Diseño de un Sistema de Seguridad de la Información Utilizando Tecnologías de Reconocimiento Facial y Dactilar para la Autenticación y Protección de Datos Personales, Mitigando los Fraudes en Entidades Públicas de Colombia

Ibonnet Luisa Fernanda Forero Santana

Asesor

Mgtr. Mariano Esteban Romero Torres

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Básicas Tecnología e Ingeniera ECBTI

Maestría en Gestión de Tecnología de Información

2025

Agradecimientos

Especial y cordial saludo a Mg. Mariano Esteban Romero, por motivarme a sacar este proyecto adelante, por su enseñanza y dedicación para la culminación de un gran esfuerzo; como también a aquellas personas que me orientaron en el camino, entre ellos a mis compañeros que fueron apoyo y energía constante en cada semestre, lo que ayudó a enfocarme para el desarrollo de este trabajo.

Dedicatoria

Especialmente a Dios, por los esfuerzos e impulsos que me animó día a día en la construcción de este trabajo; a mi abuela que desde el cielo me acompaña y siempre oró para que me fuera bien en la vida, a mi hijo para enseñarle que por más difícil que sea el camino se debe persistir hasta lograrlo, a mi madre por el empuje que me ha dado en la vida y a mi compañero de vida que fue el artífice de que estudiara esta Maestría porque solo a través de sus ojos he podido ver el mundo de manera diferente.

Resumen

Una de las principales problemáticas que atraviesan las entidades que cumplen funciones de servicio a la ciudadanía, se debe a la seguridad en los servicios digitales del sector público colombiano, agravando las vulnerabilidades sistémicas en las transacciones, afectando gravemente la confianza ciudadana en el Estado y la perdida reputacional. Por ende el objetivo principal del diseño de un sistema conceptual de seguridad de información, basado en tecnologías biométricas para la autenticación de los ciudadanos y la mitigación de fraudes en entidades públicas de Colombia, hace necesario un enfoque de investigación mixto (cualitativo y descriptivo) con un diseño no experimental y documental, desarrollado en tres fases secuenciales, desplegando un modelo abstracto basado en tecnologías de autenticación biométrica (facial y dactilar) y Automatización Robótica de Procesos (RPA). Como resultados, se espera que se demuestre la necesidad de tener un ecosistema tecnológico maduro en Colombia, en donde la integración con la tecnología propuesta es técnicamente posible y operativamente escalable y favorable. Se concluye, que es factible el diseño de un sistema conceptual robusto alineado con el contexto colombiano para mitigar el fraude por suplantación en el sector público.

***Palabras claves*:** Seguridad de la información, Autenticación biométrica, Automatización robótica de procesos, Ciberseguridad, Mitigación de fraudes.

Abstract

One of the main problems facing entities that serve citizens is the security of digital services in the Colombian public sector. This exacerbates systemic vulnerabilities in transactions, severely impacting citizen trust in the State, and resulting in reputational loss. Therefore, the main objective of designing a conceptual information security system based on biometric technologies for citizen authentication and fraud mitigation in Colombian public entities requires a mixed research approach (qualitative and descriptive) with a non-experimental and documentary design. This approach is developed in three sequential phases, deploying an abstract model based on biometric authentication technologies (facial and fingerprint) and Robotic Process Automation (RPA). The results are expected to demonstrate the need for a mature technological ecosystem in Colombia, where integration with the proposed technology is technically feasible and operationally scalable and favorable. It is concluded that it is feasible to design a robust conceptual system aligned with the Colombian context to mitigate identity theft fraud in the public sector.

***Keywords*:** Information security, Biometric authentication, Robotic process automation, Cybersecurity, Fraud mitigation.

Tabla de contenido

Listado de Tablas

Introducción

En el marco de la transformación digital de Colombia, la creciente sofisticación de las amenazas cibernéticas presenta un desafío crítico para las entidades públicas. El país ha experimentado un aumento superior al 100% en los intentos de fraude digital entre 2019 y 2023 (Pérez-Martínez, 2023), con la suplantación de identidad como un vector de ataque principal que no solo genera pérdidas económicas, sino que erosiona la confianza ciudadana en las instituciones.

Esta problemática se ve agravada por vulnerabilidades sistémicas identificadas en la Estrategia Nacional de Seguridad Digital, tales como la debilidad institucional y una capacidad insuficiente para mitigar riesgos, lo que deja expuestos los servicios esenciales y la información personal de los colombianos. Ante este escenario, se justifica la necesidad de una intervención tecnológica que fortalezca los mecanismos de seguridad y restaure la confianza.

Esta investigación propone una solución que articula estratégicamente tecnologías maduras: la autenticación biométrica robusta (facial y dactilar) y la automatización de procesos mediante "robots de software" (RPA). Este enfoque es pragmático, ya que no busca crear una infraestructura desde cero, sino aprovechar el ecosistema ya regulado en el país, como los servicios de validación de identidad ofrecidos por la Registraduría Nacional del Estado Civil (RNEC) a través de sus operadores tecnológicos certificados (Bazurto-Mecias et al., 2024).

El alcance de este trabajo, se delimita al diseño de un sistema conceptual, proporcionando un modelo de alto nivel que define la estructura, los componentes y sus interacciones, en lugar de una arquitectura técnica lista para la implementación. El objetivo es, por tanto, un diseño cuyo sistema conceptual para mitigar el fraude por suplantación, proteger los datos sensibles de los ciudadanos y optimizar la eficiencia operativa de las entidades públicas.

El Problema de Investigación

Descripción del Problema

Dentro del día a día de las entidades que brindan servicios a la ciudadanía existen múltiples falencias dentro de los procesos, que hacen cuestionar si son lo suficientemente robustos para la mitigación de robos de información, fraude y delitos económicos irrecuperables; de esta manera, muchos de los trámites que un usuario va a realizar a una entidad pública terminan siendo interceptados por personas que se aprovechan del desconocimiento de la persona o por faltas de garantías de la misma entidad (Rodríguez-Ponce, 2024), lo que se aplica sobre todo al poder ejecutivo. Esto incluye no solo al gobierno, sino también a la administración pública, sus empleados y agentes.

Consecuentemente, la responsabilidad de los empleados públicos es, en rigor, uno de los requisitos de la existencia de un sistema democrático, basado en el respeto a los derechos fundamentales, y del propio Estado de derecho. La responsabilidad de los empleados públicos suele adoptar tres formas diferentes: civil, penal y disciplinaria, que componen la llamada ‘tríada de la responsabilidad” (Otero, 2024, p. 15).

Ahora bien, uno de los mayores problemas con los que cuenta un ciudadano al realizar trámites en las entidades públicas es enfrentarse con lo inexplorado, la falta de acercamiento de la entidad hacia los usuarios y el desconocimiento del deber ser, lo cual hace posible que estén involucradas personas inescrupulosas que se acercan al usuario con engaños de poder ayudarlos, robando información personal de ellos y realizando una fachada de la aplicación que maneja la entidad.

Así, desde tiempo atrás, se vienen presentando robos y fraudes, esto obedece a la pérdida de información pública, y a la falta de cultura o escrúpulos que deben tener las personas; y es que

esto no es reciente, es una cadena por falta de controles y mecanismos que limiten al ladrón a realizar trámites fraudulentos con un único beneficio económico.

Del mismo modo, muchas de estas personas que asisten a las entidades públicas van en búsqueda de soluciones en sus procesos; muchos casos se han reportado en el robo y estafa del dinero como del proceso que nunca se realizó, pues los estafadores no solo cobran por el trámite si no que nunca llegan a realizarlo, ya que no tienen el alcance para hacer lo que prometen.

Es entonces, cuando la desilusión por la pérdida del dinero y el engaño cobran el efecto para buscar una solución rápida, eficaz y eficiente con los procesos de atención al usuario; así, Salinas (2023) indica que los delincuentes financieros han adoptado técnicas cada vez más sofisticadas y tecnológicamente avanzadas, los controles de detección defraudes estándar suelen ser derrotados por estas poderosas estrategias, lo que requiere el uso de estrategias más sofisticadas y especializadas. De esta manera, se plantea desarrollar una propuesta innovadora que ayude tanto a la ciudadanía como a la entidad a controlar y prevenir la estafa de manera abierta a como se ve hoy.

Es crucial, resaltar que las soluciones actuales de seguridad en las entidades públicas no son suficientes para combatir eficazmente el robo de información y el fraude. Los métodos tradicionales de autenticación y control presentan limitaciones en cuanto a su capacidad de adaptarse a las nuevas y sofisticadas técnicas utilizadas por los estafadores, por lo que estas deficiencias incluyen sistemas de verificación que pueden ser falsificados o manipulados con relativa facilidad, así como procedimientos de autenticación basados en datos estáticos que no ofrecen la flexibilidad necesaria para identificar amenazas en tiempo real. Aquí es donde la incorporación de tecnologías avanzadas, como la biometría y la RPA, agregan un valor diferencial.

La RPA, combinada con sistemas de reconocimiento facial y de huellas digitales, proporciona un nivel de seguridad más robusto al permitir un monitoreo constante, análisis de patrones y respuestas automatizadas a posibles fraudes. Un análisis más profundo de estas fallas y la manera en que las tecnologías biométricas y RPA pueden superarlas resulta fundamental para un diseño de un sistema que brinde una protección más completa y eficiente.

De esta manera, la propuesta de integrar la RPA en un sistema de seguridad de la información para el sector público colombiano permite: en primer lugar, fortalecimiento de la confidencialidad: la confidencialidad busca prevenir la divulgación no autorizada de información. En el sector público, esto es crucial para proteger los datos personales de los ciudadanos, especialmente los datos sensibles, cuyo tratamiento está estrictamente regulado por la Ley 1581 de 2012. La combinación de biometría y RPA refuerza este principio de las siguientes maneras: control de acceso basado en identidad inequívoca, minimización de la exposición humana a datos sensibles y gestión segura de la interacción (Mecías et al., 2024).

En segundo lugar, garantía de la integridad: la integridad se refiere a la exactitud y completitud de la información, así como a la protección contra su modificación no autorizada. Las vulnerabilidades en las entidades públicas colombianas a menudo se deben a procesos manuales propensos a errores y a la falta de controles de validación robustos. La RPA aborda directamente estos desafíos: eliminación de errores en la entrada y procesamiento de datos, validación automatizada y cruzada y trazabilidad y pistas de auditoría inmutables (Mecías et al., 2024).

Por último, aseguramiento de la disponibilidad: la disponibilidad garantiza que los usuarios autorizados tengan acceso a la información y a los servicios cuando lo requieran. La sobrecarga de los canales de atención, los horarios de oficina limitados y los procesos manuales

ineficientes son barreras comunes para la disponibilidad en el sector público. La RPA, combinada con la biometría, mejora la disponibilidad de forma sustancial, de acuerdo con la visión de Kuehl (2009):

- Operación Continua 24/7: A diferencia de los funcionarios humanos, los robots de software (tanto RPA como chatbots) pueden operar de manera ininterrumpida, 24 horas al día, 7 días a la semana.
- Escalabilidad y Gestión de la Demanda: Los sistemas automatizados pueden gestionar un gran volumen de solicitudes simultáneas sin degradar el rendimiento. Durante picos de demanda (por ejemplo, al abrir una convocatoria de subsidios), los chatbots pueden atender a miles de usuarios a la vez.
- Optimización de Recursos Humanos: Al automatizar tareas repetitivas y consultas frecuentes, la RPA libera al personal humano para que se concentre en casos más complejos que requieren juicio crítico y empatía. Esto no solo mejora la eficiencia, sino que también aumenta la disponibilidad de personal experto para atender las necesidades ciudadanas que la automatización no puede resolver, optimizando la prestación del servicio en su conjunto.

En síntesis, la integración de la RPA con la autenticación biométrica no es una solución genérica, sino un enfoque estratégico que fortalece de manera específica y medible cada componente de la tríada CID. Asegura que el acceso sea confidencial al verificar rigurosamente la identidad y minimizar la exposición de datos; garantiza la integridad al eliminar errores humanos y crear registros inmutables; y mejora la disponibilidad al ofrecer servicios escalables y continuos.

Formulación del Problema

Por lo que de acuerdo con el análisis realizado anteriormente parte la siguiente pregunta:

¿De qué manera se puede diseñar un sistema conceptual que integre tecnologías de autenticación biométrica (facial y dactilar) y Automatización Robótica de Procesos (RPA) para mitigar eficazmente los riesgos de suplantación y proteger la información de los ciudadanos, asegurando al mismo tiempo la viabilidad técnica, jurídica y operativa dentro del contexto nacional?

Sistematización del Problema

De acuerdo con la pregunta problema planteado de investigación, surgen las siguientes sub preguntas que le darán respuesta:

¿Cuáles son las principales tipologías de fraude (como la suplantación de identidad) y las vulnerabilidades críticas de seguridad de la información que afectan la prestación de servicios al ciudadano en las entidades públicas de Colombia?

¿Bajo qué condiciones técnicas, jurídicas (conforme a la Ley 1581 de 2012) y operativas es viable integrar un sistema de autenticación biométrica con los servicios de la Registraduría Nacional del Estado Civil para su uso en el sector público?

¿Cómo se puede estructurar un modelo conceptual que articule la autenticación biométrica con la Automatización Robótica de Procesos (RPA) para crear un flujo de servicio seguro y eficiente en trámites críticos de atención al ciudadano?

