Tipo de artículo: investigación
Sección: Administración y Gestión

Artículo resultado del proyecto de investigación "plataforma tecnológica para fortalecer los servicios ciudadanos digitales que permita la transición a la identidad digital en Colombia para tramites y servicios no presenciales" de Olimpia IT

Biometría en el contexto de la ciberseguridad, retos empresariales

Biometrics in the context of cybersecurity, business challenges

Biometria no contexto da cibersegurança, desafios empresariais

Doi: 10.53995/23463279.1631

Recibido:16/03/2024 Aprobado: 10/10/2024

Por: Jeffry Restrepo Suárez[1]; Federico Clavijo López[2] & Juan Gonzalo Castellanos[3]

Resumen

La biometría se ha convertido en un elemento clave dentro de la ciberseguridad, permitiendo la autenticación segura de usuarios en diversos sectores, con especial impacto en el sector financiero y empresarial. Su implementación contribuye a la prevención del fraude, la protección de datos y la optimización de procesos digitales.

Sin embargo, la adopción de tecnologías biométricas también presenta retos significativos. Aspectos como la regulación, la privacidad, la infraestructura tecnológica y la resistencia al cambio son factores críticos que influyen en su implementación.

Este artículo analiza los desafíos y oportunidades de la firma digital biométrica dentro del panorama de la ciberseguridad, destacando su relevancia en la transformación digital de empresas y entidades financieras. Se abordan aspectos técnicos, regulatorios y socioeconómicos, proporcionando un marco de referencia para su implementación efectiva y segura.

[1] Especialista en Inteligencia de Negocios. Data Manager en Olimpia IT. Contacto: john.rincon@olimpiait.com Orcid: https://orcid.org/0009-0009-4127-9830

[2] Máster en desarrollo emprendedor e innovación. Subdirector Innovación y Productividad en Tecnalia Colombia. Contacto: fclavijo@tecnaliacolombia.org; federicoclalo@gmail.com Orcid: https://orcid.org/0000-0002-9763-8881

[3] Especialista Department Of Health And Social Security- Hospital Engineering. Consultor en temas de implementación de tecnología en Tecnalia Colombia. Contacto: Orcid:

Palabras clave: Información; Ciberseguridad; Biometría; Banca; Desarrollo

Abstract

Biometrics has become a key element in cybersecurity, enabling secure user authentication across various sectors, with a significant impact on the financial and business landscape. Its implementation helps prevent fraud, protect data, and optimize digital processes. However, the adoption of biometric technologies also presents significant challenges. Regulatory compliance, privacy concerns, technological infrastructure, and resistance to change are critical factors influencing their implementation. This article analyzes the challenges and opportunities of biometric digital signatures within the cybersecurity landscape, highlighting their role in the digital transformation of businesses and financial institutions. It explores technical, regulatory, and socioeconomic aspects, providing a framework for their effective and secure implementation.

Key Words: Information; Cybersecurity; Biometrics; Banking; Development

Resumo

A biometria tornou-se um elemento-chave na cibersegurança, permitindo a autenticação segura de usuários em diversos setores, com impacto significativo no setor financeiro e empresarial. Sua implementação contribui para a prevenção de fraudes, a proteção de dados e a otimização de processos digitais. No entanto, a adoção de tecnologias biométricas também apresenta desafios importantes. Questões regulatórias, preocupações com privacidade, infraestrutura tecnológica e resistência à mudança são fatores críticos que influenciam sua implementação. Este artigo analisa os desafios e oportunidades das assinaturas digitais biométricas no contexto da cibersegurança, destacando seu papel na transformação digital de empresas e instituições financeiras. São abordados aspectos técnicos, regulatórios e socioeconômicos, fornecendo um referencial para sua implementação eficaz e segura.

Palavras-chave: Informaçã; Segurança cibernética; Biometria; Bancos; Desenvolvimento

Códigos JEL: M1, M4

introducción

La ciberseguridad, también conocida como seguridad de la tecnología de la información, es un proceso formal que se implementa en las organizaciones con el propósito de proteger sus activos digitales y la información sensible frente a diversas amenazas. Estas amenazas pueden originarse tanto desde el interior como desde el exterior de la organización e incluyen intentos de acceso no autorizado, análisis de configuraciones de dispositivos, ingeniería social para la obtención de credenciales y suplantación de identidad. El objetivo de estas acciones malintencionadas suele ser el robo de información confidencial, la interrupción de operaciones o incluso el chantaje a empresas mediante el uso indebido de datos.

