Análisis de las medidas de mitigación comunicadas con la ciberseguridad en el sector financiero colombiano en relación con la prevención de la suplantación biométrica

Ingrid Marcela Téllez Cerón

Asesor

Edgar Roberto Dulce Villarreal

Universidad Nacional Abierta y aDistancia - UNAD

Escuela Ciencias Básicas, Tecnología e ingeniería ECBTI

Ingeniería de sistemas

2025

Dedicatoria

Dedico este trabajo primeramente a Dios, quien me ha permitido llegar hasta aquí, También a mi Madre hermosa que siempre ha estado a mi lado motivándome para que pueda avanzar en mis estudios, y me ha infundado las ganas de superarme cada vez más, y salir adelante en este proyecto de vida.

Agradecimiento

Agradezco especialmente a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su asesoramiento continuo me motivan a aprender, y especialmente agradezco al asesor de curso Edgar Roberto Dulce Villareal, quien ha tenido bastante paciencia en explicarme paso a paso de esta Monografía, y quien me va a asesorar y orientar en esta nueva etapa de adquirir conocimiento nuevo día a día.

Resumen

Los sistemas biométricos son una tecnología que permite tomar, registrar y comparar las características físicas o datos biométricos de las personas para autenticarlas o identificarlas correctamente.

En Colombia, el sector financiero utiliza la biometría para autentificar plenamente a sus usuarios, se utilizan estas herramientas para identificar a sus clientes con eficacia.

Algunos ejemplos de rasgos que se utilizan son las huellas dactilares, el iris, el reconocimiento facial y la voz, el propósito de la biometría financiera es confirmar la identidad del usuario y prevenir la suplantación y el fraude en transacciones y operaciones financieras.

Al implementar este método, no se necesitan contraseñas, tarjetas o números PIN. La biometría financiera se implementa para asegurar la autenticación y proteger la información de los usuarios contra el fraude y los posibles delitos financieros.

En el sector financiero colombiano, se emplean herramientas de ciberseguridad para evitar la suplantación por parte de ciberdelincuentes, aunque no todas son adecuadas, eficientes, efectivas suficientes o contundentes.

Las medidas que se están utilizando en la actualidad para este problema, serán las adecuadas.

Palabras clave Fraude, Suplantación, Biométrica, Colombiano, Huella.

Abstract

Biometric systems are a technology that allows taking, recording, and comparing the physical characteristics or biometric data of people to authenticate or identify them correctly.

In Colombia, the financial sector uses biometrics to fully authenticate its users; these tools are used to identify their clients effectively.

Some examples of traits used are fingerprints, iris, facial recognition, and voice.

The purpose of financial biometrics is to confirm the identity of the user and prevent impersonation and fraud in financial transactions and operations.

When implementing this method, no passwords, cards, or PIN numbers are needed. Financial biometrics are implemented to ensure authentication and protect user information against fraud and potential financial crimes.

In the Colombian financial sector, cybersecurity tools are used to avoid impersonation by cybercriminals, although not all of them are adequate, efficient, effective, sufficient, or forceful.

The measures that are currently being used for this problem will be appropriate.

Keywords: Fraud, Impersonation, Biometric, Colombian, Fingerprint

Tabla de Contenido

Lista de Figuras

Introducción

En los últimos años, el avance de la tecnología ha revolucionado la forma en que se llevan a cabo las operaciones financieras. Sin embargo, este progreso también ha traído consigo nuevos desafíos en cuanto a la seguridad de los datos personales y financieros de los usuarios, es por eso por lo que las entidades financieras en Colombia han decidido implementar sistemas biométricos como medida de seguridad adicional, esta tecnología utiliza características físicas o comportamentales únicas de cada individuo, como huellas dactilares, reconocimiento facial o de voz, para verificar su identidad de manera precisa y confiable.

La implementación de sistemas biométricos en el sector financiero tiene como objetivo Agilizar las operaciones y generar confianza entre los usuarios, con esta tecnología, los clientes pueden realizar transacciones de forma más rápida y sencilla, sin la necesidad de recordar contraseñas o llevar consigo tarjetas y dispositivos de seguridad.

Sin embargo, es importante cuestionar si estas medidas son suficientes, y eficientes para garantizar la seguridad de la información en el sector financiero, a pesar de la implementación de sistemas biométricos, la suplantación biométrica sigue siendo un riesgo latente que debe ser abordado de manera integral.

En la siguiente monografía se analizarán las medidas de ciberseguridad implementadas en el sector financiero colombiano, se validará si las tecnologías biométricas son idóneas y suficientes para mitigar los riesgos de suplantación y fraude financiero, además, se examinará la legislación y regulación existente en materia de protección de datos personales y las políticas de seguridad adoptadas por las entidades financieras.

Formulación del Problema

Cada día la ciberdelincuencia, crea estrategias para vulnerar los sistemas Biométricos financieros en Colombia, para suplantar la identidad de los usuarios y crear un ambiente idóneo, para cometer fraudes con cifras millonarias, que obviamente afectan al usuario en las entidades financieras, esto puede ocurrir por varias razones, como la falta de seguridad en los sistemas biométricos utilizados, la vulnerabilidad de los dispositivos biométricos, el robo de información biométrica o la manipulación de la tecnología biométrica.

En algunos casos, la suplantación biométrica puede tener graves consecuencias, como el robo de identidad, la falsificación de documentos o la comisión de fraudes, es importante que las organizaciones y usuarios sean conscientes de los riesgos de la suplantación biométrica y tomen medidas para proteger su información biométrica y prevenir este tipo de fraude, esto lleva a realizar el siguiente cuestionamiento.

¿Las Medidas de mitigación implementadas por la ciberseguridad en el sector financiero en Colombia específicamente son efectivas y confiables para prevenir la suplantación Biométrica?

Antecedentes del Problema

La implementación de la biometría usa las características únicas de una persona llámese Iris, huella, voz, rostro, para autenticar la identidad de una persona, estos sistemas son muy apetecidos gracias a nivel de precisión y seguridad.

Por eso el sistema financiero adopto este método desde el 2011, cuando se empezó a implementar en algunos bancos, pero la Superentendía Financiera de Colombia en 2014 estableció las regulaciones para la implementación del sistema biométrico en las entidades financieras del país y en 2015 empezó sus implementaciones en el sector financiero, este sector ha implementado cada vez la utilización de la biometría, para sus operaciones, también ha surgido muchos desafíos para la ciberseguridad frente a la suplantación biométrica, cada día la ciberdelincuencia se ha valido, de estrategias cada vez más imperceptibles para manipular y suplantar a los usuarios y realizar robos de identidad y fraudes millonarios. (Ramirez, 2015)

Esto ha revelado la necesidad de implementar medidas de mitigación efectivas para prevenir la suplantación biométrica y proteger la integridad de los sistemas financieros en Colombia.

Justificación

Desde finales de los años 90, el sector financiero en Colombia ha utilizado la biometría como método de verificación de la identidad de sus clientes, inicialmente, se implementaron lectores de huellas dactilares, pero con el tiempo se han desarrollado otros métodos biométricos, como el reconocimiento facial y de voz, el objetivo de estos avances es mejorar la seguridad en los sistemas financieros del país.

A pesar de la implementación de estas tecnologías, el número de estafas digitales en el sistema financiero colombiano ha aumentado notablemente en los últimos años.

La mayoría de los casos de fraude en el sector financiero están relacionados con la suplantación de identidad en compras en línea, el uso de aplicaciones móviles y la falsificación de tarjetas de crédito, Bogotá ha registrado la mayor cantidad de casos de suplantación, seguida de Medellín, Cali, Barranquilla, Bucaramanga y Cartagena.

Una de las formas más comunes de suplantación de identidad es a través de correos electrónicos fraudulentos, esto muestra la importancia de implementar medidas más eficientes para prevenir este tipo de delitos, durante la primera mitad de 2021, los delitos cometidos con tarjetas de crédito aumentaron un 70%, los fraudes en Colombia crecieron un 243% y los intentos de robo se incrementaron en un 61% esto es una cifra bastante alta lo cual pone en Jake a las entidades financieras. (Gomez f., 2021)

En la era tecnológica en la actualidad, es crucial mantenerse a la vanguardia de la innovación en todos los sectores, especialmente en la protección de la información personal y financiera, la biometría se ha presentado como una solución para combatir la suplantación de Identidad, ya que permite identificar a los usuarios a través de características únicas, como las huellas digitales, la retina, la palma de la mano, la voz y el reconocimiento de escritura.

A pesar de los avances en la implementación de tecnologías biométricas en el sector financiero colombiano, el número de casos de suplantación de identidad ha aumentado de manera preocupante, esto plantea la necesidad de evaluar la eficacia de las medidas de seguridad implementadas y desarrollar estrategias más efectivas para combatir esta problemática.

La protección de la información y la seguridad de los usuarios son aspectos fundamentales en un entorno digitalizado, sin embargo es importante tener en cuenta que la biometría no es un sistema completamente infalible, por lo tanto es necesario analizar la eficacia de este sistema frente a los ciberdelincuentes, evaluar las herramientas de ciberseguridad utilizadas para combatir la suplantación biométrica en el sector financiero y asegurarse de que se estén tomando las medidas adecuadas para mitigar los riesgos asociados en Colombia.

Objetivos

Objetivo General

Analizar las acciones específicas en el campo de la ciberseguridad para abordar y prevenir la suplantación biométrica en el sector financiero colombiano a través de revisión bibliográfica y análisis de datos proporcionados por entidades relevantes en el tema.

Objetivos Específicos

Identificar las características principales de la suplantación biométrica en el sector financiero en Colombia, incluyendo los métodos utilizados, los riesgos asociados y los impactos en la seguridad de la información mediante una revisión bibliográfica y análisis de datos proporcionados por entidades relevantes en el tema.

Evaluar la eficacia de las acciones de ciberseguridad emitidas por la Superintendencia Financiera y las implementadas por las entidades bancarias en Colombia para prevenir la suplantación biométrica, a través de análisis de vulnerabilidades detectadas.

Formular recomendaciones basadas en las mejores prácticas identificadas durante la investigación, para establecer un marco de prevención de la suplantación biométrica en el sector bancario colombiano, considerando aspectos técnicos, legales y éticos para mejorar la seguridad de las transacciones financieras.

Antecedentes o Estado Actual

Dentro de los sistemas biométricos que se utilizan en Colombia en el sector financiero se destacan los siguientes:

Bancos Que Utilizan La Biometría En La Actualidad

Bancolombia utiliza la huella dactilar como método de identificación biométrica en sus servicios de banca móvil y en algunos cajeros automáticos.

Banco de Bogotá Ofrece la opción de utilizar la huella dactilar como método de autenticación en sus servicios de banca en línea y banca móvil.

Davivienda implementa la autenticación biométrica a través de la huella dactilar en algunos de sus procesos de seguridad, como la verificación de identidad en sus cajeros automáticos.

BBVA Colombia Ofrece la opción de utilizar la huella dactilar como método de autenticación en su aplicación de banca móvil.

Banco Popular utiliza la autenticación biométrica mediante la huella dactilar en sus servicios de banca móvil y banca en línea.

La entidad Asobancaria en 2019 muestra que el 70% de los bancos del país emplean algún tipo de biometría para la autenticación de sus clientes, las principales instituciones financieras, como Bancolombia, Davivienda y BBVA Colombia, han adoptado la tecnología biométrica en sus sistemas de seguridad. (Jhonatan, s.f.)

La aplicación de la biometría también ha facilitado la experiencia del cliente al eliminar la necesidad de recordar múltiples contraseñas y códigos de seguridad. Según un estudio

realizado por BDO Colombia en 2018, el 80% de los clientes bancarios encuestados afirmaron sentirse más seguros al utilizar la autenticación biométrica en lugar de contraseñas tradicionales.

Por otro lado, durante el 14° Congreso de Prevención del Fraude y Seguridad, Asobancaria y Certicámara presentaron los avances del programa de biometría dactilar en el sector financiero, ambas organizaciones afirman que este programa ha protegido más de 60 millones de transacciones en el sector, contribuyendo así a la seguridad de bancos y usuarios mediante el uso de la biometría dactilar, según Hernando José Gómez, presidente de Asobancaria, este programa ha permitido por primera vez que las entidades financieras tengan acceso a la biometría oficial del país, la implementación de esta tecnología biométrica ha mejorado significativamente el proceso de acceso a los servicios financieros, garantizando altos niveles de seguridad, eficiencia y una mejor experiencia para los clientes y usuarios financieros en Colombia. (Gomez, 2019)

La seguridad de los datos de los clientes es fundamental para los bancos, debido a las diversas formas de fraude y robo utilizadas por los delincuentes en la actualidad, según el presidente de Asobancaria, la industria bancaria se destaca por cumplir con altos estándares en la protección y manejo de datos personales, demostrando un mayor desempeño en comparación con otras industrias, como resultado tanto Asobancaria como el sector financiero están enfocados en desarrollar pilotos de biometría facial en colaboración con la Registraduría Nacional y sus agremiadas, Certicámara, por su parte, ha manifestado su interés en participar en el piloto para implementar esta tecnología en Colombia y ya cuenta con programas que ofrecen seguridad y confiabilidad para los usuarios en la lucha contra la suplantación de identidad. (Moncayo, s.f.)