Objetivos

Objetivo General

Diseño de un sistema conceptual de seguridad de la información basado en tecnologías biométricas de reconocimiento facial y dactilar, para la autenticación de los ciudadanos y la
mitigación de fraudes en entidades públicas de Colombia.

Objetivos Específicos

Diagnosticar el ecosistema de fraude y las vulnerabilidades de seguridad de la información en la prestación de servicios al ciudadano por parte de entidades públicas en Colombia.

Evaluar la viabilidad técnica, jurídica y operativa de integrar un sistema de autenticación biométrica con los servicios de la Registraduría Nacional del Estado Civil, en el marco de la Ley 1581 de 2012 y las políticas de seguridad digital vigentes.

Delinear el modelo conceptual de un sistema de seguridad integrado que articule los servicios de autenticación biométrica con la Automatización Robótica de Procesos (RPA) para la validación de la identidad y la optimización de trámites críticos de atención al ciudadano.

Justificación

La transformación digital en Colombia ha traído consigo una paradoja: a medida que los servicios se vuelven más accesibles, también aumenta la exposición de los ciudadanos y las instituciones a amenazas cibernéticas cada vez más sofisticadas. El país enfrenta un panorama crítico de seguridad digital, evidenciado por un crecimiento superior al 100% en el volumen de sospechas de fraude digital entre 2019 y 2023. Informes recientes indican que el 40% de los consumidores colombianos fueron objeto de intentos de fraude a través de canales digitales en los últimos meses de 2023, lo que subraya la magnitud del riesgo.

Esta problemática, es especialmente aguda en el sector público. La Estrategia Nacional de Seguridad Digital 2025-2027 del propio gobierno colombiano diagnostica desafíos estructurales que facilitan el fraude, tales como la "debilidad institucional", la "falta de coordinación efectiva" entre entidades y una "insuficiente capacidad para identificar, evaluar y mitigar riesgos cibernéticos". Estas vulnerabilidades sistémicas, son explotadas para cometer delitos como la suplantación de identidad en trámites críticos, el desvío de recursos a través de "beneficiarios fantasmas" y el acceso no autorizado a información sensible de los ciudadanos.

En este sentido, el impacto de esta situación trasciende las pérdidas económicas. Se produce una erosión sistemática de la confianza pública, un activo intangible pero fundamental para la gobernabilidad. Cuando los ciudadanos perciben que los canales oficiales son inseguros o ineficientes, se ven orillados a recurrir a intermediarios informales o "tramitadores", lo que no solo los expone a mayores riesgos de estafa, sino que también perpetúa un ciclo de corrupción y deslegitimación institucional. Por lo tanto, la necesidad de una intervención que fortalezca la seguridad y la confianza en los servicios digitales del Estado no es solo una necesidad técnica, sino un imperativo social.

Frente a esta problemática, la presente investigación propone el diseño de un sistema conceptual de seguridad de la información. El aporte fundamental de este trabajo no radica en la invención de una tecnología aislada, sino en la articulación estratégica e innovadora de tecnologías existentes para crear una solución integral y adaptada al contexto colombiano. La contribución se puede desglosar en tres dimensiones clave:

- Contribución Tecnológica: La innovación principal no es el uso de la biometría o la RPA por separado, sino el diseño de un modelo conceptual que integra tres componentes:
- Autenticación Biométrica Robusta: Utilizando tecnologías de reconocimiento facial y dactilar para una verificación de identidad inequívoca.
- Infraestructura de Confianza Existente: Apalancándose en los servicios de validación de identidad ya regulados y ofrecidos por la Registraduría Nacional del Estado Civil (RNEC) a través de sus operadores tecnológicos certificados.

Del mismo modo, este trabajo resulta relevante debido a la Automatización Robótica de Procesos (RPA): empleando "robots de software" para ejecutar de manera segura y eficiente las tareas administrativas después de una autenticación exitosa, minimizando el error humano y la exposición de datos sensibles. El valor diferencial reside en proponer un flujo de servicio seguro de extremo a extremo: el ciudadano se autentica de forma segura con biometría, y un robot de software completa el trámite en el back-end sin intervención humana vulnerable, garantizando la confidencialidad e integridad del proceso.

En cuanto a la contribución social, al mitigar el fraude por suplantación, el sistema protege directamente el patrimonio y la información personal de los ciudadanos. Esto contribuye a restaurar la confianza en las instituciones públicas, fomenta la inclusión digital al ofrecer

canales más seguros y accesibles, y fortalece el ejercicio de los derechos ciudadanos en un entorno digital protegido bajo los principios de la Ley 1581 de 2012.

Igualmente, el estudio contribuye a la contribución institucional: el proyecto ofrecerá a las entidades públicas un modelo conceptual replicable para modernizar sus servicios, mejorar su eficiencia operativa y cumplir con los objetivos de la política nacional de transformación y seguridad digital.

Del mismo modo, en cuanto a la viabilidad del proyecto, la factibilidad de esta investigación se sustenta en un enfoque pragmático que aprovecha el ecosistema tecnológico y regulatorio existente en Colombia, en lugar de proponer desarrollos desde cero. Viabilidad Técnica y Operativa: El proyecto es viable porque no pretende construir una nueva base de datos biométrica ni desarrollar un conector a la Registraduría. En su lugar, se basa en la evaluación y selección de los servicios ya ofrecidos por operadores biométricos certificados por la RNEC, como BTC, SecurID y Certicámara, que ya prestan este servicio a sectores como el financiero, notarial y de salud.

Por lo tanto, la exitosa implementación y operación a gran escala de la autenticación biométrica por parte de la banca colombiana, en alianza con la RNEC desde 2016 y con pruebas piloto de reconocimiento facial culminadas con éxito, sirve como un caso de estudio y prueba de concepto a nivel nacional, demostrando que la integración es técnicamente posible y operativamente escalable.

En cuanto a la viabilidad jurídica, la investigación reconoce la sensibilidad del tratamiento de datos biométricos y, por ello, uno de sus objetivos específicos es evaluar el marco legal. El proyecto se desarrollará en estricto cumplimiento de la Ley 1581 de 2012 y la jurisprudencia de la Superintendencia de Industria y Comercio (SIC). Se analizarán precedentes,

como la sanción impuesta a Mercado Libre por el uso obligatorio del reconocimiento facial, para asegurar que el modelo conceptual propuesto incorpore por diseño los principios de consentimiento informado, finalidad explícita y la existencia de mecanismos de autenticación alternativos, garantizando así su legalidad.

Con relación a la viabilidad de recursos, al tratarse de una investigación que culmina con un diseño conceptual, los recursos necesarios son principalmente de carácter académico e intelectual (acceso a bases de datos documentales, análisis de normativas, estudio de casos), y no requieren de un presupuesto significativo para desarrollo de software o implementación de pilotos físicos. El alcance está deliberadamente acotado para ser ejecutable en el tiempo y con los recursos disponibles en un marco investigativo.

En cuanto a la delimitación del alcance y enfoque estructurado, para superar la dispersión de argumentos, esta justificación se enmarca en un enfoque metodológico claro y secuencial, derivado directamente de los objetivos específicos. El alcance del trabajo está claramente delimitado: el resultado final no será un software funcional, sino un modelo conceptual detallado. Este modelo definirá los componentes del sistema, sus funciones, las interacciones entre ellos y los flujos de proceso para casos de uso críticos. La investigación seguirá una estructura lógica en tres fases:

- Fase de Diagnóstico: Se identificarán y categorizarán las vulnerabilidades y tipologías de fraude específicas del sector público colombiano, utilizando fuentes oficiales y reportes de la industria.
- Fase de Evaluación: Se analizará la oferta de los operadores biométricos certificados y se evaluará la viabilidad de su integración bajo el marco técnico y legal colombiano.

- Fase de Diseño Conceptual: Se sintetizarán los hallazgos de las fases anteriores para construir el modelo conceptual del sistema integrado, demostrando cómo la articulación de biometría y RPA responde directamente al problema diagnosticado.

Alcance y Delimitación

Alcance

La presente investigación tiene como alcance fundamental el diseño de un sistema conceptual que articula tecnologías de autenticación biométrica (facial y dactilar) y
Automatización Robótica de Procesos (RPA) para fortalecer la seguridad en la prestación de servicios al ciudadano en entidades públicas de Colombia.

Se aclara explícitamente que el resultado final de este trabajo no será un software funcional ni un prototipo implementado, sino un modelo conceptual detallado. Este modelo, como entregable principal de la investigación, comprenderá:

- La definición de la arquitectura lógica del sistema, identificando sus componentes clave (ej. módulo de captura, middleware de integración, motor de RPA).
- La descripción de las funciones e interacciones entre dichos componentes.
- El modelado de los flujos de proceso que ilustran cómo el sistema operaría en casos de uso críticos, como la solicitud de un certificado o la validación de identidad para un trámite.
- Las consideraciones técnicas, jurídicas y operativas que deben tenerse en cuenta para una futura implementación, basadas en los hallazgos de la investigación.

Delimitación

Para garantizar la claridad y viabilidad del proyecto, se establecen las siguientes delimitaciones explícitas:

- Delimitación Conceptual: El estudio se centra en la mitigación de fraudes por suplantación de identidad en el contexto de los servicios al ciudadano ofrecidos por

entidades públicas en Colombia. Se delimita el concepto de "RPA" a la Automatización

- Robótica de Procesos (RPA) en el ámbito del software, excluyendo explícitamente la RPA física o hardware industrial.
- Delimitación Temporal y Geográfica: El análisis de la problemática, las tecnologías y el marco normativo se circunscribe al contexto colombiano durante el periodo comprendido entre 2023 y 2025.
- Delimitación Técnica y de Implementación: El proyecto no incluye las siguientes actividades:
  - El desarrollo de código fuente o la programación de aplicaciones.
  - La implementación de pruebas piloto funcionales en un entorno real o productivo.
  - La adquisición o configuración de hardware (escáneres, servidores) o licencias de software específicas.
  - La intervención directa o la integración con los sistemas de información de ninguna entidad pública en particular.

Así, el enfoque se mantiene estrictamente en el plano del diseño conceptual, proporcionando un marco de referencia estratégico y metodológico que podría servir de base para futuros proyectos de desarrollo e implementación.

Marco de Referencia

Antecedentes Internacionales

Como guía y sustento de esta propuesta de grado se respaldó en trabajos de investigación que tienen que ver con los temas de estudio tales como los que se mencionan a continuación:

En cuanto al reconocimiento facial, existe un trabajo denominado como “Enhancing facial recognition in surveillance systems through embedded super- resolution” (Gómez Bautista & Calderón Bocanegra, 2024), en este estudio, el objetivo principal fue destacar la importancia del diseño y desarrollo de red neuronal para mejorar la resolución de lasimágenes, implementándola en sistemas de vigilancia en tiempo real; este se relaciona de manera directa con la investigación actual ya que lo que se propone es un diseño de un sistema de autenticación facial en tiempo real que capte los rasgos físicos de una persona.

En otro artículo, denominado como “Sistema de control de acceso biométrico mediante reconocimiento facial con técnicas de vivacidad” (Rodríguez-Ponce et al., 2024); se detalla el tema de la seguridad ante fraudes utilizando el reconocimiento facial por medio de un sistema denominado como vivacidad, haciéndolo robusto en el control de acceso de la información.

Por otro lado, en el artículo “Riesgos y desafíos vinculados a la asistencia en efectivo mediada por la biometría” (Roda, 2024), se definen los problemas asociados como olsdesafíos que se vinculan a la construcción de medios biométricos tales como la integración de los mismos sistemas que puede considerarse en la asistencia que pueda tener el usuario a la hora de agregar los datos. Esto permite, que se revisen los riesgos que pueden surtir en la planeación del diseño a la hora de efectuar la implementación y cómo prevenirlos creando mecanismos que permitan la mitigación anticipada de daños o fugas de información dentro de la misma estrategia.

Por último, se menciona un artículo de investigación denominada como “Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil” (Huacho, 2024), que se realizó como estudio del proyecto a una universidad en donde el acceso al área administrativa desean implementarlo por medio del reconocimiento facial del personal laborante.

Para ello, realizaron una encuesta de aceptación y la recopilación de datos del usuario para robustecer la seguridad de la información y acceso por medio de un sistema; este artículo constituye un aporte relevante ya que se requiere de un diseño de sistema de autenticación por medio de un sistema de reconocimiento facial para abrir el trámite del ciudadano que visita la entidad, lo que brinda una orientación mucho más cercana.

Seguridad Cibernética y Riesgos Digitales

El entorno cibernético ha evolucionado rápidamente, generando un aumento significativo en la frecuencia y sofisticación de los ataques cibernéticos. Mapas de ciber amenazas en tiempo real, como los dispuestos por firmas especializadas como Kaspersky Lab, revelan que, en promedio, alrededor de cien países son víctimas de ataques cibernéticos en menos de un minuto. Esta realidad, subraya la rentabilidad que ofrece la explotación de la información robada, el daño económico que se puede infligir a las empresas y los riesgos asociados con la sustracción de datos personales y corporativos. Además, el ciberespacio facilita el anonimato de los atacantes, lo que complica su trazabilidad y seguimiento (Refsdal et al., 2015; Instituto de Auditores Internos de España, 2016).

