las empresas instaladoras aliadas asumen la ejecución técnica en campo, que abarca desde la implementación de videoporteros y sistemas de alarma hasta la realización de pruebas iniciales y el mantenimiento preventivo y correctivo. Para garantizar la cohesión del servicio, estos aliados operan bajo estrictos protocolos y lineamientos definidos por la compañía, asegurando que la ejecución técnica sea homogénea y se alinee con los estándares de calidad institucional, independientemente del actor que realice la intervención física.

Para mitigar los riesgos inherentes a la delegación operativa, el modelo incorpora mecanismos de control rigurosos que salvaguardan la experiencia del cliente. La gestión del canal

tercerizado exige la certificación técnica de los aliados, el cumplimiento de manuales de procedimientos estandarizados y la adhesión a acuerdos de nivel de servicio (SLA) que regulan los tiempos de respuesta y la calidad del soporte. Asimismo, la implementación de auditorías técnicas periódicas y la integración obligatoria de todo hardware a la plataforma central aseguran que el control estratégico y operativo permanezca centralizado. De esta manera, se neutralizan riesgos potenciales como la pérdida de calidad o la inconsistencia en la prestación del servicio mediante una supervisión remota y una normativa contractual sólida.

Finalmente, la adopción de este canal de distribución aporta beneficios significativos en términos de escalabilidad y flexibilidad financiera. Al prescindir de equipos técnicos internos, la organización reduce drásticamente sus costos fijos laborales y logísticos, permitiendo un crecimiento geográfico acelerado y una mayor capacidad para atender múltiples proyectos simultáneamente. Este enfoque no solo refuerza el carácter multimarca y la flexibilidad tecnológica del sistema, sino que permite a la empresa enfocar su capital intelectual en la evolución constante de la plataforma y el fortalecimiento de la gobernanza de seguridad. En conclusión, el modelo se consolida como un ecosistema colaborativo que armoniza la especialización técnica externa con el liderazgo estratégico interno, garantizando una solución robusta, escalable y centrada en la generación de valor.

La definición estratégica sobre la ubicación de la venta y la gestión de inventarios de hardware como el sistema de alarma y los videoporteros constituye una decisión crítica para la sostenibilidad y escalabilidad del modelo de negocio. Al analizar las alternativas, se observa que centralizar la propiedad del inventario en la compañía garantiza un control técnico absoluto y uniformidad en los componentes; no obstante, esta práctica demanda una inmovilización significativa de capital de trabajo y desvía el enfoque organizacional hacia la gestión logística y

de suministros. Por el contrario, delegar estas funciones enteramente en las empresas instaladoras aliadas optimiza la eficiencia financiera y transfiere los riesgos de obsolescencia técnica al ejecutor, aunque introduce la posibilidad de una pérdida de control sobre la calidad y homogeneidad del sistema. Ante este dilema, la propuesta más coherente con la esencia del producto es la adopción de un modelo híbrido controlado, donde la empresa propietaria actúa como el ente certificador y normativo, mientras que los aliados operan como el brazo logístico y comercial del hardware.

En este esquema híbrido, la organización central asume la responsabilidad de definir, certificar y homologar las marcas y referencias compatibles con su plataforma, asegurando que cualquier dispositivo integrado cumpla con los estándares de seguridad y rendimiento exigidos. Bajo esta premisa, las empresas instaladoras aliadas gestionan de forma autónoma la compra, venta e inventario del hardware, facturándolo directamente al cliente como un componente del proyecto de instalación inicial. Esta estructura permite que la empresa propietaria del producto se desvincule de las complejidades de la rotación de inventarios y la dependencia de proveedores físicos, concentrando sus esfuerzos en el desarrollo de la plataforma central y la prestación de servicios recurrentes, que representan el verdadero núcleo de valor del negocio.

La justificación de este modelo se fundamenta en la protección de la ventaja competitiva y la escalabilidad operativa. Siguiendo principios de estrategia empresarial, se reconoce que la esencia del negocio no reside en la comercialización de equipos tangibles, sino en la inteligencia de la integración y la gestión de la información. Al trasladar el riesgo financiero de la tenencia física al instalador, la empresa protege su flujo de caja y permite que el crecimiento no se vea limitado por la capacidad de financiar inventarios, sino por la habilidad de expandir la red de servicios y operar la plataforma. Este enfoque otorga una notable flexibilidad tecnológica,

permitiendo que el sistema sea multimarca y se adapte a las disponibilidades locales o cambios en el mercado sin comprometer la integridad de la solución centralizada.

