



Universidad de San Andrés

Escuela de Negocios

Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Servicios de Video vigilancia hogareño con soporte de inteligencia Artificial

Alumno/Autor: Gonzalo Britti

DNI: 23.805.068

Director del trabajo final: Enrique Hofman

Buenos aires

1 Julio de 2021



Universidad de
San Andrés

Escuela de negocios

**Maestría en servicios tecnológicos y de
telecomunicaciones.**

**Servicios de Video vigilancia hogareño con soporte de
inteligencia Artificial**

Alumno/Autor: Gonzalo Britti

DNI: 23.805.068

Buenos aires

1 Julio de 2021

Director del trabajo final: Enrique Hofman

Índice

Resumen.....	4
1. Introducción.....	5
Problemática del plan de negocios	5
2. Tesis de negocio	8
Preguntas de la tesis de negocio	8
Tesis de negocio	8
Objetivos del plan de negocio	9
3. Marco teórico.....	11
La inteligencia artificial	11
La Industria de la Seguridad privada	18
4. Análisis de Servicios de la Industria.....	22
Servicios de la industria.....	22
5. Benchmark.....	27
Consideraciones.....	27
Relevamiento.....	27
Análisis de benchmark.....	30
Conclusiones de Benchmark	31
6. Justificación del negocio	32
El mercado argentino	32
Análisis estratégico.....	37
El Modelo de negocio comparado	40
Efectos de red.....	42
Cinco fuerzas.....	44
FODA.....	45
Modelo de servicios comparado.....	47
7. Plan de negocio.....	49
Introducción del negocio.....	49
La empresa	49
Visión, Misión y Valores	49
Segmentos de mercado	50
Producto / Propuesta de valor.....	51
Diseño de la organización	55

Modelo de negocios	59
Mercados.....	61
Etapas de ejecución.....	61
Progresión del negocio.....	65
Análisis económico.....	67
Proyección de negocio	70
Flujo de la inversión	72
Resultados	72
8. Conclusiones.....	74
Conclusiones del trabajo	74
Conclusiones del plan de negocios	76
Prospectiva de la industria	77
9. Bibliografía.....	80
10. Anexos.....	83
Anexo I : Relevamiento de Benchmark.....	83
Anexo II – Encuesta complementaria.....	93
Anexo III : Empathy maps	95
Anexo IV: Value Proposition Canvas.....	97
Anexo V: Business Model Canvas	98

Resumen

A partir de la demanda de seguridad por parte de los mercados en las últimas décadas, tanto en nuestro país como en la región, se vislumbra un crecimiento de ofertas y propuestas proveniente de la industria de la seguridad privada. La también creciente sensación de inseguridad de la ciudadanía ha favorecido a dicho incremento, incentivando a que muchas empresas privadas de Seguridad se esfuercen en mejorar sus propuestas de valor y logren mejores productos y servicios que los que venían ofreciendo; apalancados por los nuevos paradigmas tecnológicos, en creciente evolución y con resultados sorprendentes en términos de aplicaciones prácticas.

La inteligencia artificial y su aplicación en los negocios se encuentra en una etapa de crecimiento exponencial. Durante la última década, el epicentro del desarrollo de esta tecnología pasó del ámbito universitario al de los negocios, donde ha encontrado en la demanda uno de los principales impulsos para su desarrollo. En la actualidad es posible encontrar aplicaciones de Inteligencia Artificial integradas a una variada gama de productos y servicios. En estos se persigue realizar tareas cada vez más complejas que antes solo podían ser realizadas por personas.

En este sentido, el presente trabajo explora la posibilidad de transformar servicios de la industria de la seguridad privada con un alto componente de mano de obra especializada, por sistemas asistidos con tecnología de Inteligencia artificial.

Específicamente se buscará trabajar sobre la seguridad en hogares particulares. Para estos, se diseñará una propuesta de valor de servicio de video vigilancia con componente de video analytics que permita automatizar tareas que tradicionalmente son realizadas por personas.

1. Introducción

De acuerdo al relevamiento efectuado por la empresa de seguridad *Securitas Argentina* sobre el mercado, un 64% de los servicios de seguridad física están basados en sistemas presenciales con personal en el mismo sitio a ser custodiado. Solo el 13,6% de los servicios de custodia son realizados con asistencia de raíz tecnológica (Garrone & Lafratti, 2015). Esto refleja que la industria de Seguridad posee una alta dependencia de mano de obra para sostener los procesos operativos.

El contexto actual de transformación digital funciona principalmente como catalizador del desarrollo de nuevas oportunidades de negocio en forma de servicios y plataformas inéditas, que además poseen una fuerte raíz tecnológica. En este sentido, dicha transformación funciona como motor de la conversión de trabajos y servicios existentes; llevados a cabo mayormente por humanos, para pasar a ser realizados por máquinas (con componentes de tecnología de inteligencia Artificial).

El presente trabajo aborda esta transformación, ,, elaborando un plan de negocios para la sustitución de servicios, que hoy poseen una fuerte componente humana, para transformarlos total o parcialmente en servicios de alto valor y/o bajo costo y con soporte de inteligencia artificial.

Se seleccionó la video vigilancia de hogares particulares, con soporte de Inteligencia artificial como campo específico de aplicación.

Problemática del plan de negocios

La problemática principal del plan de negocios es validar la factibilidad de diseñar una solución que permita sustituir al humano en el proceso de vigilancia de hogares.

Este problema parece sencillo para los tecno-optimistas, pero presenta tres dimensiones principales que es necesario explorar: La tecnología, el mercado y la industria.

La Tecnología

Al nombrar a la tecnología de inteligencia artificial, estamos haciendo referencia a uno de los principales elementos a considerar, ya que, como componente primario del nuevo servicio, cuenta con las capacidades suficientes para poder realizar las tareas que le permitan desarrollar de manera aceptable la labor (antes realizada por un humano).

El concepto de Inteligencia Artificial no es moderno, fue creado hace más de 60 años y durante este tiempo pasó de ser un concepto a una tecnología casi exclusiva del ámbito

académico donde se mantuvo y desarrolló incipientemente. A principios de este siglo se combinaron dos factores que permitieron salir de esa exclusividad, y comenzase a aplicarse mayormente en el ámbito comercial y de negocios. Estos factores fueron el hardware, nuevo hardware más potente estuvo disponible para su aplicación, y el segundo factor fue el crecimiento exponencial de Internet que permitió tener grandes cantidades de datos disponibles para entrenamiento de modelos.

Ya en la década pasada, la tecnología tiene su propia industria con crecimiento y desarrollo exponencial como se puede ver en el siguiente cuadro de Statista.

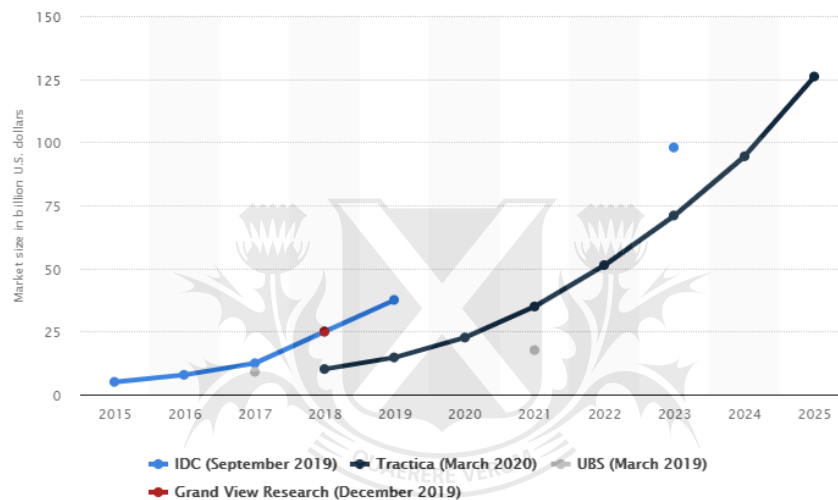


Gráfico I: Revenue de la industria de IA 2015-2025 (fuente: Statista 2020)

Llevando estos conceptos al problema de aplicación, si se pretende reemplazar un humano en servicios de seguridad, la tecnología debería lograr que la maquina sea capaz de realizar las mismas actividades que las personas llevan a cabo.

Se debe explorar el estado del arte de la misma para comprender sus capacidades, limitaciones y los aspectos a considerar para la arquitectura de software, con el objeto de conseguir un panorama claro sobre los alcances que se pudieran definir en el diseño del plan de negocios.

La industria de la seguridad

La segunda dimensión que se debe explorar es la industria. Es necesario entender como son y qué es lo que hacen hoy las empresas que la conforman, para poder construir una

propuesta de valor superadora que permita posicionar la video vigilancia con soporte de AI como un servicio cuya ventaja competitiva esté por encima del resto.

De acuerdo a la *Cámara Argentina de Empresas de Seguridad e Investigación (CAESI)*, en la actualidad, los servicios de seguridad física están basados en un 64% en sistemas presenciales, con personal en el mismo sitio a ser custodiado. Aproximadamente el 14% de los servicios de custodia son realizados con asistencia de raíz tecnológica. Esto revela que la Industria tiene un alto porcentaje de dependencia de la mano de obra y un bajo porcentaje de cobertura con medios tecnológicos.

El Mercado

El Mercado es una de las dimensiones más complejas del análisis, el trabajo incluye un relevamiento comparativo de los servicios de mercado para los objetivos seleccionados. Ellos son: el mercado local (Argentina), Brasil, México y USA. Los tres primeros son los más grandes de Latinoamérica y representaron en el año 2018 un volumen total de facturación cercano a los 1.000 millones de dólares solo en Argentina (Carballo et al., 2018).

2. Tesis de negocio

Preguntas de la tesis de negocio

La pregunta que define mejor los aspectos explorados es la siguiente:

¿Es viable brindar servicios de seguridad hogareños con la utilización de sistemas de video vigilancia con inteligencia artificial?

Pero esta pregunta se descompone en:

- *¿La tecnología de IA posee la madurez necesaria para el trabajo que se intenta desarrollar?*
- *¿Se puede crear una propuesta de valor superadora respecto de la industria actual?*
- *¿Es propicio el mercado para desarrollar esta propuesta de valor?*

Tesis de negocio

Como se viene mencionando de manera general, el plan de negocios pretende definir y evaluar el desarrollo de servicios de video vigilancia con una fuerte componente de inteligencia artificial. A fin de avanzar, fue necesario realizar una descripción con un grado de aproximación mayor, que permitiera definir algunos aspectos claves del servicio, aunque luego estos pudiesen ir modificándose o evolucionar conforme al avance del desarrollo del concepto.

Por lo tanto, en esta sección se pretende plantear un modelo conceptual del servicio que permita definir algunos aspectos de la exploración y la investigación sobre los distintos factores que incidirán en el desarrollo.

Todo *Sistema de Protección Fija* (Jiménez, 2016) posee tres componentes principales que lo definen como tal en este orden: *la detección, el retardo y la respuesta*.

La detección

La vigilancia es exclusivamente realizada por sistemas con inteligencia artificial, esto implica que no existen personas observando las imágenes de las cámaras de vigilancia. Por lo tanto, de esta característica se desprenden algunos conceptos tácitos que vale la pena mencionar por su grado de relevancia:

- **Biometría:** El sistema debe identificar parámetros biométricos como quien es cada persona que ingresa al hogar y determinar si corresponde con alguno de

los habitantes regulares del hogar. La manera de identificar debe ser por reconocimiento facial.

- **Accesos:** además de rostros, es necesario identificar cuando una persona no acceda de la manera esperada, por ejemplo, saltando una pared o reja.
- **Privacidad:** si bien el sistema tiene el control de todo lo que suceda en el hogar, el suscriptor goza de total privacidad sobre el movimiento habitual del hogar, horarios, días, actividades, visitas, etc. Esto se considera uno de los principales aportes a la propuesta de valor.

El retardo

El retardo en los SPF representa todas las medidas físicas que se interponen entre el intruso y el bien a ser resguardado, un ejemplo de esto último son las rejas, paredones, puertas, etc. Este elemento por tratarse de un componente edilicio no será considerado dentro del alcance del sistema propuesto.

La respuesta

El sistema realiza la vigilancia sobre quienes o como lo hacen, los que ingresan a la propiedad. En los casos donde se identifiquen situaciones no esperadas, el software debe ser capaz de reportarlo al propietario. Estas situaciones no esperadas que generan reportes al usuario se referenciarán de aquí en más como anomalías de seguridad o simplemente anomalías.

La intervención humana

Una de las premisas del servicio es la de sustituir parcial o totalmente la mano de obra especializada ya que se espera, a partir de la incorporación de IA, llegar a realizar tareas con un alto grado de especialización que permita prescindir total o parcialmente de la necesidad de intervención humana.

Como se verá más adelante, durante la descripción del servicio, será necesario evaluar algunas tareas que no pueden ser reemplazadas íntegramente con el uso de esta tecnología, como por ejemplo la asistencia a domicilio o el contacto con las fuerzas de seguridad pública.

Objetivos del plan de negocio

- Desarrollar una propuesta de valor superadora respecto de los servicios existentes.
 - Para esto es necesario entender de qué manera se debe aplicar la tecnología para desarrollarla.

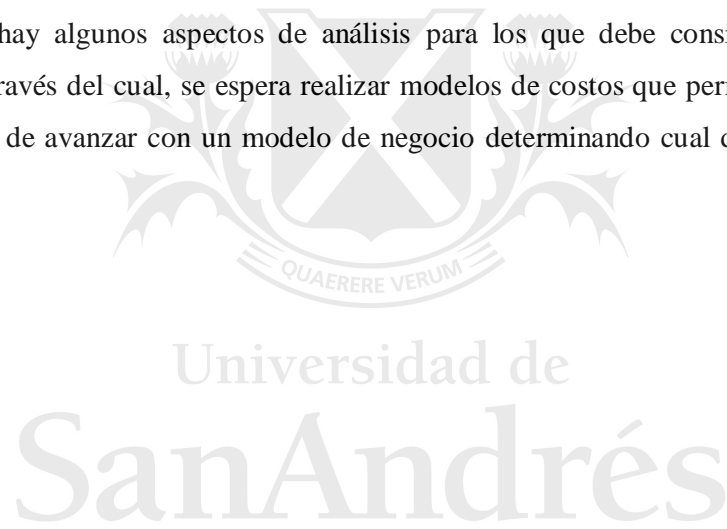
- Comprender la situación de la competencia de la industria de la seguridad, el nivel de adopción tecnológica y el mercado.
- Identificar y relevar la propuesta de valor que hoy ofrece la industria de la seguridad privada.

Metodología

Para el estudio de la tesis de negocio se pretende desarrollar distintos análisis que permitan una comprensión amplia de la problemática.

El análisis cualitativo en primera medida permite analizar la capacidad de la tecnología para el desarrollo de un nuevo tipo de servicio, y también posibilita una revisión de la variedad de servicios actualmente existentes, de modo que se puede concluir realizando un contraste entre ambos.

Por otro lado, hay algunos aspectos de análisis para los que debe considerar el análisis cuantitativo; a través del cual, se espera realizar modelos de costos que permitan entender la real factibilidad de avanzar con un modelo de negocio determinando cual de ambos captura mejor el valor.



3. Marco teórico

La inteligencia artificial

La Inteligencia artificial debe su origen al estudio fisiológico del cerebro humano y el intento por imitar su funcionamiento (DEEP LEARNING for Computer Vision: A Brief Review). Uno de los precursores de la idea de Inteligencia artificial fue Alan Turing quien, en el año 1950 diseñó el conocido test de Turing cuya función era la de poder identificar, en un diálogo, a una persona real de una máquina, asumiendo que algún día las máquinas tendrían la capacidad de sostener una conversación, es decir serían entes inteligentes.

En 1955, pocos años después del test de Turing, en la Western joint Computer Conference de Esta dos Unidos, se presentaron diversos trabajos Sobre lo que podrían considerarse implementaciones de sistemas de Inteligencia artificial (López de Mántaras Badia & Meseguer González, 2017) y redes neuronales artificiales (Voulodimos et al., 2018)

Las redes neuronales

Las redes neuronales artificiales son, cómo se mencionó anteriormente, técnicas de IA que intentan imitar el funcionamiento del cerebro humano, particularmente sobre cómo las neuronas se configuran para resolver una tarea específica. En este sentido uno de los trabajos presentados ese año (1955) incluían técnicas o mecanismos “sobre cómo ajustar los pesos de las conexiones entre las neuronas de una red neuronal artificial” (López de Mántaras Badia & Meseguer González, 2017). Este ajuste de pesos entre las conexiones es el que logra que una red neuronal se especialice para la resolución de un problema, ya sea reconocer, patrones, comprensión de texto o identificar objetos dentro de una imagen, qué es un problema particular de reconocimiento de patrones.

Una red neuronal computacional es un modelo computacional construido a semejanza de una red neuronal cerebral, y que posee objetos denominados neuronas que están interconectados entre sí por vínculos. Estas “neuronas” están dispuestas en capas que se agrupan genéricamente en tres tipos o capas:

- De entrada, o input: Reciben la entrada del problema a resolver
- Intermedias o escondidas (hidden): resuelven el problema, comparar, identificar, etc,
- De salida u output: emiten una respuesta o solución al problema.

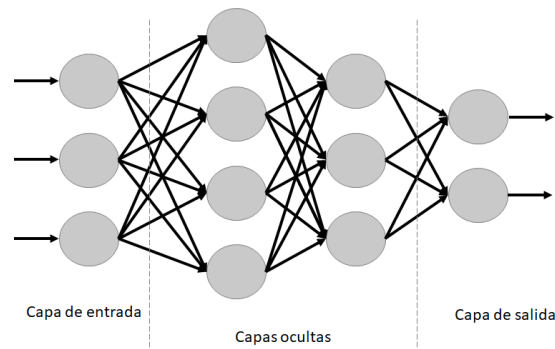


Grafico II: Red neuronal computacional (fuente: elaboración propia)

En el gráfico II se puede observar una representación conceptual de las redes neuronales computacionales, los círculos representan neuronas y las flechas representan las conexiones entre ellas, nótese que el flujo de los datos se mueve en el sentido de las flechas, en este caso, de izquierda a derecha.

En un modelo entrenado, las neuronas almacenan valores y las conexiones tienen asignado un distinto peso estadístico, cuando los valores se operan con los pesos estadísticos de las capas ocultas, los valores van mutando hasta llegar a la capa de salida, donde lo que se obtiene es una probabilidad asociada a cada respuesta esperada (LeCun et al., 2015)

Entonces, los verdaderos responsables de la resolución del problema son los pesos estadísticos que posee cada conexión, las neuronas sólo almacenan los resultados intermedios y de salida. La manera de que las conexiones adopten el valor adecuado para resolver un problema específico se consigue realizando un entrenamiento.

Deep learning

El Deep learning es una serie de métodos que se utilizan para el entrenamiento de redes neuronales basadas en modelos probabilísticos y algunos algoritmos de aprendizaje de características supervisadas y no supervisadas. Toda red neuronal debe ser entrenada para poder realizar una tarea específica y los métodos de Deep learning permiten esta tarea. (Voulodimos et al., 2018).

El entrenamiento supervisado es un método de Deep learning que permite entrenar a una red neuronal para realizar un trabajo específico. El método comprende tres etapas:

- I. Ingreso de datos de entrenamiento.
- II. Proceso de los datos y emisión de resultados.
- III. Evaluación de resultados y retroalimentación del modelo.

El proceso de retroalimentación consta de recorrer la red en el sentido inverso haciendo pequeños ajustes al peso estadístico de cada uno de los vínculos. Repitiendo este proceso N veces es posible conseguir una red neuronal entrenada para la tarea que se pretende (LeCun et al., 2015).

Computer vision

La tecnología es la denominada “Computer Vision” (Voulodimos et al., 2018) que es un concepto originado en los años 60 y que resume la posibilidad de dotar a los ordenadores de la capacidad de ver. Entendiendo por “ver” a poder analizar y comprender imágenes obtenidas de cámaras de video, permitiéndole identificar objetos o situaciones.

Surge de la aplicación de técnicas de Deep learning al análisis de imágenes de video para determinar o analizar cualquier aspecto que se desee. El Computer Vision evolucionó lentamente desde sus orígenes hasta la primera década de este siglo, donde comenzó a cobrar relevancia principalmente por dos motivos.

En primer lugar, comenzó a estar disponible y con acceso público, una gran cantidad de imágenes debido a la rápida expansión de internet en el período. Las imágenes obtenidas de internet pasaron a ser un recurso de entrenamiento muy valioso ya que cuantas más imágenes se utilicen para entrenar el modelo tanto mejor es la precisión que este consigue, a modo de ejemplo, si quisiéramos entrenar un modelo de redes para identificar un vaso o una copa, necesitaremos muchas imágenes de vasos y copas para que la red aprenda cómo identificarlos con un margen de error aceptable.

El segundo factor que contribuyó al impulso del Deep learning fue el hardware, particularmente porque comenzó a estar disponible en el mercado una gran oferta de hardware con GPUs (Voulodimos et al., 2018). Las GPUs, del inglés, Graphics Processor Units, es un tipo de hardware especial concebido originalmente para el procesamiento de animaciones en 3D al que, por ese entonces, se le encontró una nueva aplicación en el costoso proceso de entrenamiento de modelos, permitiendo acelerar los tiempos de esta etapa de manera casi exponencial, y adicionalmente reducir su costo.

Estos factores fueron en alguna medida acompañados por distintas innovaciones en el software utilizado mejorando su eficiencia, no solo por la disminución de los recursos necesarios para el entrenamiento y el procesamiento, sino que también, por la posibilidad de tener modelos pre-entrenados que combinados otros entrenamientos específicos serían capaces realizar tareas más complejas.

Face Recognition

Un ejemplo de estos modelos pre-entrenados es el del caso de “Face Recognition at a Distance for a Stand-Alone Access Control System” (Hansung Lee et al., n.d.), donde el proceso de identificar una persona, consta de distintas etapas resumidas en el siguiente orden:

- I. *Determinación de un rostro en la imagen:* En la imagen recibida determinar donde hay un rostro y seleccionarlo.
- II. *Normalizar el rostro:*
 - a) Recortar de la imagen todo rostro determinado en el paso 1.
 - b) Redimensionar la imagen de los rostros a un tamaño estándar: La mejor manera de comparar dos objetos es tenerlos en la misma escala.
- III. *Aplicar filtros:* a la imagen normalizada para corregir problemas de iluminación o baja calidad de la misma.
- IV. *Comparación:* del resultado con la base de datos de rostros para su identificación individual.

Los servicios computacionales en la actualidad están basados en los denominados servicios de tipo Cloud, que son capacidades de cómputo brindados desde instalaciones ubicadas en sitios remotos a los que se accede a través de Internet. Aplicar el modelo de servicio para detección de anomalías por video implicaría transmitir las imágenes captadas, desde el hogar de cada suscriptor, hacia un sitio en el Cloud de cómputo a través de internet donde la red neuronal interpretaría las imágenes.

Planteado de esta forma, el modelo tiene un problema importante: el throughput de datos, que es la cantidad de datos que se deben transferir por unidad de tiempo y representa un problema por la naturaleza del dato (imágenes/video) que son tipos de datos de gran tamaño.

