REVISTA CIENTÍFICA
CONECTIVIDAD
Instituto Superior Tecnológico Rumiñahui

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

Artículo Científico

Un estudio de usabilidad de la autenticación basada en passkeys

A usability study of authentication based on access keys

Erick Arnie Zavaleta Galarza[1], Alexander Josué Venturo Ramos[2], Cristhian André Jondec Delgado[3], Alberto Carlos Mendoza de los Santos[4]

[1] Universidad Nacional de Trujillo, ezavaletag@unitru.edu.pe, Trujillo - Perú
[2] Universidad Nacional de Trujillo, aventuror@unitru.edu.pe, Trujillo - Perú
[3] Universidad Nacional de Trujillo, cjondec@unitru.edu.pe, Trujillo - Perú
[4] Universidad Nacional de Trujillo, amendozad@unitru.edu.pe, Trujillo - Perú

Autor para correspondencia: ezavaletag@unitru.edu.pe

RESUMEN

Las contraseñas tradicionales presentan limitaciones críticas en usabilidad y seguridad, con tasas de reutilización superiores al 60% y elevada fatiga cognitiva en usuarios. Los passkeys, implementados bajo estándares FIDO2/WebAuthn, emergen como alternativa passwordless basada en criptografía de clave pública. La finalidad de este trabajo en una muestra latinoamericana de estudiantes universitarios es la de poder comparar la usabilidad y la satisfacción percibida en la entrada de las cuentas de diferentes usuarios mediante el uso de passkeys o de contraseñas tradicionales mediante evidencia numérica. El diseño de este trabajo experimental controlado fue between-subjects (n=30 participantes universitarios; media de edad=21.4 años), con una aleatorización de los individuos de la muestra en dos grupos (passkeys y contraseña) a lo largo de una de la semana de pruebas. Se utilizó el System Usability Scale (SUS), un cuestionario demográfico y preguntas de satisfacción de tipo Likert. Se realizaron varias pruebas no paramétricas (Mann-Whitney U) y correlaciones de Spearman entre los diferentes datos obtenidos. En este sentido, los passkeys mostraron una puntuación SUS media de 83.2 (DE=5.04), significativamente superior a las puntuaciones obtenidas en las contraseñas tradicionales (71.8, DE=2.2). En general, la satisfacción y la faciliad de uso obtenidos con passkeys (8.53 y 8.86 respectivamente) también eran superiores a aquellos que se obtuvieron para contraseñas (7.73 y 7.46). Las correlaciones entre satisfacción-SUS (ρ=0.41) y facilidad-SUS (ρ=0.35) resultaron moderadas-débiles. Esto evidencia que el uso de passkeys constituyen una alternativa viable para sustituir las contraseñas en aplicaciones comerciales, especialmente para la población joven con conocimientos tecnológicos moderados.

Palabras clave: Autenticación sin contraseña, contraseñas, experiencia de usuario, ciberseguridad, System Usability Scale.

ABSTRACT

Traditional passwords present critical limitations in usability and security, with reuse rates exceeding 60% and high cognitive fatigue among users. Passkeys, implemented under FIDO2/WebAuthn standards, are emerging as a passwordless alternative based on public-key cryptography. The aim of this study, conducted with a Latin American sample of university students, is to compare the usability and perceived satisfaction of logging into accounts using passkeys versus traditional passwords, using numerical evidence. This controlled experimental study employed a between-subjects design (n=30 university participants; mean age=21.4 years), with participants randomly assigned to two groups (passkeys and passwords) during the week-long testing period. The System Usability Scale (SUS), a demographic questionnaire, and Likert-type satisfaction questions were used. Several non-parametric tests (Mann-Whitney U) and Spearman correlations were performed on the different data obtained. In this regard, passkeys showed a mean SUS score of 83.2 (SD=5.04), significantly higher than the scores obtained for traditional passwords (71.8, SD=2.2). Overall, the satisfaction and ease of use obtained with passkeys (8.53 and 8.86, respectively) were also higher than those obtained for passwords (7.73 and 7.46). The correlations between satisfaction and SUS (ρ=0.41) and ease of use and SUS (ρ=0.35) were moderate to weak. This shows that the use of passkeys is a viable alternative to replace passwords in commercial applications, especially for young people with moderate technological knowledge.

Keywords: Passwordless authentication, passwords, user experience, cybersecurity, System Usability Scale.

