FRAUDES EN LÍNEA

MurallApp

Diego Camilo Ochoa Fuentes
Código: 2474813 CC: 1030615199
Santiago Andrés Daza Contreras
Código: 2310813 CC: 1000708752
Kheren Viviana Geraldino Guerrero
Código: 2478980 CC: 1019117295
Geraldin Tatiana Rodriguez Álvarez
Código: 2486243 CC: 1018483806

UNIVERSIDAD SANTO TOMÁS
ESPECIALIZACIÓN GERENCIA MULTIMEDIA Y COMUNICACIÓN DIGITAL
BOGOTA D.C
2025

1. Tema objeto de estudio

Riesgos asociados a fraudes y pérdida de información en línea.

2. Justificación

El fraude en línea se refiere a cualquier actividad delictiva que se lleva a cabo a través de internet, donde los delincuentes buscan obtener dinero o información personal de manera engañosa. En el contexto de fraude en línea en Colombia este ha crecido significativamente en los últimos años, sobre todo en ciudades principales como Bogotá, Medellín, Cali, Barranquilla y Cartagena, donde Bogotá se presenta como uno de los epicentros de fraudes cibernéticos según estudios realizado por La Corporación Unificada Nacional de Educación Superior, siendo la capital colombiana una de las má afectadas por estos robos cibernéticos que para lo que lleva corrido el 2025, la capital presentan una cifra de 15.551 casos según los reportes de Hablamos Bogotá. Según informes como el de TransUnion (2023), los intentos de fraude digital en el país aumentaron un 859% entre 2019 y 2022, con un incremento del 960% en el volumen de operaciones en línea. De estas transacciones digitales, aproximadamente el 3% fueron objeto de intentos de fraude. Este crecimiento refleja una tendencia global, pero en Colombia se destaca por la rapidez de la digitalización y la falta de preparación en algunos sectores para enfrentar estas amenazas. Pero existe una nueva forma de delinquir y es por el sexting, donde en Colombia, como en muchas partes del mundo, es una práctica que ha crecido con el auge de la tecnología y las redes sociales. Consiste en el envío de mensajes, fotos o videos de contenido sexual o erótico a través de dispositivos electrónicos, generalmente entre personas que consienten en ello. Sin embargo, esta práctica, que puede ser una forma de expresión personal o de intimidad, se convierte en un problema cuando es utilizada como herramienta de manipulación y explotación, dando lugar a fenómenos como la sextorsión o el uso no consentido de material íntimo.

En el caso de Colombia, la situación refleja tanto las tendencias globales como los desafíos locales específicos. El país ha experimentado un crecimiento acelerado en la conectividad y el uso de internet con un incremento que alcanzó el 70% de la población en 2023, según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Sin embargo, este avance ha venido acompañado de un incremento en los incidentes de ciberseguridad. El Centro Cibernético Policial de la Policía Nacional reportó más de 30,000 denuncias relacionadas con fraudes en línea en 2022, incluyendo estafas por phishing, suplantación de identidad y robo de información bancaria. Además, la Superintendencia Financiera ha

advertido sobre el aumento de casos de pérdida de datos sensibles debido a la falta de medidas preventivas por parte de los usuarios, un problema que se acentúa en zonas rurales y entre poblaciones con menor acceso a educación formal.

La combinación de estos factores evidencia una necesidad urgente de abordar el problema desde un enfoque educativo y desde la prestación de servicios mediados por la tecnología en pro del fortalecimiento de la ciberseguridad de los usuarios El proyecto de multimedia busca promover una estrategia integral entre la educación en riesgos asociados a fraudes y pérdida de información en línea, y el desarrollo de un aplicación de ciberseguridad que genera una alerta en tiempo real, de posibles fraudes en línea con el objetivo de generar conocimiento aplicado y soluciones prácticas, en ciudades como Bogotá, siendo una de las más afectadas en ciberseguridad y posterior a nivel nacional con las principales ciudades donde se identifica esta problemática como Cali, Barranquilla, Medellín, Bogotá y Cartagena En el ámbito global. El estudio contribuirá a entender cómo las tendencias internacionales en ciberdelincuencia afectan a países en desarrollo y cómo la educación y herramientas digitales pueden ser una herramienta clave para contrarrestarlas. En Colombia, se enfocará en identificar las vulnerabilidades específicas de la población, como el desconocimiento de técnicas de fraude o la baja adopción de medidas de seguridad digital, y en proponer una estrategia educativa que se adapte a la diversidad cultural, social y económica del país. Sin embargo, para esto tenemos que ser anfibios entre la seguridad digital, fraudes y los usuarios que nos permita identificar las principales vulnerabilidades a las que se enfrentan las empresas y los usuarios, analizar los métodos más comunes utilizados por los Hackers o delincuentes y proponer un programa de educación, prestación de servicios de seguridad por medio de una aplicación de ciberseguridad que esté adaptado a diferentes públicos. Con ello, se busca empoderar a individuos y organizaciones para reducir la incidencia de estos problemas y fomentar un uso más seguro y responsable de la tecnología, contribuyendo así al bienestar social y al desarrollo sostenible en la era digital.

3. Objetivo General

Promover una cultura de seguridad de la información en las ciudades principales del país a través de la educación, donde el usuario pueda navegar de forma segura en internet, además de una herramienta digital para la detección de fraudes en tiempos real (aplicación), con el fin de reducir los riesgos asociados a ciberataques, fraudes y pérdida de datos, fortaleciendo las

capacidades de ciudadanos, empresas privadas e instituciones públicas en la protección de la información.

4. Objetivos específicos

Mejorar de forma integral la seguridad en el entorno digital, implementando medidas de protección robustas para salvaguardar la información y la integridad de los usuarios en línea, por medio de una aplicación que permite a los usuarios realizar de manera segura sus operaciones financieras.

Desarrollar y difundir programas de educación digital accesibles y efectivos, dirigidos a la población bogotana, con el fin de aumentar la conciencia sobre los riesgos en línea, promover prácticas seguras en el uso de internet y redes sociales, y capacitar a los ciudadanos en la identificación de información falsa y fraudes cibernéticos

Reducir significativamente la propagación de información falsa y engañosa en cuentas personales en línea, fortaleciendo la capacidad de los usuarios para identificar y responder a este tipo de contenido, y promoviendo la verificación de la información antes de su difusión.

5. Naturaleza de la investigación enmarcada en la viabilidad del proyecto

La naturaleza de la investigación se enmarca en un **enfoque mixto**, combinando metodologías cualitativas y cuantitativas para asegurar la viabilidad del proyecto, generar conocimiento aplicado y proponer soluciones prácticas.

<u>Enfoque cuantitativo:</u>

Herramienta Principal: Una Encuesta sobre "Experiencias con Fraudes en Pagos en Línea".

Datos a Medir: Porcentaje de personas estafadas, tipo de estafa más funcional, rango de edad más propenso, y ubicación donde ocurren más estafas (pagos en internet o *phishing*).

Análisis: Permite analizar el número de casos denunciados, las tendencias en el tiempo y el perfil de las víctimas, aplicando datos numéricos para identificar patrones.

Enfoque Cualitativo:

Herramienta Principal: Entrevistas cualitativas a involucrados clave.

Participantes Clave: Se entrevistará a entidades públicas y privadas (como bancos y aseguradoras), víctimas de fraude, y delincuentes (*hackers* o personas que delinquen con estos métodos).

Objetivo de las Entrevistas: Explorar experiencias, percepciones de riesgo, estrategias de seguridad utilizadas y el *modus operandi* de los delincuentes

Indagación Documental (Fundamento Teórico y Legal)

Se realizará una revisión exhaustiva para establecer una base sólida de información.

- **Material a revisar:** Documentos, informes, estudios previos, textos académicos, datos estadísticos e informes gubernamentales.
- **Enfoque Normativo:** Examen de **marcos normativos vigentes** (local e internacional) sobre protección de datos y políticas implementadas para la seguridad de la información.