Face detection vs anomalías

Es necesario hacer una distinción entre la detección de rostros y la de anomalías de detección, comenzando por la definición. Para el caso de un rostro, el sistema “pre conoce” cómo es un rostro, sabe dónde ubicar los ojos, la nariz y todas las partes que lo conforman y que luego deberá comparar contra otros rostros que tiene almacenados y así encontrar la coincidencia. En el caso de las anomalías (Lu, 2020), como su nombre lo indica, lo que puede ocurrir es algo distinto a lo normal, no previsto y por lo tanto el problema a resolver es distinto porque no hay contra qué compararlo, por ejemplo, el rostro posee barbijo, anteojos o sencillamente el ángulo en el que la cámara captó el rostro es insuficiente para

lograr una detección completa del mismo. Estos dos casos contemplan lo que Lu denomina anomalías de detección.

La manera de detectar anomalías tiene un abordaje distinto, donde el sistema debe meta-entrenarse (Lu, 2020) para asimilar en su red neuronal la capacidad de “ver” los comportamientos que están fuera de lugar.

Edge Computing

Una aproximación a la solución de este problema está planteada en el caso de mVideo (Sun et al., 2020) que introduce un concepto denominado “Edge Computing”. Este caso toma las partes del proceso de la detección ya mencionadas y propone repartir la carga entre la capacidad de cómputo local, denominada Edge, y la remota (Cloud).

Bajo este concepto o arquitectura del servicio, el módulo edge es quien recibe localmente la transmisión del video de los dispositivos (cámaras) y realiza las dos primeras etapas de la comprensión de la imagen:

- I. Determinar un rostro en la imagen
- II. Normalizar el rostro.

Luego el rostro normalizado es transmitido al otro componente del servicio que se encarga de la aplicación de filtros e identificación de la persona. Este modelo permite reducir significativamente el *throughput* ya que las imágenes transmitidas son de un tamaño significativamente menor al que se transmitiría en el esquema anterior.

En el gráfico II, se puede ver el modelo de arquitectura de mVideo: sobre el lado izquierdo se focalizan las actividades desarrolladas en el edge computing, se interpreta la imagen y se extraen los rostros normalizándolos para ser transmitidos al Cloud (sector derecho) donde se realizan las actividades de mayor nivel de complejidad como la identificación comparativa del rostro.

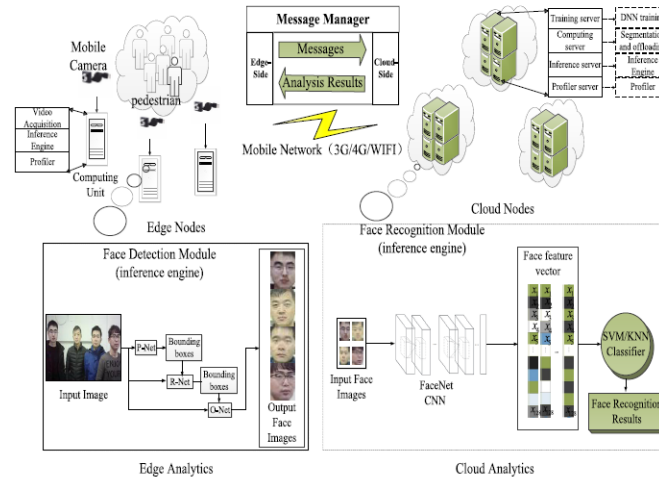


Grafico III - modelo de arquitectura de mVideo (Sun et al., 2020)

3D Face recognition

Otra tecnología que ya está presente en el mercado en productos de consumo masivo como el iPhone y que es una tendencia en crecimiento en el ámbito académico es el reconocimiento facial en un nuevo campo conocido como 3D scanning o 3D recognition (Zhou & Xiao, n.d.).

Esta tecnología combina escáneres de tres dimensiones, con varios de los componentes mencionados con anterioridad (como Deep Learning y las redes neuronales) y los utiliza para realizar procesos comparativos de identificación de rostros. La ventaja de la imagen tridimensional por sobre la convencional de dos dimensiones obtenida de una cámara de video es que el resultado de la primera es de una precisión superior a la original.

Si bien, esta tecnología es superior por que mejora en precisión y erradica problemas como la iluminación, existentes en el reconocimiento facial tradicional, comparte con este último, algunos problemas que hasta el momento son difíciles de resolver como, por ejemplo, la expresión, la pose o ángulo y los accesorios (anteojos, piercing, etc.).

Arquitectura propuesta de IA

Lo anteriormente descrito en este capítulo, permite contar con una comprensión de los distintos componentes que posee la tecnología de IA, respecto de las capacidades tecnológicas disponibles. También permite discernir que componentes deberán estar presentes y cuáles no, dado que no poseen características que permitan definirlos como viables para el problema que se pretende resolver, como es el caso de el escaneo en 3D.

Por consiguiente, se desprende que la tecnología a ser aplicada debe ser de redes neuronales, puesto que cuenta con la capacidad de realizar actividades verdaderamente complejas como identificar a rostros o detectar anomalías o situaciones fuera de lugar.

Su aplicación para este modelo, requiere incluir como componente de la arquitectura, el denominado Edge Computing. El mismo tiene dos ventajas fundamentales:

- a) Optimización del tiempo de respuesta en el proceso de reconocimiento facial a partir de realizar el proceso de manera local. En el caso del procesamiento en el cloud, los tiempos de respuesta se incrementan por los tiempos de transferencia de los datos.
- b) Optimización del volumen de datos transferidos hacia el compute en cloud, solo se transfieren para identificación, los rostros que no pudieron ser identificados localmente.

Para el desarrollo de producto no será posible considerar las tecnologías actuales de reconocimiento facial 3D, que, aunque son más precisas, su utilización depende de que la persona adopte una postura específica para el escaneo, al menos con la tecnología actual. La aplicación de esta, más que para detectar anomalías de seguridad cobra relevancia como sistema de detección biométrica para sistemas de control de acceso, pero como tal, tiene las mismas dificultades de poses o accesorios, que reducen su precisión, tal como al reconocimiento por video.

La Industria de la Seguridad privada

La industria de la seguridad en Latinoamérica está compuesta por varios miles de compañías generalmente nucleadas en cámaras de la industria locales a cada país.

Los países con mayor desarrollo de la industria en Latinoamérica son: Argentina, Brasil, Colombia y México. Este desarrollo está dado por el impulso que generan los mercados locales con la demanda de seguridad, solo en Argentina, el mercado de la seguridad alcanzó niveles de facturación anual cercanos a MMU\$S 1000 en el año 2018 (Carballo et al., 2018).

Entre los países mencionados, es posible identificar varias asociaciones de empresas que integran distintos componentes de la cadena de valor de la industria, que en líneas generales es posible asociarlos a cuatro categorías principales:

- **Fabricantes:** Por fabricantes es común pensar en componentes electrónicos como cámaras de video, alarmas, etc. Pero debe considerarse una visión más amplia, por ejemplo, sistemas de defensa personal no letales (gases, cascos) u otros componentes para sistemas de protección de incendio (detectores, gases inertes, etc.).
- **Integradores:** Integradores de componentes de seguridad en sistemas avanzados, típicamente fabricantes de sistemas de monitoreo, video, alarmas, centrales de incendio.
- **Distribuidores:** Distribuidores y canales de comercialización de sistemas de seguridad.
- **Proveedores de servicios:** Empresas de seguridad, que además de integrar componentes de corte tecnológico ofrecen una gama de servicios e integran en muchos casos todos los sistemas mencionados en soluciones compuestas y agregan componentes propios como ser la mano de obra del vigilador.

La industria y los mercados

En Latinoamérica es posible encontrar al menos dos organizaciones internacionales que nuclean a su vez otras agrupaciones y empresas de distintos países. La organización ALAS (Asociación Latinoamericana de seguridad) posee una fuerte participación de empresas fabricantes o integradoras de productos de seguridad, del mercado mexicano y argentino. El segundo organismo internacional tiene una representatividad más acotada, ya que existe a nivel regional la “Federación de Seguridad de los países del Mercosur”, FESESUL o FESESUR, que nuclea organizaciones -como su nombre lo indica- principalmente de los integrantes del Mercosur.

A nivel local encontraremos distintas organizaciones o agrupaciones que nuclean a la mayoría de las más de 10.000 empresas que operan en la región. Las distintas agrupaciones de empresas vinculadas al sector en los países mencionados son:

México

existen al menos 6000 empresas (Rodríguez, 2018), pero solamente hay registradas unas 3400 declaradas en el registro formal del organismo de control gubernamental, la DGSP: Dirección General de Seguridad Privada: <https://siesp.ssp.gob.mx>

Las asociaciones de empresas de seguridad mexicanas son:

CNSP: Consejo nacional de seguridad privada: www.cnsp.org.mx

AMESP : Asociación Mexicana de Empresas de Seguridad Privada, A.C.: www.amesp.mx

AMESIS: Asociación Mexicana de Empresas de Seguridad Privada e Industria Satelital A.C.: www.amesis.org.mx

El mercado mexicano sería el más grande de Latinoamérica, Esta industria emplea a más de seiscientos mil personas en todo el país y obtiene un volumen total de algo más de diez y siete mil millones de dólares (Rodríguez, 2018) que representarían el 1,5% de su PBI, según los datos obtenidos de la “Oficina de Económica y Comercial de España en México”.

Brasil

En datos oficiales del IBGE para el año 2020, Brasil posee 4618 empresas de seguridad nucleadas en la mayoría de los casos en sindicatos que poseen un ámbito de injerencia a nivel de estado. A continuación, las dos organizaciones más relevantes:

ABREVIS - Associação Brasileira das Empresas de Vigilância e Segurança: www.abrevis-seg.com.br

SESVESP, “Sindicato das empresas de segurança privada, segurança eletrônica e cursos de formação do estado de São Paulo.”, www.sesvesp.com.br

Brasil es el segundo de los mercados regionales en tamaño, el volumen total de facturación alcanza los treinta y seis mil millones de reales o siete mil millones de dólares, representado casi medio punto porcentual de su PBI (2018), posee cerca de un millón de personas registradas y aptas para formar parte de la industria, pero solo emplea a la mitad (Reinach, 2020).

Colombia

según estadísticas oficiales, posee unas 1355 empresas de seguridad privada registradas en el organismo de control gubernamental denominado SuperVigilancia: Superintendencia de vigilancia y seguridad privada: www.supervigilancia.gov.co

CCSP: Cámara Colombiana de la Seguridad Privada www.ccseguridadprivada.org

Colombia es el tercer país en volumen de mercado con unos tres mil quinientos millones de dólares, emplea cerca de doscientas mil personas y la actividad representa un total del 1,2% de su PBI.

Argentina

No existen datos formales relevados por organismos oficiales a nivel nacional, sin embargo, la estimación de un informe privado muestra un total de 1390 empresas.

Las distintas cámaras empresarias son:

CAESI, “Cámara Argentina de empresas de seguridad e investigación”, www.caesi.org.ar

CAESBA, “Cámara de empresas de seguridad de Buenos Aires”, www.caesba.org.ar

CELSI, “Cámara de empresas líderes en seguridad e investigaciones.”, www.celsi.com.ar

CASEL, “Cámara Argentina de seguridad electrónica”, www.casel.org.ar

CEMARA, “Camara de empresas de monitoreo y alarmas de la República Argentina” www.cemara.org.ar

CESEC, “Cámara de empresas de seguridad electrónica del centro”, www.facebook.com/cesecarg

A continuación, el Cuadro I con un resumen de lo antes expuesto.

	Año relevado	Población	Empleados	Empresas	PBI (MMU\$D)	% PBI	Facturación (MMU\$D)
Brasil	2019	211.000.000	545.417	4618	\$ 1.869.000	0,4%	\$ 7.017,84
Colombia	2015	50.000.000	~= 200.000	1355	\$ 293.047	1,2%	\$ 3.583,00
Argentina	2018	45.000.000	132.000	1390	\$ 519.871	0,2%	\$ 965,00
México	2018	127.000.000	> 600.000	6000	\$ 1.157.700	1,5%	\$ 17.365,50
USA	2021	328.000.000	-	-	\$ 21.430.000	0,2%	\$ 46.300,00

Cuadro I: Datos generales de la industria (fuentes: diversas)

Según las estadísticas oficiales de seguridad, solo en Argentina, durante el año 2018, el total de robos alcanza la cifra de 456.600 de delitos contra la propiedad (Estadísticas Criminales

En La República Argentina – Año 2018, 2019) que representa una tasa de 1026 delitos por cada 100 mil habitantes. Esta cifra, salvo pequeñas variaciones, se mantiene estable durante los últimos años y por supuesto no incluye otros delitos como violaciones, homicidios, etc. que incrementaría la estadística haciendo que la cifra sea superada fácilmente.

No debe pasarse por alto que estos datos corresponden solamente a los hechos denunciados, por lo tanto, son solo una parte del total de hechos ocurridos. Esta visión de que no todos los hechos de inseguridad son denunciados, coinciden en buena medida, con otras estadísticas realizadas fuera del ámbito gubernamental, como por ejemplo, el “Observatorio de la Deuda Social Argentina de UCA” emitido en 2016, que dice que, para ese mismo año, el 24,3% de los hogares urbanos han sufrido un hecho de delincuencia o violencia (Bonfiglio et al., 2017). A manera de ejemplo, si se extrapolase este valor para el centro urbano más grande de Argentina, Buenos Aires y Gran Buenos Aires, la estadística representa más de 850.000 hogares con hechos de inseguridad, casi el doble respecto de las estadísticas oficiales.

Otro dato, también relevante y que se puede utilizar para aproximar una comprensión de la situación del mercado, es el de la percepción de riesgo (Bonfiglio et al., 2017) que es una medida subjetiva determinada por el porcentaje de personas mayores de 18 años cuya valoración de la posibilidad de ser víctima de un delito es alta. En el estudio, dicho índice alcanza el valor de 72,3% de las personas con alta percepción del riesgo que representado en el total de la población de la ciudad de Buenos Aires más los 24 partidos del Gran Buenos Aires, se corresponde con aproximadamente 9 millones de personas con una percepción de riesgo elevada.

Hasta este punto de la revisión, los datos aportados son referencia, fundamentalmente del volumen total del mercado. Será necesario incluir un dato más que permita realizar una aproximación que se ajuste más a la realidad, puesto que no resulta lógico pensar que habrá efectivamente más de 9 millones de personas dispuestas o con capacidad de comprar servicios de seguridad solo porque su percepción de la inseguridad es elevada.

Esta selección de una parte del mercado o segmentación se realiza aplicando a los valores anteriores el indicador de nivel socioeconómico para los segmentos que más se ajusten como potenciales suscriptores de servicios de seguridad. Los segmentos seleccionados son el ABC1 y C2 (Muraro, 2018) que representa el 23,4% de las familias y por lo tanto un volumen aproximado de poco más de 800.000 hogares.

4. Análisis de Servicios de la Industria

Servicios de la industria

La Industria de Seguridad Privada ofrece servicios para los distintos objetivos de mercado. Estos objetivos van desde las personas individuales, hogares (casas, edificios y grandes consorcios), luego las PyMES y por último las grandes empresas (de servicios o industriales), con custodias de sus activos, ya sean estos oficinas, edificios, mercaderías o caudales.

Adicionalmente, se observan algunas pocas nuevas empresas de corte tecnológico que han liberado productos con premisas como las del servicio propuesto. En el próximo capítulo se explorará un poco más sobre este tipo de compañías.

A continuación, en el cuadro II, se puede observar los distintos objetivos de mercado en relación con las distintas categorías de servicios y recursos de los que la industria dispone para satisfacer la demanda:

Servicios	Individuos	Hogares		PyMES		Grandes clientes			
	Personas	Casas	Complejos habitac	Comercios	Empresas	Bancos y entidades Financieras	Superficies comerciales	Empresas de servicios	Empresas Industriales
Custodias personal	Si		Si						
Control electrónico		Si	Si	Si		Si			
Garitas		Si	Si			Si		Si	Si
Control de acceso			Si		Si	Si	Si	Si	Si
Monitoreo perimetral electrónico			Si						
Consultoría de seguridad						Si	Si	Si	Si
Control físico				Si	Si	Si			
Custodia de mercaderías en tránsito					Si		Si		Si
Depositos y almacenes									Si
Garitas (Con armas)						Si			
Monitoreo de cajas y tesorería							Si		
Rondas de video							Si		Si
Transporte de caudales						Si		Si	Si
Trazabilidad de cargas							Si		Si
Vigilancia de salones							Si		

Cuadro II: Servicios ofrecidos por objetivo de mercado (Garrone & Lafratti, 2015)

Este cuadro permite establecer un panorama general de los servicios asociados por tipo de segmento. A partir de esta construcción es posible discernir cuales son los servicios de la industria que se ofrecen para el segmento específico que se ha seleccionado como objetivo (en color verde).

Entonces, los servicios asociados al segmento de “hogares”, son dos: “Control electrónico” y Garitas que son explicados con algo más de detalle:

Control electrónico

En la categoría de Control electrónico, podemos ubicar a todos los sistemas de seguridad con soporte electrónico, ya sean Circuitos Cerrados de Televisión CCTV, alarmas electrónicas (habitualmente tienen una implementación de sensores de: presencia, movimiento, apertura de puertas y ventanas, infrarrojos, etc.). La industria ofrece dos tipos de opciones para el producto alarmas: las alarmas autónomas, son habitualmente vendidas e instaladas por distribuidores, y las alarmas con “Monitoreo”.

El Monitoreo es el servicio por el cual el prestador mantiene control constante del bien custodiado, una conexión permanente desde donde se notifica de anomalías de seguridad, y a partir de las mismas, puede emitir una respuesta asociada. Lo habitual, para los servicios de alarma con monitoreo, es una respuesta inicial que implique contactar al dueño de la propiedad, esto se hace para determinar la realidad de la anomalía y evitar el reporte de falsos positivos a las autoridades.

Vigilancia física o Garitas

El otro tipo de servicio asociado a la custodia de casas, edificios, vecindarios, y propiedades en general es lo que se denominan garitas, el nombre en realidad hace referencia al puesto de vigilancia donde cumple el servicio un vigilador o vigilante que esta presencial en el lugar o propiedad a ser custodiada.

Es uno de los servicios más utilizados por la mayoría de los segmentos y la custodia de hogares no es una excepción, aunque lo más habitual es verlo asociado a custodia de un conjunto de propiedades como en edificios o barrios cerrados, y en menor medida en las esquinas de barrios de mayor nivel adquisitivo medio.

Servicios asociados a la custodia de hogares particulares

Uno de los primeros criterios (probablemente el más importante) que se puede utilizar para clasificar los servicios de seguridad, es por tipo de producto, ya que esto permite diferenciar claramente los distintos actores que intervendrán dentro del proceso operativo interno en cada caso, de esta forma se puede identificar, cuáles de estos procesos tienen fuerte componente electrónica y cuáles poseen mayor intervención de mano de obra.

De un relevamiento a de empresas de las agrupaciones mencionadas anteriormente, se han identificado los siguientes servicios, los que guardan similitudes entre las distintas empresas y países:

- *Vigilancia presencial*: Personal de seguridad en el sitio a ser custodiado.

- *Custodia de mercaderías*: Escolta de activos móviles
- *Custodia personal o VIP*: Escolta personal en traslado.
- *VSS / CCTV*: Sistema de video vigilancia / Circuito cerrado de televisión.
- *Alarma monitoreada*: Alarma con monitoreo.
- *Sistemas de control de Acceso*
- *Sistemas de protección de incendios*
- *Alarma no monitoreada*: Alarma de respuesta auditiva.
- *Servicios de inteligencia e investigación*
- *Rastreo vehicular Satelital*
- *Control de acceso*

Es importante destacar que no todas las empresas ofrecen la totalidad de los servicios arriba descritos; algunas empresas tienen un perfil de seguridad basado en personal y en custodia física, otras están orientadas a la seguridad soportada por componente tecnológico (electrónico) y finalmente están las empresas que poseen una gama más amplia de servicios, ofreciendo estos productos de manera individual y también combinados para lograr soluciones que se adaptan mejor a las necesidades del cliente.

Análisis cualitativo de los servicios

Realizar un análisis comparativo, requiere revisar cada una de las características que componen los distintos servicios asociados a la vigilancia de hogares particulares. Esta revisión permite comprender si el producto definido en la hipótesis posee características de diferenciación o si debe tener un liderazgo de costos (Porter, 2015).

Para este análisis se consideran los siguientes servicios de la industria:

- Alarmas con monitoreo, VSS/CCTV,
- Vigilancia presencial y
- Alarma sin monitoreo,

por tratarse de servicios que pueden aplicar para el segmento de hogares particulares, y poder contrastarlo con el servicio de Video vigilancia con AI planteado.

La comparación se realiza con las siguientes características normalizadas:

- *Identificación Biométrica*: Comprende la identificación de la identidad por rasgos físicos como la huella digital, el iris, el rostro. Este tipo de identificación requiere un soporte de consulta propio donde se almacenan los rasgos de cada individuo

asociado a la identidad y el proceso solamente realiza la identificación por comparación.

- *Identificación personal:* Es realizada por una persona que constata la identidad solicitando documentación formal.
- *Detección de intrusión:* Capacidad de detectar eventos de acceso por vías y lugares no habituales, o por personas no autorizadas.
- *Privacidad:* Según si la privacidad es se puede asegurar o no, generalmente cualquier servicio basado en personas es susceptible a no respetar la privacidad del monitoreado.
- *Activación manual:* Según si el sistema requiere ser activado manualmente o no al dejar la propiedad.
- *Base de datos de sospechosos:* Capacidad de tener registro de sospechosos, algo poco habitual en la custodia de hogares.
- *Siempre Activo:* Según si puede estar activo siempre, independientemente haya habitantes en la propiedad.
- *Aviso:* Si posee capacidad de dar aviso.
- *Delivery de seguridad o escalación:* Si posee capacidad de llamar a la fuerza pública o policía para garantizar la seguridad del bien custodiado.

Como se puede observar en el Cuadro III, se incluyen características para evaluar en los distintos sistemas según si están presentes o no.

Servicio	Análisis cualitativo								
	Detección			Operación				Respuesta	
	Identificación Biométrica	Identificación personal	Detección de intrusión	Privacidad	Armado manual	Base de datos de sospechosos	Siempre activo	Aviso	Delivery de la seguridad
Alarma con monitoreo			Si		Si			Si	Si
Alarma sin monitoreo			Si	Si	Si				
VSS / CCTV			Si				Si	Si	Si
Vigilancia presencial		Si	Si					Si	Si
Sistema de video Vigilancia con IA	Si		Si	Si		Si	Si	Si	

Cuadro III: características de servicios de vigilancia a hogares particulares.

Dadas las características de los distintos servicios presentados en el Cuadro I, se puede confirmar, para el servicio de Video Vigilancia con AI, que posee las principales características de los demás servicios contrastados excepto el Delivery de la seguridad.

A pesar de contar con características positivas conjugadas de distintos sistemas existentes que lo dotan de lo que pareciera ser una propuesta de valor superadora, el hecho que la mayoría

de los productos de similares características realicen el Delivery de la seguridad, pareciera que lo sume en una evidente desventaja competitiva.