El ciberespacio, definido como un entorno no físico sin límites geográficos, conecta sistemas interdependientes y los hace vulnerables a múltiples tipos de amenazas. Según Kuehl (2009), este espacio es un dominio operacional similar a otros como tierra, mar, aire y espacio,

en donde los ataques pueden tener impactos tanto en el mundo físico como en el digital. De acuerdo con la XIX Conferencia de directores de Colegios de Defensa Iberoamericanos (2018), el ciberespacio se considera un escenario estratégico que influye en la seguridad nacional y en la estabilidad económica y política.

Por otro lado, la naturaleza y evolución de los ciberriesgos destacan su creciente peligrosidad y complejidad. El Foro Económico Mundial (2017) señaló que el ciberespacio es uno de los diez principales riesgos globales debido a la Internet de las cosas y la interconexión de personas y dispositivos, lo que crea una ciberdependencia que amplifica la posibilidad de ataques masivos y de efecto dominó.

Limitaciones y Efectividad del Reconocimiento Facial y Control de Acceso en Contextos Similares

A pesar de los avances tecnológicos, tanto el reconocimiento facial como el control de acceso presentan diversas limitaciones que afectan su efectividad en entornos prácticos, especialmente cuando se aplican a sistemas complejos y de alta demanda. Estas limitaciones deben ser analizadas a la luz del contexto específico de la investigación o implementación.

Así, una de las principales limitaciones del reconocimiento facial es la variabilidad de las condiciones en las que se lleva a cabo la captura de imágenes. Factores como la iluminación, la calidad de la cámara y las posiciones del rostro afectan directamente la precisión del sistema.

Según la investigación de Zhang et al. (2017), el rendimiento de los sistemas de reconocimiento facial puede verse significativamente afectado por condiciones ambientales como la iluminación deficiente o los ángulos extremos. Esta vulnerabilidad es especialmente crítica en entornos con múltiples usuarios, como edificios gubernamentales o accesos públicos, en donde las condiciones de captura no siempre son controlables.

Otro desafío importante, está relacionado con los sesgos algorítmicos que afectan la precisión del reconocimiento en diferentes grupos demográficos. Diversos estudios, como el de Buolamwini y Gebru (2018), evidencian que los sistemas de reconocimiento facial tienen un rendimiento inferior al identificar personas de color y mujeres, lo que genera preocupaciones sobre la equidad en su aplicación. Este vacío, puede generar una experiencia desigual en la implementación de la tecnología, especialmente en entornos públicos o corporativos con una base diversa de usuarios.

Antecedentes Nacionales

Los riesgos digitales más comunes incluyen el fraude financiero, el robo de información, la indisponibilidad de servicios, el sabotaje de infraestructuras y la pérdida de reputación. Estos riesgos han experimentado una adaptación tecnológica que permite a los ciberdelincuentes explotar las debilidades de los sistemas de seguridad existentes. La falta de medidas de protección adecuadas y efectivas, combinada con la exposición que ofrece el uso extendido de internet, contribuye a la vulnerabilidad de las organizaciones y entidades gubernamentales (Sack y Ierache, 2015; CAI Virtual de la Policía Nacional, 2019).

De este modo, la RPA y las tecnologías biométricas emergen como soluciones para mitigar estos riesgos, aportando mayor control y precisión en la identificación de amenazas y en la autenticación de usuarios. Sin embargo, se requiere una implementación cuidadosa y adaptada a los contextos específicos para superar los desafíos que los sistemas de seguridad actuales no logran abordar completamente.

De esta manera, los agentes generadores de riesgos externos son aquellos que provienen de terceros ajenos a la propia red o sistema, los cuales logran acceder a información no autorizada, modificar o interferir el funcionamiento de un sistema mediante la explotación de sus

vulnerabilidades. Según Medina (2016), se ha hablado de la "profesionalización del cibercrimen", lo cual se basa en el conocimiento experto de los atacantes.

Este fenómeno, también es respaldado por informes periciales en revistas de la Policía Nacional, que afirman que los ciberdelincuentes cuentan con recursos humanos, técnicos y financieros a su disposición cuando se trata de realizar ataques a entidades gubernamentales (Semana, 2017).

De allí, que el mercado actual está repleto de amenazas capaces de infiltrarse en los sistemas y obtener información. Entre las amenazas más relevantes, se encuentran las siguientes, basadas en un informe presentado por Symantec (2019):

- Ataque de denegación de servicio (DoS): Un intento de hacer que un recurso deje de estar disponible para sus usuarios. El ataque de denegación de servicio distribuido (DDoS) se produce cuando varios atacantes lanzan ataques simultáneos DoS contra un solo objetivo.
- Ataques de inyección de código: Estas técnicas, como la inyección SQL, el cross- site scripting (XSS) y la solicitud de falsificación a través del sitio (CSRF), buscan extraer datos, robar credenciales o tomar el control de servidores web.
- Botnet: Conjunto de ordenadores comprometidos, conocidos como "zombies", que están bajo el control de un atacante. Estos se comunican con el sistema maestro, el cual puede dirigirlos.
- Drive-by Exploits: Este tipo de ataque inyecta código malicioso en el código HTML de sitios web que explotan vulnerabilidades en los navegadores web de los usuarios.
- Exploit kits: Paquetes de software diseñados para automatizar delitos informáticos, descargando código malicioso en sitios web comprometidos.
- Falsos antivirus: Software falso distribuido por ciberdelincuentes para infectar equipos mediante alertas de seguridad falsas.

- Gusanos: Programas maliciosos con capacidad de replicarse y redistribuirse explotando vulnerabilidades de los sistemas de destino.
- Troyanos: Programas maliciosos que se inyectan sigilosamente en los sistemas de los usuarios, permitiendo que un atacante remoto pueda acceder al equipo infectado y robar datos y credenciales.
- Spam: El uso abusivo de correos electrónicos para saturar los buzones de los usuarios con mensajes no solicitados.

De esta manera, la evolución de estas amenazas y sus combinaciones marcó el panorama de los ataques en 2018 y 2019. La aparición de los cryptoworms, un tipo especializado de ransomware que elimina la necesidad del elemento humano, es un ejemplo claro de cómo las amenazas se vuelven cada vez más sofisticadas. Estos worms, mediante campañas de ransomware auto propagadas, se consideran una de las amenazas más peligrosas, con el potencial de desestabilizar toda la infraestructura de la Internet, según los investigadores de amenazas de Cisco. Además, como lo evidenció el malware Nyetya, algunos ataques no solo buscan el lucro, sino también la eliminación de sistemas y la destrucción de datos.

Para entender el panorama de estos ataques, es clave clasificar a los ciberdelincuentes. La empresa Arkavia Networks (2017) ofrece una lista de tipos de hackers, que se dividen en: Black hat: Hackers con malas intenciones que usan sofisticadas técnicas para acceder a sistemas, robar o destruir datos; White hat: Hackers éticos que trabajan en la protección y seguridad de sistemas TI; Grey hat: Hackers que a veces actúan ilegalmente, pero con buenas intenciones, como denunciar a empresas por prácticas no autorizadas de recopilación de datos. Dentro de los black hat, existen perfiles específicos que describen a los ciberdelincuentes según su tipo de ataque y motivación, tales como:

- Carder: Especializados en fraudes con tarjetas de crédito.
- Cracker: Se dedica a penetrar sistemas informáticos con el fin de robar o destruir información valiosa.
- Defacer: Busca vulnerabilidades en páginas web para modificarlas.
- Lammers: Hackers novatos que utilizan herramientas disponibles sin tener

conocimientos profundos.

- Pharmer: Realiza ataques de phishing mediante la creación de sitios web falsos para robar credenciales.
- Phreaker: Tiene conocimientos avanzados en telefonía y puede interceptar llamadas telefónicas sin que los usuarios lo sepan.
- Piratas informáticos: Utilizan software robado para realizar actividades delictivas.
- Script-kiddie: Ciberdelincuentes inexpertos que recopilan herramientas para probar su efectividad en víctimas.
- Spammer y diseminador de spyware: Se dedica a crear spam y publicidad ilegal.
- Trasher: Recoge información secreta a través de la revisión de la basura de una entidad o persona.
- War driver: Hacker que explota vulnerabilidades en redes de conexión móvil.

Estos ciberdelincuentes, se han vuelto expertos en evadir la detección, utilizando herramientas como el cifrado y servicios de nube, además de mecanismos de sandboxing para ejecutar programas sin que causen daño en los sistemas productivos. Este tipo de evasión les permite prolongar su operativa y seguir causando daños.

Aplicabilidad conjunta: Reconocimiento Facial y Control de Acceso

El reconocimiento facial y el control de acceso son tecnologías clave en la seguridad moderna, ampliamente utilizadas en entornos privados y públicos para garantizar la protección de información y el control de la identidad. El reconocimiento facial, como tecnología biométrica, permite identificar o verificar a una persona a partir de su rostro, aplicándose en varios campos. En la seguridad pública, se utiliza para identificar sospechosos en multitudes o en espacios públicos como aeropuertos y estaciones de tren.

En entornos corporativos y gubernamentales, ayuda a controlar el acceso a áreas restringidas, eliminando la necesidad de contraseñas o credenciales físicas que pueden ser robadas u olvidadas. Además, se emplea en el comercio para personalizar la experiencia del cliente y ofrecer publicidad dirigida, analizando patrones de comportamiento. Sin embargo,

presenta desafíos, como la precisión y fiabilidad, que pueden verse afectadas por factores como la iluminación y los ángulos de la cámara, además de los sesgos en las bases de datos de imágenes que afectan a ciertos grupos étnicos o de género. También surgen preocupaciones sobre la privacidad y el uso indebido de los datos faciales, lo que genera debates sobre la regulación de esta tecnología.

Por otro lado, el control de acceso, que restringe la entrada a personas no autorizadas a determinadas áreas o recursos, incluye tecnologías como tarjetas RFID, huellas dactilares y reconocimiento facial. Este tipo de control se implementa tanto en accesos físicos, como en oficinas y edificios gubernamentales, como en el ámbito digital, protegiendo datos sensibles mediante autenticación de dos factores o biometría. Aunque es una herramienta clave para la seguridad, el control de acceso presenta desafíos relacionados con su integración con otros sistemas de seguridad y su costo, que puede ser elevado debido a la instalación y mantenimiento de tecnologías avanzadas.

La combinación del reconocimiento facial con el control de acceso puede crear un sistema de seguridad más robusto, integrando la verificación de identidad tanto en el ámbito físico como digital. Esto es especialmente útil en instituciones gubernamentales o bancarias, donde se necesita garantizar la seguridad de las personas en las instalaciones y, a la vez, controlar su acceso a sistemas informáticos.

Al integrar ambas tecnologías, se mejora la seguridad, ya que se asegura que solo personas autorizadas puedan acceder a áreas restringidas o recursos sensibles, reduciendo los riesgos de suplantación de identidad o ataques cibernéticos. Además, la automatización de estos procesos mejora la eficiencia operativa, minimizando los errores humanos, y su escalabilidad permite adaptar los sistemas a un mayor volumen de usuarios o instalaciones sin perder efectividad.

En conclusión, tanto el reconocimiento facial como el control de acceso son herramientas esenciales en la seguridad moderna, con aplicaciones en diversos sectores. Sin embargo, para

optimizar su uso, es necesario abordar desafíos relacionados con la precisión, el costo y la privacidad. La integración de ambas tecnologías puede proporcionar una solución más completa y eficiente, garantizando un control de acceso robusto y seguro.

Por su parte, los sistemas de control de acceso basados en biometría, como la huella dactilar o el reconocimiento facial, aunque eficaces, no están exentos de limitaciones. En términos de eficacia, los dispositivos biométricos pueden presentar fallos en la autenticación, especialmente si la base de datos está mal gestionada o si los sensores no están correctamente calibrados.

Además, la adopción de sistemas como las tarjetas RFID o los lectores de huellas dactilares puede verse afectada por fallos técnicos o mal funcionamiento de los dispositivos, como lo señala Pérez et al. (2019), quienes destacan que los errores en la lectura de huellas o la pérdida de tarjetas pueden comprometer el acceso seguro.

Así mismo, la implementación de sistemas de control de acceso también enfrenta desafíos relacionados con el costo y la infraestructura necesaria para su despliegue y mantenimiento. De acuerdo con Ortega (2020), los sistemas avanzados de control de acceso, como aquellos basados en biometría o reconocimiento facial, requieren una inversión considerable en términos de instalación, mantenimiento y actualización tecnológica. Esto puede ser una barrera en organizaciones con recursos limitados, como algunas entidades gubernamentales o empresas locales.

Por otra parte, en el contexto de diseño de un sistema de seguridad de la información utilizando tecnologías de reconocimiento facial y dactilar para la autenticación y protección de datos personales, mitigando los fraudes en entidades públicas de Colombia, como se propone en el caso de estudio, la combinación de tecnologías como el reconocimiento facial y el control de acceso presentan tanto oportunidades como desafíos. A nivel de efectividad, la implementación de estas tecnologías en un sistema de acceso a áreas restringidas debe ser cuidadosamente

planificada para mitigar las limitaciones mencionadas anteriormente, como los sesgos en el reconocimiento facial y los errores en la autenticación biométrica.

Por ejemplo, en la Alcaldía de Bogotá, donde se busca implementar un sistema de seguridad de acceso para el personal y la ciudadanía, la precisión del reconocimiento facial podría verse comprometida por la variabilidad de las condiciones de las cámaras de seguridad en diversas zonas del edificio. De acuerdo con Medina (2016), en entornos públicos, la implementación de sistemas de reconocimiento facial requiere un ajuste constante de las condiciones técnicas para asegurar su efectividad.

