

Artículo original

Accesibilidad y autenticación segura para personas con discapacidad visual en entornos digitales

Accessibility and Secure Authentication for People with Visual Impairments in Digital Environments

Luis Alfonso Palomares⁽¹⁾

⁽¹⁾Universidad Nacional de la Matanza

lpalomares@unlam.edu.ar

Orcid ID:0009-0008-6029-8968

Resumen:

El acceso a plataformas digitales que requieren autenticación suele implicar barreras significativas para personas con discapacidad visual. Mecanismos como CAPTCHA visuales, códigos de verificación o interfaces gráficas limitan la autonomía de estos usuarios y comprometen su experiencia de uso. Esta situación evidencia una brecha persistente entre los avances en ciberseguridad y las prácticas de accesibilidad digital. Este estudio tiene como propósito examinar distintas estrategias que buscan facilitar la autenticación segura sin depender exclusivamente de estímulos visuales. Diversos trabajos recientes han explorado enfoques alternativos para superar estas barreras, promoviendo la integración de canales sensoriales diversos y estrategias adaptativas. Entre las líneas más destacadas se encuentran aquellas que facilitan la interacción mediante reconocimiento de voz, entradas auditivas y respuestas táctiles. Estas aproximaciones permiten reconfigurar la relación entre seguridad y usabilidad, incorporando nuevas perspectivas sobre el diseño

inclusivo. El análisis realizado sobre estudios publicados entre 2005 y 2025 permitió identificar elementos clave que favorecen una autenticación más equitativa y robusta. Se observa una evolución progresiva en la forma en que se concibe la validación de identidad, donde la compatibilidad con tecnologías de asistencia y la reducción de dependencias visuales resultan centrales. En conjunto, los hallazgos abren el camino hacia modelos más integradores que atienden tanto a las exigencias de seguridad informática como a los principios de accesibilidad.

Abstract:

Access to digital platforms that require authentication often poses significant barriers for people with visual impairments. Visual CAPTCHAs, verification codes, and graphical interfaces limit these users' autonomy and compromise their overall experience. This situation reveals a persistent gap between advances in cybersecurity and digital accessibility practices. This study aims to examine various strategies designed to enable secure authentication without relying solely on visual cues. Recent research has explored alternative approaches to overcome these barriers by integrating diverse sensory channels and adaptive techniques. Among the most notable are methods that support interaction through voice recognition, auditory prompts, and tactile feedback. These approaches allow us to rethink the balance between security and usability, introducing fresh perspectives on inclusive design. An analysis of studies published between 2005 and 2025 identified key factors that contribute to more equitable and robust authentication. We observe a progressive evolution in how identity validation is conceived, with compatibility with assistive technologies and reduced visual dependence taking center stage. Together, these findings pave the way for more inclusive models that meet both the demands of information security and the principles of accessibility.

Palabras Clave: *Accesibilidad digital, Autenticación segura, Discapacidad visual, Interfaces multimodales, Reconocimiento de voz, Inteligencia artificial*

Key Words: *Digital accessibility, Secure authentication, Visual impairment, Multimodal interfaces, Voice recognition, artificial intelligence*

I. INTRODUCCIÓN

La autenticación digital segura representa un componente crítico en el diseño de servicios tecnológicos contemporáneos. A medida que se incrementa la digitalización de procesos cotidianos —como operaciones bancarias, gestión de identidad y acceso a información personal— también crece la necesidad de mecanismos de autenticación robustos. Sin embargo, esta evolución no ha sido acompañada por un diseño universal que contemple a personas con discapacidad visual. En contextos donde la verificación de identidad requiere interacciones visuales, como CAPTCHA, contraseñas temporales o lectura de códigos QR, se observan fuertes limitaciones de accesibilidad que vulneran los principios de equidad y autonomía digital. En consecuencia, muchas de estas tecnologías terminan siendo excluyentes o generando dependencias innecesarias con terceros.

Estudios previos [1], [2], [3] y [4] han documentado ampliamente estas barreras y proponen líneas de trabajo centradas en rediseñar la experiencia de autenticación desde una perspectiva accesible. A su vez, el trabajo de Campi [5] enfatiza la importancia de enfoques cognitivos adaptativos y tecnologías de apoyo como los asistentes de voz.

