PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

Modelo ProLab: Segurazo, una propuesta digital para combatir el fraude financiero en el Perú

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRA EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS

QUE PRESENTA:

Lucero Steffy, Alvarado Nuñez

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS

QUE PRESENTA:

Álvaro Benjamín, Contreras Navarro

Kevin Emilio, Gonzales Pilco

Franco Oswaldo, Mori Acosta

ASESOR

Carlos Arturo, Hoyos Vallejo

Surco, agosto 2025

Declaración Jurada de Autenticidad

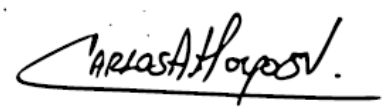
Yo, Carlos Arturo Hoyos Vallejo, docente del Departamento Académico de Posgrado en Negocios de la Pontificia Universidad Católica del Perú, asesor de la tesis de investigación titulada “Modelo ProLab: Segurazo, una propuesta digital para combatir el fraude financiero en el Perú”, de los autores:

- Lucero Steffy Alvarado Núñez, DNI: 74944529
- Álvaro Benjamín Contreras Navarro, DNI: 47467606
- Kevin Emilio Gonzales Pilco, DNI: 72022225
- Franco Oswaldo Mori Acosta, DNI: 44830341

dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 13%. Así lo consigna el reporte de similitud emitido por el software Turnitín el 09/10/2025.
- He revisado con detalle dicho reporte y confirmo que cada una de las coincidencias detectadas no constituyen plagio alguno.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 10 de octubre de 2025



Carlos Arturo, Hoyos Vallejo

CE: 001944142 - ORCID: 0000-0003-3571-7178

Resumen Ejecutivo

El problema identificado en esta investigación radica en la falta un mecanismo rápido efectivo para proteger a los usuarios peruanos tras el robo de un celular, un incidente cada vez más común en nuestro país. "Segurazo" surge como una solución innovadora que actúa como un asistente virtual que guía a los usuarios paso a paso en momentos de alta tensión. La aplicación permite contactar de manera ágil a las entidades financieras y operadores móviles para bloquear cuentas bancarias, líneas telefónicas y dispositivos, además de brindar orientación para interponer denuncias.

Para desarrollar "Segurazo", se llevó a cabo un proceso exhaustivo que incluyó encuestas para entender las necesidades de los usuarios, el diseño de prototipos, la creación de un Producto Mínimo Viable (PMV) incorporando mejoras basadas en feedback. Este enfoque permitió adaptar la propuesta de valor directamente a los Gains y Pains identificados, guiando nuestra propuesta de valor hacia el usuario.

La aplicación demostró ser deseable a través de pruebas que reflejan altos índices de disposición y confianza en su uso. Además, pruebas de usabilidad garantizaron un porcentaje de éxito constante y tiempos de interacción adecuados para su propósito. La factibilidad se confirmó mediante simulaciones aplicadas al plan de marketing (CAC y LTV), mientras que la viabilidad económica se avaló con un VAN proyectado de S/ 4,346 mil y una TIR del 178%, lo que indica que el proyecto es rentable. En términos de sostenibilidad, el proyecto se alinea con el ODS 16.4, contribuyendo a la protección de activos digitales y financieros. Con un Índice Total de Alcance en Sostenibilidad (TSRI) del 66.70%, "Segurazo" reafirma su impacto positivo en la ODS 16.4.

El análisis realizado evidencia la necesidad de soluciones integrales en seguridad financiera móvil. "Segurazo" fomenta la confianza en el sistema financiero a través de la colaboración estratégica entre bancos, operadoras y proveedores de software.

Tabla de Contenidos

Lista de Tablas

Lista de Figuras

Capítulo I. Definición del problema

1.1. Contexto del problema a resolver

En la era digital, los dispositivos móviles se han vuelto esenciales para la comunicación, las transacciones financieras y las actividades cotidianas. Según la Unión Internacional de Telecomunicaciones (UIT), en 2023, el 78% de la población mundial de 10 años o más poseía un teléfono móvil (UIT, 2023). Sin embargo, este avance también ha generado nuevas exposiciones al riesgo, especialmente vinculadas al fraude financiero.

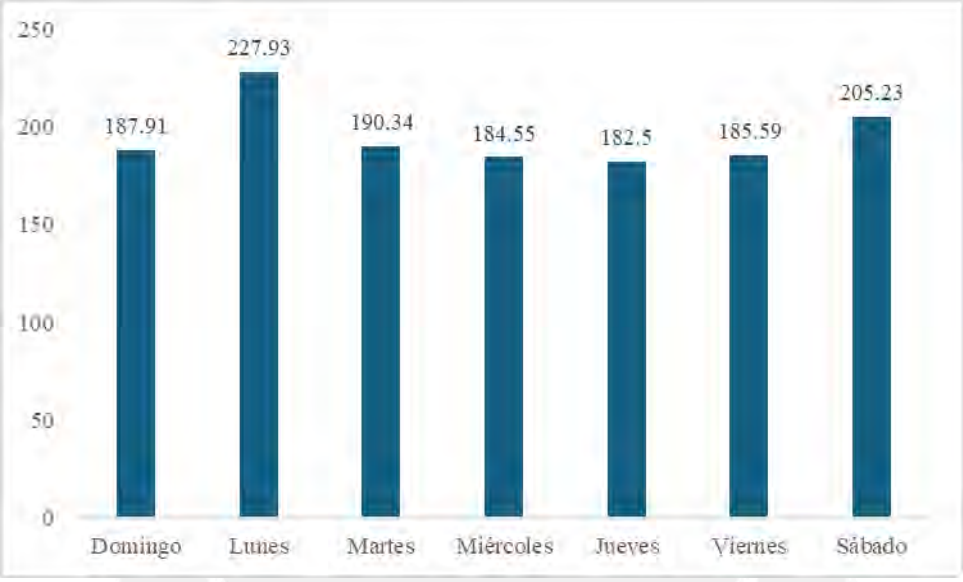
Durante 2023, el fraude financiero relacionado con el robo de teléfonos móviles se convirtió en una preocupación global significativa. Según el Global Ecommerce Payments and Fraud Report 2023 del Merchant Risk Council (MRC), Cybersource y Verifi, los ataques de phishing, pharming y whaling[1] mostraron un incremento importante, afectando al 43% de las empresas frente al 35% del año anterior. También se reportó un aumento en fraudes por apropiación de cuentas y pruebas de tarjetas, lo que agravó la situación tanto para empresas como para usuarios finales, particularmente en regiones como Europa y Asia-Pacífico (Merchant Risk Council, Cybersource & Verifi, 2023).

En América Latina, la situación es similar. La tasa de penetración de dispositivos móviles alcanzó el 72% en 2023, lo que acorta la brecha digital, pero también propicia un aumento en los delitos cibernéticos (GSMA, 2023). En el caso peruano, el Instituto Nacional de Estadística e Informática (INEI) informó que el 94.9% de los hogares cuenta con al menos

[1] Phishing es una técnica de fraude donde los atacantes se hacen pasar por entidades legítimas para obtener información confidencial. Pharming redirige a los usuarios desde un sitio web legítimo hacia uno falso sin que lo noten. Whaling, por su parte, es un ataque dirigido a personas de alto perfil, como ejecutivos, para robar información sensible.

un miembro que posee un teléfono celular (INEI, 2023). Estos dispositivos son utilizados activamente para servicios financieros, lo que incrementa el riesgo de exposición al fraude. Según OSIPTEL, aproximadamente 4,400 celulares son robados diariamente en el país (OSIPTEL, 2023) y, de acuerdo con el INEI, cerca de 15 de cada 100 peruanos ha sido víctima de robo o intento de robo de su celular en algún momento (INEI, 2023).

Figura 1. Promedio equipos móviles robados por hora durante 2023



Fuente: OSIPTEL

La Figura 1 muestra que el lunes es el día con mayor incidencia, con un promedio de 227.93 robos de celulares por hora, muy por encima del resto de la semana.

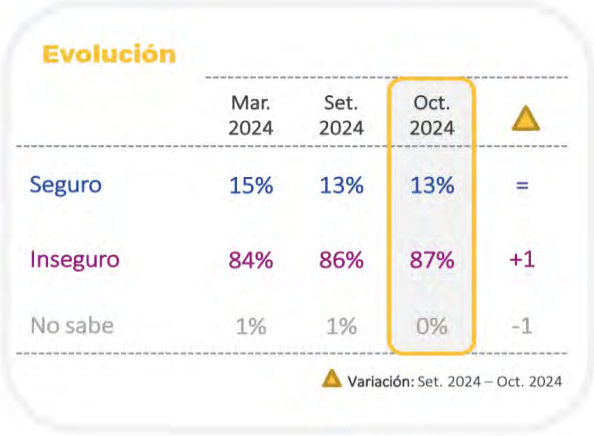
El impacto de estos robos va más allá de la pérdida material. Los teléfonos móviles almacenan información crítica, como credenciales bancarias, datos personales y acceso a plataformas de pago (Symantec, 2019). Esta situación genera una sensación de impotencia y vulnerabilidad, ya que los delincuentes pueden acceder rápidamente a información sensible y realizar operaciones fraudulentas antes de que el afectado pueda reaccionar (Kaspersky Lab, 2020).

La respuesta del usuario suele verse limitada por la falta de orientación clara y centralizada que le permita actuar rápidamente frente al robo. En momentos de urgencia, la dispersión de canales y procesos incrementa el riesgo de fraude y puede provocar altos niveles de ansiedad y frustración, al no contar con una guía inmediata que lo dirija a contactar a las instituciones correspondientes de forma eficaz. Además de la pérdida económica inmediata, las víctimas enfrentan un proceso complejo para asegurar sus cuentas. Contactar a entidades financieras, operadoras móviles y plataformas digitales puede tomar horas, y cada minuto de retraso aumenta el riesgo de fraude (Asociación de Bancos del Perú, 2020). Muchas personas no logran actuar a tiempo y dejan expuestos sus datos personales y financieros durante ese periodo (Ponemon Institute, 2019).

La situación se agrava por el desconocimiento generalizado respecto a los pasos correctos a seguir tras un robo. Muchas víctimas no bloquean sus líneas ni los accesos vinculados a aplicaciones móviles, lo que amplía la exposición (INDECOPI, 2019).

Además, la percepción de inseguridad en el país es alarmante. Según la encuesta nacional de Datum (2024), el 87% de los peruanos afirma sentirse inseguro al transitar por las calles de su ciudad, siendo Lima y Callao las zonas con mayor preocupación (94%), como se aprencia en la Figura 2.

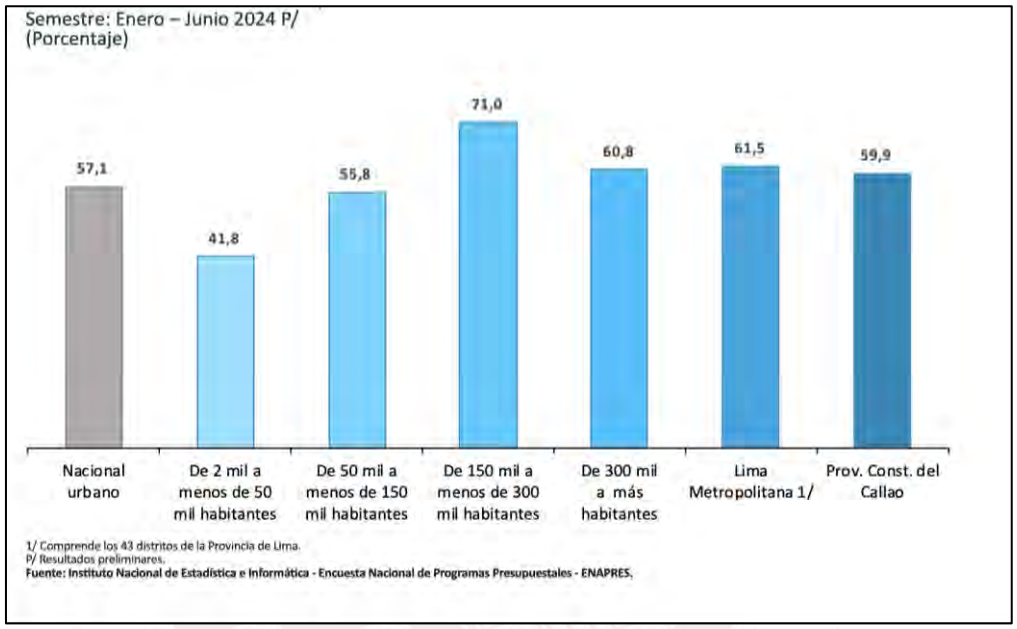
Figura 2. Percepción de inseguridad en Perú



Fuente: Datum 2024

La Figura 3 evidencia que la percepción de inseguridad al caminar solo(a) por su zona o barrio de noche es particularmente alta en el contexto urbano peruano. Este entorno de alerta constante aumenta la sensibilidad ante eventos como el robo de celulares.

Figura 3. Población de 15 años y más de edad con percepción de inseguridad al caminar solo/a en su zona o barrio de noche, por tamaño de centros urbanos poblados



Fuente: INEI

Esta realidad refuerza la importancia de soluciones como la propuesta digital de esta tesis, que busca ofrecer una guía eficiente para mitigar las consecuencias del robo de celulares, desde la pérdida económica hasta el impacto psicológico que enfrentan las víctimas.

A pesar de la magnitud del problema, la respuesta institucional aún presenta limitaciones. Solo el 15.5% de las víctimas de delitos reportaron el hecho ante la Policía Nacional del Perú o el Ministerio Público (INEI, 2024). Esta baja tasa de denuncias no solo limita la capacidad del Estado para diseñar estrategias preventivas, sino que también deja a los usuarios sin una red de contención clara frente al delito.

Las consecuencias emocionales también son significativas. Las víctimas reportan altos niveles de estrés, ansiedad e inseguridad tras el robo, lo que puede afectar su bienestar y su

confianza en el uso de servicios digitales (Organización Mundial de la Salud [OMS], 2018). Esto subraya la necesidad de desarrollar soluciones que, además de resguardar la información financiera, acompañen al usuario con una experiencia de respuesta rápida, clara y tranquilizadora.

Exploración de las causas raíz del problema basado en entrevistas

A partir del análisis de las entrevistas realizadas a usuarios que fueron víctimas de fraude tras el robo de sus dispositivos móviles, se identificaron diversas causas raíz que explican la persistencia y gravedad del problema. Estas causas fueron agrupadas en cinco categorías principales, que reflejan patrones comunes en los testimonios recogidos:

- Desconocimiento y falta de educación financiera y digital

  Uno de los hallazgos más recurrentes fue el desconocimiento generalizado sobre cómo proteger la información financiera y qué hacer ante un robo. Muchos entrevistados señalaron que no reciben información clara ni oportuna sobre seguridad digital por parte de las entidades financieras ni de los entes reguladores.

- Procesos fragmentados y tiempos de respuesta limitados

  Los usuarios entrevistados describieron que, tras el robo de sus dispositivos móviles, se enfrentaron a procesos dispersos y poco coordinados para bloquear sus cuentas o líneas telefónicas. En muchos casos, se requiere contactar múltiples canales, realizar llamadas sucesivas o acudir presencialmente a una agencia, lo que limita la capacidad de respuesta inmediata.

- Vulnerabilidades en los sistemas de autenticación y seguridad

  Varios entrevistados mencionaron casos de fraude por SIM swapping, en los que los delincuentes logran suplantar la identidad del usuario ante el operador móvil y obtener el control de la línea. Esto les permite recibir claves de verificación y acceder a las

cuentas bancarias vinculadas, evidenciando fallas en los mecanismos de autenticación y verificación de identidad.

- Impacto financiero y percepción de riesgo

  Las pérdidas económicas reportadas por los entrevistados varían, pero en muchos casos alcanzan montos elevados. Algunos mencionaron que no recibieron reembolsos por parte de los bancos, bajo el argumento de que el usuario fue negligente. Esta situación genera desconfianza en las instituciones financieras y una percepción creciente de inseguridad en el entorno digital.

Impacto en actores clave del sector

El fraude financiero asociado al robo de dispositivos móviles genera consecuencias significativas para distintos actores del ecosistema financiero, tecnológico y regulatorio. A continuación, se describe su impacto por segmento:

Usuarios (clientes del sistema financiero)

Las personas afectadas pueden perder montos considerables en transacciones no autorizadas antes de lograr el bloqueo de sus cuentas o dispositivos. Según la Policía Nacional del Perú, durante 2023 se registraron 1,487 denuncias de estafas digitales, con un perjuicio económico que ascendió a S/ 53 millones y USD 26.9 millones (Infobae, 2023). Esta situación no solo impacta a nivel financiero, sino que también deteriora la confianza del usuario en los canales digitales y en las entidades responsables de su protección.

Entidades financieras

Los bancos enfrentan un doble impacto: por un lado, la carga reputacional ante incidentes de fraude, y por otro, el costo operativo de reforzar sus sistemas de autenticación y monitoreo. En 2023, se reportaron más de 2,100 reclamos mensuales por operaciones no reconocidas (Gobierno del Perú, 2023). Cuando se demuestra que el usuario no autorizó las

transacciones, las entidades deben asumir las pérdidas, generando costos significativos. Muchas han invertido millones en infraestructura tecnológica, sistemas antifraude y personal especializado (Management Solutions, 2023).

Operadoras de telecomunicaciones

El fraude por SIM swapping continúa siendo una vulnerabilidad crítica. Al obtener un duplicado de la tarjeta SIM, los delincuentes acceden a claves de autenticación enviadas por los bancos, comprometiendo así las cuentas de los usuarios. El sector telecomunicaciones ha sido impactado no solo por este tipo de delitos, sino también por fraudes contractuales y ciberataques más amplios (PwC Perú, 2023).

Entidades reguladoras

La gestión del riesgo sistémico frente al robo de celulares presenta desafíos regulatorios. La ausencia de normativas integradas que obliguen a bancos y operadoras a actuar de forma conjunta y en tiempo real ante un incidente limita la capacidad de respuesta institucional. Como respuesta, OSIPTEL ha propuesto modificaciones a las condiciones de uso del servicio móvil, orientadas a una actuación más proactiva frente a este tipo de delitos (OSIPTEL, 2023).

Impacto de la complejidad del problema en las decisiones de los actores clave

Clientes de los bancos

El contexto de inseguridad digital genera desconfianza en el uso de servicios financieros virtuales. Muchos usuarios en Perú han manifestado su temor hacia la banca móvil tras haber experimentado intentos de fraude (Ojo Público, 2023). Esto ha llevado a que algunas personas prefieran realizar transacciones presenciales, lo que frena el avance de la digitalización financiera. Además, los clientes demandan procesos más claros y rápidos para bloquear cuentas y dispositivos robados, debido a la falta de procedimientos estandarizados entre bancos.

Entidades financieras

Las entidades financieras han tenido que reforzar sus sistemas de autenticación y detección de fraudes. Según LexisNexis Risk Solutions (2024), el 60% de las instituciones en América Latina han incrementado su inversión en tecnología antifraude. Esta presión operativa no solo representa un costo adicional, sino que también afecta la percepción de seguridad de los usuarios. Un estudio de Management Solutions (2021) advierte que el temor frente al fraude puede reducir la captación de nuevos clientes.

En Perú, la creciente cantidad de reclamos por operaciones no reconocidas —que supera las dos mil atenciones mensuales (Gobierno del Perú, 2023)— ha intensificado la carga de las áreas de atención y ha evidenciado la necesidad de soluciones que agilicen la respuesta ante incidentes.

Operadoras de telecomunicaciones

Uno de los desafíos principales para las operadoras es la verificación de identidad previa al cambio de SIM o bloqueo de líneas. La ausencia de protocolos estandarizados puede facilitar el fraude por SIM swapping, una modalidad que permite a los delincuentes tomar control de líneas telefónicas y acceder a servicios digitales (PwC Perú, 2023).

Según OSIPTEL (2023), en Perú se reciben más de 50,000 solicitudes mensuales de bloqueo de líneas por robo, lo cual genera una alta carga operativa y puede ocasionar demoras en la atención.

Además, la falta de integración tecnológica entre operadoras y entidades financieras complica una respuesta coordinada y rápida ante incidentes. Existen experiencias internacionales, como el caso de Brasil, donde ya se han implementado mecanismos conjuntos para bloquear líneas y cuentas bancarias en simultáneo, lo que reduce la ventana de acción de los delincuentes (Banco Central de Brasil, 2023).

Reguladores y organismos gubernamentales

Desde el ámbito regulatorio, persisten desafíos importantes en la actualización normativa. El informe de la Defensoría del Pueblo (2023) advierte sobre vacíos legales en la lucha contra el fraude digital, los cuales son aprovechados por redes delictivas.

Esto evidencia la necesidad de adaptar el marco regulatorio a la evolución de los delitos tecnológicos, así como de promover una articulación más eficiente entre bancos, operadoras y entidades gubernamentales para asegurar una protección efectiva de los ciudadanos.

1.2. Presentación del problema a resolver

El fraude financiero derivado del robo o pérdida de dispositivos móviles representa un problema crítico que impacta tanto a los usuarios como a las instituciones del ecosistema digital. Estos dispositivos se han convertido en herramientas esenciales para realizar operaciones bancarias, gestionar datos personales y acceder a múltiples plataformas. En consecuencia, almacenan información altamente sensible, como credenciales bancarias, contraseñas, fotos, correos electrónicos, redes sociales y aplicaciones de pago; que los convierte en un objetivo atractivo para los delincuentes.

Según el INEI (2024), la tasa de víctimas de robo de dinero, carteras y celulares aumentó un 18% respecto al 2021. Esta tendencia refleja una creciente exposición al riesgo, ya que los delincuentes pueden acceder a datos financieros y personales para realizar transferencias no autorizadas, compras en línea, cambios de contraseñas y, en algunos casos, actividades delictivas como la extorsión o suplantación de identidad.

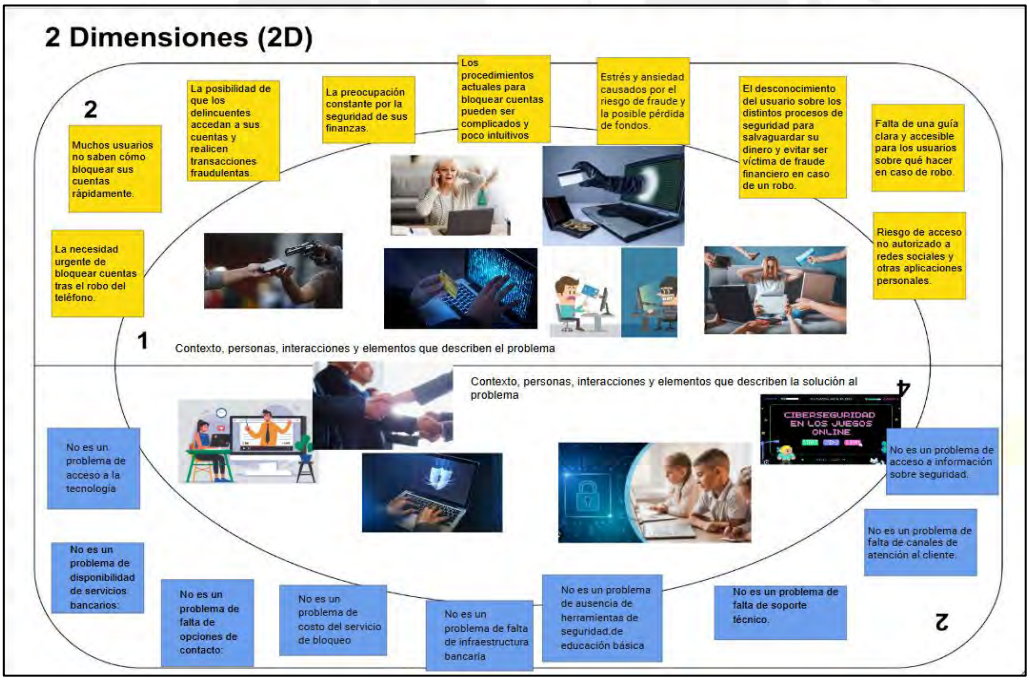
Uno de los principales factores que agrava esta problemática es el desconocimiento de los usuarios sobre las acciones inmediatas que deben tomar tras un robo. Muchos no saben que deben bloquear la SIM, reportar el incidente a su banco, modificar contraseñas ni cómo hacerlo de manera ágil. Aunque OSIPTEL (2023) recomienda contactar de forma inmediata

al operador móvil y a las entidades financieras, los procedimientos actuales suelen ser complejos, poco estandarizados y dispersos en múltiples canales. Esta fragmentación dificulta una respuesta oportuna, dando ventaja a los delincuentes para ejecutar fraudes rápidamente.

El bloqueo del chip y del dispositivo móvil son medidas clave para evitar accesos indebidos, pero la falta de una guía clara sobre estos pasos expone a los usuarios a riesgos financieros y emocionales. Si no se actúa con rapidez, las consecuencias pueden escalar: pérdida de fondos, violación de la privacidad, suplantación de identidad e incluso afectaciones a terceros.

Osiptel (2023) subraya que la falta de educación sobre cómo manejar estas emergencias aumenta la vulnerabilidad de las víctimas y facilita los delitos.

Figura 4. Lienzo dos dimensiones del usuario



Fuente: Elaboración Propia

Con el fin de ilustrar esta situación, se elaboró un lienzo de doble dimensión (Figura 4) que analiza el caso de Juan, un profesional de 55 años que sufrió el robo de su celular. Este dispositivo contenía sus accesos bancarios, aplicaciones de pagos, redes sociales y WhatsApp. En los primeros minutos posteriores al robo, Juan no contaba con una guía clara

que le indicara cómo proteger su información. Esta falta de conocimiento lo llevó a perder tiempo valioso en buscar soluciones, durante el cual los delincuentes no se limitaron a solo ejecutar transacciones fraudulentas, sino que también lograron acceder a su cuenta de WhatsApp, haciéndose pasar por él para solicitar dinero a sus contactos cercanos. Esta situación intensificó el daño emocional y social, ya que algunos de sus amigos fueron engañados y realizaron transferencias, pensando que ayudaban a una emergencia personal.

Desde la dimensión técnica, Juan enfrentó procesos de bloqueo poco intuitivos y diferentes en cada institución. El desconocimiento sobre cómo gestionar el incidente desde un solo canal lo llevó a actuar de forma desorganizada, aumentando su exposición al fraude. Desde la dimensión emocional, experimentó altos niveles de ansiedad, frustración e inseguridad al sentir que había perdido el control de su información y que sus datos estaban en manos de terceros. Según un estudio de Kaspersky (2023), muchos usuarios en situaciones similares reportan sentirse desprotegidos porque desconocen los procedimientos correctos para bloquear sus cuentas, lo que incrementa el riesgo de sufrir pérdidas financieras. Las frustraciones de Juan reflejan una problemática más amplia, los usuarios se sienten desprotegidos ante un evento tan crítico, con la expectativa de que las entidades ya deberían ofrecer soluciones automatizadas.

Los hallazgos del lienzo de dos dimensiones destacan que el fraude financiero asociado al robo de dispositivos móviles no se limita a pérdidas económicas directas. Este problema revela un desconocimiento extendido entre los usuarios sobre las medidas de protección necesarias, lo cual se agrava por el estrés y la ansiedad que experimentan en momentos críticos. La falta de orientación clara y accesible amplifica la vulnerabilidad de las víctimas, permitiendo que los delincuentes aprovechen las demoras para causar mayores daños financieros, emocionales y sociales. Por ello, se requiere una solución integral que

simplifique los pasos a seguir, permita actuar rápidamente y brinde al usuario seguridad y tranquilidad en momentos críticos.

En base al lienzo de dos dimensiones, a continuación, se analizará las frustraciones y motivaciones del usuario, Juan.

Frustraciones del usuario

Uno de los sentimientos más frecuentes que experimenta Juan tras el robo de su celular es la sensación de vulnerabilidad extrema. Perder su celular significó perder el control sobre su información financiera, personal y digital, generándole una fuerte incertidumbre sobre los pasos a seguir.

Una fuente crítica de frustración fue la complejidad de los procesos actuales. Los procedimientos para bloquear cuentas y líneas varían entre bancos y operadores, y suelen ser poco intuitivos. Esto obligó a Juan a buscar información por su cuenta y a contactarse con varias instituciones en un momento de alta tensión emocional.

La ausencia de una herramienta unificada que lo guiara en los primeros minutos tras el incidente incrementó su desamparo. Cada minuto perdido implicaba una mayor exposición al fraude, al uso indebido de su identidad o a la pérdida de fondos.

Además, Juan partía de una expectativa: confiaba en que su banco u operador contaban con mecanismos automáticos de protección. Al comprobar que debía gestionar todo por separado y sin orientación, sintió una pérdida de confianza en las instituciones.

Motivaciones del usuario

Pese al escenario adverso, Juan mantenía motivaciones fuertes para buscar soluciones. Su necesidad inmediata era proteger su identidad y su dinero. Valora especialmente soluciones prácticas, intuitivas y veloces que le permitan recuperar el control con rapidez.

También desea recuperar estabilidad emocional. El miedo a que accedan a su información y el desconocimiento sobre los procedimientos correctos lo hicieron sentirse

expuesto. Por eso, propuestas como Segurazo, plataforma en desarrollo planteada en esta tesis, responden a una necesidad real: ofrecer una guía rápida y centralizada que reduzca el impacto del robo.

Además, una solución así ayudaría a restablecer la confianza en sus instituciones financieras y operadoras. Un acompañamiento claro y efectivo puede marcar la diferencia entre sentirse abandonado y sentirse protegido.

Contexto y respaldo del problema

El entorno confirma la urgencia de este tipo de herramientas. Según la Defensoría del Pueblo (2023), entre 2018 y 2021 las denuncias por ciberdelitos en Perú se cuadruplicaron, siendo el fraude informático la modalidad más recurrente, con un 71.7% de los casos. En 2023, este tipo de fraude volvió a liderar las estadísticas con 2,382 denuncias registradas (El Peruano, 2023).

A nivel regional, un estudio de LexisNexis Risk Solutions reveló que el 60% de las organizaciones en América Latina reportaron un incremento en los niveles generales de fraude en los últimos 12 meses, atribuyendo el 51% de las pérdidas generales por fraude a canales digitales (LexisNexis Risk Solutions, 2024). Asimismo, las alertas diarias por fraude financiero en América Latina superaron a las de Norteamérica en el último año, evidenciando la creciente sofisticación y frecuencia de estos delitos en la región (Bloomberg Línea, 2024).

Análisis comparativo con otros países

A nivel internacional, diversas iniciativas han sido implementadas para atender los riesgos vinculados al robo de dispositivos móviles. A continuación, se presentan tres casos relevantes que ofrecen referencias útiles para el diseño de propuestas como Segurazo.

Brasil: Aplicación "Celular Seguro"

En diciembre de 2023, el Gobierno brasileño lanzó la aplicación "Celular Seguro", diseñada para que las víctimas de hurto o robo de teléfonos móviles puedan bloquear de

manera rápida y sencilla sus dispositivos. Al registrar el número de celular en la aplicación, los usuarios pueden, en caso de robo, activar un botón de aviso que notifica automáticamente a la Agencia Nacional de Telecomunicaciones (Anatel) para cancelar el funcionamiento del aparato. Además, el sistema envía alertas a las instituciones bancarias asociadas para bloquear las aplicaciones financieras en el dispositivo, previniendo posibles fraudes.

Diferencias con Segurazo: “Celular Seguro” se enfoca en bloquear el dispositivo y las aplicaciones financieras de forma inmediata, mediante una integración directa con entidades reguladoras y bancarias. En cambio, Segurazo, propuesta desarrollada en el presente estudio, no realiza bloqueos automáticos, pero ofrece una guía centralizada que permite al usuario contactar rápidamente a su operador, entidad financiera y autoridades competentes, brindando orientación clara y simplificada para mitigar el daño en los primeros minutos tras el robo. A diferencia de otras soluciones, incluye también componentes de apoyo legal, facilitando una respuesta más integral.

Reino Unido: Servicio "Immobilise"

“Immobilise” es una plataforma oficial del Reino Unido que permite a los ciudadanos registrar dispositivos electrónicos como teléfonos móviles, laptops o bicicletas en una base de datos nacional utilizada por la policía. En caso de pérdida o robo, el usuario puede reportar el incidente a través del sitio web, lo que facilita la identificación y recuperación del bien si es encontrado. Aunque no cuenta con aplicación móvil ni realiza bloqueos automáticos, actúa como medida de respaldo y disuasión frente a la reventa de objetos robados.

Diferencias con Segurazo: A diferencia de Immobilise, que se centra en la recuperación de dispositivos mediante un registro previo, la propuesta de Segurazo brinda orientación inmediata al usuario tras el robo, guiándolo paso a paso para contactar a las entidades necesarias y reducir el riesgo de fraude financiero.

México: Línea de emergencia 01800-DNUNCIA

En México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) habilitó la línea gratuita 01800-DNUNCIA (01800-368-6224), que permite a los usuarios reportar de inmediato el robo o extravío de sus dispositivos móviles. A través de esta línea, se puede solicitar el bloqueo de tarjetas bancarias y recibir orientación sobre los pasos para proteger la información financiera. Esta iniciativa busca ofrecer un canal centralizado y de atención directa para reducir el impacto de fraudes derivados del robo de celulares.

Diferencias con Segurazo: Mientras esta solución depende de la disponibilidad y rapidez de la atención telefónica, la propuesta de Segurazo busca brindar al usuario una plataforma digital interactiva, donde encuentre de manera clara y ordenada los pasos a seguir para contactar rápidamente a entidades clave y mitigar riesgos financieros o de suplantación de identidad.

A continuación, se muestra en la Tabla 1, el resumen comparativo de soluciones internacionales frente al robo de celulares.

Tabla 1. Resumen comparativo de soluciones internacionales frente al robo de celulares

País	Solución	Canal principal	Bloqueo automático	Asesoría legal	Plataforma digital	Nivel de orientación inmediata
Brasil	Celular Seguro	App móvil	Sí	No	Sí	Alta (bloqueo directo)
Reino Unido	Immobilise	Sitio web	No	No	Parcial	Baja (registro previo)
México	01800-DNUNCIA	Línea telefónica	No (depende del banco)	No	No	Media (requiere llamada)
Perú (propuesta)	Segurazo	App web/guía interactiva	No (contacto directo)	Sí (en guía)	Sí	Alta (acción guiada)

Fuente: Elaboración Propia

1.3. Sustento de la complejidad y relevancia del problema a resolver

El robo de dispositivos móviles en Perú representa una amenaza creciente, que expone a los usuarios a riesgos financieros, emocionales y de seguridad. Según la Memoria Anual de

ASBANC (2023), se reportan más de 2,100 reclamos mensuales por operaciones no reconocidas, muchas de ellas relacionadas con la pérdida de celulares. Asimismo, la SBS informó que en 2020 las pérdidas por fraude externo en canales virtuales, considerando todo tipo de incidentes digitales, ascendieron a S/ 51.3 millones, frente a los S/ 38.8 millones registrados en 2019, reflejando un incremento significativo en el periodo.

Esta situación se ha intensificado por el fuerte avance de la digitalización en el país. Entre 2020 y 2023, las operaciones por banca virtual crecieron en 405%, con la banca móvil concentrando el 88% de estas transacciones. En el caso particular del robo de dispositivos móviles, se estima que en 2023 aproximadamente 24,698 personas en Perú sufrieron pérdidas económicas, con un perjuicio agregado de hasta S/ 49 millones para el sistema financiero.

Además del impacto financiero, este problema revela una alta complejidad operativa. Las víctimas deben reaccionar en un contexto de urgencia, pero se enfrentan a procesos dispersos y poco intuitivos. Los canales de atención de las entidades financieras y operadoras no están integrados, lo que impide una respuesta eficaz en los primeros minutos tras el robo. Esto incrementa el riesgo de transacciones fraudulentas antes de que el usuario logre recuperar el control.

A este escenario se suma la necesidad de actualizar los marcos regulatorios. A pesar de los esfuerzos realizados por entidades como la SBS, INDECOPI y ASBANC, persisten vacíos legales y operativos que dificultan una actuación rápida y coordinada frente al fraude. Las instituciones aún operan bajo marcos regulatorios que no han sido diseñados para responder con la inmediatez y adaptabilidad que exigen los delitos digitales actuales, lo que limita una acción eficiente ante estos riesgos emergentes.

El robo de dispositivos móviles genera consecuencias que van más allá de la pérdida material. Las víctimas enfrentan riesgos financieros por accesos indebidos a cuentas, pero también impactos emocionales como ansiedad y desconfianza hacia los servicios digitales. En

paralelo, las entidades financieras deben asumir pérdidas por operaciones no reconocidas y afrontar una creciente presión regulatoria. Esta problemática compleja requiere una solución ágil y coordinada entre usuarios, bancos, operadoras y reguladores. Segurazo responde a esta necesidad, al permitir acciones inmediatas y guiadas tras un robo, reduciendo el daño y fortaleciendo la confianza en el sistema financiero. Su enfoque contribuye directamente al cumplimiento de la meta 16.4 del ODS, que promueve la reducción de flujos financieros ilícitos y la consolidación de instituciones más seguras.

Impacto en los usuarios

Más allá del impacto emocional y operativo mencionado, las cifras muestran la gravedad del fraude digital para los ciudadanos. En 2023 se reportaron más de 6,000 denuncias de estafas digitales en Perú, con pérdidas que ascendieron a S/ 53,089,692 y USD 26,977,635, siendo la mayoría relacionadas con accesos indebidos tras el robo de dispositivos móviles (Infobae, 2023). Entre enero y julio del mismo año, Indecopi recibió 4,372 reclamos por operaciones no reconocidas, cifra que casi igualó los 5,308 reclamos de todo 2022, reflejando la tendencia al alza (Ojo Público, 2023).

Estas cifras evidencian la magnitud del problema para los usuarios, quienes enfrentan pérdidas económicas y, a la vez, carecen de acompañamiento inmediato. Ante esta situación, Segurazo se presenta como una herramienta de orientación rápida que ayuda a reducir el riesgo de que las personas actúen tarde o de forma equivocada. Además, al brindar una guía clara y accesible, la solución también contribuye al cumplimiento del ODS 4, fomentando el desarrollo de competencias digitales básicas para la protección de la información personal y financiera en contextos de riesgo.

Impacto en las Entidades Financieras

Para las entidades financieras, el fraude vinculado al robo de celulares genera pérdidas económicas directas y obliga a movilizar recursos operativos y tecnológicos. Solo en el

primer semestre de 2023, los fraudes bancarios crecieron en 90% respecto al mismo periodo del año anterior (Expreso, 2023). Además, Indecopi sancionó a más de 1,000 entidades financieras con multas cercanas a 2,000 UIT por no proteger adecuadamente a sus clientes (Gobierno del Perú, 2023).

Este escenario llevó a la SBS a emitir la Resolución N.º 02286-2024, que obliga a los bancos a asumir las pérdidas de operaciones fraudulentas cuando el cliente no incurre en negligencia (Infobae, 2024). Esta regulación, junto con la presión reputacional, incrementa la necesidad de soluciones que permitan prevenir, contener y responder rápidamente ante incidentes. Segurazo puede integrarse como un soporte inicial que complemente los protocolos internos de las entidades, fortaleciendo la confianza y reduciendo la exposición al riesgo.

1.4 Conclusión

El robo de dispositivos móviles y el consecuente fraude financiero representan un problema de gran magnitud en Perú. Las cifras demuestran un crecimiento alarmante en estos delitos, evidenciando la falta de mecanismos de respuesta rápida y efectiva que permitan a las víctimas minimizar los daños financieros y emocionales. En este contexto, Segurazo contribuirá significativamente a fortalecer la seguridad digital, generar confianza en los servicios financieros y reducir los costos asociados al fraude.

Además, el desarrollo de este proyecto impulsa un modelo de negocio sostenible, ya que atiende una problemática real del mercado peruano con un enfoque escalable y adaptable a otras regiones. Su implementación generará valor para los usuarios y también ofrecerá beneficios económicos a los actores del ecosistema financiero, mejorando la eficiencia operativa y reduciendo las pérdidas asociadas al fraude. Se contribuye al fortalecimiento del sistema financiero y a la seguridad digital en el Perú, avanzando en la construcción de un entorno más confiable y resiliente para los ciudadanos y las instituciones.

Capítulo II. Análisis del mercado

2.1. Descripción del mercado

2.1.1. Panorama del mercado de seguridad móvil

Contexto global

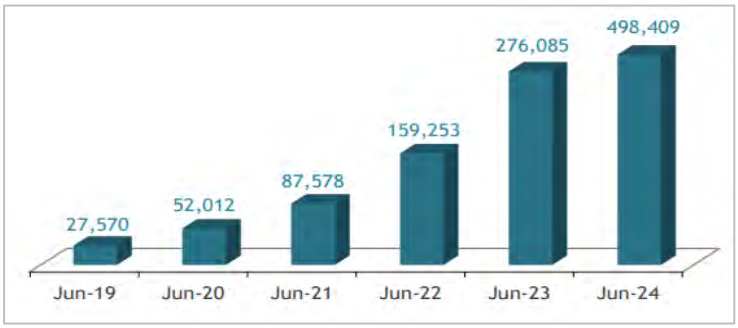
El mercado de seguridad móvil ha experimentado un crecimiento significativo a nivel global debido al aumento en la penetración de dispositivos móviles y a la creciente preocupación por la protección digital. Según la Unión Internacional de Telecomunicaciones (UIT), en 2023 el 78% de la población mundial de 10 años o más poseía un teléfono móvil, aunque no todos estaban conectados a redes móviles avanzadas, lo que incrementa las vulnerabilidades frente a amenazas cibernéticas (UIT, 2023).

A medida que crece el uso de smartphones, también se intensifican los riesgos de seguridad. Fortinet (2024) advierte que entre los principales peligros destacan la explotación de vulnerabilidades en aplicaciones móviles y los ataques de phishing diseñados para capturar datos sensibles. Kaspersky (2024), por su parte, identifica como amenazas más relevantes los programas maliciosos dirigidos a extraer datos y las apps fraudulentas creadas para robar credenciales bancarias. Además, Escudo Digital (2024) resalta la importancia de tecnologías como la autenticación biométrica y los servicios de borrado remoto de datos, que han cobrado notoriedad en eventos globales como el Mobile World Congress.

Análisis del mercado local en Perú

En los últimos años, Perú ha experimentado un notable avance en la adopción de tecnologías móviles y la digitalización, con un crecimiento significativo en la penetración de smartphones y acceso a internet. Según el Reporte de Indicadores de Inclusión Financiera (SBS, 2024), el número de operaciones por banca virtual (a través de internet, software corporativo, software de cliente, banca por teléfono y banca móvil), ha crecido más de 10 veces desde 2017 (Figura 5).

Figura 5. Operaciones en Banca Virtual 2017 -2024



Fuente SBS

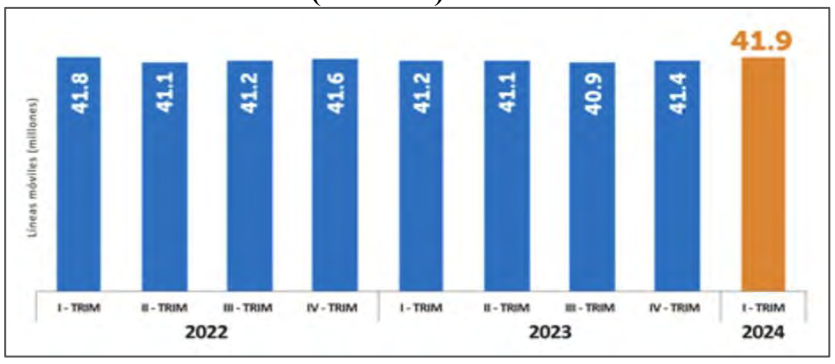
En 2023, según la Encuesta Residencial de Servicios de Telecomunicaciones, el 76% tiene un smartphone con acceso a internet, al igual que el 92.8% de hogares (Osiptel, 2024), ver figura 6.

Figura 6. Acceso a Smartphone 2019 -2023

Fuente: OSIPTEL

A esto se suma que, al cierre del primer trimestre de 2024, el mercado móvil en Perú repuntó, alcanzando 41.9 millones de líneas móviles en servicio (Figura 7), lo que representa un incremento del 1.66% en comparación con el mismo período del año anterior (OSIPTEL, 2024).

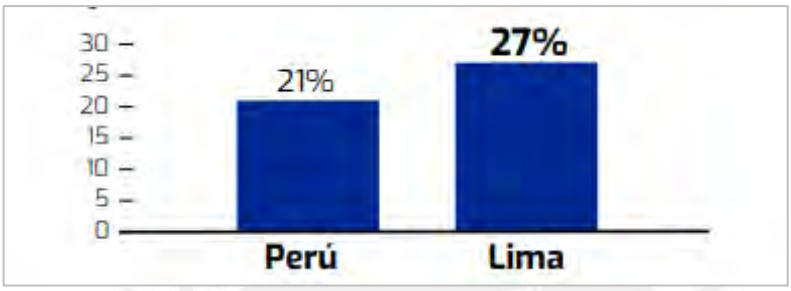
Figura 7. Líneas móviles en servicio (millones)



Fuente: OSIPTEL

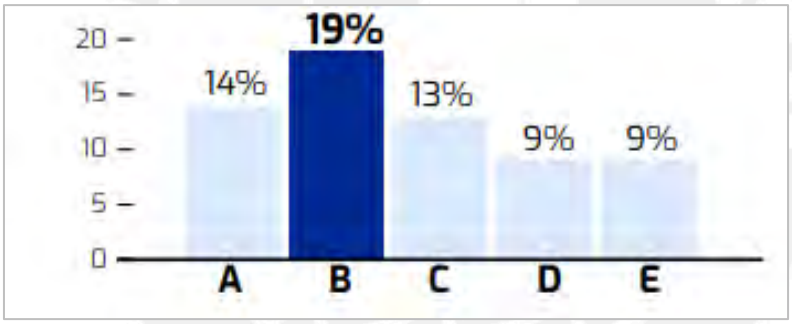
El crecimiento de las personas con acceso a internet y smartphone ha llevado a que sean vulnerables al acceso a sus cuentas bancarias. Según el Primer Reporte de Crimen y Violencia (BCP, 2024), a noviembre de 2024 el 27% de la población peruana ha sido o conoce a alguien víctima de robo de celular, y de dicha población el 16% fue víctima de acceso a sus cuentas bancarias. Ver figura 8 y 9.

Figura 8. Víctimas de robo de celular



Fuente: BCP

Figura 9. Afectados por acceso a cuentas bancarias



Fuente: BCP

Con base en estos datos, y considerando que la población mayor de 14 años representa el 77% del total (INEI, 2024), se estima el tamaño del mercado objetivo al que se dirige Segurazo. Ver tabla 2.

Tabla 2. Mercado Objetivo

	2023
Población Total	33,726,000
Población Mayor a 14 años	26,002,746
Población con Teléfono Celular y acceso a internet movil	19,762,087
Población en Riesgo de Robo o Pérdida de Celular	4,150,038
Personas que Buscarían Bloquear	664,006

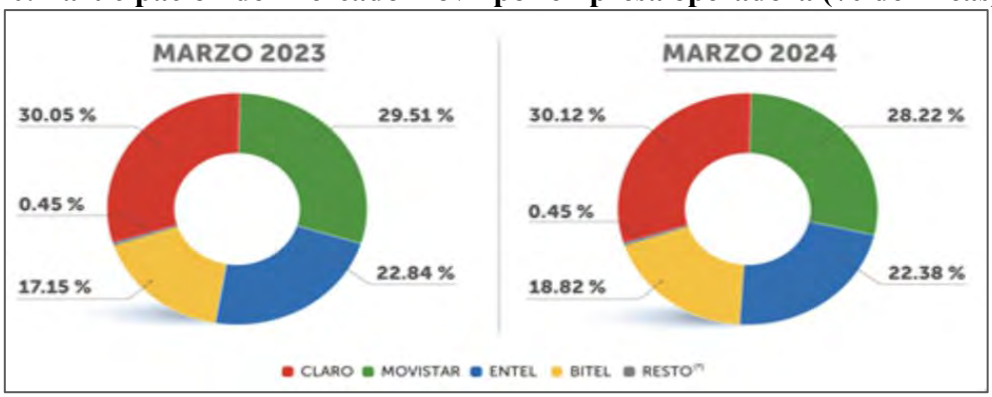
Fuente: Elaboración Propia

Actores del mercado local

El mercado de seguridad móvil en Perú se puede segmentar en varios actores clave que desempeñan roles críticos en la provisión y protección de servicios digitales. En primer lugar, las instituciones financieras y el Gremio, como el Banco de Crédito del Perú (BCP), Interbank, BBVA y ASBANC, han implementado aplicaciones móviles que permiten a los usuarios realizar transacciones financieras y bloquear cuentas bancarias en caso de pérdida o robo del dispositivo. Estas aplicaciones, aunque efectivas en la prevención de fraudes básicos, a menudo carecen de la integración necesaria con otros sistemas de seguridad, lo que limita su capacidad para ofrecer una respuesta rápida y completa en situaciones de emergencia (Banco de Crédito del Perú, 2023; Interbank, 2023; BBVA, 2023). ASBANC ha implementado la línea 1820 para centralizar el bloqueo de cuentas, pero aún enfrenta retos para abordar integralmente los riesgos.

En el sector de telecomunicaciones, compañías como Claro, Movistar y Entel dominan el mercado (Figura 10), ofreciendo servicios de bloqueo remoto de la SIM y, en algunos casos, del dispositivo completo en situaciones de robo o pérdida. Sin embargo, los procesos para llevar a cabo estas acciones suelen ser complicados y no están completamente integrados con las soluciones bancarias, lo que dificulta una respuesta eficiente en momentos críticos (Claro, 2023; Movistar, 2023; Entel, 2023).

Figura 10. Participación del mercado móvil por empresa operadora (% de líneas)



Fuente: OSIPTEL

Los proveedores de soluciones tecnológicas y de ciberseguridad juegan un papel fundamental en la protección de las transacciones digitales y la integridad de los datos en el mercado peruano. Empresas como FICO, Visa, Mnemo, y ADO Techconsulting son clave en este ecosistema, ofreciendo desde soluciones de análisis de riesgo hasta tecnologías avanzadas de autenticación y protección de datos. Estas empresas colaboran tanto con instituciones financieras como con operadores de telecomunicaciones para asegurar que las transacciones digitales sean seguras y que los usuarios estén protegidos frente a amenazas emergentes.

2.1.2. Análisis del entorno: Factores PESTEL del mercado local

Para comprender el entorno que rodea al desarrollo de una solución como Segurazo, se realiza un análisis PESTEL que identifica los factores políticos, económicos, sociales, tecnológicos, ecológicos y legales que influyen en su implementación en el mercado peruano.

a) Político

El escenario político peruano atraviesa un periodo de inestabilidad institucional, fragmentación en el Congreso y desconfianza ciudadana hacia las autoridades. A esto se suma un estado de emergencia decretado en múltiples distritos del país debido al aumento de la criminalidad y extorsión, especialmente en regiones como Lima, Trujillo, Pataz y Piura (Presidencia del Consejo de Ministros [PCM], 2024). Según Ipsos Perú (2024), el 85% de la población considera que la delincuencia ha aumentado, y el Gobierno ha respondido con medidas limitadas como la declaración de estados de emergencia sin un acompañamiento tecnológico integral.

Además, se espera un clima de mayor tensión política en vista de las elecciones generales programadas para 2026, lo que podría traducirse en reformas de seguridad y presión legislativa sobre temas de protección ciudadana y ciberseguridad. Esta situación

genera oportunidades para soluciones privadas complementarias, capaces de actuar más ágilmente que el aparato estatal.

b) Económico

Pese a un contexto económico regional desafiante, Perú ha mostrado signos de recuperación moderada tras la pandemia. Según el Banco Central de Reserva del Perú (BCRP, 2024), el crecimiento del PBI para 2024 se estima en 2.5%, impulsado principalmente por minería y servicios. Sin embargo, la inflación acumulada de los últimos dos años ha afectado el poder adquisitivo de los hogares urbanos.

En paralelo, la digitalización de los servicios financieros continúa en expansión. La Superintendencia de Banca, Seguros y AFP (SBS, 2024) reporta que el 88% de las transacciones digitales se realizan mediante banca móvil, lo que evidencia una adopción acelerada de canales digitales por parte de los ciudadanos. Esta transformación exige plataformas seguras, ágiles y confiables que minimicen riesgos ante eventos como robos de celulares o fraudes financieros.

c) Social

Desde la dimensión social, el principal reto es la desinformación de los ciudadanos ante un evento de robo o fraude digital. Según el Instituto Nacional de Estadística e Informática (INEI, 2024), más del 65% de personas que han sufrido el robo de su celular no realizaron una denuncia formal, y solo una minoría conoce el procedimiento para bloquear cuentas bancarias o líneas móviles de forma inmediata.

Esta falta de información, sumada a una percepción generalizada de vulnerabilidad, crea un entorno propicio para herramientas tecnológicas que eduquen y acompañen al usuario en tiempo real. Además, la alta penetración de smartphones, combinada con el crecimiento de las billeteras digitales y el comercio electrónico, incrementa la exposición al riesgo,

especialmente entre jóvenes adultos de 18 a 35 años, quienes representan el grupo más activo digitalmente (Datum Internacional, 2024).

d) Tecnológico

Segurazo se encuentra inmerso en un proceso de transformación digital en nuestro país que abarca diversos sectores, especialmente el financiero. De acuerdo con el estudio Fintech Radar Perú 2024, el número de empresas fintech en el país ha alcanzado las 237, con una tasa de crecimiento promedio anual del 17%. Estas empresas se enfocan principalmente en pagos, préstamos y asesoría financiera, lo que evidencia una clara apertura del mercado a nuevas soluciones tecnológicas orientadas al usuario final (Finnovista, 2024).