Martha Moreno, presidenta ejecutiva de Certicámara, destaca que la biometría facial ya es una realidad en Colombia, esta tecnología permite hacer una verificación facial en vivo,

conocida como "Facial livenses detection”, comparando el rostro con las imágenes de las bases de datos de la Registraduría, esto garantiza que la validación de identidad no se realice utilizando imágenes fácilmente alterables, sino que se base en información biométrica administrada por la autoridad competente en este campo, la incorporación de la biometría facial en las transacciones digitales agregará tecnología y seguridad adicional. (Moreno, 2021)

la implementación de la Biometría dactilar en el sector financiero ha sido exitosa en la mitigación del riesgo de suplantación de identidad reduciéndolo en un 98%, gracias al cotejo de huellas dactilares se han protegido más de 60 millones de transacciones en el sector financiero. Además, cada mes se realizan entre 1,1 y 1,3 millones de validaciones biométricas de huella digital en línea por parte de usuarios y clientes financieros, los cotejos dactilares realizados por Certicámara representan el 65% de todos los cotejos realizados en Colombia con las bases de datos de la Registraduría. (https://www.registraduria.gov.co/, s.f.)

Marco Conceptual

Objeto De La Biometría En El Sector Financiero

Los sistemas biométricos se incluyeron en los bancos a través de la superintendencia financiera en el año 2016, está la incluye en el sector financiero con el fin de utilizar características físicas o comportamentales únicas para identificar a las personas de manera precisa y confiable. Algunos de los principales motivos para su creación son:

Mejorar la seguridad. La biometría permite establecer sistemas de identificación más seguros que no pueden ser fácilmente falsificados, esto es especialmente útil en áreas como la seguridad de acceso a instalaciones o sistemas informáticos.

Simplificar y agilizar procesos de identificación a través de la biometría no es necesario recordar contraseñas o portar documentos físicos de identificación, además los sistemas

biométricos pueden ser rápidos y eficientes lo que facilita el acceso a servicios y reduce el tiempo de espera. (Santiago, s.f.)

Prevenir fraudes y suplantaciones de identidad.

Al utilizar características únicas y difíciles de reproducir, los sistemas biométricos ayudan a prevenir la suplantación de identidad y minimizar el riesgo de fraudes, para el sistema financiero era muy necesario utilizar nuevas técnicas para reconocer a sus usuarios de una forma eficaz y de forma segura, además para que ellos pudiesen acceder a servicios financieros, para ello implementaron los sistemas biométricos que consisten en reconocer al usuario de forma segura, para este sector especialmente en Colombia era importante tener ofrecer facilidad para las transacciones bancarias para los usuarios.

En la nueva era tecnológica y debido a su evolución, requiere nuevos desafíos frente a los sistemas biométricos, para ello ha implementado sistemas biométricos lo cual ofrece a sus clientes beneficios en términos de seguridad y eficiencia, para esto la superintendencia financiera de Colombia ha implementado, la autenticación por medio de sistemas biométricos para asegurar que los procesos financieros se realizan correctamente.

Pero qué pasa cuando la ciberseguridad a pesar de sus esfuerzos no ha podido mitigar la suplantación biométrica en el sector financiero colombiano, que pasa cuando la ciberdelincuencia crea estrategias cada vez más innovadoras para vulnerar el sistema, a continuación, se mencionaran los sistemas más utilizados para vulnerar los sistemas biométricos en Colombia.

Amenazas de Usuario

Usuarios que tienen permiso proporcionan su información biométrica sin saberlo, bajo amenaza o intencionalmente a un impostor, esta captura la muestra biométrica de un usuario

autorizado, como una fotografía de su rostro o una grabación de su voz ,el impostor roba la información biométrica de un usuario autorizado, un usuario autorizado proporciona voluntariamente su información biométrica al impostor, un usuario autorizado modifica su información biométrica para facilitar un ataque por parte del impostor. (Incibe, s.f.)

Amenazas de Usuario Captura de muestra biométrica.

El impostor presenta una muestra biométrica falsa, como una huella digital de gelatina o una grabación de voz, para hacerse pasar por un usuario autorizado, posteriormente el impostor presenta una muestra biométrica de baja calidad con el objetivo de coincidir con una muestra biométrica débil o de baja calidad, el ciberdelincuente utiliza una imagen biométrica residual, como una huella dactilar latente, dejada en el sistema biométrico para hacerse pasar por el último usuario autorizado.

El impostor presenta su propia muestra biométrica después de que esta haya sido:

Alterada de forma efectiva, otro método empleado por los ciberdelincuentes es el impostor intercepta una muestra biométrica autorizada durante la transmisión entre los subsistemas de Captura y Extracción., el impostor inserta directamente una muestra biométrica autorizada en el subsistema de Extracción, Comparación durante la Verificación, el impostor intercepta las características biométricas extraídas durante la transmisión entre los subsistemas de extracción y Comparación.

El impostor inserta directamente las características biométricas extraídas en el subsistema de Comparación. almacenamiento de la muestra durante la Inscripción,

Un usuario autorizado presenta una muestra biométrica de baja calidad, con ruido y variaciones, o presenta una muestra falsa para crear y almacenar un patrón biométrico débil, un

usuario no autorizado queda registrado debido a un error del administrador, la intercepción del patrón de un usuario autorizado y su reemplazo por el patrón del impostor. (Lefevre, 2020)

El impostor roba el patrón biométrico de un usuario autorizado del medio de almacenamiento o de otro sistema biométrico, el atacante modifica o elimina los patrones biométricos almacenados, el impostor intercepta el patrón biométrico autorizado durante la transmisión entre los subsistemas de extracción y almacenamiento del patrón.

El impostor intercepta una muestra biométrica autorizada durante la transmisión entre los subsistemas de almacenamiento del patrón y comparación, el impostor inserta directamente su propio patrón en el subsistema de usuario autorizado hostil puede adquirir privilegios de administrador a través de medios no biométricos, como contraseñas o sistemas de respaldo, y así modificar el umbral de comparación, los privilegios de los usuarios, permitir el acceso no autorizado a los patrones almacenados o inscribir a un usuario no autorizado.

El atacante corta la fuente de energía del sistema biométrico.

El atacante obtiene acceso no autorizado a los privilegios con o sin ayuda de un usuario autorizado después de que el usuario ha sido autenticado. (Castro, 2020)

Sin embargo, es importante tener en cuenta preocupaciones de privacidad y protección de datos en la implementación de sistemas biométricos, los usuarios deben tener la confianza de que sus datos biométricos serán almacenados y utilizados de manera segura y ética, las instituciones financieras deben garantizar la adopción de políticas de seguridad y cumplimiento regulatorio, así como la obtención de consentimiento expreso de los usuarios para el uso de sus datos Biométricos.

Marco Teórico

Para hablar de marco teórico se tiene que hablar del concepto de biometría y cómo funciona, la biometría este es un mecanismo de reconocimiento de personas basado en sus características fisiológicas o de comportamiento, cuando se refiere a fisiológico hace referencia al reconocimiento de huella dactilar, de iris retina y de rostro, voz, venas entre otros:

Huella

Las huellas dactilares consisten en un patrón único de crestas y surcos presentes en la piel de los dedos, esta característica es utilizada para identificar y distinguir a cada individuo.

La técnica de identificación a través de las huellas dactilares es altamente confiable, ya que se considera que es prácticamente imposible encontrar dos personas con huellas idénticas.

También estas son utilizadas en tecnología de dispositivos electrónicos para desbloquear y autorizar transacciones en este caso el sistema financiero. (Cena 2018)

Figura 1 se observan los surcos que se tienen en cuenta, para la identificación de una persona a través de la huella dactilar.

Figura 1

Huella Dactilar

Nota. La huella dactilar es la impresión de las crestas y surcos de la piel que se encuentran en las yemas de los dedos Tomado de (Cena, 2018)

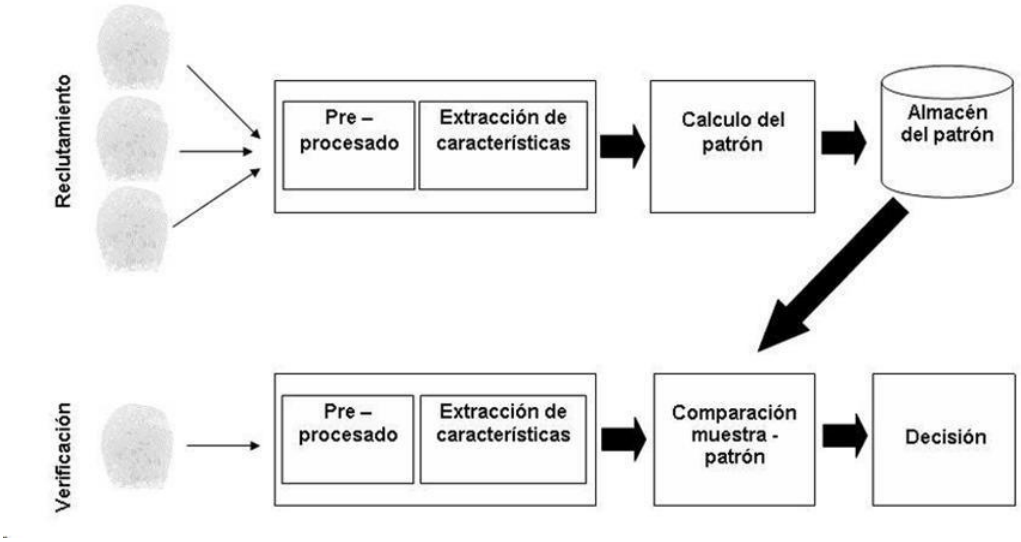
Etapas De Un Sistema Biométrico

Estas son las etapas que realiza en sistema biométrico en sus procesos de identificación, realiza el proceso de reclutamiento en este se da el preprocesado, la extracción de las características, el cálculo del patrón pasa al almacén del patrón, luego se verifica a través de la Comparación de muestra patrón, y el sistema identifica plenamente al usuario.

En la figura 2, se observa las etapas del sistema biométrico, el proceso que conlleva a la identificación de la huella dactilar.

Figura 2

Etapa de un Sistema Biométrico



Nota. Etapa de un sistema Biométrico es el proceso para la identificación y verificación de la huella dactilar Tomado de (Moreno I. , 2017)

Iris

El iris se encuentra en el área circular y coloreada alrededor de la pupila, y contiene patrones únicos en forma de fibras y múltiples texturas que no cambian a lo largo de la vida de una persona, esto lo convierte en un medio altamente confiable para la identificación biométrica, ya que la probabilidad de encontrar dos iris iguales es extremadamente baja.

El proceso de escaneo del iris se realiza utilizando una cámara especializada que captura una imagen de alta resolución del iris, luego, se extraen y analizan los patrones específicos del iris utilizando algoritmos sofisticados, que los convierten en una serie de características numéricas conocidas como "códigos de plantilla".

Estos códigos de plantilla se comparan con una base de datos previamente almacenada de iris conocidos para determinar la identidad de una persona, si existe una coincidencia cercana o exacta, el sistema de reconocimiento biométrico considera que la persona es autenticada.

El reconocimiento del iris en biometría es muy acertado, ya que permite conocer patrones únicos, este mecanismo es inalterable a lo largo de nuestra existencia, este mecanismo se realiza por medio de una cámara infrarroja, el reconocimiento está disponible incluso de noche o en la oscuridad, la biometría ocular es efectiva para identificar a las personas, pero según

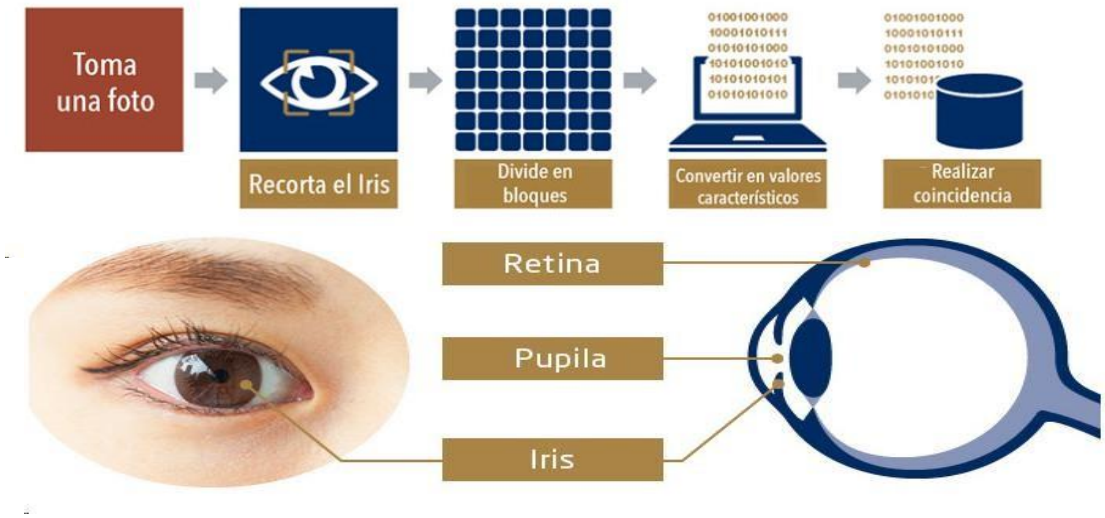
investigaciones, hay diferencias significativas y clínicas en la longitud y curvatura del ojo entre hombres y mujeres, las mujeres tienden a tener ojos más cortos y corneas más curvas.

No obstante, la edad también influye en estos aspectos y es necesario analizarlos detalladamente, lo que se puede deducir de este estudio es que la biometría ocular es efectiva para la identificación tanto de hombres como mujeres (Fedtke C, 2020).