Universidad de
SanAndrés

5. Benchmark

Consideraciones

A continuación, se presenta el relevamiento realizado sobre empresas que ofrecen soluciones y servicios de video vigilancia con soporte de AI. Del presente relevamiento se han excluido los innumerables fabricantes de sistemas autónomos de grabación de video y funciones básicas de AI como detección de movimiento, por considerarlos sistemas simples que no ofrecen una solución avanzada en materia de seguridad, sino que son sistemas de grabación.

Relevamiento

Referencias

A continuación, se expone una tabla con el resultado de las características destacadas de los sistemas relevados de todo el mundo. Para simplificar un resumen tan complejo se ha optado por utilizar referencias simples en las columnas de la tabla que serán detalladas a continuación:

Cámaras STD: Cámaras estándar, dispositivos de captura de video que no contienen funciones de AI para el mejoramiento digital de la imagen.

Cámaras c/Ajuste: Cámaras con ajuste de imagen, dispositivos de captura de video que contienen funciones de AI para el mejoramiento digital de la imagen.

App. Mobile: Aplicación para dispositivos Mobile para la gestión del producto.

Consola central: Solución de software y hardware para gestión de monitoreo y alertas centralizadas.

VSSAI SW: Software de video vigilancia con soporte de Inteligencia artificial,

VSSAI HW: Hardware específico para software de video vigilancia con soporte de Inteligencia artificial o para aplicaciones de AI en general.

Puerta: Solución de video cámara para la puerta del hogar con capacidad permitir en algunos caso reconocimiento facial o simplemente la notificación de arribo de alguien a la propiedad.

Rec. Facial: Capacidades de reconocimiento facial para identificación de personas.

Rec. Objetos: Capacidades de reconocimiento de objetos, algunos ejemplos de esto son, personas, autos, paquetes, etc.

Manipulación: Hace referencia a la capacidad de identificar la manipulación de la propia cámara.

Detección por áreas: forma simple de aplicación de IA en sistemas de VSSAI donde se delimita un área de la imagen donde el sistema responderá a estímulos, por ejemplo, la detección de movimiento en una ventana.

Mascotas: capacidad de hacer seguimiento a mascotas que quedan solas en el hogar.

Grabación de video: soportan grabación de video.

Gestión de alertas: Permite realizar gestión de alertas, lo más habitual en este punto es la configuración de notificaciones.

Segmento de mercado: a que mercado o aplicación está destinado el producto.



Tabla consolidada

Relación con el mercado		Componentes					Servicios asociados					Segmento de mercado								
		B2B	B2C	Cámaras STD	App Mobile	Consola central	VSSAI HW	Puerta	Rec.Facial	Rec.Obj.	Manipula- ción	Detección por áreas	Mascotas	Grabación de video	Gestión de alarms	Costo (USD /Month)	Hogarero	Comercios	Espacio público	
SI																				
SI																				
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															
SI		SI	SI	SI	SI															

Tabla I: Benchmark de Soluciones de Video vigilancia

Análisis de benchmark

Para el análisis de las ofertas disponibles del mercado se contempla la revisión más detallada de aquellas que incluyan soluciones de video vigilancia con complemento de IA para hogares, por ser las que compartirán el segmento objetivo de mercado. La selección de las soluciones abarca los siguientes fabricantes:

- Intellivision
- Google Nest + Nest Aware
- SmartSentry AI
- Arlo
- Ring
- Guardian Systems

Intellivision

Es un software para integrar a cámaras inteligentes fabricados por terceros con características de AI avanzadas, pero no conforman un producto que compita directamente por que no tiene un modelo de servicios. Tampoco comercializa directamente a clientes, sino que tiene una modalidad de relacionamiento B2B y su objetivo de mercado son integradores de soluciones o fabricantes de hardware.

Google Nest + Nest Aware

Google Nest es una serie de dispositivos hogareños y para domótica que permiten integración de toda la línea de productos con aplicación Mobile.

Nest Aware, es un servicio que se integra a la línea de cámaras “Google Nest” y los complementa con un servicio que permite grabación del hogar y una serie limitada de configuración de alertas.

El usuario debe adquirir cámaras y luego debe suscribir el servicio.

El servicio permite detectar una persona, sonidos, o movimiento en zonas de actividad restringida, pero no puede identificar rostros.

El costo es US\$ 5 mensual

SmartSentry AI

Es una solución de Hardware para análisis de video con capacidades de reconocimiento de personas u objeto, sin reconocimiento facial y puede reportarlo en el dispositivo mobile.

Reconoce objetos y movimiento en zonas específicas de la imagen.

El costo del servicio es US\$ 10 mensual

Arlo

Arlo ofrece cámaras de video con capacidad de reportar eventos que pueden estar en el orden de personas apareciendo en cuadro, o, por ejemplo, hacer seguimiento de objetos tales como paquetes.

El suscriptor debe comprar cada cámara más el costo del servicio que asciende aproximadamente a US\$ 3 por cámara.

Ring

Cámaras de video con capacidad de reportar eventos de movimiento, o de actividad en zonas específicas, sin capacidad de reconocimiento facial o ID.

Guardian Systems

Sistema de seguridad con video cámaras con funciones avanzadas de AI que incluyen el reconocimiento facial, objetos, personas, etc.

El servicio tiene un costo de la suscripción de US\$ 40 mensuales.

Conclusiones de Benchmark

De todos los proveedores identificados, solamente es posible reconocer la solución a la empresa “Guardian Systems” como un producto muy similar con el que se compartiría un mismo target de mercado. El producto se presenta en la forma de un servicio mensual, aunque con un costo algo elevado respecto de otros productos observados.

Para poder competir en el mercado contra este tipo de empresas, con modelos de negocio similares al propuesto, con bajos costos operativos, es necesario construir valor a través de algún diferenciador que permita crear tracción sobre el mercado.

6. Justificación del negocio

Para la justificación del negocio se plantea realizar una validación por comparación de un caso de negocio de sistema de vigilancia con soporte de AI versus un típico servicio de alarma con monitoreo.

El motivo de la selección para el caso comparativo es el resultado de una encuesta realizada (ver Anexo II) que determina el sistema de alarma con monitoreo es el más elegido entre aquellos que poseen sistemas de seguridad con monitoreo.

Adicionalmente, por las características comparativas del modelo de servicio, se trata del tipo de servicio con mayor similitud entre todos los posibles servicios existentes.

La comparativa se realiza para el mercado argentino porque de acuerdo a lo observado en el capítulo anterior, se trata del mercado más chico de entre los cuatro mercados evaluados: proponer una justificación de negocio para un mercado pequeño plantea un real desafío para un nuevo modelo de negocios.

El mercado argentino

El análisis del mercado debe considerar como mínimo dos aspectos fundamentales para poder ser evaluados posteriormente en el plan de negocios. En primer lugar, estimar su tamaño, es decir el volumen posible de la demanda que permita luego calcular el valor total del negocio. En segundo lugar, incluir algunos parámetros que permitan comprender qué tan propenso podrá ser el mercado a adoptar nuevos servicios o productos que contribuyan a la seguridad personal.

Según las estadísticas oficiales de seguridad, solo en Argentina, durante el año 2018, el total de robos alcanza la cifra de 456.600 de delitos contra la propiedad (Estadísticas Criminales En La República Argentina – Año 2018, 2019) que representa una tasa de 1026 delitos por cada 100 mil habitantes. Esta cifra, salvo pequeñas variaciones, se mantiene estable durante los últimos años y por supuesto no incluye otros delitos como violaciones, homicidios, etc. que incrementaría la estadística haciendo que la cifra sea superada fácilmente.

No debe pasarse por alto que estos datos corresponden solamente a los hechos denunciados, por lo tanto, son solo una parte del total de hechos ocurridos. Esta visión de que no todos los hechos de inseguridad son denunciados, coinciden en buena medida, con otras estadísticas realizadas fuera del ámbito gubernamental, como por ejemplo, el “Observatorio de la Deuda Social Argentina de UCA” emitido en 2016, que dice que, para ese mismo año, el 24,3% de los hogares urbanos han sufrido un hecho de delincuencia o violencia (Bonfíglío et al., 2017). A manera de ejemplo, si se extrapolase este valor para el centro urbano más

grande de Argentina, Buenos aires y Gran Buenos Aires, la estadística representa más de 850.000 hogares con hechos de inseguridad, casi el doble respecto de las estadísticas oficiales.

Otro dato, también relevante y que se puede utilizar para aproximar una comprensión de la situación del mercado, es el de la percepción de riesgo (Bonfíglio et al., 2017) que es una medida subjetiva determinada por el porcentaje de personas mayores de 18 años cuya valoración de la posibilidad de ser víctima de un delito es alta. En el estudio, dicho índice alcanza el valor de 72,3% de las personas con alta percepción del riesgo que representado en el total de la población de la ciudad de Buenos Aires más los 24 partidos del Gran Buenos Aires, se corresponde con aproximadamente 9 millones de personas con una percepción de riesgo elevada.

Hasta este punto de la revisión, los datos aportados son referencia, fundamentalmente del volumen total del mercado. Será necesario incluir un dato más que permita realizar una aproximación que se ajuste más a la realidad, puesto que no resulta lógico pensar que habrá efectivamente más de 9 millones de personas dispuestas o con capacidad de comprar servicios de seguridad solo porque su percepción de la inseguridad es elevada.

Esta selección de una parte del mercado o segmentación se realiza aplicando el indicador de nivel socioeconómico a los valores anteriores para los segmentos que más se ajusten como potenciales suscriptores de servicios de seguridad. Los segmentos seleccionados serán el ABC1 y C2 (Muraro, 2018) que representan el 23,4% de las familias y por lo tanto un volumen aproximado de poco más de 800.000 hogares.

Respecto de la información de la industria, solamente se han conseguido datos de CASEL. El resto de las cámaras de la industria no proveen información de mercado, por lo menos de manera pública, solamente algunas pocas empresas publican información de gestión, pero no relevante para comprender la situación de Mercado.

Es razonable, para este trabajo, considerar los datos de aportados por CASEL debido a dos motivos principales:

- el volumen de empresas afiliadas, con un 38% del total de empresas relevadas,
- es una cámara que agrupa empresas con afinidad a brindar soluciones técnicas o tecnológicas comparables al servicio planteado en la tesis.

La Universidad Católica de Argentina en conjunto con CASEL elaboró dos informes de situación de la industria el primero del año 2012 y el segundo del año 2018. Se trabaja con el último informe disponible puesto que no sólo es el más actualizado, sino que incluye los datos relevados en el informe anterior.

Facturación

La facturación total relevada en el informe CASEL, muestra los siguientes datos que resultan interesantes resaltar:

- La industria experimentó un crecimiento durante los ocho años previos, en algunos casos, la variación inter-anual, fue superior a un dígito (Ver Gráfico IV). Todo esto en un contexto de país cuya actividad económica, refleja todo lo contrario, es decir que, a pesar de una economía con valores de crecimiento negativo, la seguridad privada y en particular electrónica, creció notablemente.

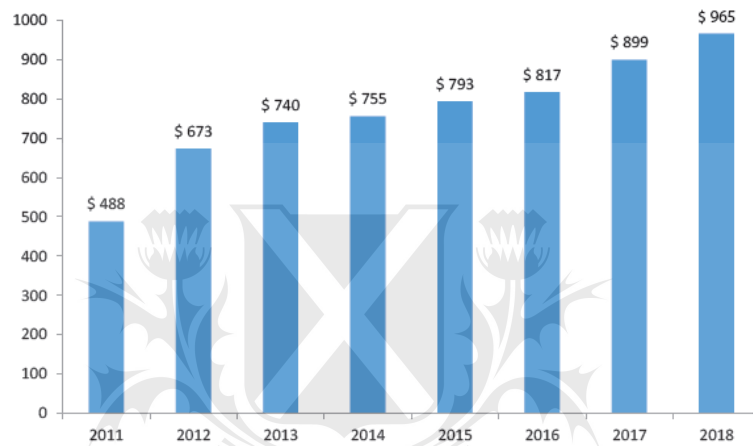


Gráfico IV: Facturación de la industria años 2011-2018 (Carballo et al., 2018)

Este crecimiento de una industria de seguridad pareciera estar sostenido por la situación social del país; el informe “Observatorio de la Deuda Social Argentina de UCA” del año 2016 refleja que la percepción de riesgo (Bonfoglio et al., 2017) que es una medida subjetiva determinada por el porcentaje de adultos cuya valoración de la posibilidad de ser víctima de un delito es alta, este índice alcanza el valor de 72,3% de las personas encuestadas.

- El nivel de facturación obtenido en el último período relevado, donde alcanzó los 965 millones de dólares.

Estos dos hechos del informe, el crecimiento interanual y el volumen total, son dos indicadores de potencialidad del crecimiento mayor de mercado, como se verá más adelante en el análisis FODA de la propia industria.

Empresas

Partiendo entonces del estudio de Mercado (Carballo et al., 2018) de CASEL, se encuentran ciertos datos importantes para tener un mayor grado de conocimiento de la Industria. El cuadro IV, fue elaborado como un resumen parcial del mencionado reporte.

Aquí se puede observar que el estudio divide las compañías en cuatro segmentos: Grandes, Medianas tipo 1 y 2 y Pequeñas. Mientras las empresas pequeñas predominan en cantidad, totalizan el 86%, las medianas alcanzan al 8% y las grandes, el restante 6%.

	Segmento de empresas			
	Pequeñas	Medianas T1	Medianas T2	Grandes.
Composición porcentual	86%	7%	1%	6%
Empleados	15221	3103	2980	4532
% Empleados	59%	12%	12%	18%
Empleados promedio	1268	239	1490	29

Cuadro IV: Composición de empleados según el tamaño de la empresa. (fuente CASEL)

Se desconoce el criterio de selección para empresas medianas tipo 1 y tipo 2, cómo se verá más adelante con la información complementaria, no se encuentra relación entre cualquiera de los indicadores y el tipo de empresa mediana, la categorización pareciera estar dada por un criterio cualitativo más que por algún criterio económico o de gestión.

Rubros de actividad de las empresas

Otro corte de la información obtenida desde el informe CASEL permite obtener datos agrupados por los distintos rubros que conforman la totalidad de los servicios de seguridad electrónica. Dichos rubros son:

- Fabricante: fabricante de distintos componentes tales como cableado, plaquetas, etc.
- Software: desarrollo de software para plaquetas y/o aplicaciones, Aunque en informe aclara que para la fecha de emisión la actividad de desarrollo de software es muy incipiente.
- Distribuidor: agrupa a intermediarios Distribución productos y componentes.
- Integrador/ instalador
- Monitoreo: los servicios de monitoreo que originan respuestas preventivas y paliativas.
- Prevención de incendios: Protección electrónica automática contra incendios (industrial).

A continuación, se presenta el Cuadro V de valores comparativos de Facturación y Empleados por cada uno de los rubros arriba listados.

	Rubros					
	Fabricante	Software	Distribuidor	Integrador/ Instalador	Monitoreo	Prevención de Incendio
% Facturación	1%	0%	8%	11%	66%	14%
Cantidad de empleados	268	24	677	3332	21370	165
Relación Empleados por cada punto porcentual	268	N/A	85	303	324	12

Cuadro V: Valores comparativos de facturación según el rubro empresa. (fuente CASEL)

La agrupación por rubro permite definir un indicador que puede ser utilizado como KPI de la industria y realizar un análisis preliminar del rendimiento de cada rubro del negocio.

La relación entre la cantidad de empleados y cada punto porcentual (p.p.) de facturación permite aproximar comparativamente el rendimiento de cada uno de los rubros. Cuanto más alto el valor, mayor es la cantidad de empleados necesaria para sostener la operación. Este valor puede variar conforme a la eficiencia de los procesos operativos de cada empresa, una empresa con mayor nivel de madurez operativa será más eficiente en el uso de los recursos y este indicador resultará menor, respecto de otras empresas cuyos procesos operativos sean más precarios.

Utilizando el KPI se pueden comparar los rubros “Monitoreo” con “Prevención de incendio”. Dado que este último posee una estructura de costos del personal asociado al servicio muy baja en relación al primero, la comparación evidencia la diferencia operativa entre ambos.

Es importante indicar que el rubro “Prevención de incendios” se asemeja al servicio desarrollado en el presente trabajo ya que no requieren una práctica operativa constante realizada por mano de obra especializada. Se necesita instalación y revisiones/inspecciones periódicas.

Otro indicador complementario a este mismo KPI, es el que relaciona Empleados con Dinero abonado en concepto de salarios. Para ello se considera el acuerdo del convenio colectivo de trabajo (Insua, 2018) del año 2018 (mismo año del informe CASEL) y se elaboró el siguiente Cuadro:

	Rubros		
	Integrador/ Instalador	Monitoreo	Prevencion de Incendio
% Facturación	11%	66%	14%
Cantidad de empleados	3332	21370	165
Acuerdo salarial CCT 507/2007 Vigencia Agosto 2018 (AR\$)	\$ 24.073	\$ 22.578	\$ 24.073
Estimación Salario + SAC y Cargas sociales	\$ 40.924	\$ 38.383	\$ 40.924
Salarios abonados en 2018 (AR\$)	\$ 1.636.309.214	\$ 9.842.833.944	\$ 81.029.718
Conversion dólar 2018 (AR\$ 28 por U\$D)	\$ 58.439.615	\$ 351.529.784	\$ 2.893.919
Relación Salarios Abonados/p.p. facturación	\$ 5.312.692	\$ 5.326.209	\$ 206.708
Porcentaje de la facturación total abonado en concepto de salarios	6%	36%	< 1%

Cuadro VI: Valores comparativos de facturación, empleados, y volumen total de salarios abonados según el rubro empresa. (fuente: CASEL y CCT 507/07 Acuerdo salarial 2018)

En el Cuadro VI se puede observar:

- El contraste entre la estimación del volumen total de AR\$ y U\$S abonados en concepto de salarios para cada rubro, donde para el caso de “Monitoreo” el gasto en salarios es 25 veces mayor que el de “Prevención de Incendio”.
- El porcentaje sobre la facturación anual que representa el total de dinero abonado en concepto de salarios para cada rubro. Se ve en la última fila del cuadro: “Porcentaje de la facturación total abonado en concepto de salarios”. Aquí el rubro “Monitoreo” destina el 36% de la facturación para el pago de salarios, mientras que “Prevención de incendio” destina menos del 1%.

Análisis estratégico

Estrategias genéricas

Realizar un análisis estratégico del nuevo producto propuesto, requiere evaluar el que tipo de estrategia de negocios se deberá aplicar. Es necesario comprender si se logrará adhesión de clientes a partir de una diferenciación o sí será sostenido, desde la propuesta de valor, por una estrategia de liderazgo de costos (Porter, 2015).

Hay dos tipos de competencia. Por un lado, están las empresas que compiten de manera directa, es decir que ya ofrecen sistemas de seguridad con soporte de IA, se trata de empresas que ofrecen servicios similares al que se plantea en el modelo de negocios. Sistemas que por una suscripción de pago mensual incorporan algunas características como el reconocimiento facial. Las empresas de este tipo fueron relevadas en el benchmarking. Para este tipo de empresas la estrategia más razonable deberá ser la diferenciación.

Por otro lado, están las que basan su servicio en métodos tradicionales, como lo son, la seguridad electrónica con monitoreo remoto o servicios de vigilancia presencial, que, tal como se viene observando, los servicios están marcados por una fuerte participación de mano de obra en los distintos procesos de operación. La estrategia para enfrentar este tipo de competencia, parece ser por liderazgo de costos.

Será necesario explorar un poco más en detalle cada una de estas opciones y que implica cada una de ellas:

Diferenciación

Como ya se revisó en el análisis cualitativo de los servicios, el sistema propuesto posee algunas características conjugadas de otras soluciones y algunas características netas de diferenciación.

Las características conjugadas (Ver Cuadro III) de otros servicios de la Industria son:

- **La identificación Biométrica:** El sistema es capaz de reconocer quiénes son los habitantes del hogar. Esta capacidad de identificar hasta el momento, sólo puede equiparada por una identificación de vigilancia presencial, es decir, sólo puede ser realizada por una persona.
- **Siempre activo:** esta característica de poder estar permanentemente activo no es aplicable a servicios de alarma con o sin monitoreo, pero si a los servicios de video vigilancia remota y vigilancia presencial.
- **El aviso:** Como casi todos los otros servicios, tendría la capacidad de avisar anomalías de seguridad a su propietario.

Las características adicionales propias de diferenciación son:

- **Base de datos de sospechosos:** capacidad de tener identificados en una base de datos propia, a sospechosos de anomalías previas ocurridas en cualquier suscriptor del servicio. Esto permite que el sistema anticipe dicha información al dueño del hogar en el momento que ocurre una anomalía y realiza el aviso.
- **Red de contactos de confianza:** el sistema habilita la posibilidad de definir grupos de destinatarios para los avisos de incidencias, enviando notificaciones a personas dentro del círculo de confianza del suscriptor del servicio. De esta forma se definen verdaderas redes de interconexión de suscriptores interesados en participar activamente del proceso de “respuesta” y realizar Delivery de la

seguridad (que como se estableció en la especificación inicial, estará a cargo del suscriptor).

Desventaja competitiva

Adicional a las características comunes entre el servicio propuesto y los demás servicios existentes, hay una que no está presente desde la definición en la propuesta de inicial, esta característica es el Delivery de la seguridad.

Este Delivery de seguridad es un proceso que implica, al momento de detectar una anomalía, un contacto inicial con los propietarios para validar la situación. En caso de no poder contactar a nadie, implica el envío de un móvil para realizar una evaluación en forma presencial. Eventualmente, con posterioridad puede implicar contacto con las fuerzas de seguridad para contrarrestar la amenaza.

Entonces, los servicios actuales se ocupan de contactar a la policía, mientras que, en el servicio propuesto es el propietario del hogar quien debe ocuparse. En este sentido, la falta de una propuesta de valor que iguale a la de la Industria en términos de Delivery de Seguridad es una desventaja competitiva permanente, y hace que la opción de orientar el servicio a un posicionamiento de liderazgo por costos sea la mejor manera de captar valor del mercado.

A los efectos de validar la relevancia que posee la desventaja competitiva antes mencionada, se diseñó una encuesta de mercado a la cual se le incorporó otra premisa asumida al comienzo del trabajo.

El diseño de la encuesta consta de un breve cuestionario, que hace énfasis en solo dos aspectos: Delivery de seguridad, y “Privacidad” (en este último caso, validando si es o no una necesidad real -Insigth-).

Es importante mencionar que, al finalizar la encuesta, si bien la muestra no resultó representativa, los resultados obtenidos permitieron recabar información valiosa (ver Anexo). Por ende, este elemento no fue considerado para efectuar conclusiones, pero permitió hacer un análisis de tendencias.

Liderazgo de costos

Para que el servicio propuesto (VSSAI) pueda liderar por costos, es necesario verificar si es factible lograr una operación de bajo costo respecto de la operación de los servicios tradicionales (Monitoreo) y que sea sostenible en el tiempo para poder compensar o contrarrestar cualquier intento del resto de la industria por defenderse.

Considerando tanto el KPI de salarios abonados por cada punto porcentual de facturación (ver Rubros de actividad de las empresas) como la relación de salarios abonados entre el total de la facturación de la industria se puede demostrar que el rubro “Monitoreo” posee altos costos operativos, por tener una elevada cantidad de personal asociado al servicio, lo que a su vez evidencia la factibilidad de poder competir con un liderazgo por costos con servicios de valor agregado de alta tecnología.