En cuanto a la automatización, el sistema financiero peruano ha duplicado sus inversiones en digitalización desde la pandemia, desplazando progresivamente los canales presenciales hacia plataformas virtuales. Según el Reporte de Estabilidad Financiera del BCRP (2024), este proceso ha permitido mejorar la eficiencia operativa y reducir costos en entidades como bancos y cajas municipales, facilitando a su vez una mayor inclusión financiera. Las operaciones digitales son más rápidas comparado con la presencialidad, lo que ha favorecido la aceptación de soluciones automatizadas tanto por parte de los usuarios como de las propias instituciones financieras (BCRP, 2024).

La conectividad es otro componente esencial del ecosistema tecnológico. Acorde a OSIPTEL, el número de líneas móviles activas en Perú alcanzó los 42.7 millones en 2024, lo cual implica un crecimiento del 3.28% respecto al año anterior. Este crecimiento se complementa con la progresiva implementación del 5G y la llegada de tecnologías satelitales como Starlink, que están permitiendo el acceso a internet incluso en zonas rurales, donde tradicionalmente no existía cobertura adecuada (OSIPTEL, 2024).

La ciberseguridad ha adquirido una relevancia estratégica a raíz de incidentes recientes. Perú ocupa el puesto 5 entre 33 países de América Latina y el Caribe en el Índice

Global de Ciberseguridad 2024, según la Unión Internacional de Telecomunicaciones. No obstante, eventos como la filtración masiva de datos de clientes de Interbank en noviembre de 2024 han puesto en evidencia vulnerabilidades críticas. Este último caso afectó directamente la reputación del banco e incrementó la desconfianza del público frente a la seguridad de los servicios digitales (BCRP, 2024).

Finalmente, el acceso a la tecnología por parte de la población continúa creciendo de forma acelerada. Acorde al INEI, en 2024, el 95.1% de los hogares peruanos contaba con al menos un miembro que tenía teléfono celular, y el 58.4% tenía acceso a internet. Además, el uso de banca móvil ha incrementado significativamente, reflejando una clara preferencia por canales digitales sobre las visitas presenciales a oficinas bancarias. Este cambio cultural es fundamental para proyectos como SEGURAZO, que busca precisamente brindar soporte digital inmediato en situaciones de fraude o robo de dispositivos (INEI, 2024).

e) Ecológico

En línea con el Acuerdo de París, el Estado peruano se ha comprometido a reducir en un 40% sus emisiones de gases de efecto invernadero (GEI) al 2030 y alcanzar la neutralidad de carbono en 2050. Estos objetivos están contemplados en la Ley Marco sobre Cambio Climático (Ley 30754) y su reglamento, que establecen principios y responsabilidades de adaptación y mitigación para los sectores público y privado (MINAM, 2023).

Uno de los pilares de la política ambiental en Perú es la sostenibilidad y reducción de la huella de carbono. El Ministerio del Ambiente ha desarrollado la plataforma “Huella de Carbono Perú”, una herramienta digital que permite a las organizaciones medir, verificar y reducir sus emisiones. Hasta fines de 2023, más de 850 empresas y entidades públicas se habían registrado, demostrando avances en la gestión ambiental corporativa. Esta herramienta, además de ser gratuita, está alineada con estándares internacionales como ISO 14064 (MINAM, 2023).

Desde el punto de vista de la legislación ambiental, Perú cuenta con marcos normativos modernos y especializados. La Ley General del Ambiente (Ley 28611) y la Ley de Gestión Integral de Residuos Sólidos (Decreto Legislativo 1278) promueven la gestión ambiental preventiva, el uso racional de recursos naturales y la valorización de residuos. Estas normas obligan a las organizaciones a integrar buenas prácticas ambientales desde sus operaciones.

Finalmente, desde una perspectiva operativa, proyectos como Segurazo pueden contribuir indirectamente a los objetivos ecológicos del país al operar completamente en formato digital. Su modelo de atención remota reduce la necesidad de traslados físicos hacia oficinas bancarias, operadoras móviles o comisarías, lo cual disminuye las emisiones de gases relacionadas al transporte urbano. Además, al evitar el uso de formularios impresos, actas y papelería, la plataforma se alinea con la tendencia "paperless" que muchas entidades están incorporando para reducir su huella ambiental.

f) Legal

Uno de los pilares más relevantes es la protección de datos personales, regulada por la Ley 29733, que garantiza el derecho de toda persona a la protección de su información personal y familiar. En 2024, se reforzó su reglamento mediante el Decreto Supremo N.º 016-2024-JUS, con el objetivo de alinear la normativa nacional a estándares internacionales de privacidad y ciberseguridad (Plataforma Digital Única del Estado Peruano, 2024).

En cuanto a la regulación financiera, se tiene la Ley General del Sistema Financiero y del Sistema de Seguros (Ley 26702), la cual es supervisada por la Superintendencia de Banca, Seguros y AFP (SBS). Esta normativa establece el marco protegiendo al usuario exigiendo estándares operativos adecuados para cualquier empresa que actúe como canal de servicios financieros (SBS, 2024).

También es fundamental considerar la protección al consumidor, regulada por el Código de Protección y Defensa del Consumidor (Ley 29571). Esta norma asegura que todos los ciudadanos accedan a productos y servicios idóneos, con derechos claros y mecanismos efectivos para presentar reclamos. Segurazo, como servicio digital de orientación en situaciones de emergencia, deberá brindar información precisa, completa y en tiempo oportuno, cumpliendo con los principios exigidos por el INDECOPI (Plataforma Digital Única del Estado Peruano, 2024).

En lo que respecta a la propiedad intelectual, se tiene el Decreto Legislativo 822, que protege derechos sobre obras literarias, artísticas y digitales, incluidos los programas de ordenador y las bases de datos. Se deberá tener atención a nuestra interfaz, software, contenidos y algoritmos propios para evitar infracciones que puedan derivar en demandas o sanciones (Plataforma Digital Única del Estado Peruano, 2024).

Riesgos legales

Uno de los más importantes es el riesgo de incumplimiento en la gestión de datos personales sensibles. La Ley 29733 y su reglamento requieren consentimiento explícito, finalidad clara y medidas de seguridad sólidas. Cualquier filtración de datos o uso indebido podría ser sancionado con multas superiores a las 100 UIT, además de generar un impacto reputacional irreversible. Segurazo solo usará el nombre, número de celular y correo electrónico de forma opcional para el registro previo al uso del servicio.

En el ámbito de la ciberseguridad, la Ley 30096 (Ley de Delitos Informáticos) establece que las organizaciones son responsables de prevenir el acceso indebido a sus sistemas. En caso de una brecha de seguridad o ataque informático, la empresa podría enfrentar consecuencias civiles y penales si se demuestra negligencia en sus mecanismos de protección.

Por último, existe riesgo vinculado a la propiedad intelectual, si la plataforma utilizara recursos de terceros (por ejemplo: interfaces o contenido visual) sin la debida autorización o

licencia. Las infracciones en esta materia pueden derivar en procesos judiciales costosos y el retiro forzado del producto del mercado.

2.1.3. Análisis del entorno competitivo

Tras revisar los factores del entorno que influyen en el desarrollo y adopción de soluciones digitales como Segurazo, resulta clave analizar también el panorama competitivo en el mercado peruano. Este análisis permite identificar a los actores que actualmente ofrecen servicios relacionados con la seguridad móvil, su grado de cobertura y las principales brechas que aún no han sido abordadas. Comprender este entorno competitivo es esencial para posicionar de manera estratégica la propuesta de Segurazo y determinar sus ventajas diferenciales.

2.1.3.1.Poder de negociación de los clientes y usuarios

Poder de negociación de las entidades financieras

Dentro del mercado objetivo de Segurazo, las entidades financieras constituyen un actor clave con un alto grado de poder de negociación, el cual varía según el tamaño y capacidad de cada institución.

Por un lado, los grandes bancos como el Banco de Crédito del Perú (BCP), BBVA y Scotiabank tienen una fuerte posición de mercado. Estas instituciones cuentan con recursos suficientes para invertir en soluciones avanzadas de seguridad digital, lo que les otorga una mayor capacidad para negociar precios, exigir altos estándares de servicio e influir en los requerimientos funcionales de las soluciones que adoptan.

Por otro lado, se tiene a las entidades financieras pequeñas y medianas, estas entidades, que incluyen bancos más pequeños, cajas municipales, entre otros, tienen menor poder de negociación debido a sus limitados recursos. Sin embargo, su flexibilidad y necesidad de diferenciarse pueden llevarlas a adoptar nuevas soluciones de seguridad más rápidamente, lo que puede ser una oportunidad para nuestro servicio.

En cuanto a las regulaciones en nuestro país, las entidades financieras están sujetas a regulaciones estrictas por parte de la Superintendencia de Banca, Seguros y AFP (SBS) y otros organismos reguladores. Estas regulaciones imponen requisitos de seguridad y protección de datos que las entidades deben cumplir, esto puede incrementar su poder de negociación para todos los tipos de entidades financieras dado que exigirán mayores estándares a nuestra solución.

Las oportunidades identificadas en el mercado de seguridad digital son numerosas y relevantes. Sin embargo, para garantizar un enfoque estratégico y eficiente, es necesario priorizarlas en función de su viabilidad técnica, financiera y su alineación con las capacidades actuales del equipo. A continuación, se presenta un análisis priorizado de las principales oportunidades:

- **Desarrollo de herramientas centralizadas para seguridad digital**:

  Viabilidad técnica: Alta, debido al avance en tecnologías de integración de sistemas y disponibilidad de APIs abiertas en el sector financiero.

  Viabilidad financiera: Moderada, ya que los costos iniciales de desarrollo son significativos, pero escalables en el tiempo.

  Alineación con capacidades del equipo: Alta, considerando la experiencia en tecnologías digitales y gestión de proyectos.

- **Implementación de sistemas de monitoreo proactivo basado en IA**:

  Viabilidad técnica: Moderada, debido a la complejidad de entrenar algoritmos efectivos y adaptados al contexto local.

  Viabilidad financiera: Baja, ya que requiere una inversión considerable en infraestructura y análisis de datos.

  Alineación con capacidades del equipo: Moderada, dado que requiere formación adicional en IA y análisis de datos avanzados.

- **Educación digital para usuarios finales sobre seguridad financiera**:

  Viabilidad técnica: Alta, ya que puede implementarse con plataformas existentes de e-learning.

  Viabilidad financiera: Alta, debido a los costos relativamente bajos de diseño de contenidos y distribución digital.

  Alineación con capacidades del equipo: Alta, considerando la experiencia previa en diseño de procesos educativos y creación de contenidos.

- **Desarrollo de alianzas estratégicas con instituciones financieras y operadores**:

  Viabilidad técnica: Alta, ya que no implica desarrollos tecnológicos complejos.

  Viabilidad financiera: Moderada, dependiendo de los términos de los acuerdos establecidos.

  Alineación con capacidades del equipo: Alta, dada la experiencia en negociación y gestión de relaciones corporativas.

2.1.3.2. Poder de negociación de los usuarios finales

Como visto al inicio del capítulo, con la creciente adopción de servicios bancarios móviles, impulsada por la expansión de la conectividad y la penetración de smartphones, los usuarios están más conscientes de los riesgos de seguridad. Sin embargo, su capacidad para negociar es baja debido a la falta de alternativas más potentes en el mercado, así también, las soluciones actuales no satisfacen completamente las necesidades de los usuarios debido a procedimientos poco intuitivos y no estandarizados. Esto nos da la oportunidad de ofrecer nuestro servicio, el cual será lo más intuitivo posible.

En cuanto a las regulaciones en nuestro país se tiene a Indecopi, que busca proteger los derechos de los consumidores, incluidas las obligaciones de los bancos de asegurar los fondos de sus clientes. Estas regulaciones pueden fortalecer el poder de

negociación de los usuarios al obligar a las entidades financieras, y en su defecto a nuestro servicio, a adoptar soluciones que protejan eficazmente a los usuarios.

Los usuarios finales de soluciones de seguridad móvil buscan simplicidad y protección integral. Valoran interfaces intuitivas que minimicen la complejidad técnica, capaces de reaccionar en tiempo real ante amenazas, especialmente para proteger datos sensibles. Además, demandan soluciones accesibles y compatibles con diversos dispositivos y sistemas operativos. Estas expectativas reflejan la creciente necesidad de herramientas que combinen efectividad, facilidad de uso y protección de la información en un entorno digital en constante evolución.

Como vimos en la sección anterior, con la adopción mayor de servicios móviles financieros, los usuarios demandan consigo seguridad digital, el cual es un factor importante al elegir entre los distintos servicios y aplicaciones financieras. Esto aumenta la presión sobre las empresas para ofrecer herramientas de seguridad más robustas. Por su lado, los usuarios también influyen mediante recomendaciones y opiniones compartidas en redes sociales. Estas recomendaciones tienen un impacto significativo en la popularidad de las soluciones de seguridad móvil. Un usuario satisfecho con una experiencia segura e intuitiva es más propenso a recomendar estas herramientas, generando una cadena de influencia que incrementa su demanda en el mercado. Junto con esto, los usuarios también participan en cierta medida en el diseño de las soluciones al dar feedback, esto ayuda a las empresas a abordar necesidades específicas, lo cual fortalece la propuesta de valor.

2.1.3.3.Poder de negociación de proveedores

Por un lado, se tienen a los proveedores de UCaaS como Genesys, Cisco y Five9, estos son actores dominantes en el mercado de comunicaciones unificadas. Estos proveedores ofrecen plataformas robustas y escalables que integran varios canales de

comunicación en una única solución. Dada la especialización y el alto nivel de competencia tecnológica en este sector, el poder de negociación de estos proveedores es alto. Las empresas que necesitan estas soluciones pueden encontrar una competencia limitada, lo que les da a los proveedores un mayor control sobre los precios y las condiciones de servicio. Además, las empresas pueden enfrentarse a costos elevados de cambio si deciden migrar a otro proveedor.

Segundo, se tiene a los integradores como Telefónica, Cirion, Claro y Entel, quienes son cruciales para la implementación y el soporte de las soluciones tecnológicas necesarias para el proyecto. Estos integradores poseen la experiencia y la infraestructura necesaria para garantizar una integración fluida de los sistemas de comunicaciones. El poder de negociación de estos integradores puede ser moderado a alto, dependiendo de la complejidad del proyecto.

Tercero, se tiene a las soluciones de IVR, los cuales son fundamentales para gestionar grandes volúmenes de llamadas y mejorar la experiencia del cliente. Los proveedores avanzados en IVR tienen un mayor poder de negociación debido a la necesidad de tecnología precisa y altamente personalizable.

La dependencia de proveedores tecnológicos clave presenta riesgos que pueden afectar la competitividad del proyecto. Por su lado, fluctuaciones en precios y fallas de proveedores afectan los márgenes y la reputación del proyecto, generando incertidumbre.

Esta dependencia puede limitar la capacidad del proyecto para mantener costos competitivos y adaptarse rápidamente a cambios en el mercado. Para mitigar este riesgo, deberemos implementar estrategias como la diversificación de proveedores, lo que permitirá reducir la dependencia. Además, negociar contratos a largo plazo con términos favorables ayudará a garantizar precios estables y condiciones claras. Asimismo, es esencial contar con un plan de contingencia que asegure la continuidad operativa en caso

de fallas o interrupciones en los servicios de los proveedores, esto con el fin de asegurar la calidad y el nivel de servicio hacia los clientes y usuarios.

Por lo tanto, se observa que el poder de negociación de los proveedores en este proyecto varía según el tipo de servicio proporcionado, concluyéndose que es alto.

2.1.3.4. Amenaza de nuevos competidores

Para demostrar la intensidad de esta fuerza, se analizarán las barreras de entrada para nuevos competidores.

En primer lugar, la entrada a la industria financiera en Perú, especialmente en áreas tecnológicas avanzadas como las soluciones de seguridad digital requiere una inversión inicial de consideración. Esto incluye la adquisición de herramientas tecnológicas y la contratación de especialistas. Además, la constante necesidad de inversión en Investigación y Desarrollo (I+D) para mantenerse al día con la digitalización creciente en el sector bancario eleva aún más esta barrera. Los nuevos entrantes, enfrentarán mayores costos iniciales y operativos, lo que dificulta su competitividad desde el inicio.

En segundo lugar, se debe considerar el entorno regulador en Perú, con instituciones como la SBS, ASBANC, MTC, Indecopi, y Osiptel, es riguroso y exige a las empresas cumplir con normas específicas para operar en el sector financiero. La interacción y coordinación cercanas con estas instituciones son esenciales, lo que puede ser un desafío significativo para los nuevos competidores que no están familiarizados con el marco legal peruano y no tienen coordinación con los reguladores.

Y, en tercer lugar, las relaciones comerciales sólidas y establecidas con las principales entidades financieras son cruciales para el éxito de la implementación de una solución como la propuesta. Ingresar al mercado una solución tecnológica requiere una estrecha colaboración desde el inicio del proyecto con las entidades financieras, lo que

puede ser difícil para nuevos competidores que carecen de coordinaciones y conexiones estratégicas en el sector. Las empresas existentes que ya han construido relaciones de confianza con los bancos y otras instituciones financieras tienen una ventaja significativa sobre los nuevos entrantes.

Estas barreras de entrada pueden evolucionar con el tiempo debido a varios factores. El acceso cada vez más fácil y económico a tecnologías avanzadas, como la inteligencia artificial y blockchain, podría reducir parcialmente las barreras tecnológicas. Esto permitiría a nuevos competidores aprovechar herramientas que antes eran inaccesibles, facilitando su entrada al mercado. Por su lado, cambios en el entorno regulador también podrían influir en estas barreras. Si las normativas se vuelven más flexibles o inclusivas para fomentar la competencia y la innovación, los nuevos entrantes podrían encontrar menos obstáculos. Así también, la digitalización acelerada que observamos del mercado financiero en Perú podría expandir las oportunidades para nuevos competidores. Aun así, los estándares de calidad y las expectativas crecientes de los consumidores mantendrán elevadas las barreras relacionadas con la reputación y las relaciones comerciales estratégicas.

Se concluye entonces que esta fuerza es relativamente baja debido a que existen altas barreras de entrada, esto desincentiva la entrada de nuevos competidores. En adición, la necesidad de contar con relaciones comerciales sólidas con las entidades financieras y la reputación ya construida por los competidores existentes actúan como barreras contra nuevos competidores. Las entidades financieras buscarán altos estándares que cuestan tiempo y recursos para construir, nuevos competidores necesitarán iniciar desde cero si desean competir con nuestra solución.

2.1.3.5.Amenaza de productos sustitutos

Actualmente, en el mercado peruano existen diversas soluciones que intentan responder a las necesidades de los usuarios ante el robo de dispositivos móviles, como los servicios ofrecidos por teleoperadores, softwares de ciberseguridad, aseguradoras y entidades financieras. Sin embargo, estas alternativas presentan limitaciones importantes tanto en funcionalidad como en experiencia de usuario.

Tabla 3. Productos sustitutos

Producto Sustituto	Mecanismo	Bloqueo de celular	Devolución de dinero	Bloqueo de cuentas
Teleoperadores	Llamada	**Sí**	No	No
Software de ciberseguridad	Membresía	**Sí**	No	No
Aseguradoras	Burocracia	No	**Sí**	No
Entidades financieras	Llamada	No	**Sí**	**Sí**

Fuente: Elaboración Propia

Como se aprecia en la tabla 3, los usuarios cuentan con diversas alternativas que funcionan como sustitutos. Sin embargo, estas soluciones presentan dos problemas principales. Primero, el mecanismo de atención: en una situación de emergencia, muchas de estas opciones requieren procedimientos lentos, poco intuitivos y dispersos, lo cual no permite actuar con la urgencia que el caso requiere. Segundo, ninguna de estas opciones cubre de forma integral todas las necesidades del usuario tras un robo, lo que deja expuestos tanto a los clientes como a las entidades financieras a riesgos financieros y reputacionales.

Aunque los sustitutos pueden influir en la decisión de algunos consumidores especialmente si ya están incluidos en servicios que actualmente utilizan, su limitado alcance funcional puede ser una desventaja importante. Por ejemplo, un usuario que no haya sufrido una pérdida grave podría conformarse con lo que ya tiene, sin percibir inicialmente el valor de una solución más completa. Sin embargo, esta percepción cambia drásticamente tras experimentar un incidente real.

Por ello, la propuesta de valor de Segurazo busca diferenciarse claramente de estos sustitutos, ofreciendo una plataforma integral que centraliza y simplifica todas las acciones críticas que el usuario debe tomar tras un robo. A través de una experiencia rápida, intuitiva y guiada, Segurazo permite actuar con inmediatez para minimizar el riesgo de fraude, facilitar los bloqueos necesarios y brindar asistencia en los trámites legales o de denuncia

Riesgos de mercado y mitigación

En el análisis del mercado, se identificaron varios riesgos que podrían impactar la implementación y adopción del proyecto. Uno de los riesgos principales es la saturación del mercado con soluciones similares. La competencia en el mercado de seguridad digital es alta, lo que dificulta la diferenciación y el posicionamiento. Para mitigar este riesgo, se propone implementar una campaña de comunicación centrada en destacar los diferenciadores clave, como la integración de múltiples servicios en una sola solución. Además, desarrollar alianzas con actores clave del mercado puede aumentar la visibilidad y el alcance del producto.

Otro riesgo identificado es la dificultad de adopción por parte de instituciones financieras pequeñas. Estas instituciones pueden carecer de recursos técnicos o financieros para implementar la solución. Para abordar este riesgo, se sugiere ofrecer incentivos financieros, como descuentos iniciales o periodos de prueba extendidos, que faciliten la adopción. Asimismo, se propone diseñar un modelo de implementación escalable que permita a estas instituciones integrar gradualmente la solución según sus capacidades.

La resistencia al cambio por parte de los clientes finales también representa un riesgo considerable. Los usuarios pueden mostrar escepticismo hacia nuevas soluciones de seguridad digital debido a la falta de conocimiento o confianza. Para mitigar este

riesgo, es fundamental implementar campañas educativas que informen sobre los beneficios y la facilidad de uso de la solución. Además, utilizar testimonios de usuarios iniciales y casos de éxito puede ser una estrategia efectiva para generar confianza.

Por último, el impacto regulatorio y normativo es otro factor para considerar. Cambios en las regulaciones financieras o de telecomunicaciones podrían afectar la operación del proyecto. Para mitigar este riesgo, se propone monitorear continuamente los cambios regulatorios para garantizar el cumplimiento normativo. Además, establecer un equipo dedicado a la gestión de riesgos regulatorios y la actualización de procesos según las normativas vigentes podría fortalecer la sostenibilidad del proyecto.

La implementación de estas estrategias de mitigación permite abordar los principales riesgos identificados y garantizar un camino más sólido hacia la adopción y sostenibilidad del proyecto en el mercado competitivo.

2.1.3.6.Rivalidad de competidores

Como mencionado al inicio del capítulo, el mercado peruano está compuesto por una variedad de competidores que ofrecen soluciones de seguridad digital desde diferentes ángulos.

Por un lado, las entidades financieras han desarrollado aplicaciones móviles que permiten a los usuarios realizar ciertas acciones de seguridad. Estas aplicaciones son una competencia directa porque ya están integradas en el ecosistema bancario y gozan de cierto nivel de confianza de los usuarios. La capacidad de los bancos para mejorar y actualizar estas aplicaciones continuamente incrementa su competitividad.

Por otro lado, la muy reciente introducción de la solución 1820 por ASBANC, que permite a los usuarios bloquear cuentas bancarias de cualquier banco a través de un número único, representa un fuerte competidor debido a su accesibilidad. Este puede ser

un gran competidor, sin embargo, se diferencia de la propuesta de valor de nuestro servicio, el cual abarcará una problemática más completa.

En cuanto a los operadores de telecomunicaciones, ofrecen servicios de bloqueo remoto de SIM y dispositivos. Su control sobre la infraestructura de telecomunicaciones y su capacidad para ofrecer soluciones a gran escala les otorgan una posición fuerte. Igualmente, a pesar de que nuestra propuesta engloba la solución de estos operadores, contar con alianzas estratégicas con estos operadores será muy importante para nuestro proyecto.

A continuación, se presenta una la tabla 4 con comparativa de los principales competidores junto con nuestra propuesta.

Tabla 4. Comparativa de los principales competidores

Competidor	Propuesta de valor (Funcionalidad)	Precio	Accesibilidad	Seguridad	Segmentación de clientes
Entidades financieras	Cada EF cuenta con app que incluye mecanismos de bloqueo	Gratuito	Aplicaciones móviles, presencial	Solicita información personal	Clientes bancarios activos de cualquier nivel socioeconómico
1820 de ASBANC	Bloqueo de cuentas de cualquier banco a través de un número único	Gratuito	Teléfono	No solicita información personal	Clientes bancarios con múltiples cuentas en distintas EF
Teleoperadores	Bloqueo de SIM y parcialmente de dispositivos móviles	Gratuito	Teléfono, presencial	Solicita información personal	Usuarios de tecnología móvil
Segurazo	Solución integral: bloqueo de cuentas, SIM y dispositivos, así como otras acciones como denuncias policiales	Gratuito	Cualquier dispositivo con acceso a web	No solicita información personal	Usuarios bancarios y tecnológicos de todos los niveles socioeconómicos.

Fuente: Elaboración Propia

Se observa que la principal oportunidad para diferenciar el proyecto radica en su enfoque integral, abordando múltiples necesidades de seguridad en un solo

servicio. Mientras los competidores se centran en soluciones y segmentos específicos, nuestra propuesta cubrirá la protección de cuentas bancarias, dispositivos y datos, con mecanismos intuitivos y tiempos de respuesta rápidos. Además, ofrecer un posible servicio Premium permitirá ampliar aún más nuestra propuesta de valor, esto se verá en secciones posteriores.

Se concluye pues que, dado el alto nivel de competencia, las alianzas estratégicas con las entidades financieras y operadores de telecomunicaciones serán clave. Es por esto por lo que nuestro proyecto buscará formar alianzas con estos actores.

2.1.4. **Relación entre las estrategias del modelo de negocio y el análisis competitivo**

Las estrategias definidas en el modelo de negocio están diseñadas para mitigar los riesgos y aprovechar las oportunidades identificadas en el análisis competitivo basado en las cinco fuerzas de Porter. A continuación, se describe cómo cada estrategia responde a estas dinámicas del mercado:

Para mitigar el poder de negociación de los proveedores de tecnología y telecomunicaciones, se plantea una estrategia que prioriza la colaboración a través de contratos a largo plazo y acuerdos estratégicos. Esto permite garantizar la estabilidad en los servicios esenciales y minimizar el impacto de posibles fluctuaciones en costos.

Frente al poder de negociación de los clientes, se propone enfocar los esfuerzos en entregar una solución altamente intuitiva y accesible, lo que reduce la sensibilidad al precio y fortalece la fidelidad de los usuarios hacia las soluciones ofrecidas.

Aprovechando las altas barreras de entrada del sector, la estrategia incluye inversión en desarrollo tecnológico continuo y el cumplimiento riguroso de las normativas del mercado. Esto no solo dificulta la entrada de nuevos competidores, sino que fortalece la posición de mercado frente a posibles amenazas externas.

Las estrategias de diferenciación buscan superar las alternativas existentes, enfocándose en la entrega de un valor adicional que los productos sustitutos actuales no proporcionan. Esto incluye simplicidad en la implementación, disponibilidad de recursos integrados y tiempos de respuesta mejorados.

En un entorno con competidores consolidados, las estrategias de alianzas estratégicas con actores relevantes en el mercado permiten establecer un posicionamiento competitivo único. Esto, combinado con la optimización de los costos operativos, asegura una ventaja sostenible frente a los competidores existentes.

A continuación, se relacionarán estrategias de nuestro modelo de negocio con los riesgos identificados en el presente capítulo (Tabla 5).

Tabla 5. Estrategias para la mitigación de riesgos

Riesgo identificado	Estrategia	Justificación
Alta rivalidad con competidores como el “1820”	Diferenciación basada en un enfoque integral: bloqueo de cuentas, SIM y dispositivos, denuncias y educación en seguridad digital	Mientras los competidores ofrecen soluciones parciales, nuestro servicio integrará todas las medidas en un solo lugar, lo que le dará una ventaja competitiva.
Dependencia de la colaboración con entidades financieras y operadoras	Alianzas estratégicas con entidades financieras	La propuesta de valor de nuestro servicio se fortalece con la integración directa con estos actores, garantizando una solución confiable.
Baja adopción por parte de usuarios finales	Campañas de concienciación y marketing educativo	La falta de conocimiento sobre seguridad digital puede ser una barrera para la adopción, por lo que se implementarán estrategias de comunicación para informar a los usuarios sobre la importancia de nuestro servicio.
Amenaza de nuevos competidores en el mercado de seguridad digital	Posicionamiento temprano y escalabilidad del modelo	Lanzamiento para establecer una base de usuarios sólida y permitir la expansión del servicio con nuevas funcionalidades antes de que surjan competidores similares.
Dependencia tecnológica de proveedores externos	Diversificación de proveedores y desarrollo tecnológico interno	Para reducir el riesgo de fallas o costos elevados, se trabajará con múltiples proveedores de tecnología y desarrollará internamente funciones clave.

Fuente: Elaboración Propia

Ahora, se relacionarán estrategias de nuestro modelo de negocio con las oportunidades identificadas en el presente capítulo (Tabla 6).

Tabla 6. Relación de estrategias con oportunidades

Oportunidad identificada	Estrategia	Justificación
Alta digitalización en Perú y aumento del uso de banca móvil	Integración con entidades financieras	La adopción de banca móvil permite que nuestro servicio sea un complemento natural a los servicios financieros, facilitando su aceptación por parte de los usuarios.
Necesidad de una solución centralizada y automatizada	Centralización del bloqueo de servicios financieros y SIM	Ofrecer un proceso rápido y sencillo para que los usuarios protejan sus activos tras un robo es clave para nuestra diferenciación.
Regulaciones que favorecen la seguridad digital y la protección del usuario	Cumplimiento normativo y colaboración con organismos como SBS, OSIPTEL e Indecopi	Cumplir con las regulaciones no solo garantiza la viabilidad del proyecto, sino que también fortalece la confianza de los usuarios y entidades financieras en la solución.
Interés creciente de los usuarios por la seguridad digital	Segmentación de usuarios y marketing dirigido	Dirigir estrategias de comunicación y publicidad a los segmentos identificados permitirá una mejor adopción del servicio.
Crecimiento del fraude digital y robo de dispositivos	Servicio Freemium con posible modelo de suscripción para usuarios avanzados	La creciente necesidad de seguridad digital permitirá ofrecer un servicio gratuito con funciones esenciales y posibles planes premium con características adicionales como asistencia prioritaria.

Fuente: Elaboración Propia

El éxito de nuestro servicio dependerá de su capacidad para diferenciarse, generar confianza y posicionarse rápidamente en el mercado. Las estrategias del modelo de negocio nos ayudarán a abordar los desafíos identificados, logrando el objetivo de convertirnos en un estándar de seguridad digital en Perú.

2.1.5. Priorización de oportunidades

A continuación, se realiza una priorización basada en viabilidad técnica y viabilidad financiera.

Oportunidades de alta prioridad

Las siguientes oportunidades han sido clasificadas como de alta prioridad debido a su combinación de viabilidad y alto impacto en la adopción y diferenciación de nuestro servicio en el mercado. Estas oportunidades pueden garantizar un impacto inmediato en la adopción del servicio.

- **Integración con entidades financieras**

  La integración con entidades financieras es un pilar fundamental para la funcionalidad

de nuestro servicio. Técnicamente, es viable mediante acuerdos de colaboración. Además, desde una perspectiva financiera, la integración con entidades financieras puede permitir el acceso a inversión y financiamiento para el desarrollo de la plataforma.

- **Desarrollo de herramientas centralizadas para seguridad digital**

  La capacidad de ayudar a los usuarios a bloquear cuentas bancarias, SIM y dispositivos móviles desde un solo lugar representa el mayor diferencial de nuestro servicio. Aunque técnicamente viable, su implementación requiere alianzas estratégicas con entidades financieras, lo que implica negociaciones y acuerdos comerciales.

- **Campañas de concienciación y marketing educativo**

  La falta de conocimiento sobre seguridad digital es una barrera para la adopción de Segurazo. Desarrollar contenidos educativos y campañas de marketing digital permitirá generar confianza en los usuarios. Esta estrategia es viable tanto técnica como financieramente, ya que su implementación tiene costos relativamente bajos y puede lograrse con herramientas existentes.

Oportunidades de baja prioridad

Estas oportunidades, aunque atractivas, presentan bajas probabilidades de implementación en las primeras etapas debido a sus costos elevados o requerimientos tecnológicos avanzados. Estas oportunidades pueden explorarse en futuras fases del proyecto, cuando Segurazo haya demostrado su éxito y cuente con más recursos para expandirse.

- **Implementación avanzada de inteligencia artificial**

  La incorporación avanzada y más compleja de IA para analizar y predecir fraudes financieros podría ser una gran ventaja en el futuro. Sin embargo, su desarrollo

implica costos altos en infraestructura, recopilación de datos y entrenamiento de modelos de aprendizaje automático.

- **Expansión internacional en mercados similares**

  Aunque el robo de dispositivos y fraudes financieros es un problema global, Segurazo debe consolidarse primero en Perú antes de considerar su expansión a otros mercados.

2.1.6. Diferenciación y sostenibilidad de la propuesta

En el mercado peruano existen opciones parciales para enfrentar el robo de dispositivos móviles, tales como el bloqueo de líneas telefónicas, el rastreo del equipo o el resguardo de contraseñas bancarias. Sin embargo, la mayoría carece de un enfoque integral que permita reaccionar de manera coordinada y minimizar las oportunidades de fraude financiero. La propuesta descrita en este documento se distingue al vincular múltiples actores (bancos, operadoras, entes reguladores) mediante una plataforma unificada, escalable y alineada con prácticas de sostenibilidad y educación en seguridad digital.

En la Tabla 7 se detallan los principales aspectos que diferencian esta propuesta de los sustitutos existentes. Se consideran, entre otros, la cobertura multientidad, la actualización continua y la inclusión de orientación legal, factores que apuntalan su valor agregado y su contribución a la sostenibilidad en el sector.

Tabla 7. Relación de estrategias con oportunidades

Aspecto de Análisis	Productos Sustitutos	Propuesta	Valor Agregado y Sostenibilidad
Alcance de Protección	Bloqueo parcial de línea	Bloqueo simultáneo (línea, cuentas y guía de denuncia)	Minimiza la ventana de tiempo para el fraude y fortalece la seguridad
Centralización de Procedimientos	Procesos dispersos	Plataforma unificada con flujo secuencial	Reduce la complejidad operativa y el riesgo de errores
Actualización de Datos	Frecuencia irregular	Conexión continua con instituciones y operadoras	Asegura protocolos vigentes, aumentando la confianza del usuario
Soporte Legal y Educativo	Escaso o nulo	Orientación para denuncia y tutoriales de seguridad	Fomenta una cultura preventiva y la

			formalización de reclamos
Visión de Sostenibilidad	Limitada o no declarada	Alineada con la meta 16.4 de los ODS y mayor eficiencia	Reduce la huella de trámites, evita flujos ilícitos y fortalece la resiliencia digital

Fuente: Elaboración propia

A diferencia de las herramientas tradicionales, que suelen enfocarse de manera fragmentada en el robo de un dispositivo (por ejemplo, solo el bloqueo de la tarjeta o de la línea), esta propuesta provee un abordaje inmediato y multidimensional. No solo facilita la anulación de accesos bancarios y de telefonía, sino que además promueve la educación preventiva, al incluir recomendaciones y guías para un uso responsable y seguro de los dispositivos.

Desde una perspectiva sistémica, este planteamiento beneficia tanto a los usuarios como a las organizaciones:

- **Mayor confianza en la banca y la digitalización:** Al centralizar la respuesta a través de un solo canal, las entidades financieras y los operadores de telecomunicaciones pueden atender eficazmente los incidentes, reduciendo el temor a transacciones en línea o las pérdidas por fraude.
- **Contribución a la sostenibilidad:** El enfoque basado en actualizaciones continuas y prácticas colaborativas disminuye la duplicidad de esfuerzos y limita la canalización de fondos sustraídos hacia actividades ilícitas, en sintonía con la meta 16.4 de los Objetivos de Desarrollo Sostenible (ODS).
- **Empoderamiento del usuario:** Incluir tutoriales y buenas prácticas fortalece el papel activo del cliente en su propia protección, promoviendo una reducción progresiva de nuevos casos de fraude.

En definitiva, la principal ventaja competitiva de esta propuesta radica en su capacidad de aunar los esfuerzos de bancos, operadoras y organismos reguladores bajo un

esquema flexible y orientado a la mejora continua. Este enfoque garantiza que la plataforma se mantenga vigente frente a nuevas modalidades de fraude, brindando una experiencia sólida y confiable a medida que evoluciona el entorno de la seguridad digital.

2.1.7. Matriz comparativa de funcionalidades

A continuación, se presenta una matriz comparativa de funcionalidades integrada, que resume la propuesta de valor de Segurazo frente a productos sustitutos y competidores directos, destacando las funciones clave (Tabla 8).

Tabla 8. Relación de estrategias con oportunidades

Criterio / Solución	Teleoperadores	Software de ciberseguridad	Aseguradoras	Entidades Financieras	1820 ASBANC	Segurazo (guía para usuarios)
Bloqueo de celular	Sí	Sí	No	No	No	Sí (integral por sistema operativo)
Bloqueo de cuenta bancaria	No	No	No	Sí (app propia por banco)	Sí (multibanco por llamada)	Sí (todos los bancos, desde un solo flujo)
Bloqueo de SIM, chip	Sí	No	No	No	No	Sí (todas las operadoras)
Devolución de dinero	No	No	Sí	Sí	No	No (no directamente)
Orientación legal, denuncias	No	No	No	No	No	Sí (tutoriales, denuncias PNP, marco legal)
Solicita datos personales	Sí	Sí	Sí	Sí	No	No
Accesibilidad	Teléfono / Presencial	Web / App con suscripción	Burocrática	App móvil y presencial	Teléfono	Cualquier dispositivo con internet

Fuente: Elaboración propia

Segurazo se posiciona como una propuesta integral y diferenciada, al centralizar múltiples acciones críticas (bloqueo, guía legal, accesibilidad universal) sin solicitar datos personales y con enfoque en seguridad digital preventiva.

Capítulo III. Investigación del usuario

3.1. Perfil del usuario

Este capítulo presenta los perfiles de los usuarios afectados por el fraude financiero derivado del robo de dispositivos móviles. Para construir estos perfiles, se realizaron entrevistas a 30 personas de diferentes géneros, con edades comprendidas entre los 18 y 65 años. Estas entrevistas exploraron sus experiencias en el uso de dispositivos móviles para transacciones financieras, desde la configuración inicial y el uso cotidiano hasta las acciones tomadas en caso de robo o pérdida del dispositivo.

El análisis permitió identificar las emociones positivas y negativas asociadas con estas experiencias, profundizando en sus frustraciones, alegrías, tareas y necesidades. Estas actividades facilitaron el desarrollo de perfiles que reflejan una representación detallada de los usuarios, destacando los eventos que generaron satisfacción y aquellos que ocasionaron situaciones de dolor.

A continuación, se describen tres perfiles representativos desarrollados a partir de entrevistas y casos reales. Estos perfiles abarcan diferentes contextos, edades y ocupaciones, con el objetivo de comprender mejor las necesidades, frustraciones y expectativas de los usuarios. Asimismo, los lienzos metausuarios, integrados en esta sección, reflejan las principales características de cada perfil, fortaleciendo el análisis de cómo las soluciones propuestas pueden abordar sus problemáticas específicas y mejorar la experiencia del usuario.

Perfil 1: Juan Pérez

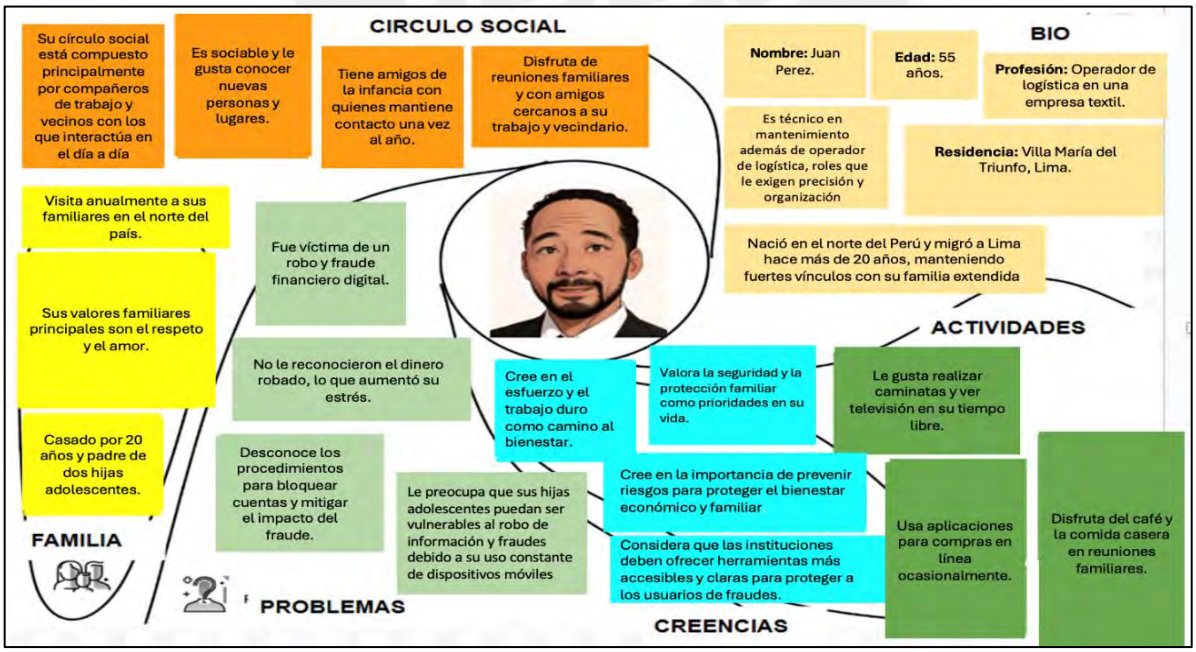
Juan Pérez, un ingeniero industrial de 55 años, trabaja como operador de logística en una empresa del sector textil, en el distrito de Villa María del Triunfo. Juan ha estado casado durante más de 20 años y tiene dos hijas en la adolescencia. Anualmente, visita a sus familiares en el norte del país, valorando mucho el tiempo que pasa con su familia y amigos

cercanos. En el ámbito social, Juan es una persona sociable que disfruta viajar y conocer nuevos lugares y personas. Le gusta reunirse con sus amigos, familiares y compañeros de trabajo, y siempre está buscando nuevas experiencias.

Sin embargo, Juan enfrenta varios desafíos. Siente que le falta tiempo para desarrollar proyectos personales debido a sus responsabilidades laborales y familiares. Además, le preocupa la inseguridad ciudadana y la seguridad de su familia. A inicios del mes de enero del presente año, Juan fue víctima de robo y fraude financiero digital, una experiencia que le causó considerable ansiedad y frustración. A pesar de sus esfuerzos, el banco no le reconoció el dinero robado, lo que aumentó su estrés y preocupación. Además, Juan no tiene claros los procedimientos de seguridad ni las implicaciones que tiene el hecho que le roben el celular.

En su vida diaria, Juan disfruta de actividades como caminatas, ver televisión y pasar tiempo con su familia. Es católico y cree firmemente en el esfuerzo y el trabajo duro como medio para alcanzar el bienestar a largo plazo, valores que inculca en su familia y refuerza al asistir regularmente a la iglesia (Figura 11: Lienzo metausuario de Juan Perez).

Figura 11. Lienzo metausuario de Juan Perez



Fuente: Elaboración Propia

Perfil 2: María Fernanda Ríos

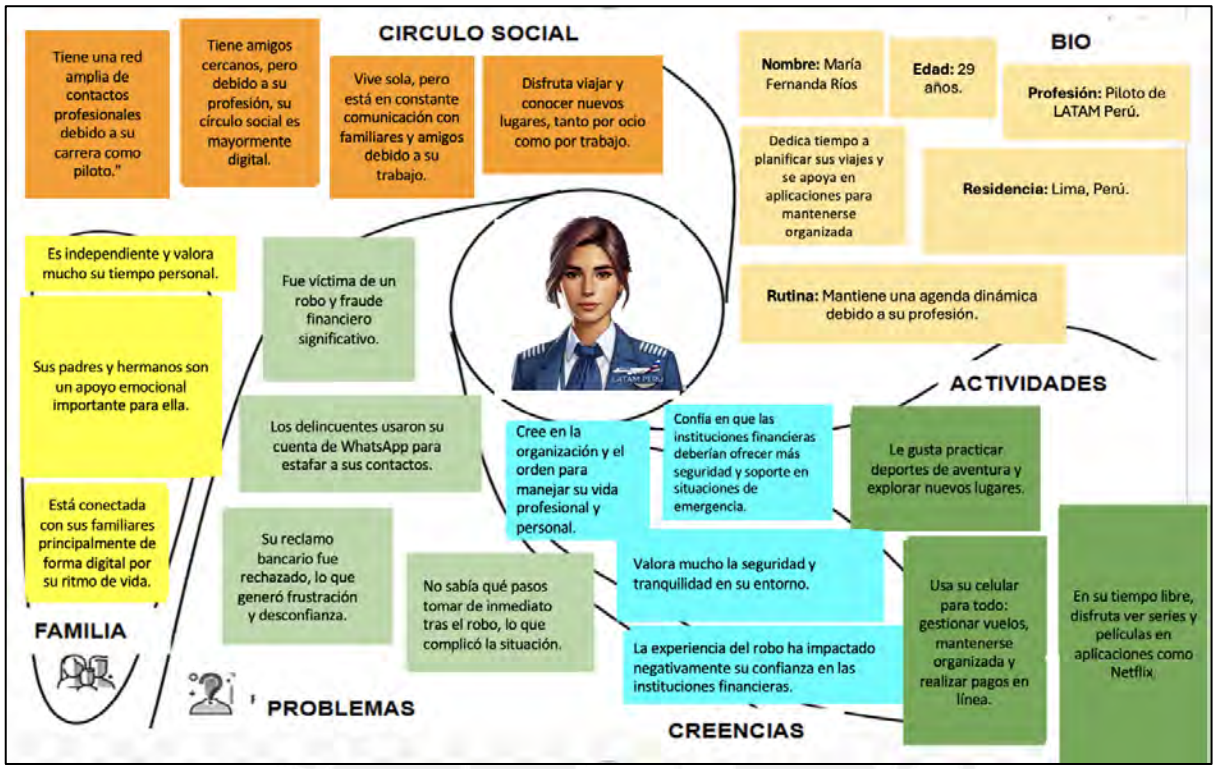
María Fernanda Ríos, una piloto de LATAM Perú de 29 años, trabaja en un entorno dinámico que exige mantenerse conectada a través de su celular casi todo el tiempo. Reside en Lima, vive sola y utiliza su celular como herramienta principal para gestionar itinerarios de vuelo, realizar pagos y compras en línea, y comunicarse con familiares y amigos. En su tiempo libre, María Fernanda disfruta desconectarse del estrés laboral viendo series y películas en aplicaciones como Netflix.

Un día, María Fernanda fue víctima del robo de su celular, una experiencia traumática debido a la dependencia que tiene de este dispositivo. Su reacción inicial fue de confusión, bloqueando su línea telefónica con la ayuda del celular de una amiga. Sin embargo, esa misma noche descubrió que los delincuentes habían tomado el control de su cuenta de WhatsApp, enviando mensajes a sus contactos para intentar estafarlos.

El impacto más grave fue descubrir dos transacciones no autorizadas en sus cuentas bancarias: una transferencia de S/9,900 y una disposición en efectivo de S/2,000. A pesar de presentar un reclamo formal al banco, este fue rechazado, dejándola frustrada y vulnerable. Ahora María Fernanda revisa constantemente sus movimientos bancarios y busca información sobre ciberseguridad, aunque considera que las herramientas actuales no son suficientes para prevenir futuros incidentes.

Como se muestra en la Figura 12: Lienzo meta usuario de María Fernanda Ríos, sus principales frustraciones incluyen la falta de conocimiento sobre qué hacer en el momento del robo y la limitada respuesta de las instituciones financieras para gestionar el fraude.

Figura 12. Lienzo metausuario de María Fernanda Ríos



Fuente: Elaboración Propia

Perfil 3: Carlos Alberto Gómez

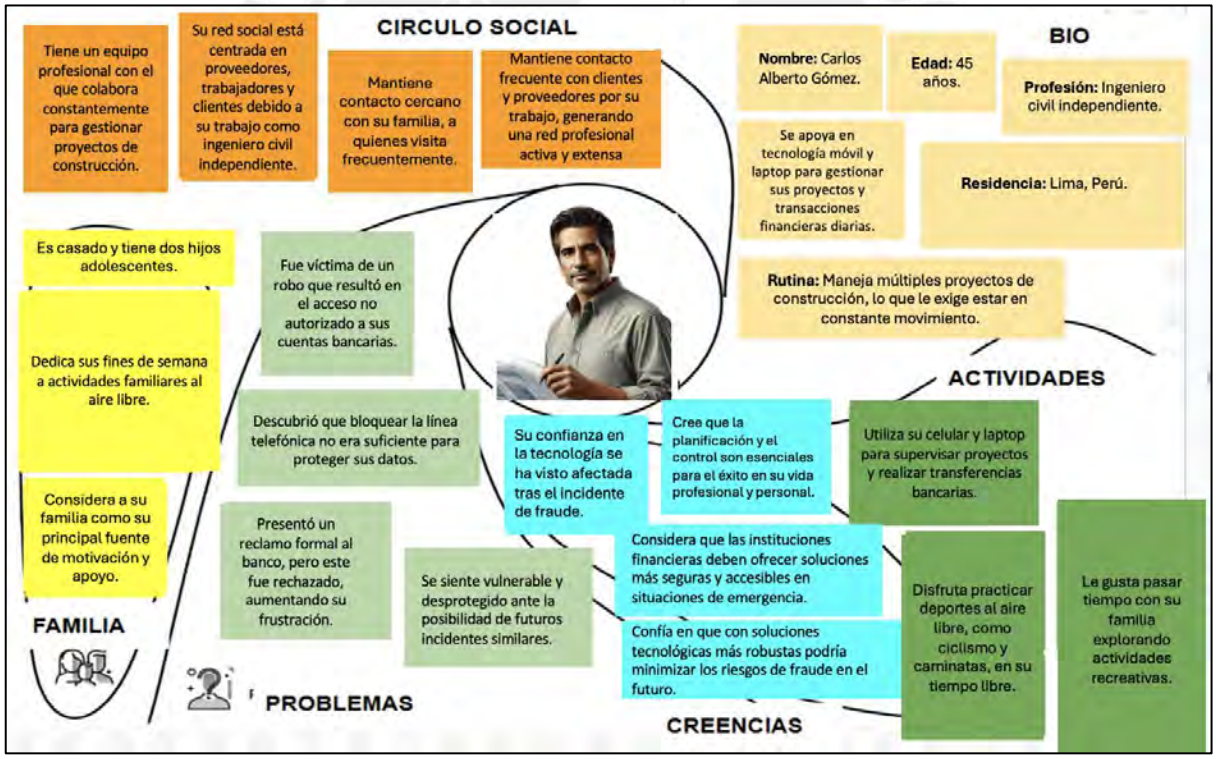
Carlos Alberto Gómez, un ingeniero civil independiente de 45 años, vive en Lima y maneja múltiples proyectos de construcción. Debido a su ocupación, su celular es una herramienta esencial para coordinar con proveedores, realizar transferencias bancarias y gestionar actividades relacionadas con sus proyectos. Además, Carlos disfruta practicar deportes al aire libre y pasar tiempo con su familia los fines de semana.

Un día, mientras esperaba en su auto en un semáforo, Carlos fue víctima de un robo. Los delincuentes rompieron la ventana de su vehículo y sustrajeron su maletín, que contenía su celular y documentos personales. Aunque logró bloquear la línea telefónica desde el celular de un transeúnte, descubrió al llegar a casa que los delincuentes habían realizado varias transacciones no autorizadas: una transferencia de S/5,000 y compras en línea por un total de S/3,800.

A pesar de presentar un reclamo formal al banco con todas las evidencias, su solicitud fue rechazada, lo que generó en Carlos una profunda frustración. Este incidente lo llevó a cambiar sus hábitos digitales, como evitar guardar credenciales en su celular y revisar sus movimientos bancarios con más frecuencia. Sin embargo, sigue desconfiando de las instituciones financieras y considera que no cuentan con herramientas efectivas para proteger a sus clientes.

Como se aprecia en la Figura 13: Lienzo metausuario de Carlos Alberto Gómez, las principales frustraciones incluyen la falta de respuesta por parte del banco y la rapidez con la que los delincuentes actuaron, lo que evidencia la necesidad de soluciones más ágiles y centralizadas para prevenir el fraude.