6. AND de su propuesta (Misión, Visión, Valores y Políticas)

Propósito:

Brindar confianza en los pagos en línea y mejorar la reputación de las empresas de recaudo online y concientizar a la población para que puedan identificar por cuenta propia todos los tipos de fraude a los que pueden estar expuestos.

Misión:

Con el uso de una aplicación móvil que permita identificar y avisar a los usuarios de distintos fraudes a los que podrían estar expuestos cuando lleguen a realizar una transacción bancaria y mediante contenidos y charlas multimedia, dar a los usuarios oportunidades de aprendizaje para que puedan aprender y poder entender por cuenta propia todos los riesgos que pueden encontrarse en línea

Visión:

En 5 años (2030) buscamos continuar como empresa teniendo un éxito notable en Colombia y habernos expandido a nivel internacional, enfocándonos primero en países cercanos de Latinoamérica como Chile, Argentina, Ecuador, Perú, etc.

Valores:

Confianza, reputación y seguridad.

Son los pilares fundamentales que definen esta marca de ciberseguridad financiera. La plataforma actúa como un sistema para alertar sobre pagos fraudulentos, garantizando la **Seguridad** de cada transacción. Esta capacidad de protección proactiva, junto con la educación continua del usuario sobre tipos de fraude, establece la **Reputación** de la marca como líder en defensa digital, generando así la **Confianza** esencial para navegar con certeza en el entorno de pagos.

Personalidad:

El concepto que se abarca para esta investigación busca enfocarse en la relación que posee la navegación sobre mar, con la navegación a través de plataformas digitales. Donde las famosas historias de piratas buscan conectarse con los riesgos asociados a fraudes y pérdida de información en línea y la enseñanza de cómo identificar estos peligros en el internet. Usando un barco que viaje por diferentes islas que muestren los peligros que puedan llegar a tener al navegar por el mar (la red), en donde todas las islas logran identificarse por los distintos tipos de peligros a los que uno puede llegar a enfrentarse, entre ellos, el fishing (Robo de identidad), phishing (Malware), estafas y sextorsión.

7. Organización (Descripción general de la investigación y/o propuesta)

La organización del proyecto MurallApp se define como una estrategia integral de seguridad de la información que aborda el creciente problema del fraude en línea en Colombia, enfocándose en la falta de educación digital de la población. La propuesta combina el desarrollo de una aplicación móvil de ciberseguridad (que emite alertas en tiempo real y de manera manual sobre posibles fraudes bancarios y sitios maliciosos) con la creación y difusión de programas de educación digital, utilizando una identidad de marca basada en la

Confianza y la Seguridad mediante un concepto pirata de cómo la gente navega con sus barcos por el internet y todo el mundo digital, que busca ser líder en el sector y expandirse a Latinoamérica en cinco años

8. Público objetivo estimado y de impacto directo e indirecto

Millennials – nativos digitales

Los millennials (nacidos entre 1982 y 1994) representan uno de los segmentos más activos en compras y pagos en línea. Son una generación digitalmente conectada, que prefiere la comodidad de comprar desde celulares, computadores, tablets y iPad, buscando experiencias de compra rápidas y personalizadas, haciendo esta actividad desde cualquier lugar.

Primarias

Los millennials de entre los **28 a los 35 años** en la ciudad de Bogotá, caracterizados por ser más activos en espacios digitales (compras en ecommerce , pagos, servicios y suscripciones) Son una generación que prefiere la comodidad de comprar desde celulares, computadores, tablets y iPad, buscando experiencias de compra rápidas y personalizadas, haciendo esta actividad desde cualquier lugar. También destacan por la adaptabilidad y el conocimiento en esta era digital. (clic aquí)

Secundarias

Entidades bancarias y fintechs con operaciones en Bogotá, cuyo propósito en brindarle una mayor confiabilidad a sus usuarios, y a su reforzar la seguridad de sus canales digitales. Estas organizaciones cada vez están invirtiendo más en sus plataformas digitales, para que sus usuarios tengan acceso fácil y rápido a cualquiera de sus servicios, desde la comunidad de un dispositivo tecnológico. (clic aquí)

Dichas entidades en principio serían bancos tradicionales donde identifique una fuerte presencia en la capital sobre todo en su portales digitales

Terciarios

Millennials entre 35 y 43 años su postura frente a lo digital es media alta dado la actividad que tienen de manera online en proceso de compra y pagos sobre todo (Créditos, pagos de seguros, escolaridad, etc. (clic aquí)

9. Públicos (Stakeholders Internos y externos y breve reseña de c/u)

Stakeholders Internos (Conexión Directa con el Proyecto):

Equipo del Proyecto: (Desarrolladores, Gerencia, Creadores). Son los responsables directos de diseñar, implementar y gestionar tanto la aplicación de alertas como los programas de educación digital. Su principal interés es el éxito, la expansión y la viabilidad a largo plazo de MurallApp, basada en sus valores de Confianza, Reputación y Seguridad.

Propietarios/Inversores Iniciales: Personas o entidades que aportan el capital para la fase de desarrollo, investigación y marketing (Tesis, prueba piloto). Su interés es obtener un retorno de la inversión (ROI), asegurar el cumplimiento de la visión a 5 años (expansión a Latinoamérica) y mantener la integridad del producto.

Empleados (futuros): Personal contratado para el soporte técnico, desarrollo continuo, atención al cliente y creación de contenido educativo. Su interés principal es la estabilidad laboral, el crecimiento profesional y la participación en un proyecto con un impacto social positivo.

Stakeholders Externos (Impacto o Afectación por el Proyecto)

Público Objetivo (Millennials 28-35): El consumidor y usuario principal de la aplicación en Bogotá y Colombia. Son el grupo más expuesto al fraude en línea y demandan una solución práctica. Su interés es obtener protección efectiva, alertas en tiempo real y educación digital simple para evitar la pérdida de dinero e información.

Entidades Bancarias y Fintechs: Empresas del sector financiero que se ven afectadas por la falta de confianza del público en las transacciones en línea. Su interés es que MurallApp aumente la seguridad y la reputación de las transacciones digitales en general, lo que promueve un mayor uso de sus servicios.

Entidades de Gobierno y Regulación: (MinTIC, Policía Nacional, Entidades Distritales y Nacionales). Son los organismos encargados de la seguridad pública y la regulación digital. Su interés es que con la aplicación se reduzcan las cifras de cibercrimen (delito de hurto por medios informáticos) en la región, alineándose con las políticas de seguridad del Estado. Su fuerza de influencia es la máxima en el proyecto.

Comunidad General: La población no directamente usuaria, pero que se beneficia de una mayor cultura de ciberseguridad y un entorno digital más seguro. Su interés se centra en el impacto social positivo del proyecto y la reducción de la vulnerabilidad en el ecosistema digital colombiano.

Estafadores / Redes Delincuenciales: Este es el Grupo de Oposición al proyecto. Su modelo de negocio se basa en la falta de educación y la inseguridad de los usuarios. Su rol es intentar frustrar o evadir las alertas y programas de MurallApp, aunque su fuerza de oposición es catalogada como media en el análisis.

10.

Diagrama de Gantt

Link Matriz 01

Link Anexo a Matriz de Actividades/Matriz de componentes/Matriz de presupuestos

11. Metodología que aplica (descripción de la manera en que realizará la investigación definiendo si la misma es de carácter exploratorio, descriptiva, correlacional o explicativa) y su naturaleza (Cualitativa, cuantitativa o mixta)

De acuerdo con los fundamentos conceptuales que abordan los riesgos asociados a fraude y pérdida de información en línea,el enfoque metodológico de esta investigación será abordada de dos maneras de forma cualitativa y cuantitativa. Esta elección responde a las necesidades de analizar en profundidad las experiencias vividas en las entidades, víctimas y delincuentes, las percepciones individuales y las barreras estructurales en la brecha digital que se enfrentan para mitigar esta problemática.El propósito central es generar un análisis comprensivo de las condiciones de seguridad de la información, incorporando la perspectiva de las entidades, víctimas y delincuentes con respecto a las diferentes cifras de fraude en internet, teniendo un comparativo cuantitativo y cualitativo que permita identificar tanto los riesgos como las oportunidades para mejorar esta problemática.