El Modelo de negocio comparado

Modelo de la industria

A continuación, se muestra Diagrama I con el modelo de negocio de las empresas de la Industria para el servicio de monitoreo de hogares particulares.

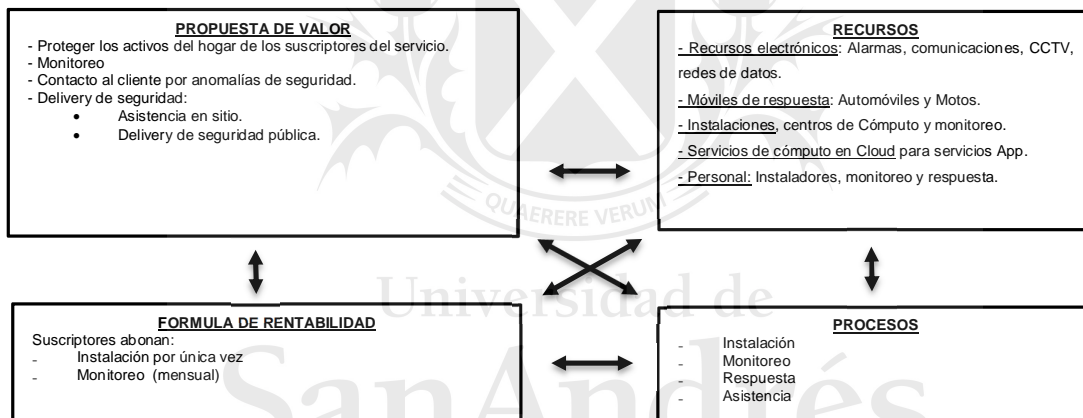


Diagrama I: Modelo de negocios de monitoreo

Para la fórmula de rentabilidad no se ha conseguido información suficiente que permita realizar un análisis cuantitativo. No obstante, se espera realizar una comparación cualitativa de los demás aspectos del modelo de negocios que propone la tesis, y así lograr un entendimiento mayor de cuáles son las diferencias fundamentales entre ambos.

Modelo de negocios de la tesis

Propuesta de valor

Tomando como base el modelo de negocios de la industria, es necesario realizar varios ajustes para convertirlo en el modelo del servicio propuesto en la tesis.

Como se viene mencionando, la modificación de la propuesta de valor se reduce específicamente en Delivery de la seguridad, siendo reemplazado por una actividad que recae en el suscriptor del servicio, ya que es el mismo quien debe revisar las imágenes de la anomalía y decidir si es necesario realizar dicho Delivery.

La propuesta incluye diferenciadores para crear valor y estar en condiciones de competir sin entrar en una guerra de precios. Los diferenciadores son dos:

- posibilidad de definir una “red de contactos de confianza” para establecer conexiones con cercanía geográfica de modo de que puedan participar activamente y recíprocamente en la seguridad del otro. Esto permite al suscriptor disparar el Delivery de la seguridad, ante una anomalía real en su domicilio y dar aviso a los vecinos cercanos. Este esquema sería homólogo a una alarma vecinal, permitiendo a los vecinos estar alerta y participar activamente del incidente.
- “Base de datos de sospechosos” que permite que el sistema centralice la identificación de personas responsables de anomalías de seguridad en hogares distintos suscriptores. El sistema guarda registro de responsables de hechos delictivos a distintos suscriptores, permitiendo obtener información más precisa sobre un individuo puntual, no solo sobre la cantidad de hechos delictivos permite cruzar la información y generar reportes de horarios, días, zonas en las que el sistema registró anomalías.

Esta diferenciación de la propuesta de valor trae aparejada la necesidad de modificar los demás componentes de la propuesta. Debido a la relación intrínseca de los cuatro pilares descritos en Diagrama I, veremos uno a uno como se van modificando.

Recursos

Para los recursos hay un recorte grande del modelo debido a que buena parte de la infraestructura como personal ya no será necesario para sostener la operación, se reducirán drásticamente los costos, no solo por la no existencia de personal asociado al monitoreo, sino que también por los costos enterrados como ser los móviles de respuesta, oficinas, infraestructura de centros de monitoreo, etc.

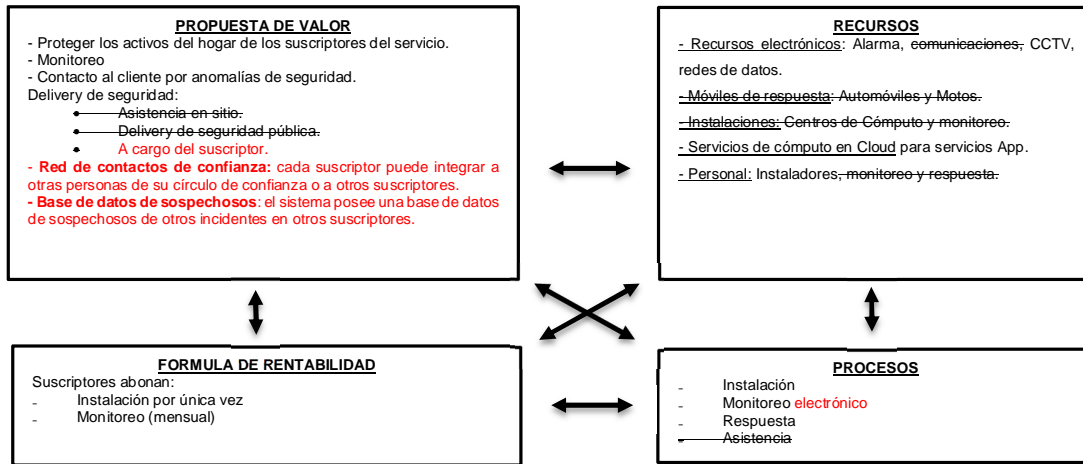


Diagrama II: Modelo de negocios de monitoreo basado en IA.

Procesos

Desde el punto de vista de los procesos operativos, solamente la Instalación conserva la mayoría de los aspectos. Se modifican notablemente el monitoreo y la respuesta (reporte de anomalías) que tomarán un corte totalmente digital. Y por último, la asistencia de móviles que no está presente.

Fórmula de rentabilidad

La fórmula de rentabilidad no cambia conceptualmente respecto de la de la industria, sigue requiriendo un pago por la instalación más la suscripción mensual por servicio de monitoreo. Es necesario alinear la fórmula de rentabilidad al tipo de estrategia genérica de liderazgo de costos. Esto permitirá adecuar el valor del servicio de modo que ofrezca un incentivo a cambiar hacia otro con una funcionalidad más acotada, (sin Delivery de seguridad), pero con un valor percibido más alto por ser económicamente más conveniente.

Efectos de red

Los efectos de red del servicio de VSSAI están dados por dos funcionalidades que se obtienen como consecuencia de su digitalización. Ellas son: la capacidad de identificar sospechosos de una base de datos central, que a su vez es alimentada por anomalías anteriores de todos los suscriptores, y la posibilidad de definir la red de contactos de confianza para el aviso de anomalías.

Estas dos capacidades aportan efectos de red, aunque de distinta forma:

- ✓ **Base de datos de sospechosos**

La base de datos central de sospechosos tiene la finalidad de almacenar el ID biométrico del rostro de cada una de las personas que fueran identificadas por suscriptores como causantes de anomalías. Esto funcionaría de manera similar a una red social de tránsito (por ejemplo, WAZE,), donde un adherente puede ingresar datos a la plataforma sobre la ubicación de un sistema de control de tránsito automático (foto-multa) y esta información es consumida por todos los otros suscriptores de la aplicación. Aquí un suscriptor podría definir el ID biométrico obtenido de un intruso, como responsable de una anomalía y enriquecer la base de datos central de sospechosos. A partir de esto, cuando el sistema de cualquier otro suscriptor le revele que la persona que está generando una anomalía en su hogar está asociada a otro hecho de inseguridad, podría reforzar el énfasis del aviso aportándolo como información adicional.

El sistema se nutre de anomalías de seguridad a través de la registración de incidentes en la base de datos, incorporando identificaciones faciales de los responsables. Con las sucesivas registraciones, el sistema aumenta su valor porque al contar con mayor volumen y nivel de precisión de la información, se puede lograr mejores resultados en la explotación de datos. Como ejemplo, se menciona el uso de mapas de calor del delito para uso de la Seguridad Pública; y a su vez, de darse esta última aplicación, el suscriptor podrá verse beneficiado por la posible captura y/o recomposición de objetos producto del delito.

✓ **Red de contactos de confianza**

La posibilidad de construir una red de contactos de confianza representa una característica que compensa la falta de Delivery de seguridad del VSSAI. Esto está dado por la posibilidad de que cada suscriptor pueda predefinir que la respuesta del sistema alcance no solo a él, sino que también a su círculo de confianza directo, permitiendo que más personas tomen conocimiento de la anomalía de seguridad que esté sucediendo y participe de la respuesta.

Este grupo de confianza puede estar integrado por:

- Personas allegadas al suscriptor, parientes, amigos, etc. que aceptan recibir alertas (por afinidad o relación estrecha).
- Personas con un interés recíproco en resolver cuestiones de seguridad que pasan a ser colaboradores solidarios, por ejemplo, vecinos. Cabe aclarar que deben ser suscriptores.

Este último, es un fenómeno de colaboración comparable a las alarmas vecinales, donde los vecinos acuerdan cuidarse unos a otros, y por lo tanto, entre todos contratan una alarma vecinal y cada uno tiene un disparador.

En relación a este último grupo, en el caso particular de vecinos, es comparable con las alarmas vecinales, donde los vecinos acuerdan cuidarse unos a otros, y por lo tanto, entre todos contratan una alarma vecinal y cada uno tiene un disparador. De la comparación surge lo siguiente:

- En el Sistema como en Alarma Vecinal, los vecinos son recíprocamente solidarios.
- En Alarma Vecinal, la detección está a cargo de los propios vecinos. Hay cercanía.
- En el Sistema, a detección está automatizada. Hay ubicuidad.

El concepto de la red de contactos de confianza eleva la capacidad de respuesta a partir de disponer de una mayor cantidad de personas recibiendo alertas, que también pueden participar del Delivery de seguridad contactando a la fuerza pública.

El efecto de red está vinculado exclusivamente a las personas del segundo grupo antes expuesto. El sistema les permite formar una red de contactos, una comunidad participativa y solidaria, donde todos contribuyen en términos de seguridad.

Cinco fuerzas

A continuación, se presenta el análisis de las cinco fuerzas de Porter:

Rivalidad de los competidores.

- Se trata de una industria con mucha fragmentación, mucha cantidad de empresas muy pequeñas, varias grandes con una facturación elevada.
- La propia industria acusa una gran capacidad de innovación
- Estructura de costos fijos elevada, esto hace complejo el camino hacia una digitalización total del servicio.

Los nuevos entrantes

- Bajas barreras de entrada por tratarse de servicios con alto nivel de digitalización.
- Servicio fácilmente imitable.

- El Switching cost bajo, es importante ser el first mover en el mercado y apalancar con pocos los efectos de red disponibles para retener clientes.

Los proveedores

- Bajos costos de hardware y múltiples proveedores disponibles.
- Los servicios de computo (Cloud) en una situación similar al hardware, varios proveedores, capacidad a demanda y bajo costo.

Los clientes

- Los clientes no tienen altos costos de transferencia. Cambiar de proveedor puede resultar relativamente fácil.
- No hay grandes diferenciadores.
- Probable alta sensibilidad al precio que juegue a favor de un servicio de bajo costo.

Los sustitutos

- Muchos sustitutos con un mayor costo operativo.
- Bajos switching cost.

FODA

FODA de la industria

El estudio de Mercado de CASEL, además de indicadores de la industria, ofrece análisis FODA realizado a partir de encuestas con diversos gerentes de la Industria. A continuación, se presenta el Cuadro VI, con el análisis FODA de la Industria.

FORTALEZAS	OPORTUNIDADES
<ul style="list-style-type: none"> • Profesionales idóneos y capacitados. • Rapidez de la innovación para adaptarse a la demanda. • Empresas con imagen de marca muy relevante. 	<ul style="list-style-type: none"> • Potencialidad de crecimiento y Expansión de mercado. • Articular medidas en seguridad público-privado. • Desarrollar el mercado externo exportador.
DEBILIDADES	AMENAZAS
<ul style="list-style-type: none"> • Falta de coordinación homogénea. • Falta de adecuación a las normativas y mejores prácticas. Necesidad de regulación/legislación clara. • Falta de desarrollo en el interior del país y las provincias. • Dependencia de productos importados. • Falta de acceso al crédito. 	<ul style="list-style-type: none"> • Macroeconomía y volatilidad política. • Sobredemanda de seguridad pública. • Competencia desleal por venta online de productos de baja calidad (distorsión de precios relativos). • Falta de conocimiento del sector por parte de funcionarios. • Empresas no “especializadas” dejan al cliente sin asesoramiento y soporte postventa.

Cuadro VII: Análisis FODA de la industria. (fuente CASEL)

FODA del servicio propuesto

Contar con un análisis FODA elaborado por la industria resulta un buen punto de partida para elaborar el propio del servicio propuesto (VSSAI).

El análisis FODA del servicio propuesto (ver Cuadro VII) incluye algunos puntos del análisis de la industria, pero obviamente cambiados en relación al rol que cumplen desde la misma, por ejemplo, mientras que las “empresas de la industria tengan una imagen de marca relevante” es una fortaleza para ellas, representa una amenaza para un producto sustituto, que intenta generar una disrupción en el mercado.

Fortalezas	Oportunidades
-La mayoría de Capacidades de otros servicio conjugadas -Menor costo operativo que el resto de la industria -Efectos de Red	-Ser el first mover en AI a nivel doméstico. -Potencialidad de crecimiento y Expansión de mercado -Desarrollar mercado exteno exportador -Falta de desarrollo en el interior del país
Debilidades	Amenazas
-Delivery de la seguridad -Dependencia de productos importados -Falta de acceso al crédito	-Empresas de la industria con imagen de marca muy relevante. -la industria con capacidad de Rapida innovación para adaptarse a la demanda -Profesionales idóneos en el resto de la industria

Cuadro VIII: Análisis FODA del servicio propuesto (VSSAI)

Puede observarse en este último análisis FODA cómo aparecen en el área de fortalezas aquellas capacidades logradas a partir de la introducción de la innovación.

Modelo de servicios comparado

A continuación, se presenta un cuadro con un ejercicio comparativo sobre costos y resultados de ambos modelos. La comparación está basada en la mayor cantidad de datos reales actualizados de la industria obtenidos del informe CASEL y en otros casos con una estimación basada en relevamientos de distinta índole.

Usuarios	Industria			Propuesta			
	Concepto	USD		Concepto	USD		
Estructura de costos del suscriptor	Instalación (única vez)	\$ 170,00		Instalación (única vez)	Computo Edge AI	\$ 50	\$ 160
					Hdd (1 TB)	\$ 20	
	2 Cámaras video	\$ 50					
	monitoreo/ asistencia (Mensual)	\$ 27,00		Servicio (Mensual)	Instalación	\$ 40	\$ 10,00
Cloud services					\$ 0,12		
Garantía equipos					\$ 1,80		
				Margen	\$ 8,09		
Estructura de costos del servicio	Concepto	Personas	USD/Mes	Concepto	Personas	USD/Mes	
	Instaladores	4	\$ 5.000	Instaladores	4	\$ 5.000	
	Técnicos	2	\$ 3.000	Técnicos	4	\$ 6.000	
	Administrativos /comerciales	4	\$ 6.000	Administrativos /comerciales	4	\$ 6.000	
	Monitoreo	36	\$ 49.349				
	Asistencia	18	\$ 26.308				
	Instalaciones	3	\$ 5.000	Cloud database Services		\$ 900	
	Servicios comunicaciones	-	\$ 3.000	Cloud Compute Services (AKS)		\$ 690	
				Network data transfer		\$ 620	
	Total		\$ 97.657	Total		\$ 19.210	
Estimación de resultados	Total facturado	\$ 162.000,00		Total facturado	\$ 60.000,00		
	Gastos de servicio	\$ 97.657,41		Gastos de servicio	\$ 19.210		
	EBITDA	\$ 64.342,59		EBITDA	\$ 40.790,00		
	Impuestos (32%)	\$ 20.589,63		Impuestos (32%)	\$ 13.052,80		
	Resultado	\$ 43.752,96		Resultado	\$ 27.737,20		

Cuadro IX: Ejercicio de resultados comparativo

Lo que se observa en el Cuadro V, es la estimación de los resultados operativos de servicio a 6000 usuarios con cada uno de los dos modelos: la industria (izquierda) y la propuesta de la hipótesis (derecha).

Consideraciones de la estimación:

- se definió monto de suscripción del servicio basado en IA USD 10. E
- La estimación radica fundamentalmente en el cálculo de personal necesario para el monitoreo, tomando seis personas por turno, se estiman tres turnos de 8 horas

los días de semana y lo mismo para los fines de semana. Para asistencia se considera la mitad de la gente requerida para Monitoreo.

El resultado del ejercicio da que la industria captura valor por un 27% de la facturación mientras que el servicio propuesto en la hipótesis captura el 46%.



7. Plan de negocio

Introducción del negocio

El negocio tiene como objetivo sustituir servicios existentes de vigilancia hogareña - con relativa a fuerte dependencia de mano de obra especializada- por servicios de vigilancia por video y componente de inteligencia artificial, es decir, eliminando total o parcialmente la mano de obra y reduciendo, de esta forma, los elevados costos de operación.

La empresa

El nombre de la empresa será Hal-O Technologies y se dedicará a desarrollar soluciones de seguridad con soporte de inteligencia artificial. Con el lanzamiento de su línea de productos en distintos mercados espera cambiar la manera en la que se concibe la seguridad de activos particulares y adquirir mercados que hoy no están explotados por las soluciones convencionales de seguridad.

Visión, Misión y Valores

Visión

Ser la empresa líder de servicios de seguridad de las américas a través de mejorar la calidad de vida de sus habitantes, para llegar a ser reconocida como sinónimo de seguridad e innovación.

Misión

Nuestra misión es desarrollar negocios basados en desarrollos de alta tecnología de inteligencia artificial con foco en el cliente y sostenidos por un proceso constante de Innovación y Mejora Continua.

Valores

Entre nuestros valores encontraremos cualidades de empresas de vanguardia como son: la honestidad, la ética, la vocación de servicio, el trabajo colaborativo, la integración de las personas, el foco en el cliente, el desarrollo personal, el desarrollo del negocio, la honestidad, y la vocación de servicio, la creatividad, la evolución, la adaptación al cambio y la eficiencia.

Segmentos de mercado

La definición de los segmentos de mercado está signada por la sensación de seguridad, como se revisó en el marco teórico, solo en Argentina, la percepción del riesgo alcanza un valor cercano al 80% (Bonfiglio et al., 2017), en otros países como México el indicador alcanza valores similares, en hogares, la sensación de inseguridad llega al 78% (Instituto Nacional de Estadística, 2020). Este indicado demuestra, que el fenómeno de la inseguridad atraviesa a la mayor parte de la sociedad en la mayoría de los países.

Adicionalmente, se considera que desarrollar un producto orientado a los hogares debido a que, si bien existe para estos segmentos, una gran oferta de sistemas tradicionales de seguridad, pocos tienen características como las de soporte de inteligencia artificial, que lo dotan de algunos factores diferenciadores respecto de los sistemas tradicionales, estos son:

- Económico: la posibilidad de ofrecer el servicio a un costo notablemente más económico. Esto se debe a que los costos operativos estarán definidos por cómputo mientras que los sistemas tradicionales deben sostenerlo con mano de obra especializada.
- Protección mejorada: Otra característica inherente a implementación con la tecnología de IA es la posibilidad de que el sistema sea totalmente automático y proteja a los propietarios aun cuando estos estén dentro del hogar.

No se considerarán productos para custodiar segmentos del sector comercial ni público debido a que, para estos, ya existe una variedad de oferta relativamente alta en el mercado. Además, se trata de soluciones más complejas que requieren no solamente identificar rostros, armas u otros objetos, sino que requieren identificar situaciones, acciones que son funciones más avanzadas, propias de sistemas más complejos de producir.

En resumen, los segmentos están compuestos por personas de una amplia franja etaria de la sociedad, que viven en hogares familiares, ya sean Casas o Departamentos. Para este gran conjunto inicial de la población, existen dos posibles estados, aquellos que hoy no cuentan con un sistema de seguridad en el hogar y los que sí lo poseen. A su vez, de estos últimos, hay dos subcategorías que están dadas por el tipo de sistema de protección con la que cuentan: Por un lado, los que tienen sistemas de seguridad con monitoreo, típicamente alarmas monitoreadas, y, por otro, los que tienen contrato de seguridad con vigilante o garita de vigilancia.

Tamaño del mercado

Para la estimación del tamaño del mercado se tomará como base el porcentaje de población con sensación de inseguridad elevada, si lo considerásemos para Argentina, nos da un tamaño máximo teórico de mercado cercano a ocho millones de hogares. El mismo indicador para México redonda en un valor tres veces más grande (cerca de veintidós millones de hogares).

Para dimensionar el mercado objetivo, se utilizará un punto de vista conservador asumiendo que solamente el 1% de los hogares mencionados en el párrafo anterior, por lo tanto, solo considerando México y Argentina el mercado esperado alcanza los 300.000 suscriptores.

Producto / Propuesta de valor

El diseño del producto parte del estudio de los Empathy maps en los que se modeló la situación y necesidades de los potenciales segmentos: Los segmentos considerados, ya mencionados en la sección de Segmentos de mercado, son:

- Los habitantes de casas y departamentos que no poseen sistema de seguridad.
- Los habitantes de casas y departamentos que poseen garita de vigilancia.
 - Los habitantes de casas y departamentos que poseen sistema de seguridad con monitoreo.

Con estos mapas de empatía se trabajó en dar forma al Value proposition canvas a partir del cual logra identificar como satisfacer necesidades de usuarios para lograr una propuesta de MVP específico.

La definición del MVP para satisfacer segmentos contiene ciertas características claves que permiten definir el producto atractivo para los segmentos. A continuación, se enumeran las características claves del producto:

- Capacidad de identificar personas
 - Sin falsas alarmas: Esta misma capacidad de identificar tiene un agregado de valor para el morador de la vivienda, porque implica que este no deberá realizar ninguna tarea específica como ingresar un código al llegar al hogar, el solo acceder normalmente y dejar que el sistema haga su trabajo.
 - Mayor disuasión: El Hecho que de que el sistema, haciendo uso de su “**Base de datos de sospechosos**”, pueda “recordar” y reconocer a

una misma persona responsable de hechos delictivos distintos lo dota de un poder de disuasión mayor, porque será “testigo” imparcial y confiable del historial delictivo de un delincuente.

- Siempre encendido: parte de mejorar la seguridad del hogar implica un sistema que siempre este activo, esto mejora la situación particularmente por que no requiere que el propietario suscriptor deba recordar encenderlo al salir o apagarlo al llegar.
- Red de contactos de confianza: Facilitará e integrará la vinculación con otras personas para protección recíproca. Esto permitirá tejer redes con personas en la misma situación, formando una red bilateral que aumenta el valor percibido del producto, ya que cuantas más personas posean el sistema y formen parte de mi red de contactos de confianza, mayor cantidad de gente habrá en capacidad de recibir una alerta del sistema y brindar ayuda.
- Costo: El costo es el último componente que permite el servicio mejore la ecuación de valor percibido por el cliente y se genere fuerte adopción.