Aparte, si bien los costos de instalación de sistemas avanzados de control de acceso pueden ser altos, la necesidad de fortalecer la seguridad y mitigar riesgos de fraudes o robo de información hace que la inversión sea necesaria. El sistema debe garantizar que solo las personas autorizadas tengan acceso a áreas sensibles, minimizando los riesgos asociados con el acceso no autorizado, como el espionaje o la filtración de información, como sugiere Pérez (2019).

No obstante, aunque tanto el reconocimiento facial como el control de acceso ofrecen soluciones efectivas para mejorar la seguridad, es fundamental considerar sus limitaciones y ajustarlas al contexto específico de cada implementación. En el caso de las entidades públicas, como la Alcaldía de Bogotá, la implementación debe ser cuidadosamente planificada para superar desafíos relacionados con la precisión de los sistemas y los costos asociados, a la vez que se aseguran la equidad y la protección de la privacidad de los usuarios.

Marco Teórico

La presente investigación, se fundamenta en un marco teórico multidisciplinario que integra principios de ciberseguridad, modelos de gobernanza digital, tecnologías de autenticación y el marco ético-legal que regula el tratamiento de datos en Colombia. Este enfoque permite no solo contextualizar la problemática del fraude en las entidades públicas, sino también sustentar teóricamente la propuesta de un sistema conceptual de seguridad basado en biometría y automatización RPA.

Fundamentos de la Seguridad de la Información: La Tríada CID

Cualquier sistema de seguridad de la información robusto se erige sobre tres pilares fundamentales conocidos como la tríada CID: Confidencialidad, Integridad y Disponibilidad. Este modelo clásico proporciona el marco conceptual para analizar las vulnerabilidades y diseño de controles efectivos.

Confidencialidad: Se refiere a la protección de la información contra la divulgación no autorizada (Refsdal et al., 2015). En el contexto de los servicios al ciudadano, este principio es de máxima importancia, ya que las entidades públicas manejan datos personales, incluyendo datos sensibles, cuyo tratamiento está estrictamente regulado por la Ley 1581 de 2012. Una brecha en la confidencialidad puede derivar en suplantación de identidad, fraudes financieros y la exposición de información privada de los ciudadanos.

Integridad: Garantiza que la información sea exacta, completa y no haya sido modificada de manera no autorizada. La falta de integridad en los sistemas públicos puede manifestarse en la alteración de registros, la creación de "beneficiarios fantasmas" en programas sociales o la manipulación de datos para cometer actos de corrupción (Huacho, 2024); ahora bien, de acuerdo

con Mecias et al. (2024), un sistema seguro debe asegurar que los datos solo puedan ser alterados por usuarios autorizados y que exista una trazabilidad completa de dichos cambios.

Disponibilidad: Según Buolamwini y Gebru (2018), asegura que los usuarios autorizados tengan acceso a la información y a los servicios cuando lo requieran. En el sector público, la falta de disponibilidad se traduce en barreras de acceso para los ciudadanos, largos tiempos de espera y la interrupción de servicios esenciales; por otra parte, Arkavia Networks (2017) señala que la tecnología debe facilitar un acceso continuo y eficiente, operando idealmente para satisfacer las demandas ciudadanas (Refsdal et al., 2015).

La propuesta de esta investigación se evalúa constantemente contra estos tres principios, buscando el diseño de un sistema que fortalezca simultáneamente la confidencialidad del acceso, la integridad de las transacciones y la disponibilidad de los servicios.

Modelo Académico para la Adopción Tecnológica: La Teoría Unificada de Aceptación y Uso de Tecnología (UTAUT)

Para sustentar científicamente el análisis sobre cómo los ciudadanos podrían adoptar el sistema conceptual propuesto, esta investigación incorpora la Teoría Unificada de Aceptación y Uso de Tecnología (UTAUT). Desarrollada por Venkatesh et al. (2003), la UTAUT es un modelo influyente que sintetiza ocho teorías previas sobre la aceptación de tecnología, incluyendo el Modelo de Aceptación de Tecnología (TAM), para ofrecer un marco más holístico y robusto.

Dentro de este contexto, el modelo UTAUT, es particularmente pertinente para este estudio, ya que ha sido ampliamente validado en el contexto de la adopción de servicios de gobierno electrónico (e-government) por parte de los ciudadanos. El modelo postula que la Intención de Comportamiento (Behavioural Intention) de un individuo para usar una tecnología es el principal predictor de su Uso Real (Use Behaviour).

A su vez, esta intención está determinada por cuatro constructos clave, según la visión de Venkatesh et al. (2003):

- Expectativa de Desempeño (Performance Expectancy): Es el grado en que un individuo cree que usar el sistema le ayudará a obtener beneficios en la realización de sus tareas. En el contexto de este proyecto, se refiere a si el ciudadano percibe que el sistema biométrico hará que sus trámites sean más rápidos, seguros y efectivos. Es el predictor más fuerte de la intención de uso.
- Expectativa de Esfuerzo (Effort Expectancy): Es el grado de facilidad asociado con el uso del sistema. Se relaciona con la percepción del ciudadano sobre qué tan intuitiva y sencilla es la interfaz del sistema de autenticación facial y dactilar. Un sistema percibido como complejo disuadirá su adopción.
- Influencia Social (Social Influence): Es el grado en que un individuo percibe que personas importantes para él (familiares, colegas, la sociedad en general) creen que debería usar el nuevo sistema. En el ámbito público, esto puede estar relacionado con la confianza en las instituciones gubernamentales y la percepción general de seguridad y modernidad del Estado.
- Condiciones Facilitadoras (Facilitating Conditions): Es el grado en que un individuo cree que existe una infraestructura organizacional y técnica para soportar el uso del sistema. Esto se conecta directamente con la percepción del ciudadano sobre si el gobierno tiene la capacidad, los recursos y el soporte técnico necesarios para que el sistema funcione de manera fiable.

Además, el modelo UTAUT reconoce que el efecto de estos constructos puede ser moderado por variables demográficas como la edad, el género y la experiencia. Investigaciones

posteriores en el ámbito del e-government han extendido el modelo, añadiendo constructos como la Confianza en el Sistema (Trust of System) y la Seguridad Percibida (Perceived Security),

reconociendo que, en el contexto de los servicios públicos, la confianza en que el gobierno

protegerá los datos es un factor crucial para la adopción (Zhang et al., 2017). La incorporación del modelo UTAUT proporciona a esta investigación un marco científico para analizar no solo los aspectos técnicos de la solución, sino también los factores humanos y sociales que

determinarán su éxito y aceptación por parte de los ciudadanos colombianos.

Estado del Arte y Vulnerabilidades: La Seguridad Digital en el Sector Público Colombiano

A pesar de contar con un marco normativo y políticas públicas como los documentos CONPES sobre seguridad digital, la implementación efectiva en el sector público colombiano enfrenta desafíos significativos. La Estrategia Nacional de Seguridad Digital 2025-2027 ofrece un diagnóstico oficial que evidencia las debilidades existentes y justifica la necesidad de nuevas soluciones.

Debilidades Institucionales y de Gobernanza: La estrategia identifica una "debilidad institucional y la falta de coordinación efectiva" como un obstáculo principal, lo que resulta en una fragmentación de iniciativas y una dispersión de recursos. Esta falta de un enfoque unificado, según Pérez et al. (2019), dificulta la implementación de defensas coherentes contra amenazas cada vez más sofisticadas.

Vulnerabilidades Técnicas y Operativas: El país presenta una "insuficiente capacidad para identificar, evaluar y mitigar riesgos cibernéticos de manera integral". Esto se agrava por la vulnerabilidad de las infraestructuras críticas y de las páginas web del Estado (dominio.gov.co), que a menudo son susceptibles a ataques incluso sin conocimientos técnicos avanzados (Pérez et al., 2019). La lenta capacitación del personal y la falta de liderazgo en TI con conocimientos avanzados en seguridad limitan la capacidad de las organizaciones para protegerse adecuadamente.

Contexto de Amenazas Crecientes: Colombia es un objetivo principal para el ciberdelito

en la región. Durante 2024, el país enfrentó cerca de 36.000 millones de intentos de ciberataques, siendo el segundo más atacado de Latinoamérica. El volumen de sospechas de fraude digital creció un 105% entre 2019 y 2023, y el 40% de los consumidores colombianos reportaron haber sido objeto de intentos de fraude a finales de 2023 (Pérez-Martínez, 2023). Estos datos demuestran que los mecanismos de seguridad actuales son insuficientes para contener la magnitud del problema.

Este panorama, evidencia un vacío crítico entre la política y la práctica, donde las soluciones existentes no logran mitigar los riesgos de manera efectiva. La presente investigación se posiciona en este vacío, proponiendo un modelo conceptual que aborda directamente estas vulnerabilidades diagnosticadas.

Tecnologías de Autenticación Biométrica

La autenticación es la primera línea de defensa de cualquier sistema. Los métodos tradicionales basados en contraseñas han demostrado ser vulnerables. La biometría surge como una alternativa superior al basarse en características fisiológicas o de comportamiento únicas de cada individuo para verificar su identidad.

Arquitectura de un Sistema Biométrico: Un sistema de autenticación biométrica según la visión de Ortega (2020) típicamente se compone de varios módulos: un dispositivo de captura (cámara o escáner de huellas), un sistema de extracción de características que convierte la captura en una plantilla matemática (template), un motor biométrico que realiza la comparación

entre la plantilla en vivo y la almacenada, y un middleware que gestiona la comunicación segura entre los componentes (Otero, 2024).

Estado del Arte en Colombia: La implementación de biometría no es una propuesta teórica en el país. Colombia cuenta con una infraestructura robusta y un ecosistema maduro para la validación de identidad. La Registraduría Nacional del Estado Civil (RNEC) posee la base de datos biométrica oficial y ha certificado a múltiples operadores tecnológicos (como Certicámara, SecurID, BTC) para que ofrezcan servicios de autenticación a entidades públicas y privadas.

Así, el caso de éxito más notable es la alianza entre la RNEC y Asobancaria, que desde 2016 utiliza la biometría dactilar para reducir el fraude por suplantación y que recientemente ha culminado con éxito las pruebas piloto para la autenticación facial en tiempo real (Pérez et al., 2019). Este precedente demuestra la viabilidad técnica y operativa de la propuesta de esta investigación.

Automatización Robótica de Procesos (RPA) en el Sector Público

Para subsanar cualquier ambigüedad, es imperativo clarificar que el término "asistencia de la RPA" utilizado en esta investigación se refiere exclusivamente a la automatización de procesos mediante software, y no a la robótica física. El alcance de este proyecto no contempla el diseño o la implementación de hardware como estaciones físicas, sensores, actuadores o sistemas embebidos. Esta delimitación es crucial para diferenciar la propuesta de otros campos de la robótica, como los programas educativos impulsados por Minciencias (ej. "Colombia Robótica"), cuyo objetivo es el fomento de vocaciones STEAM y no la automatización de servicios gubernamentales.

Por lo tanto, el componente robótico se define como la aplicación de dos tecnologías de software maduras: la Automatización Robótica de Procesos (RPA), que utiliza "robots de

software" para emular tareas humanas en sistemas digitales, y la Inteligencia Artificial Conversacional (chatbots), que automatiza la interacción con los ciudadanos (Otero, 2024).

De allí, que la factibilidad de este componente (software) es alta y se sustenta en su probada eficacia y en precedentes existentes (Zhang et al., 2017). La RPA es una tecnología madura con numerosos casos de uso documentados en el sector público a nivel global para tareas como el procesamiento de solicitudes, la generación de informes y la migración de datos, mejorando la integridad y la disponibilidad de los servicios. Su capacidad para interactuar con sistemas legados a través de la interfaz de usuario la hace particularmente viable para el entorno tecnológico gubernamental (Medina, 2016).

Por su parte, la viabilidad de los chatbots en Colombia es demostrable con ejemplos concretos como "DIANA" de la DIAN y "Candelaria" de la oficina de turismo de Bogotá, que ya operan exitosamente para mejorar la atención al ciudadano. Por ende, la elección de la RPA no es solo una aclaración conceptual, sino una decisión estratégica basada en la viabilidad, los beneficios documentados y los precedentes locales (Foro Económico Mundial, 2017).

La RPA, consiste en el uso de software para emular las acciones de un ser humano interactuando con sistemas digitales para ejecutar un proceso de negocio. En el sector público, la RPA tiene casos de uso documentados para tareas como la validación de documentos, la migración de datos, la generación de informes y el procesamiento de solicitudes. Su implementación impacta directamente en la tríada CID, según la visión de Gómez-Bautista y Calderón-Bocanegra (2024), lo cual se describe en las siguientes líneas.

- Mejora la Integridad: Al automatizar tareas repetitivas, la RPA reduce drásticamente el error humano, asegurando que los datos se procesen de manera consistente y precisa.

- Fortalece la Confidencialidad: Un robot de software puede ser programado para manejar información sensible sin que un funcionario necesite visualizarla, minimizando la exposición de los datos y creando pistas de auditoría inmutables de cada acción realizada.
- Aumenta la Disponibilidad: Los robots pueden operar 24/7, procesando solicitudes y trámites fuera del horario de oficina y gestionando altos volúmenes de transacciones sin fatiga.