En la figura 3 Se observa el. Proceso de código plantilla, que es el método para que el lector reconozca en este caso el Iris, como método de autenticación. (Cruz, 2020**)**

Figura 3

Codigo Plantilla



Nota. el proceso de código plantilla es el proceso para que el lector reconozca en este caso el iris Tomado de *(Cruz, Belltech, 2023).*

Biometría facial

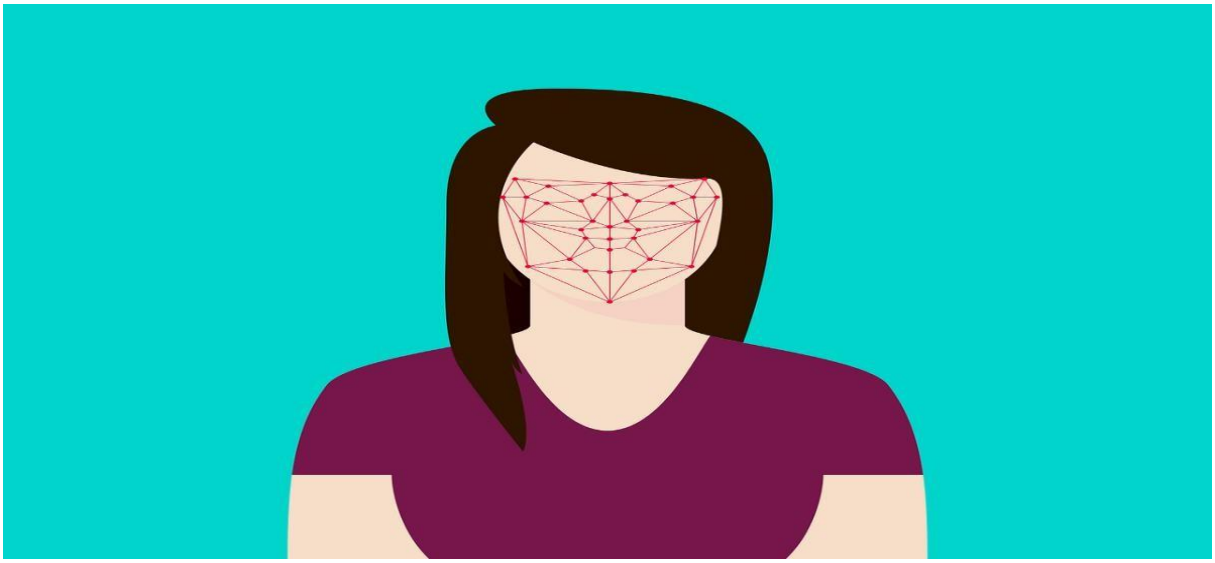
El análisis de biometría facial es una tecnología empleada para reconocer a las personas a través del estudio de sus características faciales únicas, se aprovecha de algoritmos y cámaras de alta definición para capturar y analizar aspectos distintivos del rostro, como la forma, las proporciones de los ojos, nariz y boca, así como detalles más específicos como arrugas o barba incipiente, esta tecnología se utiliza extensamente en sistemas de seguridad y control de acceso, ya que ofrece una manera precisa y rápida de identificar a las personas sin necesidad de contacto físico.

Los principales sistemas de reconocimiento facial incluyen Amazon Rekognition, Kairos, Affectiva, Microsoft Face API y OpenCV FaceRecognizer, estos sistemas utilizan algoritmos de visión por computadora y aprendizaje automático para detectar y analizar rostros, así como para identificar emociones, características demográficas y atributos faciales, cada sistema tiene sus propias fortalezas y debilidades, pero todos están enfocados en mejorar la precisión y la eficacia del reconocimiento facial. (https://www.bilib.com., s.f.)

En la figura 4, se muestran los ángulos que reconoce el lector biométrico para el reconocimiento facial**.**

Figura 4

Biometría Facial



Nota. Biometría facial es la alineación de algoritmos, para iniciar el reconocimiento facial.

Tomado de (https://alicebiometrics.com/, 2018).

Marco Científico o Tecnológico

En el sector financiero el sistema biométrico, utiliza las características físicas como se han mencionado anteriormente como lo son, la huella dactilar, el iris, la voz firma, patrones de venas entre otros para autenticar la identidad del usuario, en Colombia esta tecnología ha sido implementada en varios sectores financieros, esto se hace con el fin de proteger los datos y las transacciones financieras.

Para ello el sector financiero en Colombia se vale de los sistemas biométricos, el cual recopila esta información utilizando diferentes dispositivos de captura, como escáneres de huellas dactilares, cámaras para el reconocimiento del rostro o el iris, micrófonos para captar la voz, entre otros, estos dispositivos convierten las características biométricas en datos digitales, que pueden ser almacenados y procesados, a través de las características biométricas han sido capturadas y convertidas en datos digitales, se utilizan algoritmos y técnicas de reconocimiento para comparar y verificar la información con una base de datos de referencia, este proceso implica la comparación de patrones biométricos y la búsqueda de coincidencias.

Los algoritmos utilizados en el sistema biométrico pueden variar según la tecnología utilizada, algunos algoritmos comunes incluyen algoritmos de reconocimiento facial, de huella dactilar, de reconocimiento de iris, de reconocimiento de voz etc. (completa, s.f.)

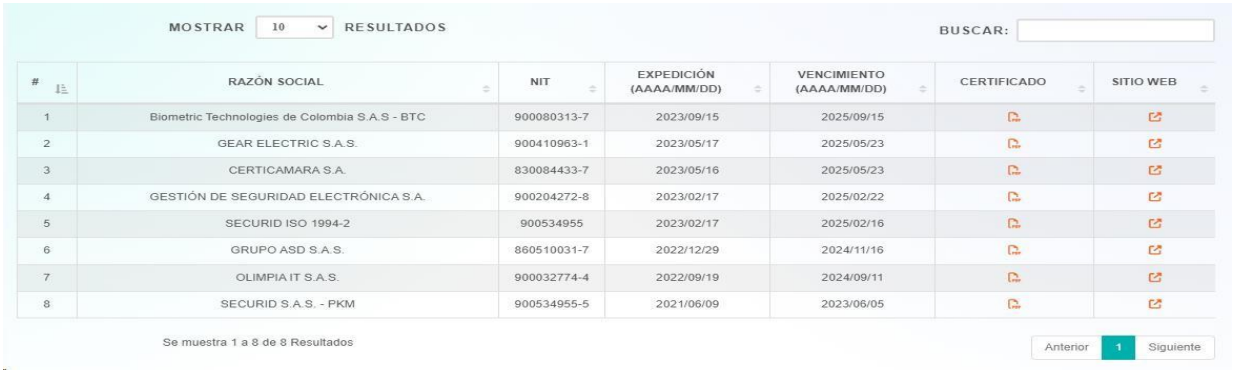
Una vez que se ha verificado la identidad de una persona utilizando el sistema biométrico, se pueden llevar a cabo diversas acciones, como el acceso a un lugar seguro, la autenticación en un sistema informático, la autorización de una transacción, entre otros.

A continuación, se mencionan los operadores biométricos que maneja la registraduría nacional del estado civil en Colombia, este organismo en atención a la normatividad vigente la

Registraduría Nacional del Estado Civil certifica a los aliados tecnológicos a través de los cuales las entidades públicas y particulares autorizados por la ley, podrán acceder al proceso de autenticación biométrica, conforme a lo establecido en el artículo 19 de la Resolución 5633 de 2016**.**

En la figura 9 se muestran los operadores vigentes según la registraduría Nacional del estado civil en Colombia.

Figura 9 *Operadores Biométricos Vigentes*



MOSTRAR 10 RESULTADOS BUSCAR:

#	RAZÓN SOCIAL	NIT	EXPEDICIÓN (AAAA/MM/DD)	VENCIMIENTO (AAAA/MM/DD)	CERTIFICADO	SITIO WEB
1	Biometric Technologies de Colombia S.A.S - BTC	900080313-7	2023/09/15	2025/09/15		
2	GEAR ELECTRIC S.A.S.	900410963-1	2023/05/17	2025/05/23		
3	CERTICAMARA S.A.	830084433-7	2023/05/16	2025/05/23		
4	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.	900204272-8	2023/02/17	2025/02/22		
5	SECURID ISO 1994-2	900534955	2023/02/17	2025/02/16		
6	GRUPO ASD S.A.S.	860510031-7	2022/12/29	2024/11/16		
7	OLIMPIA IT S.A.S.	900032774-4	2022/09/19	2024/09/11		
8	SECURID S.A.S. - PKM	900534955-5	2021/06/09	2023/06/05		

Se muestra 1 a 8 de 8 Resultados

Anterior 1 Siguiente

Nota. Operadores Biométricos Vigentes estos son los operadores autorizados por la registraduría para prestar el servicio de identificación biométrica. Tomado de (https://www.registraduria.gov.co/, Biometria, 2023).

Figura 10

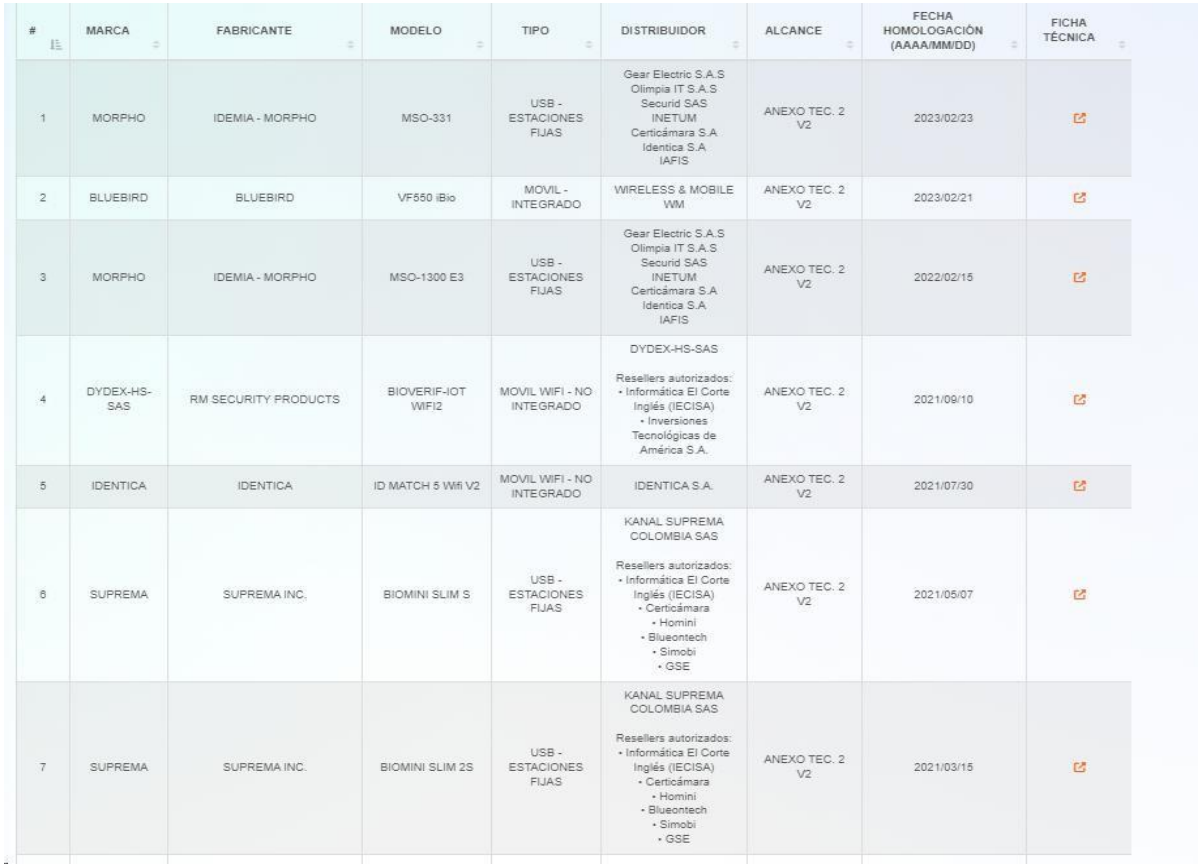
Certificado Operador Biométrico

Nota. el certificado que emite la registraduría nacional del estado civil en este caso de Colombia, a los operadores biométricos que ellos previamente han autorizado. Tomado de (https://www.registraduria.gov.co/, Biometria, 2023)

En la figura 11 se ven los operadores biométricos que son previamente autorizados por la registraduría Nacional del registro civil en Colombia, para ellos existe esta lista que son los únicos avalados por la registraduría.

