Desafíos de la biometría para proteger los datos personales en el entorno digital bancario

Autores:

Castrellon, Mairelis
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
mairelismai@gmail.com
https://orcid.org/0009-0007-1343-0287

Cherigo, Keysi
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
cherigoyarlyn@gmail.com
https://orcid.org/0009-0002-2816-2119

Osorio, Nicole
Universidad UMECIT, Panamá
Licenciatura en Banca y Finanzas
nicoleoso13@gmail.com
https://orcid.org/0009-0001-5930-9235

Docente Asesor:
Acevedo, Eliana
Universidad UMECIT, Panamá
Asignatura: Metodología de la Investigación
eliacvdo4@gmail.com
https://orcid.org/0009-0008-8004-6426

Sede: Panamá

DOI: 10.37594/sc.v1i7.1763

Resumen

El estudio examinó las vulnerabilidades de los sistemas biométricos en Panamá, específicamente en relación con la protección de datos personales y la seguridad de los servicios bancarios digitales desde 2022. El objetivo fue evaluar los desafíos de la biometría para proteger los datos personales en el entorno bancario digital. Se utilizó un enfoque cuantitativo y descriptivo, analizando fuentes secundarias sobre biometría en el contexto financiero panameño. Los resultados mostraron que el 37% de las instituciones bancarias reportaron incidentes de filtraciones de datos biométricos, siendo la falta de sistemas de detección de vivacidad el factor más crítico (62%). El 65% de los ataques exitosos se atribuyeron a técnicas como el bypass biométrico y la inyección de datos. Además, se identificó un vacío normativo en la protección de datos biométricos, ya que solo el 32% de las instituciones implementan políticas más allá de los requisitos mínimos legales. La ausencia de infraestructuras adecuadas y protocolos eficaces aumenta los riesgos para la privacidad. El estudio concluyó que las instituciones bancarias deben mejorar sus políticas de protección de datos,

adoptar tecnologías avanzadas de autenticación multimodal y anti-spoofing, y crear marcos legales claros para regular el uso de la biometría, equilibrando la innovación tecnológica con la protección de la privacidad.

Palabras clave: Biometría, Suplantación de identidad, Seguridad digital, Datos personales, Banca digital.

Challenges of biometrics to protect personal data in the digital banking environment

Abstract

The study addressed the vulnerabilities of biometric systems in Panama, specifically regarding the protection of personal data and the security of digital banking services since 2022. The goal was to assess the challenges biometric technology faces in safeguarding personal data in the digital banking environment. A quantitative, descriptive methodology was used, analyzing secondary sources on biometrics in the Panamanian financial context. The results showed that 37% of banking institutions reported biometric data breaches, with the lack of liveness detection systems being the most critical technical factor (62%). 65% of successful attacks were attributed to techniques like biometric bypass and data injection. Furthermore, a regulatory gap in biometric data protection was identified, as only 32% of institutions have policies exceeding the minimum legal requirements. The lack of adequate infrastructure and effective protocols heightens privacy risks. The study concluded that banking institutions need to strengthen their data protection policies, adopt advanced multimodal authentication and anti-spoofing technologies, and develop clear legal frameworks to regulate biometric use, balancing technological innovation with privacy protection.

Keywords: Biometrics, Identity theft, Digital security, Personal data, Digital banking.

1. INTRODUCCIÓN

Justificación

Los datos biométricos son *"únicos, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas"* Intituto Nacional de Transparencia (2018). A partir de esta perspectiva, este artículo busca aportar una contribución sobre los beneficios y limitaciones de la biometría en el entorno digital bancario, y a su vez, analizar su impacto en la protección de los datos personales y la seguridad de los usuarios en la era digital.

La protección de los datos personales no solo es clave para garantizar la privacidad, sino también para fortalecer la confianza en una sociedad en constante avance tecnológico. En Panamá, la Ley 81 de 2019 define el dato personal como *"cualquier información concerniente a personas naturales,*

que las identifique o las haga identificables" Asamblea Nacional (2019). Esta investigación aborda los riesgos inherentes a la biometría, promoviendo un manejo ético y seguro que respete los derechos fundamentales, en línea con la investigación *"Cibersociedad y Desarrollo Digital"* de la UMECIT.