Citar como:

Zavaleta Galarza, E. A., Venturo Ramos , A. J., Jondec Delgado , C. A., & Mendoza de los Santos, A. C. (2026). Un estudio de usabilidad de la autenticación basada en passkeys. *CONECTIVIDAD*, *7*(2), e429. https://doi.org/10.37431/conectividad.v7i2.429

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

1. INTRODUCCIÓN

La autenticación mediante contraseñas tradicionales sigue siendo la técnica predominante en la protección de sistemas digitales, a pesar de las crecientes críticas por su baja usabilidad y vulnerabilidad a incidentes de seguridad. Estudios recientes muestran que hasta el 78% de los usuarios reporta dificultades para gestionar múltiples contraseñas, con elevados niveles de fatiga cognitiva y tasas de reutilización que superan el 60% (Abdrabou et al., 2021; Mujeye, 2016; Kennesaw State University, 2025). Estas limitaciones no solo ponen en riesgo la seguridad de los sistemas, sino que generan barreras de experiencia de usuario e incrementan la demanda de soporte técnico (Abdrabou et al., 2021; Mujeye, 2016; Kennesaw State University, 2025).

Varios estudios han evidenciado que las políticas de complejidad y cambio regular de contraseñas incrementan la cantidad de intentos infructuosos, el periodo de autenticación y la insatisfacción del usuario, lo cual ocasiona que prácticas como almacenar contraseñas sin seguridad o reutilizarlas sean comunes incluso entre usuarios con un alto dominio en seguridad (Feinberg & Murphy, 2000; Grawemeyer & Johnson, 2011). Mujeye (2016), por ejemplo, determinó que aumentar el nivel de complejidad de las contraseñas produce un incremento en la carga cognitiva, una disminución en la capacidad de recordar y un aumento en las solicitudes para restablecer credenciales. Además, Abdrabou et al. (2021) demostraron a través de métodos de pupilometría que el establecimiento de contraseñas seguras conlleva un esfuerzo mental más elevado, lo cual indica una tensión entre la seguridad y la facilidad de uso.

En respuesta a esta problemática, se han puesto en marcha a nivel internacional métodos de autenticación sin contraseña, entre ellos los passkeys que utilizan los estándares WebAuthn y FIDO2. Un passkey es un sistema que se basa en la criptografía de clave pública y que protege al usuario de ataques de phishing y robo de credenciales, eliminando los secretos compartidos entre el usuario y el servidor (Ashish et al., 2024; FIDO Alliance, 2023). Cuando un usuario registra una clave de acceso, su equipo produce un par de claves: la privada se mantiene resguardada localmente (en el enclave seguro del aparato o a través de hardware como las llaves USB), mientras que la pública es enviada al servidor (Lyastani et al., 2020; Ashish et al., 2024). El protocolo WebAuthn asegura que las credenciales estén ligadas al dominio legítimo, impidiendo que sean interceptadas por sitios maliciosos (FIDO Alliance, 2023).

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

El estado del arte hace referencia a una tendencia emergente de realizar evaluaciones empíricas de métodos passwordless en contextos reales. En los últimos años se ha puesto de relieve la usabilidad de los sistemas de contraseñas basadas en FIDO2/WebAuthn y de las passkeys en configuración entre-subjects y longitudinal, evaluando la satisfacción y la adopción mediante la Escala de Usabilidad de Sistemas (System Usability Scale, SUS), así como las métricas de la eficiencia de los métodos de autenticación considerados, como son los tiempos de autenticación y los errores (Lyastani et al., 2020). Por ejemplo, Reese et al. (2019), en un estudio de dos semanas, reportaron una mediana de 95 en la puntuación SUS para contraseñas tradicionales y valores de entre 73,1 y 83,1 para métodos de autenticación en dos pasos (2FA) como U2F y TOTP. Resultados similares han sido documentados en investigaciones más recientes sobre passkeys y autenticadores biométricos (Lyastani et al., 2020; Owens et al., 2021).

Sin embargo, persiste una brecha en la literatura respecto a estudios de usabilidad de passkeys realizados en el mundo hispanohablante o latinoamericano, estudios longitudinales y en relación explícita con métodos de autenticación tradicionales bajo condiciones equiparables. En línea con ello, la mayor parte de las investigaciones han empleado muestras de conveniencia, han presentado una falta de comparación sistematizada entre métodos y no han descrito sistemáticamente el análisis estadístico que permita interpretar los resultados del SUS en términos de significancia y relevancia práctica (Lyastani et al., 2020). Por ello, hace falta analizar ventajas y desventajas de los passkeys en comparación con las contraseñas en contextos experimentales y con métricas robustas.

Este trabajo pretende aproximar la comprensión de la usabilidad de los passkeys con información cuantitativa reciente y recomendaciones que puedan ser aplicadas por implementadores y por académicos del área de la seguridad digital (FIDO Alliance, 2023).