Figura 11

Dispositivos Biométricos



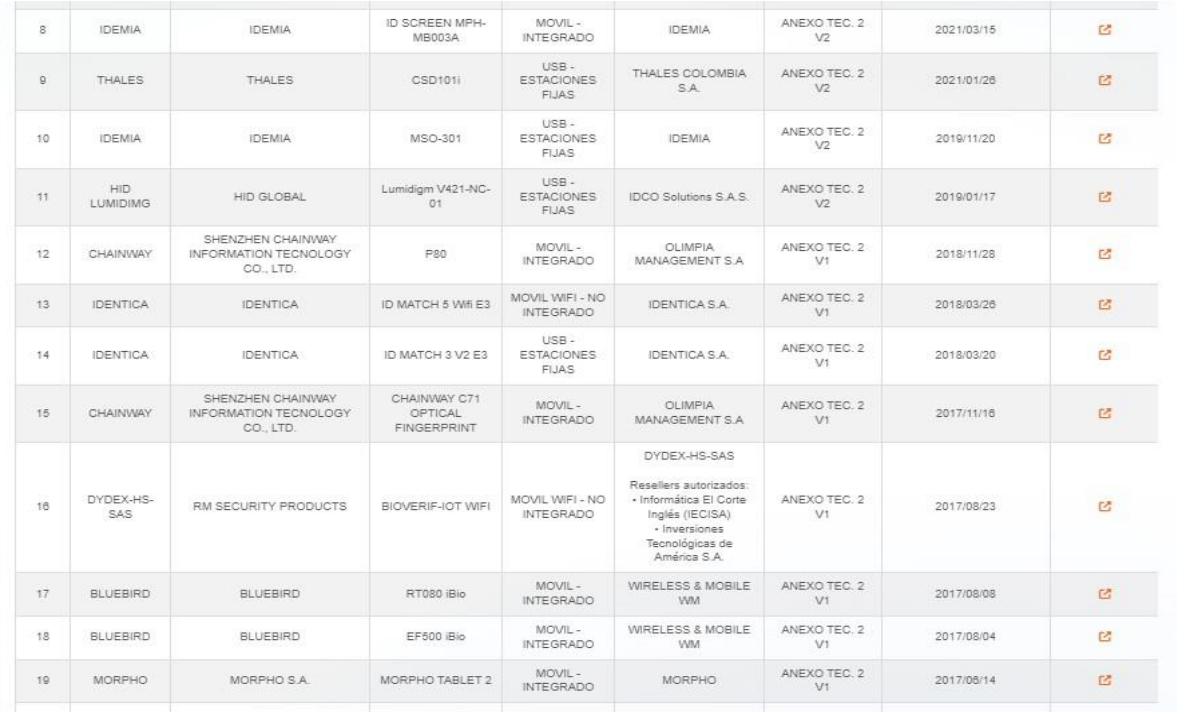
#	MARCA	FABRICANTE	MODELO	TIPO	DISTRIBUIDOR	ALCANCE	FECHA HOMOLOGACIÓN (AAAA/MM/DD)	FICHA TÉCNICA
1	MORPHO	IDEMIA - MORPHO	MSO-331	USB - ESTACIONES FIJAS	Gear Electric S.A.S Olimpia IT S.A.S Securid SAS INETUM Certicámara S.A Identica S.A IAFIS	ANEXO TEC. 2 V2	2023/02/23	
2	BLUEBIRD	BLUEBIRD	VF550 iBio	MOVIL - INTEGRADO	WIRELESS & MOBILE WM	ANEXO TEC. 2 V2	2023/02/21	
3	MORPHO	IDEMIA - MORPHO	MSO-1300 E3	USB - ESTACIONES FIJAS	Gear Electric S.A.S Olimpia IT S.A.S Securid SAS INETUM Certicámara S.A Identica S.A IAFIS	ANEXO TEC. 2 V2	2022/02/15	
4	DYDEX-HS-SAS	RM SECURITY PRODUCTS	BIOVERIF-IOT WIFI2	MOVIL WIFI - NO INTEGRADO	DYDEX-HS-SAS Resellers autorizados: • Informática El Corte Inglés (IECISA) • Inversiones Tecnológicas de América S.A.	ANEXO TEC. 2 V2	2021/09/10	
5	IDENTICA	IDENTICA	ID MATCH 5 Wifi V2	MOVIL WIFI - NO INTEGRADO	IDENTICA S.A.	ANEXO TEC. 2 V2	2021/07/30	
6	SUPREMA	SUPREMA INC.	BIOMINI SLIM S	USB - ESTACIONES FIJAS	KANAL SUPREMA COLOMBIA SAS Resellers autorizados: • Informática El Corte Inglés (IECISA) • Certicámara • Homini • Blueontech • Simobi • GSE	ANEXO TEC. 2 V2	2021/05/07	
7	SUPREMA	SUPREMA INC.	BIOMINI SLIM 2S	USB - ESTACIONES FIJAS	KANAL SUPREMA COLOMBIA SAS Resellers autorizados: • Informática El Corte Inglés (IECISA) • Certicámara • Homini • Blueontech • Simobi • GSE	ANEXO TEC. 2 V2	2021/03/15	

Nota. los operadores biométricos que son previamente autorizados por la registraduría Nacional del registro civil en Colombia Tomado de (https://www.registraduria.gov.co/, Biometria, 2023)

En la figura 12 se observa la otra lista de operadores biométricos que son previamente autorizados por la registraduría Nacional del registro civil en Colombia, para ellos existe esta lista que son los únicos avalados por la registraduría.

Figura 12

Lista Dispositivos Biométricos



8	IDEMIA	IDEMIA	ID SCREEN MPH-MB003A	MOVIL - INTEGRADO	IDEMIA	ANEXO TEC. 2 V2	2021/03/15	
9	THALES	THALES	CSD101i	USB - ESTACIONES FIJAS	THALES COLOMBIA S.A.	ANEXO TEC. 2 V2	2021/01/26	
10	IDEMIA	IDEMIA	MSO-301	USB - ESTACIONES FIJAS	IDEMIA	ANEXO TEC. 2 V2	2019/11/20	
11	HID LUMIDIMG	HID GLOBAL	Lumidigm V421-NC-01	USB - ESTACIONES FIJAS	IDCO Solutions S.A.S.	ANEXO TEC. 2 V2	2019/01/17	
12	CHAINWAY	SHENZHEN CHAINWAY INFORMATION TECNOLOGY CO., LTD.	P80	MOVIL - INTEGRADO	OLIMPIA MANAGEMENT S.A	ANEXO TEC. 2 V1	2018/11/28	
13	IDENTICA	IDENTICA	ID MATCH 5 Wifi E3	MOVIL WIFI - NO INTEGRADO	IDENTICA S.A.	ANEXO TEC. 2 V1	2018/03/26	
14	IDENTICA	IDENTICA	ID MATCH 3 V2 E3	USB - ESTACIONES FIJAS	IDENTICA S.A.	ANEXO TEC. 2 V1	2018/03/20	
15	CHAINWAY	SHENZHEN CHAINWAY INFORMATION TECNOLOGY CO., LTD.	CHAINWAY C71 OPTICAL FINGERPRINT	MOVIL - INTEGRADO	OLIMPIA MANAGEMENT S.A	ANEXO TEC. 2 V1	2017/11/16	
16	DYDEX-HS-SAS	RM SECURITY PRODUCTS	BIOVERIF-IOT WIFI	MOVIL WIFI - NO INTEGRADO	DYDEX-HS-SAS Resellers autorizados: • Informática El Corte Inglés (IECISA) • Inversiones Tecnológicas de América S.A.	ANEXO TEC. 2 V1	2017/08/23	
17	BLUEBIRD	BLUEBIRD	RT080 iBio	MOVIL - INTEGRADO	WIRELESS & MOBILE WM	ANEXO TEC. 2 V1	2017/08/08	
18	BLUEBIRD	BLUEBIRD	EF500 iBio	MOVIL - INTEGRADO	WIRELESS & MOBILE WM	ANEXO TEC. 2 V1	2017/08/04	
19	MORPHO	MORPHO S.A.	MORPHO TABLET 2	MOVIL - INTEGRADO	MORPHO	ANEXO TEC. 2 V1	2017/06/14	

Nota. lista de operadores biométricos que son previamente autorizados por la Registraduría Nacional en Colombia Tomado de (https://www.registraduria.gov.co/, Biometria, 2023).

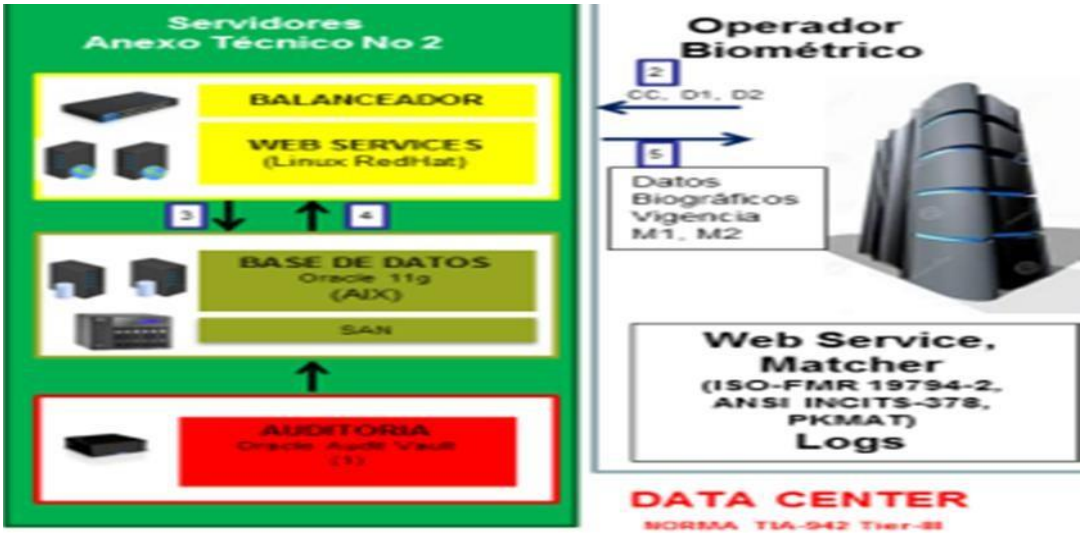
El Proceso De Autenticación Biométrica Dactilar

Este es un proceso probabilístico, el cual, al momento de realizar la transacción de cotejo de la huella de un ciudadano, hace uso de algoritmos que permiten extraer puntos característicos (que dan información de coordenadas y ángulos de las terminaciones y bifurcaciones de las crestas dactilares) los cuales establecen similitudes con los puntos específicos de la huella de referencia (la que tiene en su base de datos la Registraduría Nacional), el factor de Similitud entre una huella y otra se establece con un componente denominado Matcher. (Ortiz, 2022)

En la figura 13 se destaca el web service matcher quien es el encargado de encontrar las similitudes en los patrones dactilares para el reconocimiento de huella**.**

Figura 13

Web Matcher



Nota. El Web service Matcher es el operador encargado de encontrar similitudes en los patrones para el reconocimiento de las huellas dactilares Tomado de (Ortiz, 2022)

Tipos De Dispositivos Utilizados En La Biometría

Dispositivos OEM son pequeños dispositivos que se utilizan para ser integrados en dispositivos más grandes, un ejemplo de esto es el lector de huellas dactilares en los Smartphone.

Dispositivos integrados son periféricos que pueden conectarse a una computadora, se utilizan para capturar grandes cantidades de datos, de modo que la información pueda almacenarse en el disco duro de la computadora a medida que las personas proporcionan su información.

Dispositivos completos son dispositivos diseñados y construidos para recopilar y analizar datos con el fin de identificar y conocer, tienen el hardware y el software necesarios para operar de forma independiente.

En los sistemas financiero se utiliza el componente Matcher, este es ampliamente utilizado en la programación para llevar a cabo diversas tareas como búsqueda y reemplazo de cadenas de texto, validación de datos y filtrado de resultados, utiliza expresiones regulares, que son patrones que describen un conjunto de posibles cadenas de texto.

El Matcher

Este analiza la secuencia de elementos y busca coincidencias con el patrón especificado. Una vez que encuentra una coincidencia, puede realizar acciones como extraer la coincidencia, reemplazarla con otra cadena de texto o simplemente indicar que se encontró una coincidencia.

El generador Matcher ofrece diferentes métodos para realizar estas operaciones, algunos de los métodos comunes incluyen:

find (): busca la siguiente coincidencia con el patrón especificado.

group (): devuelve la subsecuencia de la coincidencia actual.

replaceFirst (): reemplaza la primera coincidencia con el patrón por una cadena de reemplazo.

match es (): verifica si toda secuencia coincide con el patrón especificado. (Stephen, 2018)

Características de las Huellas Dactilares

Si bien cada huella digital es única en cada individuo, es de destacar que todas comparten tres tipos principales de patrones, uno de ellos son los bucles que son semejantes a curvas delgadas donde las líneas de la huella entran y regresan por el mismo camino, se destacan dos clases de bucles:

Los radiales, que se orientan hacia el pulgar (relacionados con el hueso radio).

Los cubitales, que se dirigen hacia el meñique (asociados al hueso cúbito).

Este último tipo es el más frecuente en las huellas dactilares.

Otro patrón común son los verticilos, que presentan crestas en forma de círculos o

espirales, estos se dividen en cuatro variantes:

Espirales simples, que son círculos concéntricos.

Bucle de bolsillo, que inicia como un bucle, pero termina en una espiral.

Doble bucle, formado por dos bucles opuestos que crean una figura similar a una “S”.

Verticilo accidental, que no sigue un diseño definido y tiene una forma irregular.

Los verticilos son el segundo patrón más común en las huellas digitales.

La tercera y última característica de la huella dactilar es el arco, estas líneas se ven como una colina, comenzando bajo en un extremo, subiendo en el medio y luego volviendo a bajar en el otro extremo, estas líneas onduladas vienen en dos tipos: lisas y con carpa, con arcos de carpa que se ven más apretados en el medio, como una carpa en el bosque, los arcos son la característica menos común de huellas dactilares. (Rodrìguez, 2020)

En la figura 14, se muestran las principales características de la huella dactilar, los elementos que se toman en cuenta para su posterior reconocimiento.

Figura 14

Características Huella Dactilar

Nota. Son los principales elementos que se tienen en cuenta, para su posterior reconocimiento, Tomado de (Rodrìguez, Carateristicas de la huella dactilar, 2020)

Marco Legal

En Colombia, el marco legal que regula la biometría en el sistema financiero se encuentra establecido principalmente en la Ley 1266 de 2008, por la cual se dictan las disposiciones generales del habeas data y la protección de datos personales, esta ley establece las normas para el tratamiento de los datos personales por parte de las entidades financieras y define los principios y procedimientos que deben seguirse en la recolección, almacenamiento, uso y circulación de estos datos.