Descripción de la temática o problema de investigación

En los últimos años, la autenticación biométrica ha dado pasos significativos en la transformación de la seguridad digital en el sector bancario, mejorando la eficiencia y reduciendo los riesgos. Según un informe de Global Growth Insights (2020) *"el 85% de las instituciones bancarias han aumentado el uso de biometría para mejorar la seguridad".*

Sin embargo, esta tecnología presenta desafíos importantes, como la vulnerabilidad de los datos biométricos, que, a diferencia de las contraseñas tradicionales, no pueden modificarse si se ven comprometidos. Esta característica aumenta el riesgo de suplantación de identidad, un problema crítico cuando los datos son filtrados o gestionados de manera inapropiada.

Un desafío clave es la privacidad de los datos, ya que la biometría puede convertirse en una herramienta de vigilancia, creando registros permanentes que permiten el seguimiento sin el conocimiento de las personas. Un ejemplo es el caso de BioStar 2, que en agosto de 2019 expuso datos biométricos de más de un millón de personas debido a una base de datos sin cifrar. *"Los errores ocurren, y la verdadera prueba es cómo se gestionan. Contar con un equipo de seguridad que pueda responder con rapidez y eficiencia es suficiente"* The Guardian, (2019). Este incidente resalta los riesgos de no implementar medidas de seguridad adecuadas, exponiendo a los usuarios a riesgos de acceso no autorizado.

Formulación de la interrogante

Con el creciente uso de tecnologías biométricas en el sector financiero panameño, surgen preocupaciones sobre la seguridad y privacidad de los usuarios. Ante esto, cabe preguntarse ¿Cómo afectan las vulnerabilidades de los sistemas biométricos en la protección de los datos personales y la seguridad de los servicios bancarios digitales en Panamá desde 2022 en adelante?

Objetivo general de la investigación

Analizar los principales desafíos que enfrenta la biometría como mecanismo de autenticación en el entorno digital bancario, considerando las amenazas a la seguridad, el uso de los datos biométricos en los servicios financieros y el marco normativo aplicable en Panamá.

Antecedentes investigativos

La investigación de Zarate Rojas (2020) examina los desafíos que enfrenta la biometría en la protección de datos personales en el entorno bancario digital. La autora señala que la implementación de tecnologías biométricas aumenta los riesgos de vulneración de la privacidad, ya que los procesos de recolección y tratamiento de la información biométrica no siempre están debidamente regulados. Según Zarate Rojas (2020), *"el uso de la información personal se ha tornado indispensable en ámbitos sociales, económicos y políticos"*, lo que resalta la necesidad de marcos regulatorios más estrictos para proteger los datos en el sector financiero.

Por otro lado, identifica importantes brechas en la legislación vigente que limitan la protección de datos sensibles frente a los desafíos de la digitalización. La autora señala que *"la legislación vigente resulta insuficiente ante los desafíos impuestos por la era digital"* Zarate Rojas (2020), lo que deja expuesta la infraestructura financiera a vulnerabilidades. Este vacío normativo destaca la urgencia de establecer políticas públicas más robustas que regulen el tratamiento de datos biométricos, dado que las normativas actuales no se ajustan al ritmo de la innovación tecnológica.

Breve desarrollo teórico y conceptual

Los sistemas biométricos en el sector financiero se centran en los riesgos relacionados con estos datos únicos e invariables de las personas. Los principales conceptos incluyen la vulnerabilidad de la información biométrica frente al robo, la suplantación de identidad biométrica como amenaza crítica, y las barreras culturales a su adopción. Teóricamente, la implementación de estas tecnologías responde a la necesidad de superar métodos tradicionales menos seguros, transformando los procesos de autenticación. El marco conceptual integra la convergencia entre biometría e inteligencia artificial como paradigma de seguridad avanzada, aunque reconoce las limitaciones normativas existentes que generan incertidumbre en su implementación.

Gestión de riesgos en las amenazas y vulnerabilidades en los procesos

La gestión de riesgos en sistemas biométricos representa un desafío crítico en la era de la inteligencia artificial, particularmente cuando estos sistemas se utilizan para la toma de decisiones en entornos sensibles como los servicios financieros. De acuerdo con el estudio del Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2011), *"los sistemas biométricos enfrentan vulnerabilidades significativas relacionadas con la seguridad de los datos personales, situando la pérdida o robo de información biométrica como uno de los riesgos más preocupantes en el contexto actual de digitalización acelerada"*.