Figura 13. Lienzo metausuario de Carlos Alberto Gómez



Fuente: Elaboración Propia

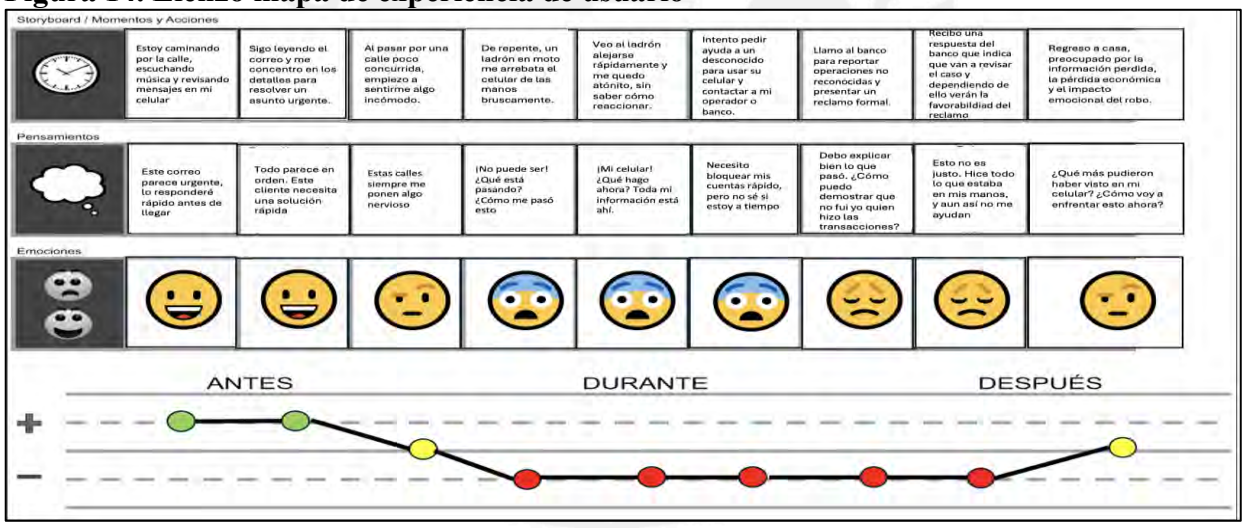
3.2.Mapa de experiencia de usuario

A través del Mapa de Experiencia de Usuario (Figura 14: Lienzo – Mapa de Experiencia de Usuario), se puede comprender con mayor profundidad las expectativas,

emociones y necesidades de los usuarios a lo largo de su interacción con los eventos de un robo de celular. Este análisis permite detallar las actividades y pensamientos que experimenta una persona en las etapas antes, durante y después del robo, destacando los puntos críticos de interacción y riesgo, así como la urgencia de implementar medidas efectivas para proteger su información personal y cuentas bancarias.

El perfil de usuario identificado en el lienzo detalla los momentos clave que vive una víctima desde el uso cotidiano de su dispositivo hasta el proceso para bloquear sus cuentas bancarias. A continuación, se describe el mapa de experiencia, enriquecido con un análisis más profundo de los momentos de mayor dolor, basado en entrevistas realizadas y casos reales.

Figura 14. Lienzo mapa de experiencia de usuario



Fuente: Elaboración Propia

Antes del robo, la persona realiza actividades diarias comunes, como escuchar música, navegar por internet, comunicarse con familiares o trabajar, utilizando su celular como herramienta principal. Durante este tiempo, su atención está enfocada en sus tareas, sin anticipar un robo. Pensamientos como: "Estoy iniciando un buen día" o "Esta llamada parece importante" reflejan su tranquilidad o concentración.

Aunque no hay una percepción inmediata de peligro, en algunos casos puede surgir una preocupación implícita por la seguridad del entorno, especialmente en calles concurridas

o al transitar por áreas que considera inseguras. Este estado emocional varía entre calma y ligera alerta, dependiendo del contexto.

Durante el robo, El momento crítico ocurre cuando el ladrón actúa. La persona puede no percatarse de inmediato del robo, ya que este suele ser rápido y aprovechando un instante de distracción. Los pensamientos se tornan caóticos y giran en torno al evento: "¿Qué está pasando?", "¿Cómo sucedió esto?" y "¿Qué debo hacer ahora?".

Este es el momento de mayor dolor, donde la víctima toma plena conciencia de la pérdida del dispositivo y enfrenta el riesgo potencial de fraude financiero. Las emociones que experimenta abarcan desde pánico y confusión hasta impotencia, generando una sensación de vulnerabilidad extrema. A esto se suma el impacto emocional de perder información personal valiosa, como correos importantes, fotografías significativas, archivos laborales o educativos, y contactos esenciales.

En este contexto, indicadores clave como los tiempos de reacción promedio de los usuarios ante robos (segundos o minutos) y el porcentaje de robos reportados de inmediato adquieren relevancia. Por ejemplo, se puede analizar cuántos usuarios logran bloquear sus dispositivos o tomar medidas de seguridad dentro de los primeros minutos tras el incidente. Asimismo, entender la frecuencia con la que las víctimas buscan apoyo puede ayudar a identificar brechas en los procesos de respuesta.

Después del robo, la persona entra en una fase donde la acción inmediata se combina con un estado de reflexión y, en algunos casos, bloqueo emocional. Los primeros pasos incluyen intentos para bloquear el celular, cambiar contraseñas y contactar al proveedor de servicios para desactivar la línea. Sin embargo, la urgencia de actuar se ve afectada por la desorientación y el estrés, lo que puede llevar a la víctima a sentirse paralizada al inicio, sin saber por dónde empezar.

Durante este tiempo, un problema adicional surge cuando los delincuentes utilizan el celular robado para acceder a aplicaciones como WhatsApp, suplantando la identidad de la víctima para estafar a sus contactos. Esto genera una profunda sensación de vulnerabilidad y culpa, ya que la víctima ve cómo su información personal es utilizada para perjudicar a sus amigos o familiares. Además, el acceso de los delincuentes a datos sensibles despierta temores de extorsiones u otros delitos, amplificando la ansiedad.

Un momento de gran impacto emocional ocurre cuando la víctima recibe la notificación de su banco sobre la resolución de sus reclamos. En muchos casos, el banco comunica que las transacciones fraudulentas no serán devueltas, argumentando que se realizaron con credenciales válidas o desde dispositivos previamente autenticados. Esta noticia profundiza el sentimiento de frustración e impotencia, generando pensamientos como: "¿Por qué no me creen?", "¿Cómo puedo demostrar que fui víctima?" y "No tengo los recursos para enfrentar esta pérdida".

Este desenlace genera enojo y desconfianza hacia las instituciones financieras, aumentando la percepción de desamparo. La combinación de la pérdida económica con la falta de apoyo institucional deja una huella emocional profunda.

Indicadores clave en esta etapa incluyen el tiempo promedio para tomar medidas como bloquear el celular y el porcentaje de usuarios que logran proteger sus cuentas y datos con éxito. También es relevante medir el nivel de satisfacción con el soporte brindado por bancos o empresas de telecomunicaciones, ya que esto influye directamente en la percepción de la experiencia post-robo. Por ejemplo, una métrica relevante sería la proporción de víctimas que resuelve sus problemas sin pérdida de datos ni dinero.

A largo plazo, las emociones oscilan entre frustración por la pérdida de información y resignación al aceptar lo sucedido. Aunque algunas personas experimentan alivio si logran

bloquear sus cuentas rápidamente, muchas ven afectada su confianza en las herramientas digitales y los sistemas de seguridad. Además, el temor de enfrentar nuevos riesgos derivados del acceso de los delincuentes a su información personal genera una vigilancia constante en su vida digital. En este punto es importante considerar el índice de retención de usuarios en servicios afectados tras el incidente, como aplicaciones financieras o redes sociales. Por ejemplo, una métrica podría mostrar que el 40% de las víctimas disminuyen su uso de aplicaciones financieras tras un robo, reflejando la necesidad de reforzar la percepción de seguridad digital.

Este análisis resalta la necesidad de soluciones que protejan los datos de forma inmediata y brinden soporte continuo para gestionar el proceso de recuperación. Al abordar las vulnerabilidades relacionadas con la pérdida del celular, se puede crear un entorno más seguro para los usuarios y minimizar el impacto emocional y financiero de estos incidentes.

3.3. Identificación de la necesidad a resolver para el usuario

El análisis de las entrevistas realizadas y del mapa de experiencia del usuario ha revelado una necesidad crítica: la protección inmediata y efectiva de datos sensibles y cuentas bancarias tras el robo o pérdida de un dispositivo móvil. En un contexto donde los dispositivos móviles se han convertido en herramientas esenciales para realizar transacciones financieras y almacenar información personal, la vulnerabilidad ante fraudes aumenta significativamente si no se cuentan con mecanismos de seguridad adecuados y se desconocen los procesos para protegerse en tales situaciones. Los usuarios expresaron una profunda preocupación por la falta de recursos rápidos y efectivos para bloquear sus cuentas en emergencias, lo que subraya la importancia de ofrecer soluciones tecnológicas que mitiguen este riesgo.

Los celulares se han convertido en una extensión de nuestras vidas diarias. En ellos almacenamos información personal, como correos electrónicos, fotografías, contactos,

documentos y credenciales financieras, que, en manos de personas malintencionadas, pueden ser utilizadas para cometer fraudes, extorsiones u otros delitos. Esto no solo afecta el patrimonio económico del usuario, sino que también genera un impacto emocional significativo.

Además, se identificó la necesidad de orientación en tiempo real para proteger la información personal y financiera. Una funcionalidad clave sería la capacidad de ayudar al usuario a contactar con su entidad financiera para proceder con el bloqueo remoto de todas las tarjetas asociadas al dispositivo robado. Esta acción es crucial, ya que reduce la ventana de tiempo en la que un delincuente podría acceder a los fondos del usuario. Por ejemplo, si un usuario como Juan, de 55 años, sufre el robo de su celular mientras se desplaza en transporte público, tener acceso inmediato a instrucciones para bloquear todas sus tarjetas bancarias con un simple toque en la pantalla podría prevenir transacciones fraudulentas.

Además de facilitar la comunicación con las entidades financieras, es esencial proporcionar una conexión directa con las operadoras telefónicas, permitiendo al usuario desactivar su línea y bloquear su dispositivo de manera inmediata. Esto es fundamental para evitar que los delincuentes utilicen el dispositivo robado para acceder a más información sensible o realizar llamadas fraudulentas.

Otro aspecto destacado es la necesidad de ofrecer asesoramiento en tiempo real. Esto incluye guiar al usuario a través de los pasos necesarios para asegurar que los datos sensibles de su dispositivo no sean accesibles a personas no autorizadas. Se podrían proporcionar recomendaciones para configuraciones de bloqueo de Android/iPhone, borrado de datos y orientación sobre cómo presentar una denuncia policial. Esta funcionalidad aseguraría que todos los aspectos legales y de seguridad sean cubiertos de manera eficiente. En el caso de Juan, después de bloquear sus tarjetas y su línea telefónica, sería aconsejable que protegiera

su dispositivo mediante el borrado seguro y recibiera instrucciones detalladas para presentar una denuncia policial de manera rápida y segura.

A partir de los hallazgos presentados, se concluye que el mayor dolor identificado en los usuarios es la sensación de vulnerabilidad extrema tras un robo, especialmente en el momento en que se dan cuenta de que su información personal y financiera está expuesta. Esta vulnerabilidad, agravada por la lentitud o falta de claridad en los procesos de bloqueo y reclamos, genera frustración, ansiedad y desconfianza hacia las instituciones financieras. Por ello, la necesidad prioritaria es contar con una solución que ofrezca una respuesta inmediata, efectiva y centralizada para bloquear cuentas, dispositivos y datos personales.

Además, se resalta que la orientación en tiempo real y la posibilidad de guiar a los usuarios en los pasos necesarios para protegerse contribuirían a mitigar el impacto financiero del fraude y reducirían el desgaste emocional que enfrentan en este tipo de incidentes. Este enfoque permite alinear las decisiones de diseño de la solución directamente con las expectativas y experiencias de los usuarios, priorizando la optimización de su seguridad y bienestar.

Para reforzar las necesidades detectadas, presentamos ejemplos concretos basados en las entrevistas realizadas. Estas historias destacan las dificultades que enfrentan los usuarios tras el robo o pérdida de sus dispositivos móviles y subrayan la importancia de una solución tecnológica más efectiva y centralizada que lo que actualmente ofrece el mercado.

- **Caso 1: Karen, 31 años, enfermera**

  Karen relató cómo fue víctima del robo de su celular mientras regresaba a casa después de su turno nocturno:

  "Me lo arrebataron en un segundo, y lo único que pensaba era en las fotos de mi familia y mi aplicación del banco. No sabía a quién llamar ni qué hacer primero".

Su testimonio demuestra la necesidad de un sistema que facilite la acción inmediata para proteger tanto información personal como financiera, especialmente en situaciones de estrés.

- **Caso 2: Nicole, 25 años, estudiante**

  Nicole explicó su frustración después de perder su celular en un café:

  "Tardé mucho tiempo buscando en internet cómo bloquear mi línea telefónica. Sentía que cada minuto que pasaba era una oportunidad para que alguien usara mi información".

  Su experiencia evidencia la falta de orientación clara y accesible, una brecha que podría resolverse con una aplicación que proporcione pasos detallados y personalizados en tiempo real.

Los testimonios de las entrevistas revelan patrones comunes: la sensación de vulnerabilidad, la falta de información clara y la frustración al intentar bloquear tarjetas, líneas y dispositivos.

Revisión con métricas detalladas - Perfil del usuario

Para comprender el impacto del fraude financiero tras el robo de dispositivos móviles, se realizaron entrevistas a 30 personas entre 18 y 65 años. La información recopilada permitió identificar patrones de comportamiento, dificultades en la reacción ante un robo y su impacto financiero y emocional.

Se identificaron los siguientes aspectos clave:

- Tiempo de reacción: Se exploró cuánto tiempo tardaron los usuarios en intentar bloquear su cuenta tras el robo de su dispositivo móvil.
- Eficacia de las acciones tomadas: Se analizó si los intentos de bloqueo fueron exitosos y qué dificultades encontraron.
- Nivel de conocimiento: Se evaluó qué tanto sabían los usuarios sobre los procedimientos adecuados de seguridad bancaria.

- Impacto financiero: Se registró cuánto dinero perdieron las víctimas y si lograron recuperarlo.
- Impacto emocional y cambios de comportamiento: Se investigó cómo la experiencia del fraude afectó su confianza en la banca digital y su uso de los servicios financieros digitales.

Estos criterios permitieron definir los datos cuantitativos de los siguientes perfiles de usuario:

1. **Juan Pérez (55 años, profesional en logística)**

- Uso del celular: 85% de sus transacciones bancarias son digitales.
- Tiempo de reacción: Intentó bloquear su línea tras 45 minutos del robo.
- Impacto del fraude: Perdió S/6,500 en transacciones fraudulentas y su reclamo fue rechazado.
- Conocimiento previo: No sabía cómo bloquear sus cuentas y dependió de un familiar para hacerlo.

2. **María Fernanda Ríos (29 años, piloto de aviación)**

- Uso del celular: 90% de sus pagos y transacciones son digitales.
- Tiempo de reacción: Bloqueó su línea en 10 minutos, pero sus cuentas bancarias en más de una hora.
- Impacto del fraude: Pérdida de S/11,900 (S/9,900 en transferencias y S/2,000 en retiros).
- Consecuencias adicionales: Suplantación de identidad en WhatsApp, causando fraudes a terceros.

3. **Carlos Alberto Gómez (45 años, ingeniero civil independiente)**

- Uso del celular: Maneja múltiples transacciones financieras diarias.
- Tiempo de reacción: No supo cómo bloquear su cuenta antes de una hora.
- Impacto del fraude: Perdió S/8,800 en transacciones no reconocidas.
- Desconfianza: Redujo su uso de banca digital en un 70% tras el incidente.

Análisis de los Puntos de Dolor con Métricas Validadas

A partir de los datos recopilados en las entrevistas, se identificaron los siguientes puntos de dolor, respaldados por información cualitativa y patrones comunes entre los afectados:

1. **Retraso en la reacción de los usuarios**

- La mayoría de los usuarios no actúa de inmediato tras el robo de su celular.
- Solo el 15% logró iniciar el proceso de bloqueo en los primeros 10 minutos.
- El 50% tardó más de una hora en reaccionar, aumentando su vulnerabilidad.
- Los testimonios indican que la falta de conocimiento sobre los procedimientos de bloqueo y la dificultad para contactar a los bancos o operadoras fueron las principales causas de retraso.

2. **Falta de conocimiento sobre seguridad financiera**

- El 75% de los entrevistados no sabía cómo bloquear su línea móvil inmediatamente.
- El 60% intentó comunicarse con familiares antes de tomar medidas efectivas.
- Los usuarios expresaron confusión sobre qué pasos seguir, dependiendo en muchos casos de información de terceros o buscando en internet en momentos de crisis. Esto generó frustración y retrasos que facilitaron el acceso de los delincuentes a sus cuentas bancarias.

3. **Baja tasa de recuperación de fondos**

- Solo el 18% de los afectados logró recuperar su dinero tras presentar un reclamo.
- En la mayoría de los casos, los bancos argumentaron que las transacciones habían sido realizadas con credenciales válidas.
- Varios entrevistados señalaron que el proceso de reclamo fue complicado, con respuestas poco claras por parte de las entidades financieras.

4. **Impacto en la confianza y hábitos digitales**

- El 63% de los entrevistados redujo el uso de banca digital tras el fraude.
- Muchos optaron por retirar dinero en efectivo en lugar de usar aplicaciones bancarias.
- El 40% dejó de realizar pagos digitales en comercios.
- El miedo a ser nuevamente víctima de fraude llevó a algunos usuarios a abandonar servicios financieros digitales, lo que podría afectar la inclusión financiera y la confianza en la digitalización del sistema bancario.

Los resultados de las entrevistas se pueden acceder desde el siguiente link del repositorio:

Apéndice A: Entrevistas

Resultados de entrevistas

3.4. **Conclusión**

El análisis presentado evidencia las profundas vulnerabilidades que enfrentan los usuarios tras el robo o pérdida de dispositivos móviles, destacando su sensación de desprotección, el estrés emocional y las dificultades para acceder a soluciones rápidas y efectivas. Estos hallazgos no solo identifican los problemas más críticos, sino que también guían el desarrollo de estrategias enfocadas en mejorar la experiencia del usuario.

En las siguientes etapas del desarrollo del producto, estos resultados permitirán diseñar soluciones alineadas con las necesidades detectadas. La conceptualización del servicio deberá centrarse en ofrecer un acceso ágil a herramientas de seguridad, interfaces intuitivas y protocolos de emergencia eficientes. Además, el diseño del Producto Mínimo Viable (PMV) incorporará funciones esenciales como bloqueos automatizados, notificaciones en tiempo real y asistencia guiada para reportes y denuncias.

La información recopilada en este capítulo servirá de base para definir las prioridades en el diseño y la implementación de las soluciones. Se debe considerar la integración de mecanismos que reduzcan el tiempo de reacción del usuario ante un robo, mejorando los tiempos de respuesta y facilitando el acceso a los procedimientos de seguridad. Asimismo, la evidencia obtenida resalta la necesidad de fortalecer la educación financiera y digital de los usuarios, lo que implica el desarrollo de campañas de concienciación y asistencia personalizada dentro del ecosistema del producto.

Otro aspecto clave en las próximas fases del desarrollo es la validación continua de las soluciones diseñadas a través de pruebas con usuarios reales, asegurando que las herramientas propuestas sean funcionales y efectivas en escenarios de emergencia. Esto permitirá iterar sobre el diseño y mejorar progresivamente las funcionalidades en función de las necesidades específicas identificadas en este estudio.

Este enfoque garantizará que el producto final responda efectivamente a las problemáticas identificadas, reduciendo el impacto financiero y emocional de los fraudes, al tiempo que refuerza la confianza en los mecanismos de seguridad digital. En los siguientes capítulos, se profundizará en la implementación de estas soluciones, asegurando que cada función propuesta esté alineada con las expectativas y comportamientos reales de los usuarios afectados por el fraude financiero derivado del robo de dispositivos móviles.

Capítulo IV. Diseño del producto o servicio

4.1. Concepción del producto o servicio

En el proceso de concepción de Segurazo, se identificaron los principales problemas en la experiencia del usuario relacionados con el riesgo de fraude financiero y la pérdida de información personal en casos de robo o extravío de dispositivos móviles. Para definir las necesidades y objetivos a alcanzar, se utilizaron herramientas de Design Thinking como el Lienzo 6x6 y la Matriz Costo-Impacto. Estas herramientas facilitaron la generación de ideas y el análisis de los resultados del prototipo ágil mediante sprints y retroalimentación de usuarios, empleando también el Lienzo Blanco de Relevancia.

Aplicación del Lienzo 6x6

El Lienzo 6x6 (Figura 15) se empleó con el objetivo principal de reducir el riesgo de fraude financiero en situaciones de robo o pérdida de dispositivos móviles y tarjetas de entidades financieras. A través de esta herramienta, se identificaron seis necesidades clave de los usuarios: protegerse en caso de robo, bloquear cuentas rápidamente, bloquear el número de teléfono, cambiar contraseñas de aplicaciones, acceder a métodos rápidos para bloquear cuentas y recibir soporte en casos de robo.

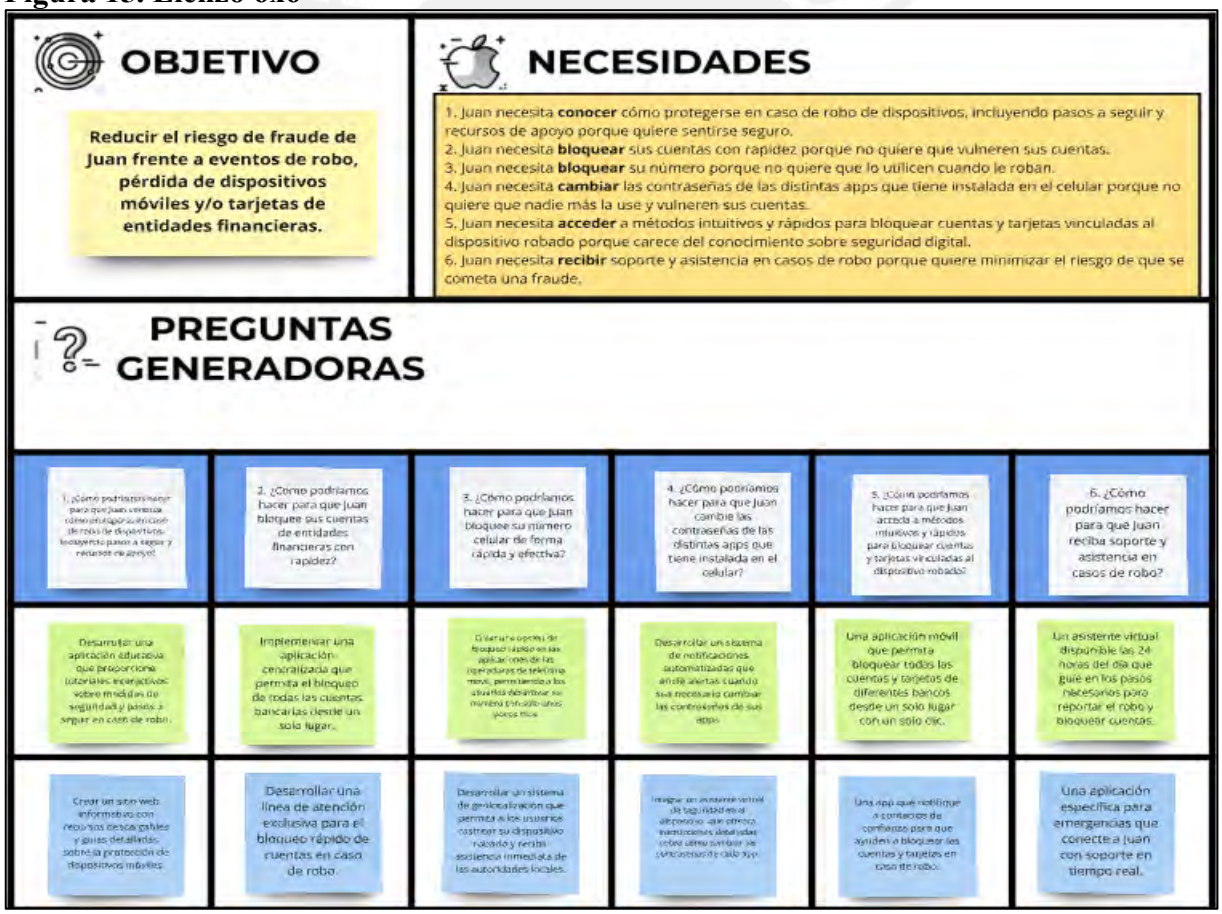
Para abordar estas necesidades, se formularon preguntas que estimularon la creatividad y permitieron generar diversas ideas. Entre las propuestas destacadas se encontró el desarrollo de un asistente virtual que permitiera el bloqueo centralizado de entidades financieras y operadores telefónicos. Esta solución facilitaría al usuario bloquear todas sus cuentas bancarias, tarjetas y líneas telefónicas desde una sola plataforma, agilizando el proceso y reduciendo el riesgo de fraude.

Otras ideas incluyeron la creación de una aplicación centralizada para el bloqueo de cuentas, un sistema de geolocalización para rastrear dispositivos robados, un asistente virtual para cambiar contraseñas, un sistema de bloqueo mediante SMS y el establecimiento de

oficinas físicas para asistencia. Sin embargo, tras evaluar cada opción, se determinó que el asistente virtual con funcionalidades integradas era la solución más efectiva y viable.

Este asistente virtual no solo permitiría el bloqueo centralizado de entidades financieras y operadores telefónicos, sino que también ofrecería acceso a tutoriales para ajustar parámetros de seguridad según el tipo de dispositivo. Además, proporcionaría información detallada para realizar la denuncia policial, orientando al usuario sobre cómo y dónde presentar una denuncia en la municipalidad correspondiente. De esta manera, la solución propuesta mejora significativamente la seguridad y reduce el riesgo de fraude financiero, al proporcionar una guía integral y personalizada en caso de robo o pérdida.

Figura 15. Lienzo 6x6



Fuente: Elaboración Propia

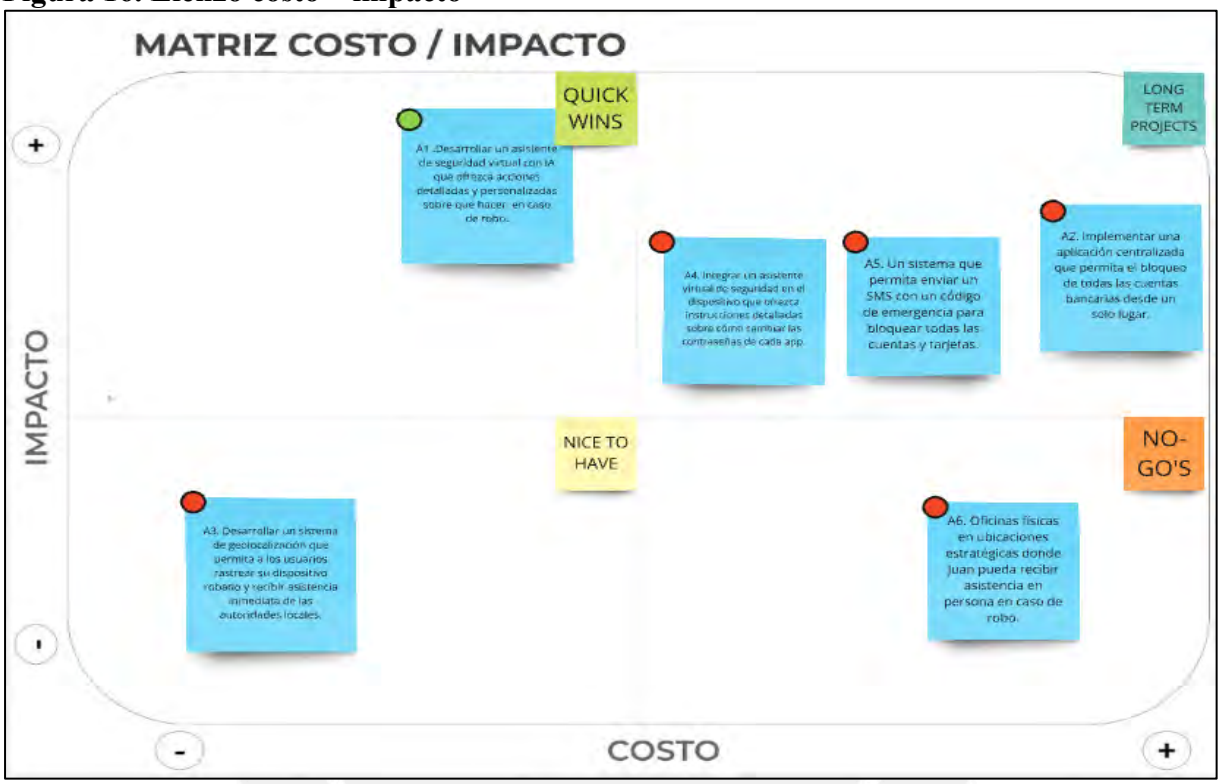
Priorización con la Matriz Costo-Impacto

Para priorizar las soluciones identificadas, se utilizó la Matriz Costo-Impacto. Las ideas fueron evaluadas según su costo de implementación y el impacto potencial en la experiencia del usuario. La implementación del asistente virtual con las funcionalidades mencionadas destacó por su alto impacto y costo moderado, convirtiéndose en la opción más viable y efectiva.

El sistema de geolocalización para rastrear dispositivos robados presentaba un impacto moderado y un costo elevado, debido a los requerimientos tecnológicos y permisos adicionales necesarios para su funcionamiento. Por otro lado, la propuesta de oficinas físicas para asistencia, aunque tendría un alto impacto en la atención al usuario, implicaba costos operativos elevados y limitaciones logísticas que la hacían menos viable en el corto plazo.

El Lienzo Costo-Impacto, mostrada en la Figura 16, permitió enfocar los esfuerzos en desarrollar el asistente virtual, optimizando la relación entre costo y beneficio, y atendiendo de manera efectiva las necesidades más críticas de los usuarios.

Figura 16. Lienzo costo – impacto



Fuente: Elaboración Propia

Iteración y Optimización con el Lienzo Blanco de Relevancia

El Lienzo Blanco de Relevancia (Figura 17), se utilizó para evaluar la eficacia del asistente virtual y detectar oportunidades de mejora. Durante este proceso, se identificaron áreas clave para optimizar la solución propuesta. Se trabajó en la integración efectiva con entidades financieras y operadores telefónicos, estableciendo acuerdos que permitieran el bloqueo centralizado y agilizaran los procedimientos, lo cual es fundamental para la funcionalidad principal de Segurazo.

Además, se actualizó y personalizó el contenido de los tutoriales y guías, proporcionando información adaptada a diferentes dispositivos y sistemas operativos. Esto

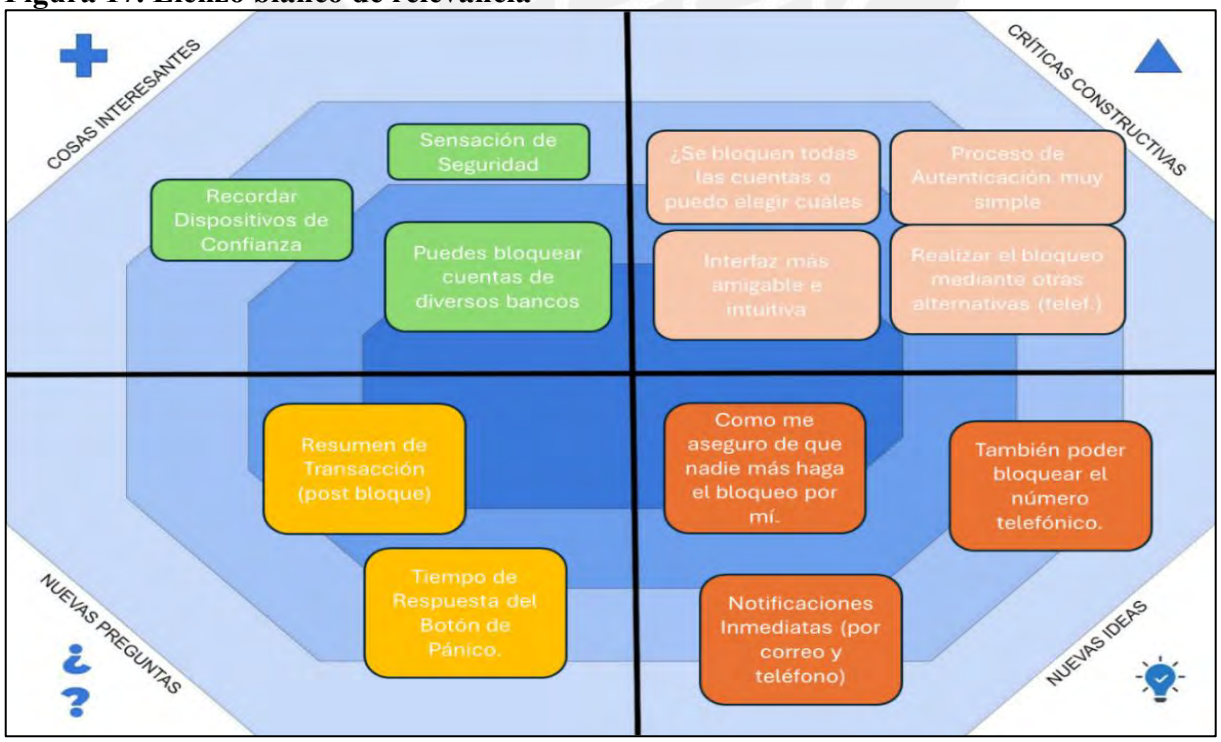
garantiza que los usuarios puedan ajustar los parámetros de seguridad de sus dispositivos de manera efectiva, independientemente del modelo o marca.

Se incluyó información detallada para realizar denuncias policiales, ofreciendo datos sobre los requisitos, ubicaciones y horarios de las comisarías y municipalidades. Esta información ayuda al usuario a realizar los trámites necesarios de manera más eficiente, reduciendo el estrés asociado a estos procedimientos.

También se mejoró la experiencia de usuario al diseñar una interfaz intuitiva que facilita el uso de la aplicación en situaciones de estrés. Se consideraron aspectos como la simplicidad en la navegación, el uso de lenguaje claro y la minimización de pasos para realizar acciones críticas, como el bloqueo de cuentas y líneas telefónicas.

Estas mejoras fueron incorporadas en el prototipo final de Segurazo, asegurando que el asistente virtual ofreciera una respuesta integral y efectiva ante situaciones de emergencia. La iteración constante y el enfoque en las necesidades reales de los usuarios garantizaron que el producto final cumpliera con las expectativas y brindara un alto valor agregado.

Figura 17. Lienzo blanco de relevancia



Fuente: Elaboración Propia

4.2. Desarrollo de la narrativa

El desarrollo de la solución Segurazo se basó en la metodología Design Thinking, la cual es ampliamente utilizada para la resolución de problemas complejos mediante un enfoque centrado en el usuario. Este proceso consta de cinco fases iterativas: Empatizar, Definir, Idear, Prototipar y Testear. Cada fase fue aplicada rigurosamente a lo largo del proyecto, asegurando que la solución respondiera a las necesidades reales de los usuarios y optimizando continuamente su funcionalidad mediante la retroalimentación obtenida en pruebas y validaciones.

Empatizar

La fase de empatizar se centró en la comprensión de los problemas que enfrentan los usuarios tras el robo de su celular. Para ello, se llevaron a cabo diversas estrategias de investigación que combinaron métodos cualitativos y cuantitativos. Se realizaron 30 entrevistas a profundidad con víctimas recientes de robo de celular, 150 encuestas digitales en comunidades de usuarios fintech y de seguridad digital, y se analizó una muestra de denuncias en redes sociales y reportes de la Policía Nacional del Perú.

Los hallazgos de esta fase evidenciaron que el 85% de los encuestados manifestó sentir confusión al intentar bloquear sus cuentas bancarias y líneas móviles tras el robo. Además, el 78% indicó haber recibido intentos de fraude (como phishing o llamadas falsas) luego del incidente. Un 90% desconocía la importancia de bloquear el IMEI de su celular para evitar que el dispositivo fuera reutilizado, y el 72% reportó impactos financieros debido a la demora en tomar medidas de seguridad. También se identificó que el 80% de los afectados no presentó una denuncia formal por desconocimiento del proceso o falta de información accesible.

Estos resultados reflejan la necesidad de contar con una herramienta que permita reducir la incertidumbre y facilite una reacción rápida y efectiva. La solución debía ofrecer

información clara, estructurada y accesible en el menor tiempo posible, evitando que los usuarios pierdan tiempo en la búsqueda de contactos de bancos, operadoras o entidades policiales.

Definir: Enfoque del problema y objetivos de la solución

Luego de la fase de empatización, en la que se recopilaron datos cualitativos y cuantitativos sobre la experiencia de los usuarios tras el robo de sus dispositivos móviles, se llevó a cabo un análisis estructurado para sintetizar la información y delimitar el problema central que debía abordarse. Para ello, se aplicaron dos enfoques metodológicos clave: la técnica How Might We? (HMW) y la Teoría del Porqué (Golden Circle) de Simon Sinek. Estas herramientas permitieron reformular el problema en términos de oportunidades de solución y profundizar en su origen, manifestación y consecuencias.

La técnica How Might We? (HMW) es utilizada en el proceso de Design Thinking para transformar desafíos en preguntas que guíen la generación de soluciones. Su aplicación en este contexto permitió identificar los principales obstáculos que enfrentan los usuarios al intentar proteger su información luego del robo de su celular. Se formuló el problema en términos de acción, buscando posibles vías de solución desde distintas perspectivas. A través de esta técnica, se evidenció que el problema radicaba en la falta de información, también en la dispersión de los canales de atención y la ausencia de un flujo de acción claro que permitiera a los usuarios tomar medidas inmediatas sin cometer errores.

Por otro lado, la Teoría del Porqué (Golden Circle) de Simon Sinek proporcionó una estructura para analizar el problema en tres niveles: la razón fundamental del problema (por qué ocurre), la forma en la que se manifiesta (cómo afecta a los usuarios) y lo que se necesita para resolverlo (qué elementos deben incluirse en la solución). Desde esta perspectiva, se determinó que el problema central radica en la incertidumbre y el riesgo financiero que experimentan las víctimas de robo de celular debido a la falta de información clara y

accesible sobre los procedimientos de seguridad que deben seguir. Este problema se manifiesta en la dificultad que enfrentan los usuarios al intentar bloquear sus cuentas bancarias y líneas móviles, ya que deben buscar información dispersa en múltiples plataformas sin un procedimiento unificado. En muchos casos, esta falta de claridad provoca demoras en la reacción, aumentando el riesgo de fraude y el acceso indebido a datos personales. Además, se identificó que la ausencia de un flujo de acción estructurado genera oportunidades para que los delincuentes ejecuten fraudes adicionales, como llamadas falsas haciéndose pasar por bancos u operadores móviles.

A partir de estos hallazgos, se concluyó que la mejor estrategia para abordar el problema era desarrollar una plataforma web interactiva con un asistente virtual que guiara a los usuarios en tiempo real, facilitando el acceso inmediato a bancos, operadoras y organismos de seguridad. La combinación de la técnica HMW y la Teoría del Porqué permitió definir el problema de manera precisa, asegurando que la solución respondiera a las necesidades reales de los usuarios y optimizando la estructura del flujo de acción para maximizar su efectividad.

Idear: Generación y evaluación de soluciones

En la fase de ideación, se aplicó la matriz 6x6 para estructurar y evaluar posibles soluciones al problema identificado. Esta herramienta permitió analizar alternativas en función de seis criterios clave: viabilidad, deseabilidad, impacto, escalabilidad, factibilidad y alineación con las necesidades del usuario.

A partir de este análisis, se generaron diversas propuestas para mitigar los riesgos asociados al robo de dispositivos móviles. Se exploraron soluciones como la implementación de una plataforma de bloqueo centralizado, el uso de notificaciones automatizadas para cambios de contraseñas y el desarrollo de una herramienta digital que guiara a los usuarios en tiempo real.

La evaluación comparativa dentro de la matriz permitió priorizar la opción más efectiva: Segurazo, una plataforma web interactiva diseñada para agilizar la gestión de bloqueos y denuncias. Se destacó por su accesibilidad, rapidez de respuesta y facilidad de integración con bancos y operadoras. Además, aseguraba que los usuarios pudieran centralizar la información necesaria para reaccionar de manera rápida y efectiva, reduciendo el riesgo de fraude financiero.

Finalmente, el proceso de ideación permitió definir los elementos clave que debía incluir Segurazo para optimizar la experiencia del usuario. Entre ellos, se priorizó una interfaz intuitiva, un flujo de acciones simplificado y la integración de recursos educativos sobre seguridad digital, garantizando que los usuarios tuvieran acceso a información clara y estructurada en situaciones de emergencia.

Prototipar: Desarrollo y validación del prototipo

En la fase de prototipado, se desarrolló una versión funcional de Segurazo para validar su propuesta de valor y evaluar su desempeño en un entorno real. Se implementó un host y un dominio web que permitieron la simulación de la experiencia del usuario, facilitando pruebas en distintos dispositivos, equipos y asegurando que la plataforma respondiera de manera efectiva a las necesidades identificadas en las fases previas.

El desarrollo del prototipo incluyó un enfoque integral en UI (Interfaz de Usuario) y UX (Experiencia del Usuario). La UI se centró en la presentación visual de la plataforma, asegurando que los botones, menús y accesos directos estuvieran organizados de manera clara y atractiva para los usuarios. Se definieron colores, tipografías y elementos gráficos que facilitaran la navegación y mejoraran la comprensión de las funciones clave.

Por otro lado, la UX se enfocó en la facilidad de uso y la eficiencia de la plataforma. Se priorizó una estructura intuitiva que guiara al usuario en cada paso, asegurando que pudiera reaccionar rápidamente en situaciones de emergencia. Se optimizó el flujo de

navegación para que los usuarios pudieran completar acciones esenciales, como la obtención de contactos de emergencia, en el menor tiempo posible. Para ello, se eliminaron pasos innecesarios, se agruparon las opciones más utilizadas y se incluyeron accesos directos para evitar que el usuario tuviera que realizar múltiples clics o búsquedas.

Las pruebas realizadas sobre el prototipo funcional permitieron obtener métricas concretas sobre su efectividad. Se midió el tiempo promedio que los usuarios tardaban en completar acciones críticas, como el bloqueo de cuentas bancarias y líneas móviles. Los resultados iniciales mostraron que el 80% de los usuarios logró realizar un recorrido completo estos procesos en **menos de tres minutos (2.57min)**, lo que evidencia una mejora significativa en comparación con los métodos tradicionales, donde estos procedimientos pueden **tardar más de 1 hora.**

Además de la evaluación del tiempo de respuesta, se incorporó una fase de observación con usuarios reales para medir la facilidad de uso y la efectividad del diseño. Se optimizó el diseño para facilitar su uso en dispositivos móviles, dado que la mayoría de los usuarios acceden a este tipo de herramientas desde sus celulares. Se realizaron ajustes en la disposición de los elementos visuales para reducir la carga cognitiva y permitir que los usuarios encontraran rápidamente la información clave.

El prototipo fue sometido a iteraciones en función del feedback de los usuarios, lo que permitió mejorar su funcionalidad y optimizar su flujo de uso. Entre los principales cambios realizados tras las pruebas se incluyeron la reorganización de los menús, la mejora en la legibilidad de las instrucciones y la optimización de los tiempos de carga de la plataforma.

Como resultado de esta fase, el prototipo de Segurazo quedó disponible en un entorno web funcional, accesible a través del enlace www.segurazo.xyz. Este entorno permitió evaluar el rendimiento real de la solución y obtener datos concretos sobre su efectividad en escenarios simulados de robo o pérdida de dispositivos.

Testear: Validación del prototipo y ajustes finales

Para evaluar la efectividad de **Segurazo**, se llevó a cabo una fase de testeo con usuarios que habían experimentado situaciones de robo o pérdida de dispositivos móviles. Se realizaron pruebas en un entorno controlado y en escenarios simulados, con el objetivo de medir la facilidad de uso, la rapidez en la ejecución de acciones críticas y la satisfacción general de los participantes con la plataforma.

El testeo se desarrolló en dos etapas principales. En la primera etapa, se realizaron pruebas de usabilidad con un **grupo de 20 usuarios**, quienes interactuaron con el prototipo en distintos dispositivos móviles y computadoras. Se les asignaron tareas específicas, como localizar contactos de bancos, operadoras y seguir los pasos sugeridos por la plataforma para presentar una denuncia. Durante la prueba, se registró el tiempo que tardaban en completar cada tarea y se analizaron los errores o dificultades que surgieron en el proceso.

En la segunda etapa, se llevó a cabo una evaluación en escenarios simulados con 5 participantes, en la que se recrearon situaciones de robo para observar cómo reaccionaban ante la plataforma en condiciones de estrés. En esta fase, se midió el tiempo de respuesta de los usuarios, la claridad de las instrucciones y la efectividad del flujo de acciones en comparación con los métodos tradicionales de gestión de bloqueos y denuncias.

Con el fin de evaluar la efectividad del procedimiento de seguridad para el borrado remoto de información en caso de robo de dispositivos, se realizaron pruebas con dispositivos Android e iOS utilizando Google Find My Device y Apple iCloud. Se configuraron escenarios donde el usuario accedía a la plataforma de gestión de su dispositivo desde otro equipo y ejecutaba la opción de "borrar datos". Los resultados indicaron que la totalidad de los usuarios lograron acceder al borrado remoto siguiendo las instrucciones de Segurazo.

Para documentar las interacciones de los usuarios con la plataforma y analizar su comportamiento en tiempo real, se realizaron grabaciones en video durante las pruebas. Estas

evidencias permiten visualizar el proceso de uso de Segurazo, identificar mejoras en la experiencia del usuario y respaldar los resultados obtenidos en el testeo. Los videos de las pruebas están disponibles en el siguiente enlace: https://onedrive.live.com/?id=D7EBDAE48CBD3F90%212665&cid=D7EBDAE48CBD3F90

Los resultados obtenidos en esta fase proporcionaron datos clave sobre la efectividad y usabilidad de la plataforma. El 100% de los usuarios encontró intuitiva la navegación dentro de Segurazo, indicando que pudieron encontrar rápidamente la información que necesitaban sin dificultad. El tiempo promedio para completar los contactos y líneas móviles se redujo de 60 minutos (métodos tradicionales) a menos de 3 minutos utilizando la plataforma. Además, el 85% de los participantes manifestó que la centralización de información y contactos fue el aspecto más valioso, ya que eliminaba la necesidad de buscar números y procedimientos dispersos en distintos canales.

A partir de estos resultados, se realizaron ajustes finales en la plataforma para mejorar la experiencia del usuario y maximizar su funcionalidad. Se optimizó la organización de los menús, se incluyeron accesos directos a recomendaciones de seguridad digital y se perfeccionaron los textos informativos para hacerlos más claros y concisos. Asimismo, se reforzó la visibilidad de los botones de acción rápida para facilitar el acceso a los procedimientos más importantes en momentos de crisis.

Finalmente, Segurazo quedó validado como una solución efectiva para asistir a los usuarios en la gestión de contactabilidad a bancos, operadores, bloqueo móvil y colocación de denuncias en situaciones de robo o pérdida de dispositivos. Su enfoque basado en la rapidez, accesibilidad y centralización de información permitió mejorar significativamente la respuesta ante incidentes de seguridad, reduciendo el riesgo de fraude y optimizando la experiencia de los afectados.

Integración del Lienzo Blanco de Relevancia

A lo largo del proceso de desarrollo, se utilizó el Lienzo Blanco de Relevancia (Figura 11) como herramienta para documentar y analizar la evolución de Segurazo. Este lienzo permitió visualizar cómo los aprendizajes y hallazgos de cada fase del Design Thinking fueron implementados para mejorar la solución.

El lienzo facilitó la identificación de áreas de mejora y la alineación constante de la herramienta con las necesidades reales de los usuarios. Por ejemplo, al reflejar en el lienzo las preocupaciones de los usuarios sobre la seguridad de sus datos personales, se reforzaron las medidas de protección de la información en la aplicación. Asimismo, se ajustaron las estrategias de comunicación y se incorporaron mensajes que brindaban tranquilidad y confianza al usuario.

4.3. Carácter innovador y disruptivo del producto o servicio

Para evaluar el carácter innovador y disruptivo de Segurazo, es esencial analizar las soluciones existentes en el mercado y cómo nuestro producto se diferencia y mejora frente a ellas. A continuación, se presenta una revisión de patentes y estudios de caso de soluciones similares, seguida de un análisis comparativo que justifica la innovación que representa Segurazo en el ámbito de la seguridad financiera y móvil.

4.3.1. Revisión de Patentes

La revisión de patentes relevantes permite comprender las tecnologías existentes y las soluciones propuestas para abordar problemas similares a los que Segurazo busca resolver.

La **US Patent No. 9,998,123 B2**, titulada *"System and Method for Securing Mobile Banking Transactions"*, describe un sistema para asegurar transacciones bancarias móviles utilizando autenticación biométrica y alertas en tiempo real. Esta tecnología permite a los usuarios bloquear sus cuentas de manera instantánea desde sus dispositivos móviles (Google Patents, s.f.).

La **EP Patent No. 2,745,888 B1**, *"Emergency Response System for Financial Accounts"*, proporciona un mecanismo para bloquear rápidamente las cuentas financieras en caso de emergencia, como el robo de un dispositivo móvil. Incluye un servicio de llamadas telefónicas automatizadas que dirige al usuario a su entidad financiera correspondiente (European Patent Office, s.f.).

La **CN Patent No. 105,389,764 A**, *"Mobile Security Alert System"*, detalla un sistema de alertas de seguridad para dispositivos móviles que utiliza tecnologías de geolocalización y detección de patrones inusuales para enviar alertas y sugerir el bloqueo temporal de cuentas (CNIPA, s.f.).

4.3.2. Estudios de Casos

Además de las patentes, es relevante considerar las soluciones implementadas en el mercado para entender el contexto en el que Segurazo operará.

El **Sistema de Bloqueo Bancario de BBVA** permite a los usuarios bloquear y desbloquear sus cuentas y tarjetas desde la aplicación móvil del banco. Este sistema ha reducido significativamente los casos de fraude bancario y ha mejorado la confianza del usuario en los servicios móviles del banco (BBVA, s.f.).

Alipay ha desarrollado un sistema de detección de fraudes en tiempo real que utiliza aprendizaje automático y análisis de big data para identificar actividades sospechosas y prevenir fraudes. La implementación de este sistema ha resultado en una notable disminución de las pérdidas por fraude (Alipay, s.f.).

En **India**, la consolidación bancaria ha llevado a la creación de centrales telefónicas que permiten a los usuarios bloquear sus cuentas a través de un número centralizado. Estas centrales mejoran la eficiencia y seguridad en el proceso de bloqueo de cuentas al direccionar las llamadas a los bancos correspondientes (Deloitte, 2021).

Desde julio de 2024, **ASBANC (Asociación de Bancos del Perú)** lanzó la línea de emergencia **1820**, un servicio diseñado para facilitar el bloqueo inmediato de tarjetas bancarias, aplicaciones financieras y canales digitales en casos de robo. Este sistema, accesible a través de un número único y fácil de recordar, está dirigido a usuarios de las principales entidades financieras del país. La iniciativa busca ofrecer una respuesta rápida y centralizada ante situaciones de emergencia, ayudando a mitigar los riesgos de fraude financiero (El Peruano, 2024).

4.3.3. Análisis Comparativo y Justificación del Carácter Innovador

Para evaluar el carácter innovador de Segurazo, se realizó un análisis de las soluciones existentes en el mercado y se identificaron las principales diferencias que hacen de Segurazo una propuesta disruptiva. Actualmente, los métodos que utilizan los usuarios para gestionar el robo o pérdida de un dispositivo móvil presentan deficiencias en la centralización de información, tiempos de respuesta y accesibilidad. A diferencia de estas soluciones tradicionales, Segurazo introduce un modelo integral que simplifica la seguridad financiera y móvil, permitiendo una respuesta más rápida y efectiva ante incidentes de robo.

Entre las soluciones existentes, se encuentra la línea 1820 de ASBANC, implementada en Perú desde julio de 2024. Esta línea permite el bloqueo de tarjetas y cuentas bancarias de múltiples entidades financieras a través de un número único. Sin embargo, su funcionalidad está limitada únicamente a la banca formal y no abarca otros aspectos esenciales, como el bloqueo de líneas telefónicas o la asistencia en denuncias policiales.

Otra opción en el mercado son las aplicaciones financieras individuales, como las de BBVA, BCP, Scotiabank e Interbank, que ofrecen la posibilidad de bloquear cuentas y tarjetas dentro de sus propias aplicaciones móviles. Sin embargo, estas aplicaciones no ofrecen centralización de múltiples entidades, lo que significa que el usuario debe ingresar a cada aplicación por separado y seguir procesos distintos en cada una.

Por otro lado, existen plataformas de seguridad digital, como Google Find My Device y Apple iCloud, que permiten el rastreo y bloqueo remoto de dispositivos móviles. Estas herramientas son útiles para evitar el acceso indebido a información en el teléfono, pero no incluyen la gestión de bloqueos bancarios ni asistencia en la presentación de denuncias policiales, dejando una brecha en la protección financiera del usuario.

Finalmente, el método tradicional de bloqueo, que consiste en buscar manualmente los números de contacto de bancos y operadores móviles para llamarlos uno por uno, sigue siendo una de las alternativas más utilizadas. Sin embargo, este método es ineficiente, ya que aumenta la fricción en la experiencia del usuario y prolonga el tiempo de respuesta, lo que incrementa el riesgo de fraude antes de que se ejecuten los bloqueos necesarios.

Como se muestra en la tabla 9, Segurazo se diferencia al integrar múltiples funcionalidades que actualmente se encuentran dispersas en distintas soluciones.

Tabla 9. Comparación de Segurazo con otras soluciones de seguridad financiera y móvil

Características	Segurazo	Línea 1820 de ASBANC	Aplicaciones Financieras Individuales	Bloqueo Tradicional (Llamadas individuales)
Bloqueo centralizado de cuentas bancarias	Si	Si	No	No
Bloqueo de líneas telefónicas con operadores	Si	No	No	No
Asistencia en denuncias policiales	Si	No	No	No
Tutoriales para ajustar seguridad del dispositivo	Si	No	No	No
Asistente virtual con IA y PNL	Si	No	No	No
Acceso a múltiples entidades financieras	Si	Si	No	No
Interfaz única e intuitiva	Si	No (Línea telefónica)	No (Múltiples aplicaciones)	No

Actualización constante y personalizada	Si	Limitada	Variable	No

Fuente: Elaboración propia

Esta comparación evidencia que Segurazo ofrece una solución más completa y eficiente que las alternativas actuales. Al combinar múltiples funciones de seguridad en una sola plataforma, Segurazo simplifica y mejora significativamente la respuesta del usuario ante situaciones de emergencia.