Ley 527 de 1999: Esta ley regula el comercio electrónico y las firmas digitales, que son herramientas fundamentales en el uso de biometría financiera.

Ley 1581 de 2012: Esta ley regula la protección de datos personales y establece los principios y normas para su manejo y tratamiento en Colombia, esta ley es relevante ya que la biometría financiera involucra la recolección y procesamiento de datos biométricos de los individuos, esta ley es conocida como la ley de Protección de Datos Personales, tiene como objetivo principal salvaguardar la privacidad y proteger la adecuada gestión de la información personal de los ciudadanos.

Estas leyes y regulaciones buscan proteger los derechos y la privacidad de los usuarios, así como fomentar el uso seguro y confiable de la biometría en el sector financiero en Colombia.

Adicionalmente, el Decreto 1377 de 2013 reglamenta parcialmente la Ley 1266 de 2008 en cuanto a la recolección y uso de datos biométricos, este decreto establece que la recolección y uso de datos biométricos debe tener consentimiento previo, expreso e informado por parte del

titular de los datos, asimismo, se exige que se implementen medidas técnicas y organizativas adecuadas para garantizar la seguridad y confidencialidad de estos datos.

Ley 1266 De 2008: Esta ley establece las normas para la protección de datos personales y regula el manejo de la información financiera, crediticia, comercial y de servicios.

Ley 1480 de 2011: Esta ley establece los derechos y deberes de los consumidores en Colombia y prohíbe prácticas comerciales abusivas o fraudulentas.

Ley 1709 de 2014: Esta ley busca prevenir y controlar los riesgos asociados al fraude en el sistema financiero colombiano, establece medidas para la detección, prevención y sanción de conductas fraudulentas.

Ley 232 de 1995: Esta ley establece normas para la protección del patrimonio económico de la Nación y regula diversas actividades y delitos relacionados con el fraude.

EL Decreto Reglamentario 1377 de 2013

Establece directrices específicas para la administración de información personal, especialmente en el ámbito de datos biométricos, este decreto regula aspectos como la recolección, almacenamiento, uso y divulgación de dicha información, es fundamental cumplir con las disposiciones de este decreto para salvaguardar la privacidad de las personas y garantizar una gestión adecuada de los datos biométricos. (Bermúdez, s.f.)

En Colombia, el uso de la biometría está respaldado por la Ley 527 de 1999 y el Decreto 2364 de 2012, estas regulaciones permiten la implementación de tecnología biométrica en medios electrónicos, tanto para la verificación de identidad como para la firma de documentos electrónicos.

Adicionalmente, el Decreto Ley Anti-trámites establece en su artículo 18 el uso de la huella dactilar como mecanismo de identificación en medios electrónicos, también se impone la

obligación a entidades públicas y ciertos particulares de verificar la identidad del titular de la huella a través de la base de datos de la Registraduría.

El Registro Nacional de Estado Civil (RNEC)

A través de la Resolución 5633 de 2016 y sus anexos técnicos, es responsable del control de acceso a la base de datos biométricos y biográficos más completa y confiable del país, esta base de datos almacena más de 500 millones de huellas dactilares correspondientes a aproximadamente 50 millones de colombianos, así mismo se encuentra protegida por rigurosos estándares de seguridad que garantizan la integridad, confidencialidad y disponibilidad de la información (Galindo, 2016).

Desarrollo Objeto Especifico 1

Identificar las características principales de la suplantación biométrica en el sector financiero en Colombia, incluyendo los métodos utilizados, los riesgos asociados y los impacto en la seguridad de la información mediante una revisión bibliográfica y análisis de datos proporcionados por entidades relevantes en el tema.

Uso de datos biométricos: los estafadores utilizan la información biométrica de las personas, como huellas dactilares, iris o voz, para acceder a sus cuentas bancarias de forma fraudulenta.

Robo de identidad biométrica: los delincuentes pueden obtener la información biométrica de las víctimas de diversas formas, como el robo de dispositivos móviles o la interceptación de comunicaciones.

Los ataques de suplantación biométrica son métodos utilizados para evadir los sistemas de seguridad y robar información confidencial en los sistemas de autenticación biométrica, estos ataques se llevan a cabo de diferentes maneras, como:

Ingeniería social: se utilizan técnicas de persuasión o manipulación psicológica para obtener información personal o biométrica de la persona a suplantar, esto puede incluir el engaño a través de llamadas telefónicas, correos electrónicos o mensajes de texto.

Ataques de presentación: el atacante utiliza materiales como máscaras de silicona o imágenes impresas para presentar un rasgo biométrico falso directamente al sensor de autenticación.

Reutilización: en este tipo de fraude, los atacantes pueden intentar usar los datos biométricos de una persona para acceder a múltiples sistemas o servicios, esto puede ocurrir si

los datos biométricos se almacenan de forma insegura o si se utilizan para múltiples propósitos sin controles adecuados.

Manipulación de datos: los atacantes también pueden intentar modificar o manipular los datos biométricos durante la transmisión o el almacenamiento, esto puede hacer que los sistemas de autenticación biométrica no reconozcan correctamente la identidad del individuo y permitan el acceso no autorizado, algunos fraudes biométricos pueden tener como objetivo el escalado de privilegios, es decir, obtener acceso a niveles más altos de autorización o privilegios dentro de un sistema, esto puede permitir que los atacantes realicen transacciones financieras fraudulentas o accedan a datos confidenciales.

Alteración de bases de datos: en primer lugar, se encuentra el hecho de que la información de los datos biométricos se almacena en bases de datos, esto es esencial en un sistema de autenticación, ya que los datos en tiempo real del usuario deben compararse con los almacenados en una base de datos, sin embargo, estas bases de datos pueden ser vulneradas, filtradas o comprometidas si no se implementa una seguridad adecuada.

También es posible generar datos biométricos sintéticos, un ejemplo de esto ocurrió en 2013, cuando Apple sufrió un hackeo en el que se burlaron de la seguridad del iPhone 5S utilizando una huella dactilar falsa, además los delincuentes e investigadores han utilizado tecnologías como las redes neuronales adversarias generales (GAN) para crear falsificaciones convincentes de la apariencia de una persona y evadir los controles biométricos, esto incluye la falsificación de voz y contenido de video. (Rivera 2022)

A veces, los estafadores encuentran algunas formas para eludir los controles biométricos establecidos, por ejemplo, pueden utilizar métodos de autenticación alternativos o permitir el uso

de documentación en papel en lugar de una video llamada, lo cual puede ser más fácil de engañar.

Es importante tener en cuenta que los métodos mencionados anteriormente están estrechamente relacionados con la suplantación de una persona específica o pueden ser aplicables a cualquier persona siempre que se engañe al sistema.

Por ejemplo, en ciertos entornos donde solo una o dos personas tienen acceso, los estafadores pueden intentar falsificar meticulosamente los datos biométricos de estas personas. Sin embargo, en situaciones donde cientos de empleados tienen acceso a un edificio de oficinas, los estafadores pueden hacer pasar una huella dactilar aleatoria como propia en lugar de la de una persona específica también es importante destacar que la biometría puede ser falsificada y que existen diferentes métodos para hacerlo, dependiendo de la característica biométrica que se intente falsificar, como huellas dactilares, rasgos faciales o la forma de escribir.

Por ejemplo, se ha evidenciado que las huellas dactilares pueden ser falsificadas de varias maneras, como reutilizar restos de huellas dactilares de alguien en una superficie o recrearlas a partir de videos o fotografías, también se han utilizado programas de edición de fotos y materiales simples para crear huellas dactilares sintéticas basadas en fotos de huellas dactilares reales.

Además, es posible falsificar voces utilizando modelos de aprendizaje automático y módulos de conversión de texto a voz de acceso libre, estas falsificaciones de voz se utilizan para engañar a los empleados haciéndoles creer que están hablando con una figura de alta dirección,

lo que facilita estafas como el fraude del CEO y otros esquemas de hackeo biométrico (Rivera Y. M., 2022)

Otros ataques que se pueden dar en la suplantación biométrica.

Ataques de reproducción: el atacante intercepta los datos biométricos durante el proceso de autenticación y los reproduce más tarde para obtener acceso al sistema.

Ataques de suplantación: el atacante crea un rasgo biométrico falso similar al original utilizando materiales como cera o gelatina, o mediante el uso de imágenes y software digitales.

Ataques intermodales: el atacante utiliza un rasgo biométrico diferente al original, como una fotografía de la cara, para evadir el sistema de autenticación. (Bertolín, 2019)

Vulnerabilidades en los sistemas de seguridad: a pesar de que la biometría se considera una medida de seguridad más avanzada, los sistemas biométricos pueden ser vulnerables a ataques, como la falsificación de huellas dactilares o la suplantación de voz.

Impacto en la seguridad financiera: la suplantación biométrica puede tener graves consecuencias para la seguridad financiera de las personas, ya que los estafadores pueden acceder a sus cuentas bancarias, realizar transacciones no autorizadas o incluso robar su identidad.

Los riesgos que se dan pueden ser

Pérdida de privacidad: La suplantación biométrica puede poner en riesgo la privacidad de una persona si sus datos biométricos son robados y utilizados sin su consentimiento.

Robo de identidad: si un delincuente logra suplantar la identidad de una persona utilizando sus datos biométricos, puede acceder a información confidencial y llevar a cabo actividades ilegales en su nombre.

Fraude financiero: los estafadores pueden utilizar la suplantación biométrica para acceder a cuentas bancarias, realizar transacciones fraudulentas y cometer otros tipos de fraudes financieros.

Daño reputacional: Si una persona es víctima de suplantación biométrica, su reputación y credibilidad pueden quedar dañadas, ya que otras personas podrían creer que ha estado involucrada en actividades delictivas.

Vulnerabilidad a ciberataques: los datos biométricos son sensibles y altamente codificados, por lo que si caen en manos equivocadas una persona podría convertirse en blanco de ciberataques y otras formas de manipulación digital.

Pérdidas millonarias cuando los ciberdelincuentes hacen transacciones monetarias de alto valor, o realizan la suplantación del cliente para sacar créditos millonarios, pérdida de confianza y de credibilidad en las entidades financieras lo que puede llevar a cerrar cuentas de manera masiva entre los usuarios, demandas millonarias etc.

Impactos en la seguridad de la información

Las entidades financieras en Colombia deben trasmitir confianza a los usuarios, donde tengan la seguridad que su dinero está protegido, pero que impactos se afectan cuando se hace la suplantación biométrica.

Integridad

Los registros financieros pueden ser modificados o manipulados, lo que distorsiona la historia real de las transacciones, volviéndose complicado confirmar si una operación fue realizada por el verdadero titular de la cuenta, lo que genera dudas sobre la legitimidad de los movimientos.

Confidencialidad

Este principio busca proteger la información sensible de accesos no autorizados, en casos de fraude biométrico:

Los datos únicos de los usuarios, como huellas o rasgos faciales, pueden quedar expuestos, lo que compromete su privacidad si estos datos son robados, pueden ser utilizados en otros sistemas o plataformas, ampliando el alcance del daño.

Disponibilidad La disponibilidad garantiza que los servicios estén accesibles cuando se necesiten. ante incidentes de suplantación:

Las entidades financieras pueden verse obligadas a suspender temporalmente sus servicios para investigar o prevenir más fraudes, el aumento de quejas y solicitudes de revisión puede colapsar los canales de atención, afectando la experiencia del usuario.

Reputación y confianza

Este aspecto está ligado a la percepción que tienen los clientes sobre la seguridad y credibilidad de una entidad:

Puede existir la publicidad voz a voz, de forma negativa además de las redes sociales los que afectarían el buen nombre de las entidades financieras.

Si se presentan casos de suplantación biométrica, los usuarios pueden perder la confianza en los sistemas digitales del banco, el temor a ser víctimas de fraude puede llevar a que los clientes abandonen la entidad o eviten usar sus canales virtuales.

Impacto Legal

Las entidades financieras en Colombia, al estar expuestas por la suplantación biométrica, vulnerando la protección de datos, puede ser objeto de penalizaciones severas, Como lo dicta la Ley 1581 establece la obligación de aplicar mecanismos efectivos para resguardar la información de los usuarios, si se comprueba que la entidad financiera no adoptó las medidas necesarias, los entes reguladores tienen la facultad de imponer sanciones económicas que podrían equivaler a una parte considerable de sus ingresos anuales.

Impacto económico

Al comenterse un acto se suplantación biométrica, en las entidades financieras, el impacto financiero puede ser significativo ya que estas entidades pueden enfrentar pérdidas millonarias por transacciones fraudulentas, créditos otorgados a suplantadores o indemnizaciones

a clientes afectados ya que por lo general estos fraudes se comenten con montos, y tendría la entidad financiera que asumir la perdida. (Galindo J. , 2024)

Desarrollo Objetivo Específico 2

Evaluar la eficacia de las acciones de ciberseguridad emitidas por la Superintendencia Financiera y las implementadas por las entidades bancarias en Colombia para prevenir la suplantación biométrica, a través de análisis de vulnerabilidades detectadas.

El fraude bancario que se da en Colombia el cual es se refiere a la utilización inapropiada de características físicas o de comportamiento de las personas en el ámbito financiero con el fin de cometer actividades fraudulentas, estas características pueden incluir huellas dactilares, reconocimiento facial, voz y firma, en el ámbito financiero, el fraude biométrico podría ocurrir cuando un delincuente utiliza la información biométrica de otra persona sin su consentimiento para acceder a sus cuentas bancarias, realizar transacciones fraudulentas o robar su identidad financiera.