A medida que la transformación digital avanza, la protección de la información se ha convertido en una prioridad para sectores como la banca, el comercio electrónico, la salud y el sector público. Según estimaciones de Cybersecurity Ventures, se espera que los daños económicos provocados por ciberataques alcancen los $10.5 billones de dólares en 2025, frente a los $3 billones de dólares en 2015, lo que evidencia la necesidad urgente de reforzar las estrategias de ciberseguridad.

Uno de los mecanismos más efectivos para la protección digital es la biometría, que se ha consolidado como una tecnología clave en la autenticación de usuarios. Su capacidad para verificar la identidad mediante características físicas o conductuales únicas, como huellas dactilares, reconocimiento facial o patrones de escritura, ha impulsado su adopción en múltiples industrias. En particular, el sector financiero ha integrado la biometría para fortalecer la seguridad en transacciones, reducir fraudes y optimizar procesos digitales.

Sin embargo, la incorporación de soluciones biométricas no está exenta de desafíos. Su implementación requiere una infraestructura tecnológica robusta, políticas claras de protección de datos y una adecuada gestión de riesgos. Además, surgen debates sobre su regulación, la privacidad de los usuarios y la aceptación social de estas tecnologías.

En este contexto, OLIMPIA IT, empresa especializada en transformación y protección digital, y TECNALIA COLOMBIA, centro de innovación y productividad reconocido por Minciencias, han unido esfuerzos para investigar y desarrollar soluciones biométricas seguras y eficientes. Su objetivo es generar conocimiento en torno a estos avances tecnológicos y contribuir a la mitigación de riesgos de fraude y suplantación en el entorno digital.

Este artículo analiza los desafíos y oportunidades de la firma digital biométrica en el contexto de la ciberseguridad. Se abordan aspectos técnicos, regulatorios y socioeconómicos, destacando su impacto en la transformación digital de empresas y entidades financieras. A partir de este análisis, se plantean estrategias que permitan su implementación efectiva y segura.

discusión /reflexión

Aclarando inicialmente los términos, se puede decir que entre las herramientas que se han ido diseñando y poniendo en operación para garantizar una identificación precisa de las personas y entidades, están las firmas electrónicas, las firmas digitales y las firmas digitales biométricas. Cada una de ellas tiene características específicas en cuanto a su funcionamiento, nivel de seguridad y validación legal.
La firma electrónica es más un término legal que técnico, y puede ser tan simple como el nombre del firmante ingresado en una página web. Para que tenga validez jurídica, debe cumplir ciertos requisitos (Ciberseguridad, 2021):

- Verificar la identidad del firmante.
- Garantizar que el firmante tenía la intención de firmar el documento.
- Asociar la firma al documento firmado, asegurando su integridad y evitando su alteración.

La firma digital, por su parte, puede considerarse un subconjunto de la firma electrónica, ya que incorpora un mecanismo criptográfico avanzado para garantizar la autenticidad y la integridad de los documentos electrónicos. Funciona a través de algoritmos matemáticos que generan un par de claves (una pública y una privada), permitiendo validar la identidad del firmante y evitar alteraciones en el contenido firmado. IBM (2021) define la firma digital como un sello electrónico cifrado de autenticación en información digital, que permite confirmar la integridad de un mensaje y demostrar su procedencia. Cualquier cambio realizado en los datos firmados invalida la firma digital, lo que la convierte en un mecanismo altamente seguro.

La firma digital biométrica va un paso más allá al incorporar la identificación de personas mediante la medición y análisis estadístico de características físicas o conductuales únicas. Su funcionamiento se basa en el almacenamiento cifrado de estos rasgos y su posterior comparación con datos medidos en el momento de la autenticación. Esta tecnología ha sido clave en la ciberseguridad para fortalecer la protección de identidades en sectores como el financiero, gubernamental y de salud.

Existen dos tipos principales de biometría aplicadas a la firma digital biométrica:

- Biometría Física: Se basa en características corporales únicas y difíciles de falsificar. Ejemplos incluyen:
    - Huellas dactilares: Método ampliamente utilizado por su bajo costo y precisión.
    - Reconocimiento facial: Análisis de geometría facial para autenticación segura.
    - Reconocimiento del iris y escaneo de retina: Alta precisión en verificación de identidad.
    - Reconocimiento de venas en dedos y palmas: Tecnología emergente con un alto nivel de seguridad.
    - Coincidencia de ADN: Método altamente preciso, pero con limitaciones en costos y tiempos de procesamiento (Wickramasinghe, 2023).
    -

- Biometría Conductual: Analiza patrones de comportamiento únicos en cada usuario, como:
    - Firma manuscrita digitalizada: Evalúa presión, velocidad y ritmo al escribir.
    - Dinámica del tecleo: Identifica usuarios según su forma de escribir en un teclado.
    - Movimientos del ratón y dedo: Reconoce patrones de uso en dispositivos digitales.
    - Reconocimiento del habla: Análisis de voz para autenticación remota.
    - Marcha al caminar: Verificación basada en patrones de movimiento.