Una característica fundamental asociada al último punto (el costo) es que el producto deberá ser presentado como un servicio, de esta forma se pretende construir una estrategia de monetización basada en pagos mensuales más accesibles al usuario facilitando el on-boarding para cualquiera de los segmentos determinados. Por lo tanto, la solución de video vigilancia con componente de Inteligencia Artificial se comercializará en modalidad de Servicio; en consecuencia, de aquí en más haremos referencia a la misma como tal.

Componentes del servicio

El servicio estará compuesto de varios componentes. A continuación, se enumeran la totalidad de los mismos:

- a) Dispositivo con Inteligencia de Borde: un componente de equipo de cómputo local o de borde que interactúa con los distintos tipos de sensores instalados en la propiedad.
- b) Núcleo de sistema en Cloud: Una componente de servicio centralizado que integrará la funcionalidad de todos los componentes conformando un sistema de seguridad integral del hogar.
- c) Base de datos de sospechosos: Registración de IDs de personas denunciadas como responsables de hechos de inseguridad.

- d) Aplicación Mobile: Interfaz de usuario desde donde este podrá realizar una gestión integral de su seguridad, su red de contactos de confianza, alertas, revisión de videos y gestiones del servicio en general, reclamos, cambios en el nivel de servicio, etc.
- e) Sensores: El tipo principal de dispositivos asociados al servicio serán las cámaras de video para captura, detección y reconocimiento de personas. Pero además será posible instalar micrófonos, altavoces, detectores humo/incendio, gas y monóxido de carbono.

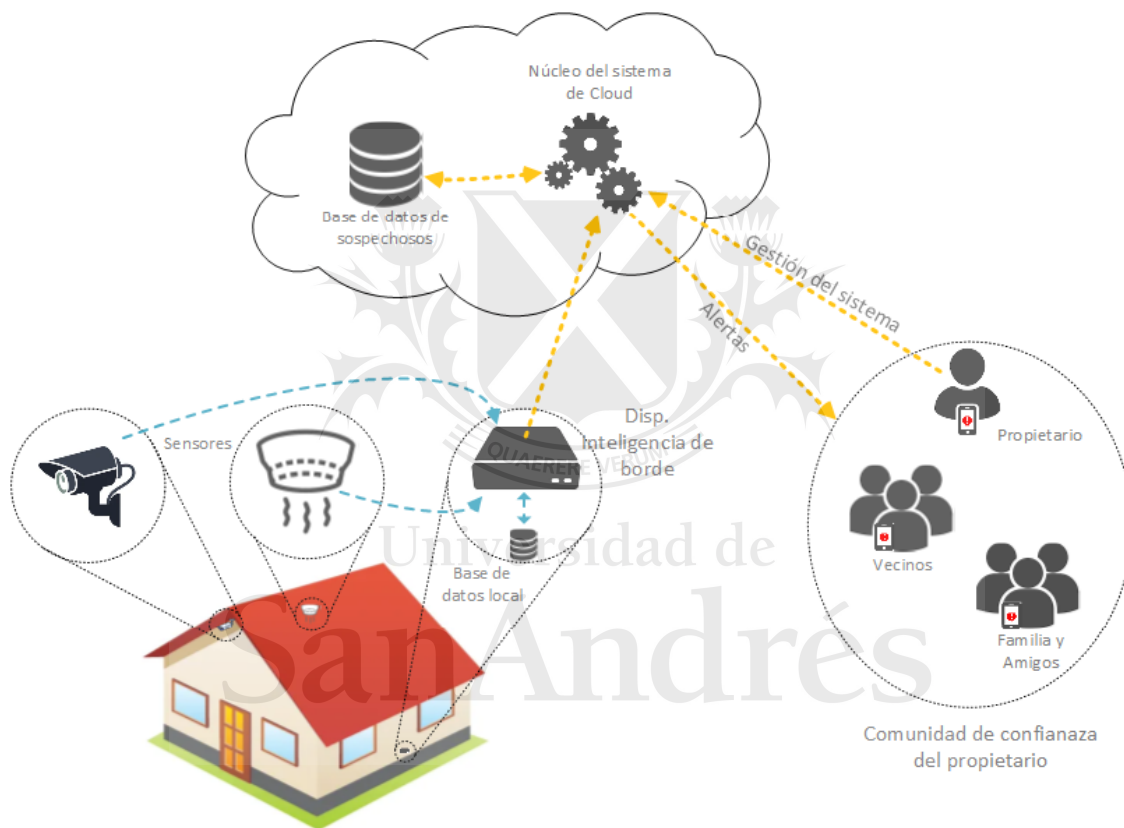


Grafico V: Descripción y componentes del servicio

Características del servicio

El servicio está orientado al segmento de mercado de hogares particulares ya sean estas casas, consorcios de edificios o barrios cerrados. Con capacidades aportadas por la inteligencia artificial se buscará dotar al sistema de las siguientes funcionalidades:

- Identificación o reconocimiento Facial: capacidad de reconocer patrones biométricos del rostro para identificar la persona que ingresa se encuentre o acceda al hogar.

- Reconocimiento de situaciones anómalas: personas trepando, saltando rejas, forcejeo y empuñando de armas.
- Plataforma: Su naturaleza de plataforma está dada por dos características diferenciadoras incorporadas en el servicio:
 - Red de contactos de confianza: donde existan varios usuarios con cercanía geográfica, el producto les permitirá formar parte de una comunidad cerrada de “vecinos en alerta” permitiendo que todos sean a la vez usuarios formen parte de un esquema recíproco donde mejoran su percepción de seguridad porque saben que sus vecinos cercanos cuidan de ellos y viceversa.
 - Base de datos centralizada: la capacidad de que el sistema pueda identificar el rostro de personas previamente identificadas como participantes de actos delictivos a otros suscriptores del servicio. Esto se logra con una base de datos centralizada de personas reportadas por los propios suscriptores del servicio. Cada sistema instalado y suscriptor tiene la capacidad de enriquecer dicha base de datos.
- Otras capacidades más habituales: la posibilidad de detectar humo, fuego y gases peligrosos en espacios cerrados.

Costo al suscriptor

Cada suscriptor contrata el servicio origina cuatro tipos de costos distintos que deben ser cubiertos para poder iniciar y sostener el servicio:

- 1) Hardware Base: el costo hardware base del servicio está compuesto por el costo del dispositivo de inteligencia de borde y dos cámaras.
- 2) Sensores extra: en caso de ser solicitado por el suscriptor, puede contratar cámaras adicionales u otros dispositivos disponibles, como sensores de gases (gas natural, monóxido, humo).
- 3) Instalación: el costo de instalación, implica mover un técnico al sitio del suscriptor y realizar la instalación de acuerdo a las recomendaciones del área de Delivery.
- 4) Servicio Mensual: este costo de servicio se descompone en el seguro del equipamiento incluido en la tarifa más el costo del cómputo en cloud necesario para articular las distintas características del mismo.

Algunos de estos costos serán absorbidos por el negocio y otros serán cargados al cliente en el momento de la instalación. El cuadro X muestra la manera en la que se distribuirán los costos de los distintos componentes del servicio de cara al on-boarding:

Costos del suscriptor				
Costos de on-boarding	Hardware Base	Disp. de inteligencia de borde	\$ 70	A cargo del negocio
		2 cámaras de video	\$ 50	
	Sensores extra	Camara de video	\$ 25	A cargo del suscriptor
		Humo	\$ 8	
		Gas	\$ 8	
		Monóxido	\$ 6	
Instalación		\$ 40		
Costo mensual del servicio		\$ 10		

Cuadro X: Distribución de los costos de on-boarding

El costo del Hardware de base será absorbido por el negocio, esto facilitará posibles suscriptores la evaluación de costos de on-boarding además porque los servicios convencionales de alarmas / cámaras monitoreadas no absorben este tipo de gasto y lo cargan íntegramente al suscriptor.

Diseño de la organización

El diseño de la organización debe considerar ciertos elementos que son característicos de empresas cuyas operaciones están distribuidas en distintos países, con un núcleo operativo único desde donde se espera dar servicio a todos los mercados.

Filiales o subsidiarias

Para los mercados más grandes, el negocio se organizará abriendo filiales locales, permitiendo definir distintas estrategias de comercialización a la medida de cada país. A su vez, los objetivos de las filiales serán ajustados a su realidad y entorno, de este modo se espera dotar a las filiales de la agilidad necesaria para que puedan proponer sus métodos de relacionamiento con su mercado; por ejemplo, alguna filial podrá optar por una modalidad de comercialización B2B, firmando alianzas estratégicas con carriers de internet quienes dispongan de su estructura se encarguen de la distribución del servicio con marca propia.

Los mercados más pequeños serán dirigidos desde las subsidiarias regionales. A continuación, se presenta la lista de las cuatro filiales definidas para Latinoamérica y USA, cada una con el listado de países de injerencia:

- Argentina: Chile, Uruguay, Paraguay y Bolivia.
- Brasil

- Colombia: Perú, Ecuador y Venezuela.
- Estados Unidos
- México: Centroamérica

Cada una de estas filiales serán responsables de desarrollar las siguientes actividades:

- ✓ Atención al cliente.
- ✓ Entrenar las áreas de “Delivery”.
- ✓ Realizar investigación y campañas de mercado.
- ✓ Promoción de ventas.
- ✓ Realizar acuerdos / alianzas comerciales.
- ✓ Cumplir los requisitos legales locales.

Delivery e Instalación

Las funciones del área de Delivery serán la de coordinar y dar soporte al área de Instalación que, como su nombre lo indica, realizará las operaciones de instalación, puesta a punto y encendido inicial del dispositivo de inteligencia de borde y los sensores en el domicilio del suscriptor. Las funciones del área de Delivery serán las de realizar la coordinación y soporte a los terceros que realicen la instalación.

El área de instalación deberá ser terciarizada debido a que no se desea sumar a este plan de negocios, la complejidad inherente a este tipo de actividades. Esta tercerización puede ser llevada adelante a través de una alianza comercial o sencillamente por contratación a empresas que realicen este tipo de servicio y se les abone por equipo instalado.

Shared Services

Se creará un área de shared services que tomará a su cargo la componente del tecnológica del servicio. El Core del servicio será desarrollado, implementado y soportado por esta área, quien a su vez venderá el servicio a las distintas subsidiarias, quienes pasaran a ser intermediarias entre el servicio y los suscriptores.

Shared services tendrá a su cargo todo lo concerniente a investigación y desarrollo más el adicional de soportar y sostener el servicio, para lo que se deberá contar con un área de tecnología necesaria para montar el servicio sobre tecnologías Cloud desde donde se podrá crecer de manera elástica racionalizando los costos.

Organigrama

El organigrama es el siguiente:

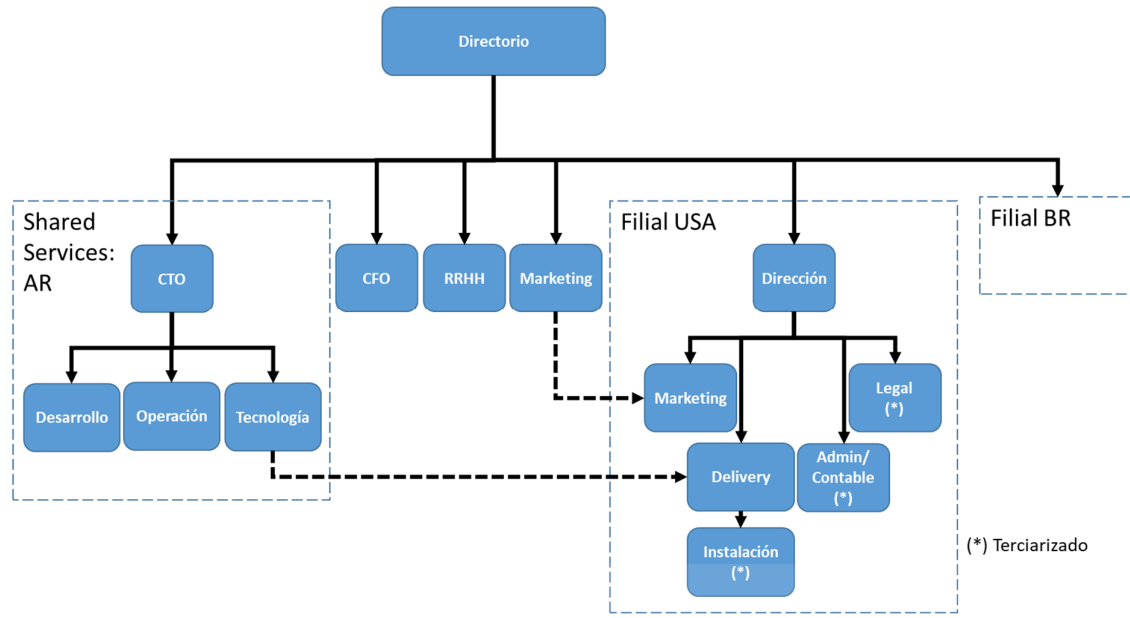


Diagrama III: Organigrama

Cada mercado deberá contar con una filial propia que será responsable por las operaciones en su mercado. Sin embargo, algunas áreas de cada filial tendrán alguna dependencia secundaria con áreas centrales tal es el caso de “Delivery” y el caso de Marketing.

El área de “Delivery” tendrá una dependencia técnica con el área de Tecnología de “Shared Services”, esto se debe a que desde Tecnología se establecen los parámetros de instalación y producto de la componente que se instala en el hogar, recordemos que el servicio cuenta con una componente en el sitio del bien a custodiar.

Marketing será el otro sector con dependencia secundaria con áreas centrales. El área de Marketing local a cada filial deberá diseñar y ejecutar los planes de introducción del servicio en su mercado de incumbencia alineado con los objetivos estratégicos de la propia subsidiaria.

Adicionalmente, la dependencia con al área central de Marketing estará dedicada a llevar una gestión unificada del reconocimiento y sondeo permanente del mercado para no pasar por alto nuevos insights y evaluar de manera centralizada y propagarlos hacia otros mercados.

Cultura

La cultura organizacional estará fuertemente marcada por rasgos propios de una empresa que perseguirá la innovación. La finalidad será el sostenimiento de la calidad del servicio y el consecuente posicionamiento del servicio en el Mercado.

La anterior definición se debe a que existe un punto de atención que radica en lo fácilmente imitable que son los diferenciadores lo que se plantea como “el problema” del plan de negocio, ya que existen competidores en capacidad de moverse con relativa velocidad y presentar una propuesta de valor que al menos iguale la propia, determinando la pérdida de la ventaja competitiva obtenida con los diferenciadores.

Contrarrestar dicha situación dependerá de continuar teniendo un producto atractivo, por lo tanto, es necesario que se continúen desarrollando nuevas capacidades o funcionalidades, para ser agregadas a la propuesta de valor. A partir de promover la innovación, se espera mantener el servicio en el estado del arte, es decir, a la vanguardia de las capacidades y funcionalidades que el mercado identifique como valiosas.

Debido a esto será necesario llevar adelante una **Planeamiento estratégico emergente**, que estimule permanentemente el aporte de innovación en todas las áreas.

Las principales características de la cultura y los valores asociados son:

- Calidad humana.
 - Honestidad
 - Ética
 - Vocación de servicio
- Trabajo en equipo.
 - Colaborativo.
 - Integración de las personas.
 - Foco en el cliente.
- Compromiso.
 - Con el negocio.
 - Desarrollo personal.
 - Eficiencia
- Innovación y Mejora Continua.
 - Evolución.
 - Creatividad.
 - Calidad
 - Adaptación al cambio.

Modelo de negocios

El modelo de negocios basado en el Business Model Canvas

Socios clave

Para este modelo de emprendimiento existen dos tipos de socios clave posibles: , los proveedores de hardware y los socios en la comercialización.

El principal insumo material será el Hardware, por lo tanto, su fabricante (como proveedor) será clave en el desarrollo del negocio. Dado que este nivel de dependencia no es deseable, una manera de mitigar su importancia o el poder del proveedor será teniendo proveedores múltiples. Esto generalmente no resulta fácil ya que, para que el componente de Software funcione en distintos tipos de Hardware, este debe ser certificado para cada uno de ellos, lo que resulta ser un trabajo mayor y un ciclo de pruebas más extenso, por ende, mayor costo de desarrollo.

Un segundo socio clave, en una estrategia para apalancar la venta y lograr rápidamente los efectos de red mencionados previamente, se dará a través de alianzas comerciales con proveedores de internet; por un lado, porque el acceso a internet es un requisito del servicio, pero también porque una alianza de este tipo permitiría obtener información para segmentar de manera más precisa los segmentos de clientes objetivos.

Actividades clave

Las principales actividades del modelo de negocio, por su criticidad son:

- La instalación: debido a situaciones técnicas inherentes a la tecnología, como la ubicación de las cámaras, la luz, la señal de Wifi, etc. Debe ser llevada adelante por personal capacitado que asegure el adecuado funcionamiento del sistema. Un sistema mal instalado representará alta tasa de errores y mal servicio.
- El servicio: el núcleo del servicio es la componente a través de la cual se centralizan varias actividades, entre estas encontramos:
 - La gestión de alertas: su distribución y reporte a los miembros de una familia o de una la red de contactos de confianza.
 - El análisis de rostros desconocidos, su identificación con elementos en la base de datos central. El componente local solo tiene la capacidad de reconocer una cantidad finita de personas.

Recursos clave:

Los recursos clave son:

- El software: una vez completo su desarrollo y ciclo de pruebas, resulta clave por su funcionalidad y certificación con distintos equipamientos de hardware.
- Los empleados: son claves por su nivel de compromiso e involucramiento en el proceso de innovación y mejora continua. Y porque, a su vez, serán involucrados en un proceso constante de desarrollo de competencias personales y capacitación.

Propuesta de valor

Tal como se describe en la comparativa del modelo de negocio de la industria versus el modelo de negocio de la Tesis, la propuesta de valor cuenta con los siguientes elementos:

- ✓ Proteger los activos del hogar de los suscriptores del servicio.
- ✓ Monitoreo
- ✓ Contacto al cliente por anomalías de seguridad.
- ✓ Delivery de seguridad: a cargo del suscriptor
- ✓ Red de contactos de confianza: cada suscriptor puede integrar a otras personas de su círculo de confianza o a otros suscriptores.
- ✓ Base de datos de sospechosos: el sistema posee una base de datos de sospechosos de otros incidentes en otros suscriptores.

Respecto de la relación con el cliente es importante mencionar que el negocio apuntará a ser totalmente digital, se pretende con esto que el relacionamiento sea a través de las mismas herramientas Mobile, el cual provee el sistema con interfaz de usuario.

En el único momento que existirá trato directo con el cliente, será durante el proceso de instalación, dado que el cliente deberá recibir un representante de la empresa en su domicilio.

Canales

En cuanto a los canales de promoción se alcanzará a los clientes por todos los medios digitales más masivos: Facebook, Instagram, Youtube, etc.

Los canales de venta también serán **digitales**, es decir que con solo instalar la aplicación el suscriptor podrá solicitar la instalación y abonar los cargos de la misma y posteriores cargos

del servicio. Adicionalmente al canal de venta digital, se podrá suscribir por acuerdo comercial a través del distribuidor de cable.

Segmentos de clientes

La cantidad de segmentos es extensa, en principio es todo propietario o inquilino de propiedad o complejo habitacional existente. El producto tiene como objetivo toda persona cuya percepción del riesgo y sentimiento de inseguridad sea elevada (Bonfiglio et al., 2017).

Mercados

Un aspecto clave del negocio será el abordaje de distintos mercados. El presente plan de negocios contempla realizar un ingreso a distintos mercados de manera escalonada e incremental, donde se primará abordar el riesgo de cada etapa de manera controlada y con claros hitos de avance.

Las operaciones iniciarán en Estados Unidos, por tratarse del mercado más grande disponible, con capacidad suficiente para lograr que los efectos de red permitan consolidar el servicio. Adicionalmente existe la necesidad de captar la mayor cantidad de volumen posible con diferenciadores que son fácilmente imitables, entendiéndose que como *fist mover* hay una ventana temporal donde la propuesta de valor diferenciada tendrá chances de prosperar rápidamente.

Etapas de ejecución

El negocio iniciará en cinco etapas. La primera etapa será el desarrollo del producto, en la cual se avanzará en la definición detallada y la construcción del servicio. Será una etapa caracterizada por un fuerte trabajo de investigación y desarrollo.

Las siguientes cuatro etapas, si bien continuará con I+D, estarán dedicadas principalmente a la operación y expansión del negocio. En estas, se pretende desarrollar los planes de comercialización del producto, el abordaje específico para cada mercado. Esto implica trabajar detalladamente en como colocar el producto de modo que se ajuste adecuadamente a los aspectos de localización, ya sean de índole técnica, legal, impositiva o cultural.

A continuación, se presenta un diagrama de etapas, donde puede observarse el inicio y la duración de cada una de ellas -en cada mercado-. También se indica el inicio de las operaciones comerciales.

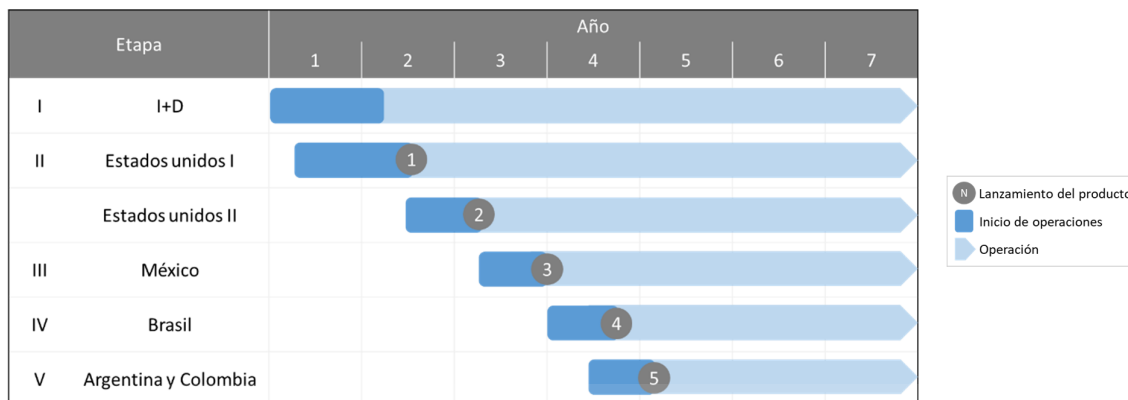


Diagrama IV: Etapas de desarrollo de producto y mercados

Etapa I: Investigación y Desarrollo

Esta etapa conlleva un fuerte trabajo de construcción de la componente de Hardware y Software del servicio. La característica principal de de la misma será un constante flujo de caja negativo, debido a que no se desarrollarán operaciones comerciales.

Una actividad importante de esta etapa será la del desarrollo de la cultura de la organización, a partir de seleccionar los candidatos más afines a la cultura delineada. Desde el inicio, se comenzarán a definir los procesos de inducción y los instrumentos de fidelización, tales como planes de evolución y desarrollo personal.