El presente estudio analiza críticamente un conjunto de propuestas tecnológicas publicadas entre 2005 y 2025 que abordan el problema desde enfoques alternativos, incluyendo interfaces multimodales, asistencia por voz, autenticación táctil y soluciones basadas en inteligencia artificial. Se priorizan aquellas contribuciones que no sólo resuelven el problema de la seguridad, sino que también integran principios de accesibilidad desde el diseño. La revisión se fundamenta en trabajos de ingeniería informática que proponen soluciones tecnológicas concretas, con foco en su aplicabilidad, viabilidad técnica y escalabilidad.

Se sigue un enfoque exploratorio basado en la revisión crítica de literatura técnica y científica reciente, enfocada en propuestas prácticas y aplicables.

I.1. OBJETIVOS ESPECIFICOS

Identificar los principales desafíos de accesibilidad enfrentados por personas con discapacidad visual en mecanismos actuales de autenticación digital.

Sintetizar soluciones tecnológicas que combinen seguridad y accesibilidad desde una perspectiva inclusiva.

Evaluar la aplicabilidad de tecnologías emergentes como inteligencia artificial y asistentes por voz para entornos críticos.

Proponer recomendaciones técnicas y éticas para el diseño de autenticación digital accesible en ingeniería informática.

II. TRABAJOS RELACIONADOS

La intersección entre accesibilidad digital y autenticación segura ha sido objeto de creciente atención en los últimos veinte años. Diversas investigaciones han evidenciado las tensiones entre la robustez técnica de los mecanismos de autenticación y la inclusión efectiva de personas con discapacidad visual (DV).

Barreras y limitaciones actuales.

Los trabajos pioneros de Dhamija y Tygar [6] ya advertían sobre las limitaciones de los mecanismos tradicionales frente a ataques de suplantación, pero sin contemplar la accesibilidad. Posteriormente, estudios como los de Dosono [1] y Andrew [4] documentaron empíricamente cómo elementos como CAPTCHA visuales, contraseñas gráficas y códigos QR imponen una carga desproporcionada en usuarios con DV. Ambore y Breban [3] ampliaron este análisis en el ámbito de servicios financieros móviles, mostrando cómo las barreras de accesibilidad pueden comprometer tanto la autonomía como la seguridad, al inducir prácticas de riesgo como la delegación de credenciales a terceros.

Más recientemente, Wolf [7], Faustino y Girouard [8] exploraron las percepciones de personas ciegas sobre mecanismos móviles de autenticación, identificando la dependencia forzada de lectores de pantalla, la frustración ante flujos no accesibles y el riesgo de *shoulder surfing*. En la misma línea, Moreno [9] realizaron un estudio en países hispanohablantes, evidenciando la persistencia de barreras culturales y técnicas, como la ausencia de alternativas auditivas en CAPTCHA o la inaccesibilidad de aplicaciones de autenticación en dos pasos.

Propuestas multimodales y enfoques alternativos.

La literatura ha propuesto diferentes modalidades para superar la dependencia visual. Kumar y Singh [10] presentaron un modelo multimodal que integra reconocimiento de voz y entradas táctiles, mientras que Fanelle [11] explora variantes de Audio CAPTCHA con mejores índices de usabilidad. En la misma línea, estudios recientes proponen extender estas alternativas con enfoques hápticos: Kuber [12] introdujeron la idea de patrones vibrotáctiles como secreto, y el más reciente de Bhole [13] demostró que el uso de háptica estructurada puede servir como segundo factor menos intrusivo y más inclusivo.

Los trabajos de Ho [14] [15] muestran cómo la aplicación del *efecto de superioridad de la imagen* en entornos no visuales puede mejorar significativamente la memorabilidad y el rendimiento de esquemas gráficos o sonoros para personas ciegas. Estas aproximaciones se suman a propuestas como ARJUNA [16], que adapta la entrada de PIN para ser accesible en smartphones mediante retroalimentación auditiva y temporización, o al método descrito por Kuppusamy [17] para evaluar la fortaleza de contraseñas con lectores de pantalla.

CAPTCHA y verificación adaptativa.

El caso de los CAPTCHA es paradigmático: Gaggi [18] demostró los problemas de accesibilidad de reCAPTCHA, mientras que Jain [19] con reCAPGen ofrecieron un modelo de generación automatizada de CAPTCHA de audio más usable y resistente a ataques automáticos. Gao [20] ya habían explorado previamente CAPTCHA auditivos como alternativa.