Desde una perspectiva técnica, la firma digital biométrica incorpora mecanismos adicionales de seguridad, como la detección de vida (Liveness Detection), que impide intentos de suplantación mediante fotos o videos falsificados. Además, emplea técnicas de cifrado avanzado y almacenamiento seguro, asegurando que los datos biométricos sean protegidos contra accesos no autorizados y alteraciones.

En este contexto, OLIMPIA IT y TECNALIA COLOMBIA han trabajado en el desarrollo y validación de soluciones de firma digital biométrica, con un enfoque en la seguridad, cumplimiento normativo y facilidad de integración en distintos sectores. Ambas organizaciones han impulsado iniciativas de investigación aplicada y proyectos tecnológicos que buscan garantizar una autenticación confiable y reducir el riesgo de fraude digital. Su colaboración ha permitido la implementación de soluciones innovadoras alineadas con estándares internacionales y regulaciones locales.

La firma digital biométrica representa una evolución en la autenticación de usuarios, pero su adopción masiva aún enfrenta desafíos relacionados con la infraestructura tecnológica, la aceptación por parte de los usuarios y la adaptación a marcos regulatorios en distintas regiones. Sin embargo, a medida que más empresas y entidades gubernamentales adopten estas tecnologías, su impacto en la ciberseguridad será cada vez más significativo, asegurando transacciones digitales más seguras y eficientes.

Algunas de las tecnologías que se pueden encontrar bajo la definición de firma digital biométrica son:

1. **Face Recognition (Reconocimiento Facial)**

El reconocimiento facial ha despertado gran interés debido a la necesidad de encontrar nuevas formas de identificar a las personas mediante métodos más seguros, el rostro se considera un rasgo distintivo único para cada individuo. Esto ha impulsado el desarrollo y la implementación de nuevas tecnologías y algoritmos para el reconocimiento facial, permitiendo así avanzar en el campo de la identificación biométrica. Las innovaciones asociadas a este tipo de firma digital facilitan la tarea de reconocer e identificar de manera más sencilla y efectiva la identidad de una persona.

El funcionamiento del reconocimiento facial consta de 3 procesos: el primero es la detección donde esencialmente se transforma un rostro en una imagen, se basa en tecnologías de visión artificial que permiten identificar a las personas en las imágenes con una precisión igual o superior a la humana y con una velocidad y eficacia mucho mayores; el segundo es el análisis que permite asignar y leer la geometría del rostro[4] y las expresiones faciales, identificando los puntos de referencia faciales que son clave para distinguir un rostro de otros objetos; y, finalmente el tercer proceso es el reconocimiento que puede identificar a una persona al comparar los rostros de dos o más imágenes y evaluar la probabilidad de que coincidan, verificando y comparando bases de datos con conjuntos de rostros. (Amazon Web Services, Inc., 2023)

A partir de estos patrones, se construye un modelo matemático que se utiliza para la extracción de características y posterior almacenamiento de la imagen facial en una base de datos. (Maltoni, Maio, D., Jain, A.K., Prabhakar, 2009), (Atta and Ghanbari, 2010).

El reconocimiento facial es una tecnología avanzada que ha revolucionado la autenticación y la seguridad en una amplia variedad de sectores, incluyendo el ámbito privado, público y financiero. Este tipo de firma digital permite una detección cada vez

[4] Por lo general, el software de reconocimiento facial busca lo siguiente: Distancia entre los ojos, distancia de la frente a la barbilla, distancia entre la nariz y la boca, profundidad de las cuencas oculares, corma de los pómulos, contorno de los labios, las orejas y la barbilla.

más precisa de los rasgos faciales a medida que una persona se autentica en diferentes sistemas y aplicaciones.

El reconocimiento facial ha tenido un impacto significativo en la mejora de la seguridad y la vigilancia de la identidad en diversas aplicaciones, como el acceso a edificios y áreas restringidas, la autenticación en dispositivos móviles, y la prevención del fraude.

2. Liveness Detection (detección de vida)

La identificación biométrica, en particular el reconocimiento facial, desempeña un papel crucial en la autenticación de individuos. Sin embargo, se ha presentado un desafío significativo en esta tecnología: la suplantación de identidad (Wang, Hao, Guo, 2013). Para abordar este problema, se ha desarrollado una técnica conocida como detección de vida (Yao, Lin, 2005), que se implementa antes del proceso de identificación biométrica facial. La detección de vida actúa como una capa adicional de seguridad en el proceso de autenticación. Esta técnica se basa en la evaluación de características faciales, centrándose en el movimiento de los ojos y la boca. Al detectar señales de vida genuina, como parpadeo o cambios en la expresión facial, la detección de vida ayuda a garantizar que la identificación biométrica se realice con la máxima precisión y evita la suplantación de identidad.