Los componentes serán los siguientes:

Indagación Documental

Se hará una revisión exhaustiva de documentos, informes, estudios previos y legislación pertinente a la seguridad de la información . La indagación documental busca establecer una base sólida de información que funcione como referencia para el análisis detallado de la situación actual y las soluciones que se proponen.

- **Revisión de textos académicos y estudios previos** sobre seguridad, fraude y educación en pérdida de la información en línea; este proceso abarcaría un examen detallado de las teorías académicas y las investigaciones previas relacionadas con estos temas.
- **Análisis de informes y datos estadísticos** de instituciones gubernamentales y organizaciones no gubernamentales relacionadas con los riesgos asociados a fraude y pérdida de información en línea.
- **Examen de marcos normativos vigentes,** tanto a nivel local como internacional, sobre la protección de datos, identificando políticas existentes y las que ya se encuentran implementadas.

Árbol de Problemas

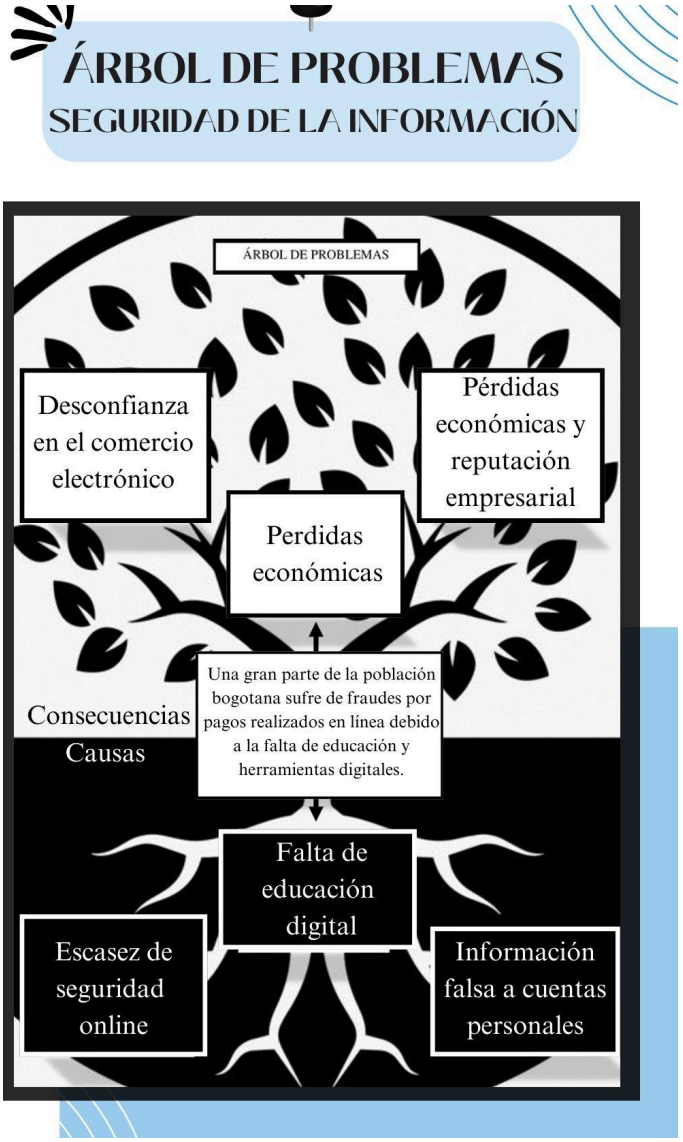


Figura 3. Fuente: Árbol de problemas.

El esquema del árbol de problemas se quiso centrar en los engaños por internet y la protección de la información, especialmente en Bogotá. El problema principal es que muchas personas en Bogotá son víctimas de fraudes cuando pagan cosas por internet, y esto pasa porque no tienen suficiente educación ni conciencia sobre cómo usar internet de forma segura.

Existen varias razones por las que se presenta este problema. Primero, no hay suficiente seguridad en internet, lo que facilita que los estafadores hagan de las suyas. Lo que conlleva a que las páginas web especificadas en compras, los sistemas para pagar y la forma de

comprobar que alguien es quien dice ser no son lo suficientemente buenos. También, la información falsa que circula por internet confunde a la gente y hace que sea más fácil engañarla. La falta de educación digital también es un problema grande, porque las personas no saben cómo darse cuenta de los peligros en línea y cómo evitarlos. Por último, la información falsa que la gente comparte por sus cuentas, a veces sin querer, ayuda a que las estafas se extiendan y que la gente deje de confiar en lo que ve en internet.
Los efectos de estos fraudes son muchos y afectan a todos.

- **Escasez de seguridad online:** La falta de medidas de protección y seguridad en las plataformas digitales facilita la ocurrencia de fraudes y robos de datos, poniendo en riesgo la información personal y financiera de los usuarios.
- **Falta de educación digital:** La carencia de conocimientos y habilidades para desenvolverse de manera segura en el entorno digital vuelve a los ciudadanos vulnerables a engaños y estafas en línea.
- **Información a cuentas personales:** La difusión de noticias falsas y contenido manipulado a través de redes sociales y otras plataformas personales confunde a la población, llevándola a tomar decisiones erróneas basadas en información incorrecta.

Las personas que son estafadas pierden dinero, a veces mucho. Las empresas que venden por internet también sufren, porque su reputación se daña cuando ocurren fraudes y los clientes ya no confían en ellas. Además, la desinformación y los engaños hacen que la gente desconfíe de comprar por internet y de usar las herramientas digitales en general. Es importante saber que este problema no es solo de Bogotá, sino que está pasando en todo el mundo. Cada vez compramos más por internet y usamos más la tecnología, y esto ha creado nuevas oportunidades para los delincuentes, que siempre están buscando nuevas formas de engañar a las personas. De ahí es donde llevamos nuestros medios como las herramientas necesarias y adecuadas para cumplir los objetivos que proponemos, con contenido digital y productos al alcance de la mayoría de la población con el único objetivo de no solo proteger los datos y dinero de la población, sino también fomentar la educación de este mundo digital y cómo podemos prevenir muchos casos de estafas tanto por compras o por engaños.

- **Pérdidas económicas:** Una de las consecuencias más directas y tangibles del fraude en línea es la pérdida económica que sufren las víctimas. Estas pérdidas pueden variar

desde pequeñas sumas de dinero hasta cantidades significativas, dependiendo de la naturaleza y la escala del fraude.

- **Desconfianza en el comercio electrónico:** El aumento del fraude en línea tiene un efecto corrosivo en la confianza de los consumidores en el comercio electrónico. Cuando los usuarios se sienten inseguros al realizar transacciones en línea, se reduce su disposición a participar en actividades de compra y venta a través de internet. Esta desconfianza puede frenar el crecimiento del comercio electrónico, limitar las oportunidades para las empresas y afectar la economía en general.
- **Pérdidas económicas y reputación empresarial:** El fraude en línea no solo afecta a los consumidores individuales, sino también a las empresas que operan en el entorno digital. Las empresas pueden sufrir pérdidas económicas directas debido a fraudes en las transacciones, pero también pueden experimentar daños a su reputación. La pérdida de confianza de los clientes, la publicidad negativa generada por incidentes de seguridad y los costos asociados a la recuperación de la confianza pueden tener un impacto devastador en la viabilidad a largo plazo de un negocio.