Inteligencia artificial y neurodiversidad.

Los aportes de Di Campi y Luccio [5] introducen la perspectiva de la neurodiversidad, sugiriendo que los enfoques accesibles deben abarcar no sólo limitaciones sensoriales sino también cognitivas. Esto conecta con una tendencia reciente a incorporar inteligencia artificial en la adaptación dinámica de flujos de autenticación, ajustando el nivel de

dificultad o los canales empleados según el perfil del usuario.

Estándares emergentes: Passkeys y WebAuthn.

El advenimiento de los estándares FIDO2/WebAuthn marca un punto de inflexión. Trabajos como los de Wagner [21] y Rivera-Dourado [22] analizan su aplicabilidad en contextos de recursos limitados y evidencian avances hacia una autenticación sin contraseñas. Sin embargo, los hallazgos de Wang [23] subrayan que la falta de señales accesibles en lectores de pantalla o el mal etiquetado de controles pueden convertir estas soluciones en barreras adicionales.

Autenticación continua y transparente.

Por otra parte, Crawford [24] investigó la aceptación de mecanismos de autenticación transparente, basados en el contexto y sensores del dispositivo, mostrando que los usuarios valoran positivamente la reducción de carga cognitiva, siempre que mantengan control y visibilidad sobre el proceso.

En conjunto, la revisión de más de veinte estudios evidencia una clara evolución: de soluciones rígidas y visuales hacia modelos multimodales, adaptativos y estandarizados, en los que la accesibilidad se posiciona no como un agregado opcional sino como una condición esencial de la seguridad digital.

III. CONCLUSIONES

El análisis crítico de la literatura publicada entre 2005 y 2025 permite identificar tendencias convergentes que reconfiguran el vínculo entre accesibilidad y seguridad en la autenticación digital para personas con discapacidad visual.

1. La accesibilidad es un componente intrínseco de la seguridad.

Los estudios muestran que la inaccesibilidad de un mecanismo no sólo limita la usabilidad, sino que debilita la seguridad en la práctica. Usuarios que no pueden interactuar con un CAPTCHA, leer un código QR o completar un flujo 2FA terminan recurriendo a terceros, exponiendo credenciales y reduciendo la eficacia de los controles. La investigación de Wang [23] confirma que las barreras de accesibilidad generan vulnerabilidades sistémicas. En este sentido, la accesibilidad debe ser entendida como un control de seguridad en sí mismo.

2. La multimodalidad supera la traducción visual.

Las propuestas más prometedoras no replican los estímulos visuales en otro canal, sino que rediseñan la experiencia de autenticación en clave multimodal. Bhole [13], Ho, Y. [14] y Balayogi [16] ejemplifican cómo la háptica, la sonoridad y la retroalimentación adaptativa pueden convertirse en componentes equivalentes o incluso superiores a lo visual, siempre que se integren desde la concepción del sistema.

3. Estándares y tecnologías emergentes requieren ajustes accesibles.

Passkeys y WebAuthn prometen reducir fricciones y riesgos asociados a las contraseñas. Sin embargo, los estudios de Wagner [21], Rivera-Dourado [22] y Akanda [23] evidencian que aún existen deudas de implementación: nomenclatura inconsistente, flujos mal anunciados a lectores de pantalla y dificultades en la vinculación de dispositivos externos. Incorporar criterios de accesibilidad en estas implementaciones es esencial para que la promesa de mayor seguridad no se traduzca en nuevas exclusiones.

4. El futuro de la autenticación inclusiva es adaptativo.

La integración de inteligencia artificial, como sugieren Di Campi y Luccio [5], abre la posibilidad de sistemas que ajusten dinámicamente la complejidad, modalidad o canal de autenticación según las capacidades y el contexto del usuario. Esta

perspectiva permite no sólo mejorar la equidad, sino también optimizar la seguridad al reducir errores y falsos positivos.

5. La agenda de investigación y práctica.

De los estudios revisados se desprende que los próximos pasos deben incluir:

- Ensayos empíricos en entornos críticos (banca, salud, educación).
- Desarrollo de guías técnicas y normativas que integren accesibilidad como requisito obligatorio en la ingeniería de software.
- Evaluaciones comparativas entre diferentes modalidades multimodales, considerando no sólo eficacia técnica sino también percepción de autonomía y dignidad del usuario.
- Implementación de métricas conjuntas de accesibilidad y seguridad como indicadores de calidad en sistemas de autenticación.