Esta etapa tendrá una duración de quince meses, donde se contratará cerca del 60% de la dotación total del área de Shared Services; l restante 40% será personal temporario o actividades terciarizadas. También se comenzarán a formar las áreas globales de RRHH y Marketing en línea con lo mencionado anteriormente, donde se espera construir la cultura organizacional -que deberá estar vigente en las etapas posteriores-.

El área estará formada en total por cuarenta y dos (42) personas, de las cuales en el área de desarrollo y tecnología en conjunto tendrán una dotación de veintisiete; de estos el 60% (16 personas) se contratarán en modalidad directa y el resto (11 personas) estarán en una modalidad temporal hasta la finalización de la etapa.

Etapa II: Inicio de Operaciones en Estados Unidos

Esta etapa comenzará tres meses después de la primera, el mercado inicial será el de Estados Unidos, abordándose de manera escalonada por tratarse de un mercado grande. Las operaciones comerciales comenzarán al final de la misma.

Se buscará formar rápidamente el equipo del área de Marketing global, quien tomará responsabilidades sobre la filial y quien, a su vez, formará su equipo de marketing local unos meses más adelante. En esta área se pretende realizar el desarrollo todo lo concerniente a las definiciones de Marketing, donde se buscará posicionar el servicio asociado a una imagen de calidad y alta fiabilidad. Se resalta que el nivel de exigencia del mercado establecerá un alto nivel de trabajo y calidad del producto, que redoblará la necesidad de contar con altos estándares de calidad.

Considerando el área de RRHH, se avanzará en el desarrollo de la cultura organizacional y la inducción del personal para las etapas venideras y apertura de las demás filiales.

El área de “Delivery” se formará como un spin-off del equipo de Shared Services, es decir que se buscará hacer sinergia con el área más técnica de la compañía, aspecto que se sostendrá en las etapas siguientes.

La dotación será de once personas, organizándose de la siguiente forma: un director de filial, cuatro personas en el área de marketing y seis personas en el área de Delivery.

Etapa III: Operaciones en México

El siguiente mercado a iniciar operaciones será México, esto se debe a que se trata de un mercado con cercanía y comunicación al norteamericano lo que facilitaría la promoción y adopción.

En esta instancia se espera contar con los procesos operativos ya delineados, lo que permitirá disminuir errores en el inicio de actividades.

La duración de esta etapa será de nueve meses y se ocupará de realizar la primera apertura a un mercado latinoamericano, donde no se buscará llegar a todo el país, sino que se desarrollará principalmente el centro-este del país y más adelante de iniciadas las operaciones, el resto.

La dotación en la filial México será de once personas con la misma distribución que la filial de Estados Unidos.

Etapa IV: Operaciones en Brasil

Brasil tiene una concentración de la actividad de seguridad sobre la zona Sudeste, donde esta zona representa el 49% del mercado local ((Reinach, 2020)) e incluye los dos conglomerados más grandes del país: São Paulo y Rio de Janeiro.

En esta etapa, de manera homóloga a la anterior, tomará al menos nueve meses comenzar la operación comercial.

La dotación en la filial Brasil también será de once personas, con la misma distribución que la filial de Estados Unidos.

Etapa V: Operaciones en Argentina y Colombia

Su objetivo es la apertura de las últimas dos filiales regionales y el inicio de operaciones comerciales.

La dotación en cada uno de estos dos países será de nueve personas, considerando, la dirección, dos personas para el departamento de marketing y seis para Delivery.

Progresión del negocio

Área	Año 1			Año 2	
	Semestre 1	Semestre 2	Semestre 3	Semestre 4	
Corporativo	<ul style="list-style-type: none"> Se constituye el directorio y la participación accionaria. Se incorporan: <ul style="list-style-type: none"> 1 Director de RRHH 1 Director de Finanzas 1 Director de Marketing 3 Colaboradores/analistas. Se comienza a definir la cultura de la empresa. Se comienza la selección de personal de Shared Services y la filial USA. 	<ul style="list-style-type: none"> Se inician conversaciones con empresas de difusión de internet para hogares (empresas de cable), para lograr acuerdos comerciales. 	<ul style="list-style-type: none"> Se consolida el diseño de la cultura e identidad de la empresa. Se diseñan los artefactos de identidad y compensación. Se establecen las metas comercialización. 	<ul style="list-style-type: none"> Se buscan oficinas en México. Se realizan los trámites de alta comercial. Se buscan relaciones que faciliten el inicio de operaciones. 	
Shared Services	<ul style="list-style-type: none"> Se constituye el área incorporando el personal propio: <ul style="list-style-type: none"> 1 CIO de sistemas 2 Líderes de desarrollo 1 Arquitecto Software 4 Desarrolladores 2 Tecnólogos (Cloud Services) 1 Líder de Tecnología Se contrataran (externos): <ul style="list-style-type: none"> 7 Desarrolladores 1 Científico de datos Se conforman las células de desarrollo. Se comienzan a evaluar plataformas de HW. 	<ul style="list-style-type: none"> Se incorporarán (Propios): <ul style="list-style-type: none"> 5 Desarrolladores 1 Líder de operación 14 Operadores/Admins Se contrataran (externos): <ul style="list-style-type: none"> 1 Especialista QA 2 Tecnólogos Se comienzan las pruebas con el primer prototipo. Se define la primera plataforma de HW, se firman acuerdos comerciales con al menos un fabricante. 	<ul style="list-style-type: none"> Continúa la búsqueda de plataformas alternativas de HW. Se comienzan a definir los procesos de instalación. Se crea la infraestructura en cloud para el soporte del servicio, se comienzan a generar los primeros gastos. Comienzan los planes de entrenamiento al personal de Delivery de México. 	<ul style="list-style-type: none"> Se definen dos plataformas de HW alternativas. Se finaliza el desarrollo del producto. Se reduce la dotación de desarrolladores contratados (7 desarrolladores). 	
Filial USA	<ul style="list-style-type: none"> Segundo trimestre, se forma la filial, se incorporan: <ul style="list-style-type: none"> 1 Director 1 Gerente de marketing local Líder de Delivery con reporte técnico a Shared Services. 	<ul style="list-style-type: none"> Se incorporan: <ul style="list-style-type: none"> 3 analistas de marketing Se buscan iniciar conversaciones con empresas de difusión de internet para hogares (empresas de cable), para lograr acuerdos comerciales. 	<ul style="list-style-type: none"> Se incorporan: <ul style="list-style-type: none"> 2 especialistas de Delivery comienzan a trabajar con la plataforma de HW. Comienzan las campañas de awareness del servicio. Se firman acuerdos comerciales con empresas de difusión de cable. 	<ul style="list-style-type: none"> Se inician las operaciones en algunas ciudades de alta densidad poblacional con mayores índices de delitos contra la propiedad en la zona Sud este. DFW, HOU, MIA. 	

Área	Año 3			Año 4	
	Semestre 5	Semestre 6	Semestre 7	Semestre 7	Semestre 8
Corporativo	<ul style="list-style-type: none"> Se inician conversaciones con empresas de difusión de internet para hogares (empresas de cable), para lograr acuerdos comerciales en México. Se establecen las metas comercialización. 	<ul style="list-style-type: none"> Se buscan oficinas en Brasil. Se realizan los trámites de alta comercial. Se buscan relaciones que faciliten el inicio de operaciones. 	<ul style="list-style-type: none"> Se establecen las metas comercialización. USA y MX Se buscan oficinas en Colombia. Se realizan los trámites de alta comercial. Se buscan relaciones que faciliten el inicio de operaciones. 	<ul style="list-style-type: none"> Se establecen las metas comercialización. USA y MX Se buscan oficinas en Colombia. Se realizan los trámites de alta comercial. Se buscan relaciones que faciliten el inicio de operaciones. 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Brasil. Ciclos de pruebas sobre nuevas plataformas de HW.
Shared Services	<ul style="list-style-type: none"> Se comienza a probar la incorporación de detectores de gases (Monóxido, GN, Humo). 	<ul style="list-style-type: none"> Incorpora funcionalidad de sensores de gases. Comienzan los planes de entrenamiento al personal de Delivery de México. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Brasil. Ciclos de pruebas sobre nuevas plataformas de HW.
Filial USA	<ul style="list-style-type: none"> Se incorporan: 2 especialistas de Delivery. Se extienden los acuerdos comerciales con empresas de cable para el Delivery de producto. Se forma la filial, se incorporan: 1 Director Gerente de marketing local. Líder de Delivery con reporte técnico a Shared Services. 2 analistas de marketing 3 especialistas de Delivery 	<ul style="list-style-type: none"> Se inicia la capacitación de instaladores del oeste. Campañas de awarress sobre detectores de Gases. 	<ul style="list-style-type: none"> Se extiende la comercialización a ciudades del oeste. SFO, LAX, LAS, SAN 	<ul style="list-style-type: none"> Se extiende la comercialización a ciudades del oeste. SFO, LAX, LAS, SAN 	<ul style="list-style-type: none"> Se extiende la comercialización a ciudades del oeste. SFO, LAX, LAS, SAN
Filial México	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awarress del servicio. Se inicia la capacitación de instaladores. Campañas de awarress sobre detectores de Gases. 	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awarress del servicio. Se inicia la capacitación de instaladores. Campañas de awarress sobre detectores de Gases. 	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awarress del servicio. Se inicia la capacitación de instaladores. Campañas de awarress sobre detectores de Gases. 	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awarress del servicio. Se inicia la capacitación de instaladores. Campañas de awarress sobre detectores de Gases. 	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awarress del servicio. Se inicia la capacitación de instaladores. Campañas de awarress sobre detectores de Gases.
Filial Brasil	<ul style="list-style-type: none"> Se incorporan: 2 especialistas de Delivery. Se extienden los acuerdos comerciales con empresas de cable para el Delivery de producto. Se forma la filial, se incorporan: 1 Director Gerente de marketing local. Líder de Delivery con reporte técnico a Shared Services. 2 analistas de marketing 3 especialistas de Delivery 	<ul style="list-style-type: none"> Se incorpora funcionalidad de sensores de gases. Comienzan los planes de entrenamiento al personal de Delivery de México. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Brasil. Ciclos de pruebas sobre nuevas plataformas de HW.
Filial Colombia y Arg.	<ul style="list-style-type: none"> Se incorporan: 2 especialistas de Delivery. Se extienden los acuerdos comerciales con empresas de cable para el Delivery de producto. Se forma la filial, se incorporan: 1 Director Gerente de marketing local. Líder de Delivery con reporte técnico a Shared Services. 2 analistas de marketing 3 especialistas de Delivery 	<ul style="list-style-type: none"> Se incorpora funcionalidad de sensores de gases. Comienzan los planes de entrenamiento al personal de Delivery de México. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Se comienza a prototipar funciones de reconocimiento de portación de armas. Evaluación de nuevas plataformas de HW. 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Brasil. Ciclos de pruebas sobre nuevas plataformas de HW.

Área	Año 5			Año 6		
	Semestre 9	Semestre 10	Semestre 11	Semestre 11	Semestre 12	Semestre 12
Corporativo	<ul style="list-style-type: none"> Se establecen las metas de comercialización. USA, MX, BRA, ARG y COL 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Argentina y Colombia. 	<ul style="list-style-type: none"> Se establecen las metas de comercialización. USA, MX, BRA, ARG y COL 			
Shared Services	<ul style="list-style-type: none"> Pruebas de funciones de reconocimiento predictivo. 	<ul style="list-style-type: none"> Comienzan los planes de entrenamiento al personal de Delivery de Argentina y Colombia. 				
Filial USA		<ul style="list-style-type: none"> Se extiende la comercialización a ciudades del noroeste. JFK, BOS, JER, IAD, BUF 				
Filial México	<ul style="list-style-type: none"> Extender el servicio a ciudades de menor escala: MTY, GUA, CJZ, TIJ 		<ul style="list-style-type: none"> Extender operaciones al resto de las ciudades. 			
Filial Brasil	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Se inicia la capacitación de instaladores. 	<ul style="list-style-type: none"> Se inician operaciones en las principales ciudades del centro este. RIO, BSB, GRU 		<ul style="list-style-type: none"> Extender operaciones al resto de las ciudades. 		
Filial Colombia y Arg.	<ul style="list-style-type: none"> Se inician conversaciones con empresas de difusión de internet para hogares (empresas de cable), para lograr acuerdos comerciales. 	<ul style="list-style-type: none"> Se firman acuerdos comerciales con empresas de distribución de cable. Comienzan las campañas de awareness del servicio. 	<ul style="list-style-type: none"> Se inician operaciones en las principales ciudades. BOG, MDE, CAL, BAR -BUE, SFE, COR, MDZ 			

Área	Semestre 13	Año 7	Semestre 14
Corporativo	<ul style="list-style-type: none"> • Se establecen las metas de comercialización. USA, MX, BRA, ARG y COL 		
Shared Services			
Filial USA			
Filial México			
Filial Brasil			
Filial Colombia y Arg.	<ul style="list-style-type: none"> • Se extienden operaciones al resto de las ciudades. 		

Análisis económico

El análisis de costos se realizará tomando como base la moneda dólares estadounidenses US\$, esto se debe a que es necesario considerar una moneda que permita establecer un patrón común a los diferentes mercados sobre los que se pretende operar.

Costos fijos

La revisión de costos fijos del análisis, considera todos los costos asociados a la operación y consideran los elementos como instalaciones, salarios, servicios (e-mail), accesos a Internet para los colaboradores y algunos servicios que serán terciarizados.

A continuación, se muestra el Cuadro XI que contiene la estimación de costos fijos sobre la premisa del plan de negocio, considerando el inicio de las operaciones en cada mercado y alineado a las etapas de ejecución del plan.

		Año						
		1	2	3	4	5	6	7
Costos Fijos	Corporativo	\$ 197.400	\$ 197.400	\$ 197.400	\$ 197.400	\$ 197.400	\$ 197.400	\$ 197.400
	Shared Services	\$ 857.520	\$ 741.360	\$ 625.200	\$ 625.200	\$ 625.200	\$ 625.200	\$ 625.200
	USA	\$ 654.930	\$ 873.240	\$ 873.240	\$ 873.240	\$ 873.240	\$ 873.240	\$ 873.240
	México			\$ 253.080	\$ 337.440	\$ 337.440	\$ 337.440	\$ 337.440
	Brasil				\$ 326.688	\$ 326.688	\$ 326.688	\$ 326.688
	Argentina					\$ 122.856	\$ 245.712	\$ 245.712
	Colombia					\$ 122.856	\$ 245.712	\$ 245.712
Costos enterrados	Shared Services	\$ 140.000					\$ 140.000	
		\$ 1.849.850	\$ 1.812.000	\$ 1.948.920	\$ 2.359.968	\$ 2.605.680	\$ 2.991.392	\$ 2.851.392

Cuadro XI: Costos Fijos en US\$

En este cuadro puede observarse la evolución de los costos fijos separados por país de manera anualizada.

Costos variables

Los costos variables están compuestos por dos componentes:

- los costos del equipamiento y su instalación, cada vez que un propietario suscribe el servicio, este costo será completamente cargado al suscriptor, del mismo modo que al suscribir otro servicio de monitoreo electrónico, deberá abobar el costo del hardware que ronda con instalación incluida en US\$ 160.
- el costo resultante del servicio, el gasto operativo de los sistemas que residen en Cloud y tienen además de costos de operación (absorbidos por Shared Services), costos de infraestructura que deben ser cubiertos.

Si bien el costo de cómputo es variable y es contratado desde Cloud, cuya característica principal es la flexibilidad, hay una cantidad mínima de infraestructura que se puede contratar para suplir el servicio. A esta cantidad mínima de hardware la llamaremos *Unidad de cómputo* (UCpt). Cada UCpt tiene un costo de operación de US\$ 2410 al mes y permite suplir el servicio hasta 6000 suscriptores sin con altos estándares de calidad. Por lo tanto, a partir del momento en que se agregue el suscriptor 6001, este requerirá contratar una nueva UCpt incrementando el costo en la misma cantidad mencionada previamente. De esta forma, la infraestructura de Cloud se incrementará en pequeños saltos a medida que se van sumando suscriptores al servicio.

Unidad de cómputo en cloud (base 6000 Suscriptores)	
Cloud Database Services	\$ 900
Cloud Compute Services	\$ 690
Respaldo	\$ 200
Network data transfer	\$ 620
	\$ 2.410

Cuadro XII: Composición de costos (US\$) por Unidad de cómputo (UCpt)

Proyección de negocio

En función de la incorporación de mercados, y teniendo en consideración su tamaño, se ha trazado una curva de adopción del servicio que resulta llamativamente más vigorosa en un mercado como el de México y Brasil, algo menos en Estados Unidos, y más conservadora en Argentina y Colombia.

La proyección de on-boarding de suscriptores asume que, al final del séptimo año, contratarán el servicio algo más de un millón de personas entre todos los mercados, por lo que esto representa el 0,2 % del total de la población de dichos mercados.

A continuación, se presenta la curva de adopción de cantidad suscriptores por país.

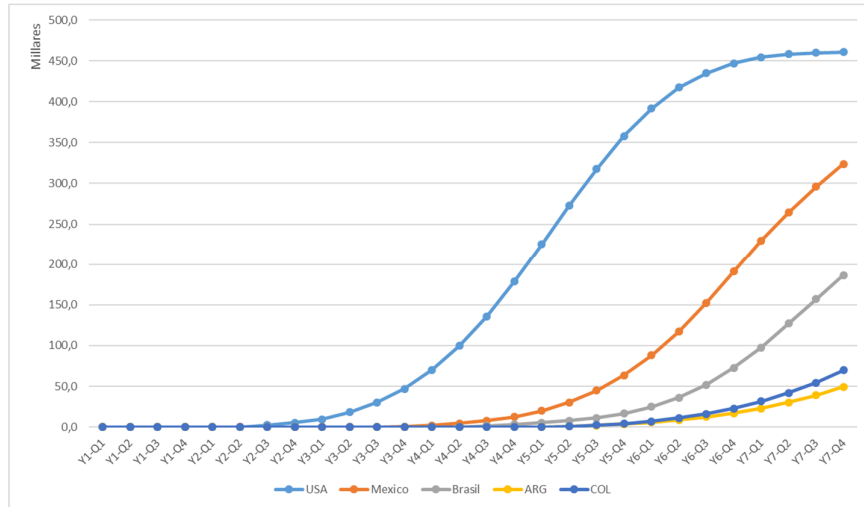


Gráfico V: On-boarding por país en cantidad de suscriptores

A partir de la estimación de on-boarding se calculó el costo total de las operaciones para los primeros siete años. Esto permitió que se definiera el monto total de la inversión para el desarrollo del negocio, a partir de conocer el punto de equilibrio. A continuación, se presenta el gráfico de Costos e ingresos totales que permiten observar este punto de equilibrio hacia el quinto año de inversión.

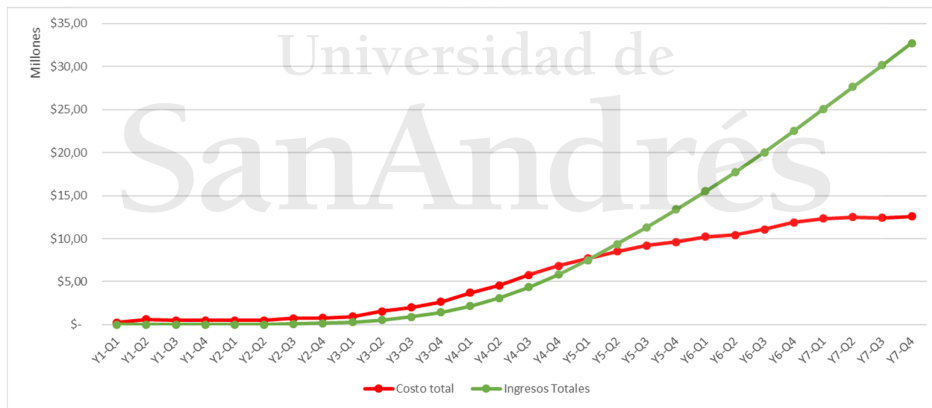


Gráfico VI: Costos e ingresos totales por Quarter en US\$

Tal como se observa en el gráfico, el equilibrio se logra en el segundo Quarter del quinto año

Flujo de la inversión

A partir de lo mencionado en los puntos anteriores, se ha determinado que el del flujo de inversión del proyecto tendrá una duración total de 5 años hasta el punto de equilibrio que se conseguirá con la incorporación una cifra cercana a los 300.000 suscriptores. A continuación, puede observarse el flujo de inversión anual para los primeros cinco años; y puede verse que el monto total de la inversión asciende a US\$ 13.706.660 a erogar en 5 años, de acuerdo a la siguiente distribución:

	Año					Total
	1	2	3	4	5	
Erogación de fondos	\$ (1.849.850)	\$ (2.251.280)	\$ (4.002.260)	\$ (5.424.128)	\$ (179.142)	\$ (13.706.660)
Valor presente (Tasa 5%)	(\$1.449.410)	(\$1.763.945)	(\$3.135.888)	(\$4.249.964)	(\$140.384)	\$ (10.739.592)

Cuadro XIII: Erogación de inversión en US\$

Resultados

A partir de las proyecciones de ventas y del análisis de costos e inversión, se ha proyectado un estado de resultados anualizado que permitirá tener una visión de la evolución del negocio A continuación, el cuadro de resultados a siete años de operación:

	Año						
	1	2	3	4	5	6	7
Suscriptores esperados		5.500	47.276	194.564	446.106	750.562	1.090.602
Facturación	\$ -	\$ 240.000	\$ 3.152.580	\$ 15.468.360	\$ 41.602.140	\$ 75.765.690	\$ 115.647.270
Costos Enterrados	\$ 140.000	\$ -	\$ -	\$ -	\$ -	\$ 140.000	\$ -
Costos Fijos	\$ 1.709.850	\$ 1.812.000	\$ 1.948.920	\$ 2.359.968	\$ 2.605.680	\$ 2.851.392	\$ 2.851.392
Costos Variables	\$ -	\$ 679.280	\$ 5.205.920	\$ 18.532.520	\$ 32.431.160	\$ 40.622.080	\$ 47.012.960
Total Costos	\$ 1.849.850	\$ 2.491.280	\$ 7.154.840	\$ 20.892.488	\$ 35.036.840	\$ 43.613.472	\$ 49.864.352
EBIT	\$ (1.849.850)	\$ (2.251.280)	\$ (4.002.260)	\$ (5.424.128)	\$ 6.565.300	\$ 32.152.218	\$ 65.782.918
Impuestos (40%)					\$ (2.626.120)	\$ (12.860.887)	\$ (26.313.167)
Resultado esperado	\$ (1.849.850)	\$ (2.251.280)	\$ (4.002.260)	\$ (5.424.128)	\$ 3.939.180	\$ 19.291.331	\$ 39.469.751

Cuadro XIV: Proyección del negocio en US\$

Conclusiones del flujo de inversión y resultados

- La incorporación de suscriptores comienza en el año 2, momento en el que se libera el producto a la venta en Estados Unidos (segundo semestre).

- Los costos fijos varían en función de la apertura de filiales en distintos mercados entre el año uno y el cinco.
- Los costos variables se incrementan en función de la cantidad de suscriptores a partir del inicio de las operaciones en el año dos.
- El punto de equilibrio sucede en el quinto año.
- Al finalizar el quinto año se recupera aproximadamente el 28% de la inversión completa.
- La recuperación completa de la inversión sucederá un año más tarde, en el Q2 del sexto año.
- El último año proyectado supone un rinde del 287% de la inversión.