2. MATERIALES Y MÉTODOS

2.1. Diseño experimental

Se llevó a cabo un experimento controlado con un diseño de between-subjects, en el que se asignaron aleatoriamente 30 participantes universitarios (media de edad: 21.4 años; 23.3% mujeres, 76.7% varones; nivel formativo: 80% en grado universitario, 20% en técnico superior) a una de ambas condiciones experimentales; es decir, autenticación por passkeys (n=15) o autenticación por password (n=15).

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

Figura 1. Arquitectura del sistema de autenticación.

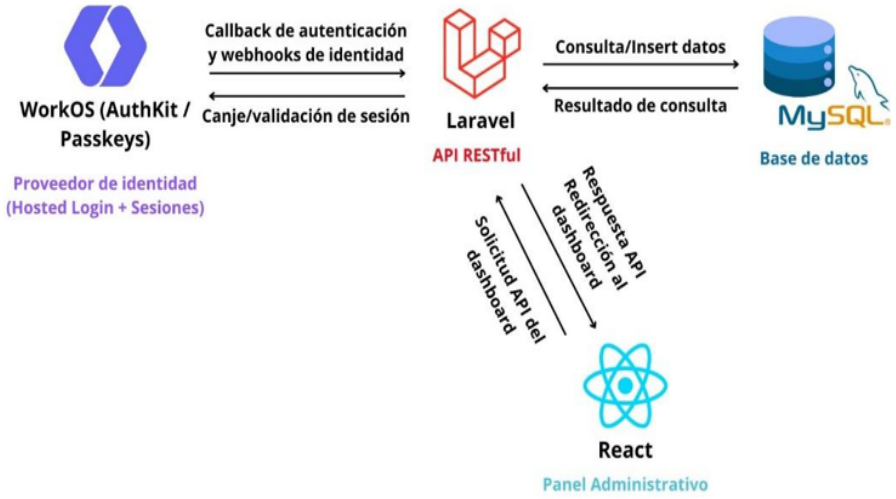


Figura 2. Formulario de registro.

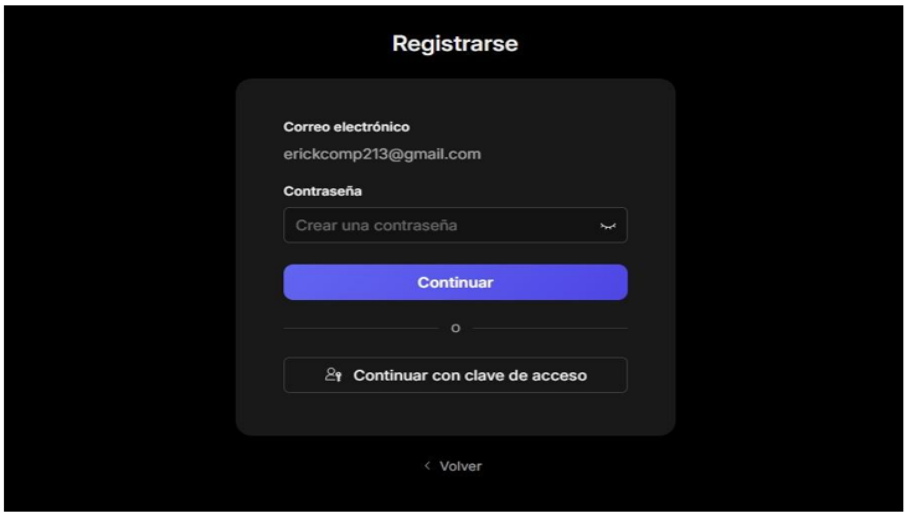


Figura 3. Registro con passkey.

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

La muestra se concibe adecuadamente en atención a los parámetros aceptados en estudios exploratorios de usabilidad sobre autenticación y donde muestras de n=8 a n=14 por grupo son habituales, permitiendo detectar diferencias medianas o grandes, pero con un poder razonable (Lyastani et al., 2020).

Durante una semana, cada participante realizó tareas diarias de inicio de sesión en una plataforma web experimental, configurando su respectivo método de autenticación desde el primer día (Figura 1, Figura 2, Figura 3, Figura 4 y Figura 5). Ambos grupos usaron el mismo sitio web y resolvieron tareas idénticas (acceso, edición de perfil, cierre de sesión y autenticación repetida tras simular pérdida/robo de dispositivo).

Figura 4. Inicio de sesión con passkey.