Análisis de involucrados

Se identifican a los involucrados como, millenials víctimas de sexting, fraude bancario, robo de información: este grupo se ve amparado por la priorización de los más expuestos a la inseguridad digital, que se vincula en buena medida a las redes sociales y plataformas de mensajería. Gran porcentaje de estos fraudes van mayormente caracterizados por el Phishing y el robo de datos mediante correos y páginas que hacen pasarse por servicios legítimos o reales, llevando variantes como El vishing, donde personas mediante comunicación a voz por llamada se hacen pasar por un soporte de atención a voz de bancos o empresas importantes. Predominando como el principal modo de hurto de información, incluyéndose a nivel global

"*Los millennials y los usuarios de Internet de la generación Z son los más propensos a ser víctimas de ataques de phishing." - Charles Griffiths, AAG 2025*

A menudo, este grupo debe ocupar un lugar en los referidos programas de prevención y asesoramiento psicológico. Los millennials suelen ser víctimas de fraudes bancarios, llamadas engañosas o estafas en línea. Debido a carencias de conocimiento sobre la

importancia del manejo de información personal en las herramientas utilizadas, conlleva un ámbito que requiere de acompañamiento, capacitación y especialización en protección digital, también sufren de estafadas por internet, víctimas por engaños en sitios de comercio, redes sociales o correos fraudulentos. Muchas veces, estos los millennials arrastran pérdidas económicas y desconfianza hacia los ámbitos digitales. Educación y centros comunitarios. Claves para la prevención que pueden brindar capacitación a los millennials sobre cómo usar Internet y las redes seguras. Negocios y plataformas tecnológicas. Un papel vital en la prevención del fraude, teniendo en cuenta que los millennials son una de las generaciones que más hace uso de las tecnologías, muchos no se aseguran de que sean tecnologías de verificación, que manejan controles de contenido perjudicial y protocolos de seguridad. Redes, delincuentes digitales – grupos de oposición activa que se benefician de la falta de cuidado con la información personal, la falta de regulación o la falta de seguridad de datos por medio de la tecnología de los millennials.

Los millennials, es una de las generaciones más conectadas a lo digital, sin embargo también de las más vulnerables frente a los peligros de internet como el sexting, el phishing, grooming, por su alto nivel de confianza en el manejo de sus datos personales sin percatarse que sean paginas y entidades seguras, su manejo constante desde sus dispositivos tecnológicos a apps bancarias, redes sociales e incluso app de citas, los convierte en un nicho objetivo para el fraude y robo de información.

Figura 4. Fuente: Análisis de involucrados

Involucrados	Expectativas	Fuerza	Resultado
Aseguradoras Seguros (Soat)	4	4	16
Empresa de Telefonia	3	3	9
Entidades Financieras (Davivienda)	3	3	9
Entidad Distritral Sec De Movilidad	5	5	25
Entidad Nacional Casur	5	5	25
Regulador Tecnico Nacional Mitic	3	3	9
Regulador Ponal	5	5	25
Victimas	5	5	25
Estafadores	3	3	9

Acercamiento con algunos implicados

Jonathan Alejandro Fajardo Beltran, una persona que casi termina involucrada en una empresa de fraudes (Entrevistado por Santiago Daza)

Durante la entrevista, se menciona que la manera en que Jonathan tuvo contacto con la empresa, fue gracias a una compañera de trabajo, donde la mujer le pidió que le acompañara a una oferta laboral algo sospechosa, que le habian preguntado por instagram, durante la reunión que tuvieron sobre la oferta laboral de manera presencial, la persona que los estaba instruyendo informaba empezaba preguntandoles cosas básicas, como nivel educativo, ocupación actual, y cosas generales. Después de que deban pagar una leve cantidad de dinero, les explican en como consistiría el trabajo, básicamente debían crear un perfil en instagram bajo su nombre real, y vender un producto ilegal y exportarlo bajo su propio nombre, así, la empresa los mantenía trabajando para ellos al estar involucrados con su verdadera identidad en algo ilegal. Por suerte, tanto Jonathan como su compañera, lograron darse cuenta de toda la farsa antes de poder aceptar algún trato, por lo que no fueron involucrados en nada peligroso.

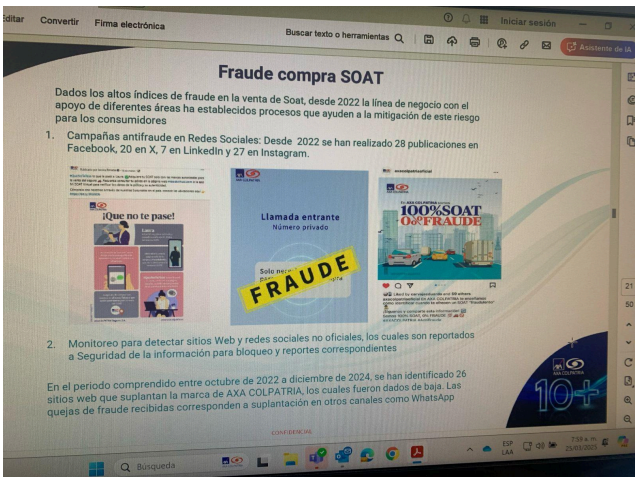
Tania - Entrevista limitada por confidencialidad - Ciberseguridad banco Davivienda

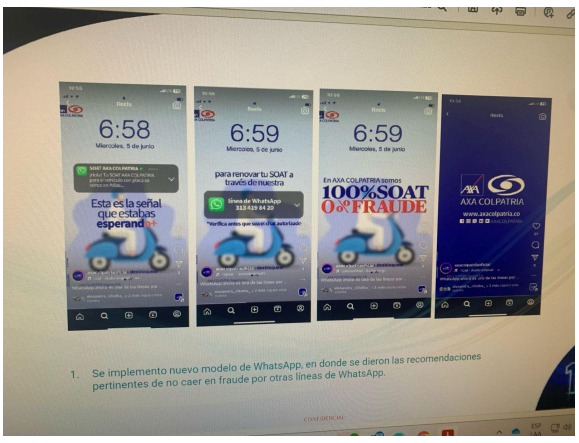
Se realizó una entrevista a esta funcionaria del Banco Davivienda, quien está en el equipo de seguridad y fraudes bancarios de dicha entidad. Desde el banco se han tratado de tomar ciertas medidas para protección de los usuarios en cuanto a la protección de datos, sin embargo por temas de confidencialidad y tácticas de seguridad mucha de esta información no fue compartida. Por tanto menciona que algunas de las acciones que se toman son “Lo habitual que se hace para esos casos son aplicaciones o herramientas tecnológicas que ayudan a detectar esos malware/o proxys”. Agrega “ Hay páginas a nivel Colombia donde se reportan

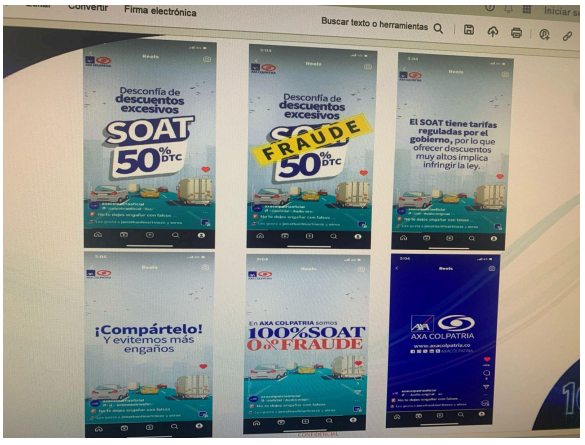
los phishing y ellos lo bajan, pero como no es un ente regulatorio, pues se demora a veces porque tienen que hacer muchas validaciones antes de tomar las consultas". Por último menciona que "Lo que sí te puedo decir es que normalmente entre el compromiso de los datos y la materialización de un fraude puede ser de 3 a 6 meses, y que posterior a que los datos están filtrados las bases vendidas de los malandros, ya se es muy difícil salir de allí. Por eso lo ideal es que todo se haga a nivel de prevención de filtración de información de protección de datos, es por eso y vital la ley de protección de datos".

- **Seguros (Venta de Soat)**

Se hace un diálogo previo con Maria Carolina Novoa Rojas Gerente Técnica Bancaseguros y Ramos de Vida · AXA COLPATRIA, quien nos da las diferentes campañas que utilizan para difundir y mitigar el fraude frente a la compra de soat en AXA COLPATRIA.







Se identifica a este involucrado como uno de los más comunes en el fraude de compra online,en el cual podemos determinar que lo que transcurre entre el año 2022 a diciembre del

2024 identificaron 26 páginas web que suplantan la marca para efectuar fraudes en la compra del soat, las cuales hicieron lo pertinente para poderlas bajar de internet y evitar el fraude.Además realizaron una campaña en redes sociales para combatir e informar a la población sobre este tipo de fraude teniendo como resultado 28 publicaciones en Facebook. 20 en X, 7 en Linkedin y 27 en instagram, vale la pena recalcar que el canal para atender las denuncias fue WhatsApp.Esto nos ayuda a determinar las formas más comunes que utilizan los Hacker o delincuentes para generar este tipo de fraude en el sector de seguros, más específicamente en el área de seguros soat.