En suma, el campo avanza desde una visión que concebía la accesibilidad como un añadido hacia un paradigma en el que **la seguridad robusta y la accesibilidad inclusiva son inseparables**. Este giro exige no sólo innovación tecnológica, sino también un cambio cultural en la ingeniería informática, orientado a garantizar que las soluciones de autenticación sean seguras para todos, sin excepciones.

IV. TRABAJOS FUTUROS

Para avanzar en esta línea de investigación, se identifican múltiples desafíos y oportunidades:

- Profundizar los estudios empíricos que evalúen la efectividad de mecanismos de autenticación inclusivos en entornos reales, como aplicaciones bancarias, educativas o de salud.
- Desarrollar estándares técnicos y guías de buenas prácticas en ingeniería de software que aseguren accesibilidad desde etapas tempranas de diseño.

- Implementar estudios comparativos entre diferentes enfoques multimodales, como autenticación por voz, gestos y biometría, evaluando su impacto en poblaciones con diversidad funcional.
- Explorar modelos de aprendizaje automático que se adapten al patrón de uso individual del usuario, reduciendo falsos positivos y aumentando la autonomía.

V. REFERENCIAS BIBLIOGRÁFICAS

- [1] B. Dosono, J. Hayes, and Y. Wang, “‘I’m Stuck!’: A Contextual Inquiry of People with Visual Impairments in Authentication,” *11th Symposium on Usable Privacy & Security (SOUPS ’15)*, pp. 151–168, 2015, Accessed: May 19, 2025. [Online]. Available: <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-dosono.pdf>
- [2] S. Furnell, K. Helkala, and N. Woods, “Accessible authentication: Assessing the applicability for users with disabilities,” *Comput Secur*, vol. 113, p. 102561, Feb. 2022, doi: 10.1016/j.cose.2021.102561.
- [3] S. Ambore, A. Breban, E. Apeh, and H. Dogan, “Evaluating Security and Accessibility Trade-off for Visually Impaired Mobile Financial Services Users,” *34th British HCI Workshop and Doctoral Consortium*, Ed., London, UK, Jul. 2021, pp. 1–5. doi: 10.14236/ewic/HCI2021-W5.1.
- [4] S. Andrew, S. Watson, T. Oh, and G. W. Tigwell, “A Review of Literature on Accessibility and Authentication Techniques,” in *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, New York, NY, USA: ACM, Oct. 2020, pp. 1–4. doi: 10.1145/3373625.3418005.
- [5] A. M. Di Campi and F. L. Luccio, “Accessible Authentication Methods for People with Diverse Cognitive Abilities,” *Univers Access Inf Soc*, Nov. 2023, doi: 10.21203/RS.3.RS-3564504/V1.
- [6] R. Dhamija and J. D. Tygar, “The Battle Against Phishing: Dynamic Security Skins,” *ACM Symposium on Usable Security and Privacy*, pp. 77–88, Jul. 2005, Accessed: Apr. 13, 2025. [Online]. Available: https://people.eecs.berkeley.edu/~tygar/papers/Phishing/Battle_against_phishing.pdf
- [7] F. Wolf, R. Kuber, and A. J. Aviv, “Perceptions of mobile device authentication mechanisms by individuals who are blind,” *ASSETS 2017 - Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 385–386, Oct. 2017, doi: 10.1145/3132525.3134793;TOPIC:TOPIC:CONFERENCE-COLLECTIONS.
- [8] D. Briotto Faustino and A. Girouard, “Bend Passwords on BendyPass,” in *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, New York, NY, USA: ACM, Oct. 2018, pp. 435–437. doi: 10.1145/3234695.3241032.
- [9] L. Moreno, H. Petrie, and S. Schmeelk, “Accessibility barriers with authentication methods for blind and partially sighted people in the Spanish-speaking world,” 2023. doi: 10.14236/ewic/BCSHCI2023.22.