Por lo tanto, la articulación de la autenticación biométrica (para verificar quién es el usuario) con la RPA (para ejecutar el proceso de forma segura después de la verificación) es el núcleo innovador de la propuesta de este trabajo.

Marco Ético y Legal: Tratamiento de Datos Biométricos

El uso de datos biométricos, al ser considerados datos personales sensibles según la legislación colombiana, impone obligaciones estrictas y plantea consideraciones éticas ineludibles, lo cual se detalla a continuación.

Regulación principal (Ley 1581 de 2012): esta ley establece el marco general para la protección de datos en Colombia. Su principio fundamental es que se prohíbe el tratamiento de datos sensibles, excepto en casos muy específicos. La ley exige que, para recolectar estos datos, se debe obtener la autorización previa, explícita e informada del titular, y ninguna actividad puede estar condicionada a que el ciudadano suministre datos sensibles.

Excepciones a la autorización: la ley contempla escenarios donde la autorización no es necesaria, como en casos de urgencia médica o sanitaria, para fines históricos o estadísticos (suprimiendo la identidad), o para el reconocimiento o defensa de un derecho en un proceso judicial.

Riesgos éticos y precedentes: el riesgo de un uso indebido de la tecnología de reconocimiento facial es una preocupación global. En Colombia, un precedente clave es la

sanción impuesta por la Superintendencia de Industria y Comercio (SIC) a Mercado Libre por condicionar el acceso de sus usuarios al uso obligatorio del reconocimiento facial. Este caso subraya la importancia de un diseño de sistemas que respeten el derecho a la elección del usuario y ofrezcan siempre alternativas de autenticación no biométricas.

Este marco teórico, demuestra que la propuesta de investigación no solo responde a una necesidad técnica y social claramente identificada en Colombia, sino que también se sustenta en modelos teóricos establecidos, reconoce el estado del arte y las soluciones existentes, y se enmarca rigurosamente dentro de las limitaciones y obligaciones que impone el ordenamiento jurídico y ético del país.

Marco Contextual

Una vez identificado el punto de partida o el foco en donde se evidencia la problemática, que es dentro del diario vivir de la calle a las afueras de las entidades públicas, en donde los ciudadanos acuden y son intervenidos por otras personas que dicen ser conocedoras del tema.

Por lo tanto, en este estudio se analiza cómo se puede mitigar el robo de información, además, que mecanismos son viables para el desarrollo de un sistema que posibilite el resguardo seguro de la información de datos de cada uno de los ciudadanos.

Así, el robo de identidad sucede cuando otra persona obtiene o utiliza información personal de forma no autorizada. Esta acción la realiza con fines fraudulentos o para cometer algún otro delito (Centurión et al., s.f.).

De esta manera, se tiene identificado que el fraude y el robo de información, hace posible la suplantación de identidad y con ello el soborno o estafa, por lo que acudir a mecanismos tecnológicos que ayuden a las entidades a ganar la confianza en el terreno perdido hará que se optimicen mejor los recursos y servicios que se tienen a la ciudadanía.

Por otra parte, en el Articulo de “La ciberdelincuencia y la protección de datos personales”, menciona que la ciberdelincuencia no solo incluye actos de intrusión y robo de datos, sino también la manipulación de información, el sabotaje cibernético y el fraude digital, entre otros. Estas actividades ilícitas no solo comprometen la privacidad de los individuos, sino que también pueden causar daños económicos y poner en riesgo la seguridad nacional (Mecías et al., 2024).

Por lo tanto, en concordancia con este trabajo, se realizó un análisis exhaustivo de la información recopilada nacional e internacional, arrojando cifras que permitieron contribuir en el desarrollo del mismo, basado en los resultados en donde se evidenciaron una cantidad de casos

de acceso no autorizados alarmante, que deja con preocupación que las entidades financieras y gubernamentales fueron las más afectadas. Consecuentemente, este estudio detalla todo el actuar delictivo de las organizaciones, las afectaciones y los porcentajes que se analizaron luego de una muestra.

Marco Legal

Marco Normativo Internacional

Aunque la aplicación directa recae en la legislación colombiana, las siguientes normas internacionales establecen los principios y estándares globales que orientan este proyecto.

- Declaración Universal de Derechos Humanos (Artículo 12): Este artículo consagra el derecho fundamental a la no injerencia en la vida privada y a la protección de la ley contra ataques a la honra y reputación. En la era digital, este principio se extiende a la protección de los datos personales, que son una manifestación de la vida privada. El sistema propuesto, al manejar datos biométricos, debe tener un diseño para ser una herramienta de protección de este derecho, no una fuente de injerencia.
- Resolución A/C.3/68/L.45/Rev.1 de Naciones Unidas, "El Derecho a la Privacidad en la Era Digital": Esta resolución reconoce que los derechos de las personas deben protegerse tanto en línea como fuera de ella. Exhorta a los Estados a establecer marcos legales sólidos para la protección de datos y a garantizar que la recopilación y el uso de datos personales, especialmente por parte de entidades gubernamentales, se realicen de manera transparente y con el consentimiento del individuo. El proyecto se alinea con esta resolución al proponer un sistema que busca fortalecer la seguridad y la confianza en el tratamiento de datos por parte del Estado.
- Convenio de Budapest sobre la Ciberdelincuencia (ETS No. 185): Este es el primer tratado internacional destinado a abordar los delitos informáticos y de internet mediante la armonización de leyes nacionales y el fomento de la cooperación internacional. Define delitos como el acceso ilícito a sistemas, la interceptación ilegal y la interferencia de datos. La propuesta de un sistema de seguridad robusto es una medida

preventiva y reactiva que se alinea con los objetivos del Convenio de Budapest, al dificultar la comisión de estos delitos y generar trazas de auditoría que podrían servir en eventuales investigaciones penales.

- Ley Orgánica 14/2022 de España (Artículo 248): Si bien no es vinculante en Colombia, esta ley, que tipifica el delito de estafa, sirve como un referente comparado. Define la estafa como el uso de engaño para inducir a error a otro y causar un perjuicio patrimonial. El sistema de autenticación biométrica propuesto busca eliminar el "engaño" en la suplantación de identidad, que es una de las formas más comunes de iniciar una estafa en trámites con el Estado, atacando así la raíz del comportamiento delictivo.

Marco Normativo Nacional (Colombia)

La legislación colombiana es el pilar fundamental que define los requisitos, límites y oportunidades para el diseño del sistema conceptual.

Ley Estatutaria 1581 de 2012 - Régimen General de Protección de Datos Personales:

Esta es la norma central que rige el proyecto. Su análisis detallado es crucial: Objeto y Principios (Art. 1): La ley busca desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar su información en bases de datos (Habeas Data). El sistema propuesto debe ser un garante de este derecho, asegurando que el ciudadano tenga control sobre su identidad digital.

Tratamiento de Datos Sensibles (Art. 6): La ley establece una prohibición general sobre el tratamiento de datos sensibles, categoría en la que se incluyen explícitamente los datos biométricos (huella dactilar, rostro). Sin embargo, el mismo artículo establece excepciones. La más relevante para este proyecto es que el tratamiento es posible cuando "el Titular haya dado su

autorización explícita". Esto implica que el sistema no puede ser obligatorio; debe solicitar un consentimiento libre, previo, expreso e informado del ciudadano para usar su biometría.

Derechos de los Titulares (Art. 8): El ciudadano tiene derecho a conocer, actualizar, rectificar y solicitar la supresión de sus datos. El diseño del sistema debe contemplar interfaces y procedimientos claros para que los usuarios puedan ejercer estos derechos de manera sencilla.

Deberes del Responsable del Tratamiento (Art. 12 y 17): La entidad pública que implemente el sistema (Responsable del Tratamiento) tiene la obligación de informar al ciudadano de manera clara la finalidad del tratamiento de sus datos, conservar la prueba de la autorización y garantizar la seguridad de la información. El sistema debe estar diseñado para cumplir con estas obligaciones de forma automatizada y auditable.

Vigilancia y Sanciones (Art. 19 y Caso Mercado Libre): La Superintendencia de Industria y Comercio (SIC) es la autoridad de vigilancia. Un precedente ineludible es la sanción impuesta a Mercado Libre por condicionar el acceso a sus servicios al uso obligatorio del reconocimiento facial. Este caso demuestra que cualquier sistema que se diseñe debe ofrecer alternativas de autenticación no biométricas para respetar la libertad de elección del ciudadano y evitar sanciones.

Decreto Ley 019 de 2012 - Ley Anti-trámites.

Identificación por Medios Electrónicos (Art. 18)

Este artículo es un habilitador directo del proyecto. Suprime la imposición de la huella dactilar en tinta y ordena que la identificación
se realice por medios electrónicos. Además, establece que las entidades deben contar con los medios tecnológicos para cotejar la identidad contra la base de datos de la Registraduría Nacional del Estado Civil. Esto proporciona el fundamento legal para la integración con la RNEC que el proyecto propone.

Decreto 1000 de 2015 - Reglamentación de la Biometría Electrónica

Este decreto reglamenta el artículo 18 de la Ley Anti-trámites, estableciendo las condiciones para que las entidades públicas y privadas que ejercen funciones administrativas implementen la interoperabilidad con la Registraduría para la verificación biométrica. En la práctica, consolida el mandato de modernización y establece el marco para que operadores tecnológicos ofrezcan este servicio.

Ley 2195 de 2022 - Medidas de Transparencia y Lucha contra la Corrupción

Objeto: Esta ley busca prevenir actos de corrupción, reforzar la coordinación del Estado y recuperar los daños ocasionados por dichos actos. El sistema propuesto es una herramienta tecnológica concreta para alcanzar estos fines. Al implementar una autenticación robusta, se mitigan fraudes como la suplantación y los "beneficiarios fantasmas", que son formas de corrupción que afectan directamente al ciudadano y al erario.

Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública

Objeto (Art. 1). Esta ley regula el derecho de acceso a la información pública. Si bien promueve la transparencia, también establece un equilibrio al definir la información que puede ser clasificada o reservada, como es el caso de los datos personales. El sistema propuesto debe operar en esta tensión: facilitar al ciudadano el acceso seguro a su propia información, mientras protege esos mismos datos de ser accedidos por terceros no autorizados, cumpliendo así con los dos lados de la balanza legal.

Documentos CONPES sobre Seguridad y Servicio al Ciudadano

CONPES 3649 de 2010 (Política de Servicio al Ciudadano)

Establece la necesidad de generar confianza y mejorar la satisfacción del ciudadano con la Administración Pública. El

sistema propuesto contribuye directamente a este objetivo al ofrecer un canal más seguro, eficiente y confiable para la realización de trámites.

CONPES 3701 de 2011 y 3854 de 2016 (Políticas de Ciberseguridad y Ciberdefensa)

Estos documentos establecen los lineamientos estratégicos para la defensa del país en el ciberespacio. Reconocen el aumento de las amenazas y la necesidad de fortalecer las capacidades del Estado. La propuesta de un sistema de seguridad avanzado se alinea con estas políticas, aportando una solución concreta a nivel de servicio al ciudadano, un frente a menudo vulnerable a los ciberataques.

En síntesis, el marco legal colombiano no solo permite, sino que en ciertos aspectos impulsa la implementación de tecnologías como la autenticación biométrica electrónica. Sin embargo, impone condiciones estrictas, especialmente en lo que respecta a la protección de datos sensibles, que deben ser el pilar fundamental sobre el cual se construya el diseño conceptual del sistema para garantizar su legalidad y legitimidad.

Metodología

Enfoque de la Investigación

Para alcanzar los objetivos propuestos, esta investigación adoptará un enfoque mixto, combinando elementos del paradigma cualitativo y descriptivo. Cualitativo: porque busca comprender en profundidad el fenómeno del fraude y las vulnerabilidades de seguridad en el sector público colombiano, interpretando documentos, políticas y contextos normativos; descriptivo: ya que se centrará en caracterizar el estado del arte de las tecnologías biométricas y de RPA, así como en detallar la estructura y componentes del sistema conceptual propuesto (Hernández-Sampieri et al., 2014).

Así mismo, el diseño de la investigación es no experimental y documental, ya que se basará en el análisis de fuentes secundarias (leyes, decretos, informes técnicos, artículos académicos, etc.) y no en la manipulación de variables en un entorno controlado.

Fases de la Metodología (Alineadas con los Objetivos Específicos)

La metodología se ejecutará en tres fases secuenciales y acumulativas, donde cada fase corresponde a un objetivo específico y su resultado es el insumo principal para la siguiente. Este enfoque estructurado reemplaza el modelo Canvas por un proceso de investigación sistemático y coherente con el diseño de un sistema conceptual.

Fase I: Diagnóstico del Ecosistema de Fraude y Vulnerabilidades:

- Objetivo Específico Asociado: 1. Diagnosticar el ecosistema de fraude y las vulnerabilidades de seguridad de la información en la prestación de servicios al ciudadano por parte de entidades públicas en Colombia.
- Actividades Metodológicas: Se realizará una revisión documental sistemática para recopilar y analizar información sobre la problemática.