3. Biometría

La biometría es la ciencia que abarca tanto el estudio de características físicas únicas como el análisis de características cuantitativas de los seres vivos, y se utiliza para desarrollar tecnologías que permiten la identificación y autenticación de personas de manera automatizada. Estos sistemas se aplican en una variedad de campos, incluyendo la seguridad, la gestión de identidades, el acceso a dispositivos electrónicos, el control de acceso a instalaciones y la gestión de recursos humanos, entre otros. (Gupta, Kacimi, & Crispo, 2022; Report, 2019; Ruiz Marín, Milton; Rodriguez Uribe, Juan Carlos; Olivares Morales, 2009; Soni, Pal, 2021).

El uso de características físicas únicas, como la configuración del rostro, en operaciones de reconocimiento de identidad, contribuye de manera significativa a mejorar la seguridad, la gestión de identificación de usuarios y la protección en transacciones. A su vez, genera confianza en los procesos de autenticación y ayuda a prevenir actividades ilícitas en los procesos realizados por sus clientes.

La adopción de tecnologías biométricas no solo asegura la protección de los dispositivos de los clientes, sino que también está presente en soluciones digitales que permiten validar y acceder a servicios bancarios. Este enfoque tecnológico aporta comodidad y confianza tanto a los usuarios como a las instituciones financieras. Por ejemplo, para contratar un crédito, bastaría con que el cliente acredite su identidad mediante tecnologías biométricas, simplificando así el proceso y proporcionando un alto nivel de seguridad.

En la práctica, bancos como BBVA ya han incorporado la biometría en sus operaciones, permitiendo a los clientes firmar diferentes transacciones bancarias utilizando datos biométricos registrados en sus dispositivos móviles, lo cual se traduce en procesos más rápidos, seguros y cómodos para el cliente.

Además, la firma digital biométrica no solo proporciona una capa adicional de seguridad en comparación con otros métodos de autenticación, como podrían ser las contraseñas estáticas o dinámicas, sino que también tiene potencial como valor probatorio ante los tribunales. Esto significa que las firmas biométricas podrían permitir firmar contratos legalmente vinculantes con plenas garantías legales, lo cual es crucial para la legalización de trámites bancarios.

En este escenario, la firma digital biométrica se presenta como una transición natural en la era digital, brindando un camino hacia la optimización de los procesos bancarios y una mayor protección contra el fraude y las amenazas cibernéticas. Sin embargo, su implementación y aceptación en Latinoamérica presenta varios retos que van desde lo tecnológico hasta consideraciones de carácter socioeconómico.

Visión general de la banca digital en Colombia.

La situación de la banca digital en Colombia ha experimentado un gran crecimiento en los últimos años. Desde 2017 hasta 2021, casi se duplicó la cantidad de bancos digitales en la región. Según un estudio de BPC, actualmente hay en Latinoamérica más de 50 de los denominados neobancos, entidades financieras que ofrecen servicios de intermediación financiera 100% digital (BPC, 2023). Esta tendencia de crecimiento se prevé que se mantenga en el futuro, ya que el 17% de los bancos en la región tienen como objetivo transformarse en entidades 100% digitales, según el "Estudio Latinoamericano de Banca Digital 2022". No solo los neobancos operan digitalmente: prácticamente todas las entidades bancarias tradicionales disponen de herramientas web o su propia aplicación en las que es posible realizar la gran mayoría de gestiones bancarias, complementando su oferta presencial. (INFOCORP, 2022)

Descripción de la firma digital biométrica y su relevancia actual.

En el contexto colombiano, la Ley 527 de 1999 define la firma digital como "*el valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje para determinar que este valor se haya obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no haya sido modificado después de efectuada la transformación.*" (CONGRESO DE COLOMBIA, 1999)

La firma digital biométrica se ha convertido en una herramienta con un enorme potencial para abordar desafíos contemporáneos en diferentes sectores de la economía, como el sector bancario, especialmente en lo que respecta a la autenticación segura y la minimización del fraude.

Adopción de firma digital biométrica, situación actual y beneficios esperados.