Justificación del Carácter Innovador

Según el Manual de Oslo (2018), la innovación se define como la implementación de un producto nuevo o significativamente mejorado que difiere de manera sustancial de los productos anteriores y que ha sido puesto a disposición de los usuarios. Segurazo cumple con esta definición al introducir una plataforma que centraliza y simplifica procesos que tradicionalmente son fragmentados y lentos.

La capacidad de Segurazo para:

- Centralizar y agilizar acciones críticas tras el robo o pérdida de un dispositivo móvil.
- Integrar tecnologías avanzadas como inteligencia artificial y procesamiento de lenguaje natural para ofrecer asistencia personalizada.
- Ofrecer recursos educativos que empoderan al usuario en la gestión de su seguridad.
- Proporcionar una interfaz intuitiva y accesible que mejora la experiencia del usuario.

Estas características innovadoras posicionan a Segurazo como una solución disruptiva en el mercado. A diferencia de Alipay, que se enfoca en la detección de fraudes en tiempo real utilizando big data, o la línea 1820 de ASBANC, que ofrece un número único para bloqueo de tarjetas, Segurazo aborda múltiples aspectos de la seguridad en una sola plataforma, proporcionando una respuesta integral que abarca desde el bloqueo de cuentas y líneas telefónicas hasta la asistencia en denuncias y la educación en seguridad.

Impacto Potencial en la Industria y Experiencia del Usuario

Segurazo tiene el potencial de transformar la manera en que los usuarios gestionan la seguridad de sus cuentas bancarias y dispositivos móviles. Al centralizar y simplificar los procedimientos de emergencia, la plataforma no solo optimiza la experiencia del usuario, sino que también reduce los costos operativos para las instituciones financieras y operadoras telefónicas mediante: la agilización de procesos y la disminución del riesgo de fraudes.

Además, al alinearse con los estándares internacionales y las mejores prácticas en innovación, Segurazo establece un nuevo estándar en el sector de seguridad móvil y prevención de fraudes, impulsando su adopción y marcando un avance significativo en la protección contra fraudes financieros y la pérdida de información personal..

4.4. Propuesta de valor

4.4.1. Usuarios de las entidades financieras

En las entrevistas con los usuarios, se identificaron sus principales frustraciones y alegrías al enfrentar el robo o pérdida de sus dispositivos móviles. Las principales frustraciones incluyen la necesidad de una respuesta inmediata, la falta de información clara y accesible, procesos engorrosos y múltiples contactos, y el temor a la pérdida de datos personales y financieros.

Los usuarios experimentan ansiedad y estrés debido a la urgencia de proteger sus cuentas bancarias y líneas telefónicas tras el robo de su celular. La demora en tomar acciones aumenta el riesgo de fraude y el uso indebido de su información personal y financiera, generando una preocupación constante por el posible acceso no autorizado a datos sensibles almacenados en sus dispositivos móviles. Además, muchos usuarios desconocen los pasos específicos que deben seguir para bloquear sus cuentas y líneas telefónicas, lo que se agrava por la dispersión de la información y la dificultad para acceder a números de contacto en situaciones de emergencia. Esta falta de claridad y accesibilidad provoca que los usuarios se

sientan abrumados al tener que contactar individualmente a cada entidad financiera y operador telefónico, enfrentando tiempos de espera prolongados y procedimientos complejos.

Por otro lado, los usuarios valoran la capacidad de actuar rápidamente y de manera eficaz para asegurar sus cuentas y líneas telefónicas, minimizando el riesgo de fraude. Valoran contar con guías específicas que los ayuden a seguir los pasos correctos en una situación de estrés, reduciendo la confusión y el tiempo de respuesta. Además, aprecian la posibilidad de acceder a todos los números y procedimientos necesarios desde una sola plataforma, lo que les ahorra tiempo y esfuerzo. La confianza y tranquilidad que surge al sentirse seguros de que están tomando las medidas adecuadas para proteger su información y activos financieros es fundamental para ellos.

Segurazo responde directamente a estas frustraciones al ofrecer una plataforma que proporciona una respuesta inmediata a través de una interfaz intuitiva, permitiendo a los usuarios iniciar acciones de bloqueo de cuentas bancarias y líneas telefónicas de forma rápida y eficiente. Por ejemplo, un usuario puede, en cuestión de minutos, acceder a Segurazo y, con pocos clics, iniciar el proceso de bloqueo de todas sus cuentas bancarias y su línea telefónica, sin necesidad de recordar números de contacto o procedimientos complejos.

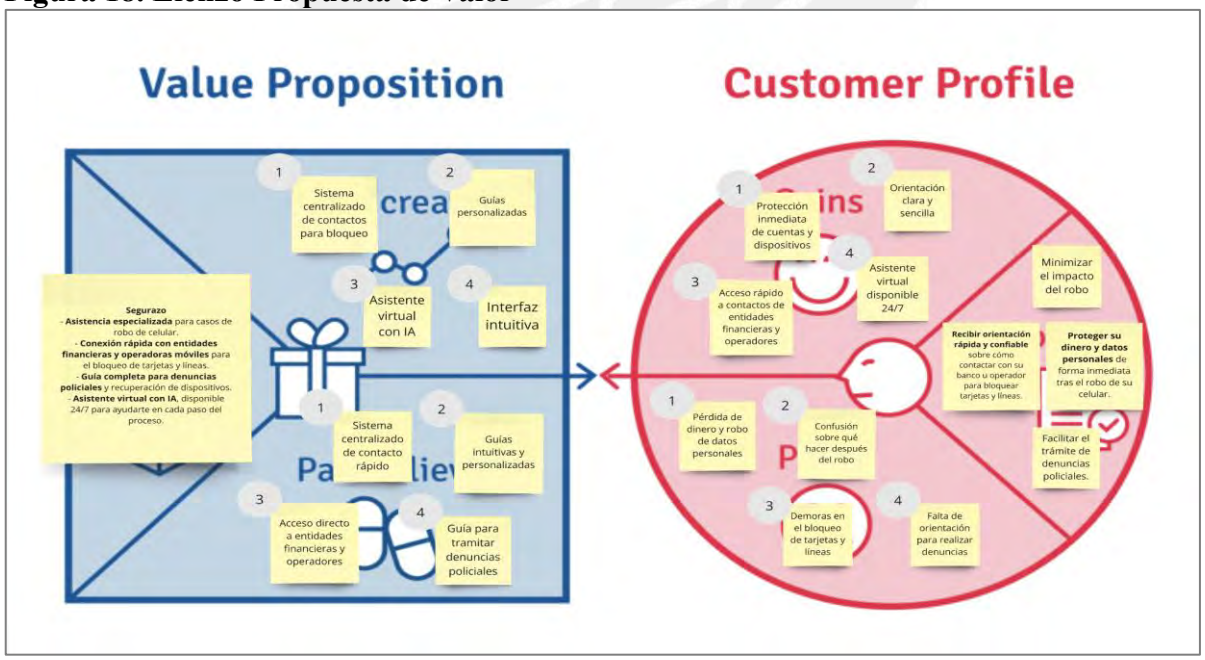
Además, Segurazo ofrece información clara y guías paso a paso, incluyendo instrucciones detalladas y personalizadas para cada usuario, facilitando la comprensión de los pasos a seguir. Si un usuario no sabe cómo bloquear su cuenta en un banco específico, Segurazo le proporciona instrucciones precisas y, en algunos casos, enlaces directos o números de contacto específicos. Al centralizar contactos y procedimientos, Segurazo simplifica el proceso que antes requería múltiples llamadas y búsquedas de información, permitiendo que el usuario encuentre toda esta información actualizada en una sola plataforma.

Segurazo también refuerza la seguridad y protección de datos al ofrecer consejos y tutoriales sobre cómo proteger la información personal y qué medidas adicionales tomar. Por ejemplo, el asistente virtual puede sugerir al usuario cambiar las contraseñas de sus aplicaciones y servicios en línea, proporcionando guías sobre cómo hacerlo de manera segura.

Los beneficios clave para el usuario incluyen la reducción del estrés y la ansiedad al contar con una herramienta que simplifica y acelera el proceso de protección, empoderamiento del usuario al proporcionar las herramientas y la información necesaria para tomar el control de la situación, y ahorro de tiempo y esfuerzo al centralizar las acciones y contactos. Al ofrecer una solución integral que aborda directamente las necesidades y preocupaciones de los usuarios, Segurazo se alinea perfectamente con las expectativas de los usuarios, proporcionando confianza y seguridad en la gestión de emergencias relacionadas con el robo o pérdida de dispositivos móviles.

Lo previamente mencionado, se puede apreciar en la Figura 18, Lienzo propuesta de valor de usuarios.

Figura 18. Lienzo Propuesta de Valor



Fuente: Elaboración Propia

Encaje entre la Propuesta de Valor y las Necesidades del Usuario

Segurazo responde directamente a los dolores identificados al ofrecer una plataforma que proporciona una respuesta inmediata, información clara y guías paso a paso, centraliza contactos y procedimientos, y refuerza la seguridad y protección de datos. Estos elementos están diseñados para aliviar las frustraciones específicas de los usuarios, facilitando una experiencia organizada y eficiente en momentos de emergencia. La centralización de servicios permite que los usuarios actúen rápidamente para proteger sus cuentas bancarias y líneas telefónicas, mientras que las guías claras reducen la confusión y el tiempo de respuesta, proporcionando una solución integral que abarca desde el bloqueo de cuentas hasta la asistencia en denuncias policiales.

Validación de la Propuesta de Valor

La validación de la propuesta de valor de Segurazo se realizó mediante las entrevistas a usuarios quienes compartieron sus principales preocupaciones y necesidades en caso de robo de sus dispositivos móviles. Este proceso se centró en identificar los puntos de dolor más críticos y las características que considerarían indispensables en nuestra solución.

El diseño del Lienzo de Propuesta de Valor partió de estos hallazgos, reflejando tanto las frustraciones como las alegrías de los usuarios. Por ejemplo, los resultados de las encuestas mostraron que la mayor parte de los participantes priorizan la rapidez y facilidad de uso en una herramienta para emergencias, así como la importancia de contar con información clara y centralizada.

Por su lado, la retroalimentación recibida a partir de la reunión con uno de los principales clientes: el BCP, garantiza que la propuesta de valor de nuestro servicio sea eficaz para abordar las situaciones de emergencia enfrentadas por los usuarios.

En la tabla 10, se muestra la manera en la que validamos la propuesta de valor a partir de los Sprints realizados.

Tabla 10. Validaciones de la Propuesta de Valor

Sprint	Retroalimentación más relevante	Mejoras en el servicio
Mybot Versión 1	El servicio debe ser multiplataforma, no solo una aplicación móvil o "app".	Se pasó a ser una aplicación que se descarga de App Store a una aplicación web capaz de adecuarse a cualquier dispositivo. **Resultado: Mybot versión 2**
Mybot Versión 2	El servicio debe ser capaz de mostrar información relevante para cada usuario en específico.	Se incorporó una base de datos para que la aplicación muestre al usuario información relevante por caso. Se cambió el nombre del servicio para que se adecúe más a nuestra propuesta. **Resultado: Segurazo versión 1**
Segurazo Versión 1	Mejorar el diseño de la aplicación web, debe transmitir tranquilidad al usuario.	Se rediseñó la aplicación web y se realizaron ajustes para facilitar la navegación. **Resultado: Segurazo versión 2**

Fuente: Elaboración Propia

4.5. Producto mínimo viable (PMV)

Durante el desarrollo de nuestro servicio, se implementó un enfoque iterativo basado en sprints, permitiendo la creación y mejora continua del Producto Mínimo Viable (PMV). En cada sprint, se desarrollaron nuevas funcionalidades y se realizaron pruebas con usuarios para validar la efectividad de la solución en escenarios reales de emergencia. A continuación, se detalla el proceso y las mejoras realizadas en cada sprint, incorporando el feedback de los usuarios para asegurar que Segurazo responde efectivamente a sus necesidades.

Sprint 1: Creación del primer prototipo

Este prototipo representa la interfaz inicial de Mybot (Figura 19), el primer nombre que dimos a nuestro servicio, diseñada como parte del primer sprint de desarrollo. El enfoque principal es proporcionar una experiencia de usuario intuitiva y accesible, dirigida a resolver las necesidades inmediatas de los usuarios en caso de robo o pérdida de dispositivos móviles.

La pantalla de inicio presenta un diseño amigable con un personaje llamado Mybot, un asistente virtual que guía a los usuarios a través de las opciones disponibles. Esta primera impresión busca generar confianza y empatía con el usuario. En esta pantalla se ofrecen dos opciones principales:

- Quiero estar más protegido: Para usuarios interesados en prevenir fraudes y mejorar su seguridad digital.
- Me robaron, ¿qué hago?: Una opción de emergencia que lleva al usuario directamente a las herramientas y guías para actuar frente a un robo.

Las características más importantes de esta fase incluyen a Mybot como una figura central que proporciona una interacción más humana y guiada. Por su lado, el usuario recibiría sus acciones recomendadas organizadas por cada categoría la cual ofrece pasos claros y accionables.

Los objetivos del primer sprint son de validar la usabilidad, así como probar la funcionalidad básica, así como obtener retroalimentación inicial de los usuarios sobre qué tan efectivas son las opciones presentadas para resolver sus necesidades inmediatas.

Figura 19. Sprint 1 – pantalla inicial de la app Mybot

Fuente: Elaboración Propia

Figura 20. Sprint 1 – pantalla de categorías de la app Mybot

Fuente: Elaboración Propia

Sprint 2: Creación de una aplicación web

En este segundo sprint, el objetivo fue de trasladar las funcionalidades de la aplicación móvil a una plataforma web accesible desde cualquier dispositivo, como laptops, tablets y celulares, manteniendo la experiencia de usuario y las opciones clave ya establecidas en el prototipo inicial. Esto amplía la accesibilidad de la plataforma, eliminando barreras relacionadas con el almacenamiento de dispositivos o la instalación de aplicaciones, y abre el servicio a una audiencia más amplia. Manteniendo el diseño amigable e intuitivo de la aplicación móvil, la interfaz web se adapta al tamaño de la pantalla del dispositivo, garantizando una experiencia consistente y fluida.

Nuestro objetivo era verificar que la aplicación web funcione de manera óptima en los principales navegadores (Chrome, Safari, Firefox, Edge) y dispositivos. Asimismo, realizar pruebas con usuarios para evaluar la usabilidad, fluidez y efectividad de la plataforma web, y también hay que asegurar que la experiencia sea igual de efectiva tanto en pantallas grandes como pequeñas.

Este segundo sprint representa un paso clave en la evolución de nuestro servicio, garantizando una plataforma inclusiva y accesible, mientras se mantiene fiel al propósito de brindar protección inmediata y efectiva frente al fraude financiero. Ver Figura 21 y 22.

Figura 21. Sprint 2 - esquema inicial Segurazo versión 1

Fuente: Elaboración Propia

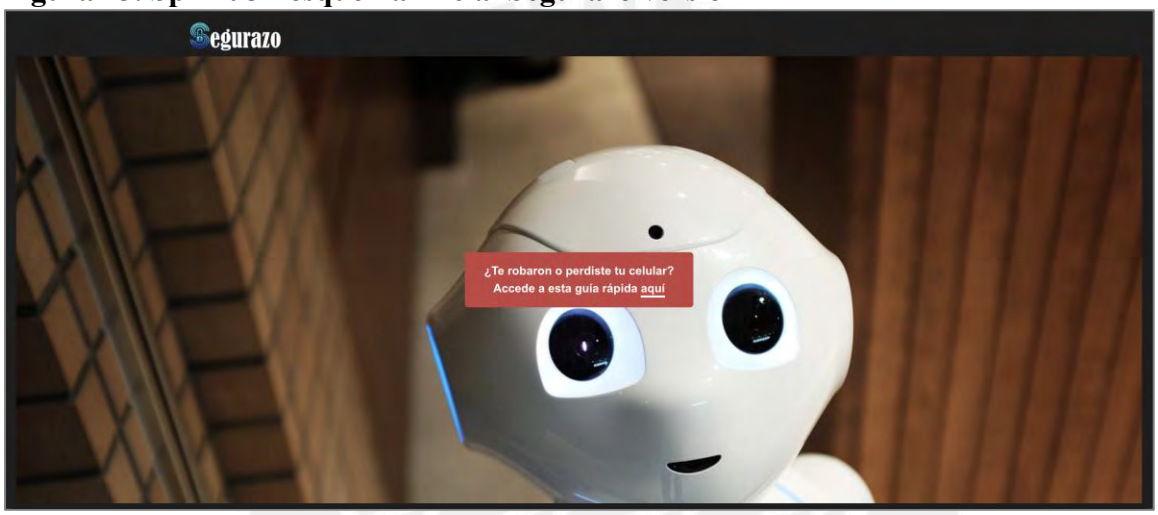
Figura 22. Sprint 2 – categorías mostradas en Segurazo versión 1

Fuente: Elaboración Propia

Sprint 3: Creación de una nueva Interfaz y más Funcionalidades

En esta fase, se desarrolló un PMV tangible que incluía una interfaz amigable y accesible para dispositivos móviles, con el objetivo de proporcionar una experiencia intuitiva tanto para usuarios en situaciones de emergencia como para aquellos que desean tomar acciones preventivas. La pantalla de bienvenida presentaba opciones claras como "Quiero estar más protegido" o "Me robaron, ¿qué hago?", facilitando la selección de las acciones necesarias (ver Figura 23).

Figura 23. Sprint 3 - esquema inicial Segurazo versión 2



Fuente: Elaboración propia

Las funcionalidades iniciales incluyeron la validación de datos por parte del usuario, tales como nombre, tipo de dispositivo y entidades financieras asociadas, con el propósito de orientar rápidamente en caso de un robo (ver Figura 24). Además, se integró un sistema de contacto directo con entidades financieras y operadores móviles para el bloqueo de tarjetas y líneas, junto con una guía para realizar denuncias ante la policía, proporcionando un flujo de acción claro y organizado.

Figura 24. Ingreso de datos de usuario

Fuente: Elaboración propia

Pruebas con Usuarios y Feedback

El PMV desarrollado en el Sprint 1 fue probado con un grupo de 10 usuarios en un contexto controlado. Estos participantes, que habían experimentado situaciones de robo o pérdida de dispositivos móviles, utilizaron la aplicación en escenarios simulados de emergencia. Se registró su experiencia y comentarios para identificar áreas de mejora.

Feedback de los Usuarios:

- **Aspectos positivos:** Los usuarios valoraron la simplicidad de la interfaz y la claridad de las opciones presentadas en la pantalla de bienvenida. Destacaron la utilidad de tener acceso rápido a las acciones necesarias en caso de robo, lo que les brindó tranquilidad y sensación de control.
- **Aspectos por mejorar:** Algunos usuarios encontraron dificultades para navegar entre las secciones y sugirieron que la interfaz podría ser más intuitiva. También señalaron que la información de contacto de las entidades financieras y operadores móviles no siempre estaba completa o actualizada, lo que podía generar retrasos en situaciones críticas.

Ajustes Realizados:

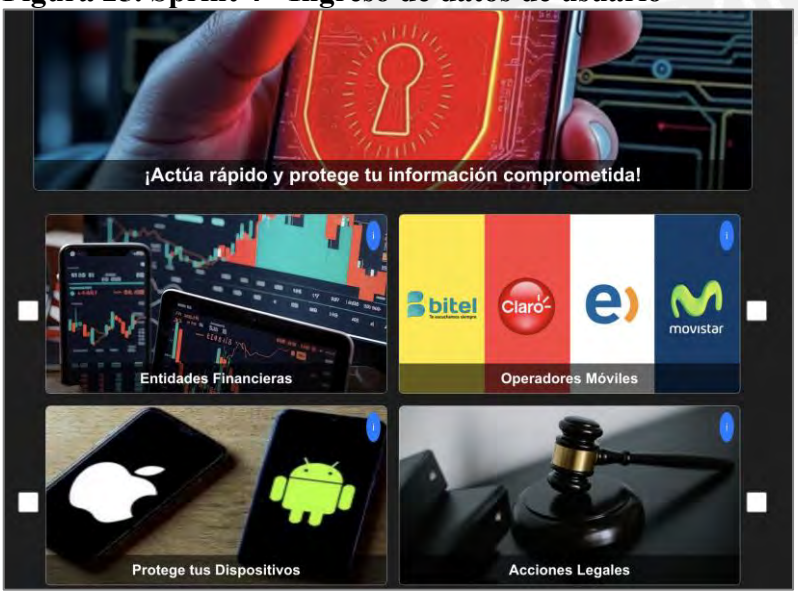
Basándose en el feedback recibido, se planificó una revisión de la interfaz para mejorar la navegación y usabilidad. Se estableció un protocolo para actualizar regularmente la información de contacto de las entidades financieras y operadores móviles. Además, se consideró simplificar el proceso de validación de datos para agilizar el acceso a las funcionalidades esenciales.

Sprint 4: Mejora de Funcionalidades y Evolución de la Interfaz

Durante el Sprint 4, se enfocó en mejorar la interfaz y expandir las funcionalidades de Segurazo, incorporando el feedback obtenido de las pruebas con usuarios. El objetivo principal fue ofrecer una experiencia de usuario más sólida y fluida, optimizando tanto la presentación visual como el acceso rápido a las herramientas clave.

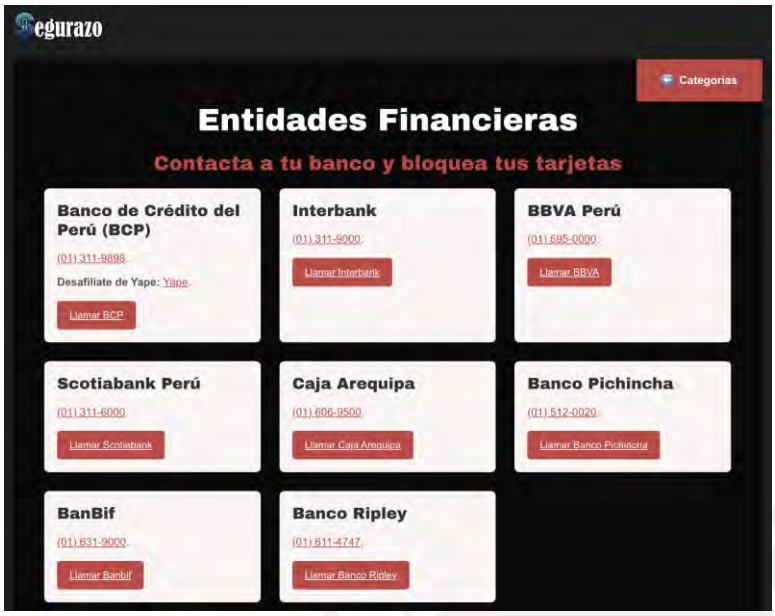
Las mejoras incluyeron una página de bienvenida rediseñada con un enfoque más directo hacia las necesidades del usuario, ahora dividida en categorías claras: Entidades Financieras, Operadores Móviles, Denuncias Policiales y Reforzar la Seguridad (ver Figura 25, 26 y 27). Este cambio facilitó una navegación más intuitiva y orientada a la acción, permitiendo que los usuarios accedieran rápidamente a los recursos críticos tras el robo de su celular.

Figura 25. Sprint 4 - Ingreso de datos de usuario



Fuente: Elaboración Propia

Figura 26. Sprint 4 - Entidades financieras



Fuente: Elaboración Propia

Figura 27. Sprint 4 - Protección de dispositivo

Fuente: Elaboración Propia

Figura 28. Sprint 4 - Acciones legales

Fuente: Elaboración Propia

Además, se añadió un acceso directo a la plataforma de denuncias policiales digitales, ofreciendo un flujo de acciones completo para mitigar los efectos de un robo de celular (ver Figura 28).

Pruebas con Usuarios y Feedback

El PMV mejorado fue nuevamente probado con usuarios, incluyendo a los participantes del primer testeo y a nuevos usuarios para ampliar la muestra a 20 participantes. Durante estas pruebas, se recopilaron observaciones sobre la nueva interfaz y funcionalidades.

Feedback de los Usuarios:

- **Aspectos positivos:** Los usuarios apreciaron las mejoras en la navegación y la claridad en la disposición de las categorías. La actualización de los contactos de entidades financieras y operadores facilitó el proceso de bloqueo, reduciendo el tiempo de respuesta en situaciones de emergencia.
- **Aspectos por mejorar:** Algunos usuarios sugirieron la inclusión de guías más detalladas sobre cómo reforzar la seguridad de sus dispositivos y cuentas. Otros mencionaron que el proceso de registro inicial aún podía simplificarse más para evitar demoras al momento de utilizar la aplicación por primera vez.

Sprint 5: Optimización del Diseño y Personalización de la Plataforma

Durante el Sprint 5, nos enfocamos en la optimización del diseño de la plataforma de Segurazo en base al feedback recibido de los usuarios, asegurando una experiencia de navegación más eficiente y adaptada a sus necesidades específicas. Además, se implementó una funcionalidad clave en el software que permite a los usuarios visualizar únicamente las entidades financieras y operadores móviles que previamente seleccionaron al ingresar sus datos (Figura 29).

El objetivo principal de esta fase fue mejorar la usabilidad y personalización de la experiencia del usuario, asegurando que cada interacción con la plataforma sea intuitiva y alineada con sus necesidades inmediatas.

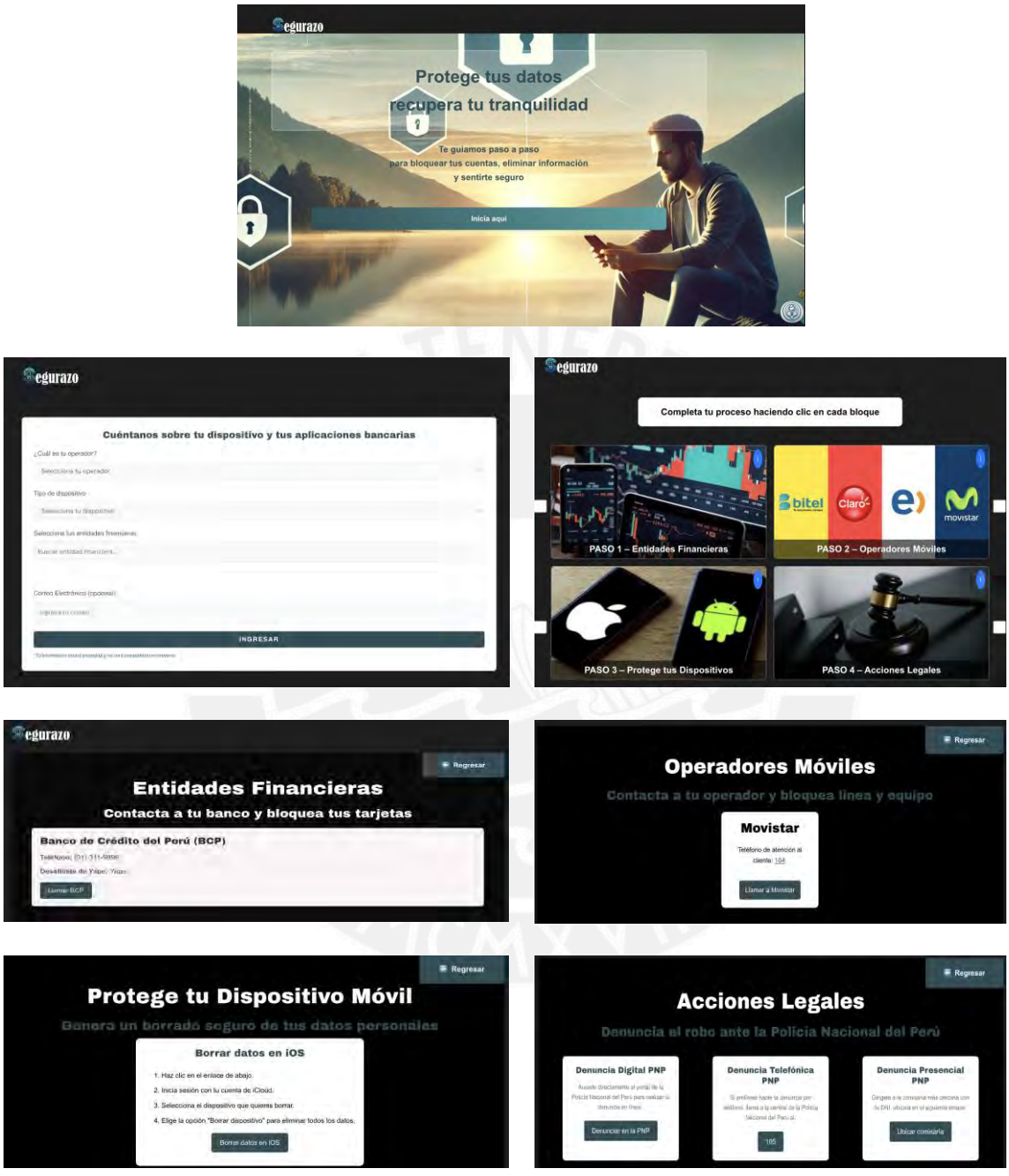
Mejoras implementadas

- Se optimizó la estética visual y la disposición de los elementos en la plataforma para facilitar la navegación y mejorar la accesibilidad en distintos dispositivos.
- Se incorporó una funcionalidad que permite filtrar automáticamente las entidades financieras y operadores móviles que el usuario haya seleccionado previamente al ingresar sus datos, eliminando la necesidad de navegar entre múltiples opciones irrelevantes.
- Se ajustaron los textos y botones para hacer más clara la secuencia de pasos a seguir en cada sección (bloqueo de cuentas, operadores móviles, protección del dispositivo y denuncia).
- Se realizaron nuevos test con 15 usuarios para validar la efectividad de los cambios, asegurando que la experiencia fuera más fluida y sin fricciones.

Estas actualizaciones mejoraron significativamente la rapidez y efectividad de la plataforma, permitiendo a los usuarios completar sus gestiones en menos tiempo y con mayor precisión, evitando distracciones o información irrelevante.

Link Segurazo: https://www.segurazo.xyz/

Figura 29. Sprint 5 - Versión Final Segurazo



Fuente: Elaboración Propia

En el diseño del producto, se han identificado características innovadoras que lo diferencian de las soluciones existentes en el mercado. En la tabla 11, se presenta una comparación detallada entre las funcionalidades de Segurazo y otras alternativas actuales,

como la Línea 1820 de ASBANC, las aplicaciones financieras individuales y el bloqueo tradicional mediante llamadas. Esta comparación resalta las ventajas competitivas de Segurazo, enfocándose en su capacidad de integración, su interfaz intuitiva y su enfoque en predicción y protección proactiva contra fraudes

Tabla 11. Comparación de Segurazo con otras soluciones de seguridad

Características	Segurazo	Línea 1820 de ASBANC	Aplicaciones Financieras Individuales	Bloqueo Tradicional (Llamadas individuales)
Bloqueo centralizado de cuentas bancarias	Sí	Sí	Sí	No
Bloqueo de líneas telefónicas con operadores	Sí	No	No	No
Asistencia en denuncias policiales	Sí	No	No	No
Predicción de fraudes con IA	Sí	No	No	No
Integración de servicios (cuentas, SIM, etc.)	Sí	No (Línea telefónica)	No (Múltiples aplicaciones)	No
Interfaz única e intuitiva	Sí	No	No	No
Educación y tutoriales sobre seguridad	Sí	No	No	No
Actualización constante y personalizada	Sí	Limitada	Variable	No

Fuente: Elaboración propia

Capítulo V. Modelo de negocio

5.1. Lienzo del modelo de negocio

El Lienzo del Modelo de Negocio de Segurazo presenta los bloques clave que conforman la propuesta de valor y la estrategia operativa de la plataforma. Segurazo es una solución web diseñada para brindar protección inmediata y eficaz contra fraudes financieros derivados del robo o pérdida de dispositivos móviles en Perú. Su objetivo es reducir las pérdidas financieras de los usuarios y disminuir el estrés y la desconfianza en situaciones de emergencia.

La Figura 30 muestra el Lienzo del Modelo de Negocio de Segurazo, donde se detallan los nueve bloques fundamentales y sus interconexiones.

Figura 30. Lienzo modelo de negocio

Fuente: Elaboración Propia

Segurazo atiende a dos segmentos principales de clientes: los usuarios finales y las instituciones financieras y operadoras móviles. Los usuarios finales son personas que desean protegerse contra el fraude financiero y buscan una solución rápida y efectiva para bloquear cuentas bancarias y líneas móviles en caso de robo o pérdida de dispositivos. Las instituciones financieras y operadoras móviles incluyen bancos, financieras, cajas de ahorro y crédito, y operadores de telecomunicaciones interesados en garantizar la seguridad de sus clientes y reducir el riesgo de fraudes asociados.

La propuesta de valor de Segurazo se centra en ofrecer protección inmediata y eficaz, facilitando el bloqueo rápido de cuentas bancarias y líneas móviles, lo que reduce la pérdida operativa por fraude financiero. Además, busca reducir el estrés y aumentar la confianza de los usuarios al proporcionar una guía clara y accesible en situaciones de emergencia, aliviando la ansiedad. Segurazo ofrece agilidad en la respuesta mediante una interfaz intuitiva y fluida que permite acciones rápidas, esenciales en momentos críticos, y centraliza servicios al reunir en una sola plataforma las herramientas necesarias para gestionar emergencias, configuraciones de seguridad y guías prácticas.

Los canales a través de los cuales Segurazo llega a sus clientes y les proporciona valor son principalmente digitales. La plataforma web es accesible desde navegadores móviles y de escritorio, permitiendo a los usuarios interactuar con la solución en cualquier momento y lugar. Las redes sociales y la publicidad digital en medios como Facebook e Instagram se utilizan para aumentar la visibilidad y atraer usuarios. La optimización en motores de búsqueda facilita que los usuarios encuentren la plataforma cuando buscan soluciones de seguridad. Además, se establecen alianzas estratégicas con instituciones financieras y operadores móviles para promover Segurazo entre sus clientes. Estos canales apoyan la propuesta de valor al facilitar el acceso a la plataforma y garantizar que los usuarios puedan utilizar sus funcionalidades de manera rápida y eficiente.

Se buscará que las estrategias de canales maximicen la entrega de la propuesta de valor, esto se logrará mediante lo siguiente.

1. Plataforma Web Accesible:

   La aplicación web estará optimizada para navegadores en dispositivos móviles, de escritorio y tablets, asegurando una experiencia fluida y uniforme en cualquier pantalla. Se realizarán pruebas continuas de rendimiento y diseño responsivo para garantizar que todas las funcionalidades sean accesibles y fáciles de usar, independientemente del dispositivo.

2. Publicidad Digital en Redes Sociales y Motores de Búsqueda:

   En cuanto a las redes sociales, las campañas estarán segmentadas para llegar a diferentes grupos de usuarios, como individuos que buscan protección digital y empresas interesadas en seguridad financiera. Los anuncios destacarán los beneficios clave de Segurazo y se personalizarán según las necesidades de los segmentos objetivos.

   Mientras que, para los motores de búsqueda, se implementarán estrategias de optimización para posicionar a Segurazo como la principal solución en búsquedas relacionadas con fraudes financieros y pérdida de dispositivos. Esto incluye palabras clave relevantes y contenido educativo en el blog de la plataforma.

3. Análisis de Datos y Métricas:

   Se monitoreará el desempeño de los canales mediante métricas como tráfico web, conversiones y tasas de interacción en redes sociales. Esta información permitirá ajustar las estrategias para mejorar continuamente la visibilidad y la efectividad de los canales.

   En cuanto a las relaciones con los clientes se establecen y mantienen a través de atención personalizada, soporte a través de Help Desk y chatbots interactivos que proporcionan asistencia inmediata y resuelven dudas. La interacción en redes sociales permite generar contenido relevante y atender consultas y comentarios, fortaleciendo la confianza y el

compromiso de los usuarios. La retroalimentación continua permite recolectar opiniones y sugerencias para mejorar la plataforma y adaptarse a las necesidades cambiantes de los usuarios. Además, se utilizan boletines informativos y notificaciones para comunicar actualizaciones, nuevas funcionalidades y consejos de seguridad, manteniendo a los usuarios informados y comprometidos. Estas relaciones refuerzan la propuesta de valor al asegurar que los usuarios se sientan apoyados y que sus necesidades sean atendidas, fomentando la lealtad y satisfacción.

Por su lado, se buscará que las estrategias de relaciones con los clientes maximicen la entrega de la propuesta de valor, esto se logrará mediante lo siguiente.

1. Atención Personalizada con Help Desk:

   Un equipo de soporte dedicado estará disponible para proporcionar respuestas rápidas y específicas a los problemas de los usuarios, especialmente en situaciones críticas. La atención se adaptará según la urgencia del caso, priorizando según el mayor impacto financiero potencial.

2. Redes Sociales como Canales Interactivos:

   Plataformas como Facebook, Instagram y otras serán utilizadas no solo para responder preguntas, sino también para generar contenido educativo y relevante sobre seguridad digital. Las interacciones en tiempo real ayudarán a fortalecer la confianza de los usuarios y a resolver consultas de manera eficiente.

3. Soporte en Línea:

   El chatbot integrado en nuestra aplicación web responderá consultas frecuentes y proporcionarán instrucciones claras sobre el uso de la plataforma. En casos más complejos, los usuarios podrán tener la opción de conectarse con agentes humanos capacitados para atender sus necesidades.

4. Boletines Informativos y Notificaciones Personalizadas:

Segurazo mantendrá una comunicación constante con los usuarios mediante boletines y notificaciones personalizadas. Estos incluirán actualizaciones de la plataforma, alertas de seguridad, consejos prácticos y nuevos tendencias de fraude, asegurando que los usuarios estén siempre informados y comprometidos.

5. Recopilación y Uso de Retroalimentación:

   Encuestas y análisis de interacción permitirán identificar áreas de mejora y ajustar las funcionalidades de la plataforma según las expectativas de los usuarios. Esto no solo reforzará la percepción de valor, sino que también garantizará que la plataforma evolucione continuamente para satisfacer las necesidades cambiantes.

Por otro lado, para entregar la propuesta de valor, Segurazo se enfoca en actividades clave como el desarrollo y mantenimiento de la plataforma, que incluye la actualización constante de funcionalidades y seguridad para garantizar un servicio fiable y efectivo. El marketing digital y las campañas de publicidad son esenciales para aumentar la visibilidad y atraer nuevos usuarios y aliados estratégicos. El soporte técnico y el servicio al cliente proporcionan asistencia eficiente para resolver problemas y mejorar la experiencia del usuario. La creación de alianzas estratégicas con bancos, operadoras móviles y entidades gubernamentales amplía el alcance y efectividad de la plataforma. Estas actividades son fundamentales para mantener y mejorar el servicio ofrecido, asegurando que se cumpla la propuesta de valor y se satisfagan las necesidades de los clientes.

Los recursos esenciales que Segurazo necesita para operar incluyen capital financiero para financiar el desarrollo, mantenimiento y expansión de la plataforma; un equipo de desarrollo tecnológico con profesionales especializados en software y seguridad informática; propiedad intelectual que protege la innovación y tecnologías utilizadas; una solución tecnológica en la nube que garantiza la disponibilidad y escalabilidad del servicio; guías y contenidos de seguridad informática que educan y empoderan a los usuarios; y una red de

contactos y alianzas con entidades financieras y operadores de telecomunicaciones que amplían el alcance y credibilidad de la plataforma. Estos recursos permiten a Segurazo ofrecer un servicio de alta calidad y mantenerse competitivo en el mercado.

La cadena de valor de Segurazo se fortalece mediante asociaciones estratégicas con ASBANC (Asociación de Bancos del Perú), que facilita la colaboración con entidades financieras; instituciones financieras como bancos, financieras y cajas de ahorro que apoyan y promueven el uso de Segurazo entre sus clientes; operadores móviles que colaboran en la integración de servicios; y entidades gubernamentales como el Ministerio de Transportes y Comunicaciones (MTC) y la Superintendencia de Banca, Seguros y AFP (SBS) para alinearse con regulaciones y políticas de seguridad. Además, se asocian con proveedores de TI y ciberseguridad que aseguran la protección de datos sensibles y la actualización tecnológica. Estas alianzas son críticas para ampliar el alcance de Segurazo, mejorar la propuesta de valor y garantizar la sostenibilidad del modelo de negocio.

Los costos asociados al funcionamiento de Segurazo se dividen en costos fijos y variables. Los costos fijos incluyen el desarrollo y mantenimiento del aplicativo, personal administrativo y técnico, marketing digital y campañas publicitarias, y soluciones en la nube y almacenamiento. Los costos variables abarcan pasarelas de pago, mantenimiento y actualizaciones de software, y gastos asociados a la adquisición de nuevos usuarios. La gestión eficiente de estos costos es esencial para mantener la rentabilidad y asegurar la sostenibilidad financiera de la empresa.

Las fuentes de ingresos que garantizan la sostenibilidad del modelo de negocio son las suscripciones de entidades financieras y operadoras móviles, que generan ingresos recurrentes provenientes de alianzas con instituciones que ven valor en ofrecer Segurazo a sus clientes como un servicio agregado. También se generan ingresos por publicidad a través de la promoción de productos y servicios relacionados dentro de la plataforma. Además, se

ofrecen servicios premium, con funcionalidades avanzadas o personalizadas a usuarios finales dispuestos a pagar por servicios adicionales. Estas fuentes de ingresos recurrentes son fundamentales para garantizar la sostenibilidad y crecimiento a largo plazo de Segurazo.

La interconexión entre los elementos del modelo de negocio es vital para el éxito de Segurazo. La propuesta de valor está respaldada por los canales y relaciones con los clientes, que facilitan la entrega eficiente del servicio y fomentan la lealtad y satisfacción del usuario. Los canales digitales permiten un alcance amplio y una interacción inmediata, esencial en situaciones de emergencia. Las actividades clave y los recursos necesarios se alinean para mantener y mejorar la plataforma, garantizando que la propuesta de valor se cumpla consistentemente. Las alianzas estratégicas con instituciones financieras y operadores móviles no solo amplían el alcance, sino que también fortalecen la credibilidad y confianza en la plataforma.

Los ingresos recurrentes provenientes de suscripciones y publicidad aseguran la sostenibilidad financiera del modelo, permitiendo reinvertir en mejoras y expansión. La estructura de costos está diseñada para ser eficiente, enfocándose en inversiones que aporten directamente al valor ofrecido al cliente.

Para fortalecer las relaciones con las instituciones financieras y operadores móviles, Segurazo implementará estrategias como el desarrollo de alianzas estratégicas, presentando propuestas de valor específicas para cada institución y mostrando cómo Segurazo puede reducir costos asociados al fraude y mejorar la satisfacción del cliente. Se facilitará la integración técnica con las plataformas de las instituciones para mejorar la experiencia del usuario y aumentar el valor agregado. Además, se implementarán programas de co-marketing, colaborando en campañas de marketing y promoción para aumentar la adopción y uso de la plataforma entre los clientes de las instituciones. Se establecerán canales de comunicación para recibir retroalimentación de las instituciones y adaptar la plataforma a sus

necesidades específicas. Estas estrategias buscan crear relaciones mutuamente beneficiosas y sostenibles, asegurando la colaboración a largo plazo y el éxito compartido.

Segurazo contribuye al Objetivo 16 de Desarrollo Sostenible de las Naciones Unidas, que busca promover sociedades pacíficas e inclusivas. Al reducir el riesgo de fraude financiero y mejorar la seguridad de los usuarios, Segurazo ayuda a disminuir la inseguridad y fortalecer la confianza en los sistemas financieros.

5.2. Viabilidad financiera del modelo de negocio

La viabilidad financiera del modelo de negocio propuesto para prevenir el fraude financiero derivado del robo o pérdida de dispositivos móviles se sustenta a través del análisis detallado de los ingresos, costos y proyecciones financieras del proyecto. A continuación, se presenta un desglose de los principales supuestos, indicadores financieros y su análisis.

5.2.1. Inversión Inicial

La inversión abarca los gastos necesarios para el desarrollo e implementación del proyecto. Estos gastos incluyen costos registrales, derechos notariales, la implementación de la infraestructura necesaria y el desarrollo de la plataforma. En la Tabla 12 se muestra el desglose de la inversión requerida. En total la inversión inicial asciende a S/145,226.

Tabla 12. Inversión inicial

Descripción	Tipo de Gasto	Costo Total S/
Derechos Notariales	Registrales	S/683
Derechos registrales	Registrales	S/148
SUNARP	Registrales	S/30
Laptops	Activo Fijo	S/13,320
Escritorios	Activo Fijo	S/10,000
Alimentacion y materiales de oficina	Gasto	S/4,000
Hosting	Desarrollo	S/700
Compra de Licencias en la Nube	Desarrollo	S/25,790
Sueldo de Desarroladores de app	Desarrollo	S/24,000
Instagram, Face, etc	Publicidad	S/6,896
Medios	Publicidad	S/17,959
B2B	Publicidad	S/41,700
Total		S/145,226

Fuente: Elaboración Propia

5.2.2. Capital de Trabajo

El capital de trabajo es crucial para cubrir los gastos operativos iniciales (primer mes) mientras el negocio comienza a generar ingresos. La inversión en capital de trabajo asciende a S/ S/45,000, el cual se encuentra desglosado en la Tabla 13.

Tabla 13. Capital de Trabajo

Capital de Trabajo (Financiamos 3 mes de Gastos)		
Alquiler de oficina y servicios (luz, agua, internet)	S/	15,000.00
Personal administrativo (4 personas)	S/	30,000.00
Total	S/	45,000.00

Fuente: Elaboración Propia

El capital de trabajo servirá para operativizar la organización durante sus primeros meses de funcionamiento. Los gastos son el alquiler de oficina y los servicios básicos, que representan un gasto crucial para asegurar que la infraestructura física necesaria esté en su lugar para apoyar las operaciones del negocio.

El segundo componente es el costo de la mano de obra, que incluye los salarios iniciales para el personal clave del proyecto. Estos costos son esenciales para asegurar que el equipo de desarrollo y soporte esté disponible para abordar cualquier problema técnico y garantizar un lanzamiento sin problemas.

5.2.3. Proyección de Ingresos

La proyección de ingresos se basa en un análisis detallado del mercado que considera el crecimiento de la industria de la seguridad financiera en el Perú y la adopción esperada del producto.

Para la determinación del precio cobrado a las entidades financieras (clientes) se estimó el ingreso que se generaría al cobrarles a los usuarios de las entidades por nuestra solución.

En primer lugar, para determinar la demanda proyectada se utiliza como fuente:

i) La encuesta realizada por Credicorp en el Reporte de Crimen y Violencia de 2024. Según dicho informe a noviembre 2024, el 27% de la población limeña fue víctima de robo o conoce a alguien que lo fue; asimismo, el 14%, 19%, 13%, 9% y 9.1% del sector socioeconómico A, B, C, D y E, respectivamente, fue víctima de acceso a sus cuentas bancarias como resultado del robo.

ii) La proyección de población del Instituto Nacional de Estadística (INEI) en 2024, según la cual la población fue de 33.7 millones en 2023 y para el 2030 será de 35.7 millones.

iii) Proyección de la Población en edad de trabajar del Instituto Nacional de Estadística (INEI) del Informe de Estado de Población Peruana 2020.

iv) Población con acceso a smartphone e internet de la Encuesta Residencial de Servicios de Telecomunicaciones 2023.

Con dicha información se estima la siguiente evolución de la población afectada y la demanda que sería atendida por Segurazo. Ver tabla 14.

Tabla 14. Población Proyectada

Año	1	2	3	4	5
Población afectada	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	35%	45%	65%	70%	75%
Demanda de Segurazo	253,520	339,957	511,275	572,385	636,607

Fuente: Elaboración Propia

Asimismo, suponemos que al menos captaremos el 35% de la población afectada en el año 1, lo cual crecerá hasta alcanzar el 75% en el quinto año.

Para la determinación del precio que podríamos cobrarles a los usuarios, asumimos que será un precio mínimo (entre 2 a 8 soles mensuales), ya que la mayoría de los competidores o apps de seguridad son gratuitos o existen seguros de bancos como Banco de Crédito del Perú que cobran 15 soles por mes por proteger tarjetas de crédito o débito. Ver tabla 15.

Tabla 15. Ingreso Objetivo generado por Usuarios

Tipo Entidad	1	2	3	4	5
Demanda Potencial	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	35%	45%	65%	70%	75%
Demanda de Segurazo	253,520	339,957	511,275	572,385	636,607
Precio	1.80	3.81	7.35	6.56	7.95
Ingresos	456,000	1,296,000	3,756,000	3,756,000	5,064,000

Fuente: Elaboración Propia

Para determinar el porcentaje en el que se debe asignar el ingreso generado por cada tipo de entidad, el supuesto es que mientras mayor cantidad de clientes tenga una entidad, entonces mayor probabilidad que sus clientes sean parte de nuestra demanda. De esta manera, se distribuirá el ingreso según el número de clientes de cada tipo de entidad en el sistema financiero. Ver tabla 16.

Tabla 16. Distribución de Ingresos según Tipo de Entidad

Tipo Entidad	Participación en el N° de Clientes del SF
Bancos	46.40%
Financieras	21.50%
Cajas	21.80%

Fuente: Elaboración Propia

De esta manera el ingreso anual que debe generar cada tipo de entidad financiera es el siguiente:

Tabla 17. Ingresos por Tipo de Entidad

Tipo Entidad	1	2	3	4	5
Bancos	247,030	601,344	1,706,242	2,096,237	2,510,777
Financieras	114,464	278,640	790,608	971,317	1,163,399
Cajas	116,062	282,528	801,639	984,870	1,179,632

Fuente: Elaboración Propia

Se espera que la cantidad de entidades afiliados al proyecto se incremente sobre todo en el año 3, dado que se buscará el ingreso de las entidades afiliadas a la Asociación de Bancos del Perú (ASBANC). Ver tabla 18.

Tabla 18. Proyección de N° Entidades

Tipo Entidad	Año 1	Año 2	Año 3	Año 4	Año 5
Bancos	2	4	10	12	14
Financieras	2	4	8	9	9
Cajas Municipales	2	4	10	12	13
N° Entidades Financieras	6	12	28	33	36

Fuente: Elaboración Propia

De esta manera el cobro mensual a las entidades financieras se incrementará progresivamente hasta alcanzar los S/ 18.5 mil, S/ 8.5 mil y S/ 6 mil mensuales para bancos, financieras y cajas, respectivamente. Ver tabla 19.

Tabla 19. Precio por cobrar a Entidades

Tipo Entidad	Año 1	Año 2	Año 3	Año 4	Año 5
Bancos	10,293	12,528	14,219	14,557	14,945
Financieras	4,769	5,805	8,235	8,994	10,772
Cajas Municipales	4,836	5,886	6,680	6,839	7,562

Fuente: Elaboración Propia

Los ingresos mensuales llegaran a S/ 5.05 millones en el año 5 del proyecto (ver Tabla 20). Estos ingresos incluyen los generados por publicidad en la web, los cuales se empezarán a cobrar a partir del tercer año. Ver tabla 20.

Tabla 20. Evolución de Ingresos

Suscripción de entidades	477,556	1,162,512	3,298,489	4,052,424	4,853,809
Bancos	247,030	601,344	1,706,242	2,096,237	2,510,777
Financieras	114,464	278,640	790,608	971,317	1,163,399
Cajas Municipales	116,062	282,528	801,639	984,870	1,179,632
Ingreso por Publicidad			154,000	181,500	198,000
Total Ingresos	477,556	1,162,512	3,452,489	4,233,924	5,051,809

Fuente: Elaboración Propia

5.2.4. Análisis de Costos

El análisis de costos incluye tanto los costos fijos como los variables asociados con la operación del negocio. Los costos de ventas, los gastos administrativos y de ventas, y la depreciación de los activos fijos son componentes cruciales de este análisis. En la Tabla 21 se detallan los principales costos.

Los costos incluyen la implementación de ChatBot con inteligencia artificial a partir del segundo año.

Se utilizará al proveedor Open AI, según la información disponible, los costos para GPT-4 Turbo son los siguientes: tokens de entrada cuesta USD 0.01 por cada 1,000 tokens, y tokens de salida son USD 0.03 por cada 1,000 tokens[2].

Teniendo en cuenta que los usuarios ingresarán para bloquear cuentas bancarias, dispositivos y líneas telefónicas, estimamos que cada usuario necesitaría como máximo 10 consultas con 200 tokens cada uno. Así en total una interacción del usuario con el ChatBot de Segurazo costaría USD 0.02 por consulta (2000 tokens a un precio de USD 0.01 por cada 1,000 tokens) y USD 0.02 por respuesta del ChatBot (2000 tokens a un precio de USD 0.01 por cada 1,000 tokens), lo que hace un total de USD 0.04 por usuario (0.15 soles).

Asimismo, se planea que el porcentaje de usuarios que entrará mediante el ChatBot irá creciendo desde el año 2, de tal manera que el costo total por la implementación de inteligencia artificial en el ChatBot será de S/ 63,299 al quinto año. Ver tabla 21.

Tabla 21. Costos de IA en ChatBot

Año	2	3	4	5
Demanda de Segurazo	339,957	216,309	318,900	509,285
% de usuarios que entrarán por Chatbot	30%	50%	60%	80%
Costo x Unidad	0.15	0.15	0.15	0.15
Costo IA	15,094	16,007	28,318	60,299
Mantenimiento de la IA	3,000	3,000	3,000	3,000
Costo Total	18,094	19,007	31,318	63,299

Fuente: Elaboración Propia

Dado que en la estructura de costos la planilla este compuesto inicialmente por 8 personas en atención al cliente (1 es el jefe mientras que 7 son operadores telefónicos), el uso de la inteligencia artificial ayudará a eliminar progresivamente a los operadores telefónicos de apoyo.

