

Desarrollo de una aplicación móvil para el reporte de delitos en tiempo real en Babahoyo, Ecuador

Development of a mobile application for real-time crime reporting in Babahoyo, Ecuador

<https://doi.org/10.5281/zenodo.20492100>

AUTORES:

Ing. Carlos Julio Soto Valle. Met
csoto@utb.edu.ec
<https://orcid.org/0000-0001-8331-4889>
Universidad Técnica de Babahoyo

Ing. Enrique Ismael Delgado Cuadro. Met
edelgado@utb.edu.ec
<https://orcid.org/0000-0002-7220-9730>
Universidad Técnica de Babahoyo

Ing. Ángel Rafael España León.
aespana@utb.edu.ec
<https://orcid.org/0000-0007-0877-8043>
Universidad Técnica de Babahoyo

Ing. Iván Rubén Ruiz Parrales
iruiz@utb.edu.ec
<https://orcid.org/0000-0001-8644-0629>
Universidad Técnica de Babahoyo

DIRECCIÓN PARA CORRESPONDENCIA: csoto@utb.edu.ec

Fecha de recepción: 20 / 11 / 2025

Fecha de aceptación: 27 / 11 / 2025

RESUMEN

La ciudad de Babahoyo, capital de la provincia de Los Ríos, Ecuador, ha experimentado un alarmante incremento de la delincuencia organizada en los últimos cinco años,

intensificándose tras la pandemia de 2020. Esta situación ha generado un estado de estrés, pánico y zozobra en la población, impactando negativamente el sector económico con cierres forzados de negocios debido a extorsiones, secuestros y amenazas. A pesar de los esfuerzos de la Policía Nacional, Los Ríos se ha consolidado como la segunda provincia más violenta del Ecuador. Ante esta problemática, la presente investigación propone el diseño de la estructura teórica de un sistema informático integral, accesible desde dispositivos móviles, que permita a la ciudadanía reportar diversos tipos de delitos (secuestro, sicariato, extorsión, amenazas, femicidio, narcotráfico) e incluya funcionalidades avanzadas. Un componente clave es un módulo innovador para la interacción con atacantes, diseñado para obtener discretamente su ubicación geográfica y, potencialmente, una fotografía a través de una simulación de transferencia enviada vía plataformas de mensajería. La metodología adoptada fue mixta, de tipo descriptivo y de diseño tecnológico, enfocada en el análisis de la problemática, el levantamiento de requerimientos conceptuales y la validación teórica de la propuesta. Los resultados detallan una arquitectura cliente-servidor robusta y el funcionamiento de los módulos, destacando su potencial para empoderar a la ciudadanía y mejorar la capacidad de respuesta policial, aunque reconociendo los desafíos técnicos y legales. Esta investigación contribuye con un marco novedoso para el uso estratégico de la tecnología en la seguridad ciudadana.

Palabras Clave: Seguridad Ciudadana; Delincuencia Organizada; Babahoyo; Sistema de Reporte; Aplicación Móvil; Extorsión; Inteligencia Policial; TIC.

ABSTRACT

The city of Babahoyo, capital of Los Ríos province, Ecuador, has experienced an alarming increase in organized crime over the last five years, intensifying after the 2020 pandemic. This situation has generated stress, panic, and anxiety among the population, negatively impacting the economic sector with forced business closures due to extortion, kidnappings, and threats. Despite efforts by the National Police, Los Ríos has become the second most violent province in Ecuador. Faced with this problem, the present research proposes the theoretical design of a comprehensive IT system, accessible from mobile devices, that allows citizens to report various types of crimes (kidnapping, contract killing, extortion, threats,

femicide, drug trafficking) and includes advanced functionalities. A key component is an innovative module for interacting with attackers, designed to discreetly obtain their geographic location and, potentially, a photograph through a simulated transfer sent via messaging platforms. The adopted methodology was mixed, descriptive, and technological design-oriented, focused on problem analysis, conceptual requirements gathering, and theoretical validation of the proposal. The results detail a robust client-server architecture and the operation of the modules, highlighting their potential to empower citizens and improve police response capacity, while acknowledging technical and legal challenges. This research contributes a novel framework for the strategic use of technology in citizen security.

