InvestiGO
Revista Científica Multidisciplinaria
ISSN 2953-6367
http://revistainvestigo.com

Marzo 2026
Vol. 7 No ,19, PP. 261-282
https://doi.org/10.56519/r5906256

ENSEÑANZA ACCESIBLE DE CIBERSEGURIDAD BÁSICA PARA PERSONAS CON DISCAPACIDAD VISUAL

ACCESSIBLE TEACHING OF BASIC CYBERSECURITY FOR PEOPLE WITH VISUAL IMPAIRMENTS

William Adriano[1], Gustavo Machado[2], Jairo Manzano [3], Kerly Chagñay[4], Edwin León[5], Steven Pusay[6]

{william_adriano@sangabrielriobamba.edu.ec[1], gmachado@sangabrielriobamba.edu.ec[2], j.manzano@sangabrielriobamba.edu.ec[3], kerly_chagniay735@sangabrielriobamba.edu.ec [4], edwin_leon111@sangabrielriobamba.edu.ec[5], steven_pusay204 @sangabrielriobamba.edu.ec[6]}

Fecha de recepción: 19/03/2026 / Fecha de aceptación: 27/03/2026 / Fecha de publicación: 31/03/2026

RESUMEN: Las personas con discapacidad visual enfrentan una doble vulnerabilidad en el ámbito digital: son susceptibles a los ciberdelitos y, simultáneamente, encuentran barreras de accesibilidad en las herramientas y en la formación en ciberseguridad, habitualmente diseñadas desde una perspectiva visual. Este estudio tuvo como objetivo diseñar, implementar y evaluar la efectividad de una aplicación web accesible para la enseñanza de ciberseguridad básica en los 30 socios de la Asociación Provincial de Discapacitados Visuales de Chimborazo (APRODVICH), en Riobamba, Ecuador. Se empleó un enfoque mixto con diseño cuasi-experimental de pre-prueba y post-prueba, enmarcado en una investigación basada en diseño. La herramienta desarrollada fue una aplicación web progresiva que cumple con los criterios de accesibilidad WCAG 2.1 nivel AA y se organizó en tres módulos temáticos. La intervención combinó talleres prácticos presenciales con la aplicación de cuestionarios adaptados antes y después del proceso formativo. Los resultados evidenciaron una mejora sustancial: el 80% de los participantes que inicialmente declaró no poseer conocimientos en ciberseguridad transitó hacia niveles intermedios (70%) y avanzados (10%). El 90% de los usuarios calificó la aplicación como de fácil o muy fácil uso, y el 80% adoptó contraseñas más robustas e incorporó conductas sistemáticas de verificación ante posibles estafas. Cabe destacar que el 96,7% de los participantes reportó un incremento en su confianza y autonomía

[1]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/0000-0003-1357-6220, +593 99 927 5406.
[2]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/0009-0008-2158-4195, +593 99 251 8554.
[3]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/ 0009-0001-9646-8390, +593 98 477 1130.
[4]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/0009-0005-5036-8027, +593 98 163 7974.
[5]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/0009-0009-4612-079X, +593 96 307 6012.
[6]Carrera de Tecnología Superior Universitaria de Desarrollo de Software, Instituto Superior Tecnológico “San Gabriel” condición Universitario – Ecuador, https://orcid.org/0009-0007-3052-5982, +593 93 972 9896.

digital. Se concluye que una intervención educativa en ciberseguridad, fundamentada en estándares de accesibilidad y en una metodología práctica, puede generar mejoras notables en los conocimientos, las prácticas y el empoderamiento digital de personas con discapacidad visual. El modelo desarrollado resulta replicable y contribuye a reducir la brecha de inclusión digital en este colectivo.

Palabras clave: Accesibilidad web; Ciberseguridad; Discapacidad visual; Inclusión digital; Tiflotecnología; WCAG 2.1

ABSTRACT: People with visual impairments face a double vulnerability in the digital realm: they are susceptible to cybercrime and, simultaneously, encounter accessibility barriers in cybersecurity tools and training, which are typically designed from a visual perspective. This study aimed to design, implement, and evaluate the effectiveness of an accessible web application for teaching basic cybersecurity to the 30 members of the Provincial Association of the Visually Impaired of Chimborazo (APRODVICH), in Riobamba, Ecuador. A mixed-methods approach with a quasi-experimental pre-test/post-test design was used, framed within design-based research. The developed tool was a progressive web application that meets WCAG 2.1 Level AA accessibility criteria and was organized into three thematic modules. The intervention combined in-person practical workshops with the application of adapted questionnaires before and after the training process. The results showed a substantial improvement: 80% of participants who initially reported having no cybersecurity knowledge progressed to intermediate (70%) and advanced (10%) levels. 90% of users rated the application as easy or very easy to use, and 80% adopted stronger passwords and incorporated systematic verification practices to combat potential scams. Particularly significant, 96.7% of participants reported an increase in their digital confidence and autonomy. It is concluded that an educational intervention in cybersecurity, based on accessibility standards and a practical methodology, can generate notable improvements in the knowledge, practices, and digital empowerment of people with visual impairments. The developed model is replicable and contributes to reducing the digital inclusion gap for this group.