Para asegurar que esta delegación no erosione la experiencia del cliente ni la confiabilidad del sistema, es imperativo establecer mecanismos de control rigurosos. Estos incluyen la creación de listados de hardware certificado, protocolos de instalación estandarizados y auditorías técnicas periódicas que verifiquen la correcta integración con la plataforma. Contractualmente, se debe garantizar que el hardware sea percibido únicamente como un habilitador del servicio, asegurando que la relación de largo plazo con el cliente se mantenga bajo la órbita de la empresa propietaria. En síntesis, el modelo redefine la estructura de ingresos, transformando la venta transaccional de equipos en un modelo de servicio gestionado. Este enfoque maximiza la rentabilidad al priorizar las suscripciones y el monitoreo, consolidando una arquitectura de negocio ligera en activos, pero robusta en control estratégico y generación de valor administrativo.

En la siguiente imagen se presenta el diseño del producto para automatización residencial

Figura 2.

Diseño del producto de automatización residencial.



Nota: Generada mediante IA (Gemini)

5.5 Estrategia para capturar valor a través de la venta

Teniendo en cuenta el modelo de “tensores clave” para el diseño de la estrategia organizacional en donde se proponen indicadores de capacidades distintivas, medición, talento, estructura, y asignación de poder, se establece el cómo se adapta el producto descrito con cada uno de estos indicadores.

El tensor dominante del producto corresponde a la capacidad distintiva, entendida como la habilidad organizacional para integrar, operar y transformar sistemas de seguridad existentes en una plataforma integral de gestión administrativa. A diferencia de las soluciones tradicionales disponibles en el mercado, cuya propuesta de valor se limita a la instalación y operación de dispositivos de seguridad, el producto propuesto se diferencia por su capacidad de orquestar múltiples tecnologías multimarca mediante interfaces de programación de aplicaciones (API). En

este sentido, la diferenciación no radica en los dispositivos de seguridad, los cuales son ampliamente accesibles, sino en el conocimiento acumulado para convertir eventos operativos en información estructurada, trazable y relevante para la gestión administrativa. Esta capacidad resulta difícil de imitar, dado que exige una combinación de competencias técnicas, entendimiento del contexto normativo de la propiedad horizontal y alineación con las necesidades reales del administrador.

El producto se encuentra diseñado bajo un enfoque de gestión, donde la medición constituye un componente central de la propuesta de valor. La plataforma central permite capturar, estructurar y analizar información derivada de la operación del sistema de seguridad y control de accesos, habilitando la generación de indicadores objetivos y verificables. Entre los principales indicadores se incluyen la frecuencia y tipología de eventos de seguridad, los tiempos de atención y respuesta ante alarmas, el desempeño de la central de monitoreo y los patrones de acceso por franjas horarias. Estos indicadores no solo facilitan el control operativo, sino que se convierten en insumos estratégicos para la toma de decisiones y la rendición de cuentas ante el consejo de administración. De esta manera, la medición se integra al ejercicio de gobernanza del edificio.

El funcionamiento y la evolución del producto dependen de un esquema de talento especializado, alineado con las exigencias técnicas y operativas del modelo. Este tensor se materializa en la articulación de perfiles diferenciados, entre los cuales se destacan los ingenieros de sistemas responsables del desarrollo y mantenimiento de la plataforma central, los operadores de medios encargados de la atención de eventos de seguridad, los operadores de portería virtual con orientación al servicio al cliente, y los ingenieros de preventa que soportan el proceso comercial. La ventaja competitiva asociada a este tensor se fundamenta en la capacidad del equipo

de tecnología para traducir necesidades administrativas en soluciones digitales y en la capacidad de los operadores de atender las demandas operativas.

El producto se apoya en una estructura organizacional ligera en activos físicos y robusta en control estratégico, coherente con los principios de concentración en las capacidades centrales. La organización conserva internamente las funciones críticas asociadas al diseño de la solución, la operación de la plataforma, la gestión de la central de monitoreo y la relación con el cliente, mientras que externaliza de manera controlada las actividades estandarizadas de instalación y mantenimiento de hardware. Esta estructura híbrida permite escalar el modelo de negocio sin un crecimiento proporcional de los costos fijos. De este modo, la estructura organizacional se configura como un habilitador de la escalabilidad y la sostenibilidad del producto en el largo plazo.