Universidad de
SanAndrés

8. Conclusiones

En esta sección se desarrollarán conclusiones desde distintos enfoques:

- Las conclusiones del trabajo: considerando la investigación y los distintos análisis realizados.
- Las conclusiones del plan de negocios: devenidas de la elaboración del propio plan
- Las conclusiones considerando la prospectiva de la industria y del mercado.

Conclusiones del trabajo

La tecnología

Durante el desarrollo de este trabajo se ha planteado y estudiado un modelo de negocio de vigilancia de hogares basado en la innovación tecnológica. Uno de los primeros aspectos tratados estuvo asociado a la revisión de la capacidad técnica, es decir, si con el avance técnico y tecnológico actual es posible desarrollar un producto o servicio con las capacidades requeridas para llevar adelante las actividades que lo conforman. Lo primero que fue posible confirmar en el desarrollo del marco teórico es que la tecnología no solo existe, sino que ya se han desarrollado las capacidades necesarias que permitirían una aplicación como la que se está planteando desde la tesis.

La estrategia de negocios

La segunda conclusión es la que lleva a determinar la estrategia de negocios. Esta estrategia podría ser catalogada como híbrida ya que, en función del contexto o del tipo de competencia, puede ser vista como un liderazgo de costos o como una estrategia de diferenciación.

Por lo tanto, esta estrategia híbrida tendrá ambas características. Se orientará hacia el liderazgo de costos, para competir con empresas con las que se posee una desventaja competitiva (Delivery de seguridad) y para empresas cuya competencia es directa, con servicios similares, se debe proponer diferenciadores que actúen sobre la percepción del valor y generen tracción sobre el mercado. Los diferenciadores propuestos son dos:

- La base de datos de sospechosos.
- Las redes de contactos de confianza

Si bien ambos diferenciadores son necesarios, las redes de contactos de confianza son particularmente especiales por que pueden generar más valor para el negocio a partir de crear efectos de red.

El abordaje de mercados

En el capítulo de plan de negocios se puede observar que el de abordaje de mercados que se da en un orden específico, las actividades comienzan en USA, luego México y posteriormente Brasil. Este orden responde a la tercera de las conclusiones que tiene que ver con que los diferenciadores desde la perspectiva de un análisis VRIO. Estos diferenciadores son valiosos y raros, pero no son difíciles de imitar, por lo tanto, se trata de una ventaja competitiva temporal. Para poder consolidar esta ventaja y que deje de ser temporal, es necesario lograr efectos de red que son los que, aumentando el valor para los suscriptores, aumentarán el valor de todo el servicio.

El lograr efectos de red con diferenciadores fácilmente imitables requiere que se capte volumen de mercado lo más rápido posible, es por esto que la estrategia contempla abordar los mercados más grandes primero.

El on boarding

La última de las conclusiones tiene que ver con el on boarding, que fue pensado de modo que facilite la adopción del servicio por parte del mercado.

Los demás servicios similares tienen un modelo de on-boarding donde el usuario debe comprar el hardware (cámaras, estaciones de proceso, etc.) e instalarlo por cuenta propia, luego, con el equipamiento instalado, puede suscribir el servicio.

En el modelo de on boarding propuesto, se definió que el hardware base se entregaría como un comodato, que incluye dos cámaras y el dispositivo de inteligencia de borde. De este modo se espera que suscribir el servicio sea más atractivo para el mercado, ya que el suscriptor no asumirá el costo de dicho hardware en la contratación. Esto facilitaría en CHRUN de la competencia.

Conclusión General

Como conclusión general del trabajo, es razonable afirmar que el modelo de negocios enfrenta un panorama complejo, que su éxito dependerá fuertemente de la capacidad de crear valor con los diferenciadores y fundamentalmente de ejecutar las etapas en los tiempos pautados.

Es necesario tener conciencia del complejo escenario de mercado, ciertamente no se trata de un océano azul, se trata de una industria con un nivel de atomización alto donde hay considerable competencia y las principales características del producto son fácilmente imitables.

Los efectos de red son cruciales, sin ellos no será posible lograr un negocio con la escala necesaria para la rentabilidad que se persigue.

Conclusiones del plan de negocios

El plan de negocios posee factores que serán determinantes en el éxito del mismo. Los que se mencionan a continuación guardan relación directa con la estrategia de negocios y la propuesta de valor:

Los factores de la estrategia, al combinarse, permiten realizar una propuesta de valor que busca ser superadora desde costos y diferenciación:

- Un primer factor es la sustitución de servicios con alta participación de mano de obra especializada por la funcionalidad aportada por la IA, esto permitirá operar el servicio con bajo costo y competir agresivamente con la industria tradicional.
- Los diferenciadores son otro factor que también consolida el plan de negocios: la “red de contactos de confianza” y la “base de datos de sospechosos” no sólo aportan a la propuesta de valor características inexistentes en servicios de la competencia, sino que también son fuente de efectos de red que permitirán potenciar el valor del servicio haciéndolo más atractivo a nuevos suscriptores.

Estos otros factores surgen de la elaboración del propio plan:

- La mitigación de la dependencia de proveedores de hardware a partir de incorporar certificaciones a la planificación.
- El ingreso en los mercados más grandes primero, que responde a la necesidad de captar la mayor cantidad de mercado posible con diferenciadores que son fácilmente imitables.
- El On-boarding facilita la decisión en la adopción del servicio.

- Las etapas del proyecto son iterativas e incrementales, para proveer punto de control y seguimiento de la inversión.
- La duración de las etapas se ajusta correctamente a los tiempos de desarrollo del producto y de los mercados.
- La estructura de la organización permitirá simplificar la operación de las filiales.
- El camino de la innovación definido en la Cultura de la empresa permitirá sostener el producto con una propuesta de valor superadora.
- El punto de equilibrio en el quinto año con una cantidad de trescientos mil suscriptores.

Respecto del último punto, el camino futuro de la innovación del producto se desarrollará en los siguientes frentes:

- Mejoras específicas de las capacidades de IA: que pueda reconocer cada vez situaciones más complejas como asaltos u objetos como armas, entre otras.
- Capacidad de extensión: integrar funcionalidades de domótica para el manejo de la iluminación, etc.
- Obtención de información consolidada: en estudios de mercado se puede obtener información estadística de los suscriptores (porcentaje de hogares con mascotas, tipo de mascota, u horarios de actividades de los hogares, etc).

Prospectiva de la industria

- La industria de servicios de seguridad se ha caracterizado por sostener procesos de innovación constante. Algunos ejemplos de esto son: las comunicaciones, el rastreo satelital, los vehículos blindados, la seguridad electrónica, etc. Esto no solo se observa en ejemplos, también puede verse en el FODA de la industria (Ver Cuadro VII), donde la propia industria reconoce como fortaleza lo siguiente: “Rapidez de la innovación para adaptarse a la demanda.” En resumen, la innovación es una característica dominante en el ADN de las empresas que la conforman, ya que constantemente adaptan sus procesos, productos y servicios a nuevas exigencias o necesidades del mercado valiéndose de nuevas tecnologías.

- La innovación en tecnologías de Inteligencia Artificial en la industria de la seguridad no es una novedad, ésta se encuentra presente desde la década pasada con el reconocimiento facial y otras aplicaciones como la detección de patentes de automotores, control de multitudes en estadios y/o vía pública o automóviles en autopistas. En estos sistemas se realiza un control en tiempo real sobre el comportamiento del flujo de gente o vehículos. Estas son soluciones para aplicación de uso público o masivo, donde los sistemas analizan, ordenan y presentan la información a personas que toman las decisiones y eventualmente, emiten una respuesta.
- El futuro de la industria de servicios de seguridad continuará este camino de innovación en Inteligencia Artificial que viene recorriendo. Apalancándose en la creciente disponibilidad de datos para entrenar nuevos modelos y casos de entrenamiento, le permitirá un desarrollo de sistemas cada vez más complejos capaces de lograr funciones más elevadas de análisis y de este modo ir mejorando el nivel de servicio y la confiabilidad.
- Está claro que además de los modelos de entrenamiento, ya existen nuevos enfoques en la resolución de problemas. Tal es el ejemplo del caso mencionado en el documento llamado “Anomaly Detection in Surveillance Videos using Deep Learning” (Lu, 2020) donde se presenta un sistema por detección de anomalías de acuerdo a una predicción, es decir, dada una secuencia de imágenes de video, el sistema predice su evolución, es decir, predice la imagen siguiente, si la evolución real de la imágenes no se ajusta a la predicción, el sistema lo reconoce como una anomalía, es decir, el sistema predice lo que puede suceder antes de que suceda. Esto da una idea de que tan ingeniosos y que tan complejos pueden ser los enfoques.
- Dado lo exponencial del desarrollo que registra la tecnología (Ver Gráfico I), es razonable asumir que dentro de los próximos tres a cinco años, se comiencen a observar en el mercado, sistemas con características predictivas incorporadas. Un sistema de este tipo podría, por ejemplo, realizar predicciones de comportamiento de una persona que está a punto de realizar un asalto o abordaje violento. Todos estos elementos, se sumarán incrementalmente a las capacidades ya disponibles para lograr sistemas cada vez más expertos, cuyo

objeto será el de reemplazar totalmente la intervención humana en el monitoreo en menos de ocho años.

- Como se mencionada previamente, las comunicaciones han sido una de las innovaciones que la industria ha incorporado como una herramienta fundamental, para asegurar entre otras cosas, el Delivery y la coordinación.
- Con el advenimiento de la total automatización de la seguridad, las comunicaciones jugarán un rol central, ya que aportarán la capacidad de interconexión de los distintos sistemas para emitir avisos que generen respuesta. La combinación de la automatización total, las comunicaciones, el IOT y el 5G (o su evolución) eventualmente permitirá disponer de sistemas en cada esquina de centros urbanos, conformando una red intrincada de “ojos” vigilando en cada cuadra, dando lugar a un virtual “gran hermano” de la seguridad.
- Otro aspecto a considerar del futuro y sobre todo en materia de sistemas de seguridad, son los nuevos tipos de sensores o detectores como es el caso de 3D Face Recognition, que son capaces de leer un mapa en tres dimensiones del rostro a identificar. Esta tecnología posee algunas ventajas considerables como, por ejemplo, no son sensibles a la poca o mucha luz (no dependen de la calidad de la imagen), son más precisos porque un análisis en tres dimensiones de un rostro es más preciso que una imagen de video en dos dimensiones.
- Sin embargo, y a pesar de estos beneficios, este tipo de sensores tiene algunas complicaciones que son propias de las capacidades actuales de la tecnología. El objeto a reconocer debe estar relativamente cerca del sensor, por ejemplo, si se pretende que el sistema reconozca un rostro, este debe ser ubicado cerca del sensor y en un ángulo franco. Esto hace que, por el momento, la tecnología tenga fundamentalmente aplicación en sistemas de control de acceso más que en sistemas de vigilancia. Estos sensores también están evolucionando y resulta razonable pensar que se incorporen de manera complementaria a sistemas de video vigilancia para mejorar las capacidades de identificación de personas.

9. Bibliografía

- Bonfíglio, J. I., Guerra, B. G., Donza, E., Muratori, M., Padín Marchioli, M., Rodríguez Espínola, S., Salvia, A., & Vera, J. (2017). *DESARROLLO HUMANO E INTEGRACIÓN SOCIAL EN LA ARGENTINA URBANA 2010-2016* (Salvia Agustín para la Fundación Universidad Católica Argentina (ed.); 1st ed.). Fundación Universidad Católica Argentina. <http://wadmin.uca.edu.ar/public/ckeditor/2017-Observatorio-Desarrollo-Humano-Integracion-Social-Anexo-Estadistico.pdf>
- Carballo, I. (UCA), Petroni, E. (CASEL), Ferreyra, L. (CASEL), & Santángelo, G. (CASEL). (2018). *Estudio de mercado de la seguridad electrónica de la República Argentina*. http://www.casel.org.ar/Estudio_de_Mercado.pdf
- Estadísticas Criminales en la República Argentina – Año 2018*. (2019). https://estadisticascriminales.minseg.gob.ar/reports/Informe_Nacional_Estadisticas_Criminales_2018_V10.pdf
- Garrone, V., & Lafratti, P. (Securitas A. (2015). *Los Desafíos de la Seguridad Privada en Argentina* (p. 71). Securitas Argentina. <https://www.securitasargentina.com/globalassets/argentina/files/medios/los-desafios-de-la-seguridad-privada-en-argentina.-presente-y-futuro-de-una-profesion.pdf>
- Hansung Lee, So-Hee Park, Jang-Hee Yoo, Se-Hoon Jung, & Jun-Ho Huh. (n.d.). Face Recognition at a Distance for a Stand-Alone Access Control System [Article]. *Sensors (Basel, Switzerland)*, 20(3), 785. <https://doi.org/10.3390/s20030785>
- Instituto Nacional de Estadística, G. e I. de M. (2020). *Tabulados de la Encuesta Nacional de Seguridad Pública Urbana (ENSU)*. https://www.inegi.org.mx/contenidos/programas/ensu/tabulados/2020/ensu_

tabulados_basicos_diciembre_2020_estimacion_xlsx.zip

Insua, L. J. A. de trabajo y S. S. (2018). *Anexo N del Convenio Coletivo de trabajo 507/2007 Acta Salarial 2018* (p. 8). Ministerio de trabajo y seguridad social. <http://data.triviasp.com.ar/files/parte4/conv50707acu87818.pdf>

Jiménez, A. D. F. (2016). Sistema de Protección Fija - CARACTERÍSTICAS Y ETAPAS DE SU DISEÑO. *Diciembre*, 54. <https://www.caesi.org.ar/site/wp-content/uploads/2017/10/Revista-CAESI-8-1.pdf>

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning [Article]. *Nature (London)*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>

López de Mántaras Badia, R., & Meseguer González, P. (2017). Inteligencia artificial [Book]. In *Inteligencia artificial*. Editorial CSIC.

Lu, Y. (2020). *Anomaly Detection in Surveillance Videos using Deep Learning*. https://mspace.lib.umanitoba.ca/bitstream/handle/1993/34793/lu_yiwei.pdf?sequence=1&isAllowed=y

Muraro, O. (2018). EVOLUCIÓN DEL NSE DE LA SOCIEDAD ARGENTINA 2004 - 2017. In *SIAMO Evolucion NSE* (Issue SIAMO (Sociedad Argentina de Investigadores de Marketing y Opinion)). <http://www.saimo.org.ar/archivos/observatorio-social/nse-2020.rar>

Porter, M. E. (2015). Estrategia competitiva [Book]. In *Estrategia competitiva*. Grupo Editorial Patria.

Reinach, S. (Fórum B. de S. P. (2020). *Anuário Brasileiro de Segurança Pública - 2020. Fórum Brasileiro de Segurança Pública*, 332. https://arquivos.sesvesp.com.br/newsletter/anexos/20/10/21/anuario_brasileiro_de_seguranca_publica_2020.pdf

- Rodríguez, D. M. D. (2018). *Seguridad privada en México. Oficina Económica y Comercial de España en México*, 5.
https://www.ivace.es/Internacional_Informes-Publicaciones/Paises/México/Méxicoseguridadprivadadicex2018.pdf
- Sun, H., Yu, Y., Sha, K., & Lou, B. (2020). mVideo: Edge Computing Based Mobile Video Processing Systems [Article]. *IEEE Access*, 8, 11615–11623.
<https://doi.org/10.1109/ACCESS.2019.2963159>
- Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. (2018). Deep Learning for Computer Vision: A Brief Review [Article]. *Computational Intelligence and Neuroscience*, 2018, 13.
<https://doi.org/10.1155/2018/7068349>
- Zhou, S., & Xiao, S. (n.d.). 3D face recognition: a survey. *Human-Centric Computing and Information Sciences*, 8(1), 1–27.
<https://doi.org/10.1186/s13673-018-0157-2>

10. Anexos

Anexo I : Relevamiento de Benchmark

Icetana

URL: <https://icetana.com>

Categoría: Producto

Descripción:

Producto para aplicación en instalaciones de gran escala en modalidad B2B, define como targets de mercado a:

- Empresas de vigilancia
- Campus
- Prisiones
- Hoteles y Casinos
- Hospitales
- Ind. Manufacturera
- Centros Comerciales
- Almacenes
- Transporte
- Inst. Financieras.

Posee una baja proporción de infraestructura requerida, hasta 300 cámaras pueden ser controladas con una instalación de un único rack.

Permite la gestión de eventos de seguridad de manera centralizada desde donde se pueden revisar todas las anomalías detectadas.

Funciona por reconocimiento de patrones de movimiento habituales del público, detectando aquellos movimientos que no lo son. Midiendo no solo el sentido y el flujo de gente, sino que también los tiempos, pudiendo alertar sobre personas que les tomó una cantidad considerablemente mayor de tiempo desplazarse de un punto al otro de la imagen.

ICETANA Motion Intelligence™ is an AI driven video analytics surveillance solution designed to automatically identify anomalous events in real-time.

Our scalable video anomaly detection solution focuses the attention of your operators to the most important or unusual events occurring in your facilities at any given time, whether they are monitoring dozens or thousands of cameras. This enables your staff to identify potential threats to security, health and safety violations, Human Resources issues, business operations challenges or opportunities, and can provide business insights all with one powerful tool.

With our industry-leading artificial intelligence tool, you can achieve a 99% reduction in video overload. This is accomplished while still achieving 100% real-time proactive monitoring which can

provide your staff with the visibility of identifying precursors to events. With our comprehensive Milestone and Genetec integrations, our solution is ready to complement your VMS and turn your cameras into the most essential tool in your business.

Key differentiators

- Identifies precursor events, allowing for timely intervention before situations escalate.
- Scales to suit size of video surveillance operation
- Detects abnormal precursor events and a wide range of incidents in real-time
- Able to work with a wide range of cameras and servers
- Learns and adapts automatically using patented technology - no rules to setup or maintain
- Includes LiveWall™ - shows only events that need further investigation (1% of total video), reducing operator fatigue and missed events
- Rapidly review historical video - 24 hours in 30 minutes
- Reporting system allows tagging of anomalies and easy extraction of reports
- Supports a wide range of fixed view cameras
- Easy integration with existing Milestone, Genetec or other video management systems
- Minimises server costs - supports up to 300 cameras per 1 RU server (density depends on camera resolution and frame rate)

Intellivision

URL: <https://www.intelli-vision.com/>

Categoría: Producto de software de video vigilancia hogareño

Descripción: Posee un modelo de negocios del tipo B2B, especializándose en comercializar el producto con a través de fabricantes de Hardware como producto OEM.

Permite funciones de video vigilancia hogareñas con características interesantes, tales como:

- **Human Detection.** As soon as a person comes within the camera's field of view an alert can be sent.
- **Intrusion Detection/Line Crossing.** Automated perimeter monitoring. Detects a moving object which crosses the defined line.
- **Facial Detection.** Faces can be scanned and recognized from a database. Can include family members, friends, carers, etc.
- **Camera Tamper Detection.** Detects any attempt to tamper with the camera, partially or completely blocking its field of view, or drastically changing the camera angle. v Video Search/Summary. Stored video can be quickly scanned or searched for events.

Adicionalmente ofrece otras funciones como monitoreo de bebés a través de audio y mascotas.

El producto de software se complementa con otro software de naturaleza mobile que permite la revisión, recepción de alertas y gestión de los distintos dispositivos asociados.

No posee servicios asociados al producto todo el soporte se canaliza a través del fabricante del hardware y aquellos que pudieran integrar este producto como parte de su portfolio para agregar servicios asociados.

Folleto: https://www.intelli-vision.com/wp-content/uploads/2017/12/IntelliVision_SmartHome_solutionbrief1117.pdf

Google Nest

NEST Cameras: https://store.google.com/us/magazine/compare_cameras?hl=en-US

NEST Aware: https://store.google.com/us/product/nest_aware?hl=en-US

Categoría: Producto que integra solución de Hardware y Software.

Descripción: Con un modelo de comercialización es B2C, Google ofrece, como parte de su Portfolio de productos para domótica, una serie de dispositivos entre los que se pueden observar cuatro cámaras para hogares que, a partir de suscripción de USD 6/Mes de NEST AWARE, permiten entre otras funciones:

- Alertas inteligentes en sectores de la imagen: Detección de personas o sonidos.
- Alertas por zona: Aviso ante movimiento o actividad en una zona específica de la imagen.
- 30 días de retención de video en cloud.

Se gestiona desde la aplicación Google Nest que permite acceso en tiempo real a cámaras de video, revisión de video guardado.

IndigoVision

<https://www.indigovision.com/products/artificial-intelligence/#features>

Categoría: Producto que integra solución de Hardware y Software.

Descripción: Suite de productos con un modelo de comercialización B2B orientado a lugares públicos con alto tránsito de personas, define como targets de mercado a:

- Aeropuertos
- Hoteles y Casinos
- Ciudades
- Policía
- Inst. Financieras.
- Otros

Es un sistema que utiliza componentes de AI como asistencia a la video vigilancia que permite simplificar horas de video en segmentos de menor tiempo con una selección de eventos de interés basados en caracteres especiales como color, sentido del movimiento y velocidad.

Características:

- Detección y el reconocimiento facial.
- Rastreo por color, sentido o velocidad del movimiento.
- Analisis offline de anomalías (el sistema revisa horas de video en background y emite un resumen de lo interesante).
- Modo colaborativo para logran sinergia en grandes instalaciones.

La gestión de la seguridad se realiza desde una consola de monitoreo que permite, el video en tiempo real, los eventos de reconocimiento facial, la revisión del resumen de incidentes.

SmartSentry AI

<https://smartsentry.ai/>

Categoría: Producto que integra solución de Hardware y Software (Blue Iris).

Descripción: el modelo de comercialización es B2C a través de canales de venta

El producto es una cámara con capacidades limitadas de AI permite detectar personas y movimiento, no posee capacidades de reconocimiento facial. Envía alertas por e-mail o SMS.

Se suscribe con un plan de U\$D 5/Mes o U\$D 30/Año para una cámara.

BOSCH

<https://www.boschsecurity.com/xl/es/>

Categoría: Suites de productos para vigilancia, Alarmas y sistemas de video con capacidades de AI y de mejoramiento de imagen.

Descripción: el modelo de comercialización es B2B o B2C. Provee una serie de productos que se pueden integrar con productos propios y de terceros para desarrollar sistemas complejos de vigilancia con AI. Fundamentalmente Cámaras de alta definición con algunas funciones de AI.

Se orienta a una amplia gama de targets de mercado pretendiendo abarcar fundamentalmente grandes clientes como:

- Retail
- Museos
- Centros comerciales
- Aeropuertos
- Industria
- Logística
- Ciudades
- Oficinas y complejos habitacionales
- Instituciones financieras
- Hospitales
- Estadios
- Etc.

HUAWEI

<https://e.huawei.com/en/products/intelligent-vision>

Categoría: Componentes de Hardware para video vigilancia con capacidades de AI.

Descripción: El modelo de comercialización es B2B a través de canales de comercialización para aplicación en diversas industrias tales como:

- Gobierno
- Salud
- Educación
- Ind. Manufacturera

- Entidades financieras
- Etc.