- [10] A. Kumar and P. Singh, "Multimodal authentication for blind users," *IEEE Access*, 2020, [Online]. Available: <https://doi.org/10.1109/ACCESS.2020.3013432>
- [11] Fanelle Valerie, Karimi Sepideh, Shah Aditi, Subramanian Bharath, and Das Sauvik, "Blind and Human: Exploring More Usable Audio CAPTCHA Designs," *16th Symposium on Usable Privacy & Security (SOUPS '20)*, pp. 205–222, 2020, Accessed: May 19, 2025. [Online]. Available: https://www.usenix.org/system/files/soups2020-fanelle_0.pdf
- [12] R. Kuber and S. Sharma, "Toward tactile authentication for blind users," *ASSETS'10 - Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 289–290, 2010, doi: 10.1145/1878803.1878875.
- [13] P. V. Bhole, Z. Li, S. Bokolia, T. Oh, G. W. Tigwell, and R. L. Peiris, "Haptic2FA: Haptics-Based Accessible Two-Factor Authentication for Blind and Low Vision People," *Proc ACM Hum Comput Interact*, vol. 8, no. MHCI, Sep. 2024, doi: 10.1145/3676509.
- [14] Y. L. Ho, S. H. Lau, and A. Azman, "Comparison of BlindLoginV2 and AudioBlindLogin with the common textual password authentication for the blind and visually impaired using smartphones," *International Journal of Human Computer Studies*, vol. 156, Dec. 2021, doi: 10.1016/J.IJHCS.2021.102718.
- [15] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human Computer Studies*, vol. 63, no. 1–2, pp. 128–152, Jul. 2005, doi: 10.1016/J.IJHCS.2005.04.020.
- [16] G. Balayogi and K. S. Kuppusamy, "ARJUNA: An accessible pin entry model in smartphones for persons with low vision," *Internet Technology Letters*, vol. 6, no. 6, p. e466, Nov. 2023, doi: 10.1002/ITL2.466;PAGEGROUP:STRING:PUBLICATION.
- [17] K. S. Kuppusamy and G. Balayogi, "Accessible password strength assessment method for visually challenged users," *Int J Inf Secur*, vol. 22, no. 6, pp. 1731–1741, Dec. 2023, doi: 10.1007/s10207-023-00714-x.
- [18] O. Gaggi, "A study on Accessibility of Google ReCAPTCHA Systems," in *Open Challenges in Online Social Networks*, New York, NY, USA: ACM, Jun. 2022, pp. 25–30. doi: 10.1145/3524010.3539498.
- [19] M. Jain, R. Tripathi, I. Bhansali, and P. Kumar, "Automatic generation and evaluation of usable and secure audio recaptcha," *ASSETS 2019 - 21st International ACM SIGACCESS Conference on Computers and Accessibility*, pp. 355–366, Oct. 2019, doi: 10.1145/3308561.3353777;PAGE:STRING:ARTICLE/CHAPTER.
- [20] H. Gao, H. Liu, D. Yao, X. Liu, and U. Aickelin, "An audio CAPTCHA to distinguish humans from computers," *Third International Symposium on Electronic Commerce and Security*, pp. 265–269, Jun. 2013, doi: 10.48550/arXiv.1306.2885.

- [21] P. Wagner, K. Heid, and J. Heider, "Remote WebAuthn: FIDO2 Authentication for Less Accessible Devices", doi: 10.5220/0010192703680375.
- [22] M. Rivera-Dourado *et al.*, "An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards," *Engineering Proceedings 2021, Vol. 7*, vol. 7, no. 1, Oct. 2021, doi: 10.3390/ENGPROC2021007056.
- [23] M. M. R. R. Akanda, A. T. Mahdad, and N. Saxena, "Broken Access: On the Challenges of Screen Reader Assisted Two-Factor and Passwordless Authentication," *WWW 2025 - Proceedings of the ACM Web Conference*, pp. 1116–1128, Apr. 2025, doi: 10.1145/3696410.3714579; GROUPTOPIC: TOPIC: ACM-PUBTYPE.
- [24] H. Crawford and K. Renaud, "Understanding user perceptions of transparent authentication on a mobile device," *Journal of Trust Management 2014 1:1*, vol. 1, no. 1, pp. 7-, Jun. 2014, doi: 10.1186/2196-064X-1-7.

Recibido: 2025-07-15

Aprobado: 2025-11-18

Hipervínculo Permanente: <https://doi.org/10.54789/reddi.10.2.2>

Datos de edición: Vol. 10 - Nro. 2 - Art. 2

Fecha de edición: 2025-12-30