- **Casur (Caja de Sueldos de Retirados de la Policía Nacional)**

BOGOTA	unid		NroReti	NETO NOMINA	NOVEDADES	VRNETO A GIRAR	
POPULAR ACH							
CONSIGNACIONES VARIA	8		22679	62.402.436.022,00		62.402.436.022,00	
BANCO BANCAFE/ DAVI	18		1974	4.557.260.267,00		4.557.260.267,00	
POPULAR CONSIGNACIO	30		51747	119.420.800.775,00		119.420.800.775,00	
BANCO PICHINCHA	39		5	11.414.977,00		11.414.977,00	
DAVIVIENDA	40		10444	32.139.411.305,00		32.139.411.305,00	
CAJA SOCIAL CONSIGNA	41		2433	6.003.061.562,00		6.003.061.562,00	
GRANAHORRAR CONSIG	43		679	1.756.591.511,00		1.756.591.511,00	
CORPLAS VILLAS	44		1765	4.737.492.892,00		4.737.492.892,00	
PROCREDIT	49					0,00	
				231.028.469.311,00	**0,00**	**231.028.469.311,00**	POPULAR
ARCHIVO PREVIO							
CENTRO 1	1		71	190.156.347,00	0,00	190.156.347,00	
CENTRO 2	2		1	1.561.438,00	0,00	1.561.438,00	
CENTRO 3	3		7	13.268.605,00	0,00	13.268.605,00	
				204.986.390,00	**0,00**	**204.986.390,00**	POPULAR
CHEQUES							
DOMICILIO NORTE	10				0,00	0,00	
AUTORIZACIONES	12		42	179.083.898,00	0,00	179.083.898,00	
DOMICILIO SUR	13		0	0,00	0,00	0,00	
PENDIENTES (NOMINA 14	14		4	4.132.565,00	0,00	4.132.565,00	AGRARIO
BANCO AGRARIO	16		1243	2.749.731.054,00	0,00	2.749.731.054,00	AGRARIO
				2.932.947.517,00	**0,00**	**2.932.947.517,00**	
GDRO PAGOS MASIVOS							POPULAR-AGRARIO
SUBOFICIALES CL43	19		30	120.477.883,00	0,00	120.477.883,00	
BBVA CRA 9	20		37	86.573.605,00	0,00	86.573.605,00	
				207.051.488,00	**0,00**	**207.051.488,00**	
CONSIGNACIONES							BBVA
BCO BOGOTA CONSG	32		4987	12.694.952.468,00	0,00	12.694.952.468,00	
GDRO CONSIGNACIONES	31		22525	60.660.762.092,00	0,00	60.660.762.092,00	BOGOTA
TOTAL NETO BOGOTA			**120.673**	**307.729.169.266,00**	**0,00**	**307.729.169.266,00**	BBVA
TOTAL NETO DPTOS			**115**	**220.651.688,00**		**430.874.432.921,00**	
TOTAL NETO NOMINA			**120.788**	**307.949.820.954,00**		430.874.432.921,00	
						0,00	
		CRUCE	**120.788**	**307.949.820.954,00**			
			0	**0,00**			

Se hace un diálogo previo con Ronald Ricardo Ruíz Velásquez de la Oficina Asesora de Planeación e Informática de Casur, el cual nos data de que en colombia se te tiene un total de 120.788 policías pensionados a corte del 31 de marzo y que esto va incrementando mes a mes, de los cuales se les paga un total de 307.949.820.950 millones de pesos mensuales que se realizan por medio de consignación, pero estos están categorizados en tres grupos o formas de pago para los pensionados; en primer lugar están los pagos directos a los pensionados que no tienen ninguna novedad, segundo los que presentan novedad ya sea porque se encuentran enfermos terminales o en algún proceso legal que les impiden realizar el cobro del mismo y por ende les toca delegar una persona autorizada para cobrar para su sueldo y tercero las personas que están fuera del país y se les gira a una en su país que residen.

Es importante reconocer que, aunque se proporcionan datos sobre el número de pensionados y los pagos mensuales, parece que las medidas para mitigar los ataques cibernéticos son limitadas, ya que no utilizan ningún tipo de método para poder prevenir ataques en el robo de la información como phishing o bloqueos de su página, porque nos referencia que han sido atacados en su página web pero al momento no han tenido una forma efectiva de evitar esto, de igual forma los Malware que utilizan los estafadores para suplantar la entidad son muy recurrentes para poder robar información en los usuarios y la única forma de poder mitigar esto es mediante charlas en internet que realizan con los pensionados para poder informarles de este tipo de fraudes, pero nos indica que las charlas virtuales de prevención son un buen primer paso, pero es fundamental que se implementen estrategias más robustas y prácticas para proteger la información sensible. La seguridad cibernética es un tema crítico, y es esencial que las empresas tomen acciones concretas para salvaguardar los datos de sus usuarios.

- **Davivienda (Entidad financiera)**

Se entabla una conversación con Laura Rodriguez, ex trabajadora del banco Davivienda en el área de fraudes, ellas nos cuenta que Davivienda maneja diferentes estrategias y herramientas para detectar fraudes en las transacciones de los clientes, nos cuenta cuáles son algunas de las medidas; como por ejemplo que el banco realiza seguimiento de las transacciones para identificar patrones no comunes que pueden ser en gran parte fraudes, inicialmente para denunciar un fraude el usuario se comunica y debe pasar un filtro de seguridad, este lo realiza un bot y posterior si pasa el filtro lo comunican con un asesor, nos cuenta que el banco hace diferentes recomendaciones de seguridad para los clientes y campañas de prevención con la información, lanzaron una iniciativa que se llama "La Tía Segura" y por este medio le informan a los clientes las modalidades de fraude más frecuentes y les explican cómo prevenirlas. El banco le recomienda a los clientes proteger su información personal y no compartirla con terceros ya que han evidenciado que muchos fraudes han sido de personas cercanas que han tenido acceso a la información personal, también sugieren cambiar las claves de forma frecuente y no compartirla con nadie, nos cuenta que muchos clientes reportaron correo electrónicos de cuentas que se hacían pasar por el banco con link fraudulentos, y sugieren comunicarse directamente con el banco ya que ellos no hacen envío de información con links, Davivienda cuenta con canales oficiales especialmente para reportar fraudes y tiene un área especializada en este tema, les dan a conocer a los clientes como comunicarse para poder reportarlo, la gran mayoría de fraudes se da por la falta de

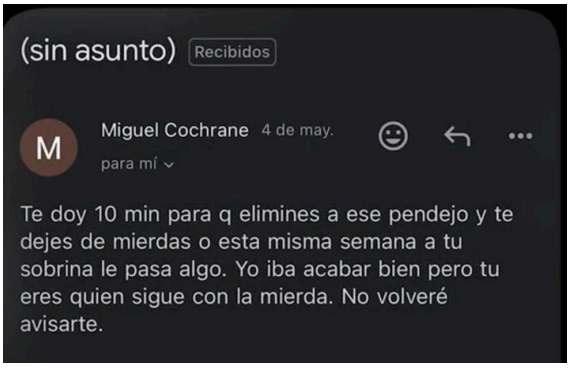
privacidad que tienen los clientes con su información personal. Davivienda combina tecnología avanzada con estrategias de educación al cliente para detectar y prevenir fraudes. Generan muchos comunicados a los usuarios, recordándoles seguir las recomendaciones de seguridad y reportando actividades sospechosas.