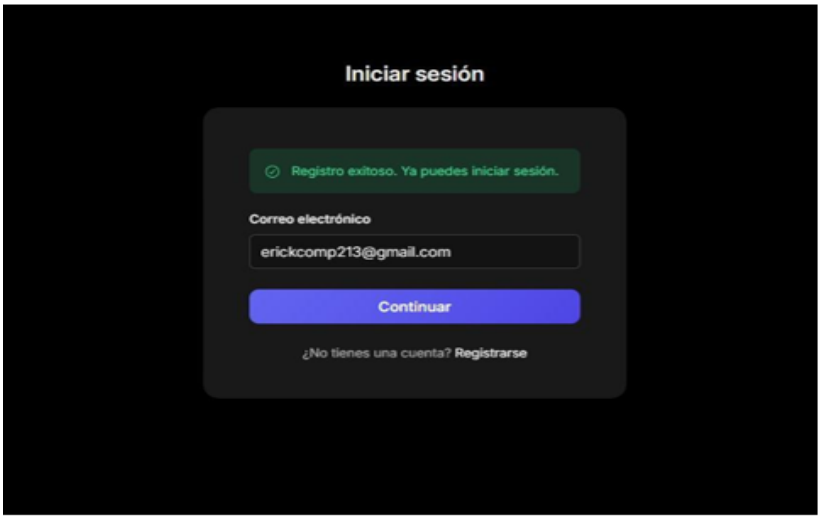


Figura 5. Verificación de inicio de sesión a través del correo electrónico.

2.2. Instrumentos de medición

Se emplearon tres instrumentos principales:

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

1. System Usability Scale (SUS): Encuesta de 10 ítems traducida y validada para español (Brooke, 1996; Suria et al., 2024; Arias Cabarcos & Meyer, 2025). El SUS es la escala más difundida y validada para medir usabilidad en sistemas de autenticación (Suria et al., 2024; Arias Cabarcos & Meyer, 2025), con valores recomendados de interpretación: <68 usabilidad baja, 68–80 aceptable, >80 excelente (Brooke, 1996; Sauro & Lewis, 2016).
2. Preguntas de satisfacción: Dos ítems tipo Likert (1–10): (a) satisfacción general con el método de autenticación y (b) probabilidad de recomendarlo a otros; se adoptó esta métrica conforme a estudios previos de benchmarking de usabilidad (Suria et al., 2024; Ruoti et al., 2016).
3. Cuestionario demográfico: Edad, género, nivel educativo, experiencia tecnológica (autoinforme en escala 1–5).

2.3. Protocolo de aplicación

El estudio fue aprobado por el comité ético de la universidad y todos los participantes firmaron consentimiento informado. Tras la semana de pruebas, se recopilaron los cuestionarios y se calcularon puntuaciones brutas y normalizadas del SUS siguiendo la fórmula de Brooke (1996) y recomendaciones para análisis de distribución (Suria et al., 2024). Se evaluó la normalidad de las distribuciones (Shapiro-Wilk) y, ante la no normalidad, se optó por análisis no paramétricos (Mann-Whitney U) para comparar grupos, justificando así la elección de la prueba debido a su robustez ante tamaños de muestra pequeños y distribuciones no normales (Suria et al., 2024). Asimismo, se calculó la correlación de Spearman para explorar relaciones entre variables ordinales como experiencia tecnológica y satisfacción (Suria et al., 2024).

El análisis estadístico se realizó con el software SPSS v29 y R v4.3, conforme a mejores prácticas de transparencia y reproducibilidad en investigación de usabilidad (Suria et al., 2024; Ruoti et al., 2016).

3. RESULTADOS Y DISCUSIÓN

3.1. Datos demográficos

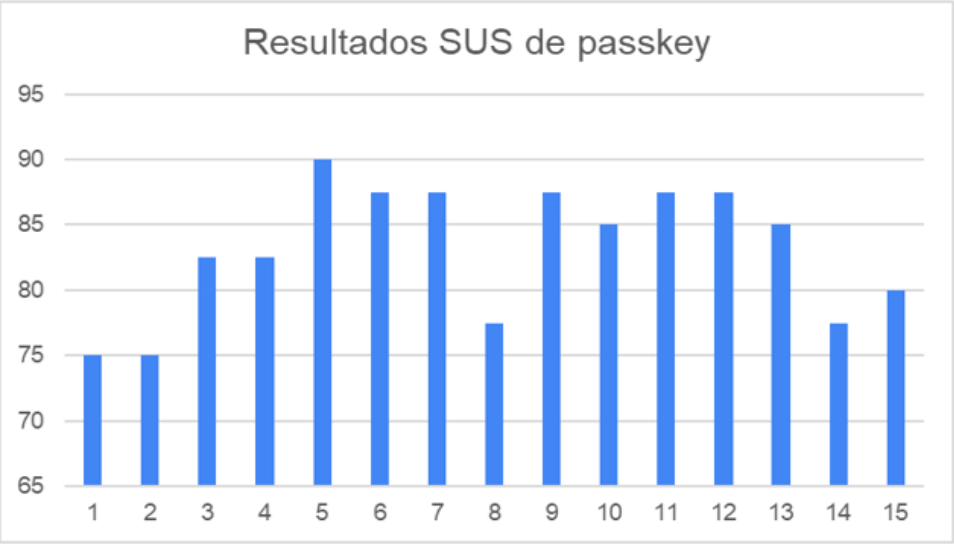
La muestra final se compuso de 30 participantes (15 por grupo), con edad media de 21,4 años (DE=2,1). La distribución de género no fue paritaria (7 mujeres, 23 varones). El 58,6% reportó un nivel de experiencia informático principiante, el 27,6% un nivel intermedio y el 13,8% un nivel avanzado.

