

FIDO2 y WebAuthn para autenticación organizacional resistente al phishing: revisión sistemática

FIDO2 and WebAuthn for Phishing-Resistant Organizational Authentication: A Systematic Review



Harry Sly Rodríguez Sandoval

Universidad Nacional de Trujillo

<https://orcid.org/0009-0005-0433-3923>

hsrodriguezsa@unitru.edu.pe

Tania Ycela Chavez Alva

Universidad Nacional de Trujillo

<https://orcid.org/0009-0008-3240-716X>

tychavezal@unitru.edu.pe

Alberto Carlos Mendoza de los Santos

Universidad Nacional de Trujillo

<https://orcid.org/0000-0002-0469-915X>

amendozad@unitru.edu.pe

Universidad Nacional Micaela Bastidas de Apurímac – Perú

Riqchary, revista de investigación en ciencia y tecnología

ISSN: 2810-8124 (en línea) / ISSN: 2706-543X

Vol. 8 Núm. 2 (2026) - Publicado: 07/10/2026

doi.org/10.57166/riqchary/v8.n2.2026

Páginas: 23 - 32

Recibido 06/08/2026 ; Aceptado 07/09/2026

<https://doi.org/10.57166/riqchary/v8.n2.2026.3>

Resumen— La vulnerabilidad de contraseñas y códigos temporales ante el phishing impulsa la adopción de FIDO2/WebAuthn, pero la evidencia sobre su implantación organizacional es escasa en Latinoamérica. El objetivo fue sintetizar los beneficios, limitaciones y controles necesarios para implantar FIDO2, WebAuthn y passkeys en organizaciones, a partir de la evidencia publicada entre enero de 2020 y julio de 2026. Se realizó una revisión sistemática conforme a PRISMA 2020 en seis fuentes bibliográficas, de 32 registros identificados y 24 textos completos evaluados, se incluyeron 21 estudios. Los resultados muestran que las credenciales vinculadas al origen reducen el phishing basado en captura o retransmisión, aunque persisten riesgos asociados con recuperación débil, clientes comprometidos, secuestro de sesión, sincronización y configuraciones defectuosas. Los autenticadores de plataforma y las passkeys favorecieron la aceptación tras el aprendizaje, pero permanecieron barreras de activación, pérdida, migración e interoperabilidad. La evidencia sugiere que FIDO2/WebAuthn debe implantarse como parte de un programa integral de identidad que incluya recuperación de alta garantía, protección del cliente y la sesión y controles operativos continuos. Debido a la heterogeneidad de los estudios y su concentración en Europa y América del Norte, estos hallazgos deben validarse en organizaciones latinoamericanas.

Palabras clave: autenticación sin contraseña, FIDO2, passkeys, phishing

Abstract— The vulnerability of passwords and temporary codes to phishing drives the adoption of FIDO2/WebAuthn, yet evidence regarding their organizational implementation in Latin America is scarce. This study aimed to synthesize the benefits, limitations, and necessary controls for implementing FIDO2, WebAuthn, and passkeys in organizations, based on evidence published between January 2020 and July 2026. A systematic review following PRISMA 2020 guidelines was conducted across six bibliographic sources; out of 32 identified records and 24 full-text articles evaluated, 21 studies were included. Results indicate that origin-bound credentials reduce phishing based on credential capture or relay attacks, although risks associated with weak recovery, compromised clients, session hijacking, synchronization, and misconfigurations persist. Platform authenticators and passkeys fostered user acceptance following an initial learning curve, yet barriers related to activation, loss, migration, and interoperability remained. The evidence suggests that FIDO2/WebAuthn should be implemented as part of a comprehensive identity program that includes high-assurance recovery, client and session protection, and continuous operational controls. Given the heterogeneity of the studies and their concentration in Europe and North America, these findings require validation within Latin American organizations.

Keywords: passwordless authentication, FIDO2, passkeys, phishing

1 INTRODUCCIÓN

La autenticación condiciona el acceso a datos, servicios e infraestructura. Las contraseñas, los códigos de un solo uso y las notificaciones de aprobación continúan expuestos a reutilización, robo de credenciales, ingeniería social y retransmisión en tiempo real. FIDO2 integra la API Web Authentication (WebAuthn) y el protocolo cliente-autenticador CTAP2 para sustituir secretos compartidos por credenciales de clave pública vinculadas a una parte confiante. La clave privada permanece en el autenticador y la firma incorpora un desafío y el identificador del servicio; por ello, una credencial registrada para un origen no puede reutilizarse directamente en otro [1], [2]. La Fig. 1 resume este flujo.

La propiedad criptográfica mejora de forma sustancial la resistencia al phishing, pero no garantiza la seguridad de extremo a extremo [1], [2]. Las organizaciones deben gestionar registro, baja, pérdida de dispositivos, recuperación de cuentas, coexistencia con sistemas heredados, sincronización de passkeys, administración de llaves, protección del navegador y continuidad de la sesión [2], [3], [4], [5], [6]. Una ruta de respaldo más débil, una extensión maliciosa o una sesión no protegida pueden convertirse en el camino preferido del atacante [7], [8], [9].

El Banco Interamericano de Desarrollo (BID) describe, en su informe de 2026, diferencias regionales en el desarrollo de procesos de identificación digital en América Latina [10], mientras que el Reporte de Ciberseguridad 2025, elaborado por el BID y la Organización de los Estados Americanos (OEA), identifica brechas persistentes de capacidad, recursos, talento y coordinación en ciberseguridad [11]. En el Perú, el Centro Nacional de Seguridad Digital mantiene acciones de prevención frente al phishing, vishing y smishing [12]. Asimismo, en 2026 la FIDO Alliance lanzó el FIDO Americas Adoption Forum con foco inicial en Latinoamérica para acelerar la adopción de autenticación FIDO y passkeys [13]. Sin embargo, la búsqueda de esta revisión no identificó despliegues organizacionales longitudinales realizados en Perú o Latinoamérica, por lo que la transferencia de la evidencia internacional a entornos regionales, incluidos aquellos con recursos limitados, sigue siendo una brecha relevante.