La adopción de este tipo de herramientas demuestra que ha tenido una gran acogida por parte de los usuarios. Por ejemplo, el número de depósitos electrónicos en Colombia se

incrementó de 4.8 millones en 2018 a 13.3 millones en 2020, mientras que se observó una tendencia similar con las cuentas de ahorro, que pasaron de 2,2 millones a 10,1 millones en este mismo periodo. (VALORA ANALITIK, 2021)

En el contexto de Latinoamérica, la firma digital biométrica ofrece un método de autenticación seguro y eficiente, lo que es crucial en una región donde el fraude y la ciberdelincuencia son grandes preocupaciones. Los bancos y las instituciones financieras están explorando cada vez más estas tecnologías para proporcionar servicios seguros y eficientes a sus clientes. Sin embargo, a medida que la banca digital continúa evolucionando en Latinoamérica, también lo hace la necesidad de estrategias legales y regulatorias que faciliten la adopción segura de la firma digital biométrica y generen confianza en los usuarios.

La firma digital biométrica se presenta como una solución innovadora en el ámbito bancario, brindando varios beneficios:

Seguridad y Autenticación Mejorada:

- La biometría proporciona un nivel de seguridad y autenticación altamente confiable al analizar características físicas únicas de los individuos como huellas dactilares, rostro o voz. A diferencia de las contraseñas o PINs, los datos biométricos están ligados indisociablemente a la propia persona, lo que reduce significativamente el riesgo de fraude y suplantación de identidad

Eficiencia en los Procesos y Reducción del Fraude:

- La implementación de firmas digitales biométricas permite una gestión más eficiente y ágil de los trámites bancarios. Además, al brindar un medio de verificación de identidad más seguro, se minimiza el riesgo de operaciones fraudulentas, lo que a largo plazo, puede traducirse en una reducción de costos asociados con el fraude.

Ahorro de Tiempo y Recursos:

- La firma digital biométrica facilita la automatización de procesos internos bancarios, que genera un ahorro significativo de tiempo y recursos. Por ejemplo, la identificación biométrica permite una rápida validación de la identidad del

cliente, lo que agiliza la apertura de cuentas o la autorización de transacciones También elimina el tiempo requerido para el procesamiento de documentación identificativa del cliente.

Conveniencia para los Usuarios:

- Los clientes se benefician de una experiencia más cómoda y accesible. Por ejemplo, la posibilidad de firmar documentos y autorizar transacciones de manera remota y segura, utilizando datos biométricos, evita la necesidad de desplazamientos o esperas prolongadas

Retos empresariales

La firma digital biométrica representa un avance significativo al facilitar y dar seguridad en los trámites bancarios. Sin embargo, su implementación y operativa en el ámbito bancario se enfrenta a varios desafíos técnicos y tecnológicos:

Infraestructura Tecnológica:

- Para implementar la firma digital biométrica, es indispensable contar con cierta infraestructura tecnológica, tanto por parte de la entidad bancaria como por el usuario. Esto incluiría sistemas de información con una capacidad de procesamiento adecuada, dispositivos biométricos con la precisión suficiente para enviar falsos positivos y negativos, y redes de comunicación seguras y rápidas que eviten errores. El despliegue de redes de internet móvil con una conexión estable y segura también puede tener un gran impacto en la viabilidad de esta tecnología.

Almacenamiento y Gestión de Datos:

- Los bancos necesitarán sistemas de almacenamiento seguros y eficientes para manejar los datos biométricos de los clientes. La gestión de estos datos es crucial para garantizar la seguridad y la privacidad, ya que se tratan de datos de alta sensibilidad.

Riesgos de ciberseguridad y fraude

Ciberseguridad:

- La firma digital biométrica introduce riesgos de ciberseguridad que deben ser reducidos al máximo. Esto incluye proteger los datos biométricos ante posibles accesos maliciosos y garantizar de esa manera la integridad de las transacciones bancarias

Autenticación y Verificación:

- Los sistemas de autenticación biométrica deben ser capaces de realizar verificaciones precisas y confiables para evitar el fraude y la suplantación de identidad.

Experiencia del Usuario:

- La usabilidad es un desafío importante. Los sistemas deben ser fácilmente utilizables por un amplio abanico de usuarios, incluyendo aquellos que no cuentan con los suficientes conocimientos tecnológicos. Las entidades bancarias deben tratar de ofrecer una experiencia de usuario simplificada y clara.

Educación y Capacitación:

- Es crucial proporcionar la educación y la capacitación necesaria tanto a los empleados del banco como a los clientes sobre cómo utilizar la firma digital biométrica de manera efectiva y segura, de manera que las ventajas teóricas en eficiencia y comodidad puedan verse reflejadas en la práctica.

Para lograr una implementación exitosa y una operatividad eficaz, es imperativo abordar los desafíos técnicos y tecnológicos. Esto requerirá un enfoque colaborativo que involucre, especialmente a instituciones bancarias y los proveedores de esta tecnología. Con la estrategia de implementación e inversión adecuada en tecnología y educación, es posible superar estos desafíos y avanzar hacia una adopción más amplia de la firma digital biométrica. La búsqueda de un proveedor tecnológico con experiencia surge como un elemento crucial en este aspecto.