3.2. Puntuaciones de usabilidad (SUS)

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

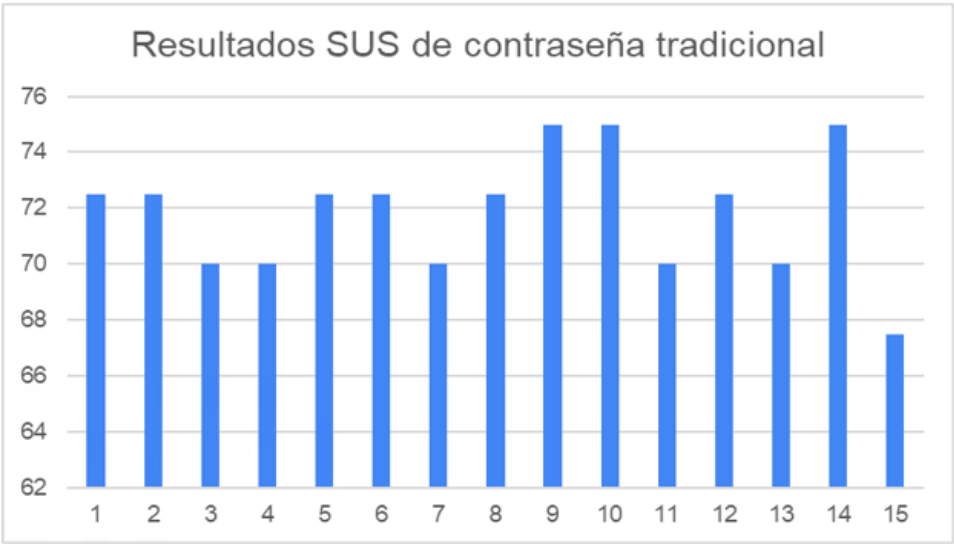
Los resultados del SUS para passkeys muestran una valoración muy favorable por parte de los participantes. La puntuación media obtenida fue de 83,2 (DE=5,04) con una mediana de 85. La Figura 6 muestra la distribución de las puntuaciones SUS individuales de cada participante.

Figura 6. Resultados SUS de passkey por participante.



Por otro lado, los resultados del SUS para contraseñas tradicionales muestran una valoración aceptable por parte de los participantes. La puntuación media obtenida fue de 71,8 (DE=2,2) con una mediana de 72,5. La Figura 7 muestra la distribución de las puntuaciones SUS individuales de cada participante para este método de autenticación.

Figura 7. Resultados SUS de contraseña tradicional por participante.



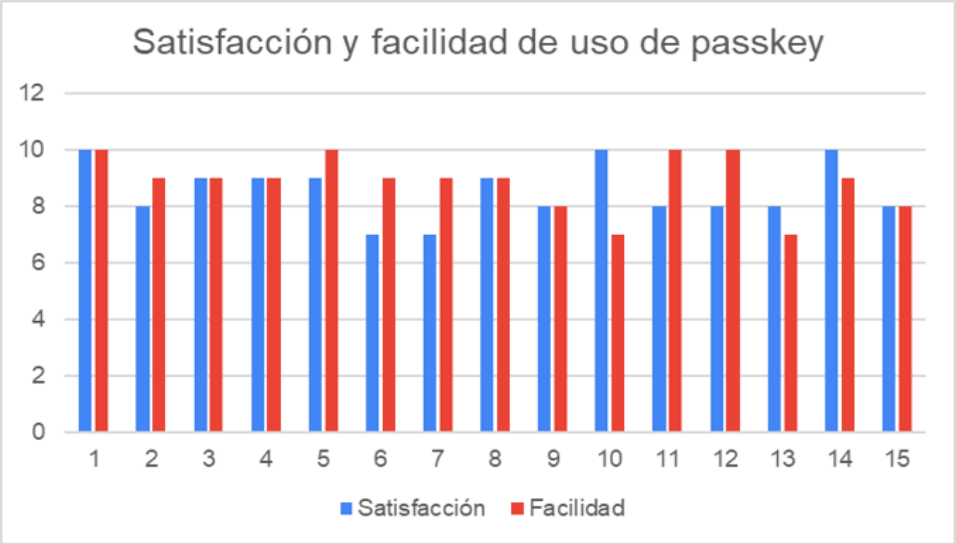
3.3. Preguntas de satisfacción

En cuanto a la satisfacción general y facilidad de uso percibida, los passkeys obtuvieron valoraciones superiores en ambas dimensiones. La satisfacción general media fue de 8,53