El periodo de análisis se inició en enero de 2020 porque ese año marcó un cambio en el contexto organizacional en el que se utiliza la autenticación. La expansión masiva del trabajo desde el hogar durante la pandemia de COVID-19 planteó desafíos de ciberseguridad y fue aprovechada por los atacantes mediante campañas de phishing y smishing [14], [15]; lo que reforzó la relevancia de los mecanismos de autenticación resistentes al phishing en las organizaciones, que es el foco de esta revisión. Las fuentes [10]-[15] se incorporan únicamente para contextualización regional y justificación del periodo de análisis, pero no forman parte

del corpus de 21 estudios incluidos.

La literatura combina estudios de usuarios, despliegues empresariales, demostraciones de ataques, mediciones de implementaciones y prototipos [4], [5], [6], [7], [16]. Esta diversidad aporta evidencia complementaria, aunque dificulta comparar resultados y separar la resistencia del protocolo de la resiliencia del sistema de identidad. El objetivo de esta revisión fue sintetizar beneficios, limitaciones y controles de implantación de FIDO2/WebAuthn en organizaciones, atendiendo a seguridad, usabilidad, recuperación, compatibilidad, privacidad y operación. La pregunta que guía esta revisión es: ¿cuáles son los beneficios, limitaciones y controles necesarios para implantar FIDO2/WebAuthn en organizaciones?

Al tratarse de una revisión sistemática con síntesis narrativa, no se generaron hipótesis contrastables. Las dimensiones analizadas se agruparon en cuatro preguntas secundarias que estructuran la presentación de los resultados:

- **PS1 (seguridad y resistencia al phishing):** ¿Qué nivel de resistencia al phishing ofrecen FIDO2/WebAuthn y en qué condiciones se reduce ese beneficio?
- **PS2 (cliente, sesión y privacidad):** ¿Qué riesgos persisten en el cliente, la sesión y la privacidad una vez que la autenticación con FIDO2/WebAuthn se completa?
- **PS3 (usabilidad y adopción):** ¿Qué factores condicionan la usabilidad y la adopción de FIDO2/WebAuthn?
- **PS4 (recuperación, compatibilidad y despliegue):** ¿Qué limitaciones de recuperación y compatibilidad se reportan y qué implican para el despliegue organizacional?

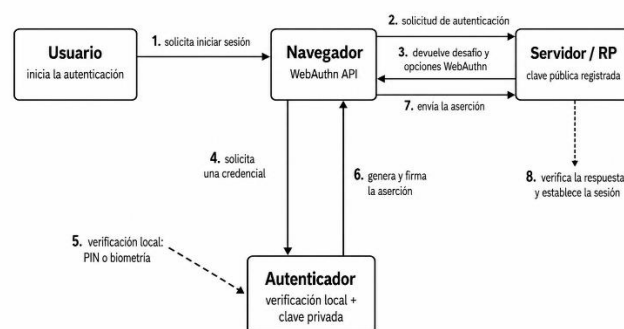


Fig. 1. Flujo simplificado de autenticación FIDO2/WebAuthn.

Fuente: Síntesis de los estudios [1] y [2].

2 METODOLOGÍA

Siguiendo PRISMA 2020 [17], se realizó una revisión sistemática. La búsqueda se cerró el 31 de julio de 2026 y cubrió publicaciones desde enero de 2020 hasta julio de 2026. Se consultaron IEEE Xplore, ACM Digital Library, USENIX, NDSS, ScienceDirect y SpringerLink. Scopus, Web of Science, Google Scholar y repositorios institucionales se utilizaron para verificar metadatos, DOI, versiones finales y referencias relacionadas. El rastreo de referencias se efectuó mediante la revisión de las listas bibliográficas de los estudios candidatos e incluidos; todo registro potencialmente elegible localizado en ese proceso se contrastó en las fuentes de verificación antes de incorporarlo. La expresión base fue: (FIDO2 O WebAuthn O passkey*) Y (phishing O seguridad O ataque* O usabilidad O adopción O empresa O organización* O recuperación O implementación O compatibilidad O privacidad).

Se incluyeron artículos de revista o congreso revisados por pares que evaluaran directamente FIDO2, WebAuthn o passkeys mediante estudios de usuarios, análisis de amenazas, ataques reproducibles, prototipos, mediciones de despliegues o comparaciones con método explícito. Se excluyeron duplicados, material comercial, documentos anteriores a 2020, trabajos centrados solo en contraseñas o en UAF/U2F sin implicaciones transferibles y preprints sin versión final revisada por pares. Se aceptaron publicaciones en inglés o español.

De cada estudio se extrajeron el año, diseño, muestra o contexto, dimensión principal, resultado y limitaciones, que se consignaron en una matriz en Excel. La calidad metodológica se evaluó según el diseño mediante claridad del objetivo, descripción del contexto, reproducibilidad, modelo de amenaza o comparador, adecuación de métricas, consistencia entre resultados y conclusiones, y reconocimiento de limitaciones. No se calculó una puntuación única porque los estudios de usuarios, ataques, prototipos y revisiones no son equivalentes. No se realizó un meta-análisis debido a la heterogeneidad de diseños, poblaciones y métricas; se utilizó una síntesis narrativa. El proceso de selección se documentó también en una matriz que registró, para cada estudio, la fuente y fecha de consulta, la decisión en cada, los campos de extracción y la verificación del segundo revisor.

La primera búsqueda produjo 26 registros y la actualización mediante rastreo de referencias añadió seis. Después de eliminar tres duplicados, se examinaron 29 registros; cinco fueron excluidos por título o resumen. Se evaluaron 24 textos completos y se incluyeron 21 estudios: 20 estudios primarios y una revisión comparativa, utilizada únicamente para contextualizar adopción y cumplimiento sin duplicar hallazgos de estudios primarios. Tres textos completos fueron excluidos: dos preprints sin versión final revisada por pares y un trabajo fuera del alcance. La selección y la extracción fueron

realizadas inicialmente por un revisor. Posteriormente, un segundo revisor las verificó de forma independiente y retrospectiva, sin encontrar desacuerdos en las decisiones de selección ni en los datos extraídos, lo que redujo el riesgo de error en ambos procesos. La Tabla 1 resume el protocolo y la Fig. 2 muestra el proceso de selección.