[2] Los tokens son el número de letras que tiene una consulta.

Tabla 22. No. Operadores Telefónicos

Año	1	2	3	4	5
No. Operadores	7	5	4	3	2

Fuente: Elaboración Propia

De esta manera se ahorrará el costo por contratar menos operadores telefónicos e implementar la inteligencia artificial en el Chat Bot. Ver tabla 23.

Tabla 23. Ahorro por Implementar IA

Año	1	2	3	4	5
Gasto en Operadores Telefónicos					
Implementando Chat Bot	214,920	187,800	174,240	160,680	147,120
Sin Implementar Chat Bot	214,920	214,920	214,920	214,920	214,920
Ahorro en Operadores Telefónicos	-	27,120	40,680	54,240	67,800
Gasto por Implementar IA en Chat Bot		18,094	19,007	31,318	63,299
Ahorro		9,026	21,673	22,922	4,501

Fuente: Elaboración Propia

En consecuencia, los costos asociados a Segurazo, serán los siguientes:

Tabla 24. Evolución de Costos

Tipo de Gasto	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Implementación/Alquiler de Oficina	23,320	-	-	-	-	-
Desarrollo de plataforma app y web	50,490	-	-	-	-	-
Marketing tradicional y moderno	66,555	157,550	486,101	75,000	66,000	60,744
Alquiler y mantenimiento de servidores en Nube	-	170,400	175,001	179,726	184,578	189,562
Gasto en IA para Chat Bot	-	-	15,094	19,007	31,318	63,299
Salarios	-	214,920	187,800	174,240	160,680	147,120
Alquiler de oficina y servicios (luz, agua, internet)	-	60,000	61,620	63,284	64,992	66,747
Alimentación, materiales de oficina	4,000	12,324	12,657	12,998	13,349	13,710
Gastos Registrales	861	-	-	-	-	-
Total Gastos	145,226	615,194	938,272	524,255	520,919	541,182

Fuente: Elaboración Propia

5.2.5. Flujo de Caja

El flujo de caja proyectado se presenta en la Tabla 25, mostrando las entradas y salidas de efectivo, así como el saldo final de cada año.

Tabla 25. Flujo de caja proyectado

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ventas		477,556	1,162,512	3,452,489	4,233,924	5,051,809
Costo de ventas		-327,950	-661,102	-254,726	-250,578	-250,306
Gastos administrativos y de ventas		-287,244	-277,171	-269,529	-270,340	-290,876
Depreciación Máquina 1		-14,762	-14,762	-14,762	-14,762	-14,762
UTILIDAD OPERATIVA		-152,400	209,478	2,913,472	3,698,243	4,495,864
UTILIDAD OPERATIVA AFTER TAX (NOPAT)		-107,442	147,682	2,053,998	2,607,262	3,169,584
Depreciación Máquina 1		14,762	14,762	14,762	14,762	14,762
FCO		-92,680	162,444	2,068,760	2,622,024	3,184,346
Inversión inicial	-145,226					
FCL	-145,226	-92,680	162,444	2,068,760	2,622,024	3,184,346
Préstamo bancario	76,090	-12,463	-13,710	-15,081	-16,589	-18,248
Intereses	0	-7,609	-6,363	-4,992	-3,484	-1,825
Escudo Fiscal		2,245	1,877	1,473	1,028	538
FCF	76,090	-17,828	-18,195	-18,600	-19,045	-19,534
FCA	-69,136	-110,508	144,248	2,050,160	2,602,979	3,164,812

Fuente: Elaboración Propia

El flujo de caja operativo (FCO) muestra una tendencia creciente año tras año, comenzando con pérdida de S/ 96,680 el primer año y aumentando a S/ 3,184,346 en el quinto año. Este incremento refleja el crecimiento proyectado en las ventas y la eficiente gestión de los costos operativos.

El flujo de caja libre (FCL) después del capital de trabajo y otros ajustes iniciales también muestra una tendencia positiva, indicando la capacidad del negocio para generar efectivo suficiente para cubrir sus costos y reinvertir en el crecimiento.

Los pagos de préstamos bancarios y los intereses se reflejan en el flujo de caja libre (FCF), mostrando los montos a devolver cada año, debido a que para iniciar la empresa la deuda inicial será de S/ 76,090, ya que se plantea iniciar con una deuda del 40% de la inversión inicial total (inversión inicial y capital de trabajo del primer año es S/ 190,226). Finalmente, el flujo de caja del accionista (FCA) presenta una posición financiera sólida con incrementos significativos cada año, alcanzando S/ 3,164,812 en el quinto año.

5.2.6. Indicadores Financieros

Para evaluar la viabilidad del proyecto se utilizan los indicadores financieros mostrados en la Tabla 24: Valor Actual Neto (VAN), Tasa Interna de Retorno (TIR), Índice de Rentabilidad (IR) y Costo Promedio Ponderado de Capital (WACC). Ver tabla 26.

Tabla 26. Indicadores financieros

FCL		FCA	
WACC	14.96%	CAMP	20.23%
VAN	S/4,346,376	VAN	S/3,624,038
TIR	178.90%	TIR	227.46%
Periodo Retorno	$1.65	Periodo Retorno	$2.17

Fuente: Elaboración propia

Estos indicadores financieros muestran que el proyecto no solo es viable, sino también altamente rentable. Tanto el accionista como el proyecto tienen un VAN positivo (S/ 3,624,038 y S/ 4,346,376). Asimismo, el periodo de retorno y el WACC también reflejan la eficiencia y la solidez financiera del proyecto, asegurando que los retornos sean superiores al costo del capital, lo cual estaría creando valor al proyecto.

Cabe indicar que el TIR del proyecto es mayor a 100% tanto con los flujos de caja libre (178%) como de accionista (227%). Esto se debe a que nuestro proyecto tendrá flujos negativos en el año 1, mientras que es a partir del año 3 que, con el ingreso de las entidades afiliadas a ASBANC, recién se obtiene una madurez del proyecto que genera el incremento de los ingresos.

5.3. Escalabilidad y exponencialidad del modelo de negocio

Para esta sección se utilizará el lienzo ExO Canvas (Tabla 27), donde el Propósito de Transformación Masiva es el siguiente: “Buscamos con el uso de nuestra aplicación reducir las pérdidas por fraude financiero, esto en beneficio de nuestros clientes y usuarios”.

Tabla 27. Lienzo ExO Canvas

Elementos externos (S.C.A.L.E.)	Elementos internos (I.D.E.A.S.)
S – Empleados a demanda Se realizarán contrataciones flexibles de profesionales en seguridad cuando sea necesario para proyectos específicos.	**I – Interfaces de procesos** Se buscará que la interfaz sea intuitiva. También se automatizarán procesos internos en la coordinación con proveedores.
C – Comunidad y entorno Se utilizarán redes sociales para interactuar con los usuarios y obtener feedback. Se creará también una comunidad con usuarios que buscan estar más seguros.	**D – Tableros con información** Monitorear en tiempo real la cantidad de bloqueos, tiempos de respuesta y tendencias de robo.
A – Algoritmos Automatizar la priorización de bloqueos y recomendaciones según el tipo de robo y perfil del usuario	**E – Experimentación** Fomentar una cultura de innovación. Mantener actualizados las guías que se muestran a los usuarios. Aprendizaje de resultados del uso de la aplicación y proponer mejoras.
L – Activos externos Integrar APIs de bancos, operadoras y entidades policiales para automatizar bloqueos y denuncias.	**A – Autonomía o autoridad distribuida** Contar con equipos autónomos de desarrollo, comercial y marketing con capacidad autónoma para tomar decisiones.
E – Compromiso Se brindará atención personalizada a clientes y/o usuarios. Por otro lado, se buscará incentivar el uso de la aplicación.	**S – Tecnologías colaborativas** Utilizar Google Office o Microsoft Office, utilizando herramientas de videoconferencia y chat. Utilizar la nube para gestionar los documentos y otros archivos internos.

Fuente: Elaboración Propia

A continuación, se detallan los aspectos de algoritmos, activos externos y dashboards del ExO Canvas:

En el ámbito de algoritmos, se implementará el ChatBot para ayudar a los usuarios a bloquear sus celulares. Esto implicará la contratación de inteligencia artificial (como Open AI) y sus algoritmos los cuales permitirán reducir costos, ya que se prescindirá de los operadores telefónicos. De esta manera se generará un ahorro de S/ 58,121[3]. Ver Tabla 23.

En el ámbito de activos externos se buscará la integración con APIs (interfaces de

[3] El coste de la implementación de la herramienta se encuentra en la sección 5.2.4. Análisis de Costos.

programación) de bancos, operadoras telefónicas y entidades policiales para que los usuarios puedan bloquear rápidamente sus cuentas, su línea y su dispositivo sin necesidad de comunicarse con cada entidad individualmente. La idea es llegar a tener una web en donde el afectado por robo ingrese su DNI y automáticamente se pueda bloquear tanto cuentas bancarias, como teléfonos y líneas telefónicas.

Para ello, se requerirá negociar acuerdos con estas entidades, lo que puede implicar costos administrativos. Además, algunas empresas cobran por el uso de sus APIs, lo que genera un costo recurrente cada vez que se ejecuta una solicitud de bloqueo. También se deben cumplir regulaciones de seguridad y privacidad, lo que podría implicar auditorías y certificaciones con costos adicionales.

Para reducir estos costos, Segurazo puede utilizar APIs estandarizadas que faciliten la conexión con múltiples bancos y operadoras sin necesidad de desarrollar integraciones personalizadas para cada entidad.

En el ámbito del dashboards (paneles de control), se desarrollará uno para monitorear el funcionamiento del servicio en tiempo real. Estos dashboards permitirán visualizar información clave como el número de bloqueos realizados, tiempos de respuesta y patrones de actividad fraudulenta.

El desarrollo de dashboards requiere programadores y diseñadores especializados en visualización de datos. Además, se necesita infraestructura en la nube para almacenar y analizar grandes volúmenes de información (Big Data).

Para reducir dichos costos, Segurazo puede usar herramientas de análisis de datos ya existentes como Google Data Studio o Power BI, en lugar de desarrollar un sistema propio desde cero. También puede implementar reportes automáticos que analicen la información sin necesidad de intervención humana, lo que minimiza los costos de operación y mantenimiento.

5.4.Sostenibilidad social del modelo de negocio

El modelo de negocio de Segurazo está firmemente alineado con la meta 16.4 de los Objetivos de Desarrollo Sostenible (ODS), que busca reducir los flujos financieros ilícitos y mejorar la recuperación de bienes robados. Segurazo responde a este desafío ofreciendo una solución tecnológica que protege a los usuarios de los riesgos financieros derivados del robo de dispositivos móviles, mitigando las pérdidas económicas y fortaleciendo la confianza en las instituciones financieras.

En cuanto a su impacto social, la contribución principal de Segurazo radica en su capacidad para limitar los flujos financieros ilícitos, bloqueando cuentas bancarias y líneas móviles inmediatamente después de un robo. Esto ayuda a reducir el acceso no autorizado a los fondos de las víctimas, protegiendo sus bienes y contribuyendo a un entorno más seguro para las transacciones digitales. Esta herramienta beneficia tanto a los usuarios como a las instituciones financieras, generando un entorno de mayor confianza y seguridad en el sistema financiero.

En términos de inclusión y equidad, Segurazo ha sido diseñado para ser accesible a personas de diferentes niveles socioeconómicos, asegurando que tanto los sectores más vulnerables como aquellos con mayor poder adquisitivo puedan beneficiarse de la protección financiera que ofrece. La interfaz intuitiva de la plataforma web facilita su uso, incluso para personas con diferentes grados de alfabetización tecnológica, promoviendo la equidad en el acceso a soluciones de seguridad financiera.

Con respecto a la contribución al ODS 16.4, al limitar los flujos financieros ilícitos y facilitar la protección y recuperación de bienes robados, Segurazo se posiciona como una herramienta clave en la consecución de esta meta. Su capacidad para bloquear cuentas bancarias y dispositivos en tiempo real minimiza las oportunidades para el fraude,

protegiendo los activos financieros de los usuarios y fortaleciendo la seguridad del sistema financiero.

Finalmente, cabe indicar que las métricas utilizadas para hallar el beneficio social que genera “Segurazo” serán presentadas en el capítulo 7, junto a las estimaciones del VAN social.

5.5. Conclusión

El análisis detallado del modelo de negocio y la viabilidad financiera de Segurazo confirma su potencial como una solución escalable, sostenible y altamente rentable para mitigar riesgos financieros derivados del robo de dispositivos móviles. La combinación de una sólida propuesta de valor, ingresos recurrentes, y un enfoque en sostenibilidad social alineado con los Objetivos de Desarrollo Sostenible, posiciona a Segurazo como una herramienta clave para fortalecer la confianza en el sistema financiero.

Desde el punto de vista financiero, los indicadores positivos, como el VAN, TIR y flujo de caja, garantizan la capacidad del negocio para cubrir costos operativos, reinvertir en innovación y generar retornos significativos para los accionistas. La estrategia a largo plazo se enfocará en optimizar la estructura de costos mediante la implementación de equipos flexibles de desarrollo y soporte, así como en la diversificación de los ingresos, ampliando la base de clientes y explorando nuevos modelos de negocio, como servicios premium y alianzas con entidades financieras más pequeñas.

La inclusión de métricas sociales en la evaluación del modelo de negocio asegurará que el proyecto continúe cumpliendo con sus objetivos de reducir flujos financieros ilícitos y fortalecer la seguridad del sistema financiero. Estas métricas también permitirán identificar áreas de mejora para adaptar la plataforma a las necesidades cambiantes de los usuarios, maximizando su alcance e impacto social.

Los resultados financieros y sociales se enfocarán en crecimiento, sostenibilidad y reputación. Se priorizará la expansión en nuevos mercados y sectores clave, fortaleciendo alianzas con entidades financieras y operadores móviles. Para garantizar la sostenibilidad, se optimizarán costos operativos y se escalará el servicio sin afectar su calidad. Finalmente, el impacto social consolidará la reputación de Segurazo como un referente en seguridad financiera, generando confianza en clientes y socios estratégicos.

Adicionalmente, en una etapa de maduración del negocio, se implementará un sistema de gestión de calidad alineado con la norma ISO/IEC 29110, orientada a organizaciones de desarrollo de software de tamaño muy pequeño, con el fin de estandarizar y optimizar los procesos de construcción y mejora de Segurazo. Asimismo, se proyecta avanzar hacia la certificación ISO/IEC 27001 para fortalecer la gestión de la seguridad de la información y garantizar la protección de los datos sensibles de los usuarios. Estas certificaciones reforzarán la confianza de clientes y aliados estratégicos, consolidando la reputación de Segurazo como una solución tecnológica segura y confiable.

Capítulo VI. Solución Deseable Factible y Viable

En este capítulo se buscará minimizar los riesgos asociados al proyecto mediante una evaluación exhaustiva de las hipótesis clave del modelo de negocio propuesto. Para ello, se realizará un análisis detallado de las hipótesis vinculadas a los bloques de deseabilidad, factibilidad y viabilidad, asegurando que cada aspecto del modelo sea validado antes de proceder con su implementación. Esta etapa es crucial, ya que permite identificar posibles fallas, ajustar estrategias y confirmar la solidez de la solución diseñada para abordar el problema identificado. De esta manera, se garantiza una base sólida y bien fundamentada para el desarrollo efectivo del proyecto, minimizando obstáculos durante su ejecución y asegurando la sostenibilidad de la propuesta a largo plazo.

6.1. Validación de la Deseabilidad de la Solución

6.1.1. Hipótesis para validar la deseabilidad de la solución

El primer paso consistió en identificar las hipótesis presentes en todos los cuadrantes del modelo de negocio (ver Tabla 28).

Tabla 28. Hipótesis del BMC

TIPO DE HIPÓTESIS	HIPÓTESIS BUSINESS MODEL CANVAS
Deseabilidad	H1: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo “Segurazo” en situaciones de robo.
Deseabilidad	H2: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.
Deseabilidad	H3: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su operador telefónico en situaciones simuladas de robo de dispositivo, facilitando el bloqueo de sus líneas telefónicas para prevenir la suplantación de su número o la copia de su IMEI.

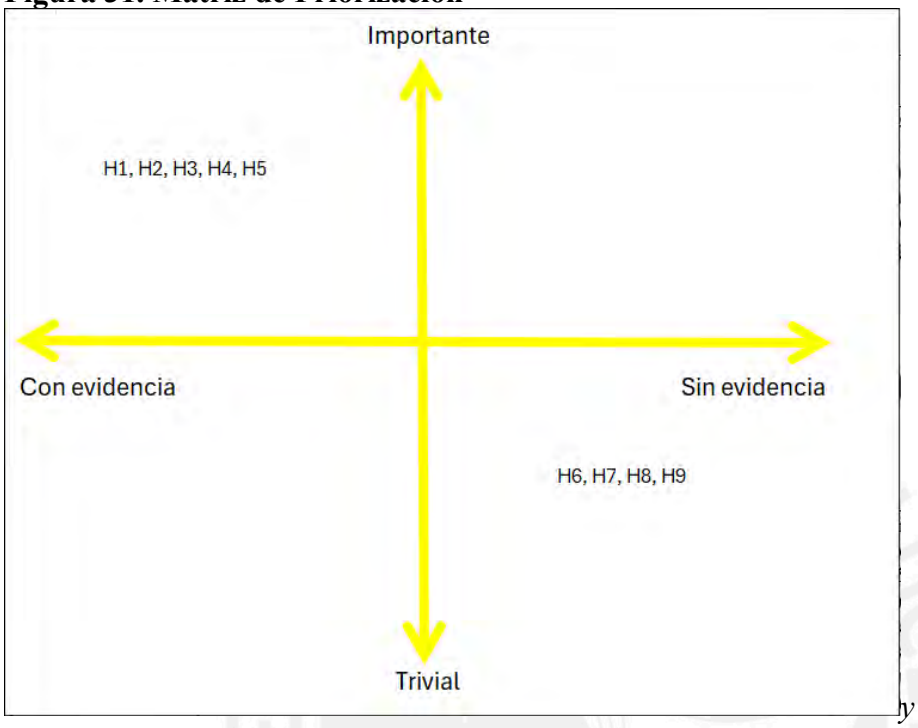
Deseabilidad	H4: Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán "Segurazo" para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.
Deseabilidad	H5: Creemos que los ciudadanos de 18 a 65 años a nivel nacional realizarán denuncias policiales a través del asistente virtual "Segurazo" en situaciones simuladas en las cuales les roben el celular y requieran realizar una denuncia ante una autoridad.
Deseabilidad	H6: Creemos que los ciudadanos entre 18 a 65 años a nivel nacional accederán a la web Segurazo en los primeros dos años del proyecto. (Trivial – sin evidencia).
Deseabilidad	H7: Creemos que el 70% de las instituciones financieras a nivel nacional preferirán nuestra solución frente a la competencia**."** (Trivial – sin evidencia).
Deseabilidad	H8: Creemos que los ciudadanos entre 18 a 65 años a nivel nacional utilizarán la funcionalidad de protección de datos tras un robo de celular. (Trivial – sin evidencia).
Deseabilidad	H9: Creemos que necesitamos como recursos claves a un equipo de desarrollo de software. (Trivial – sin evidencia).
Factibilidad	H10: Creemos que la relación VTVC/CAC será mayor a 7 y menor a 9 soles de beneficio por cada sol invertido en estrategias de retención de clientes en Segurazo. (Importante – sin evidencia).
Viabilidad	H11: Creemos que la propuesta de negocio “Segurazo” será rentable porque obtendrá ganancias por US $1 '000,000 al quinto año de iniciar operaciones. (Importante – sin evidencia).

Fuente: Elaboración Propia

Posteriormente, debido a la limitación de recursos y tiempo, organizamos las hipótesis en una matriz de priorización. El objetivo fue enfocarnos en las hipótesis más relevantes que

aún no cuentan con evidencia suficiente. Para ello, será necesario realizar experimentos que permitan validarlas. En la Figura 31 se presenta la matriz de priorización utilizada.

Figura 31. Matriz de Priorización



Fuente: Elaboración Propia

De esta forma se identificó las hipótesis de deseabilidad las cuales se procederán a validar. Ver Tabla 29.

Tabla 29. Listado de hipótesis de deseabilidad priorizadas

HIPÓTESIS BUSINESS MODEL CANVAS
H1: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo Segurazo en situaciones de robo, validado mediante pruebas de usabilidad que demuestren su efectividad y aceptación.
H2: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.
H3: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su operador telefónico en situaciones simuladas de robo de dispositivo, facilitando el bloqueo de sus líneas telefónicas para prevenir la suplantación de su número o la copia de su IMEI.
H4: Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán "Segurazo" para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.
H5: Creemos que los ciudadanos de 18 a 65 años a nivel nacional realizarán denuncias policiales a través del asistente virtual "Segurazo" en situaciones simuladas en las cuales les roben el celular y requieran realizar una denuncia ante una autoridad.

Fuente: Elaboración Propia

Detalle de las pruebas, métricas y criterios de aceptación a utilizar:

Tabla 30. Hipótesis 1

HIPÓTESIS	TIPO DE PRUEBA	DETALLE DE LA PRUEBA	MÉTRICAS	CRITERIOS DE ACEPTACIÓN
H1: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo Segurazo en situaciones de robo, validado mediante pruebas de usabilidad que demuestren su efectividad y aceptación.	Se realizarán pruebas de usabilidad basadas en tareas definidas y escenarios simulados para validar la hipótesis. En relación con el porcentaje de éxito, dado que se trata de una simulación inicial, se utilizará la escala SUS (System Usability Scale), considerando como aceptable un puntaje igual o superior a 68%. En cuanto al tiempo promedio necesario para completar una rutina, se tomará como referencia el tiempo estimado para realizar una llamada a una entidad, el cual, según observaciones, es de aproximadamente 2 minutos, más 1 minuto adicional para el registro, resultando en un tiempo total esperado de 3 minutos para la prueba.	**Tareas Específicas:** 1. Simulación de acceso a la plataforma 'Segurazo': -El usuario ingresa al sitio web o abre la aplicación móvil de 'Segurazo'. 2. Simulación del registro de información personal y servicios: 3. El usuario introduce los datos de sus bancos, dispositivos móviles y proveedor de servicios telefónicos. 4. Simulación de navegación hacia la sección de gestión financiera: -El usuario accede a la sección destinada a la administración de entidades financieras dentro de 'Segurazo'. 5. Simulación de selección de una entidad financiera: -El usuario selecciona su banco o institución financiera desde una lista desplegable disponible en la plataforma. 6. Simulación del inicio del proceso de bloqueo: -El usuario elige entre realizar una llamada a su entidad financiera o utilizar una función de la aplicación para bloquear su tarjeta. Simulación de confirmación del bloqueo exitoso: El usuario marca una casilla que confirma la finalización exitosa del proceso de bloqueo de la entidad financiera.	**1.Porcentaje de Éxito en la Compleción de Tareas Específicas** -Porcentaje de usuarios que completan cada una de las funciones clave sin errores ni asistencia adicional. **2.Tiempo Necesario para Completar Cada Tarea** -Tiempo promedio que tardan los usuarios en completar cada una de las funciones clave.	**1.Aceptación**: >68% de los usuarios completan exitosamente cada función clave sin errores. **2.Aceptación**: Si el tiempo promedio para completar cada tarea es igual o menor al estándar establecido en aplicaciones similares de seguridad. Por ejemplo, completar el proceso de llamada a entidad financiera para el bloqueo en menos de 4 minutos.

Fuente: Elaboración Propia

Tabla 31. Hipótesis 2

HIPÓTESIS	TIPO DE PRUEBA	DETALLE DE LA PRUEBA	MÉTRICAS	CRITERIOS DE ACEPTACIÓN
H2: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.	Se llevarán a cabo pruebas de usabilidad que incluyen tareas específicas y escenarios de simulación para evaluar la hipótesis. Respecto al porcentaje de éxito y debido a que esta es una simulación inicial se tomará en cuenta la escala SUS con un valor aceptable >=68%. Respecto al tiempo promedio en completar una rutina se tomará en cuenta el tiempo promedio en completar un proceso de llamada a una entidad el cual según notas de observación está en 02 minutos + 01 minuto en registro la prueba total debe ser en 03 minutos.	**Tareas Específicas:** 1.Simular ingresar a la plataforma 'Segurazo': -El usuario accede al sitio web o aplicación móvil de 'Segurazo'. 2.Simular el registro de sus entidades financieras, dispositivos y operador: -El usuario introduce información sobre sus bancos, dispositivos móviles y proveedor de telefonía. 3.Simular ingresar a la sección de entidades financieras: -El usuario navega hasta la sección específica para gestión de entidades financieras dentro de 'Segurazo'. 4.Simular seleccionar su entidad financiera: -El usuario elige su banco o institución financiera de una lista desplegable. 5.Simular iniciar el proceso de bloqueo: -El usuario opta por llamar a la entidad financiera o utiliza una función dentro de la aplicación para bloquear su tarjeta. 6.Simular confirmar la finalización del bloqueo: -El usuario hace clic en la casilla que indica que ha completado la tarea de bloqueo de entidades financieras.	**1.Porcentaje de Éxito en la Compleción de Tareas Específicas** -Porcentaje de usuarios que completan cada una de las funciones clave sin errores ni asistencia adicional. **2.Tiempo Necesario para Completar Cada Tarea** -Tiempo promedio que tardan los usuarios en completar cada una de las funciones clave.	**1.Aceptación**: >68% de los usuarios completan exitosamente cada función clave sin errores. **2.Aceptación**: Si el tiempo promedio para completar cada tarea es igual o menor al estándar establecido en aplicaciones similares de seguridad. Por ejemplo, completar el proceso de llamada a entidad financiera para el bloqueo en menos de 4 minutos.

Fuente: Elaboración Propia

Tabla 32. Hipótesis 3

HIPÓTESIS	TIPO DE PRUEBA	DETALLE DE LA PRUEBA	MÉTRICAS	CRITERIOS DE ACEPTACIÓN
H3: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su operador telefónico en situaciones simuladas de robo de dispositivo, facilitando el bloqueo de sus líneas telefónicas para prevenir la suplantación de su número o la copia de su IMEI.	Se llevarán a cabo pruebas de usabilidad que incluyen tareas específicas y escenarios de simulación para evaluar la hipótesis. Respecto al porcentaje de éxito y debido a que esta es una simulación inicial se tomará en cuenta la escala SUS con un valor aceptable >=68%. Respecto al tiempo promedio en completar una rutina se tomará en cuenta el tiempo promedio en completar un proceso de bloqueo de líneas celulares el cual según notas de observación está en 02 minutos.	**Tareas Específicas:** 1.Simular ingresar a la web o aplicación del asistente virtual 'Segurazo'. 2. Simular el registro de datos iniciales (información personal y detalles del operador telefónico). 3. Simular el lanzamiento de la llamada telefónica al operador telefónico. 4. Simular el contacto con el área de bloqueo del operador telefónico. 5. Terminar el registro de la operación de llamada. 6. Verificar que la tarea esté completada a través del menú principal.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Descripción: Porcentaje de usuarios que completan todas las tareas sin errores ni asistencia adicional. **2.Tiempo Necesario para Completar el Proceso de Bloqueo** -Descripción: Tiempo promedio que tardan los usuarios en completar todas las tareas relacionadas con el bloqueo de la línea telefónica.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Aceptación: Si es >=68% de los usuarios completan todas las tareas sin errores. **2.Tiempo Promedio para Completar el Proceso** -Aceptación: Si el tiempo promedio para completar el proceso es igual o menor a 2 minutos.

Fuente: Elaboración Propia

Tabla 33. Hipótesis 4

HIPÓTESIS	TIPO DE PRUEBA	DETALLE DE LA PRUEBA	MÉTRICAS	CRITERIOS DE ACEPTACIÓN
H4: Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán "Segurazo" para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.	Se llevarán a cabo pruebas de usabilidad que incluyen tareas específicas y escenarios de simulación para evaluar la hipótesis. Respecto al porcentaje de éxito y debido a que esta es una simulación inicial se tomará en cuenta la escala SUS con un valor aceptable >=68%. Respecto al tiempo promedio en completar una rutina se tomará en cuenta el tiempo promedio en completar un proceso de ajuste de parámetros de seguridad el cual según notas de observación está en 10 minutos.	**Tareas Específicas:** 1.Simular ingresar a la web o aplicación de 'Segurazo'. 2. Simular el registro de sus entidades financieras, dispositivos y operador. 3. Simular ingresar a la sección de dispositivos. 4. Simular seleccionar su dispositivo. 5. Simular seguir los pasos de la web de Google o iCloud para ajustar la seguridad (ejemplo: bloqueo remoto, borrado de datos). 6. Simular hacer clic en la casilla para indicar que completó la tarea de ajuste de seguridad de dispositivos.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Descripción: Porcentaje de usuarios que completan todas las tareas sin errores ni asistencia adicional. **2. Tiempo Necesario para Completar el Ajuste de Seguridad** -Descripción: Tiempo promedio que tardan los usuarios en completar todas las tareas relacionadas con el ajuste de seguridad del dispositivo.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Aceptación: Si >= 68% de los usuarios completan todas las tareas sin errores. **2.Tiempo Promedio para Completar el Proceso** -Aceptación: Si el tiempo promedio para completar el proceso es igual o menor a 10 minutos.

Fuente: Elaboración Propia

Tabla 34. Hipótesis 5

HIPÓTESIS	TIPO DE PRUEBA	DETALLE DE LA PRUEBA	MÉTRICAS	CRITERIOS DE ACEPTACIÓN
H5: Creemos que los ciudadanos de 18 a 65 años a nivel nacional realizarán denuncias policiales a través del asistente virtual "Segurazo" en situaciones simuladas en las cuales les roben el celular y requieran realizar una denuncia ante una autoridad.	Se llevarán a cabo pruebas de usabilidad que incluyen tareas específicas y escenarios de simulación para evaluar la hipótesis. Respecto al porcentaje de éxito y debido a que esta es una simulación inicial se tomará Se tomará en cuenta la escala SUS con un valor aceptable >=68%. Respecto al tiempo promedio en completar una rutina se tomará en cuenta el tiempo promedio en completar un proceso de de denuncia policial el cual según notas de observación está en 30 minutos vía telefónica (dependiendo del distrito y comisaria)	**Tareas Específicas:** 1.Simular ingresar a la web o aplicación de 'Segurazo'. 2. Simular realizar una denuncia digital ante la Policía Nacional del Perú (PNP). 3. Simular el lanzamiento de la llamada al 105 (número de emergencias). 4. Simular ubicar una comisaría cercana. 5. Verificar que la tarea esté completada en el menú principal.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Descripción: Porcentaje de usuarios que completan todas las tareas sin errores ni asistencia adicional. **2. Tiempo Necesario para Completar el Proceso de Denuncia** -Descripción: Tiempo promedio que tardan los usuarios en completar todas las tareas relacionadas con la realización de la denuncia.	**1.Porcentaje de Éxito en la Compleción de Tareas** -Aceptación: Si >= 68% de los usuarios completan todas las tareas sin errores.**2. Tiempo Promedio para Completar el Proceso** -Aceptación: Si el tiempo promedio para completar el proceso es igual o menor a 30 minutos.

Fuente: Elaboración Propia

6.1.2. Experimentos empleados para validar la deseabilidad de la solución

A continuación, se realizaron diversas pruebas considerando las métricas y criterios de aceptación definidos anteriormente. Cabe indicar que el número de personas que realizaron la validación fue 20.

En el siguiente link se encuentran las evidencias, en este caso grabaciones de las entrevistas realizas a cada uno de los usuarios que participaron en las pruebas de usabilidad.

Apéndice A: Pruebas de Usabilidad

Evidencias pruebas de usabilidad de hipótesis

Hipótesis 1 (H1): Métrica 1. Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo Segurazo en situaciones de robo, validado mediante pruebas de usabilidad que demuestren su efectividad y aceptación.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo, se realizaron dos pruebas de usabilidad con 20 usuarios. Cada prueba evaluó una métrica clave: el porcentaje de éxito en la compleción de tareas específicas y el tiempo necesario para completar cada tarea. Los resultados obtenidos permitieron confirmar la hipótesis de negocio. Ver Tabla 35.

Tabla 35. Porcentaje de éxito en la compleción de tareas específicas

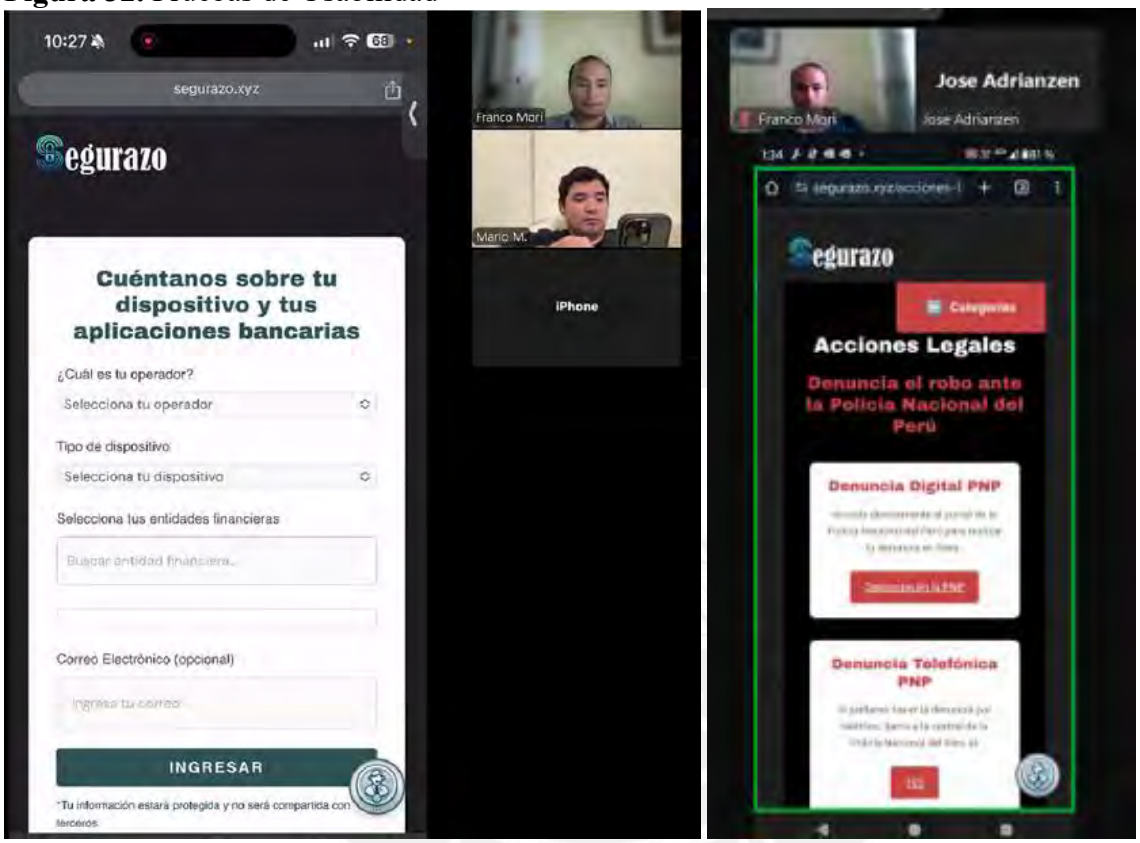
Pasos en el uso del aplicativo "Segurazo"	Cumplimiento (%)	Cumple con el requisito (≥68%)
Simulación de acceso a la plataforma 'Segurazo'	95%	
Simulación del registro de información personal y servicios:	95%	
Simulación de navegación hacia la sección de gestión financiera:	95%	
Simulación de selección de una entidad financiera:	95%	

Simulación del inicio del proceso de bloqueo:	95%	
Simulación de confirmación del bloqueo exitoso:	95%	
Cumplimiento promedio de las tareas en 20 usuarios	95%	Si

Fuente: Elaboración Propia

A continuación, algunas imágenes de las pruebas de usabilidad.

Figura 32. Pruebas de Usabilidad



Fuente: Elaboración propia

Se realizaron dos pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional pueden usar fácilmente el aplicativo **Segurazo** en situaciones de robo. Según los resultados obtenidos, el 95% de los usuarios completaron las tareas requeridas sin errores ni necesidad de asistencia adicional, superando el criterio de aceptación establecido de ≥68%. Estas tareas incluyeron el acceso a la plataforma, el registro de información personal, la navegación hacia módulos específicos, la selección de entidades financieras, y el inicio y confirmación del bloqueo de cuentas. Los

resultados confirman que el aplicativo es altamente intuitivo y fácil de usar, validando su deseabilidad y funcionalidad.

Durante las pruebas, los usuarios comentaron que las opciones disponibles en el aplicativo son intuitivas y están bien organizadas, lo que facilita su uso incluso para personas con niveles básicos de experiencia tecnológica. En general, describieron a **Segurazo** como una herramienta con mucho potencial para ayudar a muchas personas en situaciones críticas, como el robo de dispositivos. La disposición de las opciones recibió comentarios positivos, ya que fue percibida como lógica y fácil de seguir, por lo que todos los usuarios pudieron concretar todas las opciones disponibles sin impedimento.

Sin embargo, también se identificaron oportunidades de mejora. Algunos usuarios sugirieron que las opciones deberían estar numeradas para facilitar su comprensión y navegación, especialmente en las secciones de denuncias. Además, se reportó que la funcionalidad de transferencia hacia **Interbank** no estaba operativa durante las pruebas, lo que representa un punto clave a solucionar en futuras iteraciones. Estas observaciones proporcionan una valiosa retroalimentación para mejorar aún más la experiencia del usuario y garantizar una operatividad fluida.

Los resultados demuestran que **Segurazo** es una aplicación intuitiva y funcional que tiene un alto potencial para asistir a los usuarios en situaciones de robo. La incorporación de las oportunidades de mejora identificadas fortalecerá su propuesta de valor, permitiendo que se consolide como una solución líder en el mercado de seguridad digital.

Hipótesis 1 (H1): Métrica 2. Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo Segurazo en situaciones de robo, validado mediante pruebas de usabilidad que demuestren su efectividad y aceptación.

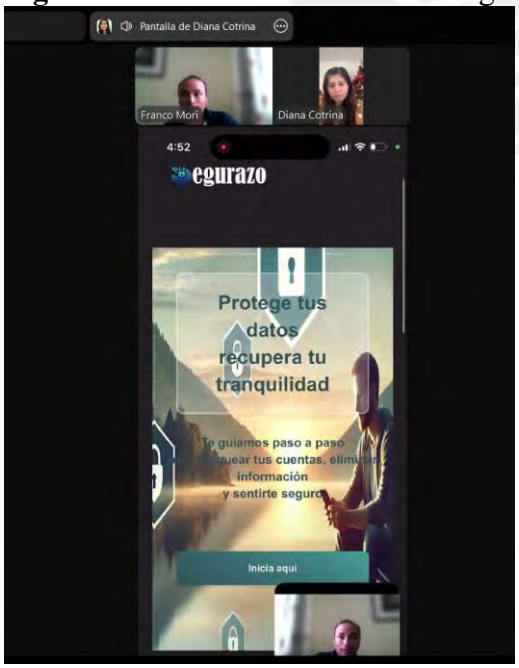
Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo, se realizaron dos pruebas de usabilidad con 20 usuarios. Cada prueba evaluó una métrica clave: el porcentaje de éxito en la compleción de tareas específicas y el tiempo necesario para completar cada tarea. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 36. Pasos en el uso del aplicativo Segurazo

Pasos en el uso del aplicativo "Segurazo"	Tiempo promedio (min)	Cumple con el requisito (≤4 min)
Simulación de acceso a la plataforma 'Segurazo'	0.45	
Simulación del registro de información personal y servicios:	0.42	
Simulación de navegación hacia la sección de gestión financiera:	0.53	
Simulación de selección de una entidad financiera:	0.38	
Simulación del inicio del proceso de bloqueo:	0.5	
Simulación de confirmación del bloqueo exitoso:	0.29	
Tiempo total promedio de uso en 20 usuarios	2.57	Si

Fuente: Elaboración Propia

Figura 33. Pruebas de Usabilidad Segurazo



Fuente: Elaboración Propia

Se llevaron a cabo pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional pueden usar fácilmente el aplicativo **Segurazo** en situaciones de robo. Las pruebas evaluaron el tiempo promedio necesario para completar tareas específicas dentro del aplicativo, considerando un umbral máximo de aceptación de ≤4 minutos. Según los resultados mostrados en la Tabla 36, los usuarios completaron todas las tareas en un tiempo promedio total de 2.57 minutos, confirmando que la solución es eficiente y cumple con los estándares de usabilidad establecidos.

Entre las tareas evaluadas estuvieron: el acceso a la plataforma, el registro de información personal, la navegación hacia la sección de gestión financiera, la selección de una entidad financiera, el inicio del proceso de bloqueo, y la confirmación del bloqueo exitoso. Cada tarea fue realizada de manera fluida y dentro del tiempo esperado, destacando que el uso completo del aplicativo tomó menos de 3 minutos en promedio, lo que refuerza su facilidad de uso. Los usuarios describieron la experiencia como altamente intuitiva y destacaron que no hay actualmente una herramienta similar en el mercado que ofrezca estas funcionalidades.

El feedback de los usuarios incluyó comentarios positivos sobre la utilidad del aplicativo, así como sugerencias para mejoras. Entre las recomendaciones principales se sugirió incorporar un botón para regresar al inicio en cualquier momento, trabajar en la interfaz gráfica para que las opciones sean visualmente más atractivas, y proporcionar un contexto más claro en la página inicial, indicando que se brindan enlaces seguros a las entidades financieras. Asimismo, se destacó la importancia de incluir un mensaje que garantice que la página no almacena información personal del usuario, con el fin de generar mayor confianza y seguridad al navegar en el aplicativo.

Los resultados obtenidos validan que **Segurazo** es un aplicativo rápido, eficiente e intuitivo, cumpliendo con los objetivos de deseabilidad y facilidad de uso. Las recomendaciones proporcionadas representan oportunidades clave para optimizar aún más la experiencia del usuario y fortalecer la confianza en la herramienta.

Hipótesis 2 (H2): Métrica 3. Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual Segurazo para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo, se realizaron dos pruebas de usabilidad con 20 usuarios. Cada prueba evaluó una métrica clave: el porcentaje de éxito en la compleción de tareas específicas y el tiempo necesario para completar cada tarea. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 37. Porcentaje de éxito en la compleción de tareas específicas

Pasos en el uso del aplicativo "Segurazo"	**Cumplimiento (%)**	**Cumple con el requisito (≥68%)**
Simular ingresar a la plataforma "Segurazo"	98%	
Simular el registro de entidades financieras, dispositivos y operador	95%	
Simular ingresar a la sección de entidades financieras	97%	
Simular seleccionar su entidad financiera	96%	
Simular iniciar el proceso de bloqueo	94%	
Simular confirmar la finalización del bloqueo	99%	
Cumplimiento promedio de las tareas en 20 usuarios		
	96,5%	Si

Fuente: Elaboración Propia

Se llevaron a cabo dos pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional podrán utilizar el asistente virtual Segurazo para contactar a su banco y gestionar el bloqueo de sus tarjetas en caso de pérdida o robo de su dispositivo celular. Los resultados demostraron que el 96.5% de los usuarios completaron todas las tareas requeridas sin errores ni necesidad de asistencia adicional, superando ampliamente el umbral de aceptación establecido de ≥68%, como se observa en la Tabla 37.

Entre las tareas evaluadas estuvieron: ingreso a la plataforma, registro de entidades financieras, dispositivos y operador, navegación hacia la sección de entidades financieras, selección de su entidad, inicio del proceso de bloqueo y confirmación de la finalización del bloqueo. Todas estas tareas mostraron altos porcentajes de cumplimiento, con un promedio de 96.5%, lo que valida que el aplicativo es intuitivo y funcional en su objetivo principal de proteger las cuentas financieras de los usuarios.

Los comentarios de los participantes fueron positivos en su mayoría. Los usuarios mencionaron que pudieron completar todas las tareas exitosamente sin inconvenientes, destacando la facilidad de uso y la utilidad de la aplicación. Sin embargo, también se identificó una oportunidad de mejora, como la incorporación de una función adicional que permita gestionar el bloqueo a través de aplicaciones de transferencia como Plin, lo que podría ampliar el alcance y funcionalidad del aplicativo.

Los resultados obtenidos no solo validan la deseabilidad del asistente virtual Segurazo, sino que también refuerzan su capacidad para asistir a los usuarios de manera eficiente en situaciones críticas. Las mejoras propuestas, como la integración de nuevas funciones, permitirán fortalecer aún más la experiencia del usuario y consolidar la solución como líder en seguridad financiera digital.

Hipótesis 2 (H2): Métrica 4. Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual Segurazo para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.

Para validar esta hipótesis de deseabilidad, se realizaron pruebas de usabilidad con 20 usuarios dentro del rango de edad de 18 a 65 años. Cada usuario fue instruido para completar una serie de tareas específicas en el aplicativo Segurazo en una situación simulada de robo. Las pruebas se centraron en evaluar la facilidad y eficiencia del proceso de contacto con el banco y el bloqueo de tarjetas mediante el asistente virtual. A continuación, se presentan los resultados obtenidos.

Tabla 38. Pasos en el uso del aplicativo Segurazo

Pasos en el uso del aplicativo "Segurazo"	Tiempo promedio (min)	Cumple con el requisito (≤4 min)
Simular ingresar a la plataforma "Segurazo"	0.55	
Simular el registro de entidades financieras, dispositivos y operador	0.82	
Simular ingresar a la sección de entidades financieras	0.63	
Simular seleccionar su entidad financiera	0.48	
Simular iniciar el proceso de bloqueo	0.7	
Simular confirmar la finalización del bloqueo	0.39	
Tiempo total promedio de uso en 20 usuarios	3.57	Si

Fuente: Elaboración Propia

El tiempo promedio de uso del aplicativo fue de 3.57 minutos (ver Tabla 38), encontrándose dentro del umbral aceptable de tiempo de navegación. Estos resultados indican que Segurazo permite a los usuarios completar el proceso de contacto y bloqueo de tarjetas de manera eficiente, validando la hipótesis de usabilidad en tiempos de emergencia.

Hipótesis 3 (H3): Métrica 5. Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual “Segurazo” para contactar a su operador telefónico en situaciones simuladas de robo de dispositivo, facilitando el bloqueo de sus líneas telefónicas para prevenir la suplantación de su número o la copia de su IMEI.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual “Segurazo”, se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave: el porcentaje de éxito en la compleción de tareas del proceso de bloqueo telefónico. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 39. Porcentaje de éxito en el proceso de bloqueo telefónico

Pasos en el uso del aplicativo "Segurazo"	**Cumplimiento (%)**	**Cumple con el requisito (≥68%)**
Simular ingresar a la web o aplicación del asistente virtual 'Segurazo'.	97%	
Simular el registro de datos iniciales (información personal y detalles del operador telefónico).	95%	
Simular el lanzamiento de la llamada telefónica al operador telefónico.	98%	
Simular el contacto con el área de bloqueo del operador telefónico.	96%	
Terminar el registro de la operación de llamada.	94%	
Verificar que la tarea esté completada a través del menú principal.	99%	
Cumplimiento promedio de las tareas en 20 usuarios	96,5%	Si

Fuente: Elaboración Propia

Se llevaron a cabo pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual **Segurazo** para contactar a su operador telefónico y facilitar el bloqueo de sus líneas telefónicas en situaciones simuladas de robo. Los resultados indicaron que el 96.5% de los usuarios completaron exitosamente todas las tareas evaluadas sin errores ni necesidad de asistencia

adicional, superando el criterio de aceptación establecido de ≥68%, como se detalla en la Tabla 39.

Las tareas evaluadas incluyeron ingresar al aplicativo, registrar datos iniciales (información personal y detalles del operador telefónico), lanzar la llamada al operador, contactar el área de bloqueo, completar la operación y verificar el éxito de la tarea en el menú principal. Los altos porcentajes de cumplimiento en cada tarea destacan la facilidad de uso y efectividad del asistente, consolidando su propuesta como una solución confiable para la protección de las líneas telefónicas en situaciones críticas.

Los comentarios de los participantes fueron positivos. Los usuarios destacaron la utilidad del aplicativo y su potencial para facilitar el contacto con operadores telefónicos, incluso en situaciones de estrés. Entre las observaciones realizadas, se sugirió incorporar soporte para futuros proveedores de dispositivos y servicios, como **Xiaomi** y **Huawei**, considerando su creciente popularidad en el mercado nacional. Además, se destacó la posibilidad de incluir notificaciones proactivas que alerten a los usuarios sobre los pasos realizados con éxito durante el proceso, mejorando aún más la experiencia.

Estos resultados confirman que **Segurazo** es intuitivo y altamente efectivo en la gestión del bloqueo de líneas telefónicas, validando la hipótesis planteada. La integración de las sugerencias recibidas permitirá mejorar la experiencia del usuario y ampliar el alcance del aplicativo, posicionándolo como una herramienta esencial en el mercado de seguridad digital.

Hipótesis 3 (H3): Métrica 6. Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán Segurazo para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo, impidiendo que sus datos sensibles sean accedidos por terceros.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo**,** se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave: tiempo

promedio necesario para completar el proceso de bloqueo telefónico. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 40. Tiempo promedio en el proceso de bloqueo telefónico

Pasos en el uso del aplicativo "Segurazo"	Tiempo promedio (min)	Cumple con el requisito (≤2 min)
Simular ingresar a la web o aplicación del asistente virtual 'Segurazo'.	0.50	
Simular el registro de datos iniciales (información personal y detalles del operador telefónico).	0.70	
Simular el lanzamiento de la llamada telefónica al operador telefónico.	0.45	
Simular el contacto con el área de bloqueo del operador telefónico.	0.60	
Terminar el registro de la operación de llamada.	0.35	
Verificar que la tarea esté completada a través del menú principal.	0.40	
Tiempo total promedio de uso en 20 usuarios	2.00	Si

Fuente: Elaboración Propia

El tiempo promedio de uso del aplicativo fue de 2 minutos (ver Tabla 40), cumpliendo con el criterio de aceptación de 2 minutos o menos. Estos resultados indican que Segurazo permite a los usuarios completar el proceso de bloqueo de líneas telefónicas de manera eficiente, validando la hipótesis de usabilidad.

Hipótesis 4 (H4): Métrica 7. Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán Segurazo para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo, se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave: el

porcentaje de éxito en la compleción de tareas para completar el ajuste de seguridad en el dispositivo. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 41. Porcentaje de éxito en el bloqueo en el proceso de ajuste de seguridad

Pasos en el uso del aplicativo Segurazo	Cumplimiento (%)	Cumple con el requisito (≥68%)
Simular ingresar a la web o aplicación de 'Segurazo'.	98%	
Simular el registro de sus entidades financieras, dispositivos y operador.	96%	
Simular ingresar a la sección de dispositivos.	97%	
Simular seleccionar su dispositivo.	94%	
Simular seguir los pasos de la web de Google o iCloud para ajustar la seguridad (ejemplo: bloqueo remoto, borrado de datos).	93%	
Simular hacer clic en la casilla para indicar que completó la tarea de ajuste de seguridad de dispositivos.	99%	
Cumplimiento promedio de las tareas en 20 usuarios	96,2%	Si

Fuente: Elaboración Propia

Se realizaron pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional podrán utilizar el asistente virtual **Segurazo** para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo. Los resultados mostraron que el 96.2% de los usuarios completaron con éxito todas las tareas requeridas sin errores ni necesidad de asistencia adicional, superando ampliamente el criterio de aceptación del 68%, como se detalla en la Tabla 41.

Las tareas evaluadas incluyeron: ingreso a la plataforma, registro de datos iniciales (entidades financieras, dispositivos y operador), navegación hacia la sección de dispositivos, selección del dispositivo afectado, ajuste de seguridad a través de plataformas externas como Google o iCloud (bloqueo remoto o borrado de datos) y confirmación del proceso mediante una casilla en el aplicativo. Estos resultados confirman que **Segurazo** es una herramienta

efectiva y confiable para gestionar la seguridad de los dispositivos en situaciones de emergencia.

Los usuarios destacaron que la funcionalidad que dirige a las opciones globales de Android e IOS es altamente útil, ya que estas plataformas no solo permiten bloquear el dispositivo, sino también rastrearlo. Sin embargo, se sugirió agregar un anuncio o notificación que informe a los usuarios que serán dirigidos a páginas externas de los fabricantes para completar el proceso de seguridad. Este mensaje debería incluir una aclaración de que no se solicitará información sensible ni se redirigirá a páginas maliciosas, lo que brindará tranquilidad al usuario durante el proceso.

Estos resultados validan que el asistente virtual **Segurazo** es intuitivo, seguro y confiable en la gestión de la seguridad de los dispositivos. Las recomendaciones de los usuarios, como la inclusión de mensajes informativos, fortalecerán la confianza y experiencia del usuario, consolidando a **Segurazo** como una solución líder en el ámbito de seguridad digital.

Hipótesis 4 (H4): Métrica 8. Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán Segurazo para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.