A continuación, se menciona las quejas por fraude en el sistema financiero de acuerdo con Asobancaria es de mencionar que este artículo es muy actual es del 27 de octubre del 2023, esto demuestra la importancia de crear estrategias para mitigar la suplantación financiera en este caso del sector financiero colombiano.

Según el presidente de Asobancaria, Jonathan Malagón González, durante el transcurso de este año se han reportado 53 instituciones afectadas por ciberataques y se han presentado 242,885 denuncias por fraudes tecnológicos, esta información se dio a conocer durante el 16° Congreso de prevención de fraude y ciberseguridad organizado por Asobancaria.

La tecnología actual representa un riesgo para cualquier empresa, pero principalmente para las entidades bancarias y financieras, ya que llevan a cabo operaciones monetarias en línea

de manera constante, de hecho, a nivel nacional se han identificado más de 40 ataques cibernéticos por segundo en el sistema financiero.

El presidente de Asobancaria mencionó que recibimos 43 ciberataques por segundo. Desde este discurso hasta que se clausure este congreso, el sistema financiero colombiano habrá sufrido siete millones de ciberataques, y al final del discurso habrá recibido 52.000, este es el gran desafío que se da diariamente, además el 96,32% de las quejas por fraude se concentra en cuatro productos financieros: cuentas de ahorro, tarjetas de crédito, depósitos de bajo monto y depósitos de bajo monto inclusivo también registran un número significativo de quejas, principalmente hacia los bancos.

Según Jaime Rodríguez Hernández, director de investigación, innovación y desarrollo de la Superintendencia Financiera, la mayoría de las quejas por fraude tecnológico se deben a técnicas de ingeniería social y suplantación de identidad, las quejas se presentan principalmente a través de internet, con un 52%, seguido de las aplicaciones móviles con un 36%. el resto de las quejas se distribuyen entre el uso de POS, ATM y otros medios, en comparación con el primer semestre del año pasado, los bancos han experimentado un aumento del 1,97% en las quejas por fraude tecnológico. (https://www.superfinanciera.gov.co/, Asobancaria infobae, 2023)

El Mayor Número De Quejas

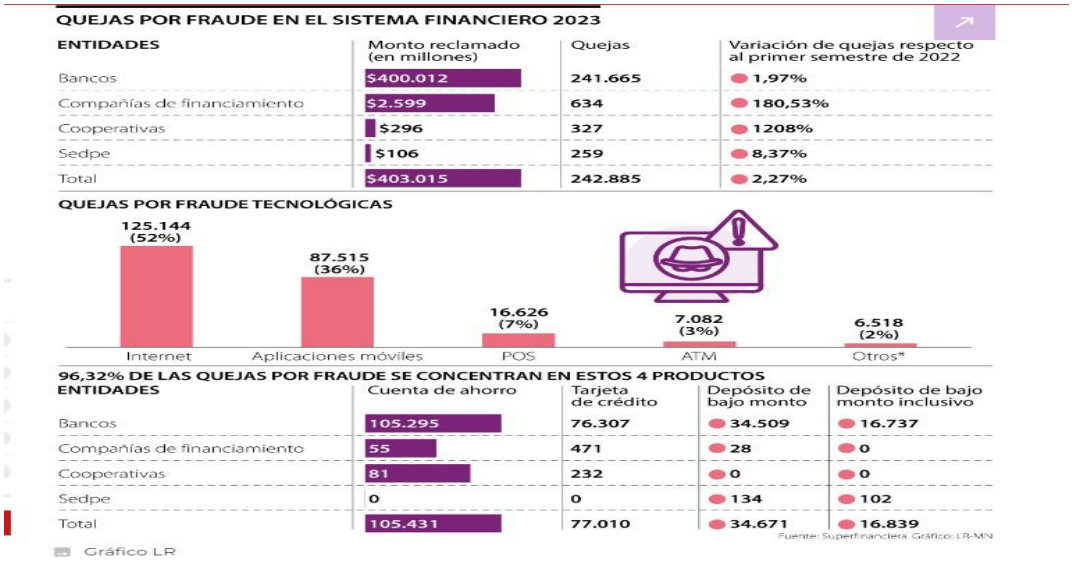
Se dirige a las cuentas de ahorro, con un total de 105.431 quejas, de las cuales la mayoría, 105.295, son hacia los bancos, las tarjetas de crédito son el segundo producto con más quejas,

con más de 77.000 en general, principalmente dirigidas a los bancos, el servicio de depósito de bajo monto.

En la figura 15 se observa las cifras de quejas que se dieron por fraudes en el sistema financiero que fueron de 241.665 esta es una cifra alta, y este informe es de 27 octubre del 2023.

Figura 15

Quejas Fraude Bancario



Nota. Principales quejas en el sistema financiero, por fraude bancario en el año 2023Tomado de (https://www.superfinanciera.gov.co/, Asobancaria infobae, 2023)

Características principales de las vulneraciones biométricas

La suplantación biométrica en el sector financiero en Colombia es un problema que presenta desafíos y riesgos significativos está cada día la ciberdelincuencia crea estrategias para vulnerar al sistema biométrico, en el caso del sistema financiero colombiano los delincuentes se valen de artimañas cada vez más sofisticadas para vulnerar el sistema biométrico a continuación se mencionarán las características más relevantes como lo son:

complejidad Tecnológica

La suplantación biométrica requiere un conocimiento técnico avanzado y el acceso a equipos y software especializados, los delincuentes deben ser capaces de copiar con precisión las características físicas de la persona que intentan suplantar y utilizarlos para sortear los sistemas de seguridad biométricos, la ciberdelincuencia debe estar en capacidad de vulnerar los sistemas biométricos, este sistema de captura de datos biométricos está determinada por la tecnología utilizada, los algoritmos de procesamiento, la infraestructura tecnológica necesaria y el cumplimiento de estándares y normativas de seguridad y privacidad, la precisión y velocidad de los escáneres de huellas dactilares y las cámaras de alta resolución y algoritmos sofisticados para sistemas de reconocimiento facial son ejemplos de la tecnología requerida, los algoritmos de procesamiento deben ser capaces de extraer y comparar características biométricas de manera eficiente y precisa, la infraestructura tecnológica consiste en servidores, bases de datos, redes y software específico, cuya complejidad depende del tamaño y capacidad del sistema.

El cumplimiento de estándares y normativas incrementa la complejidad al requerir medidas de protección y control de datos adicionales.

Falsificación de características físicas: los suplantadores deben ser capaces de crear réplicas falsas de las características biométricas de una persona, como huellas dactilares, iris o rostro. Esto puede implicar el uso de moldes, impresoras 3D o incluso productos químicos para crear una falsa huella digital.

En la figura 16 se muestra la técnica de fraude bancario, que consiste en huellas sobrepuestas de goma.

Figura 16

Huella Goma

*Nota.*Huella goma esta técnica, consiste en sobreponer huellas con siliconas, o pegamentos especiales para alterar una huella dactilar Tomado de (https://canal1.com.co/, 202.

Riesgo de robo de identidad: La suplantación biométrica puede conducir al robo de identidad, donde un individuo puede acceder a información personal y llevar a cabo actividades delictivas en nombre de otra persona, esta técnica la utiliza mucho la ciberdelincuencia ya que envuelven a las personas con artimañas maliciosas para sustraer información privada de cada individuo y hacer el fraude este caso el fraude bancario como lo son trasferencias de altas sumas de dinero, compras en línea, créditos

Cambio de Características Biométricas

Aunque las características biométricas son únicas, en algunas ocasiones pueden ser alteradas intencionalmente, como a través de cirugías plásticas o el uso de productos químicos, lo

que dificulta la autenticación de la identidad de una persona entre las cuales las más utilizadas son:

Huellas dactilares falsas: se crean réplicas de las huellas dactilares de la persona a suplantar utilizando moldes, impresiones en 3D u otros métodos similares, estas réplicas se usan para autenticarse en sistemas de identificación biométrica.

En la figura 17 se muestra otra técnica de falsificación en goma, en este caso son moldes de huellas digitales.

Figura 17

Falsificación Huella Goma

Nota. Falsificación huellas goma, a través de molde de silicona que se sobrepone para simularla huella digital de un usuario y así cometer el fraude. Tomado de (https://colcert.gov.co/, 2019).

En la figura 18 se muestra otra técnica que utilizan los delincuentes para cometer fraude bancario en este caso se aplican una especie de talco para que no se les desprendan las huellas de goma falsas.

Figura 18

Aplicación Huella Fraude

Nota. Aplicación huella fraude en este se aplica un talco especial que se adhiere a la huella, para que por el sudor de la mano no se despegue Tomado de (https://colcert.gov.co/, 2019).

Reconocimiento facial

Se utilizan imágenes o videos de la persona a suplantar para engañar a los sistemas de reconocimiento facial, estas imágenes o videos pueden ser generados artificialmente o extraídos de fuentes públicas o privadas, a medida que el reconocimiento facial se vuelve más común en diversas aplicaciones, también aumentan las preocupaciones sobre su vulnerabilidad ante la suplantación.

Una forma de engañar a estos sistemas es utilizando imágenes o videos de la persona a suplantar, ya sea generados artificialmente o extraídos de fuentes públicas o privadas, las imágenes generadas artificialmente pueden ser muy realistas y difíciles de distinguir de las reales para los sistemas de reconocimiento facial, además, las imágenes o videos pueden ser obtenidos de fuentes como las redes sociales o cámaras de seguridad, para engañar al sistema, se utilizan técnicas como el uso de máscaras tridimensionales impresas en 3D o la proyección de imágenes en tiempo real sobre el rostro de otra persona, estas técnicas plantean problemas de seguridad y privacidad, ya que permiten a los atacantes acceder a información o lugares protegidos en

nombre de otra persona, en respuesta a estas preocupaciones, los investigadores y desarrolladores están trabajando en mejorar los sistemas de reconocimiento facial mediante el uso de técnicas avanzadas de detección y autenticación, así como la combinación de múltiples factores de autenticación para aumentar la seguridad y dificultar la suplantación. (Torres, 2019)

En la figura 19 se muestra cómo se simula la suplantación de los usuarios en este caso la suplantación facial.

Figura 19

Suplantación Facial

Nota Suplantación facial esta se da a través de prótesis creadas con siliconas especiales, para simular los rasgos de un usuario Tomado de (Khade, 2023).

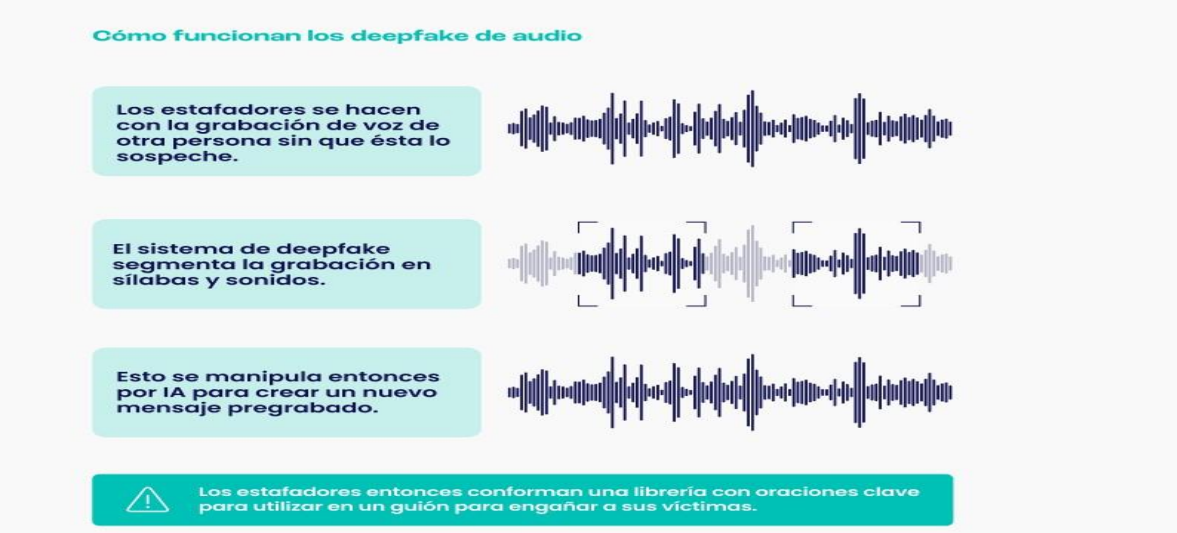
Grabaciones de Voz

Se utilizan grabaciones de la voz de la persona a suplantar para engañar a los sistemas de reconocimiento de voz, estas grabaciones pueden ser utilizadas para acceder al sistema o realizar transacciones fraudulentas.

En la figura 20 se observa la técnica Deep fake donde se guarda la voz del cliente y luego con una técnica de IA se simula ser el usuario.

Figura 20

Deep Fake Audio



Nota. Deep fake de audio es una simulación a través de la inteligencia artificial para suplantar la voz del usuario y cometer así el fraude Tomado de (Garcia, 2021).

La suplantación biométrica a nivel de Deep fake biométrico en el ámbito bancario, es una forma avanzada de suplantación de identidad mediante el uso de tecnología de generación de imágenes falsas llamada Deep fake, esta tecnología utiliza algoritmos de aprendizaje automático para crear videos o imágenes realistas y modificadas que hacen que una persona parezca otra.

En el ámbito bancario, el Deep fake biométrico se utiliza principalmente para suplantar la identidad de los clientes con el propósito de llevar a cabo actividades fraudulentas, como acceder a cuentas bancarias, retirar dinero o realizar transferencias ilegales.