El diseño del producto redefine la asignación de poder, estableciendo una clara separación entre control estratégico y ejecución operativa. La empresa propietaria del producto mantiene la soberanía sobre la plataforma, los estándares tecnológicos, la certificación de hardware y la relación de largo plazo con el cliente, mientras que los proveedores e instaladores operan bajo un marco normativo y contractual claramente delimitado. Así mismo, el administrador del edificio adquiere un mayor grado de autonomía al disponer de información en tiempo real, reportes estructurados y evidencia de la gestión realizada.

En conjunto, los factores clave del producto configuran una arquitectura estratégica coherente, en la cual las capacidades distintivas actúan como eje central, los indicadores de medición habilitan una gestión basada en evidencia, el talento sostiene la integración tecnológica, la estructura organizacional permite la escalabilidad y la asignación de poder garantiza la gobernanza del sistema. Esta alineación asegura que el producto no solo responda a una necesidad

operativa de seguridad, sino que se consolide como una herramienta estratégica para la administración eficiente y sostenible en edificios residenciales.

Teniendo en cuenta la estrategia, se debe definir como la compañía debe concebir el modelo de venta del producto para poder generar valor. El producto se concibe y se ofrece al cliente final como un modelo CAPEX + OPEX, lo anterior teniendo en cuenta que el producto lo integran tres grandes subproductos que hemos denominado sistema de alarma, control de acceso y plataforma central. Los dos primeros subproductos lo componen el hardware de la solución, mientras que el tercero lo integra el software. El servicio prestado al cliente debe verse como un todo en donde una vez instalado el hardware, el cliente percibe el servicio a través de un canal de operación recurrente compuesto por una central de monitoreo de alarmas, central de portería virtual, plataforma web de gestión administrativa y soporte técnico y de mantenimiento.

El modelo CAPEX lo integra el hardware que comprende los dos primeros subproductos compuestos por el sistema de alarma y los videoporteros. La estructura del gasto de capital, o CAPEX, para la implementación del sistema se fundamenta en tres pilares esenciales que garantizan la puesta en marcha técnica y operativa de la solución. El primer bloque corresponde al hardware base, el cual comprende la adquisición de todos los dispositivos físicos debidamente homologados y certificados que constituyen la infraestructura técnica necesaria para el funcionamiento del ecosistema de seguridad. Complementariamente, se integra el componente de instalación, que abarca tanto la mano de obra especializada para el montaje físico y la canalización de los sistemas, como la configuración inicial requerida para habilitar los dispositivos en el entorno específico del edificio. Más allá del despliegue físico, el CAPEX contempla el proceso de integración, una etapa crítica orientada a la parametrización exhaustiva de la plataforma central y la ejecución de pruebas de conectividad que aseguren la interoperabilidad entre el hardware y el

software. Este enfoque integral del CAPEX asegura que el desembolso inicial no solo cubra la adquisición de activos, sino que garantice una transición fluida hacia la fase operativa del modelo de negocio. La gestión de la variabilidad de precios en un modelo de negocio que integra múltiples proveedores de hardware exige una posición estratégica de la venta de activos. El principio rector de esta estrategia establece que el cliente no adquiere dispositivos físicos, sino un resultado operativo y administrativo centrado en la seguridad, la trazabilidad y la eficiencia. Por consiguiente, el precio de la solución no se construye mediante la agregación de costos de componentes individuales, sino en función del valor generado por la reducción de costos en vigilancia física y la optimización de los procesos de acceso y seguridad. Este enfoque permite trasladar el foco de la negociación desde la comparación técnica de marcas hacia el impacto económico y funcional que la plataforma ofrece al edificio. Para operativizar esta visión, se propone una arquitectura de precios estructurada en donde se conceptualiza el hardware como un habilitador técnico organizado en paquetes predefinidos según el tamaño y la complejidad de la infraestructura. Al presentar el hardware como una solución empaquetada, el cliente percibe un valor de referencia uniforme, permitiendo que la variación de costos internos entre diferentes marcas homologadas sea absorbida dentro de la estructura de margen del instalador, sin afectar la propuesta económica final. La homogeneización del costo se refuerza mediante un mecanismo de precio objetivo, donde la compañía define el valor de la solución basándose en parámetros como la disposición a pagar, los beneficios financieros proyectados para el cliente y el benchmark del mercado. Bajo este esquema, el instalador aliado asume la responsabilidad de seleccionar el hardware dentro de un listado certificado, gestionando las fluctuaciones de costo mediante el uso de bandas de precio internas. Este sistema de subsidio cruzado permite que proyectos con componentes de menor costo compensen a aquellos con requerimientos más onerosos,