TABLA 1
Protocolo de búsqueda y selección

Elemento	Definición operativa
Periodo	Enero de 2020 a julio de 2026; búsqueda cerrada el 31/07/2026.
Fuentes	IEEE Xplore, ACM DL, USENIX, NDSS, ScienceDirect y SpringerLink; verificación en Scopus, WoS, Google Scholar y repositorios; rastreo de las listas bibliográficas de estudios candidatos e incluidos.
Inclusión	Estudios revisados por pares con evaluación empírica, técnica o comparativa de FIDO2, WebAuthn o passkeys.
Exclusión	Duplicados, material comercial, preprints sin versión final y trabajos fuera del alcance temporal o temático.
Selección	32 identificados; 3 duplicados; 29 examinados; 24 textos completos; 21 incluidos.
Pre-registro	No realizado antes de la ejecución; decisiones metodológicas y flujo reportados de forma retrospectiva y explícita.
Calidad y extracción	Objetivo, contexto, reproducibilidad, amenaza/comparador, métricas, coherencia y limitaciones; diseño, muestra, resultado y restricciones. Selección y extracción por un revisor; verificación independiente posterior por un segundo revisor.
Síntesis	Narrativa por seguridad, cliente/sesión, privacidad, usabilidad, recuperación, compatibilidad y despliegue.

Nota. ACM DL = ACM Digital Library; WoS = Web of Science; DOI = Digital Object Identifier.

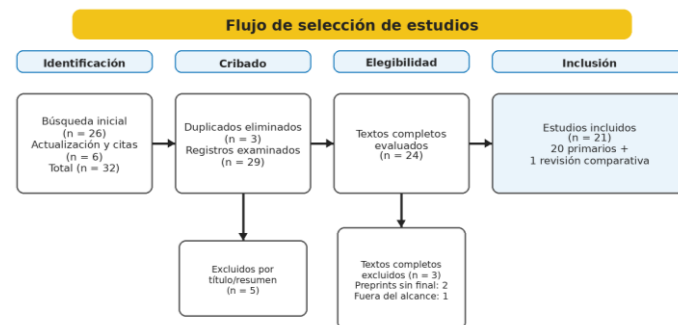


Fig. 2. Diagrama de flujo PRISMA 2020.

Fuente: Síntesis del proceso de selección de los estudios incluidos, conforme a PRISMA 2020 [17].

3 RESULTADOS

Los 21 estudios incluidos abarcaron experimentos de laboratorio, estudios de campo, entrevistas con profesionales, mediciones de implementaciones web, ataques reproducibles, prototipos y una revisión comparativa. La evidencia principal se dividió en cuatro áreas: resistencia al phishing; cliente, sesión y privacidad;

usabilidad y adopción; recuperación, compatibilidad e implementación. La Tabla 2 caracteriza individualmente los 21 estudios incluidos mediante su diseño, muestra o contexto, dimensión principal y hallazgo clave. Las Tablas 3 y 4 resumen la evidencia técnica y organizativa, mientras que las Figs. 3 y 4 muestran la distribución temporal y por dimensión principal, respectivamente.

TABLA 2
Caracterización de los 21 estudios incluidos

Ref.	Diseño	Muestra o contexto	Dimensión principal	Hallazgo clave
[3]	Evaluación heurística comparativa	12 estrategias de recuperación	Recuperación	Las rutas basadas en contraseña o correo pueden reintroducir un factor susceptible al phishing.
[4]	Estudio de usabilidad empresarial	118 profesionales	Implementación / recuperación	Recuperación, migración, sistemas heredados y costos aparecen como preocupaciones centrales.
[5]	Entrevistas semiestructuradas	28 responsables y expertos	Implementación / adopción	Barreras técnicas, de recuperación, regulación, fricción y cultura de seguridad.
[6]	Estudio de campo longitudinal	Fase 1: 5 057 usuarios; fase 2: 2716 durante 6 meses	Usabilidad adopción	La aceptación mejora con el uso; persisten fricciones de activación, sincronización e intercambio.
[7]	Análisis de servicios + estudio de usuarios	Servicios FIDO en Alexa Top 100; estudio de usuarios	Seguridad phishing	55 % cayó en el ataque y otro 35 % fue potencialmente susceptible mediante factores degradables.
[8]	Análisis de ataques + dos estudios de usuarios	10 servicios; n=80 y n=20	Seguridad cliente	Siete ataques locales muestran que extensiones, XSS, clonación y cookies pueden eludir expectativas del usuario.
[9]	Prueba de concepto de ataque	Escenario BitM + XSS reflejado	Seguridad / sesión	Una autenticación válida no impide el compromiso si navegador, API o sesión están controlados.
[16]	Medición de implementaciones web	Despliegues reales en sitios web	Seguridad implementación	Configuraciones y mitigaciones difieren entre servicios; el cliente comprometido conserva relevancia.
[18]	Modelo de amenazas + prototipo	4 ataques de confirmación de transacciones	Seguridad transacción	La integridad requiere vincular de forma confiable el mensaje mostrado con el contenido firmado.
[19]	Ataque reproducible por superposición	Autenticadores con pantalla limitada	Seguridad interfaz	Las superposiciones pueden ocultar sesiones e inducir autorizaciones maliciosas.
[20]	Framework / prototipo de detección	Passkeys sincronizadas y almacenamiento en nube	Sincronización / seguridad	CASPER detecta uso de credenciales filtradas desde almacenamiento en nube con bajo impacto operativo.
[21]	Medición de canales temporales	8 autenticadores certificados	Privacidad	Dos de ocho autenticadores permitieron correlación remota de cuentas mediante diferencias temporales.
[22]	Estudio de laboratorio comparativo	n=94 (48 contraseña; 46 FIDO2)	Usabilidad adopción	FIDO2 passwordless mostró buena aceptación, junto con preocupaciones por pérdida y recuperación.
[23]	Despliegue de campo	8 empleados; 4 semanas	Usabilidad despliegue	La pérdida de la llave y el tiempo de acceso preocuparon; los beneficios de seguridad fueron poco tangibles.
[24]	Tres estudios de usuarios	n=42; n=27 en grupos focales; n=345 en línea	Usabilidad modelos mentales	67 % creyó inicialmente que la biometría se enviaba al sitio; la explicación redujo solo parte de la confusión.
[25]	Estudio comparativo de campo	n=97; 2 semanas	Usabilidad	El teléfono se percibió como seguro, pero el prototipo fue más lento y menos usable que la contraseña.
[26]	Estudio de laboratorio comparativo	n=87	Usabilidad adopción	Se prefirió el autenticador de plataforma; persistieron barreras para escenarios multidispositivo.
[27]	Estudio de campo corporativo	34 empleados; 5 semanas	Usabilidad despliegue	Las llaves biométricas redujeron tiempos y aumentaron satisfacción; persistieron problemas de compatibilidad y flujo.
[28]	Prototipo	Autenticación continua; navegadores web varios	Compatibilidad / despliegue	La evolución del estándar y las diferencias entre navegadores complican la implementación.
[29]	Prototipo + prueba multiplataforma + usuarios	15 usuarios	Compatibilidad / usabilidad	Más del 69 % completó la conexión inicial y el desempeño mejoró en el segundo intento.
[30]	Revisión comparativa	FIDO U2F, UAF y FIDO2	Implementación / cumplimiento	FIDO2 mostró mayor adopción, mientras U2F y UAF conservaron usos específicos.