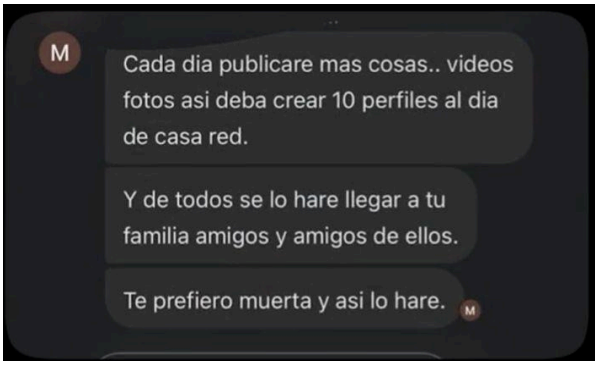
- **Un podcast sobre sextorción y manipulación de datos personales**

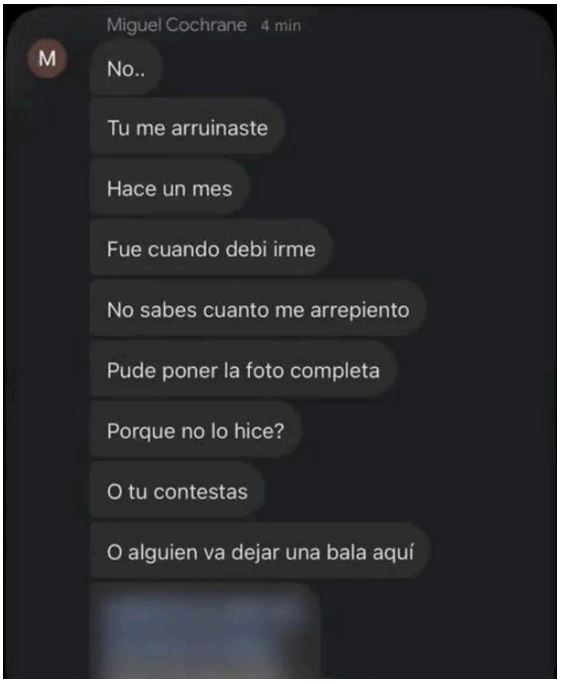
Durante la búsqueda de involucrados, se ha logrado encontrar un caso particular de estafas involucradas al phishing, el robo de información mediante correo electrónico y al catfishing, creación de identidades falsas, donde una víctima de estas actividades maliciosas fue engañada al intentar encontrar una pareja en una aplicación en línea para citas. Gracias a este caso, podemos tener una perspectiva mucho más analítica y clara sobre cómo el estafador controla a sus víctimas para conseguir la información que busca y cómo logra manipularlas para su propio beneficio, sin siquiera tener la necesidad de tener algún contacto físico con la persona, solo mediante el teléfono, dejando en claro la gran falta de seguridad cibernética que nuestros dispositivos móviles poseen.

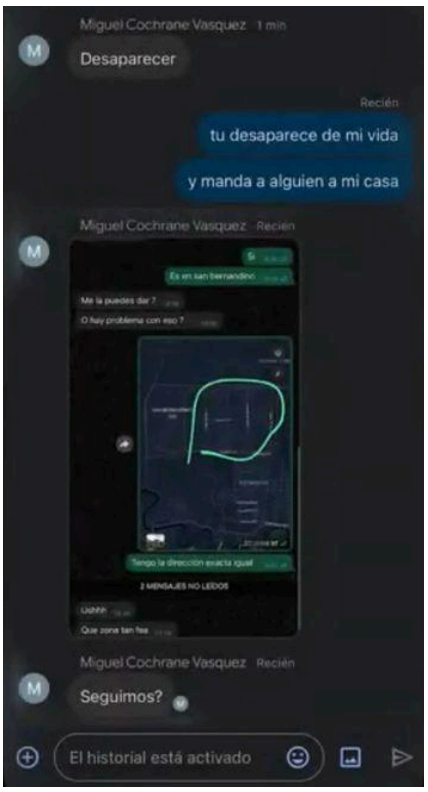
Al principio se habla que la supuesta persona que la chica había conocido mediante la aplicación en línea era un hombre apuesto que vivía en los Estados Unidos, demostrándole con fotos y pruebas "verídicas" la verdad sobre su supuesta historia, aprovechándose de sucesos claves de la víctima, como la muerte de un pariente, con el único objetivo de ganarse su confianza. Cuando ya la chica logra confiar con seguridad en el hombre que ella creía que hablaba, el estafador aprovecha para conseguir información personal, como los miembros de su familia, redes sociales, el lugar donde trabaja e incluso el lugar en donde vivía. La misma chica durante el podcast, menciona que el estafador ya tenía acceso a todas sus redes sociales y podía ver que es lo que ella mantenía oculto en su perfil o con quien chateaba. Cuando ella comienza a sospechar sobre el hombre con el que hablaba, es en donde descubre que todas las imágenes que ella vio en las redes sociales eran sacadas de otro perfil, y que en realidad el estafador ni siquiera vivía en Estados Unidos. Ahí es cuando la chica logra enterarse de la verdad y se descubre la mentira sobre el perfil y la identidad de la persona con la que llevaba hablando por más de un año, de ese modo, el estafador al enterarse de esto procede a pasar a la defensiva, con amenazas hacia la chica, con chantajes como el uso de unas fotos íntimas del cuerpo de la mujer, y publicarlas en redes para que sean vistas por todos sus conocidos y familiares, al final, como el estafador terminó con el control absoluto de su celular, la chica optó por conseguir uno nuevo, con un nuevo correo, nueva cuenta y nuevo número, dando a

entender el gran impacto que esto puede generar en el robo de datos personales, siendo esto último, una de las principales consecuencias de las estafas también en otros asuntos como los pagos en línea o páginas de internet falsas. A continuación se presentan imágenes representativas del caso, donde la víctima fue amenazada y chantajeada en varias ocasiones en contra de su voluntad, aquí se demuestra como el estafador mediante correos y chats amenazaba con mensajes homicidas o con publicar fotos íntimas del cuerpo de la mujer y enviarla a contactos cercanos a ella, como familiares y amigos:






Miguel Cochrane 4 min
M
No..
Tu me arruinaste
Hace un mes
Fue cuando debi irme
No sabes cuanto me arrepiento
Pude poner la foto completa
Porque no lo hice?
O tu contestas
O alguien va dejar una bala aquí


Miguel Cochrane Vasquez 1 min
M
Desaparecer
Recién
tu desaparece de mi vida
y manda a alguien a mi casa
Miguel Cochrane Vasquez Recién
M
Es en san bernardino
Me la puedes dar ?
O hay problema con eso ?
Tengo la dirección exacta igual
2 MENSAJES NO LEÍDOS
Ushhh
Que zona tan fea
Miguel Cochrane Vasquez Recién
M
Seguimos?
El historial está activado

Árbol de objetivos

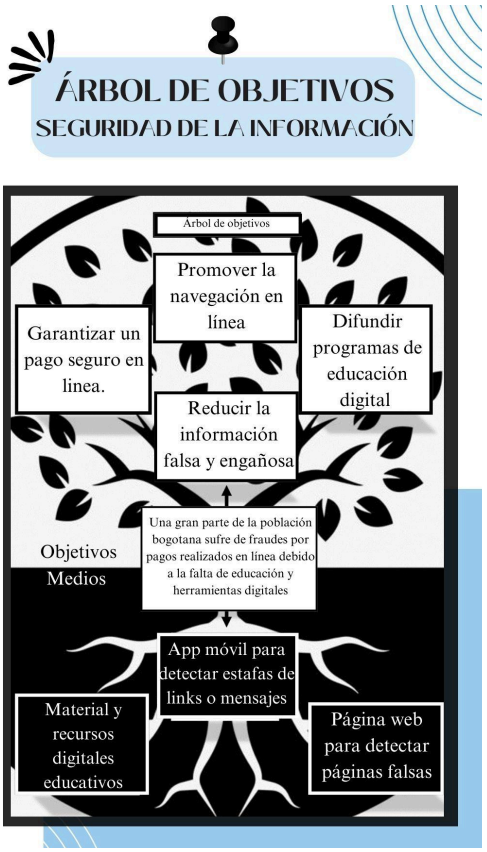


Figura 5. Fuente: Árbol de objetivos

Acciones investigativas:

- Entrevistas a empresas,víctimas y delincuentes que son claves dentro de los diferentes tipos de fraudes y pérdida de información.
- Recopilación y análisis de datos obtenidos por las diferentes entidades, víctimas y delincuentes, en los tipos y formas de fraudes utilizados en cada caso.
- Caracterización de los diferentes tipos de riesgos en fraudes y pérdida de la información.
- Investigación documental en el Ministerio de Tecnologías de la Información y las Comunicaciones con referente a la regulación de las empresas para la protección de la información.
- Caracterización de los diferentes tipos de riesgos en fraudes y pérdida de la información.