manteniendo la rentabilidad global del ecosistema. Para garantizar el cumplimiento de esta política, se establecen contratos marco que impiden a los instaladores desagregar precios por marca, transformándolos en ejecutores eficientes subordinados a la estrategia comercial central. Finalmente, la transparencia hacia el cliente se logra mediante una narrativa comercial que prioriza la inversión inicial de implementación, evitando cotizaciones detalladas por dispositivo. Esta estructura no solo facilita la escalabilidad y protege los márgenes operativos, sino que también refuerza la plataforma como el núcleo de valor del negocio. Al alinear la estrategia de precios con la esencia del producto, se reducen las fricciones en el proceso de venta, consolidando un modelo de negocio robusto frente a la volatilidad de los proveedores de hardware.

El modelo OPEX es el valor recurrente que cancela el cliente por el servicio, el cual está compuesto por el servicio de seguridad operado a través de la central de monitoreo de alarmas, el servicio de control de acceso operado por la central de portería virtual, la plataforma web de gestión administrativa y el soporte técnico y de mantenimiento. Este esquema comienza con la operación remota, que integra el capital humano especializado encargado del monitoreo constante y la atención inmediata de eventos tanto de seguridad como de control de acceso. Complementariamente, el componente de la plataforma central se basa en una infraestructura tecnológica, el desarrollo de la solución la cual abarca el licenciamiento de software y los servicios de hosting en la nube hasta la implementación de protocolos avanzados de ciberseguridad. Estos elementos aseguran que el ecosistema digital escale conforme a las demandas del mercado tanto en funcionalidad como en infraestructura. La integración del mantenimiento tercerizado dentro del esquema de gastos OPEX se fundamenta en el principio de responsabilidad unificada, donde la compañía actúa como el único interlocutor y responsable frente al cliente final. Bajo esta premisa, el usuario no gestiona una multiplicidad de proveedores individuales, sino que contrata un servicio

integral. Esta estructura implica que el mantenimiento de hardware no se factura de forma independiente por el aliado técnico, sino que la empresa matriz adquiere dicho servicio como un insumo operativo, consolidándolo dentro de una factura única mensual. De este modo, se garantiza que el cliente perciba una solución cohesionada, mientras la organización conserva el control sobre la experiencia del usuario y la calidad del soporte técnico. Para operativizar esta relación, el mantenimiento se ubica técnicamente como un subcomponente del OPEX, lo que permite estandarizar la oferta económica independientemente del aliado instalador que ejecute la labor. La relación con las empresas instaladoras se formaliza a través de un contrato marco que establece acuerdos de nivel de servicio (SLA) estrictamente definidos, tarifas estándar y penalizaciones por incumplimiento. Dentro de este marco, el mantenimiento preventivo se gestiona mediante un esquema de tareas programadas, tales como la revisión de videoporteros, la verificación de cámaras y pruebas del sistema de alarmas, cuyo costo se proratea mensualmente. Este enfoque transforma el gasto por evento en un flujo de caja previsible, eliminando las fluctuaciones financieras tanto para el edificio como para la empresa integradora. En cuanto al mantenimiento correctivo, el modelo propone una segmentación clara en dos niveles para proteger la sostenibilidad del negocio. El Nivel 1, incluido íntegramente en el OPEX recurrente, abarca el diagnóstico remoto, reconfiguraciones de software y desplazamientos técnicos que no impliquen la sustitución de componentes físicos. El Nivel 2, se reserva para casos que requieren el reemplazo de hardware, ampliaciones del sistema o reparaciones por mal uso, situaciones que se cotizan como una inversión de capital (CAPEX) adicional. Esta distinción permite que la tarifa operativa cubra la estabilidad del sistema, mientras que los eventos extraordinarios de infraestructura son gestionados de manera independiente, evitando la erosión del margen operativo por imprevistos técnicos mayores. Finalmente, la estrategia de homogeneización se garantiza mediante un proceso