Keywords: *Citizen Security; Organized Crime; Babahoyo; Reporting System; Mobile Application; Extortion; Police Intelligence; ICT.*

INTRODUCCIÓN

La creciente preocupación por la seguridad ciudadana es un fenómeno global, pero adquiere una urgencia particular en contextos donde la delincuencia organizada se ha consolidado como un actor disruptivo. Babahoyo, capital de la provincia de Los Ríos en Ecuador, ejemplifica esta problemática con un alarmante incremento de la actividad delictiva en los últimos cinco años. Este recrudecimiento, exacerbado tras la pandemia de 2020, ha sumido a la sociedad en un estado de estrés, pánico y zozobra. La extorsión, el secuestro y las amenazas son prácticas cotidianas que no solo socavan la paz social, sino que también han forzado el cierre de numerosos emprendimientos económicos, impactando negativamente el desarrollo local. A pesar de los esfuerzos de la Policía Nacional y sus grupos especiales, la provincia de Los Ríos ostenta hoy el preocupante título de la segunda más violenta del Ecuador, lo que evidencia la insuficiencia de las estrategias actuales frente a la complejidad del fenómeno.

La delincuencia organizada en entornos urbanos presenta características complejas que requieren enfoques multifacéticos para su contención. Estudios previos, como los de Castells (2000) sobre la sociedad en red y el crimen organizado transnacional, resaltan cómo las estructuras criminales contemporáneas se adaptan y explotan las tecnologías de la información para sus operaciones. A nivel local, la literatura científica sobre la seguridad

ciudadana en Ecuador, si bien aborda la violencia y el crimen, a menudo carece de análisis profundos sobre el impacto específico de la delincuencia organizada en la economía local y la necesidad de herramientas tecnológicas innovadoras para la participación ciudadana en la denuncia. La brecha entre la capacidad de denuncia ciudadana y la respuesta policial efectiva, especialmente en situaciones de coerción, sigue siendo un desafío poco explorado. Esta investigación se asienta en la necesidad de cerrar dicha brecha mediante la innovación tecnológica en el ámbito de la seguridad.

Esta investigación se nutre de varias teorías relevantes en los campos de la criminología, la seguridad de la información y la interacción humano-computadora. Desde la perspectiva criminológica, se consideró la Teoría de las Ventanas Rotas de Wilson y Kelling (1982), que subrayó cómo el desorden y los pequeños delitos no abordados pueden escalar a crímenes más graves, justificando la importancia de la denuncia temprana. Asimismo, la Teoría de la Elección Racional del Delincuente (Cornish y Clarke, 1986) informó sobre cómo los delincuentes sopesan riesgos y beneficios, sugiriendo que un sistema que incremente el riesgo de ser capturado puede disuadir la

actividad criminal. En el ámbito tecnológico, la investigación se apoyó en los principios de Criptografía y Seguridad de la Información (Stallings, 2021) para asegurar la integridad y confidencialidad de los datos de los usuarios. La Teoría de la Usabilidad (Nielsen, 1993) fue crucial para el diseño de la interfaz de la aplicación móvil, garantizando que fuera intuitiva y funcional incluso bajo condiciones de

estrés. Finalmente, la Teoría de Redes Sociales (Wasserman y Faust, 1994) fue pertinente para comprender cómo la información puede fluir y ser explotada en la interacción con actores criminales a través de plataformas digitales, sentando las bases para el diseño del módulo de recolección de inteligencia.

Según (Linares et al., 2023) estos sistemas son sumamente importantes ya que son fundamentales para garantizar un almacenamiento organizado, tener una buena consistencia de datos, acceso concurrente, seguridad y apoyo a la toma de decisiones en las organizaciones.

Dada la naturaleza del presente estudio, que fue un diseño teórico de un sistema informático y no una implementación empírica completa con pruebas de campo extendidas, no se trabajó

con una población o muestra en el sentido estadístico tradicional para la recolección masiva de datos cuantitativos directos de usuarios finales.

Sin embargo, para el levantamiento de requerimientos y la validación conceptual, la investigación consideró de manera cualitativa a los siguientes grupos clave como informantes y expertos:

- Ciudadanos de Babahoyo: Personas afectadas directa o indirectamente por la delincuencia, cuyas necesidades y experiencias fueron el fundamento para el diseño de las funcionalidades de la aplicación móvil. La información se obtuvo a través de la revisión de informes locales y la comprensión de la problemática reportada en medios.
- Personal de la Policía Nacional (Provincia de Los Ríos): Miembros de las fuerzas del orden, incluyendo personal operativo y de inteligencia, cuyas perspectivas fueron cruciales para definir las funcionalidades del panel de control policial y los requisitos para la recolección de inteligencia. La información se obtuvo a través de análisis de reportes de prensa y conocimiento general sobre las operaciones policiales en la zona.
- Expertos en Seguridad y Tecnología: Profesionales con conocimiento en ciberseguridad, desarrollo de software y legislación ecuatoriana, quienes actuaron como validadores conceptuales del diseño propuesto, especialmente en lo referente al módulo de interacción con atacantes.