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

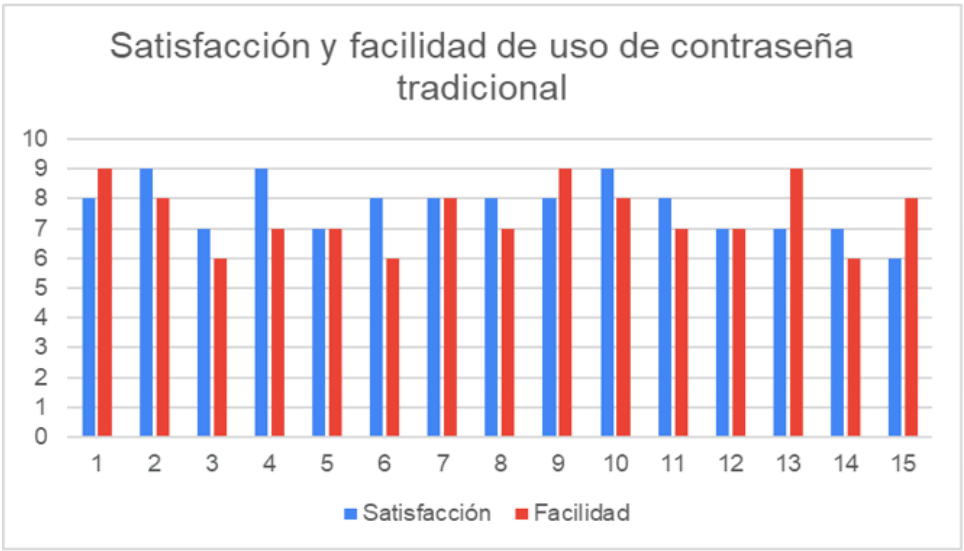
(DE=0,99) y la facilidad de uso alcanzó una media de 8,86 (DE=0,99), como se observa en la Figura 8, que muestra la distribución de estas valoraciones por participante.

Figura 8. Satisfacción y facilidad de uso de passkey por participante.



Por su parte, las contraseñas tradicionales presentaron valoraciones moderadas en ambas dimensiones. La satisfacción general media fue de 7,73 (DE=0,8) y la facilidad de uso obtuvo una media de 7,46 (DE=1,06). La Figura 9 muestra la distribución de estas puntuaciones individuales.

Figura 9. Satisfacción y facilidad de uso de contraseña tradicional por participante.



3.4. Correlaciones

El análisis de correlación de Spearman reveló una relación positiva moderada-débil entre la satisfacción general y la puntuación SUS ($\rho = 0,41$), así como entre la facilidad de uso y la puntuación SUS ($\rho = 0,35$). Estos resultados sugieren que, si bien existe una asociación entre estas variables, otros factores también influyen en la percepción de usabilidad del sistema.

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

3.5. Discusión

El estudio de Reese et al. (2019) reportó una mediana SUS de 95 para contraseñas tradicionales y 73,1–83,1 para métodos de autenticación en dos pasos (2FA). Nuestros resultados arrojan una media significativamente menor para contraseñas (71,8) y una media similar o incluso ligeramente superior para passkeys (83,2). Esta diferencia sugiere una transición en las percepciones de usabilidad a lo largo de los últimos seis años.

Una posible explicación radica en la evolución de las expectativas de los usuarios y el contexto tecnológico. El inicio de sesión con contraseña única, que se consideraba rápido y sin fricciones, continuaba siendo el estándar de referencia en usabilidad en 2019. No obstante, investigaciones recientes han registrado un incremento en la fatiga y frustración vinculadas con la administración y complejidad de las contraseñas (Abdrabou et al., 2021; Owens et al., 2021), así como una mayor comprensión acerca de peligros como el credential stuffing y el phishing, lo que tiene el potencial de hacer que los usuarios sean más críticos con la experiencia tradicional (Abdrabou et al., 2021; Kennesaw State University, 2025). Asimismo, el avance y la difusión de las experiencias passwordless han aumentado la expectativa de eficiencia y seguridad, lo que ha llevado a una disminución en la valoración relativa de las contraseñas.

En nuestro estudio, la preferencia y aceptación de passkeys puede haber sido influenciada por el contexto experimental, la participación de jóvenes universitarios que tienen una exposición tecnológica elevada y el movimiento social hacia sistemas sin contraseña. Esto es consistente con lo reportado por Lyastani et al. (2020) y Owens et al. (2021).