Brecha socio-económica

Existen por otro lado, desafíos en el ámbito socioeconómico que, si bien no afectan de manera similar a todos los potenciales usuarios de la firma digital biométrica, si pueden suponer un obstáculo para ciertos sectores de la población, que pueden quedar excluidos y sin capacidad de aprovechar todos los beneficios que ofrece esta tecnología.

Brecha Digital:

- La brecha digital, donde ciertas poblaciones no tienen acceso o tienen un acceso limitado a la tecnología y a internet, puede limitar la capacidad de las personas para beneficiarse de los servicios bancarios digitales, incluyendo la firma digital biométrica.

Costos Asociados:

- La implementación de tecnologías de firma digital biométrica puede involucrar costos significativos para los usuarios. Para poder realizar este tipo de trámites y transacciones son necesarios dispositivos capaces de captar y procesar los datos biométricos, que tienen costos que pueden no ser fácilmente asumibles por ciertos grupos socioeconómicos.

Educación y Conciencia:

- La falta de educación y conciencia sobre cómo utilizar la tecnología de firma digital biométrica y los beneficios que ofrece puede ser un obstáculo para su adopción, especialmente en lugares donde la penetración de las tecnologías de la información y la comunicación en otros ámbitos es limitada.

Adopción por Parte de las Instituciones Financieras:

- Las instituciones financieras deben estar dispuestas a adoptar y promover la tecnología de firma digital biométrica para facilitar su uso entre los clientes. Aunque los costos asociados en términos de infraestructura y adaptación de procesos puedan ser altos en un principio, los beneficios esperados de su adopción tienen la capacidad de compensarlos ampliamente. Por otro lado, la incorporación de tecnología en los procesos puede encontrar resistencia entre los trabajadores de

las entidades bancarias, tanto porque requieren un cambio en los procedimientos habituales, como por el miedo a que la tecnología elimine puestos de trabajo.

Conclusiones

La firma digital biométrica ha emergido como una solución innovadora dentro del ecosistema de ciberseguridad, proporcionando autenticación segura, optimización de procesos y una mayor confianza en la validación de transacciones digitales. Su implementación ha demostrado beneficios en sectores como el financiero, gubernamental, salud y comercio electrónico, permitiendo mejorar la seguridad y reducir riesgos de fraude.

Sin embargo, la adopción de esta tecnología enfrenta desafíos importantes. La necesidad de una infraestructura tecnológica robusta, la adecuada gestión de datos biométricos y la alineación con regulaciones de protección de datos son factores críticos para su éxito. Además, persisten brechas en términos de acceso y adopción, ya que no todas las organizaciones cuentan con los recursos necesarios para su implementación efectiva.
A nivel empresarial, más allá del sector bancario, la firma digital biométrica ofrece nuevas oportunidades en áreas como el control de accesos, la gestión documental, la digitalización de procesos legales y la automatización de flujos de trabajo que requieren autenticación avanzada. La exploración de estas aplicaciones en distintos sectores puede impulsar su adopción y generar estándares que garanticen su interoperabilidad y seguridad.

Desde una perspectiva de desarrollo futuro, la integración de la firma digital biométrica con tecnologías emergentes como blockchain, inteligencia artificial y dispositivos IoT podría fortalecer aún más su confiabilidad y ampliación de uso. La investigación en métodos de detección de fraudes y el perfeccionamiento de algoritmos de autenticación son áreas clave para seguir avanzando en la madurez de esta tecnología.

Para garantizar una implementación exitosa, es fundamental la colaboración entre empresas de tecnología, reguladores y sectores estratégicos que permitan definir marcos

normativos claros y estrategias de adopción accesibles. En este sentido, la experiencia de proveedores especializados como OLIMPIA IT se convierte en un factor determinante para facilitar la transición hacia entornos digitales más seguros y eficientes, asegurando que la firma digital biométrica se convierta en un estándar confiable para la validación de identidad en el entorno empresarial y digital.

Referencias

Amazon Web Services, Inc. (2023). *AWS*. Obtenido de Centro de conceptos de computación en la nube: https://aws.amazon.com/es/what-is/facial-recognition/#:~:text=Funciona%20mediante%20la%20identificaci%C3%B3n%20y,gran%20colecci%C3%B3n%20de%20im%C3%A1genes%20existentes.