Para confirmar la deseabilidad y facilidad de uso del asistente virtual Segurazo, se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave tiempo promedio necesario para completar el ajuste de seguridad en el dispositivo. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 42. Tiempo promedio en el proceso de ajuste de seguridad

Pasos en el uso del aplicativo Segurazo	Tiempo promedio (min)	Cumple con el requisito (≤10 min)
Simular ingresar a la web o aplicación de 'Segurazo'.	0.60	
Simular el registro de sus entidades financieras, dispositivos y operador.	1.00	
Simular ingresar a la sección de dispositivos.	0.70	
Simular seleccionar su dispositivo.	0.50	
Simular seguir los pasos de la web de Google o iCloud para ajustar la seguridad (ejemplo: bloqueo remoto, borrado de datos).	1.20	
Simular hacer clic en la casilla para indicar que completó la tarea de ajuste de seguridad de dispositivos.	0.50	
Tiempo total promedio de uso en 20 usuarios	4.50	Si

Fuente: Elaboración Propia

El tiempo promedio total para completar el proceso de ajuste de seguridad en el aplicativo Segurazo fue de 4.5 minutos (ver Tabla 42), lo cual está significativamente por debajo del criterio de aceptación establecido de 10 minutos. Este resultado demuestra que los usuarios pueden realizar el ajuste de seguridad en un tiempo breve y sin complicaciones, incluso en una situación simulada de emergencia.

Hipótesis 5 (H5): Métrica 9. Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán Segurazo para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.

Para validar la facilidad de uso y eficiencia del asistente virtual Segurazo en el proceso de realizar denuncias en situaciones de emergencia, se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave: el porcentaje de éxito en la

compleción de tareas específicas necesario para completar el proceso de denuncia. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 43. Porcentaje de Éxito en el proceso de denuncia policial

Pasos en el uso del aplicativo Segurazo	Cumplimiento (%)	Cumple con el requisito (≥68%)
Simular ingresar a la plataforma "Segurazo"	97%	
Simular realizar una denuncia digital ante la PNP	94%	
Simular lanzamiento de la llamada al 105	96%	
Simular ubicar una comisaría cercana	95%	
Verificar la tarea completada en el menú principal	98%	
Cumplimiento promedio de las tareas en 20 usuarios	96%	Si

Fuente: Elaboración Propia

Se llevaron a cabo pruebas de usabilidad con 20 usuarios para validar la hipótesis de que los ciudadanos de 18 a 65 años a nivel nacional pueden utilizar el asistente virtual **Segurazo** para gestionar denuncias en situaciones simuladas de pérdida o robo de dispositivo. Los resultados mostraron que el 96% de los usuarios completaron todas las tareas requeridas sin errores ni necesidad de asistencia adicional, superando ampliamente el criterio de aceptación del 68%, como se observa en la Tabla 43.

Las tareas evaluadas incluyeron: ingreso a la plataforma, simulación de una denuncia digital ante la Policía Nacional del Perú (PNP), lanzamiento de una llamada al 105, ubicación de una comisaría cercana y verificación de la tarea completada en el menú principal. La funcionalidad de **Segurazo** para asistir en la denuncia policial fue bien valorada por los usuarios, quienes destacaron que nunca habían considerado la importancia de contar con información de las comisarías más cercanas. Más de la mitad de los participantes expresó estar dispuesta a realizar su denuncia policial, gracias a la facilidad de uso del aplicativo.

Una funcionalidad que recibió comentarios especialmente positivos fue la capacidad de ubicar automáticamente la comisaría más cercana al lugar donde se encuentra el usuario. Sin embargo, se identificaron algunas áreas de mejora. Por ejemplo, se reportó que la web de la PNP para realizar denuncias en línea estaba en mantenimiento, lo que afectó parcialmente la experiencia del proceso digital. Además, se sugirió reordenar las opciones en el menú, colocando la opción de búsqueda de comisarías en primer lugar para facilitar su acceso.

Los resultados validan la efectividad y facilidad de uso de **Segurazo** en el proceso de realizar denuncias en situaciones de emergencia. Incorporar mejoras basadas en el feedback, como ajustar el orden de las opciones y optimizar el flujo de navegación, fortalecerá la experiencia del usuario y consolidará a **Segurazo** como una herramienta esencial en la seguridad digital y ciudadana.

Hipótesis 5 (H5): Métrica 10. Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán Segurazo para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.

Para validar la facilidad de uso y eficiencia del asistente virtual **"Segurazo"** en el proceso de realizar denuncias en situaciones de emergencia, se realizaron pruebas de usabilidad con 20 usuarios. Esta prueba evaluó la métrica clave: el tiempo promedio en la compleción de tareas específicas necesario para completar el proceso de denuncia. Los resultados obtenidos permitieron confirmar la hipótesis de negocio.

Tabla 44. Tiempo promedio en el proceso de denuncia policial

Pasos en el uso del aplicativo Segurazo	Tiempo promedio (min)	Cumple con el requisito (≤30 min)
Simular ingresar a la plataforma "Segurazo"	0.75	
Simular realizar una denuncia digital ante la PNP	1.20	

Simular lanzamiento de la llamada al 105	10.60	
Simular ubicar una comisaría cercana	0.95	
Verificar la tarea completada en el menú principal	0.50	
Cumplimiento promedio de las tareas en 20 usuarios	14.00	Si

Fuente: Elaboración Propia

El tiempo promedio de uso fue de 14 minutos, muy inferior al criterio de 30 minutos, lo cual valida que el asistente virtual Segurazo es eficiente para completar el proceso de denuncia en situaciones de emergencia (Tabla 44).

6.2.Validación de la factibilidad de la solución

6.2.1. Plan de mercadeo

El plan de mercadeo desarrollado tiene como objetivo posicionar a Segurazo como la solución más confiable y efectiva para actuar ante robos de celulares, atendiendo las necesidades tanto de los usuarios finales como de las entidades financieras. A través de estrategias detalladas de segmentación, un enfoque integral en la propuesta de valor, y campañas estructuradas por fases (lanzamiento, atracción y consolidación), el plan busca generar reconocimiento de marca, captar socios estratégicos y garantizar la fidelización de los clientes, maximizando el impacto de la aplicación en el mercado peruano.

6.2.1.1. Modelo de Negocio

Descripción del Modelo

Nuestro modelo de negocio se centra en ofrecer una aplicación de seguridad que guíe a los peruanos en caso de robo de celular. La aplicación proporciona un recurso crucial y fácil de usar, permitiendo a los usuarios realizar acciones rápidamente ante la emergencia de un robo. Nuestros clientes directos son las entidades financieras, quienes verán valor en aliarse

con la aplicación para proteger mejor a sus usuarios ante incidentes de robo y fraude. Los usuarios finales de la aplicación serán los clientes de estas entidades financieras.

Analizaremos los bloques del modelo de negocio relevantes para esta sección, lo cual nos permitirá luego identificar los elementos esenciales para la operación y los recursos necesarios.

Actividades Clave

Una de las actividades más importantes de nuestro modelo es el desarrollo y mantenimiento de la aplicación. Será importante una interfaz intuitiva que permita a los usuarios actuar rápidamente en caso de emergencia, en adición realizaremos un continuo mantenimiento y actualización para garantizar compatibilidad con nuevos sistemas operativos y normas de seguridad.

Por su lado, será crucial nuestros esfuerzos e inversiones en Marketing. Las estrategias tendrán tanto un enfoque B2B, para conseguir que más entidades financieras sean nuestros socios, así como B2C, para que más personas conozcan nuestra aplicación y sus beneficios. En adición, se realizarán campañas de sensibilización y educación en seguridad para promover la aplicación como un recurso necesario y preventivo.

Será necesario también brindar soporte a los usuarios. Durante el desarrollo del proyecto, buscaremos contar con un equipo de soporte que pueda responder rápidamente a usuarios que necesiten ayuda en momentos de emergencia, por ejemplo, con orientación en el uso de las funciones de la aplicación, especialmente en los procedimientos de bloqueo y denuncia, esto junto con el diseño y mantenimiento de canales de atención.

Finalmente, enfatizamos que será esencial la creación de alianzas estratégicas con las entidades financieras. Se tendrán negociaciones sobre los acuerdos con bancos para que se conviertan en socios clave, ofreciendo el servicio de calidad a sus clientes. Se buscará el

posicionamiento de la aplicación como un recurso que refuerza la seguridad de los servicios bancarios y mejora la satisfacción del cliente.

Recursos Clave

Uno de nuestros recursos más importantes será nuestro equipo de desarrollo, un equipo de expertos en tecnología móvil, ciberseguridad y UX/UI, responsables de desarrollar y mantener la aplicación en su mejor nivel de funcionamiento y a la vanguardia.

Por su lado, deberemos proteger nuestra propiedad intelectual: la aplicación. Es un recurso clave que debe asegurar la diferenciación de la competencia.

Socios Estratégicos

Primero ASBANC (Asociación de Bancos del Perú), quien puede facilitar las relaciones y el contacto con los principales bancos en el Perú, ayudando a la negociación de acuerdos de colaboración.

Por otro lado, y como ya mencionado las entidades financieras. La aplicación necesita captar a estas entidades como clientes directos y socios, quienes pueden ofrecer la aplicación a sus clientes como un servicio agregado de protección, promoviendo la lealtad y mejorando la seguridad en sus cuentas.

Tercero, el Ministerio de Transportes y Comunicaciones (MTC). El MTC puede actuar como un aliado para asegurar que la aplicación esté alineada con las regulaciones locales e incluso, en un futuro, promoverla como parte de sus iniciativas de seguridad pública.

Cuarto, la Superintendencia de Banca y Seguros (SBS). La SBS puede también ayudar a fomentar la adopción de soluciones de seguridad como la aplicación.

Finalmente, los proveedores de TI. Los productos de las compañías de tecnología con las que trabajaremos serán muy importantes durante el desarrollo y luego del lanzamiento de la aplicación al mercado para mantener un alto nivel de servicio y calidad.

6.2.1.2. Objetivos del Plan de Marketing

Dado que para nuestro proyecto los clientes son las entidades financieras y los usuarios son los clientes de las entidades financieras, usaremos dos enfoques para nuestro plan de Marketing, uno B2B y otro B2C, respectivamente.

Enfoque B2B

El sentido de este enfoque es llegar a establecer alianzas estratégicas con entidades financieras, tales como bancos, cajas municipales y financieras, promoviendo la aplicación como un valor agregado en la protección de sus clientes ante robos y fraudes.

Objetivos B2B

- En nuestra búsqueda de captación de entidades financieras clave, un primer objetivo será lograr que al menos tres entidades financieras adopten la aplicación antes del lanzamiento, sobre todo las más importantes en nuestro entorno, como son el BCP, BBVA e Interbank. Hacia el segundo año, nuestro objetivo será expandir la red de socios a al menos cinco entidades financieras de distintos tipos, además de los bancos, buscaremos incluir a cajas municipales, financieras, entre otros.
- Buscaremos también promover el valor añadido de la seguridad digital para las entidades financieras. Debemos posicionar la aplicación como un recurso de protección ante fraudes y robos que mejora la confianza y fidelización de los clientes de cada entidad financiera- Debemos demostrar a las entidades financieras el potencial de reducción de fraudes y costos asociados a la pérdida de activos o fraudes que pueden producirse tras el robo de un celular de sus clientes.
- Como tercer objetivo B2B, buscaremos construir relaciones duraderas a través del soporte y la innovación continua. Esto permitirá a las entidades financieras sentir que tienen un socio confiable en seguridad digital. Será entonces importante recibir y analizar feedback de los socios para actualizar y adaptar la aplicación continuamente a

las necesidades del mercado financiero peruano, esto para mantener el nivel de calidad siempre alto y a la vanguardia.

Enfoque B2C

El sentido de este enfoque es fomentar la adopción y el uso de la aplicación entre los clientes de las entidades financieras peruanas, los usuarios, resaltando su utilidad como una herramienta esencial para protegerse ante el robo de celular, el bloqueo de cuentas y la realización de denuncias. En otras palabras, debemos buscar aquí el "Top of Mind".

Objetivos B2C

- Se buscará aumentar el conocimiento y la confiabilidad de la aplicación entre los usuarios de entidades financieras. Se lanzarán campañas informativas sobre cómo la aplicación puede proteger de manera integral a los usuarios en casos de robo, enfatizando la facilidad de uso en situaciones de emergencia.
- Se buscará también crear una relación de confianza y seguridad con el usuario final. A través de un sistema de feedback dentro de la aplicación, se obtendrán comentarios para evaluar la satisfacción del usuario, permitiendo optimizaciones continuas en base a la experiencia del cliente. Nuestro equipo de servicio al cliente trabajará en dar respuestas rápidas y efectivas ante dudas sobre el uso de la aplicación en momentos críticos.

6.2.1.3. Segmentación de Mercado

Segmento 1: Usuarios finales

El primer segmento objetivo está compuesto por usuarios finales, quienes son clientes de las entidades financieras y potenciales beneficiarios directos de la aplicación. Este grupo está integrado por personas entre 18 y 60 años que poseen cuentas bancarias y dispositivos móviles, lo que los convierte en una población activa y conectada tecnológicamente.

Geográficamente, este segmento incluye individuos distribuidos en todo el Perú, desde grandes centros urbanos como Lima hasta áreas rurales, gracias a la accesibilidad de la aplicación en diferentes dispositivos con conexión a internet.

Según lo psicográfico, estos usuarios son personas preocupadas por la seguridad de su información financiera y personal. Valoran la rapidez y facilidad en el uso de herramientas tecnológicas, especialmente en situaciones de emergencia, donde el tiempo es crítico. Desde un punto de vista de comportamiento, muchos de ellos realizan transacciones financieras con frecuencia a través de sus celulares, mientras que otros pueden haber sido víctimas de fraudes financieros o robos, o tienen una alta preocupación por estas eventualidades. Este segmento busca soluciones confiables y rápidas que les permitan recuperar el control y proteger su información en momentos críticos.

Segmento 2: Entidades financieras

El segundo segmento objetivo incluye a las entidades financieras, que son los clientes directos de la aplicación y su principal fuente de ingresos. Este grupo está formado por bancos, cajas municipales y financieras con presencia en todo el Perú. Las instituciones de mayor tamaño y alcance nacional representan una prioridad inicial, mientras que las entidades regionales o más pequeñas también son relevantes, especialmente en etapas avanzadas del proyecto.

Desde un punto de vista demográfico, estas entidades suelen contar con amplias bases de clientes, lo que las expone a una alta incidencia de fraudes financieros. Geográficamente, la concentración de estas instituciones en ciudades principales como Lima es significativa, aunque su alcance puede incluir también áreas rurales. En términos psicográficos, estas instituciones valoran la innovación y la seguridad, priorizando soluciones que fortalezcan la confianza de sus clientes en sus servicios. Según el comportamiento, buscan reducir los costos asociados a fraudes financieros y reembolsos, así como mejorar la

percepción de su marca mediante herramientas tecnológicas que proyecten modernidad y confiabilidad.

Perfil del Cliente y del Usuario

El perfil del cliente final puede representarse a través de Juan Pérez, un ingeniero de 35 años que vive en Lima. Juan utiliza su celular diariamente para realizar transacciones bancarias, pagar servicios y comprar en línea. Preocupado por la seguridad de su información, busca herramientas que le permitan reaccionar rápidamente en caso de pérdida o robo de su dispositivo. Prefiere aplicaciones intuitivas que le brinden soluciones claras y que sean accesibles en momentos de crisis, como un robo. Juan siente frustración ante la falta de guías específicas para actuar en emergencias y valora la tranquilidad que una solución como esta le puede proporcionar.

Por otro lado, el perfil del cliente corporativo puede representarse por Financiera Proactiva, una institución con 600,000 clientes activos y presencia nacional. Esta financiera busca diferenciarse en el mercado ofreciendo herramientas innovadoras que incrementen la confianza de sus usuarios y mejoren su experiencia de seguridad financiera. Preocupada por los costos y las repercusiones reputacionales de los fraudes financieros, Financiera Proactiva considera que implementar esta solución no solo les permitirá fidelizar a sus clientes, sino también posicionarse como líderes en innovación y seguridad dentro del sector.

6.2.1.4. Análisis de la competencia

Basándonos en lo visto en el capítulo 2, ahora nuestro análisis detallará las propuestas de valor, canales de distribución, puntos fuertes y débiles, y política de precios para poder así tener una mejor visión del entorno competitivo de nuestra aplicación.

Análisis de competidores directos e indirectos

A continuación, en la Tabla 45, se realiza una comparación de los principales competidores de nuestra aplicación actualmente presentes en el mercado peruano.

Tabla 45. Comparativo de competidores de Segurazo

Competidor	Propuesta de Valor	Canales de Distribución	Puntos Fuertes	Puntos Débiles	Precios
Entidades Financieras	Seguridad y bloqueo de cuentas dentro de apps bancarias	Apps bancarias	Confianza y fidelidad del usuario	Limitado solo a ámbito bancario	Sin costo para clientes
ASBANC - Servicio 1820	Bloqueo de cuentas bancarias mediante número único	Número telefónico nacional	Accesibilidad, confianza institucional	No incluye bloqueo de SIM ni asesoría en denuncias	Sin costo
Teleoperadores	Bloqueo de SIM y dispositivos en caso de pérdida o robo	Atención en tiendas, apps de autogestión	Control de infraestructura, respuesta rápida	No cubre bloqueo bancario ni orientación en casos de robo	Generalmente gratuito
Apps de Seguridad de Terceros	Localización, bloqueo y borrado de datos en dispositivos	App Stores (Google Play, App Store)	Especialización en protección de datos	Sin integración bancaria o de SIM, requiere preactivación	Gratuitas o $5 - $20/mes

Fuente: Elaboración propia

Se puede observar en cuanto a las entidades financieras la función de bloque se encuentra ya incluida en sus aplicaciones y servicios web. Sin embargo, estas soluciones se limitan al ámbito bancario y no abarcan una respuesta integral que incluya bloqueo de dispositivos, SIMs o asesoría en denuncias.

Por su lado, es importante mencionar el nuevo servicio lanzado recientemente por ASBANC, el 1820. Este número telefónico 1820, facilita un uso rápido y sencillo en situaciones de emergencia. Sin embargo, similar al punto anterior, su alcance se limita al bloqueo de cuentas bancarias, lo cual reduce la respuesta integral al problema del robo de celulares.

En cuanto a las empresas operadoras de telecomunicaciones, estas cuentan con centros de atención al cliente, aplicaciones de autogestión, y centros de llamadas, sin embargo, también tienen el problema de ser específicos, evidentemente no abordan el

bloqueo de cuentas bancarias ni asistencia en denuncias policiales. En adición, la complejidad de procedimientos puede dificultar el acceso inmediato para algunos usuarios.

Finalmente, tenemos las aplicaciones de seguridad de terceros, entre ellos Avast, McAfee, Find My Device de Google y Find My iPhone de Apple. El enfoque de estas aplicaciones está orientadas a ofrecer protección en caso de pérdida de dispositivos, con un enfoque en la protección de información y recuperación del dispositivo. Sin embargo, se ven limitados en que no ofrecen un alcance integral en términos de bloqueo de cuentas bancarias o SIM, y requieren activación previa del usuario, lo cual puede resultar en una baja adopción en segmentos que no son conscientes de estas opciones, de hecho, los delincuentes pueden encontrar otros caminos para seguir robando a los usuarios.

Identificación de oportunidades

Como se puede observar, la aplicación tiene la oportunidad de posicionarse como una solución completa y diferenciada que engloba bloqueo de dispositivos, SIM, cuentas bancarias y asesoría en denuncias, algo que los competidores actuales no ofrecen de manera integrada. La falta de soluciones de seguridad completas sugiere una oportunidad para captar usuarios que buscan una solución confiable y fácil de usar en situaciones de emergencia.

Buscaremos colaborar con entidades financieras y operadores de telecomunicaciones para ofrecer una respuesta coordinada y potente puede fortalecer el alcance y valor percibido de la aplicación.

6.2.1.5. Propuesta Única de Venta

La aplicación ofrece una solución integral y accesible para guiar a los usuarios en los pasos críticos a seguir inmediatamente después del robo de su celular. Nuestra propuesta de valor diferenciada será como sigue: "Nuestra aplicación es tu guía de acción rápida en caso de robo. Una sola aplicación, todos los pasos para recuperar tu seguridad."

La aplicación brinda a los usuarios la tranquilidad de saber que no se les escapará nada importante después de una emergencia. Ofrece una guía clara y detallada de todas las acciones necesarias para bloquear su dispositivo, SIM y cuentas bancarias, asegurando que, al seguir estos pasos, recuperen el control y seguridad de sus datos y finanzas sin dejar cabos sueltos.

Es evidente que después de un robo la confusión y el miedo pueden hacer que los usuarios no actúen con rapidez ni claridad. Es entonces que la aplicación proporciona instrucciones específicas y personalizadas en tiempo real basadas en los detalles que el usuario ya ha ingresado (entidades financieras, operador de celular y tipo de dispositivo). Con un flujo de instrucciones ordenado y relevante, el usuario puede actuar de inmediato, lo que maximiza sus posibilidades de proteger su información y activos, recuperando el control rápidamente.

Elementos diferenciadores

La aplicación tendrá una funcionalidad integral. En una sola plataforma, el usuario puede bloquear el dispositivo, la SIM y las cuentas bancarias de acuerdo con sus servicios específicos. Ninguna otra aplicación en el mercado ofrece este nivel de cobertura integral.

Buscaremos siempre que la aplicación sea de fácil acceso y uso intuitivo. Diseñada para ser usada por personas de todas las edades, incluso aquellas con limitado conocimiento tecnológico, la aplicación requiere solo tres inputs básicos (entidades financieras, operador de celular y tipo de dispositivo). Además, se contará con una interfaz minimalista y un proceso de pasos claros, lo cual es ideal para momentos de alta tensión.

En adición, la aplicación guiará al usuario de manera personalizada, brindándole únicamente la información necesaria. Además, el chatbot integrado proporciona soporte adicional en caso de dudas, y, en casos extremos, podemos incluir para el usuario un servicio

con el cual podrá comunicarse con un agente especializado para recibir ayuda detallada, esta opción puede estar disponible en una versión Premium.

Se debe recordar que la aplicación actúa exclusivamente como guía y no se conecta directamente a las plataformas bancarias ni de telecomunicaciones, ofrece una barrera "natural" de seguridad al no tener acceso directo a datos sensibles del usuario. La aplicación, sin embargo, estará en constante actualización para reflejar los últimos procesos de seguridad de las entidades financieras y operadores.

Por último, enfatizamos que, de cara a las entidades financieras, la aplicación se convierte en una extensión de sus esfuerzos de protección y fidelización de clientes. Al utilizar esta solución, los usuarios ganan confianza en las entidades financieras, pues perciben que están protegidos de manera efectiva en caso de una emergencia, lo que mejora la imagen de seguridad y confiabilidad de estas instituciones en el mercado.

Planes de desarrollo futuro

Para hacer que la aplicación sea aún más útil, se tiene en evaluación como proyecto de mejora buscar siempre la compatibilidad con nuevos tipos de dispositivos, tecnologías y modalidades de robo. Esto nos permitirá estar a la vanguardia y ser relevantes en el mercado tanto para los clientes como los usuarios.

6.2.1.6. Estrategia de Marketing

A continuación, se detalla los puntos clave de cada componente del Marketing Mix.

Producto

La aplicación web se destaca por guiar al usuario paso a paso tras el robo de un celular, ofreciendo un flujo sencillo de instrucciones adaptadas a su situación. A través de una interfaz intuitiva y un Chatbot amigable que lo acompañará durante el uso del servicio ayudando a resolver dudas puntuales, permite realizar bloqueos de cuentas bancarias, SIM, y dispositivo, además de facilitar la denuncia policial.

En adición, se considera una versión premium que ofrezca soporte personalizado mediante un agente en tiempo real en casos extremos. Esta opción ampliaría las alternativas de servicio, especialmente para usuarios con necesidades urgentes. Sin embargo, se debe considerar que el ingreso principal se generará a partir de contratos B2B con entidades financieras.

Precio

La aplicación web buscará mantenerse gratuita para el usuario final, como comentado, será financiada a través de contratos con entidades financieras (el cliente B2B). La opción premium, en caso de implementarse, buscará dar un servicio adicional gracias a un agente, el pago será por servicio específico dada la naturaleza del producto.

Plaza (Distribución)

La aplicación será una dispuesta a través de plataforma web universal, accesible desde cualquier dispositivo sin necesidad de descarga en una tienda de aplicaciones. La web se adapta a distintos tamaños de pantalla para una experiencia amigable en cualquier tipo de celular, Tablet, entre otros.

En cuanto a los métodos de distribución para entidades financieras, la captación de estas se hará a través de reuniones directas con ASBANC y las mismas entidades, presentando avances y demostraciones de funcionalidades en fases previas al lanzamiento. Después del lanzamiento, se realizarán actualizaciones frecuentes sobre proyectos de mejora y parches adaptados a nuevos escenarios, tecnologías y modalidades de robo.

Promoción

Inicialmente se implementará una campaña de marketing digital en redes sociales, junto con publicidad en vallas publicitarias y espacios visuales de alta visibilidad, como estadios de fútbol. También se considerarán activaciones de en las calles para maximizar la exposición del público objetivo. Se buscará crear una alta visibilidad en redes sociales, en

espacios públicos y mediante marketing de influencia para construir el “Top of mind” y “Awareness”.

En adición, se lanzarán campañas de sensibilización con el objetivo de posicionar la aplicación como un servicio esencial para protegerse en situaciones de emergencia. Este esfuerzo incluirá campañas para crear una asociación directa entre nuestra aplicación con la sensación de seguridad y tranquilidad del usuario.

Finalmente, buscaremos la consolidación de mercado a través de campañas continuas para mantener la app en el "Top of mind" de los usuarios y reforzar su imagen de seguridad y fiabilidad.

Personas

La experiencia del usuario estará centrada en la guía paso a paso y el chatbot amigable como primer punto de contacto. En caso de adquirir la opción premium, los usuarios tendrán acceso a agentes para un soporte más especializado.

Nuestro equipo de Comercial tendrá la tarea de recopilar y reaccionar con agilidad a comentarios y retroalimentación de usuarios, manteniendo estándares de calidad y atención inmediata. Este alto nivel de servicio será un punto clave en las relaciones B2B, mostrando la confiabilidad y preparación en situaciones críticas.

Procesos

La aplicación incluirá una sección de preguntas frecuentes (FAQ) accesible, ayudando a los usuarios a resolver dudas comunes de manera independiente. Además, la interfaz de inicio de la aplicación mostrará noticias recientes y casos de éxito para mantener a los usuarios informados. Estas actualizaciones estarán orientadas a reforzar la percepción de seguridad y valor constante.

Por su lado, se establecerán reuniones periódicas con las entidades financieras y otros socios clave para revisar el rendimiento, implementación de nuevas funciones y respuesta a necesidades emergentes.

Evidencia Física (Physical Evidence)

Nuestro material de soporte visual B2B se basará en materiales visuales digitales distribuidos a los socios estratégicos y clientes B2B, como presentaciones, infografías y estudios de caso que respalden el valor agregado de la aplicación en términos de seguridad.

Finalmente, en cuanto a la identidad de marca, la aplicación contará con un personaje visual, un pequeño robot blanco de cara amigable, que representará a la aplicación y será la "personificación" del chatbot. El diseño de este robot amigable busca generar confianza y tranquilidad, permitiendo que el usuario asocie visualmente la aplicación con seguridad y acompañamiento efectivo.

6.2.1.7. Estrategia de Medios y Campañas

Nuestro plan de medios buscará asegurar una presencia sólida y en constante crecimiento en el mercado, brindando tanto visibilidad como confianza. Estará compuesta por tres fases: de lanzamiento, de atracción y de consolidación.

6.2.1.7.1. Fase de Lanzamiento: Reconocimiento de Marca

Esta fase busca lograr que el mercado peruano reconozca la existencia de la aplicación, de forma que, en caso de robo de celular, el servicio sea una primera opción en la mente de los usuarios. se recalca que nuestro público objetivo son todos los ciudadanos usuarios de celular y cuentas bancarias, de 15 años en adelante.

Estrategia de Contenidos:

Se buscará explicar los pasos para usar la aplicación en caso de emergencia y destacar la rapidez con que los usuarios pueden recuperar su seguridad. Asimismo, se enfocará los mensajes en la facilidad de uso, la rapidez de respuesta y la confianza que brinda la aplicación.

Una herramienta importante para cumplir el objetivo será el mostrar casos de éxito de nuestro servicio, esto es mostrar ejemplos de cómo la aplicación ha sido efectiva en ayudar a las personas a proteger su información después de un robo.

Canales:

Se utilizarán canales digitales como redes sociales, entre ellos Facebook, Instagram y TikTok para maximizar la visibilidad en segmentos jóvenes y adultos. También será necesario el uso de Google Ads, esto no permitirá la utilización de palabras clave y anuncios de display orientados a búsquedas relacionadas con seguridad móvil y protección de información. Otra herramienta que explorar será el contenido orgánico y pagado, podemos iniciar con contenido orgánico en redes, seguido de anuncios pagados para reforzar la visibilidad.

En cuanto a medios tradicionales, se tiene planificado el uso de vallas publicitarias, colocadas en zonas de alto tráfico, incluyendo avenidas principales y cercanía a estaciones de transporte público. Así como publicidad en eventos deportivos, sobre todo eventos de fútbol para llegar a una audiencia amplia y variada.

Cronograma:

Los primeros tres meses se enfocarán en esta fase, con evaluaciones mensuales para ajustar el alcance y el tipo de contenido.

6.2.1.7.2. Fase de Atracción de Clientes: Captación Activa

Por el lado de usuarios finales, esta fase buscará aumentar las visitas y uso del servicio, recopilar feedback, y contabilizar casos atendidos. Mientras que para las entidades financieras buscará maximizar la cantidad de entidades participantes, enfocándose en bancos que tienen alta participación de mercado.

Estrategia de Contenidos:

Se buscará la educación y sensibilización a través de la publicación de artículos y posts educativos sobre la importancia de la seguridad digital y cómo la aplicación puede proteger a los usuarios en caso de robo. Asimismo, se tendrán presentaciones dirigidas a las entidades financieras, organizando reuniones personalizadas para demostrar el valor de la aplicación y obtener acuerdos de uso.

Canales:

Se continuará con publicidad en zonas de alto tráfico, en estaciones de transporte, centros comerciales y zonas concurridas de la ciudad.

Por su lado, se utilizarán canales de comunicación directa, como Email Marketing, es decir, campañas de correo para entidades financieras con datos sobre el impacto de la app en la seguridad de los usuarios. en adición, se programarán reuniones presenciales y online con los bancos y entidades financieras clave, en donde el equipo comercial demostrará la efectividad y las actualizaciones o la evolución de la aplicación.

Cronograma:

La fase de atracción se mantendrá por los siguientes seis meses, con seguimiento mensual a las métricas para hacer ajustes en las estrategias.

6.2.1.7.3. Fase de Consolidación: Fidelización y Expansión de Marca

El objetivo de esta fase será la fidelización de entidades financieras. Se buscará mantener la relación con los bancos y enfocarse en la retención, priorizando las instituciones más importantes del mercado basándonos en su participación de mercado.

Estrategia de Contenidos:

Se basará en casos de éxito y actualizaciones a nuestro servicio, mostrando ejemplos reales de usuarios que se beneficiaron de la aplicación y dar a conocer nuevas funcionalidades que se acomodan a nuevas tecnologías y modalidades de robo. Algo que puede ayudar a la marca serán los reconocimientos de nuestra idea de negocio, compartir menciones o premios de organizaciones públicas y privadas que validen la efectividad de la aplicación.

Canales de Comunicación:

Con alianzas con las entidades financieras haremos uso de boletines de noticias, estos contendrán consejos de seguridad, noticias relevantes, y casos de éxito de nuestro servicio. En adición, otra herramienta a explorar serán los SMS y notificaciones web, enviado alertas y recordatorios para sensibilizar sobre la importancia de la seguridad digital.

Cronograma:

Esta fase se extenderá de manera continua tras los primeros nueve meses, con ajustes trimestrales para optimizar la retención y la relación con entidades.

6.2.1.8. Inversión y Presupuesto de Marketing

Se presentará a continuación nuestra estrategia y presupuesto de inversión en marketing estructurada en las fases previamente vistas: Lanzamiento, Atracción y Consolidación, esto con el fin de maximizar la visibilidad y el posicionamiento de la marca durante los cinco años del proyecto.

El presupuesto de marketing total para los cinco años es de 911,950 soles.

Siguiendo la distribución planeada:

- Lanzamiento (Años 0 y 1): Equivalente a 224,150 soles
- Atracción (Años 2 y 3): Equivalente a 561,101 soles
- Consolidación (Años 4 y 5): Equivalente a 126,744 soles

Dado que se trata de un servicio que busca alta visibilidad y adopción, nos basaremos en un enfoque combinado entre marketing digital y marketing tradicional. Primero, el marketing digital representará el 10% del presupuesto de cada fase, enfocándonos en captar usuarios directamente a través de redes sociales, publicidad en buscadores, y marketing de contenidos educativos. Por su lado, los medios tradicionales representarán el 25% del presupuesto de cada fase, haciendo uso de herramientas como vallas publicitarias en Lima y anuncios en eventos deportivos, siendo el fútbol muy popular en nuestro país.

6.2.1.8.1. Plan de marketing para la fase 1: Lanzamiento (Años 0 y 1)

El objetivo de esta fase es el posicionamiento y reconocimiento de marca para generar "top of mind" entre usuarios que posean celulares y cuentas bancarias en caso de robo. Por su lado, tenemos proyectado que durante el primer año del proyecto es nos asociaremos con la menor cantidad de entidades financieras de los cinco años, es decir nos focalizaremos en las unas cuantas entidades financieras. Por este motivo, el gasto en marketing de esta fase representa el 25% de nuestro presupuesto de marketing de los cinco años que dura el proyecto.

En cuanto al marketing digital, haremos uso de las redes sociales a través de publicaciones pagas y orgánicas en Facebook, Instagram, y YouTube con testimonios y casos de uso. Nos serviremos también de tutoriales y videos informativos sobre los beneficios de la aplicación. Esto irá de la mano de Google Ads para captar la atención de usuarios buscando opciones de seguridad y protección. Finalmente, consideramos importante mostrar contenido

de testimonios y casos de éxito, en sitios de noticias y colaboraciones con influencers en tecnología.

Por su parte, para medios tradicionales haremos uso de vallas publicitarias y publicidad en eventos deportivos: Espacios en estadios o vallas en juegos de fútbol para maximizar la visibilidad a nivel nacional.

6.2.1.8.2. Plan de marketing para la fase 2: Atracción (Años 2 y 3)

El objetivo de esta fase es aumentar las visitas a la web y el uso de la aplicación, así como afianzar alianzas con entidades financieras.

En cuanto al marketing Digital, se basará en campañas educativas y de sensibilización, así como en email marketing con campañas dirigidas entidades financieras para mantener el interés y ofrecer casos de éxito y testimonios.

Para medios tradicionales, seguiremos utilizando vallas en puntos estratégicos de alto tráfico. En adición, utilizaremos las presentaciones B2B dirigidas a las entidades financieras.

6.2.1.8.3. Plan de marketing para la fase 3: Consolidación (Años 4 y 5)

Finalmente, en esta fase se buscará retener las entidades financieras, destacando la confiabilidad y constante actualización del servicio. Se debe notar que el presupuesto para estos dos años representa más del 22% del presupuesto de marketing de los cinco años, esto se debe a que buscaremos consolidarnos hacia el quinto año asociándonos con la mayor cantidad de entidades financieras de todo el proyecto, cerca del 75% de la industria financiera.

El marketing digital se basará en boletines y noticias dirigidos a entidades financieras que incluyan nuevas funcionalidades, reconocimientos de entidades públicas, y mejoras en el servicio.

Mientras que para medios tradicionales se reforzará la publicidad en redes de transporte y espacios públicos. Asimismo, se intensificarán los esfuerzos en eventos de

seguridad bancaria, esto para mantener la visibilidad y la reputación de nuestro servicio como un aliado confiable de las entidades financieras.

Tabla 46. Presupuesto de Marketing por año

Años	Presupuesto Total de Fase	Marketing Digital	Medios Tradicionales	Marketing B2B
0 y 1	224,105	42,883	92,822	88,400
2 y 3	561,101	115,255	243,581	202,265
4 y 5	126,744	40,542	43,332	42,869
Total	911,950.02	198,680.85	379,735.33	333,533.83

Fuente: Elaboración Propia

6.2.2. Simulaciones empleadas para validar las hipótesis de Marketing

La hipótesis de nuestro plan de mercadeo: “Creemos que el plan de marketing de Segurazo impactará positivamente el modelo del negocio con más ingresos que egresos desde el primer año”.

Para verificarlo, se calcula el costo de adquisición del cliente (CAC) y el valor del tiempo de vida del cliente (LTV) durante los primeros cinco años, para esto nos basaremos en las entidades financieras captadas durante los cinco años del proyecto, así como los gastos en Marketing presupuestados para captarlos.

En primer lugar, se planea afiliar más clientes en el tercer año, como se observa en la tabla 47.

Tabla 47. Nuevos clientes por año

Tipo Entidad	1	2	3	4	5
Bancos	2	4	10	12	14
Financieras	2	4	8	9	9
Cajas	2	4	10	12	13
Total Entidades	6	12	28	33	36
Nuevos Clientes	6	6	16	5	3

Fuente: Elaboración Propia

Dado que se proyecta agregar a la mayor cantidad de entidades en el tercer año, el gasto en marketing para adquirir nuevos clientes se incrementará sobre todo en ese año. De esta manera el CAC tendrá un comportamiento creciente del primer al quinto año, sin

embargo, mayor incremento es en el primer año (31%), hasta alcanzar solo crecimientos de 2% y 10% en el cuarto y quinto año.

Tabla 48. Gasto en Marketing

Año	1	2	3	4	5
Instagram, Face, etc	1,149	1,799	2,024	438	642
Medios	2,993	3,743	4,211	1,140	1,671
B2B	6,950	7,783	9,597	9,743	14,290
Costo de Marketing por Entidad	11,093	13,326	15,832	11,320	16,603
Nuevas Entidades	6	6	16	5	3
Gastos MKT para adquirir nuevo cliente	66,555	79,955	253,315	56,600	49,808

Fuente: Elaboración Propia

De esta manera, el CAC (Gasto Adquisición / Entidades Nuevas) será el de la tabla 49.

Tabla 49. CAC anual

Año	1	2	3	4	5
CAC (Gasto Adquisición / Entidades Nuevas)	13,326	15,832	11,320	16,603	13,326

Fuente: Elaboración Propia

Para el cálculo del LTV [4], se utiliza el precio promedio que se cobra a las entidades en cada año, y se asume que dado que es un contrato anual (12 meses) la duración es de 12 meses. Asimismo, el ingreso promedio por entidad tendrá incremento año a año, sin embargo, se planea disminuir precios en el cuarto año, como estrategia para mantener a los clientes adquiridos durante el tercer año. Ver tabla 48.

Tabla 50. LTV

Año	1	2	3	4	5
Ingreso Promedio por Entidad	6,633	8,073	9,712	10,130	11,093
Duración por Entidad	12	12	12	12	12
LTV (Ingresos promedio cliente*duración por cliente)	79,593	96,876	116,538	121,561	133,116

Fuente: Elaboración Propia

En consecuencia, la ratio LTV/CAC será en promedio 8.11 en los 5 años del proyecto. La ratio será 7.1 en el primer año y se incrementa a 10.7 al cuarto año, con

[4] LTV = Ingresos promedo cliente*Duracion por cliente

disminución en el quinto año, ya que para esos años el CAC aumenta menos que en los años 1 a 3 (etapa donde se invierte más en marketing), y los ingresos se mantienen. Ver Tabla 51.

Tabla 51. LTV entre CAC

Año	1	2	3	4	5
LTV/ CAC	7.18	7.27	7.36	10.74	8.02

Fuente: Elaboración Propia

Para asegurar que la ratio LTV entre CAC es robusto, se realizó el análisis de sensibilidad al CAC y LTV, asumiendo que el primero crece inicialmente en 10% y el segundo en 8%.[5] Ver Tabla 52.

Tabla 52. Sensibilidad a LTV y CAC

Crecimiento LTV	crecimiento CAC	LTV	CAC	LTV / CAC
0.0%	0.0%	109537	13635	8.0
10.0%	5.0%	120491	14317	8.4
20.0%	15.0%	144589	16464	8.8
30.0%	25.0%	187965	20580	9.1
40.0%	35.0%	263152	27783	9.5

Fuente: Elaboración Propia

De esta manera, al realizar el análisis de Montecarlo la ratio LTV a CAC, se obtuvo que la eficiencia (ratio entre 7 y 9) es de 99%, confirmando que el plan es robusto. Ver tabla 53.

Tabla 53. Simulación de Montecarlo para 5000 escenarios

Simulación en 5000 escenarios	
Promedio	8.105
Desviación estándar	0.051
Mínimo	7.962
Máximo	8.249
Alta eficiencia: > 7; <9	99%

Fuente: Elaboración Propia

[5] En promedio el crecimiento del LTV en los 5 años fue de 14.2% mientras el CAC aumentó en 19%. Por ello, se asume que la diferencia en la sensibilidad será de 5%.

6.2.3. Plan de operaciones

El plan de operaciones establece una estructura eficiente para garantizar el correcto funcionamiento y sostenibilidad de nuestra propuesta en el mercado. Este plan abarca desde el diseño de procesos clave, hasta la organización del personal, los recursos tecnológicos necesarios y el cumplimiento de regulaciones.

6.2.3.1. Descripción general de la aplicación

Nuestra aplicación es una herramienta de respuesta rápida diseñada para ayudar a los usuarios a protegerse tras un robo de celular. Funciona como una guía personalizada que les indica paso a paso qué hacer para proteger su información, bloquear dispositivos, tarjetas y líneas telefónicas, y realizar las denuncias correspondientes. Esta solución tiene como objetivo ser la primera opción en la que los usuarios piensen al sufrir un robo, gracias a su rapidez, facilidad de uso y enfoque intuitivo.

Para los usuarios, los beneficios son que proporciona información puntual, relevante y actualizada para resolver su problema en el menor tiempo posible. Además, ofrece tranquilidad al garantizar que no se escapen pasos críticos en un momento de alta tensión. Para las entidades financieras, la aplicación fortalece la relación de confianza con sus clientes, al proyectar una imagen de cuidado y seguridad, contribuyendo a la fidelización de sus usuarios.

6.2.3.2. Diseño de Procesos

En el diseño de procesos, se utiliza un enfoque SIPOC para visualizar las interacciones clave de la operación (ver Tabla 54).

Tabla 54. Diagrama SIPOC

Suppliers	Inputs	Processes	Outputs	Customers
• Desarrolladores, empresas de TI, proporcionan los sistemas necesarios para la operación de la app. • Ayudan al desarrollo inicial, mantenimiento y actualizaciones de la plataforma.	• Acceso a información no confidencial, como números telefónicos actualizados de operadores, procesos actuales para realizar bloqueos (bancarios, SIM, dispositivos) • Acceso a los procedimientos de la policía para realizar denuncias. • Estar al día con las tendencias tecnológicas y las modalidades de robo emergentes.	• Guiar al usuario a través de pasos personalizados para proteger su información y dispositivos. • Incluye funciones como un chatbot para resolver dudas, acceso a un agente humano (opción premium), bloqueo de dispositivos y líneas, y guías actualizadas para realizar denuncias.	• Garantiza resultados como bloqueos exitosos, la tranquilidad del usuario, y soluciones rápidas que minimizan el impacto del robo.	• Diseñado para usuarios finales (personas que han sufrido robos) • Propuesto a entidades financieras, quienes se benefician del aumento de confianza y la reducción de fraudes.

Fuente: Elaboración Propia

6.2.3.3. Organización y Estructura del Personal

La estructura organizacional inicial estará compuesta por cuatro fundadores, quienes asumirán roles clave:

- CEO: Responsable de la dirección estratégica y la gestión de relaciones (comercial, marketing B2B) con socios clave.
- CFO: Encargado de las finanzas, presupuestos y cobros a las entidades financieras.
- COO: Responsable de las operaciones, incluyendo la coordinación con los proveedores de TI y la supervisión de procesos internos.
- CTO: Líder técnico que gestiona el desarrollo, mantenimiento y actualizaciones de la aplicación.

Para optimizar recursos, se tercerizarán funciones como contabilidad, soporte legal y algunos desarrollos técnicos específicos, contratando equipos por proyecto con pagos por honorarios.

6.2.3.4. Instalaciones y Recursos Necesarios

El equipo trabajará inicialmente de manera remota o desde oficinas compartidas como WeWork. Esto permitirá reducir costos y mantener flexibilidad operativa en las primeras etapas. Conforme el proyecto madure, se evaluará la transición a oficinas in-house.

En cuanto a la infraestructura tecnológica, los recursos clave incluirán servidores en la nube para almacenar información y garantizar el rendimiento de la app, herramientas de desarrollo de software, y sistemas de análisis para monitorear el uso de la plataforma y la satisfacción del cliente.

6.2.3.5. Licencias y Regulaciones

Para operar legalmente en Perú, la app deberá cumplir con la Ley de Protección de Datos Personales, garantizando la seguridad y privacidad de los usuarios. Además, será fundamental obtener la aprobación de ASBANC y de cada entidad financiera que desee suscribirse al servicio. Estas certificaciones no solo garantizarán el cumplimiento normativo, sino que también reforzarán la confianza de las entidades y los usuarios en la plataforma.

6.2.3.6. Costos de Operación

Como visto en nuestro modelo financiero, los costos de operación incluirán gastos administrativos, sueldos, marketing, mantenimiento de servidores, y otros gastos operativos como el alquiler de oficinas compartidas. Estos gastos estarán alineados con las proyecciones financieras previas, con un fuerte enfoque en optimizar recursos a través de la tercerización y el uso de herramientas digitales.

6.2.3.7. Proyección de Demanda

El crecimiento se proyecta en función del número de entidades financieras captadas. Durante el primer año, se espera trabajar con seis entidades, alcanzando 37 entidades para el quinto año, con un total de 49 entidades financieras en el mercado peruano. A continuación, se muestra el detalle en la Tabla 55.

Tabla 55. Proyección de entidades financieras asociadas por año

Tipo Entidad	Año 1	Año 2	Año 3	Año 4	Año 5
Bancos	2	4	10	10	14
Financieras	2	4	8	9	19
Cajas Municipales	2	4	10	10	13
No. Entidades Financieras	6	12	28	28	37

Fuente: Elaboración Propia

6.2.3.8. Gestión de riesgos operativos

Para garantizar la continuidad del servicio y el cumplimiento normativo, se implementará un enfoque proactivo para la gestión de riesgos operativos. Los principales riesgos identificados incluyen interrupciones tecnológicas, barreras regulatorias y baja adopción por parte de los usuarios.

En cuanto a las interrupciones tecnológicas, los riesgos abarcan fallos en los servidores o en la infraestructura de la nube, así como errores en el software que puedan impactar la funcionalidad de la aplicación. Para mitigar estos riesgos, se utilizarán herramientas de monitoreo en tiempo real que permitan detectar y resolver problemas técnicos antes de que afecten a los usuarios. Además, se realizarán copias de seguridad automáticas diarias de la base de datos para garantizar una recuperación rápida en caso de incidentes, junto con pruebas de estrés y actualizaciones frecuentes del software para mantener la capacidad y la seguridad del sistema.

Las barreras regulatorias representan otro desafío importante. Segurazo deberá cumplir con requisitos legales como la Ley de Protección de Datos Personales en Perú y

obtener certificaciones de entidades financieras asociadas, como ASBANC. Para abordar estos riesgos, se contratarán servicios de asesoría legal especializada que aseguren el cumplimiento normativo en todos los aspectos operativos. También se llevarán a cabo auditorías internas y externas periódicas para verificar que los procesos de manejo de datos cumplen con las regulaciones vigentes.

Un tercer riesgo identificado es la baja adopción de la plataforma por parte de los usuarios finales. Esto puede deberse a la falta de conocimiento sobre Segurazo en segmentos clave del mercado o a dificultades para generar confianza en usuarios que no están familiarizados con herramientas tecnológicas. Para enfrentar este desafío, se implementarán campañas de marketing educativo en redes sociales y medios digitales, diseñadas para concienciar a los usuarios sobre los riesgos de fraude financiero y las soluciones que ofrece la plataforma. Asimismo, se realizarán pruebas piloto con grupos focales para ajustar las funcionalidades según sus comentarios y mejorar la experiencia del usuario.

Impacto potencial en costos y cronogramas

Desde el punto de vista financiero, la implementación de servidores redundantes, estimamos que las herramientas de monitoreo y estrategias de marketing educativo podría incrementar los costos operativos en un 10%. Además, las auditorías regulatorias y la diversificación de alianzas requerirán inversiones adicionales en equipos legales y técnicos.

En cuanto a los cronogramas, la baja adopción inicial podría extender los tiempos previstos para alcanzar los objetivos de usuarios activos, ajustando las metas de crecimiento a mediano plazo. Por otro lado, los retrasos en la integración con aliados estratégicos podrían afectar los cronogramas de lanzamiento de ciertas funcionalidades clave.

6.2.3.9. Factibilidad operativa

Costos de Implementación y Capital de Trabajo

Como visto previamente, la inversión inicial de Segurazo asciende a S/145,226,01 cubriendo costos de desarrollo, publicidad y adquisición de infraestructura tecnológica. Adicionalmente, el capital de trabajo inicial es de S/45,000, destinado a cubrir los primeros meses de operación, incluyendo costos de alquiler y personal administrativo.

Los costos operativos anuales muestran una tendencia de estabilización después del segundo año, disminuyendo de S/938,272 en el año 2 a S/541,182 en el año 5, reflejando una optimización en la estructura de costos mediante la implementación cada vez más avanzada de la IA.

Productividad de la Mano de Obra

Uno de los aspectos clave de la eficiencia operativa de Segurazo es la optimización del equipo de atención al cliente. La implementación de inteligencia artificial en el chatbot permitirá reducir progresivamente el número de operadores telefónicos de 7 en el año 1 a 2 en el año 5, logrando un ahorro anual en costos laborales.

- Costo anual de operadores telefónicos en el año 1: S/94,920
- Costo anual de operadores telefónicos en el año 5: S/27,120

La IA requerirá un gasto progresivo, iniciando en S/18,094 en el año 2 hasta alcanzar S/63,299 en el año 5, pero el ahorro en personal permitirá una compensación financiera a mediano plazo.

Tiempo de Procesamiento y Nivel de Servicio

El objetivo de Segurazo es proporcionar una respuesta rápida e inmediata a los usuarios en caso de robo de dispositivos móviles. La implementación cada vez más avanzada del chatbot con IA permitirá reducir significativamente los tiempos de atención, ya que un usuario podrá gestionar el bloqueo de su línea, tarjetas bancarias y otros servicios en cuestión

de segundos con aun mayor rapidez que el servicio lanzado inicialmente. El uso de IA optimiza el nivel de servicio, permitiendo que los usuarios reciban asistencia en tiempo real.

Márgenes Operativos y Rentabilidad

El análisis financiero proyecta que Segurazo alcanzará márgenes operativos positivos desde el segundo año, aumentando progresivamente su rentabilidad.

- Margen operativo en el año 2: 18%
- Margen operativo en el año 4: 87%
- Margen operativo en el año 5: 89%

Estos márgenes reflejan una estructura de costos eficiente, con ingresos crecientes y una optimización en los gastos operativos.

Por su lado, el flujo de caja libre proyectado muestra una sólida capacidad de generación de efectivo, en el año 1 se genera pérdida por S/92,680 y en el año 5 se logra obtener flujos de S/3,184,346. Esto indica que la empresa podrá financiar su crecimiento.

6.2.4. Simulaciones empleadas para validar las hipótesis de operaciones

El parámetro principal de las operaciones de Segurazo es el tiempo de atención, que se valida gracias a la simplicidad de la solución. Por tanto, el plan operativo de Segurazo es adecuado y factible, ya que responde a las necesidades clave del usuario y presenta ventajas competitivas claras frente a las alternativas del mercado. Este tiempo está directamente relacionado con el nivel de servicio y la experiencia del usuario en momentos críticos.

En base a esto, la hipótesis de nuestro plan de operaciones será: “Creemos que, durante el primer año de operaciones, el 90% de los usuarios que utilicen Segurazo lo harán en un tiempo menor a 5 minutos desde que inician la interacción”.

Para verificarlo, se realizará una simulación de Montecarlo basándonos en las pruebas de usabilidad, donde obtuvimos que en promedio el tiempo de uso de Segurazo fue de 3.57 minutos para realizar todas las acciones de bloqueo en caso de emergencia.

Este tiempo de 3.57 minutos será el escenario esperado, a partir del cual se estimarán los demás escenarios. El tiempo de uso de Segurazo es óptimo mientras menos sea el necesario por usuarios durante un caso de emergencia, mientras que será pesimista cuando el tiempo de uso sea mayor.

Tabla 56. Escenarios del tiempo de uso de Segurazo en caso de emergencia

Análisis de sensibilidad	crecimiento	**Tiempo de uso**
Muy optimista	0.00	**2.71**
Optimista	0.10	**2.98**
Esperado	0.20	**3.57**
Pesimisita	0.30	**4.64**
Muy pesimista	0.40	**6.50**
	Promedio	**4.08**
	DesvEstand	**1.54**

Elaboración propia

Luego de realizar la simulación de Montecarlo considerando 5,000 pruebas se obtienen los siguientes resultados.

Tabla 57. Resultados de la simulación de Montecarlo para Operaciones

Promedio	**4.000**
Desviación estándar	**1.566**
Mínimo	**-1.615**
Máximo	**8.914**
Alta eficiencia: <5min	**73.26%**

Elaboración propia

A partir de esto, se llega a la conclusión de que más del 70% de casos los usuarios que elijan a Segurazo en un caso de emergencia les tomará menos de cinco minutos en lograr

bloquear su información sensible, siendo guiado con rapidez lo cual minimizará el impacto en caso de una emergencia.

6.3. Validación de la viabilidad de la solución

6.3.1. Presupuesto de inversión

Como se mencionó en la sección 5.2., la inversión inicial será de S/ 135,871 soles y está compuesto por presupuesto para activo fijo, desarrollo de la web, plan de marketing y el costo de partidas registrales. Asimismo, añadimos un saldo generado por el capital de trabajo que se necesitará para cubrir los gastos operativos iniciales (primer mes) por valor de S/ 45,000. Ver tabla 58 y 59.