Nota. La tabla resume diseño, muestra o contexto, dimensión principal y hallazgo clave a partir de la extracción de la revisión. Cuando un estudio incluyó varias fases, se conservan los tamaños relevantes de cada fase.

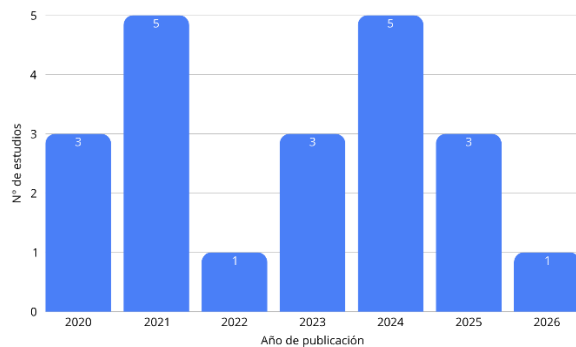


Fig. 3. Distribución de los estudios incluidos por año de publicación.

Fuente: Síntesis de los estudios incluidos.

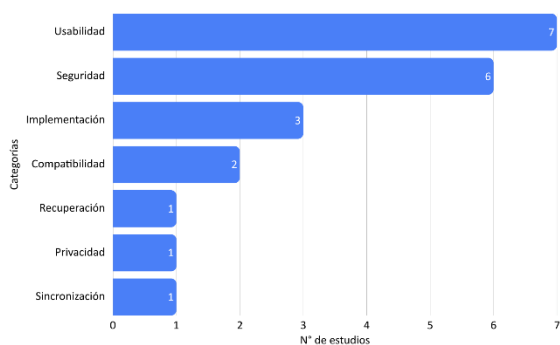


Fig. 4. Distribución de los estudios por dimensión principal de análisis.

Fuente: Síntesis de los estudios incluidos.

Se evaluó la posibilidad de realizar una síntesis cuantitativa de los resultados de los estudios; sin embargo, esta alternativa no se consideró apropiada debido a la heterogeneidad de estos, en cuanto a diseños, contextos, variables y métricas de evaluación.

Para complementar la distribución temporal y la clasificación por dimensión principal, se realizó un cruce entre ambas variables, con el propósito de identificar cómo se distribuyen las dimensiones de análisis a lo largo del periodo estudiado. Esta relación se representa mediante el mapa de calor presentado en la Fig. 5.

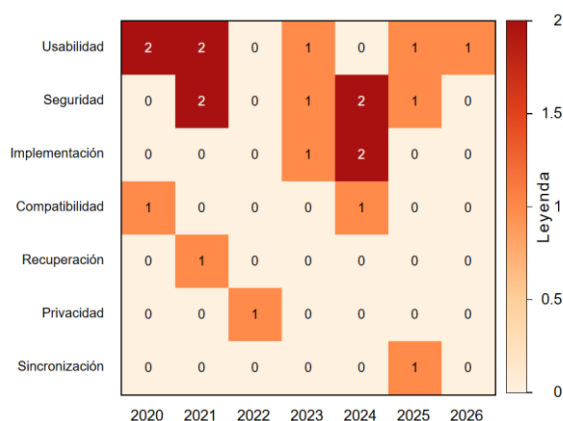


Fig. 5. Estudios por dimensión principal y año de publicación.

Fuente: Síntesis de los estudios incluidos.

Entre los estudios con participantes humanos, los tamaños de muestra variaron desde ocho empleados durante cuatro semanas [17] hasta 5057 usuarios en la primera fase del estudio longitudinal de Reittinger y Pernul [6]. Debido a los diseños multifase y a la heterogeneidad de métricas, no se calcularon una media combinada ni intervalos de confianza entre estudios.

TABLA 3
Estudios de seguridad, cliente, sesión y privacidad

Estudio	Diseño / Dimensión	Hallazgo principal
Ulqinak u et al. (2021)	Phishing en tiempo real y rutas alternativas	El 55 % cayó en el ataque y otro 35 % fue potencialmente susceptible cuando existían factores degradables [7].
Xu et al. (2021)	Ataques a confirmación de transacciones	La integridad exige vincular el mensaje visualizado con el contenido firmado [18].
Kepkow ski et al. (2022)	Ocho autenticadores certificados	Dos permitieron correlación remota de cuentas mediante diferencias temporales [21].
Kuchhal et al. (2023)	Despliegues web reales	La configuración y las mitigaciones variaron; el cliente comprometido conservó relevancia [16].
Yadav y Seamon s (2024)	Siete ataques locales; diez servicios; dos estudios de usuarios	Extensiones, XSS, clonación y ciclo de cookies permitieron ataques que los usuarios no detectaron adecuadamente [8].
Mahdad et al. (2024)	Ataques de superposición contra llaves	Interfaces limitadas permitieron ocultar sesiones y engañar al usuario para autorizar solicitudes maliciosas [19].
Catalan o et al. (2025)	BitM combinado con XSS	Una autenticación válida no impidió el compromiso cuando el navegador, la API o la sesión estaban controlados [9].
Islam et al. (2025)	CASPER para passkeys sincronizadas	El prototipo detectó el uso de credenciales filtradas desde almacenamiento en nube con bajo impacto operativo [20].