METODOLOGÍA

La creciente preocupación por la seguridad ciudadana es un fenómeno global, pero adquiere una urgencia particular en contextos donde la delincuencia organizada se ha consolidado como un actor disruptivo. Babahoyo, capital de la provincia de Los Ríos en Ecuador, ejemplifica esta problemática con un alarmante incremento de la actividad delictiva en los últimos cinco años. Este recrudecimiento, exacerbado tras la pandemia de 2020, ha sumido a la sociedad en un estado de estrés, pánico y zozobra. La extorsión, el secuestro y las amenazas son prácticas cotidianas que no solo socavan la paz social, sino que también han forzado el cierre de numerosos emprendimientos económicos, impactando negativamente el desarrollo local. A pesar de los esfuerzos de la Policía Nacional y sus grupos especiales, la provincia de Los Ríos ostenta hoy el preocupante título de la segunda

más violenta del Ecuador, lo que evidencia la insuficiencia de las estrategias actuales frente a la complejidad del fenómeno.

DESARROLLO

La delincuencia organizada en entornos urbanos presenta características complejas que requieren enfoques multifacéticos para su contención. Estudios previos, como los de Castells (2000) sobre la sociedad en red y el crimen organizado transnacional, resaltan cómo las estructuras criminales contemporáneas se adaptan y explotan las tecnologías de la información para sus operaciones. A nivel local, la literatura científica sobre la seguridad ciudadana en Ecuador, si bien aborda la violencia y el crimen, a menudo carece de análisis profundos sobre el impacto específico de la delincuencia organizada en la economía local y la necesidad de herramientas tecnológicas innovadoras para la participación ciudadana en la denuncia. La brecha entre la capacidad de denuncia ciudadana y la respuesta policial efectiva, especialmente en situaciones de coerción, sigue siendo un desafío poco explorado. Esta investigación se asienta en la necesidad de cerrar dicha brecha mediante la innovación tecnológica en el ámbito de la seguridad.

Esta investigación se nutre de varias teorías relevantes en los campos de la criminología, la seguridad de la información y la interacción humano-computadora. Desde la perspectiva criminológica, se consideró la Teoría de las Ventanas Rotas de Wilson y Kelling (1982), que subrayó cómo el desorden y los pequeños delitos no abordados pueden escalar a crímenes más graves, justificando la importancia de la denuncia temprana. Asimismo, la Teoría de la Elección Racional del Delincuente (Cornish y Clarke, 1986) informó sobre cómo los delincuentes sopesan riesgos y beneficios, sugiriendo que un sistema que incremente el riesgo de ser capturado puede disuadir la actividad criminal. En el ámbito tecnológico, la investigación se apoyó en los principios de Criptografía y Seguridad de la Información (Stallings, 2021) para asegurar la integridad y confidencialidad de los datos de los usuarios. La Teoría de la Usabilidad (Nielsen, 1993) fue crucial para el diseño de la interfaz de la aplicación móvil, garantizando que fuera intuitiva y funcional incluso bajo condiciones de estrés. Finalmente, la Teoría de Redes Sociales (Wasserman y Faust, 1994) fue pertinente para comprender cómo la información

puede fluir y ser explotada en la interacción con actores criminales a través de plataformas digitales, sentando las bases para el diseño del módulo de recolección de inteligencia.

Según (Linares et al., 2023) estos sistemas son sumamente importantes ya que son fundamentales para garantizar un almacenamiento organizado, tener una buena consistencia de datos, acceso concurrente, seguridad y apoyo a la toma de decisiones en las organizaciones.

Población y Muestra

Dada la naturaleza del presente estudio, que fue un diseño teórico de un sistema informático y no una implementación empírica completa con pruebas de campo extendidas, no se trabajó con una población o muestra en el sentido estadístico tradicional para la recolección masiva de datos cuantitativos directos de usuarios finales.