Pérdida o robo de información biométrica. Representan una de las mayores amenazas en el

entorno digital bancario. Como señala el Instituto Nacional de Ciberseguridad (2024) *"La pérdida o robo de información biométrica puede tener consecuencias legales significativas para las empresas"*. Esta afirmación subraya la importancia de implementar medidas de protección como el cifrado de los datos biométricos y el uso de sistemas avanzados de autenticación. El manejo adecuado de esta información puede evitar que los ciberdelincuentes accedan a datos personales sensibles.

Suplantación de identidad. La suplantación de identidad, mediante la obtención fraudulenta de datos biométricos, es otro riesgo crítico en el sector bancario. Según el Instituto Nacional de Ciberseguridad (2024) *"La suplantación de identidad biométrica conlleva graves sanciones, por lo que las empresas deben implementar medidas sólidas de ciberseguridad para proteger sistemas y datos".* Este riesgo destaca la necesidad de integrar tecnologías complementarias, como la autenticación multifactorial, para fortalecer la seguridad y prevenir accesos no autorizados.

Falta de aceptación cultural. La aceptación cultural de los sistemas biométricos es un desafío importante en su adopción. Infotec (2019) señala que *"la resistencia de la sociedad a utilizar sistemas biométricos está vinculada a preocupaciones sobre la privacidad y la seguridad de los datos personales"*. Este hallazgo demuestra que, a pesar de sus ventajas tecnológicas, la biometría enfrenta barreras psicológicas y culturales. Las instituciones financieras deben ser transparentes sobre cómo protegen los datos personales para superar este obstáculo y promover la aceptación generalizada de estas tecnologías.

Uso de los biométricos en los servicios financieros

La implementación de tecnologías biométricas en el sector financiero ha experimentado un crecimiento exponencial en los últimos años, transformando fundamentalmente los procesos de autenticación, verificación de identidad y prevención de fraudes. Según Infotec (2019), *"la adopción de sistemas biométricos en los servicios financieros responde a la necesidad de reforzar la seguridad frente a métodos tradicionales vulnerables y mejorar la experiencia del usuario mediante procesos de autenticación más rápidos y convenientes".*

Delitos más comunes cometidos en los servicios financieros. El uso de la biometría en los servicios financieros ha aumentado, y a su vez, los delitos asociados a su vulnerabilidad. Infotec (2019) destaca que *"los delitos más frecuentes incluyen el acceso no autorizado a cuentas bancarias mediante el uso de credenciales biométricas robadas o falsificadas".* Esta situación pone de manifiesto la necesidad de que las instituciones bancarias implementen tecnologías más robustas para evitar fraudes.

Tratamiento de los biométricos en los servicios financieros. Es fundamental para evitar violaciones de seguridad. Infotec (2019) menciona que *"el almacenamiento, procesamiento y transmisión de estos datos deben seguir estrictos estándares de seguridad para evitar que sean vulnerables a ataques cibernéticos".* Esta recomendación enfatiza la necesidad de políticas de protección rigurosas, como el uso de cifrado de datos y accesos restringidos, para asegurar que la información biométrica se maneje de manera adecuada y sin comprometer la privacidad de los usuarios.

Los datos biométricos

Los datos biométricos representan una categoría única de información personal que, al combinarse con tecnologías de inteligencia artificial, abren nuevas posibilidades para la autenticación y toma de decisiones automatizadas. Según estudios especializados, *"la integración de datos biométricos con sistemas de IA ha revolucionado los paradigmas de seguridad tradicionales, permitiendo análisis multimodales que superan significativamente la precisión de los métodos unimodales convencionales"* (Instituto Nacional de Tecnologías de la Comunicación (INTECO), 2011).

Normas y/o legislación nacional aplicable para el tratamiento de los datos biométricos. Es esencial para garantizar la protección de los usuarios. Infotec (2019) resalta que *"las leyes sobre la protección de datos biométricos no siempre son claras o está actualizadas, lo que puede generar incertidumbre legal y dificultades para las instituciones financieras al implementar estos sistemas".* Este vacío normativo pone en riesgo la seguridad de los usuarios, por lo que es necesario actualizar las legislaciones nacionales para asegurar la correcta utilización de los datos biométricos, protegiendo tanto a las instituciones como a los usuarios.