Tabla 58. Detalle de inversión inicial

Descripción	Saldo	
Registrales	S/	861
Activo Fijo	S/	23,320
Intangibles (Desarrollo en nube, software)	S/	50,490
Marketing	S/	66,555
Alimentación	S/	4,000
Total	**S/**	**145,226**

Fuente: Elaboración Propia

Tabla 59. Detalle de capital de trabajo inicial

Descripción	Costo Total S/
Alquiler de oficina y servicios (luz, agua, internet)	S/15,000
Personal administrativo (4 personas)	S/30,000
Total	S/45,000

Fuente: Elaboración Propia

En total se requerirá de S/ 190,226 para iniciar el proyecto. El 60% será cubierto por los 4 accionista.

6.3.2. Análisis financiero

Para llevar a cabo este análisis financiero, se ha establecido un horizonte de evaluación de cinco años para el proyecto. Se emplea una tasa de descuento del 15.7%,

correspondiente al costo promedio ponderado de capital. El 40% de la inversión inicial, equivalente a S/ 76,090, será financiado por una entidad financiera, aplicando una tasa activa de mercado en moneda nacional del 10.09%, que es la tasa para medianas empresas mínima que existe en el mercado bancario según la Superintendencia de Banca, Seguros y AFP (SBS) a noviembre 2024, tal como se detalla a continuación. Ver tabla 60 y 61.

Tabla 60. Estructura de Capital

Estructura de Capital	
Deuda Bancaria	S/76,090.41
Aporte Accionistas	S/114,135.61
Total	S/190,226.01

Fuente: Elaboración Propia

Tabla 61. Obtención del costo promedio ponderado de capital (WACC)

Calculo WACC	
Porcentaje de Deuda de la Inversión (Wd)	60%
Porcentaje de aporte de la Inversión (Ws)	40%
Tasa activa del mercado	10%
Tasa efectiva anual	20%
Impuesto a la renta	29.5%
WACC	**15%**

Fuente: Elaboración Propia

Para la elaboración del VAN financiero y económico se obtuvo el Flujo de Caja Libre (FCL) a partir de las proyecciones de ingresos y costos desarrollados en el capítulo 5.2. Asimismo, para la elaboración de dicha proyección se asume el principio de empresa en marca, lo cual significa que la empresa seguirá operando de manera perpetua. Ver tabla 62.

Tabla 62. Evaluación económica y financiera

Evaluación Económica y Financiera						
Evaluación Económica	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Inversión Inicial	-145,226	-	-	-	-	-
Flujo Anual	-	-92,680	162,444	2,068,760	2,622,024	3,184,346
Flujo Descontado	-145,226	-80,621	122,923	1,361,768	1,501,391	1,586,142
VAN Económico	4,346,376	-	-	-	-	-
TIR Económica	1.79	-	-	-	-	-
Evaluación Financiera	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**

Inversión Inicial	-145,226	-	-	-	-	-
Flujo Anual		-110,508	144,248	2,050,160	2,602,979	3,164,812
Flujo Descontado	-69,136	-91,915	99,792	1,179,685	1,245,781	1,259,830
VAN Financiera	3,624,038	-	-	-	-	-
TIR Financiera	2.27	-	-	-	-	-

Fuente: Elaboración Propia

6.3.3. Simulaciones empleadas para validar las hipótesis

Para validar la hipótesis de viabilidad, consideramos que el negocio generará un VAN de S/ 4,346,376.01. Como primer paso, se efectuó un análisis económico y financiero, obteniendo los indicadores VAN y TIR, que confirman la posibilidad de alcanzar el VAN señalado en ese periodo. Los detalles de estos datos se encuentran en el apartado de análisis financiero 6.3.2, en la tabla 60,61 y 62. Además, se llevó a cabo una simulación de Montecarlo para evaluar escenarios posibles. Ver tabla 63.

Tabla 63. Simulación de Montecarlo para validación de viabilidad del negocio

Años	0	1	2	3	4	5
Flujo de caja neto	-69,136	-110,508	144,248	2,050,160	2,602,979	3,164,812
CAMP	15%					
Valor Actual Neto (VAN)	4,360,311					
Tasa Interna de Retorno	227%					
Periodo de retorno	2.17					

Simulación en 5000 escenarios	
VAN promedio simulado	4,594,678
VAN desviación estándar simulada	941,958
VAN mínimo	1,084,293
VAN máximo	8,220,587
Riesgo de Pérdida	5.5%

Fuente: Elaboración Propia

Al analizar el Valor Actual Neto (VAN) promedio de los 5000 escenarios evaluados, se observa una probabilidad del 94% de lograr un VAN superior a US$1,000,000. Ver Apéndice D.

Por otro lado, se realizó el análisis de sensibilidad en el cual se consideraron diferentes escenarios del porcentaje de mercado de usuarios que logramos captar año a año.

El escenario esperado es que Segurazo tenga el 35% del mercado en el año 1, hasta llegar a 75% en el año 5. Estos porcentajes variaran según el escenario muy optimista (con tasas de 555 en el año 1 hasta 95% en el año 5), optimista, pesimista y muy pesimista. Asimismo, como se describe en el capítulo 5.2.3, la participación de mercado es clave para calcular los ingresos que generarían los usuarios y en consecuencia el tarifario que determinaríamos para cada tipo de entidad financiera.

Tabla 64. Porcentaje de participación de mercado para cada escenario

Año	1	2	3	4	5
Muy optimista	55%	65%	85%	90%	95%
Optimista	45%	55%	75%	80%	85%
Esperado	35%	45%	65%	70%	75%
Pesimista	25%	35%	55%	60%	65%
Muy Pesimista	15%	25%	45%	50%	55%

Fuente: Elaboración Propia

Se debe aclarar que VAN y TIR serán impactados según el escenario que se elija de la tabla 64. Por ejemplo, si se elije un escenario muy optimista, entonces el número de usuarios que se atendería será mayor, por tanto, bajo los supuestos descritos en el capitulo 5.2.3, el ingreso a exijir a cada entidad será mayor, por lo que el precio exigido en el contrato a la entidad financiera se elevará. Para mayor detalle de cada escenario ver el Apéndice E.

Tabla 65. Resultados de sensibilidad de modelo de negocio

Escenario	Muy pesimista	Pesimista	Esperado	Optimista	Muy optimista
WACC	14.96%	14.96%	14.96%	14.96%	14.96%
CAMP	20.23%	20.23%	20.23%	20.23%	20.23%
VAN (FCL)	S/2,283,536	S/3,238,953	S/4,346,376	S/5,149,788	S/6,105,205
VAN (FCA)	S/1,852,598	S/2,674,407	S/3,624,038	S/4,318,025	S/5,139,834
TIR (FCL)	96.77%	135.42%	178.90%	222.69%	270.99%
TIR (FCA)	324.14%	243.99%	217.42%	160.22%	135.59%

Fuente: Elaboración Propia

Las tarjetas de pruebas y aprendizajes son las siguientes tablas:

Tabla 66. Consolidado de tarjetas de pruebas de viabilidad

Hipótesis (Riesgo)		
H1: Creemos que la propuesta de negocio será rentable porque obtendrá ganancias por US $1'000,000 al quinto año de iniciar operaciones.		
Prueba (Viabilidad)	**Métrica (tiempo)**	**Criterio**
Prueba 1: Para verificarlo, nosotros se realizará una evaluación económica y financiera para obtener indicadores como el VAN y la TIR.	**M1:** Se espera conseguir un beneficio de US $1'000,000 al quinto año de haber iniciado operaciones.	Estamos bien si al quinto año de operación se obtiene un beneficio de US $1'000,000 o más.
Prueba 2: Para verificarlo, se realizará la simulación de Montecarlo con 5,000 iteraciones.	**M2:** Se medirá la probabilidad de obtener un VAN de US $1'000,000 o más.	Estamos bien si la probabilidad de obtener un VAN de US $1'000,000 o más alcanza al 70%.

Fuente: Elaboración Propia

Tabla 67. Consolidado de tarjetas de aprendizaje de viabilidad

Hipótesis (Riesgo)		
H1: Creemos que la propuesta de negocio será rentable porque obtendrá ganancias por US $1'000,000 al quinto año de iniciar operaciones.		
Observación	**Aprendizaje y Reflexiones**	**Decisiones y acciones**
Obtuvimos como resultado un VAN de S/ 3,727 mil en el escenario esperado	De ello aprendimos que la evidencia apoya nuestra hipótesis.	Se consideró realizar un análisis de sensibilidad y simulación de Montecarlo
Se observo que se tiene una probabilidad de 93% de obtener un VAN superior a USD 1 millón en el escenario esperado	De ello aprendimos que la evidencia apoya nuestra hipótesis	Por lo tanto, concluimos con la prueba de viabilidad

Fuente: Elaboración Propia

Tabla 68. Resultados de validar las hipótesis de negocio

Dimensión	Hipótesis	Prueba	Resultado	¿Se acepta?
Deseabilidad	H1: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar fácilmente el aplicativo Segurazo en situaciones de robo, validado mediante pruebas de usabilidad que demuestren su efectividad y aceptación	Prueba 1: Prueba de usabilidad donde tiempo promedio de uso >= 3 min	2.57	Sí
		Prueba 2: Prueba de usabilidad donde tiempo promedio de uso >= 3 min	95%	Sí
	H2: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su banco en caso de pérdida o robo de su dispositivo celular, gestionando el bloqueo de sus tarjetas para proteger sus cuentas financieras.	Prueba 3: Prueba de usabilidad donde porcentaje de éxito >=68%	96.5%	Sí
		Prueba 4: Prueba de usabilidad donde tiempo promedio de uso >= 3 min	3.57	Sí
	H3: Creemos que los ciudadanos de 18 a 65 años a nivel nacional podrán usar el asistente virtual 'Segurazo' para contactar a su operador telefónico en situaciones simuladas de robo de dispositivo, facilitando el bloqueo de sus líneas telefónicas para prevenir la suplantación de su número o la copia de su IMEI.	Prueba 5: Prueba de usabilidad donde porcentaje de éxito >=68%	96.5%	Sí
		Prueba 6: Prueba de usabilidad donde tiempo promedio de uso >= 2 min	2	Sí

Dimensión	Hipótesis	Prueba	Resultado	¿Se acepta?
		Prueba 7: Prueba de usabilidad donde porcentaje de éxito >=68%	96.2%	Sí
	H4: Creemos que los ciudadanos de 18 a 65 años a nivel nacional utilizarán "Segurazo" para ajustar la seguridad de sus dispositivos en situaciones simuladas de pérdida o robo de dispositivo para impedir que sus datos sensibles sean accedidos por terceros.	Prueba 8: Prueba de usabilidad donde tiempo promedio de uso >= 10 min	4.5	Sí
Deseabilidad		Prueba 9: Prueba de usabilidad donde porcentaje de éxito >=68%	96%	Sí
	H5: Creemos que los ciudadanos de 18 a 65 años a nivel nacional realizarán denuncias policiales a través del asistente virtual "Segurazo" en situaciones simuladas en las cuales les roben el celular y requieran realizar una denuncia ante una autoridad.	Prueba 10: Prueba de usabilidad donde tiempo promedio de uso >= 30 min	14	Sí
Factibilidad	H10: Hipótesis sobre desempeño del plan de marketing	Simulación de Montecarlo del Plan de Mercadeo	El 92.06% de las simulaciones la ratio LTV/CAC esta entre 7 y 9	Sí
Viabilidad	H 11: Hipótesis sobre simulación del VAN	Simulación de Montecarlo del VAN	Riesgo de VAN menor a USD 1 MM es 5.49%	Sí

Fuente: Elaboración Propia

Capítulo VII. Solución Sostenible

7.1. Relevancia Social de la Solución

En un mundo cada vez más digitalizado, la seguridad de la información personal y financiera es una preocupación clave para los usuarios. Segurazo contribuye a la sostenibilidad social al prevenir fraudes y mejorar la seguridad digital, reduciendo la exposición de los usuarios a riesgos derivados del robo de dispositivos móviles.

Actualmente, los teléfonos móviles almacenan una cantidad significativa de información personal, profesional y financiera, lo que los convierte en objetivos atractivos para el fraude y la delincuencia digital. Las pérdidas económicas y el impacto psicológico asociado a estos incidentes afectan directamente la calidad de vida de las personas, generando una necesidad urgente de soluciones eficientes y accesibles.

Segurazo responde a esta necesidad de manera sostenible al proporcionar una plataforma accesible, gratuita y centralizada que agiliza los procesos de bloqueo y denuncia, disminuyendo el tiempo de respuesta ante incidentes de robo o pérdida. Esta solución reduce el impacto negativo del fraude y refuerza una cultura de prevención digital al educar a los usuarios sobre la importancia de la seguridad cibernética.

El Lienzo Modelo Próspero de la Figura 34 para Segurazo representa cómo la solución interactúa con el contexto social, económico y ambiental, considerando recursos, relaciones, y los impactos positivos y negativos de la solución en la sociedad. A continuación, se presenta el lienzo en el cual se detallan los elementos clave para lograr un impacto social y ambiental positivo.

Figura 34. Lienzo modelo próspero

<table>
<tr><td rowspan="3">Medio Ambiente</td><td colspan="5">En Perú, los usuarios de dispositivos móviles enfrentan el riesgo de robo y vulneración de su información financiera y personal, por lo que es necesaria una herramienta accesible que contribuya a la seguridad digital.</td></tr>
<tr><td>Sociedad</td><td colspan="4">En la sociedad actual, el uso de dispositivos móviles se ha convertido en un elemento indispensable en la vida cotidiana, lo que ha incrementado la exposición de los usuarios a riesgos de seguridad y fraude digital. Según datos del estudio realizado, cuando un usuario sufre el robo o pérdida de su celular, el proceso de búsqueda de contactos de bancos, operadores y entidades policiales para gestionar bloqueos puede tomar hasta 20 minutos, lo que prolonga su vulnerabilidad ante posibles fraudes. En este contexto, Segurazo optimiza este proceso al centralizar en una sola plataforma la información necesaria, reduciendo el tiempo de acceso a estos contactos a un promedio de 3.45 minutos. Al contar con esta información de manera inmediata, los usuarios pueden iniciar sus gestiones de bloqueo de manera más eficiente, minimizando riesgos y acelerando la respuesta ante incidentes de seguridad. Su diseño accesible y gratuito permite que cualquier persona, independientemente de su nivel de conocimientos tecnológicos, utilice la plataforma sin dificultad. Además, Segurazo fomenta una cultura de prevención digital, incentivando prácticas seguras para reducir la exposición al fraude.</td></tr>
<tr><td colspan="5">El impacto económico de los fraudes digitales y del robo de identidad representa una pérdida significativa tanto para los usuarios individuales como para las instituciones financieras. Segurazo contribuye a reducir estos costos al facilitar un contacto rápido y centralizado con bancos, operadores móviles y autoridades, lo cual permite una respuesta ágil y minimiza las pérdidas financieras. Además, Segurazo apoya la economía al reducir la necesidad de servicios de atención física y los costos operativos relacionados con la atención de incidentes de robo y fraude digital.</td></tr>
<tr><td rowspan="2">Existencias Biofísicas</td><td colspan="2">Procesos</td><td>Valor</td><td colspan="2">Personas</td><td rowspan="2">Actores del Ecosistema</td></tr>
<tr><td>Recursos</td><td>Alianzas</td><td>Co-creación de valor</td><td>Relaciones</td><td>Actores clave</td></tr>
<tr><td>El ecosistema digital en el que opera la plataforma Segurazo, que incluye servidores de almacenamiento en la nube y dispositivos de los usuarios, depende de varios recursos físicos. Entre estos se encuentra la energía eléctrica utilizada para el funcionamiento de los servidores y el acceso de los usuarios. La tecnología en la nube ayuda a reducir la necesidad de infraestructura física extensa, disminuyendo así la huella de carbono asociada a centros de datos.</td><td>Equipo especializado en desarrollo de software y ciberseguridad para mantener altos estándares de protección.
Personal administrativo y de soporte técnico para la gestión y atención al cliente.
Capital financiero para cubrir los costos operativos y de infraestructura tecnológica.
Infraestructura tecnológica en la nube que permite escalar la plataforma y garantizar la seguridad de los datos.</td><td>Colaboración con entidades financieras como bancos y cooperativas, que permiten la integración y uso de sus servicios.
Alianzas estratégicas con operadores de telecomunicaciones para facilitar la rapidez en la respuesta ante incidentes.
Acuerdos con autoridades de seguridad (policía, ministerios) para mejorar los procesos de denuncia de robo de dispositivos.
Relación con instituciones educativas y ONGs para promover la concientización sobre seguridad digital en el país.</td><td>Para los usuarios: Brindar una plataforma que permita reaccionar rápidamente ante situaciones de robo o pérdida de dispositivos, facilitando el contacto directo con instituciones financieras, operadores móviles y autoridades para proteger sus activos e información personal.
Para instituciones financieras y operadores móviles: Aumentar la confianza de los clientes en la seguridad de sus transacciones, contribuyendo a una reducción de fraudes y fortaleciendo el ecosistema digital seguro. Segurazo se convierte en un aliado estratégico que promueve una respuesta ágil y efectiva ante incidentes de seguridad digital, alineándose con los objetivos de sostenibilidad y prevención de fraudes.
Para la sociedad en general: Fomentar una cultura de seguridad digital y prevención en un contexto donde la información personal es vulnerable. La solución contribuye al bienestar social y financiero de los usuarios al minimizar los riesgos asociados a la pérdida de dispositivos, promoviendo prácticas de protección de datos en la comunidad.</td><td>Segurazo establece una comunicación constante y de apoyo con los usuarios mediante atención personalizada y orientación en momentos críticos. Esto incluye una relación directa a través de su plataforma, con una guía práctica en situaciones de emergencia para proteger la información y los recursos financieros del usuario.</td><td>Los actores principales incluyen usuarios finales (personas que desean proteger sus datos y recursos en caso de robo o pérdida), instituciones financieras y operadores móviles, que juegan un rol esencial en la conexión rápida y eficiente en momentos de necesidad. Otros actores importantes son las autoridades, quienes facilitan el proceso de denuncia en caso de incidentes.</td><td>Usuarios finales: personas que desean proteger su información y sus activos digitales ante situaciones de inseguridad.
Instituciones financieras y bancarias: actores clave en la prevención de fraude y en la protección de activos financieros.
Operadores de telecomunicaciones: permiten el bloqueo o gestión de líneas móviles en casos de pérdida o robo de dispositivos.
Entidades reguladoras y gubernamentales: supervisan la seguridad digital y promueven la responsabilidad social en las prácticas de protección de datos.
Comunidad en general: se beneficia de una reducción en el fraude y de un entorno digital más seguro.</td></tr>
<tr><td>Servicios Ecológicos</td><td>Actividades</td><td>Gobernanza</td><td>Destrucción de Valor</td><td colspan="2">Canales</td><td>Necesidades</td></tr>
<tr><td>Reducción en el uso de papel al digitalizar los procesos de denuncia y bloqueo de dispositivos.
Uso de energía renovable para los servidores que alojan la plataforma, contribuyendo a una menor huella de carbono.
Optimización de recursos tecnológicos para disminuir el consumo energético en el almacenamiento y procesamiento de datos.</td><td>Desarrollo continuo de la plataforma para adaptarse a nuevas amenazas de ciberseguridad.
Campañas de concientización y educación en seguridad digital y prevención del fraude para usuarios finales.
Soporte técnico especializado en tiempo real para ayudar a los usuarios durante situaciones de emergencia, como el robo de dispositivos.</td><td>Supervisión de la plataforma por un equipo de liderazgo en ciberseguridad y protección de datos.
Cumplimiento de normativas de privacidad y regulaciones de seguridad para proteger la información de los usuarios.
Monitoreo constante y mejora de la infraestructura para garantizar una respuesta eficiente y segura ante posibles incidentes.</td><td>Posibles brechas de seguridad que resulten en el acceso no autorizado a información sensible.
Mala experiencia de usuario debido a problemas técnicos o falta de usabilidad, lo cual podría disminuir la confianza en la plataforma.</td><td colspan="2">Segurazo utiliza varios canales de comunicación y soporte, como su plataforma web y las redes sociales, para llegar a los usuarios y brindar la ayuda necesaria de manera ágil. También se prevé la integración de notificaciones automáticas para alertar a los usuarios sobre la importancia de proteger sus datos.</td><td>Seguridad: necesidad de proteger los datos personales y financieros ante situaciones de robo o pérdida.
Acceso rápido a información de contacto y guías de emergencia para actuar en momentos críticos.
Educación en prácticas de seguridad digital para reducir el riesgo de fraudes.
Accesibilidad: facilidad de uso para que la plataforma esté disponible para todos los usuarios, sin importar su nivel de conocimiento tecnológico.
Cumplimiento con las regulaciones de seguridad y protección de datos.</td></tr>
<tr><td colspan="7">RESULTADOS</td></tr>
</table>

Fuente: Elaboración Propia

Alineación con el Objetivo de Desarrollo Sostenible 16.4

Segurazo tiene un impacto significativo en la vida de los usuarios y en la comunidad al ofrecer una solución integral para la protección de información personal y financiera en situaciones de robo o pérdida de dispositivos. Con el creciente uso de teléfonos móviles en la vida cotidiana, la dependencia de estos dispositivos para gestionar aspectos personales y profesionales ha aumentado considerablemente. En este contexto, la seguridad de los datos almacenados en los dispositivos móviles adquiere una importancia esencial para la estabilidad financiera y digital de los usuarios.

Uno de los principales beneficios de Segurazo es la reducción del tiempo de respuesta ante incidentes de seguridad digital. Los métodos tradicionales de gestión de bloqueos y denuncias pueden tardar hasta 20 minutos, mientras que Segurazo reduce este tiempo a un promedio de 3.45 minutos al centralizar contactos con bancos, operadores móviles y autoridades. Esta reducción minimiza la exposición del usuario al fraude y fortalece su capacidad de reacción inmediata.

Segurazo también contribuye a disminuir las pérdidas económicas derivadas del fraude digital y el robo de identidad. Según datos recopilados en el estudio, una intervención temprana permite reducir la probabilidad de transacciones fraudulentas y el acceso no autorizado a información confidencial. Al proporcionar una plataforma de acceso inmediato, Segurazo facilita la recuperación de cuentas y disminuye el impacto financiero en los usuarios afectados.

Otro aspecto clave del impacto de Segurazo es su contribución al fortalecimiento de la cultura de prevención digital. A través de su plataforma, los usuarios reciben orientación clara y accesible sobre los pasos a seguir en caso de robo, promoviendo prácticas de autoprotección y educación en seguridad digital. Esto reduce la vulnerabilidad a incidentes de fraude y promueve un ecosistema digital más seguro y resiliente.

Para medir la efectividad de Segurazo y su contribución al ODS 16.4, se han definido indicadores específicos que permiten evaluar su impacto en la protección de datos personales, la reducción del fraude y la cooperación entre entidades financieras y de telecomunicaciones. En la Tabla 69, se detallan estos indicadores junto con sus respectivas métricas de medición.

Tabla 69. Metas e indicadores para evaluar la efectividad

Meta (ODS 16.4)	Impacto del modelo de negocio	Indicador de medición
16.4.1: Reducir los flujos financieros ilícitos	Segurazo contribuye a la reducción del fraude digital al facilitar el bloqueo rápido de cuentas y la eliminación de datos personales en dispositivos robados.	Porcentaje de usuarios que han bloqueado sus cuentas o eliminado su información de dispositivos robados de manera efectiva.
16.4.2: Proteger la información personal y financiera de los usuarios	Segurazo permite que los usuarios eliminen de forma remota la información confidencial de sus dispositivos para que no caiga en manos equivocadas.	Porcentaje de usuarios que lograron eliminar su información de manera remota tras el robo de su dispositivo.
16.4.3: Mejorar la cooperación entre entidades financieras y tecnológicas	Segurazo facilita la colaboración entre bancos, operadores móviles y autoridades para proteger al usuario y evitar el fraude financiero.	Cantidad de alianzas con entidades financieras y operadores móviles para agilizar el proceso de bloqueo y protección de datos.
16.4.4: Fomentar la educación en seguridad digital	Segurazo proporciona orientación clara y accesible para que los usuarios tomen las medidas necesarias para proteger su información tras un robo, promoviendo la autoprotección.	Nivel de satisfacción de los usuarios en encuestas sobre la educación en seguridad digital brindada.
16.4.5: Facilitar el acceso rápido a servicios financieros en emergencias	Segurazo permite a los usuarios gestionar de forma rápida y centralizada el bloqueo de cuentas bancarias y líneas móviles tras un robo.	Tiempo promedio que tardan los usuarios en completar el proceso de bloqueo tras el robo de su dispositivo.
16.4.6: Reducir el riesgo de acceso no autorizado a información sensible	Segurazo ayuda a minimizar el riesgo de acceso a información privada mediante su sistema de guía para bloquear cuentas y dispositivos.	Reducción porcentual en casos de fraude digital reportados por usuarios tras usar Segurazo.
16.4.7: Fomentar una cultura de autoprotección entre los usuarios	Segurazo promueve prácticas seguras para el manejo de datos digitales, reduciendo el riesgo de exposición al fraude.	Porcentaje de usuarios que adoptan medidas preventivas después de utilizar Segurazo.
16.4.8: Apoyar la sostenibilidad mediante la reducción de visitas físicas	Segurazo ayuda a evitar visitas físicas a sucursales, facilitando la gestión digital de bloqueos y denuncias.	Porcentaje de usuarios que realizan gestiones digitales sin necesidad de acudir a una sucursal.

Fuente: Elaboración Propia

Luego de analizar el impacto de Segurazo en relación con los Objetivos de Desarrollo Sostenible (ODS) vinculados, se calculó el Índice Total de Alcance en Sostenibilidad (TSRI). El ODS 16.4 cuenta con un total de 12 metas, de las cuales Segurazo contribuye a 8, lo que representa un TSRI de 66.70%. Este índice se obtiene al dividir el número de metas movilizadas en la propuesta entre el total de metas establecidas para el ODS correspondiente, permitiendo medir el grado de contribución del proyecto a la sostenibilidad.

Este análisis se basa en los tiempos de respuesta y adopción esperada determinados en capítulos previos, donde se evaluaron los procesos actuales de toma de contacto con bancos, operadores móviles y autoridades para gestionar bloqueos y denuncias. En este sentido, Segurazo agiliza el acceso a la información y los canales adecuados para que los usuarios puedan tomar acción de manera rápida y efectiva. Este resultado sitúa a Segurazo como una solución con un impacto significativo en la optimización de tiempos de respuesta y en la prevención del fraude, facilitando la reacción inmediata de los usuarios ante incidentes de seguridad digital.

En la Tabla 70, se presentan los resultados obtenidos tras la evaluación del TSRI..

Tabla 70. Medición del TSRI

ODS	Metas de la ODS	Metas movilizadas
ODS 16	12	8
TSRI		**66.70%**

Fuente: Elaboración Propia

Para reforzar el impacto de Segurazo en la optimización del tiempo de respuesta y la prevención del fraude, resulta relevante compararlo con otras soluciones existentes en el mercado. En Perú, la alternativa más cercana es ASBANC 1820, una central telefónica que permite a los usuarios contactar a su banco para gestionar bloqueos de cuentas. Sin embargo, esta solución está enfocada exclusivamente en la banca y no abarca una gestión integral de la seguridad digital tras un robo.

A diferencia de ASBANC 1820, Segurazo integra múltiples actores clave en un solo lugar, permitiendo a los usuarios acceder rápidamente a bancos, operadoras y comisarías, además de proporcionar guías para la eliminación remota de datos. Además, Segurazo ha desarrollado un Índice de Relevancia Social (IRS) para medir su impacto en la reducción del tiempo de respuesta ante incidentes y la prevención del fraude, alineándose con los Objetivos de Desarrollo Sostenible (ODS).

A continuación, se presenta una comparación entre Segurazo y ASBANC 1820, resaltando las diferencias clave en funcionalidad, eficiencia y alcanc (Tabla 71):

Tabla 71. Segurazo vs. ASBANC 1820

Característica	**Segurazo**	**ASBANC 1820**
Centraliza contactos en una sola vista	☑ Sí (bancos, operadores y comisarías en un solo lugar)	❌ No (el usuario debe llamar a cada banco individualmente)
Acceso a bancos y operadoras móviles	☑ Sí (muestra números y enlaces directos)	☑ Sí (solo bancos)
Incluye guías de eliminación de datos	☑ Sí (pasos para borrar información del celular y proteger cuentas)	❌ No
Facilita la denuncia en comisarías	☑ Sí (contactos y orientación para la denuncia)	❌ No
Tiempo estimado de respuesta	**3.45 min** (acceso inmediato a contactos y guías)	**20 min** (llamadas separadas a cada banco)
Proceso de bloqueo	☑ El usuario selecciona su banco y llama directamente desde la plataforma	❌ El usuario debe marcar el 1820 y luego llamar a cada banco

Fuente: Elaboración Propia

Actualmente, ASBANC 1820 es la única iniciativa en Perú enfocada en la centralización de contactos para el bloqueo de cuentas bancarias en casos de robo. Sin embargo, no cuenta con un sistema de medición de impacto social ni con un Índice de Relevancia Social (IRS). A diferencia de esta alternativa, Segurazo ha desarrollado una metodología propia para cuantificar su contribución a la reducción del tiempo de respuesta ante incidentes, la prevención del fraude y la protección de datos personales. En la región, no se han identificado soluciones comparables que integren una medición estructurada de impacto

social en seguridad digital, lo que posiciona a Segurazo como una propuesta pionera en su categoría.

Para validar la viabilidad y el impacto de Segurazo en la prevención de fraudes y la optimización de la respuesta ante incidentes, se sostuvieron reuniones con el Gerente General de ASBANC y con el Presidente del Comité Estratégico de Gestión de Riesgos Integrales de Seguridad de ASBANC. Durante estas sesiones, se destacó la capacidad de Segurazo para centralizar la información clave y agilizar la toma de decisiones en situaciones críticas. Ambos representantes identificaron a Segurazo como una alternativa innovadora con potencial para generar sinergias dentro del ecosistema financiero y de seguridad digital en el país.

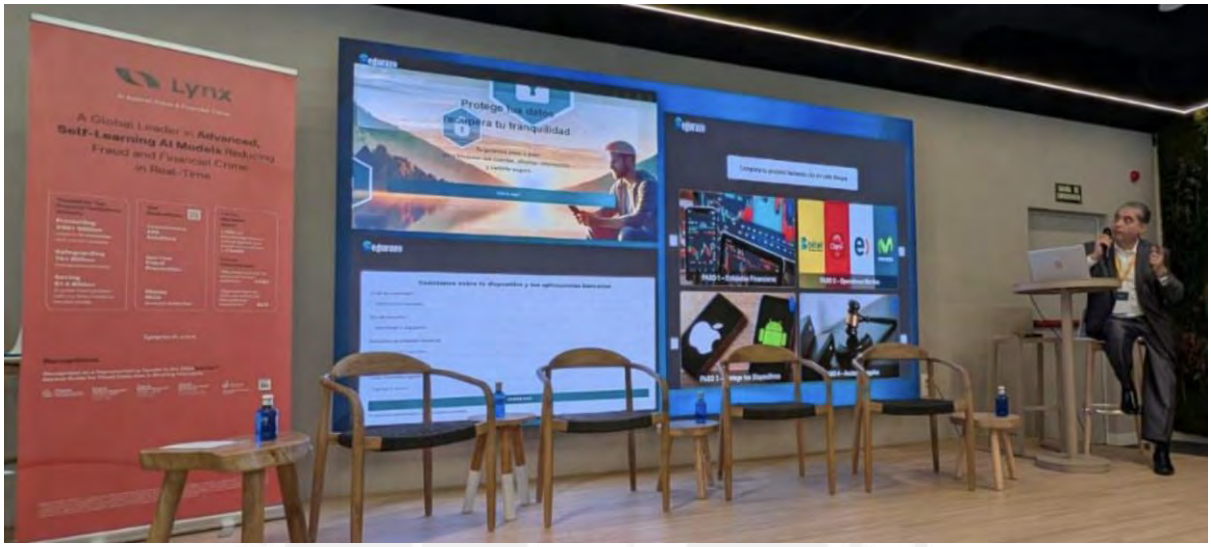
Reconocimiento y Validación del Proyecto

Como parte del desarrollo y validación de la propuesta, hemos trabajado en conjunto con el Presidente del Comité Estratégico de Gestión de Riesgos Integrales de Seguridad de ASBANC, quien nos brindó apoyo para presentar nuestro proyecto en un entorno de alto nivel. En particular, nuestra propuesta recibió una gran aceptación tanto desde la perspectiva del Gremio ASBANC como desde el ámbito académico, a través de Segurazo, por su enfoque innovador en la prevención de fraudes en cuentas y tarjetas bancarias en distintos medios de pago.

Un hito relevante en este proceso de validación fue la presentación realizada el 18 de febrero de 2025 en el evento organizado por Lynx y NTT Data en España. Este evento reunió a los principales referentes de seguridad de fraudes a nivel mundial, lo que permitió que nuestra propuesta captara especial atención y generara consultas debido a su versatilidad y alcance, ya que no se limita únicamente a instituciones financieras. La aceptación y el interés generado en este foro internacional refuerzan la relevancia y aplicabilidad del modelo

propuesto en distintos escenarios de riesgo, como se aprecia en la siguiente imagen. Ver Figura 35.

Figura 35. Validación de Segurazo con respaldo del Presidente del Comité Estratégico de ASBANC



7.2.Rentabilidad de la Solución

La rentabilidad social de Segurazo se centra en los beneficios que aporta a los usuarios, instituciones financieras y a la sociedad en su conjunto, promoviendo un entorno digital más seguro y accesible. La solución reduce los costos asociados al fraude digital, mejora la confianza en la protección de datos y facilita la adopción de medidas preventivas en situaciones de emergencia. Este análisis considera tanto los beneficios sociales como los costos asociados al funcionamiento de la herramienta, permitiendo evaluar su impacto integral.

Para dimensionar el impacto social de Segurazo, es fundamental considerar la demanda proyectada de usuarios basada en datos relevantes de estudios y encuestas previas. En el análisis realizado en capítulos anteriores, se estableció la demanda potencial del servicio a partir de las siguientes fuentes:

Encuesta de Credicorp sobre Crimen y Violencia (2024): Indica que el 27% de la población limeña ha sido víctima de robo o conoce a alguien que lo ha sido. Asimismo, se presentan datos sobre el porcentaje de afectados por acceso no autorizado a cuentas bancarias, segmentado por nivel socioeconómico.

Proyecciones de población del INEI (2024): Se estima que la población peruana alcanzará los 35.7 millones en 2030, lo que permite proyectar el crecimiento del mercado objetivo de Segurazo.

Distribución de la población por sector socioeconómico: Según el Informe de Niveles Socioeconómicos de la Asociación Peruana de Empresas de Inteligencia de Mercados (2024), lo que permite definir el alcance del servicio en los distintos segmentos.

Penetración de smartphones e internet: Datos obtenidos de la Encuesta Residencial de Servicios de Telecomunicaciones (2023) determinan la accesibilidad del servicio para distintos grupos de usuarios.

Tasa de adopción esperada: Se estima que el uso del servicio comienza en un 30-35% y crece hasta un 70-75% en cinco años, en función de la tendencia de adopción de soluciones digitales de seguridad financiera.

A partir de estos factores, se ha modelado la demanda estimada de usuarios de Segurazo y su impacto proyectado en la reducción del tiempo de reacción ante robos de dispositivos móviles. Este contexto permite desarrollar un modelo de evaluación de beneficios sociales basado en dos criterios principales:

Beneficios Sociales de Segurazo

Los beneficios sociales de Segurazo se reflejan en el impacto positivo que genera al proporcionar una herramienta eficiente para gestionar incidentes relacionados con el robo o pérdida de dispositivos móviles. Además, la solución fortalece la seguridad digital, reduce el

estrés de los usuarios en situaciones de emergencia y fomenta prácticas preventivas. A continuación, en la Tabla 70, se detallan los principales beneficios sociales:

Tabla 72. Beneficios sociales de Segurazo

Beneficio	Definición	Métrica
Optimización del tiempo en gestiones	La plataforma centraliza los pasos necesarios tras un robo, reduciendo significativamente el tiempo y los costos asociados a las gestiones de bloqueo de cuentas, denuncias y reposiciones.	Valor del ahorro por tiempo invertido y movilidad.
Fomento de una cultura preventiva	Educa a los usuarios sobre las medidas de protección necesarias en el manejo de sus datos digitales, promoviendo hábitos responsables de seguridad digital.	Porcentaje de usuarios que adoptan medidas preventivas después de usar la plataforma.
Reducción de pérdidas económicas por fraude	Segurazo disminuye la probabilidad de transacciones no reconocidas y accesos indebidos a cuentas bancarias, gracias a la reducción del tiempo de exposición tras el robo o pérdida de dispositivos.	Monto promedio de pérdidas económicas evitadas por usuario (S/ 1,000 en promedio, según supuestos de modelado) o ahorro total anual estimado.

Fuente: Elaboración Propia

El impacto económico y social de Segurazo se fundamenta en el siguiente criterio clave:

Criterio 1: Ahorro por tiempo y movilidad.

El tiempo requerido para realizar gestiones administrativas tras un robo representa un costo significativo. Según estimaciones, los usuarios invierten en promedio 6 horas en trámites relacionados con bloqueos de cuentas, reposiciones de tarjetas, denuncias policiales y contactos con operadores móviles. Considerando el salario mínimo actual de S/ 1,025 mensuales, equivalente a S/ 4.27 por hora, el costo promedio por tiempo perdido se calcula en S/ 25.62. Además, se considera un gasto promedio de movilidad de S/ 10.00 por persona.

Para estimar la cantidad de Personas Afectadas por Robo de Información, se ha utilizado como base la demanda proyectada de Segurazo. A partir de esta, se han aplicado dos factores clave que permiten determinar el número de personas que experimentan un impacto significativo y requieren realizar trámites administrativos tras un incidente de seguridad.

En primer lugar, se considera el porcentaje de reclamos resueltos a favor del usuario, que corresponde al 56%. Según la Superintendencia de Banca, Seguros y AFP (SBS), este es el porcentaje de reclamos por operaciones no reconocidas en el sistema financiero peruano que son resueltos a favor de los clientes. Esto implica que más de la mitad de las personas afectadas no lograron evitar el acceso indebido a sus cuentas bancarias y, en consecuencia, sufrieron algún nivel de perjuicio económico antes de que la entidad financiera pudiera mitigar el daño (Superintendencia de Banca, Seguros y AFP, 2023).

Por otro lado, no todas las víctimas de fraudes o accesos indebidos a sus cuentas realizan una denuncia formal o inician trámites administrativos. Basándonos en datos de estudios previos sobre el comportamiento de usuarios afectados por fraudes digitales en Perú, aproximadamente el 20% de las víctimas opta por realizar gestiones administrativas, como la denuncia policial, trámites en entidades bancarias u operadoras, y procesos de reposición de documentos o tarjetas.

Para calcular la cantidad de personas afectadas, se ha aplicado la siguiente fórmula:

Personas Afectadas por Robo =Demanda Proyectada de Segurazo×56%×20%

Esto significa que del total de usuarios proyectados de Segurazo, se estima que un 56% enfrenta accesos indebidos a sus cuentas bancarias. De estos, el 20% opta por realizar trámites administrativos tras el robo. Como resultado, se obtiene la cantidad de personas que, anualmente, experimentan la necesidad de gestionar bloqueos, denuncias o trámites financieros para mitigar los efectos de un robo de información. Ver tabla 73.

Criterio 2: Ahorro por pérdidas económicas evitadas (fraude).

La reducción del tiempo de exposición del usuario ante un incidente de robo de dispositivo disminuye la probabilidad de que se produzcan transacciones no reconocidas o accesos indebidos a cuentas bancarias. Para su estimación se considera: S/ 1,000 por persona afectada por robo de información, según la demanda proyectada en esta tesis. Este valor es un

supuesto conservador, sustentado en las entrevistas realizadas a personas afectadas durante el desarrollo del estudio y en casos documentados en el mercado peruano.

Tabla 73. Proyección de beneficios sociales de Segurazo

	AÑOS	1	2	3	4	5
Criterio 1: Estimación del ahorro por Tiempo en gestiones administrativas						
	Costo por tiempo perdido	S/ 25.62	S/ 25.62	S/ 25.62	S/ 25.62	S/ 25.62
	Costo promedio de movilidad	S/ 10.00	S/ 10.00	S/ 10.00	S/ 10.00	S/ 10.00
	Personas afectadas por robo de información	28,394	38,075	57,263	64,107	71,300
Criterio 2: Estimación Ahorro por pérdidas económicas evitadas (Fraude)						
	Ahorro promedio por pérdida económica	S/ 28,394,281	S/ 38,075,193	S/ 57,262,768	S/ 64,107,113	S/ 71,299,962
	Ahorro del criterio 1	**S/ 1,011,404.3**	**S/ 1,356,238.4**	**S/ 2,039,699.8**	**S/ 2,283,495.4**	**S/ 2,539,704.6**
	Ahorro del criterio 2	**S/ 28,394,280.5**	**S/ 38,075,193.3**	**S/ 57,262,767.6**	**S/ 64,107,113.4**	**S/ 71,299,961.6**
Valor del beneficio total social (S/)		**S/ 29,405,684.8**	**S/ 39,431,431.7**	**S/ 59,302,467.4**	**S/ 66,390,608.7**	**S/ 73,839,666.2**

Fuente: Elaboración Propia

Costos Sociales de Segurazo

Si bien Segurazo ofrece numerosos beneficios sociales, también genera ciertos costos sociales que deben considerarse para evaluar integralmente su impacto. Estos costos están relacionados principalmente con el consumo de recursos tecnológicos, el impacto ambiental derivado de su operación digital, y el esfuerzo requerido para educar a los usuarios en seguridad digital. A continuación, se detallan estos costos en términos medibles (Tabla 74):

Tabla 74. Costos sociales de Segurazo

Costo	Definición	Métrica
Consumo energético	La operación de los servidores en la nube y el tráfico digital de la plataforma generan consumo eléctrico constante.	Total de kWh consumidos por los servidores asociados a Segurazo por año.
Huella de carbono digital	Las emisiones de CO2 derivadas del uso de servidores, almacenamiento y transmisión de datos generan un impacto ambiental.	Toneladas de CO2 emitidas anualmente, calculadas según el consumo energético.
Educación y adopción del usuario	El tiempo necesario para educar a los usuarios y familiarizarlos con la plataforma requiere esfuerzos en comunicación y soporte técnico.	Horas promedio invertidas en capacitaciones o soporte por usuario.
Costo de mantenimiento	La actualización constante de la plataforma para garantizar su seguridad y funcionalidad genera costos operativos significativos.	Porcentaje del presupuesto anual destinado a mejoras y mantenimiento de la plataforma.

Fuente: Elaboración Propia

El funcionamiento de los servidores y laptops necesarios para operar Segurazo genera un consumo energético constante. Según estimaciones actualizadas, un servidor de alto rendimiento consume aproximadamente 400 kWh al mes, lo que se traduce en un costo mensual de S/ 280.00 considerando un costo por kWh de S/ 0.70 (INEI, 2023). Adicionalmente, las 4 laptops necesarias para la operación consumen en conjunto 250 kWh al mes, incrementando el costo energético mensual a S/ 175.00. Esto eleva el costo energético total mensual a S/ 455.00.

Este consumo energético genera emisiones de CO_2, debido a la dependencia de la matriz energética peruana de combustibles fósiles. Según el factor de emisión promedio de 0.44 kg de CO_2/kWh (MINEM, 2022), el servidor produce 176 kg de CO_2 al mes, mientras que las 11 laptops generan adicionalmente 110 kg de CO_2 al mes, sumando un total de 286 kg de CO_2 mensuales. Esto equivale a 0.286 toneladas de CO_2 por mes.

El impacto ambiental de estas emisiones se calcula en S/ 27.96 mensuales, considerando un valor social del carbono de S/ 97.75 por tonelada de CO_2 (CEPAL, 2022). Este costo subraya la importancia de considerar medidas de sostenibilidad energética en la operación de Segurazo.

El tiempo requerido para educar a los usuarios sobre el uso de Segurazo constituye otro costo significativo. Considerando que el salario mínimo en Perú es de S/ 1,025 mensuales, equivalente a S/ 4.27 por hora (MTPE, 2023), el costo promedio por una capacitación de una hora es de S/ 4.27 por usuario. Este esfuerzo es fundamental para maximizar la eficacia de la solución y garantizar que los usuarios estén preparados para responder adecuadamente en caso de robo o pérdida de dispositivos.

El uso de la plataforma Segurazo por parte de las personas afectadas por robo de información genera un costo energético indirecto asociado al uso de sus dispositivos móviles durante el acceso a la web. Basándonos en un tiempo promedio de uso de 15 minutos por usuario y un costo por minuto de carga del celular de S/ 0.0135 (INEI, 2023), se ha calculado el impacto económico estimado para el periodo proyectado de cinco años. Este análisis toma en cuenta el crecimiento anual en el número de usuarios de la plataforma, considerando el 100% de las personas afectadas, incluyendo aquellos que no realizan reclamos formales. Los resultados reflejan el costo acumulativo generado por el consumo de energía necesario para garantizar el acceso y uso de la plataforma por parte de los usuarios, subrayando la importancia de incorporar medidas de sostenibilidad en el uso de dispositivos personales.

Tabla 75. Proyección de costos sociales de Segurazo

	AÑOS	1	2	3	4	5
Criterio 1: Impacto energético y ambiental						
	Consumo energético del Servidor (kWh)	400	412.00	424.36	437.09	450.20
	Costo mensual promedio (kWh)	0.7	0.7	0.7	0.7	0.7
	Costo energético del Servidor (S/)	**S/ 280.0**	**S/ 288.4**	**S/ 297.1**	**S/ 306.0**	**S/ 315.1**
	Consumo energético de las laptops (kWh)	62.5	64.38	66.31	68.30	70.34
	Costo mensual promedio (kWh)	0.7	0.7	0.7	0.7	0.7
	Costo energético de las 11 laptops (S/)	**S/ 481.3**	**S/ 495.7**	**S/ 510.6**	**S/ 525.9**	**S/ 49.2**
	Costo energético total (S/)	**S/ 761.3**	**S/ 784.1**	**S/ 807.6**	**S/ 831.8**	**S/ 364.4**
	Factor de emisión del Servidor (kg CO_2/kWh)	0.44	0.44	0.44	0.44	0.44
	Emisiones de CO_2 del Servidor (kg)	176.00	181.28	186.72	192.32	198.09
	Conversión a toneladas (toneladas de CO_2)	0.18	0.18	0.19	0.19	0.20
	Valor social del carbono del Servidor(S/ 97.75/tonelada)	97.75	97.75	97.75	97.75	97.75
	Costo ambiental por emisiones del Servidor (S/)	**S/ 17.2**	**S/ 17.7**	**S/ 18.3**	**S/ 18.8**	**S/ 19.4**
	Factor de emisión de las laptops (kg CO_2/kWh)	0.44	1.44	2.44	3.44	4.44
	Emisiones de CO_2 de las laptops (kg)	110	370.8	647.149	939.74522	1249.314779
	Conversión a toneladas (toneladas de CO_2)	0.11	0.37	0.65	0.94	1.25
	Costo ambiental por emisiones de las 4 laptops (S/)	**S/ 10.8**	**S/ 36.2**	**S/ 63.3**	**S/ 91.9**	**S/ 122.1**
	Costo ambiental total (S/)	**S/ 28.0**	**S/ 54.0**	**S/ 81.5**	**S/ 110.7**	**S/ 141.5**
Costo total del imapcto energético y ambiental (S/)		S/ 789.2	S/ 838.1	S/ 889.1	S/ 942.5	S/ 505.9
Criterio 2: Costos de capacitación y operación						
	Tiempo en capacitaciones (horas)	1,000	1,030	1,061	1,093	1,126
	Costo por HH de capacitción (S/)	4.27	4.27	4.27	4.27	4.27
	Costo por capacitaciones (S/)	**S/ 4,270.0**	**S/ 4,398.1**	**S/ 4,530.0**	**S/ 4,665.9**	**S/ 4,805.9**
Criterio 3: Impacto energético y ambiental asociado al uso de dispositivos móviles						
	Tiempo de uso en minutos por usuario	15	15	15	15	15
	Costo por minuto de carga (S/)	S/ 0.0135	S/ 0.01	S/ 0.01	S/ 0.01	S/ 0.01
	Costo de usuario por año (S/)	**S/ 5,749.8**	**S/ 7,710.2**	**S/ 11,595.7**	**S/ 12,981.7**	**S/ 14,438.2**
Valor del costo social total (S/)		S/ 10,809.0	S/ 12,946.4	S/ 17,014.9	S/ 18,590.1	S/ 19,750.0

Fuente: Elaboración Propia

La Tabla 76, presenta un desglose de los beneficios y costos sociales proyectados para los primeros cinco años de implementación, así como el flujo social neto resultante:

Tabla 76. Flujo de beneficios y costos sociales proyectado

AÑOS	1	2	3	4	5
Beneficios Sociales	S/ 29,405,684.80	S/ 39,431,431.70	S/ 59,302,467.43	S/ 66,390,608.75	S/ 73,839,666.21
Costos Sociales	S/ 10,809.0	S/ 12,946.4	S/ 17,014.9	S/ 18,590.1	S/ 19,750.0
Flujo	**S/ 29,394,875.75**	**S/ 39,418,485.32**	**S/ 59,285,452.56**	**S/ 66,372,018.61**	**S/ 73,819,916.17**

Fuente: Elaboración Propia

El cálculo del VAN Social se realizó aplicando una tasa de descuento del 8% para traer a valor presente los flujos sociales proyectados. Este análisis considera tanto el impacto financiero como el social, lo que permite evaluar la viabilidad del modelo desde una perspectiva integral.

- **VAN Social:** S/207,101,188.54
- **VAN Financiero:** S/ 3.624.038
- **Proporción del VAN Social respecto al Financiero:** 5715%

El análisis financiero–social muestra que, por cada sol generado en términos económicos, Segurazo aporta aproximadamente S/ 57 en valor social, lo que representa una proporción de 5 715 % entre el VAN Social (S/ 207,101,188.54) y el VAN Financiero (S/ 3,624,038).

Este resultado se explica principalmente por el ahorro asociado a las pérdidas económicas evitadas: al reducir de manera drástica el tiempo de exposición tras el robo de un dispositivo, la plataforma disminuye la probabilidad de transacciones fraudulentas y, con ello, los montos que los usuarios habrían perdido.

Dichos beneficios sociales (dinero que no llega a ser robado y que permanece en manos de los usuarios y del sistema financiero) superan ampliamente los ingresos directos del proyecto, lo que confirma que el impacto social de Segurazo es sustancialmente mayor que su retorno financiero. Esta diferencia evidencia la relevancia de Segurazo como una solución de alto valor para la seguridad digital y la prevención del fraude.

7.3.Análisis de Sensibilidad Social

El análisis de sensibilidad permite evaluar el impacto de variaciones en la demanda proyectada de Segurazo sobre los resultados del Valor Actual Neto (VAN) Social y Económico. Se consideran tres escenarios: optimista, esperado y pesimista, que reflejan distintos niveles de adopción de la solución.

El escenario optimista supone una alta aceptación, alcanzando hasta un 85% de la demanda proyectada en el quinto año. El escenario esperado corresponde a la proyección base, con una adopción de hasta 75% en el mismo periodo. Finalmente, el escenario pesimista considera una menor adopción por barreras de entrada, con un 65% en el quinto año.

Tabla 77. Análisis de Sensibilidad del VAN Social y Económico bajo Diferentes Escenarios

Escenario	VAN Social (S/)	VAN Económico (S/)	Proporción Social/Económico
Optimista	S/ 8,301,839.96	S/ 4,878,067.01	4988%
Esperado	S/ 7,063,617.66	S/ 4,878,067.01	5715%
Pesimista	S/ 5,825,393.78	S/ 4,878,067.01	3503%

Elaboración: Fuente Propia

Los resultados del análisis muestran que, en todos los escenarios, el impacto social de Segurazo continúa siendo muy superior al impacto económico.

En el escenario optimista, con una adopción más acelerada, la relación entre el valor social y el económico alcanza aproximadamente 4 988 %, evidenciando el alto aporte de la solución a la sociedad. En el escenario esperado, la proporción se eleva a 5 715 %, confirmando que incluso con una adopción moderada, Segurazo sigue generando un beneficio social claramente superior a su retorno financiero. Finalmente, en el escenario pesimista, pese a una menor adopción, la ventaja social se mantiene con una proporción de 3 503 %, lo que demuestra la resiliencia del modelo y su capacidad de mantener un alto impacto social.

Estos resultados significan que, por cada sol de rentabilidad financiera, el beneficio social equivalente oscila entre 35 y 57 soles, según el escenario analizado. En otras palabras, el valor que Segurazo crea para la sociedad (principalmente por las pérdidas económicas evitadas en casos de fraude) es varias decenas de veces mayor que su retorno económico directo.

Esto implica que la solución es financieramente viable y su verdadero aporte radica en el impacto social, al proteger a miles de usuarios de sufrir pérdidas económicas significativas y al fortalecer la confianza en la seguridad digital.

Capítulo VIII. Implementación

8.1. Plan de implementación y equipo de trabajo

El proyecto del aplicativo móvil de seguridad, denominado Segurazo, seguirá un plan de implementación estructurado en seis fases, cada una con hitos clave y métricas de éxito para evaluar su avance.

Fase 1: Preparación y Evaluación de Recursos

Objetivo: Asegurar la inversión necesaria y optimizar la estructura financiera para la viabilidad económica del proyecto.

Hitos:

- Aprobación del presupuesto operativo.
- Identificación de fuentes de financiamiento y cierre de inversión inicial.
- Definición del modelo financiero sostenible.