- Técnicas e Instrumentos:
    - *Análisis Documental:* Se examinarán documentos estratégicos como la Estrategia Nacional de Seguridad Digital, documentos CONPES sobre seguridad y servicio al ciudadano y normativas sobre ciberdelincuencia.
    - *Análisis de Informes de la Industria:* Se estudiarán informes de empresas de Ciberseguridad y riesgo, como los de TransUnion, para cuantificar las tendencias de fraude por suplantación en Colombia.
- Resultado Esperado: Un documento de diagnóstico que categorice las principales tipologías de fraude y mapee las vulnerabilidades institucionales, técnicas y operativas del sector público colombiano, justificando la necesidad de la solución propuesta.

Fase II: Evaluación de Viabilidad Técnica, Jurídica y Operativa

- Objetivo Específico Asociado: 2. Evaluar la viabilidad técnica, jurídica y operativa de integrar un sistema de autenticación biométrica con los servicios de la Registraduría Nacional del Estado Civil.
- Actividades Metodológicas: Se llevará a cabo un análisis comparativo y normativo de las soluciones y marcos existentes.
- Técnicas e Instrumentos:
    - *Análisis Comparativo Técnico:* Se identificarán los operadores biométricos certificados por la RNEC (ej. Certicámara, BTC, SecurID) y se compararán sus ofertas de servicios (biometría facial, dactilar), estándares de seguridad (ej. ISO 30107-3 para detección de vida) y modelos de integración.

- *Análisis Normativo:* Se realizará un análisis detallado de la Ley 1581 de 2012, sus decretos reglamentarios y la jurisprudencia de la SIC (ej. caso Mercado Libre) para definir los requisitos de cumplimiento legal del sistema.
- *Estudio de Caso:* Se analizará el caso de la alianza RNEC-Asobancaria como prueba de concepto de la viabilidad operativa a gran escala en Colombia.

- Resultado Esperado: Un informe de viabilidad que presente una matriz de evaluación de las alternativas tecnológicas y justifique la selección de un enfoque de integración que sea técnica, legal y operacionalmente factible en el contexto colombiano.

Fase III: Diseño del Modelo Conceptual:

- Objetivo Específico Asociado: 3. Delinear el modelo conceptual de un sistema de seguridad integrado que articule los servicios de autenticación biométrica con la Automatización Robótica de Procesos (RPA).
- Actividades Metodológicas: Se utilizarán técnicas de modelado de sistemas para sintetizar los hallazgos de las fases I y II en un diseño coherente.
- Técnicas e Instrumentos:
  - *Modelado Arquitectónico:* Se definirán los componentes lógicos del sistema (capa de presentación, módulo de captura, middleware de integración, motor de RPA) y sus interacciones, basándose en arquitecturas de referencia.
  - *Modelado de Procesos:* Se utilizarán diagramas de flujo (ej. BPMN o UML) para ilustrar el funcionamiento del sistema en casos de uso críticos (ej. solicitud de un certificado), mostrando la secuencia desde la autenticación biométrica hasta la ejecución de la tarea por el robot de RPA.

- Resultado Esperado: El entregable final de la investigación: un documento de diseño conceptual que describa en detalle la estructura, componentes y funcionamiento del sistema de seguridad propuesto.

Población y Muestra

Dado que la investigación es de carácter documental y conceptual, la población no está constituida por personas, sino por el universo de documentos pertinentes al objeto de estudio.

- Población: Todas las leyes, decretos, resoluciones, informes técnicos, artículos académicos y documentos de política pública emitidos en Colombia y a nivel internacional entre 2012 y 2025, relacionados con seguridad digital, protección de datos, biometría y fraude.
- Muestra: Se utilizará un muestreo no probabilístico por criterio, seleccionando aquellos documentos que son considerados fuentes primarias y de mayor autoridad en cada área:
  - *Legal:* Ley 1581 de 2012, Ley 2195 de 2022, Decreto Ley 019 de 2012.
  - *Política Pública:* Estrategia Nacional de Seguridad Digital 2025-2027, documentos CONPES.
  - *Técnico:* Informes de la industria (ej. TransUnion), documentación de operadores biométricos certificados.
  - *Académico:* Artículos de investigación sobre RPA en el sector público y arquitecturas biométricas.

Plan de Validación del Diseño Conceptual

Al ser el resultado un modelo conceptual y no un prototipo funcional, la validación no se realizará mediante pruebas piloto o simulaciones de fraude. En su lugar, se empleará una

validación teórica por triangulación de criterios. El modelo conceptual diseñado en la Fase III será evaluado contra un conjunto de criterios derivados de las fases anteriores para asegurar su robustez y pertinencia.

Los criterios de validación serán:

1. Pertinencia con el Diagnóstico: ¿El modelo conceptual aborda directamente las vulnerabilidades y tipologías de fraude identificadas en la Fase I?
2. Cumplimiento Normativo: ¿El diseño respeta todos los principios y obligaciones de la Ley 1581 de 2012 y la jurisprudencia de la SIC analizados en la Fase II (ej. consentimiento explícito, alternativas no biométricas)?
3. Viabilidad Técnica y Operativa: ¿El modelo se basa en tecnologías y arquitecturas cuya factibilidad fue demostrada en la evaluación de la Fase II?
4. Coherencia con la Tríada CID: ¿El diseño fortalece de manera equilibrada los principios de Confidencialidad, Integridad y Disponibilidad?

Esta metodología, asegura un proceso de investigación riguroso, trazable y directamente enfocado en la construcción de un diseño conceptual sólido y bien fundamentado.

Procedimiento

El desarrollo de esta investigación se ejecutará siguiendo un Procedimiento sistemático estructurado en las tres fases metodológicas previamente definidas. Cada fase se construye sobre los resultados de la anterior, asegurando una progresión lógica desde el diagnóstico del problema hasta el diseño de la solución conceptual.

Fase I: Procedimiento de Diagnóstico

Recopilación Documental

Se iniciará con la recolección de fuentes secundarias clave. Se compilarán documentos estratégicos del Estado, como la Estrategia Nacional de Seguridad Digital 2025-2027, y normativas pertinentes a la ciberdelincuencia y la protección de datos. Simultáneamente, se recopilarán informes de la industria sobre tendencias de fraude en Colombia, con especial atención a los datos de suplantación de identidad.

Análisis y Sistematización

La información recolectada será analizada para categorizar las tipologías de fraude más comunes que afectan a los ciudadanos y para mapear las vulnerabilidades (institucionales, técnicas y operativas) del sector público. El resultado de este análisis será un documento de diagnóstico que servirá como insumo fundamental para la siguiente fase.

Fase II: Procedimiento de Evaluación de Viabilidad

Identificación y Comparación de Soluciones: se identificarán los operadores biométricos certificados por la Registraduría Nacional del Estado Civil (RNEC). Se procederá a realizar un análisis comparativo de sus servicios, evaluando aspectos técnicos como las

modalidades biométricas ofrecidas (facial, dactilar) y los estándares de seguridad que cumplen.

1. Análisis Jurídico y de Cumplimiento: se llevará a cabo un estudio detallado de la Ley 1581 de 2012 y la jurisprudencia relevante de la Superintendencia de Industria y Comercio

(SIC). El objetivo es extraer los requisitos legales específicos que el sistema conceptual debe cumplir, como los mecanismos de consentimiento explícito y la obligatoriedad de ofrecer

alternativas de autenticación.

2. Estudio de Caso Operativo: se analizará la implementación de la biometría en el sector financiero colombiano a través de la alianza RNEC-Asobancaria como un caso de éxito.

Se extraerán lecciones aprendidas sobre la viabilidad operativa, la adopción por parte de los usuarios y la efectividad en la mitigación del fraude.

Fase III: Procedimiento de Diseño Conceptual

1. Síntesis de Requerimientos: se consolidarán los hallazgos de las fases I y II. Las vulnerabilidades diagnosticadas y los requisitos técnicos y legales identificados se traducirán en un conjunto de requerimientos funcionales y no funcionales para el sistema.

2. Modelado del Sistema: utilizando los requerimientos definidos, se procederá a un diseño del modelo conceptual. Mediante diagramas de flujo y de arquitectura, se delineará la

estructura del sistema, sus componentes principales (módulo de captura, middleware, motor de RPA) y las interacciones entre ellos. Se modelará el flujo de un trámite crítico

para ilustrar cómo la autenticación biométrica se articula con la Automatización Robótica de Procesos (RPA) para crear un servicio seguro y eficiente. El producto final de este procedimiento será el documento
de diseño conceptual que constituye el resultado principal de la investigación.

Resultados Obtenidos

Esta sección presenta los resultados detallados derivados de la ejecución de cada una de las fases metodológicas del proyecto. Los hallazgos se exponen de manera secuencial, respondiendo a los objetivos específicos planteados y construyendo una base sólida y teóricamente fundamentada para el diseño conceptual propuesto.

Objetivo 1. Diagnóstico del Ecosistema de Fraude y las Vulnerabilidades de Seguridad de la Información en la Prestación de Servicios al Ciudadano por parte de Entidades Públicas en Colombia

La primera fase de la investigación consistió en un diagnóstico exhaustivo del entorno de seguridad digital en Colombia. Para contextualizar estos hallazgos, se utiliza como marco de referencia la norma internacional ISO/IEC 27001, que define un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la protección de la tríada CID: Confidencialidad, Integridad y Disponibilidad. Las vulnerabilidades identificadas en el sector público colombiano representan fallas directas en uno o más de estos pilares.

Ecosistema de Fraude: La Suplantación de Identidad como Falla de Confidencialidad e Integridad

El análisis de fuentes de la industria y reportes de seguridad confirma que Colombia enfrenta un desafío significativo en materia de fraude digital, que compromete directamente la confidencialidad de la identidad de los ciudadanos y la integridad de los procesos estatales.

Crecimiento Acelerado del Fraude. El volumen de transacciones digitales sospechosas de fraude en Colombia experimentó un crecimiento del 105% entre 2019 y 2023. Este ritmo supera significativamente el aumento del 90% en el total de transacciones digitales legítimas durante el

mismo periodo, lo que indica que la actividad fraudulenta está ganando terreno de manera desproporcionada.

Alta Exposición Ciudadana. La exposición de los ciudadanos al fraude es masiva. Hacia finales de 2023, un 40% de los consumidores colombianos declararon haber sido objeto de intentos de fraude a través de canales como correo electrónico, llamadas telefónicas o mensajes de texto. Estas tácticas de ingeniería social, como el phishing y el smishing, son a menudo el preludio de delitos más graves como la suplantación de identidad.

La Suplantación como Amenaza Central. La suplantación de identidad, definida como el acto de hacerse pasar por otra persona para obtener un beneficio ilícito, es la amenaza central que este proyecto busca mitigar. Este delito, tipificado en el Código Penal colombiano, es una violación directa de:

- Confidencialidad: Un tercero no autorizado accede a información y servicios que solo le corresponden al titular legítimo.
- Integridad: Las acciones realizadas por el suplantador (solicitudes, transacciones) alteran los registros de la entidad de manera fraudulenta, creando información que no es veraz ni comprobable

La siguiente

- Tabla *1* resume las estadísticas clave que dimensionan la problemática del fraude en el país.

Tabla 1

Estadísticas Clave que Dimensionan la Problemática del Fraude en Colombia

Métrica de Fraude	Hallazgo Clave	Período de Referencia
Crecimiento de Sospechas de Fraude Digital	Aumento del 105%	2019 - 2023
Exposición de Consumidores	40% de los consumidores colombianos	Septiembre - Diciembre
Métrica de Fraude a Intentos de Fraude	Hallazgo Clave	Período de Referencia 2023
Tasa de Sospecha de Fraude Digital (Anual)	Aumento interanual en 2024	2023 - 2024
Fraude en Comercio Electrónico	19% de los usuarios experimentaron fraude	Último año (reportado en marzo de 2024)
Apertura de Cuentas Fraudulentas (Global)	13.5% de las transacciones de creación de cuentas fueron sospechosas	2023

Nota. Adaptado de TransUnion, 2024.

Vulnerabilidades Sistémicas del Sector Público Colombiano

El análisis de la Estrategia Nacional de Seguridad Digital 2025-2027 revela que las entidades públicas colombianas presentan una serie de vulnerabilidades estructurales que impiden garantizar la tríada CID. Estas debilidades, en lugar de mitigar, a menudo facilitan la materialización de los fraudes descritos.

Gobernanza y Coordinación. Existe una "debilidad institucional y la falta de coordinación efectiva" entre las distintas entidades con responsabilidades en seguridad digital. Esto resulta en una fragmentación de iniciativas y una dispersión de recursos, impidiendo la aplicación de un SGSI coherente a nivel nacional, como lo promovería un marco como ISO/IEC 27001.

Capacidad Técnica y de Respuesta. Se diagnostica una "insuficiente capacidad para identificar, evaluar y mitigar riesgos cibernéticos de manera integral". Esto se alinea con la falta de un proceso de gestión de riesgos sistemático, que es el pilar de la norma ISO/IEC 27001. La infraestructura tecnológica, incluyendo las páginas web del dominio.gov.co, ha sido señalada como extremadamente vulnerable, afectando directamente la Disponibilidad e Integridad de los servicios.

Talento Humano y Cultura de Seguridad. Hay una notable escasez de talento especializado y una falta de cultura de seguridad digital generalizada. La falta de liderazgo en TI con conocimientos avanzados en seguridad limita la capacidad de las organizaciones para implementar protecciones efectivas, y la capacitación del personal es a menudo lenta e insuficiente. La siguiente **Tabla *2*** detalla estas vulnerabilidades y su impacto directo en los principios de la tríada CID.

Tabla 2.