Andrews, TJ, Rogers, D., Mileva, M., Watson, DM, Wang, A. y Burton, AM (2023). Una banda estrecha de dimensiones de imagen es fundamental para el reconocimiento facial. Investigación de la visión, 212, 108297. https://www.sciencedirect.com/science/article/pii/S0042698923001219

Anton Firc, Kamil Malinka, Petr Hanácek. (2023). Deepfakes as a threat to a speaker and facial recognition. Czech Republic. www.cell.com/heliyon

Arora Shefali, Bhatia MPS. (2022). Challenges and opportunities in biometric security: A survey. Inf Secur J: Glob Perspect 2022;31(1):28–48).

Barbas Rebollo, D. (2020). Detección de noticias falsas y caras de personas manipuladas (Doctoral dissertation, Universitat Politècnica de València). https://riunet.upv.es/handle/10251/149028

BBVA. (25 de 01 de 2023). *Tendencias 2023.* Obtenido de BBVA: https://www.bbva.com/es/pe/tendencias-2023-reemplazara-la-banca-digital-a-la-atencion-presencial/

BPC. (2023). *Neobank*. Recuperado el 15 de 02 de 2014, de https://www.bpcbt.com/use-case/neobank

Canazas, A. P., Blaz, J. J. R., Martínez, P. D. T., & Mamani, X. J. (2022). Sistema de identificación de emociones a través de reconocimiento facial utilizando inteligencia artificial. Innovación y Software, 3(2), 140-150.

Capcha Huaman, A. (2021). Sistema de reconocimiento facial basado en los algoritmos Haar Cascade, DeepFace Y Luxand FaceSDK. https://repositorio.ucv.edu.pe/handle/20.500.12692/86897

Capistrán, J. I. B. (2022). Evolución del Deepfake: campos semánticos y géneros discursivos (2017-2021). Icono14, 20(1), 8. https://dialnet.unirioja.es/servlet/articulo?codigo=8560688

CAF. (2 de 12 de 2022). *Inclusion financiera.* Obtenido de Conocimiento visiones: https://www.caf.com/es/conocimiento/visiones/2022/12/inclusion-financiera-en-america-latina-que-tanto-hemos-avanzado/

Ciberseguridad. (2021). Recuperado el 01 de 02 de 2024, de Suplantacion de identidad: https://ciberseguridad.com/amenzas/suplantacion-identidad/

Ciberseguridad. (2021). Recuperado el 12 de 02 de 2024, de Firma digital que es y para que sirve: https://ciberseguridad.com/servicios/firma-digital/

CONGRESO DE COLOMBIA. (1999). *Ley 597 de 1999.* Recuperado el 09 de 02 de 2024, de Función Pública: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

Dailé Osorio-Roig, Christian Rathgeb, Pawel Drozdowsk, Philipp Terhörst, Vitomir Štruc, Christoph Busch. (2022). An Attack on Facial Soft-Biometric Privacy Enhancement. Slovenia. IEEE Transactions on Biometrics, Behavior, and Identity science, Vol. 4, No. 2.

Diaz Carrasco, N. A. (2023). Evaluación de algoritmos para la detección de huellas dactilares alteradas. https://repositorio.uss.edu.pe/handle/20.500.12802/11545

Docusign. (23 de enero de 2023). *Docusign*. Obtenido de https://www.docusign.com/es-mx/blog/que-es-la-firma-electronica

Firc, A. (2021). Applicability of Deepfakes in the Field of Cyber Security. Brno University of Technology, Faculty of Information Technology, Brno. Superviso r Mgr. (Kamil Malinka, Ph. D). Pp.72.

Gutiérrez Yánez, AE (2022). Estado del arte de registros biométricos estáticos usados para autenticar la identidad de una persona (Tesis de licenciatura). https://dspace.ups.edu.ec/handle/123456789/22173

Gutierrez, N. (17 de 02 de 2022). *Fundamentos de ciberseguridad*. Recuperado el 15 de 01 de 2024, de 30 estadisticas importantes de seguridad informatica: https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Hangaragi, S., Singh, T. y Neelima, N. (2023). Detección y reconocimiento de rostros mediante Face Mesh y red neuronal profunda. Procedia Informática, 218, 741-749. https://www.sciencedirect.com/science/article/pii/S1877050923000546

IBM. (5 de marzo de 2021). *IBM*. Obtenido de IBM B2B Advanced Communications 1.0.0: https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=overview-digital-signature

INFOCORP. (11 de 2022). *3er Estudio latinoamericano de banca digital.* Recuperado el 20 de 02 de 2024, de https://4850065.fs1.hubspotusercontent-na1.net/hubfs/4850065/3erEstudio%20Lationamericano%20de%20Banca%20Digital/Informe%20Estudio/3er_Estudio-Latinoamericano_Banca_Digital-INFORME_FINAL_ORIGINAL%23INFOCORP.pdf

Ilkka Kaate, Joni Salminen, Joao Santos, Soon-Gyo Jung, Rami Olkkonen, Bernard Jansen. (2023). The realness of fakes: Primary evidence of the effect of deepfake personas on user perceptions in a design task. Finland. www.elsevier.com/locate/ijhcs.