Sin embargo, para el levantamiento de requerimientos y la validación conceptual, la investigación consideró de manera cualitativa a los siguientes grupos clave como informantes y expertos:

- **Ciudadanos de Babahoyo:** Personas afectadas directa o indirectamente por la delincuencia, cuyas necesidades y experiencias fueron el fundamento para el diseño de las funcionalidades de la aplicación móvil. La información se obtuvo a través de la revisión de informes locales y la comprensión de la problemática reportada en medios.

- **Personal de la Policía Nacional (Provincia de Los Ríos):** Miembros de las fuerzas del orden, incluyendo personal operativo y de inteligencia, cuyas perspectivas fueron cruciales para definir las funcionalidades del panel de control policial y los requisitos para la recolección de inteligencia. La información se obtuvo a través de análisis de reportes de prensa y conocimiento general sobre las operaciones policiales en la zona.

- **Expertos en Seguridad y Tecnología:** Profesionales con conocimiento en ciberseguridad, desarrollo de software y legislación ecuatoriana, quienes actuaron como validadores conceptuales del diseño propuesto, especialmente en lo referente al módulo de interacción con atacantes.

Diseño Estadístico y Procedimientos para el Análisis de Datos

Los procedimientos para el análisis de los datos conceptuales y documentales fueron los siguientes:

- **Análisis Cualitativo de Contenido:** Se realizó un análisis sistemático de la información obtenida de la revisión documental y de los antecedentes delictivos. Esto implicó la identificación de patrones, tendencias y categorías relacionadas con las modalidades delictivas, el impacto social y económico, y las necesidades no cubiertas por los sistemas de denuncia actuales.
- **Análisis de Requerimientos Funcionales y No Funcionales:** Se sistematizaron y clasificaron los requisitos para el sistema informático, derivados del análisis de la problemática y de los casos de uso esperados tanto para el ciudadano como para la Policía Nacional.
- **Evaluación de Factibilidad Técnica y Legal:** Se llevó a cabo un análisis de la viabilidad tecnológica para el desarrollo de las funcionalidades más complejas, como el módulo de interacción con atacantes, considerando las limitaciones de los sistemas operativos móviles y las plataformas de mensajería. Paralelamente, se efectuó un análisis preliminar de la concordancia con la legislación ecuatoriana en materia de privacidad y recolección de pruebas.

Para la organización, conceptualización y visualización del diseño del sistema, se utilizaron herramientas de software de productividad y diseño conceptual:

- **Microsoft Office Suite (versiones 2019/365):** Para la redacción del documento, organización de información y creación de tablas y diagramas básicos.
- **Herramientas de Diseño de Prototipos (ej. Figma o Balsamiq Mockups - en su versión de diseño conceptual):** Aunque no se generaron prototipos interactivos funcionales, estas herramientas fueron consideradas y conceptualmente utilizadas para la esquematización de las interfaces de usuario y los flujos de la aplicación móvil y el panel policial.
- **Software de Diagramación (ej. draw.io):** Para la creación de diagramas de arquitectura y flujo de datos que clarificaron la estructura del sistema propuesto.

Diseño de Arquitectura del Sistema.

Se ha definido una arquitectura cliente-servidor robusta y escalable, compuesta por:

- **Aplicación Móvil (App):** Interfaz principal para la ciudadanía, desarrollada para Android e iOS, priorizando la usabilidad y la rapidez en situaciones de emergencia. Incorpora módulos para el registro seguro, reporte categorizado de delitos (secuestro, extorsión, sicariato, amenazas, femicidio, narcotráfico), adjunto de evidencia multimedia y geolocalización automática del incidente.
- **Servidor Backend Central:** Encargado de la recepción, procesamiento, almacenamiento seguro y gestión de los datos. Integra funcionalidades de análisis de datos, generación de alertas y comunicación con el panel policial.
- **Base de Datos Segura:** Fundamental para el almacenamiento cifrado de los reportes y la información sensible, garantizando la confidencialidad y la integridad de los datos.
- **Panel de Control Policial:** Una interfaz web o de escritorio para la Policía Nacional, que ofrece una visualización georreferenciada de los incidentes en tiempo real, herramientas de análisis de patrones delictivos, gestión de casos y asignación de recursos, mejorando la capacidad de respuesta operativa.