Las puntuaciones SUS para passkeys, cifradas en 83.2, definitivamente superan el corte de 80, considerado “excelente” en el modelo de usabilidad (Sauro & Lewis, 2016; Suria et al., 2024). Estos valores son parecidos o también se considera que son más altos que los reportados en estudios previos de FIDO2/WebAuthn (Lyastani et al., 2020; Owens et al., 2021). Por el contrario, la puntuación de contraseñas tradicionales está viva por debajo del rango de “aceptable” y muy por debajo del benchmark histórico (Reese et al., 2019).

Estos resultados apuntan a la hipótesis de que la experiencia de los usuarios con passkeys, no solo es más rápida y fluida, sino que además se considera mucho más satisfactoria, al igual que la probabilidad de recomendación, cosa que es bastante importante para el despliegue de la

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

solución en escenarios reales (Suria et al., 2024).

Los resultados sugieren que los passkeys pueden ser una alternativa viable y provechosa para las contraseñas básicas en las aplicaciones empresariales. La facilidad para utilizarlas, su seguridad y su aprecio más alto llevan a una buena predisposición para su adopción a gran escala, sobre todo en personas adultas jóvenes y en personas usuarias con un nivel de tecnología moderado. Sin embargo, la literatura también identifica grandes barreras, como por ejemplo la necesidad de educación sobre los mecanismos para la restauración y la confianza en la seguridad local generada por la clave privada (Ashish et al., 2024).

Para aumentar la adopción y disminuir el rechazo, es fundamental que los elementos como la integración con dispositivos ya existentes, la compatibilidad tecnológica y el desarrollo de procesos transparentes para recuperar dispositivos perdidos estén presentes. Estos facilitadores deben ser considerados en el diseño de experiencias para los usuarios (tutoriales, mensajes claros y “onboarding”) y en los planes de implementación organizativa.

La muestra del presente estudio es de tamaño y composición limitados, sólo se realizó durante una semana y no incluye a personas de edad avanzada o con poca alfabetización digital. Estos factores pueden restringir la posibilidad de aplicar los resultados a otros perfiles demográficos o contextos de uso constante.

Investigaciones anteriores han reportado limitaciones semejantes, en las que seguir teniendo acceso a muestras diversas o longitudinales se mantiene como un reto metodológico (Lyastani et al., 2020; Reese et al., 2019). Además, los autoinformes de satisfacción y usabilidad, así como las métricas objetivas, tales como la tasa de error y el tiempo de autenticación, podrían contribuir a una mejor comparación directa entre métodos.

5. CONCLUSIONES

El presente análisis experimental comprueba que la autenticación con passkeys resulta muy ventajosa en términos de usabilidad y satisfacción con respecto a las passwords convencionales, lo que se observa en las puntuaciones SUS altas y en las recomendaciones (very pleasant). Por lo tanto, los datos obtenidos confirman y amplían la evidencia recogida en la literatura internacional, y también muestran con claridad la tendencia hacia la utilización de métodos sin password dentro del contexto tecnológico y universitario-juvenil.

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

La principal aportación se refiere a que se dispone de evidencia estructurada en la que se muestra que los passkeys son superiores en relación a la usabilidad y a la aceptación. Estos resultados, además, se pueden considerar como el punto de partida para tomar decisiones adecuadas para la implantación de autenticación sin password, y abrir líneas de investigaciones más extensivas, a largo plazo y con diferentes poblaciones.

Para las investigaciones futuras sería recomendable: ampliar el rango de la muestra; realizar trabajos en contextos no académicos; y ahondar en el estudio de las barreras para la adopción y la recuperación de credenciales. También, se afirma que es recomendable hacer estudios longitudinales que estudien la permanencia de uso y la percepción a largo plazo.

Desde el enfoque de las implicaciones prácticas, los hallazgos obtenidos sugieren que las organizaciones e instituciones educativas, en particular, pueden ver beneficiadas también en otras dimensiones las posibilidades de adopción progresiva de passkeys como mecanismo principal de autenticación. La puntuación SUS obtenida de 83,2 por parte de los passkeys no sólo supera el punto de “excelente” en la escala de Brooke (1996), sino que avala también la asequibilidad de la curva de aprendizaje asociado a esta tecnología para los usuarios jóvenes con un nivel de experiencia tecnológica moderada (grande o bajo). Por lo que los responsables de las políticas de seguridad informática deberían incorporar passkeys en sus políticas asociadas a mecanismo de autenticación, y sí posiblemente por parte de procesos de onboarding y mecanismos de recuperación de credenciales claros como elementos clave, que situamos en una de las formas para reducir la resistencia al cambio y potenciar la aceptación del usuario final.