Nota. XSS = cross-site scripting; BitM = Browser-in-the-Middle; CASPER = mecanismo de detección para passkeys sincronizadas.

Seguridad y resistencia al phishing

La evidencia concuerda en que las credenciales de clave pública vinculadas al origen eliminan la característica de secreto reutilizable de las contraseñas y los códigos de un solo uso [1], [2]. Pero el beneficio depende de que el servicio no mantenga rutas de respaldo

universales. En el experimento de Ulqinaku et al., los usuarios podían ser desviados a otros mecanismos susceptibles de phishing [7].

Xu et al. mostraron que la confirmación de transacciones requiere un canal confiable entre lo que se muestra y lo que se firma [18]. Yadav y Seamons identificaron ataques de extensiones, XSS, clonación y gestión de cookies [8]; Mahdad et al. demostraron que las pequeñas pantallas de las llaves pueden facilitar el engaño a través de superposiciones [19]. Estos trabajos no vulneran la criptografía subyacente, sino que explotan la interfaz, el cliente o la interpretación humana.

Cliente, sesión y privacidad

La resistencia al phishing se neutraliza después de la autenticación si la siguiente sesión está expuesta [8], [9], [16]. Kuchhal et al. midieron diferencias significativas entre las implementaciones reales [16]. Catalano et al. demostraron que es posible que un navegador controlado o una vulnerabilidad XSS eludan la autenticación y secuestren la sesión [9].

La sincronización de claves de acceso reduce el impacto de la pérdida de dispositivos, pero transfiere parte del riesgo al proveedor de gestión [2], [6], [20]. Islam et al. propusieron la detección del abuso de claves de acceso extraídas del almacenamiento en la nube [20]. En términos de privacidad, Kepkowski et al. observaron canales de correlación temporal en dos de ocho autenticadores certificados [21]; la certificación no reemplaza las pruebas de implementación ni el principio de minimización de atestación.

TABLA 4
Estudios de usabilidad, recuperación y despliegue

Estudio	Diseño/ contexto	Hallazgo principal
Lyastani et al. (2020)	Laboratorio comparativo	Aceptación favorable, con preocupación por pérdida, transporte y recuperación [22].
Farke et al. (2020)	8 empleados, cuatro semanas	La pérdida de la llave y el tiempo de acceso preocuparon; los beneficios de seguridad fueron poco tangibles [23].
Klieme et al. (2020)	Prototipo de autenticación continua	La evolución del estándar y las diferencias entre navegadores complicaron el despliegue [28].
Lassak et al. (2021)	42 participantes, 27 en grupos focales y 345 en línea	El 67 % creyó inicialmente que la biometría se enviaba al sitio; la explicación redujo solo parte de la confusión [24].
Owens et al. (2021)	97 participantes durante dos	El teléfono fue percibido como seguro, pero el prototipo fue más lento y

Estudio	Diseño/ contexto	Hallazgo principal
	semanas	menos usable que la contraseña [25].
Kunke et al. (2021)	Evaluación de 12 estrategias de recuperación	Contraseña o correo como respaldo pueden anular el objetivo passwordless [3].
Würsching et al. (2023)	87 participantes	Se prefirió el autenticador de plataforma; persistieron barreras multidispositivo [26].
Kepkowski et al. (2023)	118 profesionales	Recuperación, pérdida, migración, sistemas heredados y costos fueron preocupaciones centrales [4].
Lassak et al. (2024)	28 entrevistas con responsables y expertos	Las barreras incluyeron recuperación, fricción, problemas técnicos, regulación y cultura de seguridad [5].
Rivera-Dourado et al. (2024)	Pruebas multiplataforma y 15 usuarios	FIDO2CAP fue viable; más del 69 % completó la conexión y mejoró en el segundo intento [29].
Angelogianni et al. (2024)	Revisión comparativa	FIDO2 mostró mayor adopción, mientras U2F y UAF conservaron usos específicos [30].
Lassak et al. (2025)	34 empleados, cinco semanas	Las llaves biométricas redujeron tiempos y aumentaron satisfacción; la compatibilidad y el flujo global siguieron siendo problemas [27].
Reittinger y Pernul (2026)	5 057 usuarios; 2 716 durante seis meses	La aceptación mejoró con el uso, pero persistieron activación, sincronización, intercambio y fricción con gestores [6].

Nota. Los tamaños se expresan como participantes, empleados, profesionales o entrevistas según el diseño. FIDO2CAP = FIDO2 Captive-portal Authentication Protocol.

Usabilidad, adopción

Los estudios de usuario muestran que la aceptación depende del tipo de autenticador, la experiencia previa y la consistencia de todo el flujo. Lyastani et al. demostraron una disposición a reemplazar las contraseñas y una conciencia de la pérdida y recuperación [22]. Farke et al. en una pequeña empresa informaron que los beneficios de seguridad eran menos tangibles que la fricción diaria [23]. Lassak et al. documentaron un concepto erróneo común: muchos participantes creían que los datos biométricos se enviaban al sitio incluso cuando la verificación era local [24].

El prototipo de un teléfono como autenticador

itinerante, como encontraron Owens et al., era más lento y menos útil que la contraseña [25]. Los autenticadores de plataforma fueron preferidos por Würsching et al. frente a las llaves itinerantes en su estudio comparativo [26]. En un estudio corporativo posterior, Lassak et al. mostraron que las llaves basadas en biometría reducían el tiempo de inicio de sesión y aumentaban la satisfacción, aunque las inconsistencias del flujo y la compatibilidad seguían siendo criticadas [27].