Desarrollo del Módulo de Interacción con Atacantes

Uno de los resultados más distintivos es la conceptualización del Módulo de Interacción con Atacantes, diseñado para situaciones de extorsión. Este módulo opera bajo un principio de ingeniería social y recolección pasiva de inteligencia:

- **Simulación de Transferencia Bancaria:** La aplicación genera una imagen que simula una notificación de transferencia bancaria exitosa. Esta imagen, al ser enviada al extorsionador a través de WhatsApp, está diseñada para ser visualmente convincente.

- **Payload Oculto y Recolección de Datos:** La imagen no es un simple archivo estático. Se conceptualiza para contener un script o código que, al ser abierto en el dispositivo del extorsionador, intentaría capturar su ubicación geográfica (GPS) y, si es técnicamente factible y legalmente permitido, tomar una fotografía discreta utilizando la cámara del dispositivo. Esta información sería transmitida de forma silenciosa y cifrada al servidor backend para uso exclusivo de la Policía Nacional.

Fortalecimiento de la Privacidad y Seguridad.

Los resultados del diseño priorizan la seguridad de la información y la privacidad del usuario. Se propone el uso de cifrado de extremo a extremo para todas las comunicaciones y el almacenamiento de datos. Se incluye la opción de reporte anónimo para fomentar la denuncia sin temor a represalias, equilibrando la necesidad de información con la protección del ciudadano.

Contribución a la Estrategia de Seguridad Ciudadana.

El sistema propuesto no solo sirve como una herramienta de denuncia, sino que se posiciona como un componente estratégico para la Policía Nacional. Al centralizar los reportes con geolocalización y permitir la obtención discreta de inteligencia, el sistema facilita la identificación de "puntos calientes" del crimen, la cartografía de redes delictivas y la optimización en la asignación de recursos policiales. Este enfoque proactivo, informado por datos en tiempo real, es crucial para contrarrestar la delincuencia organizada que opera con rapidez y adaptabilidad.

RESULTADOS OBTENIDOS.

La propuesta de diseño de un sistema informático para el reporte de delitos en Babahoyo representa una respuesta innovadora y necesaria a la creciente problemática de la delincuencia organizada en la región. Los resultados obtenidos, enmarcados en una metodología de diseño teórico, demuestran la viabilidad conceptual de un sistema que empodera al ciudadano y potencia la capacidad de inteligencia policial. La arquitectura planteada es coherente con las necesidades actuales de seguridad, que requieren inmediatez, precisión y la capacidad de actuar en entornos digitales (Castells, 2000).

La inclusión del módulo de interacción con atacantes, que simula una transferencia para recolectar datos de ubicación y posible identificación visual, es particularmente notable. Esta funcionalidad se alinea con principios de ingeniería social aplicada a la ciberseguridad, buscando explotar la confianza o el descuido del perpetrador para obtener información valiosa (Stallings, 2021). Su diseño responde directamente a la modalidad de extorsión, una de las más prevalentes y perjudiciales en Babahoyo, que a menudo deja a las víctimas sin opciones de respuesta segura. La capacidad de obtener inteligencia encubierta de esta manera podría ser un cambio de juego en la desarticulación de redes extorsivas, ofreciendo a las autoridades una herramienta que complementa los métodos tradicionales de investigación.

Sin embargo, la implementación de un módulo con tales capacidades no está exenta de desafíos significativos. La viabilidad técnica depende en gran medida de la capacidad de generar un "payload" efectivo que funcione en entornos de mensajería como WhatsApp, los cuales están diseñados para ser seguros y evitar la ejecución de código arbitrario. Esto podría requerir el descubrimiento y explotación de vulnerabilidades, lo cual es éticamente complejo y legalmente delicado, y podría enfrentar contramedidas rápidas por parte de los desarrolladores de las aplicaciones.

Más allá de lo técnico, las implicaciones legales y éticas son críticas. La obtención de datos personales (ubicación, fotografía) sin el consentimiento explícito del individuo, incluso si este es un delincuente, puede colisionar con las leyes de privacidad y los derechos fundamentales, dependiendo de la interpretación de la legislación ecuatoriana. Una implementación futura debería requerir una rigurosa consulta legal y, posiblemente, la creación de un marco normativo específico que ampare este tipo de acciones bajo estrictas condiciones y supervisión judicial. La confianza pública en el sistema dependerá directamente de la transparencia y la legalidad con la que se manejen estas funcionalidades. La justificación de un sistema robusto es clara, como lo evidencia el deterioro de la seguridad en Babahoyo y la provincia de Los Ríos. La Teoría de las Ventanas Rotas (Wilson & Kelling, 1982) sugiere que abordar los delitos menores y mantener el orden puede prevenir crímenes mayores. Un sistema de reporte eficiente podría facilitar esta acción temprana. Asimismo, desde la perspectiva de la elección racional del delincuente (Cornish

& Clarke, 1986), un mayor riesgo de identificación y captura, como el que podría ofrecer este sistema, debería disuadir la actividad criminal.