Acciones de diseño:

- Crear una identidad visual acorde a los valores tanto de marca como comunicacionales (branding)
- Intervención de edición en la ejecución de videos para generar un material audiovisual con una narrativa acorde al grupo objetivo.
- Generar una interfaz que facilite la navegación e interacción del usuario con la página web.

Acciones de producción:

- **Realizar una multimedia que permita educar e informar a los usuarios de internet** sobre los diferentes tipos de riesgos de fraude y pérdida de información en línea.
- **Crear una ruta segura** en el momento de navegar en interner.
- **Prueba o testeo de la plataforma:** La prueba o testeo se genera cuando la plataforma web ya está casi lista y ha pasado por todo el proceso de construcción narrativo,visual, estructural y analítica.
- **Publicación de la plataforma:** Una vez la plataforma web está lista después de realizar el testeo correspondiente se debe pensar en su publicación.
- **Campañas de marketing y promoción:** crear contenido atractivo y relevante para las redes sociales (colaboraciones) y otros canales de comunicación seleccionados.
- Programas de seguimiento y retroalimentación
- **Recursos audiovisuales:** Banco de entrevistas para el respectivo análisis
- **Recursos de narrativa y diseño:** Narrativa audiovisual para la creación de personajes e identidad de la marca.
- **Recursos audiovisuales:** Videos educativos y explicativos de los diferentes tipos de riesgos en fraudes y pérdida de la información en línea
- **Recursos Audiovisuales:** Guía segura para navegar e interactuar en internet.
- R**ecurso de programación:** Desarrollo de la plataforma.

Síntesis narrativa del proyecto

F.1. Conocer diferentes medios de fraude más frecuentes con sus modalidades de hurto.

F.2. Qué tipo de participación tienen los millennials en estos tipos de fraudes.

F.3.Conocer los mecanismos utilizados por las entidades y usuarios en la prevención de los riesgos asociados a fraude y pérdida de información en línea.

P. Identificacion y caracterizacion de los diferentes modos operandi de fraude y pérdida de información en línea, teniendo en cuenta los mecanismos utilizados para mitigar esta problemática

C.1. Estudio de las condiciones actuales de las diferentes formas de fraude y pérdida de información en línea.

C.2. Lazos entre las diferentes entidades y los usuarios para informar y mitigar los fraudes.

C.3. Promoción de la multimedia para que el alcance sea masivo.

A.1. Entrevistas a empresas,víctimas y delincuentes que son claves dentro de los diferentes tipos de fraudes y pérdida de información.

A.2. Recopilación y análisis de datos obtenidos por las diferentes entidades, víctimas y delincuentes, en los tipos y formas de fraudes utilizados en cada caso

A.3. Caracterización de los diferentes tipos de riesgos en fraudes y pérdida de la información.

A.4. Investigación documental en el Ministerio de Tecnologías de la Información y las Comunicaciones con referente a la regulación de las empresas para la protección de la información.

A.5. Caracterización de los diferentes tipos de riesgos en fraudes y pérdida de la información.

A.6. Crear una identidad visual acorde a los valores tanto de marca como comunicacionales (branding)

A.7. Intervención de edición en la ejecución de videos para generar un material audiovisual con una narrativa acorde al grupo objetivo.

A.8. Generar una interfaz que facilite la navegación e interacción del usuario con la página web.

A.9. Realizar una multimedia que permita educar e informar a los usuarios de internet sobre los diferentes tipos de riesgos de fraude y pérdida de información en línea.

A.10. Crear una ruta segura en el momento de navegar en internet.

A.11. Prueba o testeo de la plataforma: La prueba o testeo se genera cuando la plataforma web ya está casi lista y ha pasado por todo el proceso de construcción narrativo,visual, estructural y analítica.

A.12. Publicación de la plataforma: Una vez la plataforma web está lista después de realizar el testeo correspondiente se debe pensar en su publicación.

A.13. Campañas de marketing y promoción: crear contenido atractivo y relevante para las redes sociales (colaboraciones) y otros canales de comunicación seleccionados.

A.14. Programas de seguimiento y retroalimentación

A.15. Recursos audiovisuales: Banco de entrevistas para el respectivo análisis

A.16. Recursos de diseño:narrativa audiovisual para la creación de personajes e identidad de la marca.

A.17. Recursos audiovisuales: Videos educativos y explicativos de los diferentes tipos de riesgos en fraudes y pérdida de la información en línea

A.18. Recursos Audiovisuales: Guía segura para navegar e interactuar en internet.

A.19. Recurso de programación: Desarrollo de la plataforma

Enfoque Cuantitativo

La investigación tiene como base un enfoque cuantitativo, porque nos ayuda a medir la magnitud de la problemática, con datos estadísticos esenciales como el porcentaje de personas que han sido estafadas durante un año (encuestas), cuál es el tipo de estafa que más tiende a funcionar, qué rango de edad es el más propenso a caer en estas estafas y conocer en donde ocurren más estafas, si por pagos en internet o por phishing. Así mismo, en Bogotá, podemos considerar que siempre se mantiene en aumento, afectando tanto a consumidores como a empresas, así como se menciona en las consecuencias de estas estafas, generando grandes pérdidas económicas y afectando esa confianza en los servicios digitales, cuando se supone que son la herramienta principal del mundo actual.

Este enfoque también nos permite analizar el número de casos denunciados, las tendencias en el tiempo y hasta el perfil de las víctimas, Donde también podríamos aplicar el uso de datos numéricos para la identificaciones de patrones y correlaciones que atribuyen a la formación de estrategias preventivas que aporten al producto final que queremos demostrar.

Base de Encuesta:

Experiencias con Fraudes en Pagos en Línea

1. Información General (Opcional o Anónima)

Puedes responder de forma anónima si lo prefieres.

1.1 Edad: _____

1.2 Género:

- ☐ **Masculino**
- ☐ **Femenino**
- ☐ **Otro / Prefiero no decir**

1.3 Localidad: _____

1.4 ¿El fraude te ocurrió a ti o a un familiar cercano?

- ☐ **A mí**
- ☐ **A un familiar**
- ☐ **Ambos**

2. Información del Fraude

2.1 ¿En qué año ocurrió el fraude? _____

2.2 ¿En qué plataforma ocurrió el fraude? (Puedes marcar más de una)

- ☐ **Redes sociales (Facebook, Instagram, etc.)**
- ☐ **Página web falsa**
- ☐ **App de compras**
- ☐ **WhatsApp / Mensajería**
- ☐ **Otra (especificar): _____**

2.3 ¿Cuál fue el método de pago que se utilizó?

- ☐ **Tarjeta de crédito**
- ☐ **Tarjeta de débito**
- ☐ **Transferencia bancaria**
- ☐ **Pago por billetera digital (Nequi, PayPal, etc.)**
- ☐ **Otro: _____**

2.4 ¿Cuál fue el monto aproximado del fraude?

- ☐ **Menos de $50.000**
- ☐ **$50.000- a $200.000**
- ☐ **$200.000 - $500.000**
- ☐ **Más de $500.000**

3. Detalles del fraude

3.1 ¿Qué producto o servicio intentabas comprar?

3.2 ¿Cómo te contactaron o cómo llegaste a la oferta fraudulenta?

- ☐ **Publicidad en redes**
- ☐ **Enlace compartido por alguien conocido**
- ☐ **Mensaje directo / correo electrónico**
- ☐ **Buscando en Google u otro buscador**
- ☐ **Otro: _____**

3.3 ¿Qué hizo que confiaras en la oferta?