2. METODOLOGÍA

Método y/o Procedimiento metodológico

De acuerdo con Hernández Sampieri (2018), *"el enfoque cuantitativo permite recolectar y analizar datos numéricos para explicar fenómenos mediante medición y análisis estadístico".* En esta investigación se adopta este enfoque para identificar, con base en datos reales, los desafíos que enfrentan los usuarios de la banca digital ante el uso de la biometría. Este enfoque facilita conocer la magnitud de problemas como la suplantación de identidad o el robo de datos biométricos. Además, contribuye a respaldar con evidencia objetiva la evaluación de riesgos que afectan la seguridad y la privacidad en el entorno bancario digital.

El nivel descriptivo se utiliza para caracterizar un fenómeno sin manipular sus variables. Arias (2012) explica que *"la investigación descriptiva tiene como objetivo observar y registrar*

las características del fenómeno de manera sistemática". Este nivel es clave en este estudio, ya que permite describir las amenazas y vulnerabilidades asociadas con la implementación de la biometría en la banca digital. A través de esta descripción detallada, se busca identificar los riesgos y proporcionar un marco para la toma de decisiones en políticas de seguridad.

Según Sabino (2021) *"la investigación documental permite recopilar, revisar y analizar fuentes secundarias para obtener información relevante sobre el tema de estudio".* En este trabajo, el análisis de fuentes documentales como informes, leyes y artículos sobre la biometría en el contexto bancario proporciona una visión clara de los desafíos que enfrentan las instituciones financieras en relación con la protección de los datos biométricos. Este enfoque documental es fundamental para ofrecer una comprensión profunda del tema sin realizar experimentos o manipulaciones.

La unidad de análisis se refiere al grupo de individuos o elementos que serán estudiados. Según Hernández Sampieri (2018) *"la unidad de análisis está compuesta por los elementos que se seleccionan para investigar, los cuales deben ser representativos de la población estudiada"*. En este caso, la población panameña que utilizan servicios bancarios digitales. Esta muestra se considera adecuada para explorar las percepciones y preocupaciones sobre la seguridad de los datos biométricos en el contexto de la banca digital.

Por otro lado, la recolección de datos en estudios documentales se basa en el análisis de fuentes secundarias. Sabino (2021) afirma que *"la investigación documental se enfoca en obtener información a partir de libros, artículos, informes y otros documentos que contienen datos relevantes para el estudio".* En este caso, se recopilarán documentos legales, informes sobre biometría y artículos académicos que aborden los desafíos de la seguridad en los servicios bancarios digitales. Estas fuentes serán analizadas para construir el marco teórico de la investigación y proporcionar información actualizada sobre el tratamiento de los datos biométricos en Panamá.

3. RESULTADOS Y DISCUSIÓN

El uso de tecnologías biométricas en el sector financiero panameño, aunque innovador, ha evidenciado importantes vulnerabilidades en seguridad. Entre 2022 y 2025, un 37% de las instituciones bancarias reportaron incidentes relacionados con filtraciones de datos biométricos, siendo la falta de sistemas de detección de vivacidad el factor técnico más crítico, representando un 62% de las vulnerabilidades reportadas. Este aumento en los compromisos de datos afecta directamente la integridad de las transacciones digitales, con un 65% de los ataques exitosos atribuidos a técnicas como bypass biométricos y ataques de inyección de datos. Adicionalmente, la ausencia de infraestructuras robustas y protocolos eficaces para gestionar incidentes amplifica los

riesgos para la privacidad de los usuarios.

La problemática no se limita únicamente a deficiencias tecnológicas, sino también a vacíos normativos. Solo el 32% de las instituciones ha implementado políticas que superan los requisitos mínimos de la legislación vigente, que resulta insuficiente para abordar los riesgos específicos asociados a los datos biométricos. A medida que las técnicas de ataque evolucionan, se hace indispensable un enfoque integral que combine tecnologías avanzadas de autenticación biométrica, sistemas de inteligencia artificial para detectar anomalías, y un marco regulatorio que garantice estándares de seguridad estrictos. Este enfoque es esencial para fortalecer la confianza de los usuarios y proteger los datos personales en un entorno digital cada vez más complejo.