IBeta. 2023. ISO 30107-3 Presentation Attack Detection Test Methodology And Confirmation Letters. https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/

Jon Bateman. (2020). Deepfakes and synthetic media in the financial system: assessing threat scenarios, Carnegie. Endow. Int. Peace i–ii. Technical Report, http://www.jstor.org/stable/resrep25783.1

Khater, MM (2023). Multivector con solitones ópticos ultracortos de núcleo no local y no singular que pulsa ondas en fibras birrefringentes. Caos, solitones y fractales, 167, 113098.

Klaire Somoray, Dan J. Miller. (2023). Providing detection strategies to improve human detection of deepfakes: An experimental study. Australia.www.elsevier.com/locate/comphumbeh.

Maltoni, D., Maio, D., Jain, AK y Feng, J. (2022). Detección de huellas dactilares. Manual de reconocimiento de huellas dactilares, 63-114. https://link.springer.com/chapter/10.1007/978-3-030-83624-5_2

Ministerio de ciencia, tecnología e innovación. (2022). Política de Investigación e Innovación Orientada por Misiones para dar solución de grandes desafíos del país. https://minciencias.gov.co/sites/default/files/politicas_orientadas_por_misiones_-_minciencias_2022-2026.pdf

Paz, V. E. L., Cerquin, J. A. L., & De Los Santos, A. C. M. (2022). Beneficios de las tecnologías biométricas para la autenticación de usuarios: una revisión sistemática. INGENIERÍA INVESTIGA, 4. https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/711

Parialò, A. (2022). Deepfakes: analysis on the role of disclosure placement in consumers' attitude towards synthetic advertisement. https://tesi.luiss.it/32847/

Que es la ciberseguridad. (2021). Recuperado el 20 de 01 de 2024, de https://www.ibm.com/mx-es/topics/cybersecurity?classId=95226537-b235-44be-ba02-6ab1425fe984&assignmentId=0d184aa4-4740-412e-aa55-c95ae9463d16&submissionId=53dcda85-451b-0dc5-6676-b7309b91e44b

Soliman, A. A. (2004). Consumers' attitudes towards the social performance of Saudi business firms: An empirical investigation. Journal of King Saud University, Administrative Sciences, 16(2), 61-85. https://cba.ksu.edu.sa/sites/cba.ksu.edu.sa/files/imce_images/v31m234r1247.pdf

Somoray, K. y Miller, DJ (2023). Proporcionar estrategias de detección para mejorar la detección humana de deepfakes: un estudio experimental. Computadoras en el comportamiento humano, 149, 107917. https://www.sciencedirect.com/science/article/pii/S0747563223002686

Suresh, B. (2021). Detección de reconocimiento de rostros vivos y detección de rostros falsos basada en parámetros de evaluación de la calidad de la imagen. https://ijisea.org/Papers/V2S2/Detection%20of%20Liveness%20Face%20recognition%20and%20Spoof%20face%20Detection%20Based%20on%20Image%20Quality%20Assessment%20Parameters.pdf

Tolosana, R., Vera-Rodríguez, R., González-García, C., Fierrez, J., Rengifo, S., Morales, A., ... & Jabin, S. (2021). Concurso ICDAR 2021 sobre verificación de firmas en línea. En Análisis y reconocimiento de documentos – ICDAR 2021: 16.ª Conferencia Internacional, Lausana, Suiza, 5 al 10 de septiembre de 2021, Actas, Parte IV 16 (págs. 723-737). Publicaciones internacionales Springer

Téllez Ortiz, J. A. (2020). Detección de vida en huellas dactilares: una revisión. Preprint submitted to Elsevier.

VALORA ANALITIK. (2021). *Depósitos electrónicos en Colombia.* Obtenido de https://www.valoraanalitik.com/2021/10/21/depositos-electronicos-pasaron-48-millones-133-millones/

Wickramasinghe, S. (03 de 05 de 2023). *Pricacy affairs*. Recuperado el 20 de 02 de 2024, de Biometria en ciberseguridad: https://www.privacyaffairs.com/es/biometria-en-ciberseguridad/

Wang, Y., Hao, X., Guo, C. (2023). "A New Multispectral Method for Face Liveness Detection." En: 2nd IARP Asian Conference on Pattern Recognition, pp. 922-926. https://www.liveness.com/

Wickramasinghe, S. (03 de 05 de 2023). *Pricacy affairs*. Recuperado el 20 de 02 de 2024, de Biometria en ciberseguridad: https://www.privacyaffairs.com/es/biometria-en-ciberseguridad/