- ☐ **Buen precio / oferta atractiva**
- ☐ **Buen diseño de la página o perfil**
- ☐ **Recomendación de alguien**
- ☐ **Parecía una empresa oficial**
- ☐ **Otro: _____**

4. Reacción y Consecuencias

4.1 ¿Denunciaste el fraude?

- ☐ **Sí, ante la policía o fiscalía**
- ☐ **Sí, ante el banco**
- ☐ **Sí, en redes sociales / comunidad**
- ☐ **No hice denuncia**

4.2¿Pudiste recuperar el dinero?

- ☐ **Sí, totalmente**
- ☐ **Parcialmente**
- ☐ **No**

4.3 ¿Qué impacto tuvo el fraude en ti o en tu familiar? (Puedes marcar más de una)

- ☐ **Pérdida económica**
- ☐ **Estrés emocional**
- ☐ **Pérdida de confianza en compras en línea**
- **Otro: _____**

5. Reflexión y Prevención

5.1 ¿Qué crees que podrías haber hecho para evitar el fraude?

5.2 ¿Qué señales te hicieron identificar que caíste en un fraude?

5.3 ¿Qué consejo le darías a otras personas para evitar caer en fraudes similares?

---

6. Autorización de uso

6.1 Autorizo el uso anónimo de mis respuestas para fines de investigación / prevención de fraude.

- ☐ **Autorizo**
- ☐ **No autorizo**

<u>Entrevistas cualitativas</u>

Se entrevistarán con las entidades involucradas, que participan en dicha problemática. El propósito es explorar sus experiencias, percepciones de riesgo y las estrategias que han utilizado para garantizar su seguridad en línea. Además, se entrevistaron a víctimas y

delincuentes para entender las medidas con las cuales fueron estafados y las modalidades de fraude que utilizan los delincuentes para sus fechorías.

- **Elaboración de entrevistas** a entidades públicas y privadas, víctimas y delincuentes que son clave dentro del fraude y pérdida de la información en línea. Crear la base de las preguntas a realizar
- **Exploración de experiencias** y percepciones en torno a la seguridad y navegación en entornos digitales.
- **Registro audiovisual** y textual de las entrevistas para su posterior análisis.

Esta investigación emplea un enfoque cualitativo. Este método permitirá profundizar en las experiencias y percepciones de los diferentes involucrados, centrándose en las técnicas más comunes de fraude y las entrevistas para explorar más detalladamente las dinámicas de seguridad y fraude en línea.

En la primera etapa, se procederá a la indagación documental clave para fundamentar el diagnóstico de la problemática y garantizar que las soluciones propuestas estén alineadas con las políticas y las buenas prácticas en las entidades para mitigar el fraude en línea. Después, se hará la recopilación de datos a través de conversaciones y notas con funcionarios y víctimas del fraude y pérdida de información en los entornos digitales , tanto en el sector público como privado las víctimas. Esta fase es importante para identificar las dinámicas de hurto y operativas que impactan directamente en las entidades como en los usuarios . Adicionalmente, se analiza el modus operandi de los delincuentes para tener un enfoque más claro de las formas y tipos de fraude utilizados por ellos. Estas observaciones buscan identificar patrones de interacción entre el delincuente y la víctima de estos espacios y comportamientos que reflejan la inseguridad y el papel de educar a las entidades y las víctimas en esta problemática.
El componente cualitativo de la investigación incluirá entrevistas a entidades públicas como privadas y víctimas. Estas entrevistas explorarán sus experiencias, percepciones de riesgo, y las estrategias empleadas para fraude y pérdida de información en línea. También se entrevistará a delincuentes,como hackers o en su defecto personas que delcan con estos métodos, para poder tener un análisis de las formas de fraude utilizadas. Junto a estas entrevistas, se pretende profundizar en estos ámbitos relacionados con la percepción relativa de cada individuo, y este material se recogerá y registrará en formatos audiovisuales y

textuales para su análisis posterior, lo que permitirá evaluar los datos recogidos y facilitará una mejor comprensión de estas dinámicas que enfrentan los riesgos asociados a fraude y pérdida de información en línea.

Para abordar las entrevistas, inicialmente, se ha elaborado un esquema de preguntas generales diseñado para capturar la perspectiva de todos los involucrados clave. Este conjunto de preguntas base abarca temas esenciales como experiencias previas con incidentes de fraudes y las medidas preventivas implementadas. Sin embargo, para obtener información más profunda y relevante, el cuestionario se adaptará. Por ejemplo, las preguntas dirigidas a representantes de corporaciones. En contraste, las preguntas para los ciudadanos o civiles se centrarán en su nivel de conocimiento tecnológico, sus hábitos en línea y las consecuencias personales o emocionales que han experimentado. Asegurando que el análisis de datos no solo sea amplio, sino también lo suficientemente detallado como para reflejar las particularidades de cada grupo de estudio.

- ¿Podría describir cómo ocurrió el incidente de fraude?
- ¿Hubo algún tipo de información personal o corporativa le fue solicitada o comprometida durante el fraude?
- ¿Hubo algún tipo de incentivo, como una oferta especial o una promesa de beneficio, que lo llevó a confiar en la comunicación o el sitio web fraudulento?
- ¿Cómo se dio cuenta de que había sido víctima de un fraude?
- ¿Qué pasos tomó inmediatamente después de identificar el fraude?

12. Aplicación de prueba piloto para ajustes de proyecto y hasta qué nivel llegará la implementación.

MurallApp Carpeta Prototipo

PROTOTIPO MURALLAPP.mp4

manual de marca MurallAPP.pdf

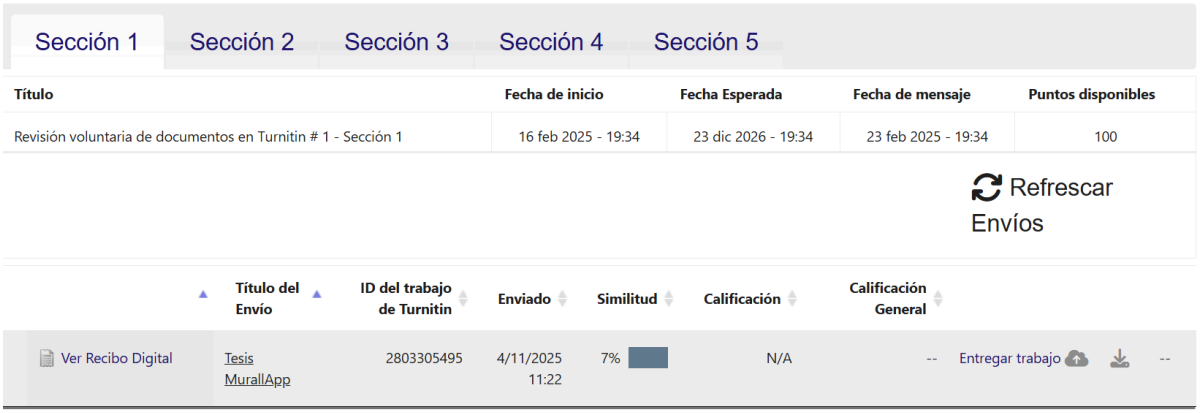
13. Resultados que se esperan obtener y/o aspiracionales sujetos en ajustes y actualizaciones durante el proceso

Los resultados esperados se orientan hacia la máxima Seguridad de la plataforma, buscando que la función automática de detección de fraudes sea reconocida por su precisión y

fiabilidad inigualables, minimizando las alertas incorrectas que comprometería la Confianza del usuario. A nivel de negocio, se busca validar la estrategia de precios logrando que los planes a largo plazo, como el "**Plan Crucero**", dominen las suscripciones, recompensando la lealtad y afianzando la certeza. A largo plazo, la aspiración es establecer una reputación de liderazgo absoluto, transformando la aplicación en el estándar definitivo para obtener "certeza en el momento del pago", y evolucionar de una herramienta a un protocolo de seguridad clave en el ecosistema financiero.

14. Certificado Turnitin

[Comprobación Turnitin.pdf]



15. Bibliografías

[Link Anexo bibliografias]