Vulnerabilidades y Su Impacto Directo en los Principios de la Tríada CID

Categoría de Vulnerabilidad	Descripción Específica	Impacto en la Tríada CID
Gobernanza y Coordinación	Fragmentación de iniciativas y falta de un marco de coordinación efectivo entre entidades.	Disponibilidad/Integridad: Inconsistencias en los niveles de seguridad entre diferentes entidades. El ciudadano enfrenta experiencias de seguridades dispares y a menudo deficientes.
Capacidad Técnica y de Respuesta	Insuficiente capacidad para mitigar riesgos; falta de un sistema robusto de respuesta a incidentes; infraestructura web vulnerable.	Confidencialidad/Integridad/Disponibilidad: Portales de trámites inseguros, riesgo de caídas del servicio, y exposición de los datos personales de los ciudadanos a brechas de seguridad.
Talento Humano y Cultura	Escasez de personal especializado en Ciberseguridad; falta de liderazgo en TI con conocimientos	Confidencialidad/Integridad: Procesos internos débiles que pueden ser explotados por ingeniería social; atención al ciudadano deficiente en caso de incidentes de seguridad.

	avanzados; capacitación lenta e ineficaz.	
Marco Normativo y de Cumplimiento	Desactualización de la normativa frente a amenazas modernas; debilidades en la persecución y castigo del cibercrimen.	Integridad: Sensación de impunidad para los ciberdelincuentes; desconfianza del ciudadano en la capacidad del Estado para protegerlo y hacer justicia.

Nota. Adaptado de MINTIC, 2025.

Objetivo 2. Evaluación de la Viabilidad Técnica, Jurídica y Operativa De Integrar un Sistema de Autenticación Biométrica con los Servicios de la Registraduría Nacional del Estado Civil, en el Marco de la Ley 1581 de 2012 y las Políticas de Seguridad Digital Vigentes

La segunda fase de la investigación evaluó la factibilidad de integrar un sistema de autenticación biométrica con los servicios de la RNEC. El resultado es que dicha integración es viable, y su robustez puede ser medida y diseñada conforme a estándares internacionales como las Guías de Identidad Digital NIST SP 800-63 del Instituto Nacional de Estándares y Tecnología de EE. UU.

Viabilidad Jurídica: Navegando la Ley 1581 de 2012

El principal desafío jurídico es el cumplimiento de la Ley Estatutaria 1581 de 2012 sobre protección de datos personales. El análisis de la norma y su reglamentación arroja las siguientes conclusiones clave para el diseño del sistema:

- Naturaleza de los Datos Biométricos: Los datos biométricos (huella, rostro) son clasificados como datos sensibles, lo que implica que su tratamiento está, por regla general, prohibido.
- Condición para el Tratamiento: La ley permite el tratamiento de datos sensibles bajo una condición fundamental: la obtención de la autorización "previa, explícita e informada" del titular.
- Prohibición de Condicionamiento: Ninguna actividad puede estar condicionada a que el ciudadano suministre datos sensibles. Este punto es reforzado por la jurisprudencia de la SIC, como lo demuestra la sanción impuesta a Mercado Libre por

exigir el reconocimiento facial como único medio para acceder a las cuentas.

- Requisito de Diseño: Para ser jurídicamente viable, el sistema conceptual debe, por diseño, ofrecer siempre una alternativa de autenticación no biométrica, garantizando así la libertad de elección del ciudadano y el cumplimiento estricto de la ley.

Viabilidad Técnica y Alineación con Estándares NIST

El ecosistema tecnológico colombiano no solo es maduro, sino que puede ser evaluado y alineado con las mejores prácticas internacionales, como las definidas en NIST SP 800-63.

Ecosistema de Operadores Certificados. Colombia cuenta con operadores biométricos certificados por la RNEC (ej. Certicámara, BTC Biometric, SecurID) que ofrecen la infraestructura de conexión necesaria.

Niveles de Aseguramiento del Autenticador (AAL). NIST SP 800-63B define tres niveles de seguridad para los autenticadores. El sistema propuesto puede ser diseñado para cumplir con los niveles más altos:

- *AAL1:* Requiere autenticación de un solo factor. Es el nivel más bajo.
- *AAL2:* Requiere autenticación de dos factores distintos y utiliza canales de comunicación cifrados. La biometría es un factor aceptado.
- *AAL3:* Requiere un autenticador criptográfico basado en hardware (como una llave FIDO2) y es resistente a ataques de "hombre en el medio". Es el nivel más alto de seguridad.

La siguiente Tabla *3* muestra cómo el sistema propuesto puede alinearse con los niveles AAL de NIST.

Tabla 3

Sistema Propuesto Alineado con los Niveles AAL de NIST

Nivel AAL (NIST SP 800-63B)	Requisito Principal	Aplicación en el Sistema Propuesto
AAL1	Un solo factor de autenticación.	La opción de "usuario y contraseña" cumpliría con este nivel mínimo.
AAL2	Autenticación multifactor (MFA). Se requieren dos de tres tipos de factores (algo que sabes, algo que tienes, algo que eres).	La combinación de biometría (algo que eres) con la posesión de un dispositivo registrado (algo que tienes) cumple y supera los requisitos de AAL2.
AAL3	MFA con un autenticador criptográfico basado en hardware.	Aunque el diseño base apunta a AAL2, podría extenderse para soportar AAL3 mediante el uso de la Cédula Digital colombiana (si funciona como un dispositivo criptográfico) o llaves de seguridad FIDO2.

Nota. Elaboración propia.

Viabilidad Operativa: El Precedente del Sector Financiero

La viabilidad operativa a gran escala ya ha sido demostrada en el país. El convenio entre la RNEC y Asobancaria, vigente desde 2016, es el principal caso de estudio.

- Implementación Exitosa: El sector financiero ha utilizado la biometría dactilar durante años para reducir el fraude por suplantación, realizando millones de consultas anuales.
- Evolución hacia la Biometría Facial: En 2024, la alianza culminó con éxito las pruebas piloto para la autenticación facial, un servicio que ya está disponible y que permite realizar trámites de forma remota y segura.

Objetivo 3. Delineación del Modelo Conceptual de un Sistema de Seguridad Integrado que Articule los Servicios de Autenticación Biométrica con la Automatización Robótica de Procesos (RPA) para la Validación de la Identidad y la Optimización de Trámites Críticos de Atención al Ciudadano

La fase final de la investigación consistió en sintetizar los hallazgos para el diseño de un modelo conceptual. Este diseño se fundamenta en los principios del Ciclo de Vida de Desarrollo Seguro (Secure SDLC), que aboga por integrar la seguridad en todas las fases del desarrollo, no como una ocurrencia tardía.

Arquitectura Conceptual y Principios de Diseño Seguro

El modelo propuesto se compone de cuatro capas lógicas, cuyo diseño conceptual debe adherirse a los siguientes principios de Secure SDLC.

Tabla 4

Modelo propuesto

Principio Secure SDLC	Aplicación en el Diseño Conceptual del Sistema
Seguridad por Diseño (Secure by Design)	El sistema se concibe desde el inicio con la seguridad como un requisito fundamental, no como un añadido. Se integra la evaluación de riesgos en la fase de diseño.
Mínimo Privilegio (Least Privilege)	Cada componente (ej. el robot de RPA) solo debe tener los permisos estrictamente necesarios para realizar su función, minimizando el daño potencial en caso de compromiso.
Defensa en Profundidad	Se implementan múltiples capas de seguridad (autenticación, cifrado, monitoreo, automatización) para que el fallo de un control no comprometa todo el sistema.
Minimizar la Superficie de Ataque	El diseño evita exponer funcionalidades o puertos innecesarios. La comunicación con la RNEC se realiza a través de un intermediario (operador biométrico), reduciendo la exposición directa.

Nota. Elaboración propia.

Requisitos Técnicos y Viabilidad del Sistema

Para que el diseño conceptual sea realista, se deben considerar los siguientes aspectos técnicos.

- Requisitos Mínimos de Infraestructura (Consideraciones para Futura Implementación):
  - *Servidores:* Infraestructura de servidores (en la nube o en las instalaciones) con capacidad para alojar el middleware de integración y el motor de RPA, con alta disponibilidad y redundancia.
  - *Red:* Conectividad de red segura y de baja latencia entre la entidad pública, el operador biométrico y los sistemas internos.
  - *Dispositivos de Usuario Final:* El sistema debe ser compatible con cámaras y navegadores web estándar en computadores y dispositivos móviles (Smartphone con menos de 4 años de antigüedad para asegurar parches de seguridad). Igual, los estándares de Ciberseguridad aplicables se muestran en la siguiente **Tabla *5***.

Tabla 5

Estándares de Ciberseguridad Aplicables

Estándar Internacional	Aplicación en el Sistema Propuesto
ISO/IEC 27001	Proporciona el marco general para el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad que implementa la solución. Guía la gestión de riesgos, la definición de políticas y los controles de Annex A.
NIST SP 800-63	Define los requisitos técnicos específicos para la identidad digital. Guía el diseño de los procesos de autenticación para alcanzar un nivel de aseguramiento (AAL) adecuado al riesgo de los trámites.

ISO 19794-2 / ANSI 378	Estándares para el formato de las plantillas de huellas dactilares, asegurando la interoperabilidad y la calidad de los datos biométricos. Los operadores como BTC ya los utilizan.
ISO 30107-3	Estándar para la detección de ataques de presentación (liveness detection). Es crucial para prevenir fraudes con fotos o videos y es una capacidad ofrecida por operadores certificados.

Nota. Elaboración propia.

Arquitectura de Referencia y Desafíos de Interoperabilidad

El sistema propuesto actuaría como una capa de orquestación moderna sobre los sistemas existentes. Sin embargo, su implementación enfrentaría los desafíos inherentes a la interoperabilidad con los sistemas legados (legacy) del gobierno.

Arquitectura de Referencia

1. Front-End (Portal/App/Chatbot): Interfaz con el ciudadano.
2. Middleware de Autenticación: Gestiona la lógica de autenticación, invoca al operador biométrico y maneja las respuestas.
3. Motor de RPA: Orquesta los robots de software.
4. Conectores/Adaptadores a Sistemas Legados: Los robots de RPA interactúan con los sistemas existentes (Bases de Datos, ERPs, CRMs) a través de sus interfaces de usuario o APIs, si existen.

Desafíos de Interoperabilidad con Sistemas Legados.

- Silos de Datos: La información del ciudadano puede estar fragmentada en múltiples sistemas que no se comunican entre sí. La RPA puede ayudar a salvar estas brechas, pero la inconsistencia de los datos es un riesgo.

- Formatos Incompatibles: Los sistemas antiguos pueden usar formatos de datos obsoletos, requiriendo que los robots de RPA realicen tareas de transformación y limpieza de datos.
- Falta de APIs: Muchos sistemas legados carecen de APIs modernas. La RPA es una solución ideal en estos casos, ya que puede interactuar con las aplicaciones a través de su interfaz gráfica, como lo haría un humano.
- Riesgos de Seguridad: Los sistemas legados pueden tener vulnerabilidades no parcheadas. Es crucial que la red donde operan los robots esté segmentada y que los robots tengan permisos mínimos para limitar la exposición.
- Resistencia Cultural: La implementación de nuevas tecnologías a menudo enfrenta resistencia por parte del personal acostumbrado a los procesos manuales, así, la gestión del cambio es un factor crítico de éxito.

Este enfoque detallado, fundamentado en estándares internacionales y conscientes de los desafíos locales, proporciona un modelo conceptual robusto y viable para transformar la seguridad y la eficiencia de los servicios al ciudadano en Colombia.

Discusión de los Resultados

Una vez finalizado el trabajo investigativo y luego de un exhaustivo análisis, se logró determinar las variables de los resultados, los pros y los contras que se encontraron en cada uno de los pasos desarrollados, avanzando así en hacer mejores integraciones y buscar alternativas que permitan integrar todas las variables de la investigación.

En este sentido, analizadas las principales vulnerabilidades de información y la población que accede a ella, como los actores implicados, se dejó rezagada una población que puede ser importante para los trámites de las entidades, como aquellos que tienen problemas de salud y la piel en donde poder identificar sus huellas es difícil, por lo que limitará el acceso a la apertura del sistema, permitiendo abrir una oportunidad de mejoramiento en la autenticación del sistema.

Otra necesidad, es la del territorio nacional y la disponibilidad de recursos económicos que son uno de los más importantes para la adquisición de equipos acordes al proyecto, dado que como es de la opinión pública en muchas de las ciudades y pueblos de Colombia la carencia de recursos económicos hacen que los servicios a los ciudadanos sean escasos e insuficientes ante las necesidades y avances tecnológicos.

Una vez diseñado el sistema, debe haber un cuadro de posibles eventos de emergencia y como mitigarlos dado ocurran, como por ejemplo catástrofes, cortes de luz, pérdida de comunicación con el canal de la Registraduría y daños de equipos, esto será un plan de contingencia que debe estar inmerso en la propuesta de desarrollo una vez se implemente.

Por último, considerar todas las variables que pudieran suceder en razón a un reconocimiento facial como ya se mencionó por temas de salud, que están asociados a temas de envejecimiento, y otros por operaciones estéticas; así, es preciso saber qué alternativas se pueden

brindar en casos en donde el sistema no pueda identificar a la persona, como se logrará la apertura del sistema en donde las huellas coincidan con la persona, pero su rostro no.