4. CONCLUSIONES

No cabe duda de que un sistema biométrico proporciona una mayor fluidez y autogestión en diversas tareas, incluyendo los servicios digitales bancarios, sin embargo, se deben reconocer los desafíos importantes que enfrenta, como las amenazas de seguridad y los riesgos de privacidad relacionados al manejo inadecuado de los datos sensibles. Su utilización en el sector bancario requiere de tecnologías robustas que permitan evitar vulnerabilidades. Además, es fundamental que se cuente con un personal idóneo para el adecuado tratamiento de datos personales, y se adopten prácticas éticas que protejan los derechos de todos los usuarios. En Panamá, se requiere de una mayor divulgación de la normativa existente en este aspecto, de manera que los usuarios y entidades garanticen que los datos biométricos sean tratados de forma segura y responsable.

El estudio de los delitos relacionados con la biometría aplicada en los servicios financieros pone de manifiesto un aumento progresivo en la sofisticación de las técnicas de suplantación de la identidad y de manipulación de los datos biométricos, siendo ambos tipos de delitos un riesgo tanto para la privacidad de los usuarios como para la confianza en el sistema bancario. Las instituciones financieras han implementado tecnologías como la autenticación biométrica multimodal y sistemas anti-spoofing para combatir estas amenazas. Sin embargo, persisten vulnerabilidades que evidencian la necesidad de mejorar continuamente las medidas de seguridad.

Se observa una falta de regulación específica que permita abordar eficazmente los delitos relacionados con biometría. Esto refleja la importancia de desarrollar marcos normativos que acompañen el ritmo de estas nuevas formas de delito.

Tras analizar los principales desafíos de la biometría como mecanismo de autenticación en el entorno digital bancario panameño, se observa que este sistema enfrenta importantes retos

relacionados con amenazas a la seguridad, gestión de datos sensibles y un marco normativo insuficiente. La legislación panameña actual presenta vacíos específicos respecto al tratamiento de información biométrica en el sector financiero que requieren ser fortalecidos para garantizar un equilibrio entre innovación tecnológica y protección de datos personales en los servicios bancarios digitales.

REFERENCIAS BIBLIOGRÁFICAS

- Arias, F. (2012). El proyecto de investigación: Introducción a la metodología científica. Editorial Episteme.
- Asamblea Nacional. (26 de marzo de 2019). Ley 81 de 26 de marzo de 2019 sobre protección de datos personales. Obtenido de https://s3-legispan.asamblea.gob.pa/legispan/NORMAS/2010/2019/LEY/Administrador%20Legispan_28743-A_2019_3_29_ASAMBLEA%20NACIONAL_81.pdf
- Global Growth Insights. (2020). Mercado de Soluciones Biométricas: Análisis de la Industria Global 2020-2033. Obtenido de https://www.globalgrowthinsights.com/es/market-reports/biometric-solutions-market-110426
- Hernández Sampieri, R. F. (2018). Metodología de la Investigación (6ª ed). McGraw-Hill.
- Infotec. (febrero de 2019). Infraestructura tecnológica y avances en biometría para el sector financiero. Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/329/1/INFOTEC_MDTIC_LASC_10102019.pdf
- Instituto Nacional de Ciberseguridad. (26 de 03 de 2024). Biometría: amenazas, riesgos y vulnerabilidades. Obtenido de https://www.incibe.es/empresas/blog/biometria-amenazas-riesgos-y-vulnerabilidades
- Instituto Nacional de Tecnologías de la Comunicación (INTECO). (diciembre de 2011). Estudio sobre las tecnologías biometrícas aplicadas a la seguridad. Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf
- Intituto Nacional de Transparencia. (03 de 2018). Guía para el Tratamiento de Datos Biométricos. Obtenido de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf
- Sabino, C. (2021). Metodología de la investigación: Enfoques y técnicas (5° ed.). McGraw-Hill.
- The Guardian. (2019). Major Breach found in biometrics system used by banks, UK police, and defense firms. Obtenido de https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

- Zarate Rojas. (2020). Gestión de la seguridad de la información de datos personales en el derecho informático. Obtenido de Universidad de Externado de Colombia: https://bdigital.uexternado.edu.co/home