Los sistemas biométricos, como la identificación de voz, la huella digital y el reconocimiento facial, se utilizan comúnmente en los bancos para autenticar a los clientes y garantizar la seguridad de las transacciones, sin embargo, el Deep fake biométrico representa una

seria amenaza para estas tecnologías, ya que puede engañar fácilmente a los sistemas biométricos y permitir que los delincuentes accedan a información confidencial y realicen actividades ilícitas.

La creación de Deep fakes biométricos requiere datos biométricos auténticos de la persona que se quiere suplantar, estos datos pueden ser obtenidos de manera ilegal o sustraídos de bases de datos comprometidas, una vez que los delincuentes tienen acceso a estos datos, utilizan algoritmos de aprendizaje automático para generar imágenes falsas o modificar videos y hacer que parezca que una persona real está llevando a cabo una transacción bancaria. (Garcia, 2021)

Acciones de ciberseguridad emitidas por la Superintendencia Financiera y las implementadas por las entidades financieras en Colombia.

la Superintendencia Colombiana emitió una norma llamada Circular Externa 007 del 2018, que obliga a los bancos y otras entidades financieras a tener un plan serio y estructurado para enfrentar riesgos cibernéticos,

Entre los puntos clave se incluyen:

Prevención

Las entidades financieras deben anticiparse a los riesgos cibernéticos mediante:

Identificación de activos críticos (como bases de datos de clientes), evaluación de amenazas y vulnerabilidades.

Diseño de controles para evitar ataques, protección y Detección se exige implementar herramientas tecnológicas para proteger los sistemas y detectar incidentes en tiempo real:

Uso de antivirus, firewalls, cifrado de datos, centros de monitoreo continuo (SOC).

Respuesta y Comunicación

Las entidades deben tener planes claros para actuar ante incidentes:

Contención del ataque, notificación a los usuarios afectados, comunicación interna y externa.

Recuperación y Aprendizaje

Después de un incidente, se deben tomar medidas para:

Restaurar los servicios afectados, analizar qué falló, Mejorar los controles para evitar que se repita.

Gobernanza y Políticas

Cada entidad financiera debe tener una política de ciberseguridad aprobada por su junta directiva, esta política define roles, responsabilidades y procedimientos.

Capacitación continua

Los empleados deben recibir formación periódica sobre ciberseguridad:

Reconocimiento de correos falsos (phishing).

Buenas prácticas digitales.

Simulacros de respuesta ante incidentes.

Información al consumidor

Las entidades deben ser transparentes con sus clientes:

Informar sobre incidentes que puedan afectarlos, explicar las medidas tomadas, ofrecer canales de atención. (Gutierrez, 2018).

Adicional se creó el Centro de Operaciones de Seguridad (SOC) es una unidad especializada dentro de los bancos que se encarga de vigilar, detectar y responder a amenazas digitales, durante las 24 horas del día, donde se supervisan todos los sistemas tecnológicos del banco las 24 horas del día, con el objetivo de prevenir fraudes y proteger la información de los clientes.

Dentro de sus funciones principales se destacan varias tareas esenciales para mantener la seguridad digital dentro de las entidades financieras en Colombia.

Supervisión constante de redes, aplicaciones y plataformas bancarias.

Identificación de actividades sospechosas, como accesos desde ubicaciones inusuales o transacciones fuera de lo común.

Respuesta inmediata ante incidentes para evitar que se conviertan en fraudes.

Análisis de patrones para anticiparse a futuros ataques y fortalecer los sistemas.

Detección de correos y sitios falsos (phishing y suplantación)

El SOC identifica intentos de engaño que buscan robar datos personales, como correos electrónicos o páginas web que imitan al banco.

Monitoreo de transacciones inusuales

El SOC analiza millones de operaciones en tiempo real para detectar movimientos que no coinciden con el comportamiento habitual del cliente.

Prevención de software malicioso (programa maligno y ransomware)

El SOC detecta archivos peligrosos que pueden robar información o bloquear el acceso a sistemas críticos.

Protección frente a engaños por ingeniería social

El SOC también monitorea intentos de fraude que se realizan por medio de llamadas, mensajes o formularios falsos que buscan manipular a los usuarios. (Gomez a. , 2022)

La Superintendencia Financiera de Colombia (SFC) ha desarrollado el micrositio ¡Alerta! Ofertas fraudulentas, una herramienta digital orientada a proteger a los ciudadanos frente a los riesgos de fraude financiero que circulan en el país.

¿En qué consiste?

Este espacio educativo, disponible en el portal oficial de la SFC, tiene como objetivo principal informar y prevenir a los consumidores financieros sobre prácticas engañosas como:

Ofertas de dinero fácil.

Créditos falsos sin requisitos.

Inversiones fraudulentas con altos rendimientos.

Esquemas ilegales como pirámides o captación no autorizada.

El micrositio está dividido en cuatro secciones temáticas, cada una enfocada en una modalidad de fraude. en cada sección los usuarios encontrarán:

Explicaciones claras sobre las prácticas ilegales.

Consejos prácticos para evitar caer en estafas.

Instrucciones para realizar denuncias.

Herramientas de autoevaluación para fortalecer el conocimiento financiero.

Resultados y contexto

Durante el periodo comprendido entre 2024 y el primer semestre de 2025, la SFC reportó:

13 medidas administrativas contra captación ilegal, que afectaron a 938 personas y representaron pérdidas superiores a COP 30.678 millones,417 denuncias relacionadas con falsos prestamistas

2.741 consultas atendidas sobre esquemas fraudulentos esta información es muy actual es del 13 de agosto 2025. (Ospina, 2025).

Desarrollo Objetivo Específico

Formular recomendaciones basadas en las mejores prácticas identificadas durante la investigación, para establecer un marco de prevención de la suplantación biométrica en el sector bancario colombiano, considerando aspectos técnicos, legales y éticos para mejorar la seguridad de las transacciones financiera.

Muchas entidades financieras han Implementado sistemas de autenticación biométrica avanzados que permiten verificar la identidad de los usuarios a través de sus características biométricas, como huellas dactilares, reconocimiento facial o iris, estos sistemas son más seguros y difíciles de suplantar que los tradicionales métodos de autenticación basados en contraseñas.

Monitorización y Detección de Anomalías

Las entidades financieras han implementado sistemas de monitorización y detección de anomalías que permiten identificar comportamientos inusuales o sospechosos en las transacciones financieras, lo que puede indicar que se está produciendo una suplantación biométrica.

Educación y concienciación de los usuarios: las entidades financieras también han llevado a cabo campañas de concienciación y educación dirigidas a sus clientes, para que estos sean conscientes de los riesgos de la suplantación biométrica y de cómo pueden protegerse de esta amenaza.

La tecnología blockchain es un sistema descentralizado de registro de datos que utiliza una red de computadoras interconectadas para almacenar información de forma segura y

transparente, en lugar de depender de un servidor centralizado, la información se almacena en múltiples ubicaciones y se actualiza de forma simultánea en todas ellas.

La información en un blockchain se organiza en bloques que contienen datos y una referencia al bloque anterior, lo que crea una cadena continua de bloques, cada bloque está cifrado y enlazado con el anterior, lo que garantiza la seguridad y la integridad de la información almacenada en la cadena.

El uso de la tecnología blockchain en el sistema financiero en Colombia traer una serie de beneficios, como mayor seguridad en las transacciones, transparencia, eficiencia, reducción de costos, prevención de actividades ilícitas. (Tobon, 2020)

Fortalecimiento y aumento de las leyes que castigan la suplantación biométrica en Colombia, además del aumento de las penas por este delito cibernético.

En el sector financiero es importante que los funcionarios, revisen las manos de las personas a las cuales les van a realizar la Biometría, esto es parte de las buenas prácticas al momento de tomar la biometría.

Tomar la huella de manera aleatoria, de esta manera se permitirá tener más control y evitar vulneraciones, en cierta parte de los sistemas biométricos.

Limpiar el lector biométrico.

Establecer un Trabajo mancomunado con las entidades financieras para capacitar y tener cada día, más estrategias para evitar la suplantación biométrica financiera.

Verificar que los dispositivos de recolección de datos biométricos sean legítimos y estén protegidos de manipulaciones o ataques físicos.

Encriptar los datos biométricos: asegurarse de que los datos biométricos estén encriptados para protegerlos de posibles robos o intercepciones durante la transmisión o almacenamiento.

Implementar la autenticación multifactorial: además de la autenticación biométrica, considera incluir otros factores de autenticación, como contraseñas, tokens de seguridad o verificaciones adicionales, para aumentar la seguridad y dificultar la suplantación biométrica.

Mantener los sistemas biométricos actualizados con los últimos parches de seguridad y actualizaciones de software, estas actualizaciones a menudo solucionan vulnerabilidades conocidas y mejoran la seguridad general.

La introducción de la modalidad de Selfie pay ha permitido a los usuarios confirmar sus compras utilizando una fotografía en lugar de contraseñas tradicionales, esta innovadora tecnología biométrica de identificación utiliza selfies para validar transacciones, convirtiendo el rostro en un método de autenticación. (https://www.xataka.com/, 2020)

Educar y crear conciencia sobre la importancia de la suplantación biométrica entre los usuarios y empleados. Proporciona pautas claras sobre cómo deben proteger y utilizar sus datos biométricos.

Participación en estándares y mejores prácticas: Mantener actualizado sobre los estándares y mejores prácticas en seguridad biométrica.

Fortalecimiento de la seguridad: La suplantación biométrica se utiliza como una medida para fortalecer la seguridad en el sector financiero, la tecnología biométrica es considerada más

segura que las contraseñas o los códigos PIN, ya que utiliza características únicas e irrepetibles de cada individuo.

Por otro lado, la inteligencia artificial y el machine learning: Los investigadores han descubierto que la IA puede detectar eficazmente la falsificación biométrica.

Sensibilizar a los usuarios: asegurarse de que los usuarios y personal bancarios sean conscientes de los riesgos y de los tipos de estafas más en los sistemas biométricos financieros.

Las técnicas basadas en blockchain almacenan los datos biométricos de manera segura y a prueba de manipulaciones, y permiten una gestión descentralizada y transparente de los datos. (Reyes, 2022)

Reconocimiento Facial De Tecnología Avanzada

Esta tecnología avanzada es un punto muy importante para identificar y autenticar a los clientes a través de sus rasgos faciales únicos, esto reduce la posibilidad de que se lleve a cabo suplantación de identidad.

Monitoreo continuo además se debe implementar estrategias como el monitoreo continuo de transacciones sospechosas y el análisis de comportamiento del cliente, estas estrategias permiten detectar patrones de actividad inusuales y alertar de posibles actividades fraudulentas.

Colaboración con instituciones Las entidades financieras están trabajando en colaboración con instituciones como la policía nacional y la superintendencia financiera de Colombia para intercambiar información y fortalecer la lucha contra la suplantación biométrica. Esta colaboración permite una respuesta más efectiva ante posibles casos de fraude**.**

Implementación de técnicas de autenticación multifactorial la autenticación biométrica debe ser complementada con otros factores de autenticación, como contraseñas, tarjetas inteligentes o tokens de seguridad, esto permite aumentar el nivel de seguridad, ya que es más difícil para un atacante obtener y utilizar diferentes factores simultáneamente.

Uso de sistemas biométricos avanzados: es importante utilizar sistemas biométricos que sean lo más precisos y confiables posible, esto implica la utilización de tecnologías avanzadas de reconocimiento facial, huella dactilar, retina o voz, que sean difíciles de falsificar o suplantar.

Establecimiento de límites y controles en las transacciones: los bancos y entidades financieras deben establecer límites y controles en las transacciones, especialmente aquellas que se consideran de alto riesgo, por ejemplo, se puede implementar un sistema de autorización adicional o exigir un proceso de verificación más riguroso antes de realizar determinadas operaciones.

Monitoreo y detección de anomalías

Es importante contar con sistemas de monitoreo y detección de anomalías que permitan identificar posibles suplantaciones biométricas, estos sistemas pueden analizar patrones de comportamiento y utilizar técnicas de inteligencia artificial para identificar actividades sospechosas y alertar a los responsables de seguridad.

La autenticación multifactorial es un proceso de seguridad que utiliza diversas características para confirmar la identidad de un usuario, esta forma avanzada de autenticación requiere la combinación de al menos dos factores, como una contraseña, una tarjeta inteligente o

una huella digital, para garantizar un mayor nivel de seguridad, al utilizar múltiples factores, se reduce la posibilidad de un acceso no autorizado a cuentas o sistemas.

Algunas características adicionales pueden incluir el uso de reconocimiento facial, escaneo de iris o verificación de voz para una autenticación aún más robusta, en conjunto, estas características refuerzan la seguridad y protegen la información personal y sensible de los usuarios. (autenticación, 2020)

Conclusiones

Las medidas de mitigación implementadas en Colombia son efectivas en parte, pero no completamente confiables dado que la suplantación biométrica representa una amenaza creciente en el sector financiero colombiano, donde la digitalización ha ampliado la superficie de ataque. Aunque las entidades financieras han adoptado medidas de mitigación como autenticación multifactor, biometría facial y dactilar, y monitoreo en tiempo real, la efectividad y confiabilidad de estas soluciones depende de varios factores, la calidad de la tecnología, la capacitación del personal, la conciencia del usuario y la actualización constante frente a nuevas técnicas de fraude.

La confiabilidad de la autenticación biométrica depende de su integración con otros controles de seguridad, como la verificación en tiempo real, análisis de comportamiento y autenticación multifactorial, adaptándose a las nuevas tecnologías y posibles amenazas futuras, para lograr esto, las entidades financieras deben invertir en el desarrollo y la integración de tecnologías biométricas avanzadas, estas soluciones deben ser diseñadas con un enfoque centrado en la seguridad, de modo que dificulten su vulneración y reduzcan la probabilidad de suplantación.