La evidencia longitudinal más amplia señala aprendizaje. Reitinger y Pernul vieron que la usabilidad y la aceptación de passkeys crecieron en un plazo de seis meses, aunque continuaron teniendo problemas con la activación manual, la sincronización multiplataforma, el intercambio y la interacción con los gestores de contraseñas [6].

Recuperación, compatibilidad y privacidad

La recuperación fue la brecha organizativa más común. Kunke et al. mostraron que reintroducir contraseñas o correos electrónicos como respaldo puede neutralizar la propiedad sin contraseña [3]. Kepkowski et al. identificaron la pérdida, la migración, la integración con sistemas heredados y el costo como preocupaciones de los profesionales [4]. Las entrevistas de Lassak et al. añadieron restricciones regulatorias, fricción y cultura de seguridad [5].

En cuanto a la compatibilidad, Klieme et al. observaron que las diferencias entre navegadores y el desarrollo del estándar complican las extensiones de autenticación continua [28]. Rivera-Dourado et al. demostraron que la experiencia mejora después de un primer intento, pero una tasa de finalización inicial por encima del 69 % aún deja a un grupo relevante sin completar el flujo [29]. La revisión comparativa de Angelogianni et al. colocó a FIDO2 como el protocolo más adoptado del conjunto analizado, sin eliminar usos específicos de generaciones anteriores [30].

4 DISCUSIÓN

Los resultados pueden distinguir entre la resistencia criptográfica al phishing y la resiliencia del sistema de identidad. La primera requiere que el origen y la firma para la parte de confianza sean consistentes [1], [2]; la segunda requiere que el registro, la recuperación, el soporte, el cliente, la sesión y los dispositivos se mantengan todos al mismo nivel [2], [3], [4], [5], [7], [9], [16]. Una organización puede usar FIDO2 pero aún sería vulnerable si mantiene SMS, OTP o contraseñas como rutas (el servicio de asistencia restablece cuentas si tienen evidencia débil) o si la siguiente sesión no está protegida [3], [4], [5], [7], [9], [16].

Las afirmaciones sobre la usabilidad deben ser contextuales. Los autenticadores de plataforma y las

claves de acceso sí reducen la fricción después del aprendizaje, pero los resultados dependen del sistema operativo, el navegador, el tipo de cuenta, la disponibilidad de dispositivos y la claridad de la interfaz [6], [25], [26], [27]. La evidencia no respalda afirmar que una modalidad es siempre superior; sí respalda medir el éxito, el tiempo, las deserciones, los incidentes y la satisfacción durante un período de uso real [6], [22], [25], [26], [27].

La recuperación debe planificarse antes del despliegue [2], [3], [4], [5]. Para cuentas críticas, el enfoque más común es registrar dos autenticadores independientes o utilizar la recuperación con una verificación más fuerte, segregación de funciones, registro de eventos, retraso de seguridad y notificación fuera de banda [2], [3], [4], [5]. Los factores susceptibles de phishing deben limitarse a excepciones documentadas y eliminarse gradualmente [5], [7]. Estas recomendaciones se alinean con ISO/IEC 27002:2022 [31]: los factores alternativos y la recuperación, con los controles de información de autenticación (5.17), gestión de identidades (5.16) y autenticación segura (8.5); el cliente y la sesión, con la gestión de la configuración (8.9), el monitoreo (8.16) y la codificación segura (8.28); la sincronización, con las relaciones con proveedores y el uso de servicios en la nube (5.19 y 5.23); y la adopción, con la concienciación y capacitación (6.3).

La revisión sistemática tiene limitaciones. El protocolo no fue pre-registrado; la verificación independiente por un segundo revisor se realizó de manera posterior; la heterogeneidad de diseños y métricas impidió combinar efectos; gran parte de la evidencia procede de prototipos o muestras pequeñas; y la mayoría de los estudios se realizaron en Europa y América del Norte. La actualización y el rastreo de referencias redujeron posibles omisiones, pero no garantizan la cobertura de todos los estudios. Además, se identificó poca evidencia longitudinal sobre costos de soporte, accesibilidad, recuperación en poblaciones diversas y despliegues en organizaciones latinoamericanas.

Estas limitaciones condicionan la generalización de los resultados. El segundo revisor se incorporó después de la selección y extracción iniciales, por lo que no equivale a una revisión por duplicado planificada desde el protocolo; las muestras pequeñas o muy contextuales reducen la extrapolación a otras organizaciones; y la concentración geográfica limita la transferencia directa a Latinoamérica y al Perú. Por ello, los controles y la hoja de ruta propuestos deben interpretarse como una síntesis cualitativa informada por la evidencia disponible, y no como estimaciones causales o efectos agrupados aplicables por igual a todos los entornos.

TABLA 5
Riesgos residuales y controles organizacionales derivados

Dimensión	Riesgo residual	Control recomendado
Factores alternativos	Phishing por contraseña, SMS u OTP	Retiro gradual por nivel de riesgo; excepciones temporales y monitoreadas [5], [7].
Recuperación	Pérdida del dispositivo y restablecimiento con evidencia débil	Dos autenticadores o recuperación reforzada, demora y notificación fuera de banda [2], [3], [4], [5].
Cliente sesión y	XSS, extensiones, navegador comprometido y secuestro de sesión	Política de seguridad de contenido (CSP), protección de cookies, reautenticación, endurecimiento de la configuración y monitoreo [8], [9], [16], [31].
Sincronización	Dependencia del proveedor o filtración de credenciales	Evaluar modelo de custodia, revocación, inventario y detección de abuso [2], [20].
Adopción	Confusión sobre biometría, activación y soporte	Pilotos, comunicación clara, métricas de éxito y capacitación diferenciada [6], [24], [25], [29].

RECOMENDACIONES DE IMPLEMENTACIÓN

La adopción debe llevarse a cabo en fases [4], [5], [6], [27], [31]. Primero, se deben inventariar las aplicaciones, poblaciones, métodos actuales y dependencias de recuperación; el acceso debe clasificarse según el impacto y la exposición; y se debe seleccionar un piloto representativo de navegadores, sistemas operativos y dispositivos [4], [5], [31]. Los indicadores mínimos son la tasa de registro, el éxito de autenticación, el tiempo de acceso, las deserciones, los incidentes de soporte y los resultados de simulación de phishing [5], [6], [27].