de certificación de instaladores, donde solo aquellas empresas que acepten el tarifario estandarizado y demuestren capacidad para cumplir con los SLA pueden formar parte del ecosistema. La compañía no traslada el costo puro del mantenimiento, sino que aplica un margen estratégico justificado por la gestión del proveedor, el control de calidad y la asunción del riesgo contractual. Este modelo no solo asegura un control total sobre el pricing y una reducción drástica de la fricción comercial, sino que permite una escalabilidad acelerada. Al alinear el mantenimiento con la esencia del producto, la organización se consolida no como un instalador, sino como un gestor tecnológico que garantiza la continuidad operativa de la seguridad del edificio. Es imperativo que la fijación de precios en este componente (OPEX) se realice bajo una lógica de análisis de costo-beneficio, donde el valor mensual del servicio se compare directamente con el costo evitado de la vigilancia física tradicional. Al posicionar la solución como una alternativa que optimiza los recursos financieros del edificio sin comprometer la seguridad, se genera una propuesta de valor altamente competitiva. Este enfoque garantiza que el OPEX no sea percibido como un gasto administrativo adicional, sino como una inversión estratégica que genera ahorros tangibles y mejoras sustanciales en la eficiencia del inmueble.

Con base en lo anterior se propone el modelo CANVAS fundado en la propuesta de valor y diseño del producto el cual se detalla en la siguiente tabla:

Tabla 1.

Formato Canvas para la empresa de automatización en seguridad residencial.

ITEM	Descripción
Propuesta de valor	Plataforma integral que transforma sistemas de seguridad electrónica existentes (alarmas, control de accesos, portería remota) en una herramienta de gestión administrativa y operativa del edificio. Permite reducir la dependencia de vigilancia física, optimizar costos, fortalecer la gobernanza y soportar la toma de decisiones mediante información trazable e indicadores.
Segmentos de clientes	Administradores de propiedad horizontal y consejos de administración de edificios residenciales, principalmente de estratos 4, 5 y 6. Dirigido a quienes operan bajo esquemas tradicionales de vigilancia física y requieren optimizar costos y control operativo.
Canales	Canal directo de venta consultiva B2B basado en diagnóstico técnico-administrativo, diseño conceptual y validación ante el consejo. Canal de distribución híbrido mediante aliados instaladores certificados.
Relación con los clientes	Relación de largo plazo mediante contratos de prestación de servicios recurrentes con acuerdos de nivel de servicio (SLA). Incluye soporte técnico continuo, acompañamiento operativo y entrega periódica de reportes.
Fuentes de ingresos	Ingresos recurrentes por suscripción a la plataforma, monitoreo de alarmas y portería virtual. Ingresos puntuales por diseño e implementación inicial. La venta de hardware es gestionada por aliados.
Recursos clave	Plataforma tecnológica central, conocimiento en integración multimarca, equipo de ingenieros, infraestructura de central de monitoreo y protocolos operativos.
Actividades clave	Desarrollo y mantenimiento de software, integración de sistemas de seguridad, operación de la central de monitoreo y gestión de indicadores.
Socios clave	Proveedores de tecnología, fabricantes con integración abierta, empresas instaladores certificadas y proveedores de infraestructura tecnológica.
Estructura de costos	Costos de desarrollo de software, infraestructura tecnológica, personal especializado y operación de la central.

En la siguiente figura se puede observar el modelo de negocio en el formato gráfico de CANVAS

Figura 3.

Formato gráfico Canvas de la empresa de automatización en seguridad residencial



Nota: Generada mediante IA (Gemini) con base en Osterwalder y Pigneur (2010).

5.6 Modelo de Escalabilidad a Futuro

Se debe tener en cuenta un plan de escalabilidad, evolución tecnológica e innovación del modelo de negocio para garantizar la continuidad del negocio. Lo que se va a describir en las siguientes líneas no se contempla dentro del producto mínimo viable descrito en los apartados anteriores, pero si debe tenerse en cuenta dentro del modelo como objetivo a mediano plazo para garantizar la expansión y continuidad del negocio. El modelo de escalabilidad se basa en tres pilares fundamentales los cuales se relacionan a continuación: la integración de la inteligencia artificial para el monitoreo de alarmas, optimizar la plataforma central con base en inteligencia

artificial, incluir una aplicación para el residente en donde tenga interacción con la administración y en donde pueda acceder a servicios adicionales.

El plan de escalabilidad del modelo de negocio se fundamenta en una transición estratégica hacia la automatización inteligente, con el objetivo de desacoplar el crecimiento de la organización de la expansión intensiva de su planta de personal. Esta evolución tecnológica se centra en la integración de la inteligencia artificial (IA) como motor de eficiencia en el monitoreo de alarmas, permitiendo que la plataforma transite de un esquema reactivo a uno preventivo y predictivo. Mediante el despliegue de algoritmos de aprendizaje profundo para la clasificación automática de eventos, el sistema logra filtrar con precisión las falsas alarmas y las alertas menores, dirigiendo la atención del operador de medios exclusivamente hacia incidentes críticos confirmados. Esta optimización le permite a la IA no solo incrementar drásticamente la capacidad de respuesta y la efectividad operativa, sino que permite a la central de monitoreo escalar su cobertura a un mayor número de edificios sin degradar la calidad del servicio con una estructura de costos optimizada.