Métricas de éxito:

- Financiamiento asegurado en su totalidad antes de avanzar a la Fase 2.
- Evaluación de costos con margen de error inferior al 10 %.

Fase 2: Constitución de la Empresa

Objetivo: Establecer los fundamentos legales y administrativos de Segurazo.

Hitos:

- Reserva del nombre comercial y registro en SUNARP.
- Obtención del RUC y trámites ante SUNAT.
- Adquisición de licencias y permisos legales necesarios.

Métricas de éxito:

- Registro de empresa completado en un plazo máximo de 45 días.
- Documentación legal validada antes de iniciar la siguiente fase.

Fase 3: Inicio del Proyecto

Objetivo: Adquirir recursos y poner en marcha la infraestructura básica para el desarrollo.

Hitos:

- Contratación del equipo técnico inicial.
- Adquisición de servicios y configuración de infraestructura cloud.
- Implementación de entornos de desarrollo.

Métricas de éxito:

- Contratación del 80 % del equipo técnico dentro de los primeros 30 días.
- Infraestructura operativa y lista para pruebas en la siguiente fase.

Fase 4: Desarrollo del Proyecto

Objetivo: Diseño, desarrollo y pruebas iniciales de Segurazo.

Hitos:

- Creación del producto mínimo viable (PMV).
- Implementación de pruebas de seguridad y rendimiento.
- Validación con primeros usuarios beta.

Métricas de éxito:

- Estabilidad del 95 % en pruebas de carga.
- Menos del 5 % de errores críticos detectados antes del lanzamiento beta.

Fase 5: Operaciones y Publicidad

Objetivo: Implementar el plan de operaciones y ejecutar la estrategia de marketing digital.

Hitos:

- Implementación de campañas de publicidad en redes sociales y Google Ads.
- Creación de alianzas con entidades financieras.
- Inicio de soporte y atención al cliente.

Métricas de éxito:

- Cinco mil pre-registros antes del lanzamiento oficial.

- Diez alianzas estratégicas establecidas en el primer trimestre.

Fase 6: Lanzamiento del Aplicativo

Objetivo: Introducir Segurazo al mercado con una estrategia escalonada.

Hitos:

- Primera evaluación de retroalimentación con usuarios reales.
- Actualización de funcionalidades según retroalimentación inicial.

Métricas de éxito:

- Más de diez mil descargas en los primeros tres meses.

Figura *36*. Diagrama de Gantt

Actividad	Responsable	Ene-25				Feb-25				Mar-25				Abr-25				May-25				Jun-25			
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
1era Fase: Preliminar Inversión y revisión de recursos																									
Gestión de documentación del plan estratégico y modelo de negocio	FM																								
Definir puestos administrativos y gerencia	LA																								
Análisis de recursos y aporte de capital	AC																								
Gestión de creación de la empresa	KG																								
Entregable: Plan estratégico y modelo de negocio finalizado.																									
Objetivo: Asegurar la inversión necesaria y optimizar la estructura financiera para la viabilidad económica del proyecto.																									
Métrica éxito: Financiamiento asegurado en su totalidad antes de avanzar a la Fase 2/Evaluación de costos con margen de error inferior al 10 %.																									
Hito: Aprobación del presupuesto operativo																									
2da Fase: Constitución de la empresa																									
Selección y reserva de nombre	LA, AC																								
Elaboración del acta constitutiva	FM, KG																								
Abono del capital y bienes	FM																								
Elaboración e inscripción de la escritura pública	LA																								
Inscripción del RUC	LA																								
Gestión de la Licencia de Funcionamiento	LA, AC																								
Entregable: Acta constitutiva firmada y licencia de funcionamiento.	LA																								
Objetivo: Establecer los fundamentos legales y administrativos de Segurazo																									
Métricas de éxito: Registro de empresa completado en un plazo máximo de 45 días.																									
Hito: Reserva del nombre comercial y registro en SUNARP																									
3era Fase: Inicio del proyecto																									
Búsqueda y contratación del diseñador del aplicativo	FM																								
Realización de pruebas iniciales del diseño	KG																								
Contratación de servicio para pasarela de pagos	LA																								
Adquisición de equipos	FM																								
Adquisición de software	FM																								
Entregable: Diseño inicial del aplicativo validado y equipos adquiridos.	KG																								
Objetivo: Adquirir recursos y poner en marcha la infraestructura básica para el desarrollo																									
Métricas de éxito: Contratación del 80 % del equipo técnico dentro de los primeros 30 días.																									
Hito: Contratación del equipo técnico inicial./Implementación de entornos de desarrollo																									
4ta Fase: Desarrollo del proyecto																									
Capacitación del equipo humano	LA																								
Capacitación de uso del aplicativo	FM																								
Seguimiento de desarrollo	KG																								
Pruebas de seguridad	KG																								
Entregable: Equipo capacitado y módulo principal funcional.	FM																								
Objetivo: Diseño, desarrollo y pruebas iniciales de Segurazo																									
Métricas de éxito: Estabilidad del 95 % en pruebas de carga.																									
Hito: Creación del producto mínimo viable (PMV).																									
5ta Fase: Operaciones y Publicidad																									
Diseño de campañas publicitarias	AC, KG																								
Contratación de servidores	FM, LA																								
Entregable: Campañas publicitarias diseñadas y servidores configurados.	AC, KG																								
Objetivo: Implementar el plan de operaciones y ejecutar la estrategia de marketing digital																									
Métricas de éxito: Cinco mil pre-registros antes del lanzamiento oficial.																									
Hito: Inicio de soporte y atención al cliente																									
6ta Fase: Lanzamiento del aplicativo																									
Lanzamiento del Asistente Virtual Segurazo	FM, KG, AC, LC																								
Entregable: Asistente Virtual Segurazo lanzado y operativo.	FM, KG, AC, LC																								
Objetivo: Introducir Segurazo al mercado con una estrategia escalonada																									
Métricas de éxito: Más de diez mil descargas en los primeros tres meses.																									
Hito: Primera evaluación de retroalimentación con usuarios reale																									

Fuente: Elaboración Propia

Nota: El cuadro muestra el detalle de las fases y la nomenclatura de las referencias de las responsabilidades son: Franco Mori (FM), Lucero Alvarado (LA), Alvaro Contreras (AC) y Kevin Gonzales (KG).

8.2. Reflexiones Individuales del Equipo sobre el Aprendizaje

Franco Mori (FM) – Liderazgo y Desarrollo Tecnológico

Desde el inicio de la tesis hasta su culminación, enfrenté múltiples desafíos, desde la delimitación del problema hasta la estructuración de la propuesta. Uno de los obstáculos más grandes fue consolidar una investigación rigurosa que estuviera alineada con la metodología requerida. Aprendí a manejar grandes volúmenes de información, sintetizar hallazgos y

presentar argumentos de manera clara y sustentada. Además, desarrollar el modelo de negocio y justificar su viabilidad fue una tarea exigente que me permitió fortalecer mis habilidades en planificación estratégica y análisis financiero. La experiencia me dejó una gran lección sobre la importancia de la organización, la disciplina y la colaboración en equipo

Lucero Alvarado (LA) – Gestión de Riesgos y Procesos

Todo este camino fue un proceso lleno de retos, especialmente en la obtención de datos relevantes y la validación de hipótesis. Uno de los momentos más complejos fue la fase de recopilación de información primaria, donde aprendí a realizar entrevistas efectivas y a analizar los resultados con un enfoque crítico. También me enfrenté a dificultades en la redacción técnica y en la aplicación del formato APA, lo que me obligó a mejorar mis habilidades de escritura académica. Esta experiencia me enseñó la importancia de la perseverancia y la adaptabilidad para superar los desafíos que surgen en una investigación extensa y detallada.

Álvaro Contreras (AC) – Regulación Financiera y Riesgos

Uno de los mayores aprendizajes durante la elaboración de la tesis fue la importancia de la gestión del tiempo. Equilibrar la investigación con otras responsabilidades personales y profesionales resultó ser un reto constante. Aprendí a priorizar tareas y a dividir el trabajo en etapas manejables para evitar retrasos. Asimismo, la colaboración en equipo jugó un papel clave, ya que la comunicación efectiva y la distribución equitativa de responsabilidades fueron esenciales para avanzar de manera eficiente. Esta experiencia reforzó mi capacidad para trabajar bajo presión y adaptarme a imprevistos, habilidades que sin duda serán valiosas en mi desarrollo profesional.

Kevin Gonzales (KG) – Operaciones y Optimización

El proceso de investigación para la tesis me permitió desarrollar una comprensión profunda de la aplicación de metodologías estructuradas como Design Thinking. Inicialmente, me

resultó complicado definir los marcos de referencia adecuados y justificar cada decisión metodológica. Sin embargo, con el tiempo aprendí a utilizar herramientas analíticas para validar nuestras propuestas y a respaldarlas con evidencia empírica. También me enfrenté al reto de elaborar conclusiones que fueran coherentes con los hallazgos obtenidos. Esta experiencia me ayudó a fortalecer mi capacidad de análisis crítico y a mejorar mis habilidades en la formulación de soluciones basadas en datos concretos.

8.3. Estructura Organizacional y Necesidades Adicionales

La estructura organizacional de Segurazo estará conformada por cuatro socios fundadores con responsabilidades específicas:

- Franco Mori (FM): Desarrollo tecnológico y estrategia digital.
- Lucero Alvarado (LA): Gestión de riesgos y procesos financieros.
- Álvaro Contreras (AC): Regulación financiera y cumplimiento normativo.
- Kevin Gonzales (KG): Operaciones y mejora continua.

Dicho equipo cuenta con conocimientos en sistemas, marketing, legal y contabilidad. Para abordar las necesidades operativas y garantizar el crecimiento sostenible del proyecto, se priorizará la contratación de un desarrollador especializado. Estos roles permitirán consolidar las capacidades clave en el desarrollo del aplicativo, el cumplimiento normativo y la expansión del negocio.

8.4. Conclusiones

1. Se concluye que la seguridad financiera móvil en el Perú requiere atención urgente ante el creciente número de fraudes y la alta vulnerabilidad de los usuarios tras el robo o pérdida de dispositivos. La masiva penetración de teléfonos móviles en el país demanda soluciones tecnológicas que sean no solo innovadoras y eficientes, sino también accesibles. En este contexto, se identifica como clave la integración entre entidades bancarias, operadoras de telecomunicaciones y autoridades para fortalecer la confianza en el sistema financiero nacional.
2. La propuesta de Segurazo representa una solución viable e innovadora que responde a las principales necesidades detectadas. Este asistente facilita la acción rápida en situaciones de emergencia, permitiendo el bloqueo de cuentas y líneas telefónicas, así como el acceso inmediato a canales de contacto con bancos y operadores. Además, proporciona orientación clara para realizar denuncias policiales, lo cual contribuye significativamente a la protección de los datos personales y activos financieros de los usuarios.
3. Desde el análisis financiero, se concluye que el proyecto es altamente rentable. El Valor Actual Neto (VAN) financiero es S/ 3,624,038 y el VAN económico es S/ 4,346,376. Asimismo, la Tasa Interna de Retorno (TIR) financiero es 227.4% y el TIR económico es 178.9%; y el Índice de Rentabilidad (IR) financiero y económico es de 2.17 y 1.6. Por último, el costo promedio ponderado de capital (WACC) del 15%, evidenciando un retorno sólido y atractivo sobre la inversión inicial.
4. Finalmente, el proyecto se alinea con los Objetivos de Desarrollo Sostenible (ODS), particularmente con el ODS 4, al promover la educación financiera y el acceso a información de calidad para la prevención del fraude, y con el ODS 16.4, al contribuir a la protección de activos financieros y la reducción de flujos ilícitos. En

conjunto, estos aportes refuerzan el compromiso del proyecto con una economía más segura, equitativa y consciente.

Referencias

Alipay. (n.d.). *Estudio de Caso: Alipay's Real-Time Fraud Detection System*. Recuperado de https://intl.alipay.com

Asociación de Bancos del Perú (ASBANC). (2020). *Informe sobre seguridad financiera y fraudes electrónicos en el Perú*. Asociación de Bancos del Perú.

Asociación de Bancos del Perú (ASBANC). (2023). *Bancos privados lanzan 1820, nuevo número de emergencias para bloquear tarjetas*. Recuperado de https://www.asbanc.com.pe/noticia/bancos-privados-lanzan-1820-nuevo-numero-de-emergencias-para-bloquear-tarjetas

Asociación de Bancos del Perú (ASBANC). (2023). *Iniciativas de seguridad financiera*. Recuperado de https://www.asbanc.com.pe

Asociación de Bancos del Perú (ASBANC). (2023). *Memoria Anual 2023*. Asociación de Bancos del Perú.

Banco Central de Brasil. (2023). *Sistema de bloqueo digital para prevención de fraudes financieros*.

Banco de Crédito del Perú (BCP). (2023). *¿Cómo bloquear mi Tarjeta de Crédito o Débito BCP?*. Recuperado de https://www.viabcp.com

Banco Central de Reserva del Perú. (2024). *Reporte de inflación – marzo 2024*. https://www.bcrp.gob.pe/docs/Publicaciones/Reporte-Inflacion/2024/marzo/reporte-de-inflacion-marzo-2024.pdf

BBVA. (2023). *Soluciones de seguridad financiera*. Recuperado de https://www.bbva.pe

Bloomberg Línea. (2024). *Alertas diarias por fraude financiero en LatAm superaron las de Norteamérica en el último año*. https://www.bloomberglinea.com/tecnologia/alertas-diarias-por-fraude-financiero-en-latam-superaron-las-de-norteamerica-en-el-ultimo-ano/

Claro. (2023). *¿Cómo puedo bloquear el equipo y línea por robo?*. Recuperado de https://www.claro.com.pe

CNIPA. (n.d.). CN Patent No. 105,389,764 A: "Mobile Security Alert System". Recuperado de https://www.cnipa.gov.cn

Comisión Económica para América Latina y el Caribe (CEPAL). (2022). *Estimación del precio social del carbono para la evaluación de la inversión pública en el Perú.* Recuperado de https://www.cepal.org/es/publicaciones/80746-estimacion-precio-social-carbono-la-evaluacion-la-inversion-publica-peru

Banco de Crédito del Perú (2024). *Primer Reporte de Crimen y Violencia.* Recuperado de https://admin.observatoriodelcrimenylaviolencia.com/media/primer-reporte-del-observatorio-del-crimen-y-la-violencia.pdf

Datum Internacional. (2024, octubre). *Encuesta nacional sobre percepción de seguridad ciudadana*

Datum Internacional. (2024). *Encuesta DATUM - Octubre 2024 - SEGURIDAD*. https://www.datum.com.pe/new_web_files/files/pdf/Encuesta%20DATUM%20-%20Octubre%202024%20-%20SEGURIDAD%20Final_241020081757.pdf

Decreto Supremo N° 016-2024-JUS. (2024). *Aprueban nuevo reglamento de la Ley de Protección de Datos Personales*.

Defensoría del Pueblo. (2023). *Informe sobre ciberdelincuencia en el Perú*. https://www.defensoria.gob.pe

Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Deloitte. (2018). *Global Survey on Economic Crime and Fraud*. Deloitte. Recuperado de https://www2.deloitte.com/global/en/pages/finance/articles/global-economic-crime-survey.html

Deloitte. (2021). *Time is Right for a Wave of Bank Consolidation*. Recuperado de https://www2.deloitte.com

Deloitte. (2021). *Bank Consolidation in India*. Recuperado de https://www2.deloitte.com

El País. (2023, diciembre 19). *Brasil crea una aplicación para bloquear celulares robados: "Serán un pedazo de metal inútil"*. https://elpais.com/america/2023-12-19/brasil-crea-una-aplicacion-para-bloquear-celulares-robados-seran-un-pedazo-de-metal-inutil.html

El Peruano. (2023). *Cada vez menos víctimas de delitos denuncian ante la PNP y la Fiscalía*. Recuperado de https://elcomercio.pe/lima/cada-vez-menos-victimas-de-delitos-denuncian-ante-la-pnp-y-la-fiscalia-noticia/

El Peruano. (2023). *Modalidades de fraudes digitales más denunciadas en Perú*.

El Peruano. (2023). *¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú*. https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

El Peruano. (2024). *Asbanc lanza línea de emergencia 1820 para bloqueo de tus tarjetas en casos de robo*. https://elperuano.pe/noticia/247391-asbanc-lanza-linea-de-emergencia-1820-para-bloqueo-de-tus-tarjetas-en-casos-de-robo

El Peruano. (2025). *Cómo prevenir fraudes y proteger tu información personal tras un robo de celular*. https://elperuano.pe/noticia/260573-conoce-como-prevenir-fraudes-y-proteger-tu-informacion-personal-tras-un-robo-de-celular

Entel. (2023). *Bloqueo y desbloqueo del equipo celular*. Recuperado de https://www.entel.pe/informacion-a-abonados-y-usuarios/bloqueo/

Escudo Digital. (2024). *Soluciones de seguridad y defensa en el Mobile World Congress 2024*. Recuperado de https://www.escudodigital.com/tecnologia/soluciones-seguridad-defensa-en-marco-mobile-world-congress-2024_58334_102.html

European Patent Office. (n.d.). EP Patent No. 2,745,888 B1: "Emergency Response System for Financial Accounts". Recuperado de https://www.epo.org

Expreso. (2023). Robo de dispositivos móviles incrementa los fraudes bancarios, según BioCatch. https://www.expreso.com.pe/tecnologia/robo-de-dispositivos-moviles-incrementa-los-fraudes-bancarios-segun-biocatch-tecnologia-noticia/1021246/

Finnovista. (2024). *Fintech Radar Perú 2024*. Latam Fintech Hub / Finnovista. https://www.latamfintech.co/reports/finnovista-fintech-radar-peru-2023

Fernández, M., Rodríguez, L., & Sánchez, P. (2021). *Diseño de aplicaciones seguras para la protección de datos en dispositivos móviles*. Revista Latinoamericana de Seguridad Informática, 14(2), 45-60.

Fiscalía General del Estado de Guanajuato. (s.f.). *Líneas de atención y denuncia en línea*. https://portal.fgeguanajuato.gob.mx/PortalWebEstatal/Genero/Formularios/lineasatencion.aspx

Fortinet. (2024). *Mobile Security: Top Threats and Protection Strategies*. Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/mobile-security

García, J., & López, S. (2020). *La necesidad de sistemas unificados para el bloqueo de dispositivos móviles robados*. Tecnología y Sociedad, 8(1), 30-42.

Gobierno del Perú. (2023). *El INDECOPI impuso más de mil sanciones a bancos y financieras por operaciones no reconocidas por sus usuarios*. https://www.gob.pe/institucion/indecopi/noticias/825526

Gobierno del Perú. (2023). *Indecopi impuso más de mil sanciones a bancos y financieras por operaciones no reconocidas por sus usuarios*. https://www.gob.pe/institucion/indecopi/noticias/825526-el-indecopi-impuso-mas-de-mil-sanciones-a-bancos-y-financieras-por-operaciones-no-reconocidas-por-sus-usuarios

Goytizolo, A. (2024). *Perú Digital 2024: Datos, Insights y Tendencias de Internet en el Perú*. Recuperado de https://www.linkedin.com/pulse/per%C3%BA-digital-2024-datos-insights-y-tendencias-de-en-la-aldo-goytizolo-dwz0e/

GSMA. (2023). *The mobile economy Latin America 2023*. Recuperado de https://www.gsma.com/latinamerica

INDECOPI. (2019). *Guía de protección al consumidor en servicios digitales*. Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

Immobilise. (s.f.). *About the Immobilise System*. https://www.immobilise.com/about

INEI. (2024). *Estadísticas de seguridad ciudadana y fraude financiero en Perú*.

Infobae. (2023). *Estafas digitales dejan millonarias pérdidas en 2023: 6 mil casos en el país y criminales ya usan la IA para engaños*. https://www.infobae.com/peru/2023/12/19/estafas-digitales-dejan-millonarias-perdidas-en-2023-6-mil-casos-en-el-pais-y-criminales-ya-usan-la-ia-para-enganos/

Infobae. (2024, julio 6). *Bancos deberán asumir pérdidas de operaciones no reconocidas en tarjetas de clientes: ¿Desde cuándo?* https://www.infobae.com/peru/2024/07/06/bancos-deberan-asumir-perdidas-de-operaciones-no-reconocidas-en-tarjetas-de-clientes-desde-cuando/

Instituto Nacional de Estadística e Informática (INEI). (2023). *Estadísticas de uso de dispositivos móviles en hogares peruano*s. Recuperado de https://www.inei.gob.pe

Instituto Nacional de Estadística e Informática (INEI). (2023). *Estadísticas de costos energéticos en dispositivos móviles en el Perú*. Recuperado de https://www.inei.gob.pe

Instituto Nacional de Estadística e Informática (INEI). (2023). *Informe técnico: Índice de precios al consumidor*. Recuperado de https://www.inei.gob.pe

Instituto Nacional de Estadística e Informática (INEI). (2024). *Boletín de Estadísticas de Seguridad. Hogares*. Recuperado de https://m.inei.gob.pe/prensa/noticias/el-773-de-la-poblacion-del-pais-de-6-anos-y-mas-de-edad-uso-internet-en-el-segundo-trimestre-del-ano-2023-

14580/#:~:text=Durante%20el%20segundo%20trimestre%20de,a%20similar%20trimestre%20de%202022

Instituto Nacional de Estadística e Informática (INEI). (2023). *Situación de la Población Peruana 2023*. Recuperado de https://cdn.www.gob.pe/uploads/document/file/6616587/5751291-situacion-de-la-poblacion-peruana-2024-una-mirada-de-la-diversidad-etnica.pdf?v=1720728622

Interbank. (2023). ¿*Cómo bloqueo desde mi celular mi usuario y/o cuenta por pérdida o robo?* . Recuperado de https://interbank.pe/pequena-empresa/centro-de-ayuda/banca-por-internet-empresas/como-bloqueo-desde-mi-celular-mi-usuario-y-o-cuenta-por-perdida-o-robo?rfid=search-menu:BLOQUEO:6

Instituto Nacional de Estadística e Informática. (2024). *Estadísticas de Seguridad Ciudadana: Enero - Junio 2024*. https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas-de-seguridad-ciudadana-enero-junio-2024.pdf

Ipsos Perú. (2024). *Informe Encuesta Seguridad - Perú, febrero 2024*. https://www.ipsos.com/sites/default/files/ct/news/documents/2024-03/Informe%20Encuesta%20%20Seguridad%20-%20Per%C3%BA21%20al%2023%20de%20febrero%202024.pdf

Kaspersky Lab. (2023). *Mobile security solutions.*

Recuperado de https://latam.kaspersky.com/resource-center/threats/data-theft?srsltid=AfmBOoqQcS5PQ6RnUHJHEzjyvxqlOkjc6-R9GCbzjjteCabPK3HhKaMo

Kaspersky. (2023). *Online Banking Fraud: How to Keep Your Accounts Secure*. Recuperado de https://usa.kaspersky.com/resource-center/threats/online-banking-theft

Kaspersky. (2024). *Top seven mobile security threats: smart phones, tablets, and mobile internet devices*. Recuperado de https://latam.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

LexisNexis. (2023). *El verdadero costo del fraude en Latinoamérica*. https://risk.lexisnexis.com/global/es/insights-resources/research/latam-true-cost-of-fraud

LexisNexis Risk Solutions. (2024). *El verdadero costo del fraude en América Latina*. https://risk.lexisnexis.com/global/es/insights-resources/research/latam-true-cost-of-fraud

Ley N° 26702. (1996). *Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros*.

Ley N° 29733. (2011). *Ley de Protección de Datos Personales*.

Management Solutions. (2021). *Reporte sobre crimen financiero y fraude bancario*.

Management Solutions. (2023). *Financial crime*. https://www.managementsolutions.com

Merchant Risk Council, Cybersource & Verifi. (2023). *Global ecommerce payments and fraud report*. Recuperado de https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2023-en.pdf

Ministerio de Energía y Minas (MINEM). (2022). *Anuario estadístico de electricidad 2022*. Recuperado de https://www.gob.pe/institucion/minem/informes-publicaciones/4742711-anuario-estadistico-de-electricidad-2022

Ministerio de Trabajo y Promoción del Empleo (MTPE). (2023). *Salario mínimo vital en Perú.* Recuperado de https://www.gob.pe/mtpe

Movistar. (2023). *Conoce los pasos para el bloqueo por robo o pérdida de tu equipo* Recuperado de https://www.movistar.com.pe/imeiNorton. (2023). Mobile security solutions. Recuperado de https://us.norton.com/mobile-security

Naciones Unidas. (2015). *Objetivos de Desarrollo Sostenible*. Recuperado de https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

OMS. (2018). *Impacto del estrés en la salud mental: Directrices para intervenciones tempranas*. Organización Mundial de la Salud.

OSIPTEL. (2020). *Equipos terminales móviles reportados como robados o perdidos*. Organismo Supervisor de Inversión Privada en Telecomunicaciones. Recuperado de https://www.osiptel.gob.pe

OSIPTEL. (2021). *Estadísticas de robo de celulares y medidas de seguridad en el Perú*. Organismo Supervisor de Inversión Privada en Telecomunicaciones.

OSIPTEL. (2023). *Informe de modificación normativa sobre servicios de telecomunicaciones*. https://www.osiptel.gob.pe

OSIPTEL. (2023). *Informe sobre bloqueo de líneas móviles por robo en Perú*.

OSIPTEL. (2023). Recuperado de https://www.osiptel.gob.pe/portal-del-usuario/noticias/osiptel-te-robaron-tu-equipo-celular-sigue-estas-recomendaciones/

OSIPTEL. (2023). *Regulaciones y protocolos de seguridad*. Recuperado de https://www.osiptel.gob.pe

OSIPTEL. (2024). M*ercado móvil repunta al cierre del primer trimestre de 2024 y supera las 41.9 millones de líneas en servicio.* Recuperado de https://www.osiptel.gob.pe/portal-del-usuario/noticias/mercado-movil-repunta-al-cierre-del-primer-trimestre-de-2024-y-supera-las-41-9-millones-de-lineas-en-servicio/

OSIPTEL. (2024). *Encuesta Residencial de Servicios de Telecomunicaciones*. Recuperado de https://sociedadtelecom.pe/wp-content/uploads/2024/10/ERESTEL-2023-final.pdf

Ojo Público. (2023). *Crecen robos financieros digitales que involucran operadoras móviles*. https://ojo-publico.com/4556/crecen-robos-financieros-digitales-que-involucran-operadoras-moviles

Ponemon Institute. (2019). *The cost of insecure mobile devices*. Ponemon Institute. https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf

Presidencia del Consejo de Ministros. (2024). *Decreto Supremo N° 138-2024-PCM*. https://cdn.www.gob.pe/uploads/document/file/7480539/6366747-ds-n-138-2024-pcm.pdf

PwC Perú. (2023). *Reporte sobre riesgos y fraudes en telecomunicaciones*.

PwC Perú. (2023). *Revista Advance 10*. https://www.pwc.pe/es/assets/document/Advance/PwC_revista_Advance_10.pdf

Superintendencia de Banca, Seguros y AFP. (s.f.). *Sistema financiero*.

Superintendencia de Banca, Seguros y AFP (SBS). (2019). *Memoria Anual 2019*. Superintendencia de Banca, Seguros y AFP del Perú. Recuperado de https://www.sbs.gob.pe/Portals/0/jer/Memoria%20Anual%20SBS%202019.pdf

Superintendencia de Banca, Seguros y AFP (SBS). (2023). *Memoria Anual 2023*. SBS.

Superintendencia de Banca, Seguros y AFP. (2023). *Reclamos de bancos y financieras resueltos a favor del cliente*. Recuperado de https://www.sbs.gob.pe/reclamos-de-bancos-y-financieras-resueltos-a-favor-del-cliente.

Superintendencia de Banca, Seguros y AFP (SBS). (2023). Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario. Recuperado de https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222?title=Autenticaci%C3%B3n%20reforzada:%20mayor%20seguridad%20para%20operaciones%20que%20puedan%20generar%20perjuicio%20al%20usuario/1000

Superintendencia de Banca, Seguros y AFP. (2024). *Informe de Estabilidad del Sistema Financiero - Primer semestre 2024*. https://www.sbs.gob.pe/Portals/0/IESF-2024-1.pdf

Superintendencia de Banca, Seguros y AFP (SBS). (2024). Reporte de Indicadores de Inclusión Financiera. Recuperado de https://intranet2.sbs.gob.pe/estadistica/financiera/2024/Junio/CIIF-0001-jn2024.PDF

Symantec. (2019). Internet Security Threat Report. Symantec Corporation. Recuperado de https://docs.broadcom.com/doc/istr-24-2019-en

Unión Internacional de Telecomunicaciones (UIT). (2023). ICT Facts and Figures. Recuperado de https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-mobile-phone-ownership/

Unión Internacional de Telecomunicaciones (UIT). (2023). *Informe sobre la penetración* móvil global en 2023. Recuperado de https://news.un.org/es/story/2023/12/1526712

VictimConnect. (2023). Fraude financiero. https://victimconnect.org/tipos-de-delitos/fraude-financiero

Apéndice

Apéndice A: Entrevistas

Resultados de entrevistas

Apéndice B: Pruebas de usabilidad

Evidencias pruebas de hipótesis

Apéndice C: Evidencia de testimonios cualitativos de usuarios

1. Entrevista a Percy

   Entrevistador: Imaginemos que acabas de perder tu celular. ¿Qué sientes en ese momento?

   Percy: Frustración, estrés, sobre todo ansiedad. Uno no sabe por dónde empezar. Sientes que todo se te viene encima, tus cuentas, tus datos, tus contactos.

   Entrevistador: Totalmente comprensible. Empecemos con la prueba. Adelante, usa Segurazo como si estuvieras en esa situación.

   Percy (navegando): Ok mira, con solo escribir unas letras ya me aparecen los bancos. Eso me da tranquilidad, porque en una situación real no tendría cabeza para buscar todo manualmente.

   Entrevistador: ¿Cómo te hace sentir eso?

   Percy: Me alivia. Siento que por fin alguien pensó en lo que uno realmente necesita en ese momento de caos. Es como tener una guía que te toma de la mano.

2. Entrevista a Milu

   Entrevistador: Cuéntame, ¿cómo te sentiste al usar la aplicación?

   Milu: Me sentí cómoda, la verdad. Apenas entré, todo estaba ordenado. El registro fue rápido, no me demoré, y eso me transmitió seguridad. Es importante cuando estás en una situación complicada, como un robo. Sentí que podía avanzar sin pensar

mucho. Sentí alivio. Me gustó que la app te diga qué hacer, paso por paso. En una situación real creo que eso te da contención. No estás sola, no te abruma. La guía me ayudó a mantenerme enfocada, y eso se agradece cuando estás nerviosa. Me encantó que todo esté centralizado. No solo es bloquear la línea o el celular, también te da opciones para hacer la denuncia. Eso me pareció completo y me dio la sensación de que estaba preparada, como si la app ya hubiese pensado por mí.

3. Entrevista a Miguel

Entrevistador: Cuéntame, ¿cómo te sentiste al navegar por la plataforma?

Miguel: Me pareció adecuada. La verdad, desde que entré sentí que no era complicado. Simplemente manejé por la página y fui haciendo lo que me pedía. Si estás en una situación de robo, creo que lo último que quieres es complicarte… y acá, todo estaba claro. Al inicio pensé que me iba a estresar un poco, pero no fue así. Como la página te lleva paso por paso, más bien sentí tranquilidad. Me gustó que puedas encontrar rápido lo que necesitas. Por ejemplo, seleccioné Entel, Android, y pasé a las entidades financieras sin perderme. Todo iba fluyendo. Me pareció una herramienta útil, pensada para actuar rápido. Y lo más importante, sentí que me acompañaba, que no estaba solo resolviendo todo.

4. Entrevista a Mario

Entrevistador: En la entrevista a Mario uno de los aspectos más destacados fue el alivio que generó la centralización de procesos en un solo entorno digital. Un usuario expresó:

Mario*: "Me han robado antes, como dos veces, y la verdad es que buscar uno por uno la información de cada banco es algo muy complicado de hacer en ese momento."*

Este testimonio evidencia el estrés y la desorientación que suelen acompañar estos eventos, y cómo la solución propuesta facilita la toma de decisiones.

Asimismo, se percibió una transición emocional hacia una mayor sensación de control y seguridad:

"Desde acá yo pueda llamar [a los bancos]. Está excelente."
"Mientras antes haga eso, mejor, porque si no, les alcanza el tiempo de desbloquearlo y acceder a toda la información."

Los usuarios también valoraron la rapidez, claridad y facilidad de uso de la herramienta:

"Muy rápido he podido hacer todo lo que normalmente... uno ni sabe en ese momento qué tiene que hacer primero."
"Me gustó que todo esté centralizado. Es muy claro, no hay demasiada información. Y está bien categorizado."

Estos testimonios confirman que la propuesta no solo resuelve una necesidad funcional, sino que también mitiga el impacto emocional negativo del robo o pérdida del dispositivo móvil, brindando al usuario una experiencia clara, rápida y segura.

5. Entrevista a Jose

Entrevistador: Uno de los testimonios clave corresponde a José Adrianzen, de 32 años, quien experimentó el flujo completo de la solución digital.

Desde el inicio de la interacción, José destacó la claridad y facilidad del sistema, enfatizando que:

Jose*: "El proceso es bastante práctico, intuitivo. Inicia aquí y me va marcando, me va guiando los pasos que debo de ejecutar…"*

Este tipo de orientación progresiva es crucial en situaciones de alta tensión emocional, donde el tiempo y la simplicidad son determinantes. Asimismo, José valoró el alcance integral del sistema:

"Incluso nos da una guía para poder hacer algo que muchas veces no completamos, que es una denuncia policial."

La propuesta de Segurazo también demostró ser pertinente para usuarios con mayor exposición financiera y digital:

"Es bastante útil para todo tipo de personas, tanto naturales como también personas que tienen negocios… ya que manejan diferentes cuentas y celulares para trabajar."

Finalmente, el entrevistado subrayó la importancia de tener una herramienta que actúe con precisión y sin ambigüedad:

"En una situación ante este tipo de incidentes, lo que uno quiere es información específica… lo que requiere es tiempo y rapidez para efectuar el bloqueo."

6. Entrevista a Josue

Entrevistador: Imaginemos que acabas de sufrir el robo de tu celular. ¿Qué pasa por tu mente en ese momento?

Josué: Pánico. Lo primero que pienso es: "¿Dónde están mis cuentas?, ¿mis datos?, ¿cómo los protejo ya?" Es una sensación de urgencia, de impotencia, incluso.

Entrevistador: Claro, es una situación difícil. Ahora, por favor empieza a usar Segurazo como si estuvieras en ese momento. ¿Cómo te sientes con el diseño?

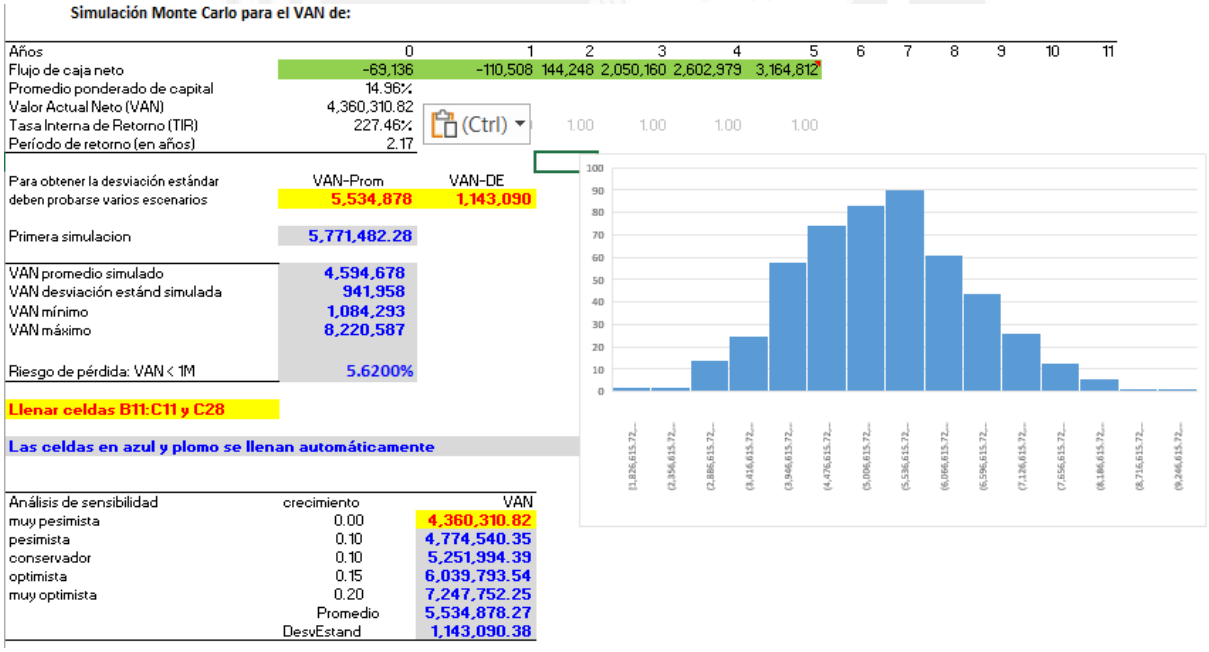
Josué: Tranquilo, me da confianza. Me lleva al grano. No siento que me voy a perder ni que tengo que ser un experto para entender.

Entrevistador: ¿Y al momento de bloquear tus cuentas?

Josué: Súper fácil. Está bien explicado. Se siente como si la página *pensara por mí*, y eso me da alivio. Porque en una situación real, uno está estresado, no piensa bien.

Durante la validación de la aplicación “Segurazo”, se aplicaron entrevistas de usabilidad

Apéndice D: Prueba de Montecarlo para Viabilidad Financiera



Simulación Monte Carlo para el VAN de:

Años	0	1	2	3	4	5	6	7	8	9	10	11
Flujo de caja neto	-69,136	-110,508	144,248	2,050,160	2,602,979	3,164,812						
Promedio ponderado de capital	14.36%											
Valor Actual Neto (VAN)	4,360,310.82											
Tasa Interna de Retorno (TIR)	227.46%											
Período de retorno (en años)	2.17											

(Ctrl)

Para obtener la desviación estándar deben probarse varios escenarios	VAN-Prom	VAN-DE
	5,534,878	1,143,090
Primera simulacion	5,771,482.28	
VAN promedio simulado	4,594,678	
VAN desviación estánd simulada	941,958	
VAN mínimo	1,084,293	
VAN máximo	8,220,587	
Riesgo de pérdida: VAN < 1M	5.6200%	

Llenar celdas B11:C11 y C28

Las celdas en azul y plomo se llenan automáticamente

Análisis de sensibilidad	crecimiento	VAN
muy pesimista	0.00	4,360,310.82
pesimista	0.10	4,774,540.35
conservador	0.10	5,251,994.39
optimista	0.15	6,039,793.54
muy optimista	0.20	7,247,752.25
	Promedio	5,534,878.27
	DesvEstand	1,143,090.38

Apéndice E: Prueba de Sensibilidad para Viabilidad Financiera

Muy Opti

Año	1	2	3	4	5
Demanda Potencial	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	55%	65%	85%	90%	95%
N°	398,389	491,049	668,590	735,923	806,369
Precio	1.80	3.81	7.35	6.56	7.95
Ingresos	716,571	1,872,000	4,911,692	4,829,143	6,414,400

Utilizamos la información para asignara un %

Año	1	2	3	4	5
Bancos	53%	57%	59%	59%	61%
Financieras	32%	28%	22%	22%	20%
Cajas	16%	15%	19%	19%	18%

Paso 7

De esta manera el ingreso anual generado por cada tipo de entidad es

Año	1	2	3	4	5
Bancos	377,143	1,074,667	2,903,077	2,854,286	3,936,800
Financieras	226,286	520,000	1,067,077	1,049,143	1,292,000
Cajas	113,143	277,333	941,538	925,714	1,185,600

Paso 8

Cantidad de Entidades

Podemos suponer que convencemos a BCP, luego en segundo año a otros bancos grande y al terecer año ya logramos captar a todo ASBANC

Año	1	2	3	4	5
Bancos	2	4	10	10	14
Financieras	2	4	8	8	10
Cajas	2	4	10	10	13

Paso 9

De esta manera el precio unitario es el siguiente:

Año	1	2	3	4	5
Bancos	15,714	22,389	24,192	23,786	23,433
Financieras	9,429	10,833	11,115	10,929	10,767
Cajas	4,714	5,778	7,846	7,714	7,600

Paso 10: VAN Financiero

	0	1	2	3	4	5
Ventas		716,571	1,872,000	5,065,692	5,010,643	6,617,900
Costo de ventas		-112,471	-317,400	-601,809	-607,943	-714,404
Gastos administrativos y de ventas		-28,000	-287,244	-277,171	-272,439	-272,519
Depreciación Máquina 1		-2,664	-2,664	-2,664	-2,664	-2,664
UTILIDAD OPERATIVA		573,436	1,264,692	4,184,048	4,127,597	5,628,314

UTILIDAD OPERATIVA AFTER TAX (NOPAT)		404,273	891,608	2,949,754	2,909,956	3,967,961
Depreciación Máquina 1		2,664	2,664	2,664	2,664	2,664
FCO		406,937	894,272	2,952,418	2,912,620	3,970,625
Inversión inicial	-140,471					
FCL	-140,471	406,937	894,272	2,952,418	2,912,620	3,970,625
Préstamo bancario	74,188	-12,152	-13,367	-14,704	-16,174	-17,792
Intereses	0	-7,419	-6,204	-4,867	-3,397	-1,779
Escudo Fiscal		2,226	1,861	1,460	1,019	534
FCF	74,188	-17,345	-17,710	-18,111	-18,552	-19,037
FCA	-66,283	389,592	876,562	2,934,307	2,894,068	3,951,588

WACC	**16%**					
CAMP	**21%**					
	0	**1**	**2**	**3**	**4**	**5**
VA FCL	-S/ 140,471	S/ 351,674	S/ 667,877	S/ 1,905,542	S/ 1,624,569	S/ 1,913,933
VAN FCL (VAN económico)	S/ 6,323,124					
TIR FCL	**413.06%**					
IR	-0.376833687					
VA FCA	-66,283	320,677	593,882	1,636,370	1,328,444	1,493,017
VAN FCA (VAN financiero)	S/ 5,306,108					
TIR FCA	**722.97%**					

Optimista

Año	1	2	3	4	5
Demanda Potencial	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	45%	55%	75%	80%	85%
N°	325,955	415,503	589,932	654,154	721,488
Precio	1.80	3.81	7.35	6.56	7.95
Ingresos	586,286	1,584,000	4,333,846	4,292,571	5,739,200

Utilizamos la información para asignara un %

Año	1	2	3	4	5
Bancos	53%	57%	59%	59%	61%
Financieras	32%	28%	22%	22%	20%
Cajas	16%	15%	19%	19%	18%

Paso 7

De esta manera el ingreso anual generado por cada tipo de entidad es

Año	1	2	3	4	5
Bancos	308,571	909,333	2,561,538	2,537,143	3,522,400
Financieras	185,143	440,000	941,538	932,571	1,156,000
Cajas	92,571	234,667	830,769	822,857	1,060,800

Paso 8

Cantidad de Entidades

Podemos suponer que convencemos a BCP, luego en segundo año a otros bancos grande y al terecer año ya logramos captar a todo ASBANC

Año	1	2	3	4	5
Bancos	2	4	10	10	14
Financieras	2	4	8	8	10
Cajas	2	4	10	10	13

Paso 9

De esta manera el precio unitario es el siguiente:

Año	1	2	3	4	5
Bancos	12,857	18,944	21,346	21,143	20,967
Financieras	7,714	9,167	9,808	9,714	9,633
Cajas	3,857	4,889	6,923	6,857	6,800

	0	1	2	3	4	5
Ventas		586,286	1,584,000	4,487,846	4,474,071	5,942,700
Costo de ventas		-112,471	-317,400	-601,809	-607,943	-714,404
Gastos administrativos y de ventas		-28,000	-287,244	-277,171	-272,439	-272,519
Depreciación Máquina 1		-2,664	-2,664	-2,664	-2,664	-2,664
UTILIDAD OPERATIVA		443,151	976,692	3,606,202	3,591,025	4,953,114
UTILIDAD OPERATIVA AFTER TAX (NOPAT)		312,421	688,568	2,542,372	2,531,673	3,491,945
Depreciación Máquina 1		2,664	2,664	2,664	2,664	2,664
FCO		315,085	691,232	2,545,036	2,534,337	3,494,609
Inversión inicial	-140,471					
FCL	-140,471	315,085	691,232	2,545,036	2,534,337	3,494,609
Préstamo bancario	74,188	-12,152	-13,367	-14,704	-16,174	-17,792
Intereses	0	-7,419	-6,204	-4,867	-3,397	-1,779
Escudo Fiscal		2,226	1,861	1,460	1,019	534
FCF	74,188	-17,345	-17,710	-18,111	-18,552	-19,037
FCA	-66,283	297,740	673,522	2,526,926	2,515,785	3,475,572

WACC	**16%**
CAMP	**21%**

	0	1	2	3	4	5
VA FCL	-S/ 140,471	S/ 272,296	S/ 516,239	S/ 1,642,611	S/ 1,413,574	S/ 1,684,482
VAN FCL (VAN económico)	S/ 5,388,732					
TIR FCL	**349.45%**					
IR	0.433680916					

VA FCA	-66,283	245,073	456,320	1,409,186	1,154,803	1,313,166
VAN FCA (VAN financiero)	S/ 4,512,266					
TIR FCA	**590.27%**					

Pesimista

Año	1	2	3	4	5
Demanda Potencial	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	25%	35%	55%	60%	65%
N°	181,086	264,411	432,617	490,616	551,726
Precio	1.80	3.81	7.35	6.56	7.95
Ingresos	325,714	1,008,000	3,178,154	3,219,429	4,388,800

Utilizamos la información para asignara un %

Año	1	2	3	4	5
Bancos	53%	57%	59%	59%	61%
Financieras	32%	28%	22%	22%	20%
Cajas	16%	15%	19%	19%	18%

Paso 7

De esta manera el ingreso anual generado por cada tipo de entidad es

Año	1	2	3	4	5
Bancos	171,429	578,667	1,878,462	1,902,857	2,693,600
Financieras	102,857	280,000	690,462	699,429	884,000
Cajas	51,429	149,333	609,231	617,143	811,200

Paso 8

Cantidad de Entidades

Podemos suponer que convencemos a BCP, luego en segundo año a otros bancos grande y al terecer año ya logramos captar a todo ASBANC

Año	1	2	3	4	5
Bancos	2	4	10	10	14
Financieras	2	4	8	8	10
Cajas	2	4	10	10	13

Paso 9

De esta manera el precio unitario es el siguiente:

Año	1	2	3	4	5
Bancos	7,143	12,056	15,654	15,857	16,033
Financieras	4,286	5,833	7,192	7,286	7,367
Cajas	2,143	3,111	5,077	5,143	5,200

	0	1	2	3	4	5
Ventas		325,714	1,008,000	3,332,154	3,400,929	4,592,300
Costo de ventas		-112,471	-317,400	-601,809	-607,943	-714,404
Gastos administrativos y de ventas		-28,000	-287,244	-277,171	-272,439	-272,519
Depreciación Máquina 1		-2,664	-2,664	-2,664	-2,664	-2,664
UTILIDAD OPERATIVA		182,579	400,692	2,450,510	2,517,882	3,602,714
UTILIDAD OPERATIVA AFTER TAX (NOPAT)		128,718	282,488	1,727,609	1,775,107	2,539,913
Depreciación Máquina 1		2,664	2,664	2,664	2,664	2,664

FCO		131,382	285,152	1,730,273	1,777,771	2,542,577
Inversión inicial	-140,471					
FCL	-140,471	131,382	285,152	1,730,273	1,777,771	2,542,577
Préstamo bancario	74,188	-12,152	-13,367	-14,704	-16,174	-17,792
Intereses	0	-7,419	-6,204	-4,867	-3,397	-1,779
Escudo Fiscal		2,226	1,861	1,460	1,019	534
FCF	74,188	-17,345	-17,710	-18,111	-18,552	-19,037
FCA	-66,283	114,037	267,442	1,712,163	1,759,219	2,523,540

WACC	**16%**
CAMP	**21%**

	0	**1**	**2**	**3**	**4**	**5**
VA FCL	-S/ 140,471	S/ 113,540	S/ 212,963	S/ 1,116,749	S/ 991,585	S/ 1,225,581
VAN FCL (VAN económico)	S/ 3,519,947					
TIR FCL	**225.29%**					
IR	1.068782481					

VA FCA	-66,283	93,865	181,195	954,819	807,522	953,462
VAN FCA (VAN financiero)	S/ 2,924,581					
TIR FCA	**339.29%**					

Muy Pesimista

Año	1	2	3	4	5
Demanda Potencial	724,344	755,460	786,576	817,693	848,809
Participación de Mercado	15%	25%	45%	50%	55%
N°	108,652	188,865	353,959	408,846	466,845
Precio	1.80	3.81	7.35	6.56	7.95
Ingresos	195,429	720,000	2,600,308	2,682,857	3,713,600

Utilizamos la información para asignara un %

Año	1	2	3	4	5
Bancos	53%	57%	59%	59%	61%
Financieras	32%	28%	22%	22%	20%
Cajas	16%	15%	19%	19%	18%

Paso 7

De esta manera el ingreso anual generado por cada tipo de entidad es

Año	1	2	3	4	5
Bancos	102,857	413,333	1,536,923	1,585,714	2,279,200
Financieras	61,714	200,000	564,923	582,857	748,000

Cajas	30,857	106,667	498,462	514,286	686,400

Paso 8

Cantidad de Entidades

Podemos suponer que convencemos a BCP, luego en segundo año a otros bancos grande y al terecer año ya logramos captar a todo ASBANC

Año	1	2	3	4	5
Bancos	2	4	10	10	14
Financieras	2	4	8	8	10
Cajas	2	4	10	10	13

Paso 9

De esta manera el precio unitario es el siguiente:

Año	1	2	3	4	5
Bancos	4,286	8,611	12,808	13,214	13,567
Financieras	2,571	4,167	5,885	6,071	6,233
Cajas	1,286	2,222	4,154	4,286	4,400

	0	1	2	3	4	5
Ventas		195,429	720,000	2,754,308	2,864,357	3,917,100
Costo de ventas		-112,471	-317,400	-601,809	-607,943	-714,404
Gastos administrativos y de ventas		-28,000	-287,244	-277,171	-272,439	-272,519
Depreciación Máquina 1		-2,664	-2,664	-2,664	-2,664	-2,664
UTILIDAD OPERATIVA		52,294	112,692	1,872,664	1,981,311	2,927,514
UTILIDAD OPERATIVA AFTER TAX (NOPAT)		36,867	79,448	1,320,228	1,396,824	2,063,897
Depreciación Máquina 1		2,664	2,664	2,664	2,664	2,664
FCO		39,531	82,112	1,322,892	1,399,488	2,066,561
Inversión inicial	-140,471					
FCL	-140,471	39,531	82,112	1,322,892	1,399,488	2,066,561
Préstamo bancario	74,188	-12,152	-13,367	-14,704	-16,174	-17,792
Intereses	0	-7,419	-6,204	-4,867	-3,397	-1,779
Escudo Fiscal		2,226	1,861	1,460	1,019	534
FCF	74,188	-17,345	-17,710	-18,111	-18,552	-19,037
FCA	-66,283	22,186	64,402	1,304,781	1,380,936	2,047,524

WACC	**16%**					
CAMP	**21%**					
	0	**1**	**2**	**3**	**4**	**5**
VA FCL	-S/ 140,471	S/ 34,163	S/ 61,324	S/ 853,817	S/ 780,591	S/ 996,130
VAN FCL (VAN económico)	S/ 2,585,555					
TIR FCL	**165.85%**					
IR	1.225751313					

VA FCA	-66,283	18,261	43,633	727,635	633,882	773,610
VAN FCA (VAN financiero)	S/ 2,130,739					

TIR FCA	229.24%

Apéndice F: Prueba de Montecarlo para el Plan de Marketing

Simulación Monte Carlo usando análisis de hipótesis

	VTVC/CAC	CAC	VTVC
Promedio esperado	8.77	18,556	165,147
Desviación estándar	0.57	5,827	62,520
Primera simulación	7.89	11,463	193,020

Promedio	8.746
Desviación estándar	0.552
Mínimo	7.156
Máximo	10.187
Alta eficiencia: > 7; <9	90.46%

Llenar celdas C21 y D21

Las celdas en azul y plomo se llenan automáticamente

Análisis de sensibilidad	crecimiento LTV	crecimiento CAC	LTV	CAC	LTV / CAC
	0.0%	0.0%	109537	13635	8.0
	10.0%	5.0%	120491	14317	8.4
	20.0%	15.0%	144589	16464	8.8
	30.0%	25.0%	187965	20580	9.1
	40.0%	35.0%	263152	27783	9.5
	Promedio	Promedio	165,146.74	18,555.96	8.77
	DesvEstand	DesvEstand	62,519.79	5,826.80	0.57

Apéndice G: Prueba de Montecarlo para el Plan de Operaciones

Simulación Monte Carlo usando análisis de hipótesis

	Tiempo de uso
Promedio esperado	4.08
Desviación estándar	1.54
Primera simulación	3.32
Promedio	3.968
Desviación estándar	1.542
Mínimo	-0.488
Máximo	8.571
Alta eficiencia: <5min	71.78%

Llenar celdas C21 y D21

Las celdas en azul y plomo se llenan automáticamente

Análisis de sensibilidad	crecimiento	Tiempo de uso
Muy optimista	0.00	2.71
Optimista	0.10	2.98
Esperado	0.20	3.57
Pesimisita	0.30	4.64
Muy pesimista	0.40	6.50
	Promedio	4.08
	DesvEstand	1.54