En segundo lugar, el ciclo de vida debe mantenerse [2], [3], [4], [5]. Las cuentas de alta criticidad requieren autenticadores redundantes o recuperación de alta seguridad [2], [3], [4]. Las credenciales para administradores y personal privilegiado pueden mantenerse vinculadas al dispositivo cuando el riesgo lo justifica [2], [31]. Otros métodos alternativos susceptibles de phishing deben ser restringidos, auditados y tener una fecha de retiro [5], [7], [31].

En tercer lugar, la implementación y la sesión deben

ser verificadas: ID de RP, validación de origen, presencia y verificación del usuario, gestión de credenciales, atestación cuando sea necesario, comportamiento multiplataforma, pérdida o reemplazo del dispositivo, protección de cookies, reautenticación y respuesta a clientes no confiables [1], [2], [8], [9], [16], [20], [31]. Finalmente, la gestión del cambio debe explicar cómo se procesan localmente las biometrías, cómo se sincronizan las credenciales y cómo se recuperará el acceso [5], [6], [24]. La Tabla 6 operacionaliza esta síntesis en una hoja de ruta propuesta, respaldada por [2], [3], [4], [5], [7], [9], [16], [31].

TABLA 6
Hoja de ruta propuesta para el despliegue organizacional

Fase	Acciones principales	Criterio de salida
1. Preparación	Inventario, clasificación de riesgo, selección de autenticadores y línea base.	Alcance y piloto aprobados.
2. Piloto	Registro controlado, pruebas multiplataforma, capacitación y medición.	Umbral de usabilidad y seguridad cumplidos.
3. Escalamiento	Alta por grupos, redundancia o recuperación reforzada y retiro de factores alternativos de respaldo.	Cobertura prioritaria y recuperación validada.
4. Operación	Monitoreo de sesiones, auditoría, simulaciones y pruebas periódicas.	Riesgo residual aceptado y mejora continua activa.

Líneas de investigación futura

La investigación futura debería comparar mecanismos de recuperación con usuarios reales; monitorear el comportamiento de passkeys sincronizadas durante interrupciones del ecosistema; investigar accesibilidad y amenazas interpersonales; y evaluar despliegues en organizaciones latinoamericanas [3], [4], [5], [6], [20]. También se necesitan estudios longitudinales sobre costos de soporte, privacidad de la atestación, compromiso del almacenamiento en la nube y resiliencia de la sesión después de la autenticación [5], [9], [16], [20], [21]. En particular, son necesarios estudios en organizaciones peruanas que comparen costos, interoperabilidad, accesibilidad, recuperación, soporte y adopción en condiciones operativas reales.

5 CONCLUSIONES

FIDO2 y WebAuthn representan una mejora sustancial frente al phishing basado en captura o retransmisión de credenciales, pero su éxito organizacional depende de todo el ciclo de identidad. La recuperación débil, las configuraciones incorrectas, los clientes comprometidos, las sesiones inseguras, la sincronización y los sistemas heredados continúan introduciendo riesgo. Los autenticadores de plataforma y las passkeys pueden favorecer la aceptación tras el aprendizaje, mientras que los escenarios de alta seguridad tienden a requerir mayor redundancia y controles complementarios.

La evidencia revisada indica que la implementación se beneficia de un enfoque basado en el riesgo, con autenticadores redundantes o recuperación de alta garantía, eliminación gradual de factores susceptibles a ser usados para phishing, protección de cliente y sesión, pruebas técnicas continuas y capacitación de usuarios. Así pues, la autenticación resistente al phishing cuadra mejor con la evidencia cuando se lleva a cabo como programa de seguridad de identidad y no como una función aislada de inicio de sesión. Estas conclusiones provienen de una síntesis cualitativa de estudios heterogéneos, mayoritariamente realizados en Europa y América del Norte y con muestras pequeñas o prototipos, por lo que deben leerse como orientaciones y no como efectos generalizables a todos los entornos. Se necesitan estudios longitudinales y comparativos en organizaciones latinoamericanas -incluyendo organizaciones peruanas- que evalúen costos de soporte, interoperabilidad, accesibilidad, recuperación y adopción antes de generalizar los resultados obtenidos principalmente en otros contextos.

REFERENCIAS

- [1] World Wide Web Consortium, "Web Authentication: An API for Accessing Public Key Credentials - Level 3," W3C Candidate Recommendation Snapshot, May 2026. <https://www.w3.org/TR/webauthn-3/>
- [2] D. Temoshok, Y.-Y. Choong, A. Regenscheid, R. Galluzzo, J. L. Fenton, J. Richer, and N. Lefkovitz, Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4, Jul. 2025. <https://doi.org/10.6028/NIST.SP.800-63B-4>
- [3] J. Kunke, S. Wiefeling, M. Ullmann, and L. Lo Iacono, "Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication," in Proc. Open Identity Summit 2021, Lecture Notes in Informatics, pp. 59-70, 2021. <https://doi.org/10.48550/arXiv.2105.12477>
- [4] M. Kepkowski, M. Machulak, I. Wood, and D. Kaafar, "Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study," in Proc. IEEE SecDev 2023, pp. 37-48, 2023. <https://doi.org/10.1109/SecDev56634.2023.00017>
- [5] L. Lassak, E. Pan, B. Ur, and M. Golla, "Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication," in Proc. 33rd USENIX Security Symp., pp. 7231-7248, 2024. <https://www.usenix.org/conference/usenixsecurity24/presentation/lassak>
- [6] T. Reitinger and G. Pernul, "No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage," in Proc. 2026 IEEE Symp. Security and Privacy, pp. 3607-3626, 2026. <https://doi.org/10.1109/SP63933.2026.00022>
- [7] E. Ulqinaku, H. Assal, A. Abdou, S. Chiasson, and S. Capkun, "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols," in Proc. 30th USENIX Security Symp., pp. 3811-3828, 2021. <https://www.usenix.org/conference/usenixsecurity21/presentation/ulqinaku>
- [8] T. K. Yadav and K. E. Seamons, "A Security and Usability Analysis of Local Attacks Against FIDO2," in Proc. 31st Network and Distributed System Security Symp. (NDSS), 2024. <https://doi.org/10.14722/ndss.2024.24327>
- [9] C. Catalano, A. Chezzi, V. S. Barletta, and F. Tommasi, "Defeating FIDO2/CTAP2/WebAuthn Using Browser in the Middle and Reflected Cross Site Scripting," *Journal of Computer Virology and Hacking Techniques*, vol. 21, art. 11, 2025. <https://doi.org/10.1007/s11416-025-00556-2>
- [10] J. L. Hernández Carrión, M. Porrúa, M. Urtasun, D. Ros Rooney, and S. Cabello, Desarrollo e implementación de procesos de identificación digital en los países de América Latina, Inter-American Development Bank, 2026. <https://doi.org/10.18235/0013931>
- [11] M. Porrúa et al., 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, Inter-American Development Bank, in collaboration with the Organization of American States and the Global Cyber Security Capacity Centre (University of Oxford), Dec. 2025. <https://doi.org/10.18235/0013872>
- [12] Presidencia del Consejo de Ministros, Centro Nacional de Seguridad Digital, "Cómo identificar ataques de Ingeniería Social," Guía, 11 Mar. 2025. <https://www.gob.pe/institucion/pcm/informes-publicaciones/6554886-como-identificar-ataques-de-ingenieria-social>
- [13] FIDO Alliance, "Launching the FIDO Americas Adoption Forum," 26 Feb. 2026. <https://fidoalliance.org/launching-the-fido-americas-adoption-forum/>
- [14] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple y X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of

- cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, art. 102248, 2021. <https://doi.org/10.1016/j.cose.2021.102248>
- [15] F. Carroll, J. A. Adejobi y R. Montasari, "How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society," *SN Computer Science*, vol. 3, art. 170, 2022. <https://doi.org/10.1007/s42979-022-01069-1>
- [16] D. Kuchhal, M. Saad, A. Oest, and F. Li, "Evaluating the Security Posture of Real-World FIDO2 Deployments," in *Proc. ACM CCS 2023*, pp. 2381-2395, 2023. <https://doi.org/10.1145/3576915.3623063>
- [17] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, art. n71, 2021. <https://doi.org/10.1136/bmj.n71>
- [18] P. Xu, R. Sun, W. Wang, T. Chen, Y. Zheng, and H. Jin, "SDD: A Trusted Display of FIDO2 Transaction Confirmation without Trusted Execution Environment," *Future Generation Computer Systems*, vol. 125, pp. 32-40, 2021. <https://doi.org/10.1016/j.future.2021.06.034>
- [19] A. T. Mahdad, M. Jubur, and N. Saxena, "Breaching Security Keys without Root: FIDO2 Deception Attacks via Overlays Exploiting Limited Display Authenticators," in *Proc. ACM CCS 2024*, pp. 1686-1700, 2024. <https://doi.org/10.1145/3658644.3690286>
- [20] M. Islam, S. S. Arora, R. Chatterjee, and K. C. Wang, "Detecting Compromise of Passkey Storage on the Cloud," in *Proc. 34th USENIX Security Symp.*, pp. 7743-7762, 2025. <https://www.usenix.org/conference/usenixsecurity25/presentation/islam>
- [21] M. Kepkowski, L. Hanzlik, I. D. Wood, and M. A. Kaafar, "How Not to Handle Keys: Timing Attacks on FIDO Authenticator Privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, no. 4, pp. 705-726, 2022. <https://doi.org/10.56553/popets-2022-0129>
- [22] S. G. Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication," in *Proc. 2020 IEEE Symp. Security and Privacy*, pp. 268-285, 2020. <https://doi.org/10.1109/SP40000.2020.00047>
- [23] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth, "You Still Use the Password After All - Exploring FIDO2 Security Keys in a Small Company," in *Proc. SOUPS 2020*, pp. 19-35, 2020. <https://www.usenix.org/conference/soups2020/presentation/farke>
- [24] L. Lassak, A. Hildebrandt, M. Golla, and B. Ur, "It's Stored, Hopefully, on an Encrypted Server: Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn," in *Proc. 30th USENIX Security Symp.*, pp. 91-108, 2021. <https://www.usenix.org/conference/usenixsecurity21/presentation/lassak>
- [25] K. Owens, O. Anise, A. Krauss, and B. Ur, "User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators," in *Proc. SOUPS 2021*, pp. 57-76, 2021. <https://www.usenix.org/conference/soups2021/presentation/owens>
- [26] L. Würsching, F. Putz, S. Haesler, and M. Hollick, "FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones," in *Proc. CHI 2023*, art. 68, pp. 1-16, 2023. <https://doi.org/10.1145/3544548.3580993>
- [27] L. Lassak, N. Lindemann, and M. Kowalewski, "From TOTP to Security Keys: Studying the Reality of Passwordless FIDO2 Authentication With PIN and Biometrics in a Corporate Environment," in *Proc. SOUPS 2025*, pp. 371-389, 2025. <https://www.usenix.org/conference/soups2025/presentation/lassak>
- [28] E. Klieme, J. Wilke, N. van Dornick, and C. Meinel, "FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication," in *Proc. IEEE TrustCom*, pp. 1857-1867, 2020. <https://doi.org/10.1109/TrustCom50675.2020.00254>
- [29] M. Rivera-Dourado, M. Gestal, A. Pazos, and J. Vázquez-Naya, "A Novel Protocol Using Captive Portals for FIDO2 Network Authentication," *Applied Sciences*, vol. 14, no. 9, art. 3610, 2024. <https://doi.org/10.3390/app14093610>
- [30] A. Angelogianni, I. Politis, and C. Xenakis, "How Many FIDO Protocols Are Needed? Analysing the Technology, Security and Compliance," *ACM Computing Surveys*, vol. 56, no. 8, art. 214, pp. 214:1-214:51, 2024. <https://doi.org/10.1145/3654661>
- [31] International Organization for Standardization, ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection - Information security controls, 2022. <https://www.iso.org/standard/75652.html>