La plataforma central se robustece mediante la incorporación de capacidades analíticas avanzadas que transforman la gestión administrativa del edificio. La inteligencia artificial aplicada a la plataforma central permite el procesamiento de grandes volúmenes de datos para generar indicadores de desempeño en tiempo real, predicciones de riesgos zonales y optimización de recursos compartidos. Bajo esta perspectiva, la plataforma deja de ser una herramienta de control pasiva para convertirse en un ecosistema de gestión inteligente que asiste a los consejos de administración en la toma de decisiones estratégicas. Al estandarizar estos procesos a través de la IA, el modelo consolida una ventaja competitiva basada en la inteligencia del software. Es aquí en donde a futuro se puede ofrecer al cliente un plan premium que contemple un módulo adicional en

la plataforma, que incorpore estas capacidades de analítica avanzada con identificaciones predictivas y de gestión de riesgos.

Por otra parte, el modelo se expande a través del desarrollo de una aplicación móvil integral dirigida al residente, diseñada para centralizar la interacción con la administración y fomentar la autogestión de servicios. Esta interfaz no solo facilita la comunicación bidireccional y el control de accesos, sino que evoluciona hacia un mercado de servicios adicionales (marketplace) donde los usuarios pueden solicitar asistencia, servicios de limpieza o reparaciones locativas directamente desde la plataforma. La integración de asistentes virtuales y sistemas de recomendación basados en el comportamiento del usuario permite personalizar la experiencia del residente, elevando el valor percibido del producto y abriendo nuevas vías de monetización recurrente.

Este plan de escalabilidad redefine la esencia del negocio al posicionar a la empresa como un proveedor de servicios tecnológicos de alto valor y no simplemente como un integrador de sistemas de seguridad. La sinergia entre el monitoreo asistido por inteligencia artificial, el fortalecimiento analítico de la plataforma central y la digitalización de la experiencia del residente asegura la sostenibilidad financiera a largo plazo. Al reducir los costos fijos asociados a la operación humana y maximizar la captura de valor a través de servicios digitales, la organización se prepara para un crecimiento exponencial capaz de adaptarse a las demandas dinámicas del mercado residencial moderno.

La consolidación de un departamento de Tecnologías de la Información (TI) robusto y permanente constituye el eje fundamental para la ejecución del plan de escalabilidad, especialmente en un modelo de negocio donde la ventaja competitiva se desplaza desde la simple instalación de hardware hacia el desarrollo y operación continua de una plataforma inteligente. A

diferencia de los modelos de seguridad tradicionales, esta propuesta fundamenta su diferenciación en la capacidad de procesar datos y automatizar respuestas mediante inteligencia artificial, lo que transforma al área de TI de una unidad de soporte técnico en un componente estratégico esencial para la creación de valor. La soberanía tecnológica sobre la arquitectura del sistema es indispensable para mitigar riesgos asociados a la propiedad intelectual y la dependencia de terceros, permitiendo una capacidad de respuesta y adaptación que garantiza la sostenibilidad de la ventaja competitiva en el largo plazo. El rol de este departamento es transversal y se manifiesta en tres dimensiones críticas del producto: la integración, la operación y la innovación. En la fase de integración, TI asegura la interoperabilidad entre diversos fabricantes de hardware mediante la implementación de interfaces de programación de aplicaciones (APIs), normalizando el flujo de datos proveniente de alarmas y sistemas de acceso. Simultáneamente, en la capa de operación, el área garantiza la alta disponibilidad y ciberseguridad de la infraestructura, gestionando servidores y redes bajo estándares que permiten el escalamiento del sistema. Finalmente, la dimensión de innovación se materializa en el entrenamiento de modelos de machine learning y el desarrollo de la aplicación móvil para residentes, transformando la plataforma en un ecosistema digital dinámico que evoluciona según las necesidades del mercado. La ciberseguridad se posiciona como una función crítica para proteger la información sensible de las copropiedades, estableciendo protocolos de defensa que son inherentes al diseño del software. La operatividad de estas funciones exige una estructura organizacional mínima compuesta por perfiles altamente especializados, tales como arquitectos de software y desarrolladores de plataformas. La inclusión de ingenieros de datos y expertos en ciberseguridad desde las etapas tempranas del proyecto evita la acumulación de deuda técnica y asegura que el sistema sea capaz de soportar un crecimiento exponencial. Esta capacidad interna permite que el incremento en el número de edificios gestionados no derive en