Por último, este trabajo contribuye a la cimentación de una línea de investigación sobre la usabilidad de autenticación en el contexto latinoamericano, que históricamente ha sido un ámbito poco representado en la literatura científica internacional sobre ciberseguridad. Los resultados presentados son algo de gran robustez empírica que puede servir de faro de ciertas políticas de implementación tecnológica en universidades y entidades públicas, así como en empresas de la región. La convergencia entre los resultados obtenidos y los reportados por estudios en contextos internacionales refuerzan, sin lugar a la duda de sus pertinencias, la validez ecológica de los passkeys como un método de autenticación seguro, usable y escalable, capaz de dar respuesta de los retos actuales de la seguridad digital sin comprometer la experiencia de usuario.

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

Contribución de los Autores (CRediT): EAZG: Conceptualización, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Software, Supervisión, Validación, Visualización, Redacción - borrador original. AJVR: Curación de datos, Investigación, Software, Visualización, Redacción - borrador original. CAJD: Investigación, Software, Validación, Visualización, Redacción - revisión y edición. ACMDLS: Administración del proyecto, Supervisión, Validación, Redacción - revisión y edición.

Conflicto de Intereses: Los autores declaran que no existen conflictos de intereses en esta publicación.

Declaración de Uso de Inteligencia Artificial: Los autores declaran que utilizaron herramientas de inteligencia artificial (IA) en la mejora de la redacción del artículo y corección de estilo. La herramienta utilizada para este fin fue: Claude.

REFERENCIAS

Abdrabou, Y., Abdelrahman, Y., Khamis, M., & Alt, F. (2021). Think Harder! Investigating the Effect of Password Strength on Cognitive Load during Password Creation. *Proceedings of the CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411763.3451636

Arias Cabarcos, P. & Meyer, P. (2025). 'The more accounts I use, the less I have to think': A Longitudinal Study on the Usability of Password Managers for Novice Users. *USENIX Proceedings of the Twenty-First Symposium on Usable Privacy and Security.* August 11–12, 2025. Seattle, WA, USA. https://www.usenix.org/conference/soups2025/presentation/cabarcos

Ashish, N., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of Physical Authentication Devices. *Comput. Secur., 139*(C). https://doi.org/10.1016/j.cose.2023.103664

Brooke, J. (1996). SUS: A "quick and dirty" usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & I. L. McClelland (Eds.), *Usability Evaluation in Industry* (pp. 189–194). London: Taylor & Francis.

Feinberg, S., & Murphy, M. (2000). Applying cognitive load theory to the design of Web-based instruction. *IPCC/SIGDOC '00: Proceedings of IEEE Professional Communication Society International Professional Communication Conference and Proceedings of the 18th Annual ACM International Conference on Computer Documentation: Technology & Teamwork*, 353–360. https://doi.org/10.1109/IPCC.2000.887293

FIDO Alliance. (2023). *Passkeys: Passwordless Authentication.* https://fidoalliance.org/specifications/

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view.

Fecha de recepción: 29 / 10 / 2025
Fecha de aceptación: 01 / 07 / 2026
Fecha de publicación: 21 / 08 / 2026

Interacting with Computers, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Kennesaw State University (2025). An Investigation on Users' In-category Password Reuse Behavior. *Coles College of Business Working Paper Series, 5*. https://campus.kennesaw.edu/colleges-departments/coles/research/docs/spring-2025/spring-2025-05.pdf

Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *2020 IEEE Symposium on Security and Privacy (SP),* San Francisco, CA, USA, 2020, pp. 268-285, doi: 10.1109/SP40000.2020.00047. https://ieeexplore.ieee.org/document/9152694

Mujeye, S. (2016). *An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity* [Doctoral dissertation, Nova Southeastern University]. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1962&context=gscis_etd

Owens, K., Anise, O., Krauss, A., & Ur, B. (2021). User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security. August 9–10*, 2021, 57–76. https://www.usenix.org/conference/soups2021/presentation/owens

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. USENIX Symposium on Usable Privacy and Security. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security.* August 12–13, 2019, Santa Clara, CA, USA. https://www.usenix.org/conference/soups2019/presentation/reese

Ruoti, S., Andersen, J. M., Zappala, D., & Seamons, K. E. (2016). Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *USENIX Symposium on Usable Privacy and Security.* https://doi.org/10.48550/arXiv.1510.08555

Sauro, J., & Lewis, J. R. (2016). *Quantifying the User Experience: Practical Statistics for User Research* (2nd ed). Morgan Kaufmann.

Suria, O. (2024). A Statistical Analysis of System Usability Scale (SUS) Evaluations in Online Learning Systems. *Journal of Information Systems and Informatics, 6*(2), 997–1004. https://doi.org/10.51519/journalisi.v6i2.750