Finalmente, la relevancia del sistema trasciende la mera denuncia. Al proporcionar datos georreferenciados y en tiempo real, permite a la Policía Nacional una gestión de la información más estratégica, facilitando el mapeo de patrones delictivos y la optimización en la asignación de recursos, lo que es esencial para una respuesta efectiva contra el crimen organizado, que opera de forma distribuida y adaptativa (Wasserman & Faust, 1994).

Los procedimientos para el análisis de los datos conceptuales y documentales fueron los siguientes:

- **Análisis Cualitativo de Contenido:** Se realizó un análisis sistemático de la información obtenida de la revisión documental y de los antecedentes delictivos. Esto implicó la identificación de patrones, tendencias y categorías relacionadas con las modalidades delictivas, el impacto social y económico, y las necesidades no cubiertas por los sistemas de denuncia actuales.
- **Análisis de Requerimientos Funcionales y No Funcionales:** Se sistematizaron y clasificaron los requisitos para el sistema informático, derivados del análisis de la problemática y de los casos de uso esperados tanto para el ciudadano como para la Policía Nacional.
- **Evaluación de Factibilidad Técnica y Legal:** Se llevó a cabo un análisis de la viabilidad tecnológica para el desarrollo de las funcionalidades más complejas, como el módulo de interacción con atacantes, considerando las limitaciones de los sistemas operativos móviles y las plataformas de mensajería. Paralelamente, se efectuó un análisis preliminar de la concordancia con la legislación ecuatoriana en materia de privacidad y recolección de pruebas.

Para la organización, conceptualización y visualización del diseño del sistema, se utilizaron herramientas de software de productividad y diseño conceptual:

- **Microsoft Office Suite (versiones 2019/365):** Para la redacción del documento, organización de información y creación de tablas y diagramas básicos.
- **Herramientas de Diseño de Prototipos (ej. Figma o Balsamiq Mockups - en su versión de diseño conceptual):** Aunque no se generaron prototipos interactivos funcionales, estas

herramientas fueron consideradas y conceptualmente utilizadas para la esquematización de las interfaces de usuario y los flujos de la aplicación móvil y el panel policial.

- Software de Diagramación (ej. draw.io): Para la creación de diagramas de arquitectura y flujo de datos que clarificaron la estructura del sistema propuesto.

Diseño de Arquitectura del Sistema.

Se ha definido una arquitectura cliente-servidor robusta y escalable, compuesta por:

- Aplicación Móvil (App): Interfaz principal para la ciudadanía, desarrollada para Android e iOS, priorizando la usabilidad y la rapidez en situaciones de emergencia. Incorpora módulos para el registro seguro, reporte categorizado de delitos (secuestro, extorsión, sicariato, amenazas, femicidio, narcotráfico), adjunto de evidencia multimedia y geolocalización automática del incidente.
- Servidor Backend Central: Encargado de la recepción, procesamiento, almacenamiento seguro y gestión de los datos. Integra funcionalidades de análisis de datos, generación de alertas y comunicación con el panel policial.
- Base de Datos Segura: Fundamental para el almacenamiento cifrado de los reportes y la información sensible, garantizando la confidencialidad y la integridad de los datos.
- Panel de Control Policial: Una interfaz web o de escritorio para la Policía Nacional, que ofrece una visualización georreferenciada de los incidentes en tiempo real, herramientas de análisis de patrones delictivos, gestión de casos y asignación de recursos, mejorando la capacidad de respuesta operativa.

Desarrollo del Módulo de Interacción con Atacantes

Uno de los resultados más distintivos es la conceptualización del Módulo de Interacción con Atacantes, diseñado para situaciones de extorsión. Este módulo opera bajo un principio de ingeniería social y recolección pasiva de inteligencia:

- Simulación de Transferencia Bancaria: La aplicación genera una imagen que simula una notificación de transferencia bancaria exitosa. Esta imagen, al ser enviada al extorsionador a través de WhatsApp, está diseñada para ser visualmente convincente.
- Payload Oculto y Recolección de Datos: La imagen no es un simple archivo estático. Se conceptualiza para contener un script o código que, al ser abierto en el dispositivo del extorsionador, intentaría capturar su ubicación geográfica (GPS) y, si es técnicamente

factible y legalmente permitido, tomar una fotografía discreta utilizando la cámara del dispositivo. Esta información sería transmitida de forma silenciosa y cifrada al servidor backend para uso exclusivo de la Policía Nacional.