un aumento proporcional de los costos operativos, ya que la automatización y la reducción de falsas alarmas facilitan economías de escala donde un solo operador puede supervisar múltiples infraestructuras con mayor efectividad. En conclusión, la ausencia de un departamento de TI propio comprometería la viabilidad del modelo al generar una vulnerabilidad estratégica frente a fallos de seguridad y obsolescencia tecnológica. La inversión en talento humano y recursos técnicos internos se justifica por su papel determinante en la optimización del monitoreo y la mejora de la experiencia del usuario a través de servicios digitales. Por tanto, el departamento de TI debe entenderse como el núcleo competitivo de la empresa, responsable de transformar los datos de seguridad en inteligencia operativa y valor administrativo, consolidando así un modelo de negocio ligero en activos físicos pero robusto en capital intelectual y capacidad de innovación.

Este plan de escalabilidad a futuro no solo garantiza la sostenibilidad financiera, sino que protege la esencia del negocio al convertir sistemas de seguridad aislados en una plataforma inteligente de gestión residencial. La inteligencia artificial robustece la propuesta de valor, haciéndola más eficiente y rentable a largo plazo, al tiempo que asegura que la información se transforme en decisiones estratégicas y valor económico tangible para los administradores y residentes. Para poder soportar esta estructura es necesario tener en cuenta la robustez del departamento de TI, no solo para el escalamiento a futuro del negocio sino para la concepción inicial del mismo.

6. Conclusiones

El desarrollo del presente trabajo permitió estructurar y analizar un modelo de negocio innovador para la gestión residencial, fundamentado en la integración tecnológica y la redefinición del rol de la seguridad electrónica dentro de la administración de edificios. A partir del análisis

estratégico se evidenció que la plataforma no debe concebirse únicamente como una herramienta operativa, sino como un sistema estratégico de gestión inteligente.

Se concluye que el uso del modelo de tensores clave de la estrategia organizacional constituye un marco analítico para evaluar el modelo de negocio. En particular, el tensor de capacidades distintivas se posiciona como el eje central de la estrategia, dado que la integración de servicios, la analítica avanzada y la personalización por edificio configuran una ventaja competitiva difícilmente replicable por soluciones tradicionales.

En relación con la cadena de abastecimiento, se concluye que el modelo propuesto se aparta de una lógica transaccional tradicional y adopta un enfoque de colaboración estratégica con proveedores clave, quienes actúan como socios tecnológicos y operativos. Esta estructura permite flexibilidad y escalabilidad, acelerando la innovación continua del sistema.

Es relevante destacar que el modelo desarrollado corresponde de manera deliberada a un Producto Mínimo Viable (PMV), conforme a los lineamientos establecidos por Bill Aulet en la disciplina de emprender. El alcance funcional del producto se limita a resolver el problema prioritario del cliente objetivo. Este enfoque metodológico permite reducir el riesgo emprendedor y evitar inversiones prematuras en funcionalidades avanzadas. Las capacidades analíticas avanzadas y la incorporación de inteligencia artificial se plantean, por tanto, como una evolución natural y progresiva del modelo, que podrá materializarse una vez validada la adopción del PMV. Este crecimiento incremental abre la posibilidad de estructurar modelos premium basados en analítica predictiva y soporte estratégico a la toma de decisiones.

Se concluye que el modelo propuesto es técnicamente viable y estratégicamente coherente, al apoyarse en tecnologías digitales y alianzas estratégicas. Su implementación contribuye a

modernizar la gestión de la propiedad horizontal, reduce la dependencia de esquemas intensivos en personal físico de seguridad y establece un nuevo estándar de administración basada en datos.