Provee lo que llama SDC o “Software defined cameras” que consta de cámaras para aplicación de video vigilancia con hardware y software embebido que permite extender la capacidad de las mismas, mejorando las imágenes, aportando capacidades de AI y reduciendo el consumo y la transferencia de datos. Las principales características del producto son:

- Mejoramiento de la imagen:
 - Condiciones de poca luminosidad.
 - Condiciones de luminosidad excesiva.
 - Cambios de luz.
- individualización de objetos:
 - personas,
 - rostros
 - vehículos
 - patentes de vehículos
 - etc.

Arlo Security Cameras

<https://www.arlo.com/es/default.aspx>

Categoría: Solución de video vigilancia con capacidades de AI.

Descripción: El modelo de comercialización es B2C que consta de componentes de AI como cámaras para el hogar que permiten transmisión de video en directo y notificaciones. Con un abono mensual se incorpora un servicio que incorpora las siguientes características:

- Historial de vídeos en la nube
- Notificaciones enriquecidas e interactivas
- Detección de personas, vehículos y animales
- Detección de paquetes
- Zonas de actividad en la nube
- Llamar a un amigo

El costo del abono mensual tiene dos sabores en cuanto a la calidad del video y grabación:

- Calidad 2K o FullHD:
 - Camara individual u\$d 3
 - Hasta 5 cámaras: u\$d 10
- Calidad 4K:
 - Camara individual u\$d 5
 - Hasta 5 cámaras: u\$d 15

Ring Security Systems

<https://latam-es.ring.com/>

Categoría: Solución de video vigilancia con capacidades de AI.

Descripción: El modelo de comercialización es B2C. Ofrece cámaras de puerto (doorbell) con timbre y cámaras de seguridad con componentes de AI y funciones estándar como:

- Notificaciones activadas por movimiento
- Imágenes en tiempo real con el video en directo
- Comunicación bidireccional
- Protección antirrobo
- Cancelación sin complicaciones

Luego se incorpora un servicio con abono mensual con las siguientes características:

- Historial de videos de hasta 60 días
- Guardar y compartir videos
- Snapshot Capture* (Captura de fotos)
- Garantías ampliadas para todos los dispositivos Ring

Dos niveles de abono a un costo de:

- Básico: USD \$3/mes o USD \$30/año
- Plus: USD \$10/mes o USD \$100/año

Oddity.ai

<https://oddity.ai/>

Categoría: Producto de software para ser integrado a Hardware de distintos fabricantes con capacidades de AI para análisis de imágenes de ámbito público y grandes instalaciones.

Descripción: Oddity is developing the future of safety by detecting high impact crimes on live video footage. Our algorithm seamlessly integrates with technology in observation centers and is trusted by municipalities, law enforcement and private security companies.

Our algorithm monitors video feeds in real time and alerts security personnel of violent incidents, car crashes, perimeter breach, or other incidents. Up to thousands of feeds at once, with a detection speed of less than half a second.

Data does not get more sensitive than in the security domain. We built right on top of this principle. Our algorithms analyze subjects in full anonymity, they function standalone and deploy on premise. Your data stays in your hands.

AxxonSoft

<https://www.axxonsoft.com/>

Categoría: Producto de software para ser integrado a Hardware de distintos fabricantes con capacidades de AI para análisis de imágenes de ámbito público y grandes instalaciones.

Axxon Intellect Enterprise has built-in intelligent video and audio analytics to recognize events as they occur, and the ability to respond appropriately. Axxon Intellect provides the option of automatic and

automated administration of security systems, including through user-defined scripts for reactions to events.

Video detection tools: Smart video detection tools process camera video and identify events that match certain criteria: motion, object appearance or disappearance, line crossing, and more. These events can be attached to specific system actions, such as beginning recording, sending a signal to the operator, displaying the image on a separate monitor, or starting a complicated custom script.

Forensic search: Our system for smart search in video archives allows quickly finding archived video that matches custom criteria. The criteria (line crossing, motion in area, movement from one area to another, etc.) are set at the time of search; no pre-configuration of detection tools is necessary.

People counting: The people counting detection tool counts the number of people who go from a certain area to another and back again. The detection tool records each time when an object of a certain size moves in any direction.

Queue management: The queue length detection tool counts the number of people standing in view of a video camera that is aimed at a customer queuing area. The detection tool counts the people who stay in the specified area for a specified length of time: only the people who are truly waiting in line are included.

Heat Map: The Heat Map tool allows determining where visitors stop and measuring their linger time in areas of interest. With the detection tool, it is possible to view the "warmest" places at a retail store or any other trafficked location thanks to corresponding visual cues on screen.

Edge analytics: Besides the video analysis functions built into the program, Axxon Intellect Enterprise also supports video detectors embedded in IP cameras and can work with specialized video analysis hardware.

Guardian Systems

<https://guardianva.com/es/>

Categoría: portfolio de distintos productos y servicios que se complementan para desarrollar distintos niveles de servicio de video vigilancia con complemento de AI.

Descripción: la modalidad comercial es B2C y ofrece la siguiente línea de productos:

AI-Sentinel: Permite la detección de personas y alarma integrada para hogares y negocios

- Plan básico (hasta 4 cámaras): u\$d 40
- Plan Pro (hasta 8 cámaras): u\$d 50

AI-lock: Sistema de control de acceso con cámaras para detección de personas con mascararas, cerradura por magneto y sensores de salida, Costo u\$d 899

AI-lock Plus: Sistema de control de acceso con cámaras para detección e identificación de personas autorizadas por reconocimiento facial, cerradura por magneto y sensores de salida, Costo u\$d 999

Motorola

https://www.motorolasolutions.com/en_xu/video-security-analytics.html

Categoría: portfolio de distintos productos que se complementan para desarrollar sistemas de video vigilancia con complemento de AI de distinta complejidad.

Descripción: modalidad comercial B2B para soluciones de video vigilancia con AI, y otros productos como cámaras de video para modalidad comercial mixta B2B o B2C. La siguiente serie de productos:

Video cámaras: cámaras Aviglong, con funciones de AI que las dotan de capacidad de identificar 50 objetos distintos de una escena.

Control de acceso: sistema de control de acceso sin AI.

Video analytics software: software para aplicaciones de AI sobre video con capacidades de identificación de situaciones por patrones o mediante ejemplos.

Software de Gestion de seguridad para centros de control.

Panasonic

<https://security.panasonic.com/es/>

https://security.panasonic.com/es/products_technology/technologies/facial_recognition/

Categoría: portfolio de productos que se complementan para desarrollar sistemas complejos de video vigilancia con complemento de AI para soluciones de gran escala.

Descripción: modalidad comercial B2B para soluciones de video vigilancia con AI con productos diversos que incluyen: cámaras, software de AI, software de gestión de seguridad.

Las industrias target de este sistemas son:

- Retail
- Logística y Transporte
- Vigilancia en la ciudad y Gobierno
- Educación
- Estadios

Dahua

<https://www.dahuasecurity.com/la/products>

Categoría: Portfolio de productos que permiten configurar sistemas de video vigilancia con complemento básico de AI para reconocimiento de caracteres.

Descripción: modalidad comercial B2B para soluciones de video vigilancia con AI de alcance industrial, con capacidades de OCR.

<https://www.dahuasecurity.com/la/products/All-Products/Machine-Vision>

The new machine vision product lineup focuses on “turning vision into productivity” for industrial and manufacturing applications via camera/lens products.

Leveraging 20+ years of know-how in image acquisition and processing, and as world's top 3 surveillance camera supplier, Dahua designs and manufactures various high-performance industrial cameras with large throughput and high accuracy.

The machine vision product portfolio includes area scan cameras, line scan cameras, smart cameras, 3D measurement cameras, and industrial lenses covering a wide range of resolutions from 0.3MP to 50MP. The camera interface supports Gigabit Ethernet, USB 3.0, CoaXPress, and Camera Link to satisfy diverse project requirements.

The products are widely used for OCR recognition, industrial defect inspection, target identification, traffic control solutions, entertainment monitoring, medical and life science, and other applications.

HikVision

<https://www.hikvision.com/es-la/>

Categoría: Fabricante de productos para sistemas de vigilancia con complemento de AI para aplicación a sectores de espacio público.

Descripción: modalidad comercial B2B con líneas de productos para captura de video (Camaras) y sistemas complejos de video analytics.

Camaras de video para captura de alta resolución con funcionalidad de mejoramiento de imagen.

Sistemas de cómputo para video analytics: Línea de servidores para procesamiento de imágenes con video analytics e integrarlos a soluciones complejas

<https://www.hikvision.com/es-la/products/IP-Products/Data-Center/DeepinMind-Server/?q=serie+deepinmind&position=2&category=Network+Products&subCategory=Centro+de+datos&series=Serie+DeepinMind&checkedSubSeries=Fusion+Big+Data+Server%3BEdge+Facial+Recognition+Server%3BIntelligent+Fusion+Server%3BFull+Analysis+Server%3BBehavior+Analysis+Server>

DeepinMind Servers are Hikvision's most advanced server products to-date. Featuring cutting-edge analytics capabilities, these servers are ideal when huge amounts of data gets processed. Yet what makes them truly stand out is their flexibility: install one of these servers in your existing security system – whether it is linked to intelligent devices or not, and whether you're using Hikvision products or third-party devices – and you'll get a fully-functioning security system with amazing analytics power. And the best thing is, you cannot only analyze your future data, your historical video recordings can also be imported and analyzed.

FLIR

<https://www.flir.com/>

Categoría: Fabricante de productos para sistemas de relevamiento visual y complemento de video analytics.

Descripción: modalidad comercial B2B con líneas de productos para captura de video (Camaras) y sistemas complejos de video analytics.

Advance video analytics (<https://www.flir.com/security/analytics/>)

Combining thermal and visible-light security cameras and analytics is a reliable, cost-effective way to protect perimeters from intrusion. FLIR analytics recognize and classify human and vehicular intruders while intelligently filtering false-positive activity, such as small animals or wind-blown foliage, resulting in more reliable threat detection with fewer false alarms.

When FLIR video analytics detect an intrusion, United VMS alerts operators and begins tracking the target. As the intruder moves, fixed cameras hand the target off to PTZ auto-tracking cameras, maintaining constant vision on the threat until security can intervene.



Universidad de
SanAndrés

Anexo II – Encuesta complementaria.

La encuesta se realizó a personas de Argentina, Colombia, Brasil y México, el total de respuestas fue 193 y la distribución de las respuestas se dio de la siguiente manera: el 60% de las respuestas son de Argentina, el 25% de Brasil, Colombia el 9% y México el 6%.

Para la mayor parte de las preguntas se estableció una escala del 1 al 5 para dar opciones de mayor gama de respuesta, y se determinó en el diseño que el 3 representa neutralidad, debajo de tres (1 y 2) representa negatividad y por encima (4 y 5) representa una respuesta positiva con distinto grado de confianza.

Cuando se consultó sobre la preocupación por la privacidad como un Insight relevante, se preguntó: *¿Le preocupa que el personal que realiza el monitoreo conozca el movimiento de personas en su hogar?* La escala para responder asignaba 1 para “Ninguna preocupación” y 5 “Me preocupa bastante”. A continuación, se puede ver el gráfico III donde se muestra los resultados clasificados por grupos de personas que poseen sistemas de seguridad y aquellos que no lo poseen:

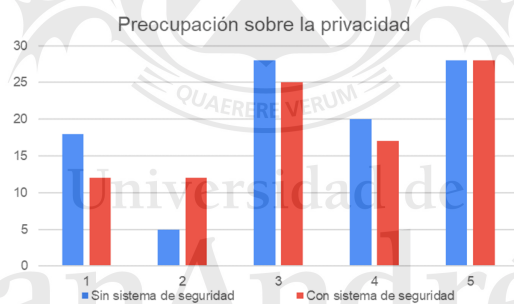


Diagrama III: Preocupación sobre la privacidad

El gráfico muestra una pequeña tendencia hacia la preocupación, pero no se puede afirmar que sea una tendencia marcada o irreversible con una mayor muestra, probablemente esta pregunta debió tener una resolución binaria más que una gama.

Respecto del Delivery de la seguridad se consultó en dos partes, primero se preguntó lo siguiente: *¿Es importante para Ud. que una Alarma de hogar de aviso a la policía?* Nuevamente contestando con una escala de 1 a 5 donde 1 es poco o nada importante y 5 es muy importante.

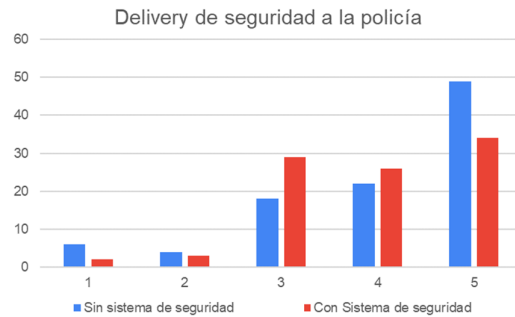


Diagrama IV: Delivery de seguridad a la policía

Aquí se pueden ver dos cosas, primero, a diferencia del anterior una clara tendencia hacia lo importante que es que los servicios de alarma den aviso a la policía, pero más interesante que esto, es ver como aquellos que ya cuentan con un sistema de seguridad, se vuelcan más a la neutralidad que los que no tienen sistema alguno.

Por último, una pregunta complementaria a esta es: ¿Qué tan aceptable sería que una alarma en lugar de avisar a la policía, avise al dueño del hogar y/o grupo de confianza? Nuevamente esta pregunta posee una escala de 1 a 5, donde 1 es inaceptable y 5 es aceptable. El resultado en el Grafico V:

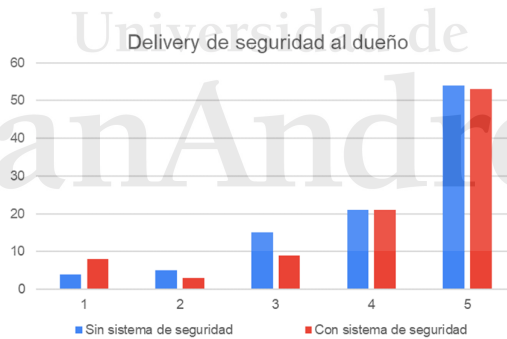
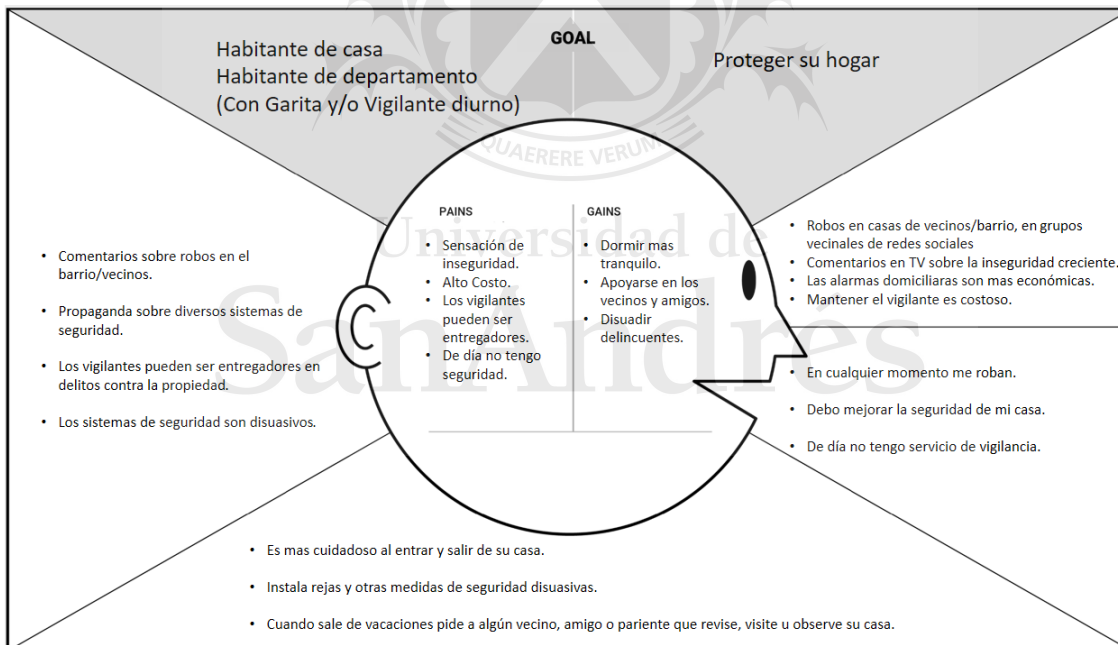
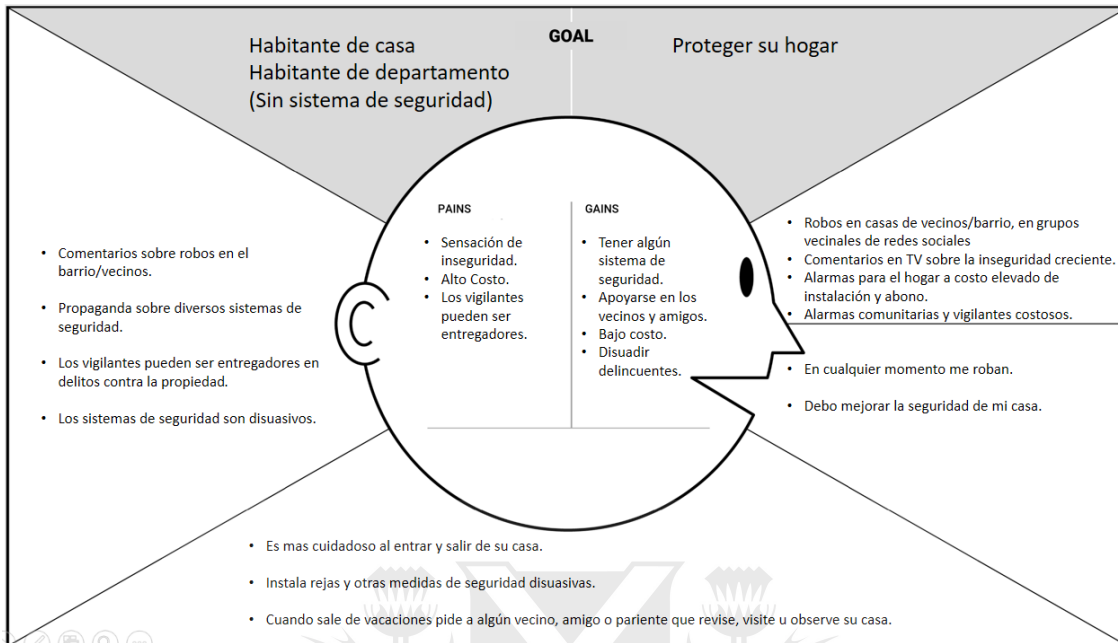
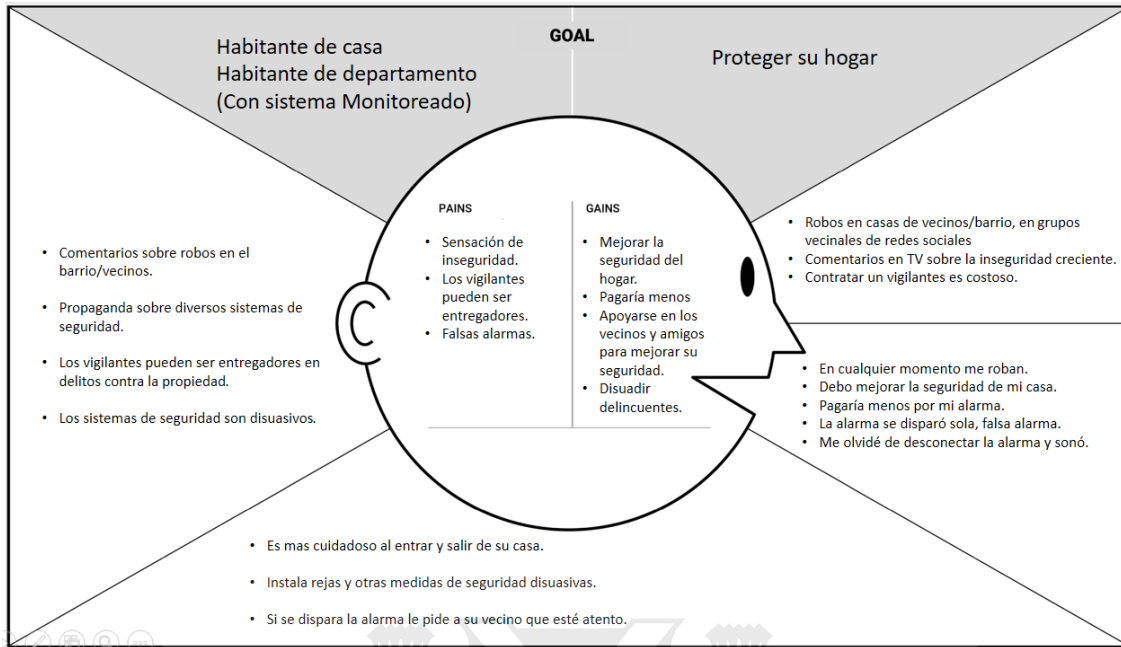


Diagrama IV: Delivery de seguridad al dueño

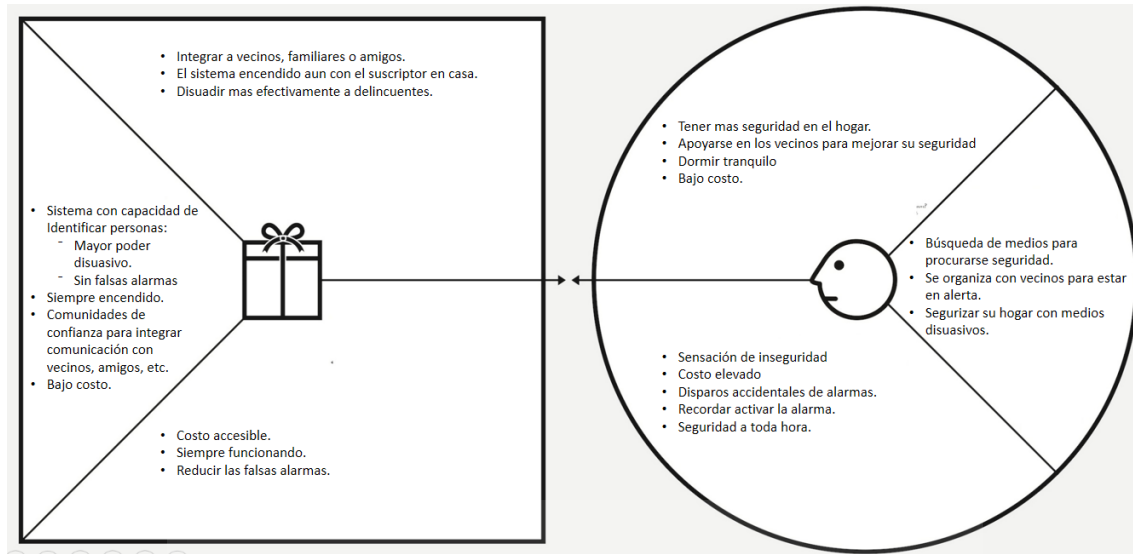
Aquí la tendencia es claramente hacia el aceptable, algo más del 50% de los que respondieron, si comprendieron correctamente la pregunta, no tienen tanta aversión a ser contactados directamente.

Anexo III : Empathy maps





Anexo IV: Value Proposition Canvas



Anexo V: Business Model Canvas