Fortalecimiento de la Privacidad y Seguridad.

Los resultados del diseño priorizan la seguridad de la información y la privacidad del usuario. Se propone el uso de cifrado de extremo a extremo para todas las comunicaciones y el almacenamiento de datos. Se incluye la opción de reporte anónimo para fomentar la denuncia sin temor a represalias, equilibrando la necesidad de información con la protección del ciudadano.

Contribución a la Estrategia de Seguridad Ciudadana.

El sistema propuesto no solo sirve como una herramienta de denuncia, sino que se posiciona como un componente estratégico para la Policía Nacional. Al centralizar los reportes con geolocalización y permitir la obtención discreta de inteligencia, el sistema facilita la identificación de "puntos calientes" del crimen, la cartografía de redes delictivas y la optimización en la asignación de recursos policiales. Este enfoque proactivo, informado por datos en tiempo real, es crucial para contrarrestar la delincuencia organizada que opera con rapidez y adaptabilidad.

CONCLUSIONES

La investigación ha logrado establecer una estructura teórica viable y altamente pertinente para un sistema informático de reporte de delitos que puede transformar la lucha contra la delincuencia organizada en Babahoyo y, potencialmente, en otras regiones afectadas de Ecuador. Las principales conclusiones son:

Necesidad Imperante de Herramientas Tecnológicas: La escalada de la delincuencia organizada en Babahoyo demanda soluciones innovadoras que trasciendan los métodos tradicionales de denuncia. La propuesta de una aplicación móvil integral responde directamente a esta urgencia, empoderando a la ciudadanía como actor clave en la seguridad.

Innovación en Recolección de Inteligencia: El módulo de interacción con atacantes, aunque complejo en su implementación técnica y legal, representa una ruptura paradigmática en la forma en que las víctimas pueden contribuir a la inteligencia policial. Su potencial para

obtener ubicación y, posiblemente, identificación visual de extorsionadores sin alertarlos, ofrece una ventaja estratégica crucial para las autoridades.

Fortalecimiento de la Colaboración Ciudadano-Policía: El sistema está diseñado para cerrar la brecha entre el ciudadano y la fuerza policial. Al simplificar el proceso de denuncia y garantizar la confidencialidad, se espera un aumento en el número y la calidad de los reportes, lo que a su vez proporciona a la policía una visión más clara y completa del panorama delictivo.

Desafíos Técnicos y Legales: Si bien el diseño teórico es prometedor, la implementación del módulo de "trampa" requiere una investigación y desarrollo profundo en ciberseguridad, así como una rigurosa validación legal para asegurar su conformidad con la legislación ecuatoriana y el respeto a los derechos fundamentales. La viabilidad de estas funcionalidades avanzadas dependerá de la evolución tecnológica y el marco jurídico.

Potencial de Impacto Socioeconómico: Al ofrecer una herramienta que infunde mayor seguridad y permite actuar frente a amenazas como la extorsión, el sistema tiene el potencial de mitigar el impacto negativo en el sector económico local, reduciendo los cierres de negocios y el estado de pánico generalizado, contribuyendo así a la recuperación y estabilidad de la comunidad.

en definitiva, este estudio conceptualiza una solución tecnológica avanzada que, de ser implementada, podría no solo mejorar significativamente la seguridad ciudadana en Babahoyo sino también establecer un modelo para la participación ciudadana activa y tecnológica en la lucha contra el crimen organizado en Ecuador.

REFERENCIAS BIBLIOGRÁFICAS

- Castells, M. (2000). *La era de la información: Economía, sociedad y cultura*. Vol. I: La sociedad Red. Siglo XXI Editores.
- Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice perspectives on Offending*. Springer-Verlag.
- Nielsen, J. (1993). *Usability Engineering*. Morgan Kaufmann.



Stallings, W. (2021). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

Wilson, J. Q., & Kelling, G. L. (1982). Broken Windows. *The Atlantic*, 249(3), 29-38.