En este sentido, el trabajo aporta un marco conceptual y práctico en el sector de servicios residenciales mediante soluciones tecnológicas de alto valor agregado. Se concluye que sí existe viabilidad estratégica, sustentada en la convergencia entre las necesidades del mercado, las tendencias tecnológicas del sector y la posibilidad de estructurar una propuesta de valor diferenciada. Desde la perspectiva de creación de valor, el modelo propuesto demuestra que es posible articular una oferta que combine reducción de costos operativos, mejora en los niveles de control y trazabilidad, y una experiencia de usuario más flexible y segura. La integración de tecnología con un enfoque estratégico permite generar ventajas competitivas sostenibles en un mercado que aún presenta niveles incipientes de adopción tecnológica. No obstante, la viabilidad identificada en este estudio debe entenderse dentro del alcance definido, el cual corresponde a la estructuración de un Producto Mínimo Viable (PMV) bajo la metodología de Bill Aulet. En este sentido, el trabajo valida la lógica de creación de valor y la coherencia estratégica del modelo de negocio, pero reconoce que su consolidación requiere etapas posteriores de validación empírica, análisis financiero detallado y pruebas de mercado que permitan cuantificar con mayor precisión su rentabilidad y escalabilidad.

Finalmente, se concluye que la transición hacia modelos de seguridad basados en automatización no solo es viable, sino necesaria para responder a las dinámicas actuales del entorno, siempre que dicha transición esté soportada en una adecuada alineación entre tecnología, propuesta de valor y ejecución estratégica.

Referencias Bibliográficas

- Alarmar. (2026). Alarmar de Colombia. <https://alarmar.com.co/>
- Alert Monitoring. (2026). Remote concierge services. <https://www.alertmonitoring.uk/services/remote-concierge/>
- Aulet, B. (2015). La disciplina de emprender: 24 pasos para tener una empresa exitosa. LID Editorial Empresarial.
- Baum, A. (2017). PropTech 3.0: The future of real estate. University of Oxford.
- Blachman, G. (s.f.). Perfil de LinkedIn. LinkedIn. <https://www.linkedin.com/in/guyblachman/>
- Brivo. (2024). Security Suite. <https://www.brivo.com/>
- Carmichael, E. (2023, 3 de mayo). Personalized Service from Anywhere: The Benefits of Remote Concierge. Humankind.
- Carson Living. (2024). How it works. <https://www.carson.live/how-it-works>
- Chopra, S., & Meindl, P. (2019). Supply Chain Management: Strategy, Planning, and Operation (7th ed.). Pearson.
- CIE Group. (2026). How remote concierge systems work. <https://cie-group.com/how-to-av/videos-and-blogs/remote-concierge/1000>
- ClickPay. (2024). Resident Experience. <https://www.clickpay.com/>
- Domosis. (2026). Domosis Domótica y Seguridad. <https://domosis.com/>
- Guardacol. (2026). Guvvi Digital. <https://guvi.digital/>
- Intelligate. (2026). Intelligate Colombia. <https://intelligate.com.co/>
- Lee, S. (2025, 25 de marzo). 10 Ways AI-Powered Virtual Assistants Drive Business Growth. Number Analytics.

- Liu, S. Q., Vakeel, K. A., Smith, N. A., Alavipour, R. S., Wei, C. (V)., & Wirtz, J. (2024). AI concierge in the customer journey: what is it and how can it add value to the customer? *Journal of Service Management*, 35(6), 136-158. Mintzberg, H., Ahlstrand, B., & Lampel, J. (2009). *Strategy Safari: A Guided Tour Through the Wilds of Strategic Management*. Pearson Education.
- Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: A handbook for visionaries, game changers, and challengers*. John Wiley & Sons.
- Porter, M. E. (1996). What is Strategy? *Harvard Business Review*, 74(6), 61-78.
- Portero Seguro. (2026). Portero Seguro Perú. <https://porteroseguro.com/>
- Remote Monitoring Services Group Ltd. (s.f.). The future of virtual concierge services in residential complexes. Remote Monitoring.
- Schoenfelder, L. A., & Jones, A. B. (2021). Scalable systems and methods for monitoring and concierge service (U.S. Patent No. 10,885,734 B2). Oficina de Patentes y Marcas de Estados Unidos.
- Spotter Security. (2026). Spotter Security Canada. <https://www.spottersecurity.com/>
- Stealth Monitoring. (2026). Stealth Monitoring USA. <https://stealthmonitoring.com/>
- Stepanian, R. (2012). Consumer electronic registration, control and support concierge device and method (U.S. Patent No. 8,280,009 B2). Oficina de Patentes y Marcas de Estados Unidos.
- Stepanian, R. (2020). Consumer electronic registration, control and support concierge device and method (U.S. Patent No. 10,798,244 B2). Oficina de Patentes y Marcas de Estados Unidos.

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into Business Transformation*. Harvard Business Review Press.

Zavodska, A., Sramova, V., & Aho, A.-M. (s.f.). *Knowledge in Value Creation Process for Increasing Competitive Advantage*. USAL.