La implementación de la autenticación multifactorial, junto con la combinación de diversas modalidades de autenticación, como contraseñas, tokens de seguridad y reconocimiento facial, fortalecerá significativamente el control sobre el proceso de autenticación biométrica de los usuarios ante las entidades financieras en Colombia, esta estrategia no solo incrementará la seguridad y protección de los datos personales, sino que también generará confianza en los usuarios al garantizar un acceso más seguro a sus cuentas y transacciones financieras.

Recomendaciones

Es necesario que las entidades financieras colombianas estén actualizadas en las medidas que se están tomando a nivel mundial para evitar la suplantación biométrica tales como son, las técnicas basadas en blockchain en las que se almacenan los datos biométricos de manera segura y a prueba de manipulaciones, esto permite un parte de seguridad en las entidades financieras.

Otra técnica que me parece muy adecuada es la de Liveness detection o prueba de vida es la capacidad de un sistema para determinar la autenticidad de un rostro, una voz u otra característica biométrica, mediante esta técnica se verifica si el rasgo presentando ante la cámara en un proceso de verificación proviene de una persona viva o se trata de un artefacto, por tanto, la prueba de vida confirma la autenticidad del sujeto que realiza el proceso.

La liveness detection hace uso de algoritmos avanzados y modelos de aprendizaje automático para analizar y procesar la información capturada, estos algoritmos son los encargados de identificar patrones y características específicas que indiquen la autenticidad del usuario, lo que permite una detección precisa y confiable esta técnica me parece muy adecuada para el sistema financiero ya que mitigara en algo la suplantación biométrica.

Implementar soluciones basadas en inteligencia artificial, machine learning y visión por computador, mitigando el fraude por suplantación e incrementando la seguridad en los clientes al realizar sus transacciones financieras.

Bibliografía

Ahmad Radzi, S. K.-H. (2016). *Finger-vein biometric identification using convolutional neural network.* Turkish Journal of Electrical Engineering and Computer Sciences, .

Altamar, N. (27 de 10 de 2023). *La Republica*. Recuperado el 05 de 11 de 2023, de https. larepublica.co/finanzas productos con mas fraude cibernético

Andeotti Christian, B. L. (22 de 06 de 2021). *Repositorio Institucional*. Recuperado el 25 de 10 de 2023, de http://hdl.handle.net/11349/29149

Asobancaria. (30 de 09 de 2021). *Avances de la Biometría en las transacciones Financieras.* Recuperado el 18 de 10 de 2023, de https www asobancaria.com

Autenticación, M. (02 de 2020). https://geekflare.com/es/multi-factor- authentication/.

Bermúdez, A. (s.f.). *Super intendencia de industria y comercio*. Recuperado el 25 de 11 de 2023, de https www.sic.gov.co /content sobre la protección de datos personales.

Bertolín, J. (2019). *Análisis en torno a la seguridad de los sistemas biométricos.*

Obtenido de CONECtrónica: https://www.conectronica.com/tecnologia/seguridad/analisis-en-torno-a-la-seguridad-de-los-sistemas-biométricos

Castro, J. (17 de 10 de 2020). *Aumentan los fraudes delincuentes usan números de Bancos para robar información.* Recuperado el 25 de 10 de 2023, de https www.campeche.com .mx

Cena, J. (2018). *Que es Huella dactilar*. Recuperado el 25 de 10 de 2023, de https informática computacion.blogspot.com

CISCO. (s.f.). https://www.cisco.com/c/es_mx/products/security/what-is- cybersecurity.html.

Completa, T. d. (s.f.). *https://recfaces.com/*. https://recfaces.com/: https://recfaces.com/

Cruz, F. (2020). *Iris* .

Cruz, F. (15 de 05 de 2023). *Belltech*. Recuperado el 25 de 10 de 2023, de https bellteche.la blog que es la Biometría de voz

D, C. (2023). what is Biometric Spoofing. *chargebacks911*, https chargesbacks 911.com.

Diccionario Enciclopedico Larousse . (2014). Barcelona : Larousse. Diccionario, L. (s.f.).

Elahee, F. (2020). Comparative study of deep learning based finger vein biometric authentication systems. *2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT 2020*, 444 - 448.

española, D. d. (s.f.). *Real Academia Española*. Recuperado el 08 de 05 de 2024, de https://dle.rae.es/sector

Fedtke C, E. K. (2020). Ocular biometry and their correlations with ocular and anthropometric measurements among ethiopian adults. Clin Ophthalmol. *Revista Mexicana de Oftamologia* , págs. 155-161.

Fernández, T. (2014). *Biografia de Alphonse Bertillon*. Obtenido de Biografias y vida en línea: https://www.biografiasyvidas.com/biografia/b/bertillon.htm

Fernández, T. T. (2004). *Biografias y Vidas* . Recuperado el 20 de 11 de 2023, de https www biografías y vidas.com /bertillom .htm

Galindo, J. (29 de 07 de 2016). *Registraduria del Siglo XXI*. Recuperado el 15 de 10 de 2023, de http www registraduria.gov.co

Galindo, J. (27 de noviembre de 2024). *https://www.datacredito.com.co/blogs/datablog*. https://www.datacredito.com.co/blogs/datablog/impacto-financiero-de-la-suplantacion-de-identidad-en-empresas/https://www.datacredito.com.co/blogs/datablog/impacto-financiero-de-la-suplantacion-de-identidad-en-empresas/

García, F. (21 de 07 de 2021). Deepfakes. *Dialnet*, 103-120. Recuperado el 22 de 10 de 2023, de https://dialnet.unirioja.es/servlet/articulo?codigo=7987666

Gómez, a. (11 de 2022). *https://www.deltaprotect.com/blog/que-es-security-operations- center*. https://www.deltaprotect.com/blog/que-es-security-operations-center: https://odint.net/posts/soc-siberseguridad/

Gómez, f. (10 de 06 de 2021). *https://www.valoraanalitik.com/.* https://www.valoraanalitik.com/aumentan-en-243-intentos-de-fraude-digital-desde-colombia/

Gómez, H. (01 de 10 de 2019). *https://www.asobancaria.com/14-congreso-de-prevención-del-fraude-y-seguridad/*. Recuperado el 22 de 11 de 2023, de https://www.asobancaria.com

González g, f. l. (2014). *Bibliotecadigital .usb.edu.co*. Recuperado el 20 de 04 de 2024, de https://bibliotecadigital.usb.edu.co/server/api/core/bitstreams/4d69628b-310e-4cf8-983a- 0348f7cc7096/content

Granados, C. (2023). *Biometria: qué es, cómo se hace y para qué sirve.* Obtenido de Truora soluciones Tecnológicas : https://blog.truora.com/es/biometria

Granados, C. (17 de 11 de 2023). *Truora Soluciones Tecnologicas.* Recuperado el 08 de 05 de 2024, de https://blog.truora.com/es/biometria: https://blog.truora.com/es/biometria

Gutiérrez, J. (06 de 2018). *https://www.fasecolda.com/cms/wp- content/uploads/2019/08/ce007-2018.pdf.* https://www.fasecolda.com/cms/wp- content/uploads/2019/08/ce007-2018.pdf

Hernández, L. (22 de 05 de 2022). Recuperado el 13 de 10 de 2023, de https://www.agenciapi.co/investigacion/empresas/el-drama-de-una-cliente-suplantada-en-siete-bancos-con-15-productos-financieros#google_vignette

https://alicebiometrics.com/. (2018). Reconocimiento Facial Biométrico. *Articulo Tecnológico*, https www bilib que es y cómo funciona la Biometría facial.

https://canal1.com.co/. (2023). Reportaje fraudes. 25-28.

https://colcert.gov.co/. (19 de 11 de 2019). cayo banda que falsificaba huellas dactialares para solicitar millonarios creditos. (c. 1, Entrevistador)

https://www.bilib.com. (s.f.). *https://www.bilib.es/actualidad/articulos-tecnologicos/post/noticia/reconocimiento-facial-biometrico-que-es-como-funciona-y-cuales-son- los-principales-actores-del-secto/*. Obtenido de Reconocimiento facial biométrico: qué es, cómo funciona y cuáles son los principales actores del sector: https://www.bilib.es/actualidad/articulos-tecnologicos/post/noticia/reconocimiento-facial-biometrico-que-es-como-funciona-y-cuales-son- los-principales-actores-del-secto/

https://www.registraduria.gov.co/. (s.f.). https://registraduria.gov.co/ https://www.registraduria.gov.co/. (2023). *Biometria*. Recuperado el 26 de 10 de 2023, de https://wsp.registraduria.gov.co/biometria/operadores/listar/ https://www.superfinanciera.gov.co/. (21 de 04 de 2022). *Superintendencia Financiera*.

Recuperado el 25 de 10 de 2023, de https www Suoerintendenciafinanciera.gov.co https://www.superfinanciera.gov.co/. (28 de 10 de 2023). *Asobancaria infobae*. Recuperado el 26 de 11 de 2023, de https www infobae.com https://www.xataka.com/. (10 de 06 de 2020). *¿Sabes qué es el selfie pay?* https://blog.payxpert.com/es/sabes-que-es-el-selfie-pay: https://blog.payxpert.com/es/sabes-que- es-el-selfie-pay

ID, R. (2022). *https://reconoserid.com/*. https://reconoserid.com/ Incibe. (s.f.). *Biometría: amenazas, riesgos y vulnerabilidades*. Obtenido de incibe : https://www.incibe.es/empresas/blog/biometria-amenazas-riesgos-y-vulnerabilidades

J, T. (22 de 07 de 2014). Liveness detection to fight biometric spoofing. United States.

Jhonatan, M. (s.f.). *https://www.asobancaria.com/*. Obtenido de https://www.asobancaria.com/.

Khade, S. ,. (2023). *tTechniques for biometric security: A systematic review of presentation attack detection systems.* London: Multimedia Tools and Applications.

Larousse. (s.f.). https://www.diccionarios.com/diccionario/espanol/FINANCIERO:.

Lefevre. (15 de 09 de 2020). *https://espaciopymes.com/noticias/la-biometria-y-la- proteccion-de-datos/*. https://espaciopymes.com/noticias/la-biometria-y-la- proteccion-de-datos/

Liu, X. (2021). *Biometric authentication deep learning for continuous user verification.* *In 2021 6th International Conference on Signal and Image Processing,.* ICSIP.

Liu, X. Y. (2021). Biometric authenticaction deep learning for continuos. *ICSIP* . Martha, A.

(2022). Cuadernos de Política Criminal. (2022). . *Suplantacion de Identidad Criminal*, 125-163.

Moncayo, w. (s.f.). *certicàmara* . https://web.certicamara.com/

Moreno, I. (2017). *Sistema De Control De Acceso Por Biometría.* Bogotá: Visión electrónica.

Moreno, M. (25 de 01 de 2021). *https://web.certicamara.com/*. Recuperado el 23 de 11 de 2023, de https://web.certicamara.com/

Ortiz, J. G. (2022). Análisis de las Técnicas de Machine learning,aplicadas a los fraudes banacarios,. *Revista Cientifica Ciencia Y Tecnologia.*, 22-33.

Ospina, A. (13 de 08 de 2025). *https://www.larepublica.co/finanzas/superfinanciera- lanza-nueva-herramienta-para-no-caer-en-ofertas-fraudulentas-4202196.* https://www.larepublica.co/finanzas/superfinanciera-lanza-nueva-herramienta-para-no-caer-en-ofertas-fraudulentas-4202196: https://www.larepublica.co/finanzas/superfinanciera-lanza-nueva- herramienta-para-no-caer-en-ofertas-fraudulentas-4202196

Pinzón, S. (2022). *Olimpia IT*. Recuperado el 18 de 10 de 2023, https://olimpiait.com/home-espanol/

Ramírez, E. (2015). *Super intendencia financiera de Colombia* . https://www.superfinanciera.gov.co/.

Reyes, M. (02 de 02 de 2022). *Modelo de seguridad y trasparencia Bancaria para trasferencias basado en Block chain*. Recuperado el 07 de 09 de 2023, de http://dspace.ups.edu.ec/handle/123456789/23336

Rivera, Y. M. (2022). *Analisis Biometrico sobre Ciberseguridad* . Brasil : RISTI Revista iberica de Sistemas y Tecnologia.

Rivera, Y. M. (2022). *Tecnica de ataque de suplantacion de identidad y evolucion.* España: RISTI Revista iberica de sistemas y Tecnologia.

Rivera, Y. M. (2022). *Tecnica de Ataque de Suplantacion de identidad y evolucion.* España: RISTI Revista iberica de sistemas y Tecnologías.

Rodríguez, R. (2020). *Características de la huella dactilar.*

Rodríguez, R. (20 de 11 de 2020). *Estuyando*. https://estudyando.com/caracteristicas-comunes-de-las-huellas-dactilares/

Sánchez, C. (2023). *Suplantación y sus Características.* España: RISTI Revista Ibérica de Sistemas y Tecnología de la información.

Santiago, P. (s.f.). *Superintendencia financiera.* https://www.superfinanciera.gov.co/: https://www.superfinanciera.gov.co/

Stephen, M. (02 de 2018). *History of Biometrics*. Recuperado el 27 de 10 de 2023, de https www biometricupdate.com

Tobon, C. (2020). *Modelo de la administración Digital sobre Block chain para la mitigación de riesgo por suplantación en sistemas e-baking.* Recuperado el 12 de 10 de 2023, de http/handle.net/20.500.12622/4457

Torres, F. (2019). suplantacion de identidad digital. En V. christian, *suplantacion de identidad digital.* (págs. 126-163). Bogota.