Por lo tanto, la incertidumbre ante la brecha digital y el mejoramiento por realizar inherente con una estrategia como mitigación de robo y fraude, permite acercarse al ciudadano, estableciendo una relación confiable y amigable con la entidad. Ahora, debe pensarse en abordar todas las causales, problemáticas y riesgos que pudiesen llegar a presentarse como a los actores de diferentes niveles y culturas, logrando así una sinergia efectiva para el aprovechamiento continuo de las tecnologías de la información.

Es preciso indicar, que esta investigación en comparación con otros artículos se desarrolló acorde y conforme con la necesidad del momento, más sin embargo se revisó la literatura que sirvió de apoyo, logrando evidenciar que este diseño puede ser pionero en las entidades públicas para la mitigación de robo de información y fraudes. Ahora bien, al ser un diseño innovador, no se encontraron artículos referentes que puedan ayudar en el comparativo de otros resultados esperados o estimados, más los que se mencionaron en este apartado.

Conclusiones

La presente investigación ha abordado una de las problemáticas más críticas que enfrenta la transformación digital del Estado colombiano: la creciente brecha entre la digitalización de los servicios al ciudadano y la capacidad de las entidades públicas para protegerlos contra el fraude. El diagnóstico inicial confirmó un escenario de alto riesgo, con un aumento superior al 105% en los intentos de fraude digital en los últimos años y la existencia de vulnerabilidades sistémicas en el sector público, como la falta de coordinación y la debilidad de las infraestructuras tecnológicas. Este contexto valido la necesidad urgente de una solución que vaya más allá de los mecanismos de seguridad tradicionales y que pueda restaurar la confianza ciudadana en los canales digitales.

En respuesta, este estudio ha diseñado un sistema conceptual cuya principal innovación no reside en la invención de una tecnología, sino en la articulación estratégica de capacidades ya existentes y probadas: la autenticación biométrica (facial y dactilar) a través del ecosistema de operadores certificados por la Registraduría Nacional, y la Automatización Robótica de Procesos (RPA) para la ejecución segura de tareas administrativas.

El impacto de este modelo conceptual es significativo, pues ofrece una hoja de ruta viable para que las entidades públicas puedan fortalecer la tríada de la seguridad de la información —Confidencialidad, Integridad y Disponibilidad—, pasando de un enfoque reactivo a uno proactivo y alineado con estándares internacionales como ISO/IEC 27001 y NIST SP 800-63.

Evaluación del Cumplimiento de los Objetivos

La ruta metodológica, estructurada en tres fases, permitió alcanzar de manera satisfactoria tanto el objetivo general como los específicos, demostrando una progresión lógica desde la identificación del problema hasta la formulación de una solución fundamentada.

Cumplimiento del Objetivo General: Se logró plenamente el objetivo del diseño de un sistema conceptual de seguridad de la información. El resultado no es un mero diagrama técnico, sino un modelo holístico que considera y se adapta a la realidad colombiana. El diseño está fundamentado en un análisis de viabilidad que abarca los planos técnico, jurídico y operativo, asegurando que la propuesta sea realista y pertinente para el contexto de las entidades públicas del país.

Cumplimiento del Objetivo Específico 1 (Diagnosticar): Este objetivo se alcanzó mediante una revisión sistemática de informes de la industria y documentos estratégicos del gobierno, como la Estrategia Nacional de Seguridad Digital. Los hallazgos validaron la premisa de la investigación, cuantificando la magnitud del fraude por suplantación y mapeando las vulnerabilidades institucionales que lo facilitan, lo que proporcionó una justificación sólida para la necesidad de la intervención propuesta.

Cumplimiento del Objetivo Específico 2 (Evaluar): Se cumplió a cabalidad con la evaluación de viabilidad, fundamentada en marcos normativos y técnicos. Se analizó el ecosistema de operadores biométricos certificados por la RNEC, se estudió el marco legal de la Ley 1581 de 2012 y se examinó el precedente operativo de la alianza RNEC-Asobancaria. Este análisis concluyó que la integración es técnicamente posible y operacionalmente escalable, pero con una restricción jurídica clave: el sistema debe ser siempre opcional para el ciudadano, ofreciendo alternativas de autenticación no biométricas para cumplir con la normativa y la jurisprudencia de la SIC. La viabilidad técnica se reforzó al alinear la propuesta con los Niveles de Aseguramiento del Autenticador (AAL) de las guías NIST SP 800-63.

Cumplimiento del Objetivo Específico 3 (Diseño): Este objetivo se materializó en la delineación de un modelo conceptual de cuatro capas (Interacción, Autenticación, Middleware y

RPA). El diseño no se realizó en el vacío, sino que se fundamentó en principios del Ciclo de Vida de Desarrollo Seguro (Secure SDLC) y se alineó con estándares internacionales como ISO/IEC 27001 para la gestión de la seguridad. Se detallaron los requisitos técnicos mínimos, los estándares de Ciberseguridad aplicables y se abordaron explícitamente los desafíos de interoperabilidad con sistemas legados, cumpliendo así con la necesidad de sustentar técnicamente la viabilidad del plan.

Proyecciones y Nuevos Desafíos

El presente trabajo, si bien concluye con un diseño conceptual, abre la puerta a nuevas líneas de investigación y desarrollo que pueden ampliar y profundizar su impacto.

Proyecciones del Sistema

Expansión Horizontal: El modelo conceptual es inherentemente modular y escalable. Podría adaptarse y replicarse en otras áreas críticas del sector público más allá de los trámites administrativos generales, como el sector salud (para la validación de pacientes y la prevención de fraudes en la dispensación de medicamentos), el sistema educativo (para la autenticación de estudiantes en plataformas de aprendizaje) y el sistema judicial (para el acceso seguro a expedientes digitales).

Profundización Tecnológica: La capa de RPA podría enriquecerse con algoritmos de Machine Learning para pasar de la automatización de tareas a la detección predictiva de fraudes, analizando patrones de comportamiento en tiempo real para identificar actividades anómalas.

Integración con la Cédula Digital: El sistema podría integrarse con la Cédula de Ciudadanía Digital, utilizándola como un autenticador de hardware para alcanzar el Nivel de Aseguramiento del Autenticador 3 (AAL3) de NIST, el más alto en seguridad.

Nuevos Desafíos y Futuras Investigaciones

Interoperabilidad con Sistemas Legados: El mayor desafío técnico para una implementación real es la interoperabilidad con los sistemas de información gubernamentales existentes, que a menudo operan en silos. Una línea de investigación futura podría centrarse en el diseño de "conectores" o "adaptadores" estandarizados para los sistemas legados más comunes en el Estado colombiano, facilitando la integración de tecnologías modernas.

Inclusión y Brecha Digital: ¿Cómo garantizar que este sistema no profundice la brecha digital? Se necesita investigar y diseñar canales de autenticación seguros alternativos para ciudadanos con acceso limitado a tecnología (Smartphone, internet de calidad) o con baja alfabetización digital, asegurando que la seguridad no se logre a costa de la exclusión.

La Amenaza de los Deepfakes: A medida que la inteligencia artificial generativa avanza, también lo hace la amenaza de los deepfakes para suplantar la identidad en sistemas biométricos. Una investigación futura crucial deberá enfocarse en el desarrollo y la evaluación de tecnologías de detección de vida (liveness detection) de próxima generación, capaces de distinguir de manera fiable entre un ser humano real y una falsificación generada por IA.

Gobernanza de Datos y Ética: La implementación de un sistema de esta naturaleza generará grandes volúmenes de metadatos sobre las transacciones. Esto abre un nuevo campo de investigación sobre la gobernanza de datos para sistemas de identidad digital en el sector público: ¿Quién debe auditar estos sistemas? ¿Cómo se garantiza la transparencia en su uso?

¿Qué políticas se deben implementar para prevenir el perfilamiento indebido de los ciudadanos? Desarrollar un marco de gobernanza ética y transparente será tan importante como la propia tecnología.

Recomendaciones

Para la continuidad del proyecto es indispensable asignar los recursos necesarios para su desarrollo.

Se recomienda revisar si en un futuro el sistema puede integrarse con los demás sistemas de información de manera interactiva, siendo un solo canal de información.

Analizar opciones diferentes para personas sordas mudas y el acceso al sistema, como personas con problemas en la piel difícil de leer la huella.

Brindar alternativas que permitan acercar más al ciudadano con discapacidad o limitaciones a las entidades asegurándole la seguridad de la información por medio de mecanismos tecnológicos y personal capacitado.

Referencias Bibliográficas

Arkavia Networks. (2017). *Clasificación de ciberdelincuentes.* www.arkavianetworks.com.

Bazurto-Mecias, C. J., Jurado Cabello, Y. K., Sifa Mueses, L. M., & Reinoso Paredes, A. G. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica,* 594-612.

Buolamwini, J. y Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency,* 77-91.

CAI Virtual de la Policía Nacional. (2019). Informe de denuncias por hurto a través de medios informáticos.

Centurión, J. B., Sánchez Silva y Sonia Gutiérrez Garcia. (s.f.). ¿Cómo proteger los datos personales? *Boletín Institucional - Instituto Nacional de Salud.*

Equipo Editorial - Boletín Jurídico Observatorio de libertad religiosa de América Latina y El Caribe. (2024). CHILE. Conferencia Episcopal -Mensaje- Ante el mal entendido de la corrupción. Se resalta la preocupación social generada por los casos de tráfico de influencias, fraudes, mal uso de información privilegiada, corrupción y malversación de fondos públicos. *Boletín Jurídico Observatorio de libertad religiosa de América Latina y El Caribe,* 19.

Foro Económico Mundial (2017). *Informe de Riesgos Globales 2017.*

Gómez-Bautista, C. y Calderón-Bocanegra, F. C. (2024). Enhancing facial recognition in surveillance systems through embedded super-resolution. *Revista Facultad de Ingeniería Universidad de Antioquia.*

Huacho, F. G. (2024). *Sistema de reconocimiento facial para el área administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil.* Universidad Católica de Santiago de Guayaquil.

Instituto de Auditores Internos de España. (2016). Ciberseguridad: una guía de supervisión.

Kuehl, D. T. (2009). *Operationalizing the Cyber Domain: Cyberpower and Strategy.*

Martínez-Tornés, B., Taburet, T., Boros, E., Rouis, K., Gomez-Krämer, P., Sidere, N., Poulain d'Andecy, V. (2023). *Jeu de données de tickets de caisse pour la détection de fraude documentaire.* HAL CCSD; ATALA.

Mecias, C. J., Yulexi Katherine Jurado Cabello, Luz Maria Sifa Mueses, & Alejandra Gabriela Reinoso Paredes. (2024). *La ciberdelincuencia y la protección de datos personales.*

Medina, R. (2016). La profesionalización del cibercrimen en Colombia. El Tiempo. MINTIC (2025). *Estrategia nacional de - seguridad digital de Colombia 2025 – 2027.*

Ortega, M. (2020). Desafíos de implementación de tecnologías biométricas en entornos corporativos. *Revista de Seguridad y Tecnología*, 15(3), 45-56.

Otero, M. R. (2024). El non bis in idem en los regímenes punitivos a los que se someten los servidores públicos en Colombia: ¿una garantía, en la práctica, inexistente? *Revista digital de Derecho Administrativo*, 35-67.

Pérez, C., Gómez, A., & Hernández, J. (2019). Sistemas de control de acceso biométricos: *Retos y oportunidades. Revista de Innovación Tecnológica*, 12(4), 33-42.

Pérez-Martínez, A. (2023). Análisis del delito de estafa desde la psicología forense: una propuesta interdisciplinaria. *Analysis of the crime of scam from forensic psychology: an interdisciplinary proposal.* https://research-ebsco-

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management.* Springer.

Revista Cubana de Ciencias Informáticas. (2022). Revisión de los métodos de reconocimiento facial en imágenes RGB-D adquiridas mediante un sensor Kinect . *Revista Cubana de Ciencias Informáticas*, 172-202.

Roda, S. (2024). Riesgos y desafíos vinculados a la asistencia en efectivo mediada por la biometría. *Revista Migraciones Forzadas.*

Rodríguez Ponce, K. J., Gutiérrez Sánchez, F. J., & Mendoza De los Santos, A. C. (2024).

Salinas, J. R. (2023). Auditoría forense en la era de la inteligencia artificial, un enfoque vanguardista para combatir el fraude financiero. *Revista Punto de Vista.*

Semana. (2017). Ciberdelincuentes y sus ataques a sistemas gubernamentales.

Semana. Symantec. (2019). *Informe de amenazas cibernéticas.* www.symantec.com

Sinergia Academica, (s.f.). Sistema de control de acceso biométrico mediante reconocimiento facial con técnicas de vivacidad. *Innovación y Software.*7, 594-612. https://research-ebsco- com.bibliotecavirtual.unad.edu.co/c/qcagk4/viewer/pdf/lkmqasax3f

TransUnion (2024). Informe sobre el Fraude Omnicanal en Colombia 2024 – *TransUnion.* https://www.transunion.co/fraud-trends/reports/2024-omnichannel-fraud-report.

Venkatesh, V.; Morris, M.; Davis, G. & Davis, F. (2003). User Acceptance of Information Technology: *Toward a Unified View. MIS Quarterly* 27(3):425-478.

Zhang, L., Wang, X., & Li, H. (2017). Deep learning for face recognition: A critical review. Journal of Computer Vision, 119(1), 1-21.