Keywords: Web accessibility; Cybersecurity; Visual impairment; Digital inclusion; Typhlotechnology; WCAG 2.1

INTRODUCCIÓN

En la era digital, la ciberseguridad se ha consolidado como una competencia fundamental para la participación plena en la sociedad. La protección de la información personal, financiera y social es un requisito previo para actividades cotidianas como la banca en línea, las compras por internet o la comunicación en redes sociales. Sin embargo, la enseñanza y los recursos de ciberseguridad no siempre consideran las necesidades de accesibilidad de las personas con discapacidad visual (PDV) (1), lo que genera una brecha de equidad digital y las sitúa en un estado de vulnerabilidad. Este colectivo enfrenta una “doble vulnerabilidad” en el entorno digital (2): por un lado, son objetivo de los mismos ciberdelitos que la población general y, por otro, se encuentran con

barreras de accesibilidad insalvables en las herramientas (3) y la educación en ciberseguridad, diseñadas predominantemente desde una perspectiva visual.

Estudios recientes confirman la gravedad y el alcance global de este problema. Khan et al. (18) demuestran que las PDV suelen desarrollar comportamientos de riesgo en línea, como la reutilización de contraseñas, no por desconocimiento, sino porque las interfaces de seguridad estándar resultan inaccesibles para sus lectores de pantalla (4). Profundizando en esta problemática, Feng et al. (5) revelan que, si bien los usuarios ciegos o con baja visión (BLV) son conscientes de los riesgos de privacidad, sus estrategias de mitigación son a menudo insuficientes, en parte porque las propias tecnologías de apoyo pueden introducir nuevas vulnerabilidades. La dependencia de terceros para tareas cotidianas como leer documentos privados o realizar transacciones, documentada por Ahmed et al. (2), expone a las PDV a riesgos únicos en la intersección de lo físico y lo digital. En esta misma línea, una revisión sistemática de la literatura en las principales bases de datos científicas (ACM e IEEE) llevada a cabo por Thoo et al. (6) confirma la escasez de soluciones educativas proactivas y accesibles diseñadas específicamente para esta población, concentrando la investigación en áreas como la movilidad (3) o la interacción no visual, pero no en la alfabetización en seguridad digital.

A pesar de los avances tecnológicos y la existencia de la tiflotecnología, entiéndase como el conjunto de técnicas y recursos que facilitan el uso de la tecnología a las PDV (7), aún persiste una notable escasez de recursos pedagógicos adaptados en el ámbito de la ciberseguridad. Los programas de formación suelen basarse en elementos visuales como diagramas, capturas de pantalla o simulaciones gráficas, excluyendo de facto a quienes no pueden acceder a ellos (2). Esta barrera metodológica es especialmente crítica si se considera que herramientas como los lectores de pantalla (p. ej., NVDA, JAWS, VoiceOver) (8) son la puerta de entrada al mundo digital para la mayoría de las personas ciegas (7), y su eficacia depende de que los contenidos y las interfaces estén diseñados siguiendo pautas de accesibilidad contrastadas (9) (10), como las Web Content Accessibility Guidelines (WCAG) 2.1 (11) (12). La evaluación de la accesibilidad (13), como señalan Acosta-Vargas et al. (14), requiere métodos heurísticos que complementen las herramientas automáticas para identificar barreras como el contraste insuficiente o la falta de alternativas textuales (15), problemas comunes que afectan incluso a los sitios web mejor posicionados (16)(17).

La literatura especializada ha documentado ampliamente estas dificultades a nivel global (18), (5), (6); sin embargo, la evidencia disponible en contextos locales, particularmente en países de ingresos medios como Ecuador, es prácticamente inexistente, lo que deja sin respuesta cómo estas barreras se manifiestan en poblaciones con características socioeconómicas y culturales específicas.

Precisamente para abordar este vacío, la presente investigación se centró en la Asociación Provincial de Discapacitados Visuales de Chimborazo (APRODVICH), una organización que agrupa a 30 socios en la ciudad de Riobamba, Ecuador. Considerando el contexto local, en la ciudad de Riobamba de acuerdo con el INEC (19) existe 7920 personas con discapacidad visual, esta problemática se materializa de forma evidente. D esta manera, un diagnóstico inicial realizado en el marco de este proyecto reveló datos que confirman la pertinencia local del problema: el 80%

de los socios declaró no tener ningún conocimiento en ciberseguridad, el 70% afirmó haber sufrido o conocer casos de estafas digitales, y otro 80% reportó haber experimentado dificultades previas para acceder a cursos o información debido a la falta de accesibilidad (13). Estos hallazgos reflejan que, tal como ocurre en contextos internacionales, la población local enfrenta una brecha crítica entre el acceso a la tecnología y la capacidad de usarla de forma segura, pero con el agravante de contar con escasas iniciativas previas orientadas a su realidad. De ahí que este proyecto se proponga llenar ese vacío mediante el diseño, implementación y evaluación de una aplicación web accesible para la enseñanza de ciberseguridad básica, con el objetivo de generar evidencia contextualizada que pueda servir de base para futuras réplicas en otras organizaciones del país y la región.

Para abordar esta necesidad, el presente proyecto de innovación se propuso como objetivo general diseñar, implementar y evaluar la efectividad de una aplicación web accesible para la enseñanza de ciberseguridad básica dirigida a los socios de APRODVICH, esta se muestra en la Figura 1. Los objetivos específicos que guiaron la investigación fueron: (1) diagnosticar el nivel de conocimiento y las prácticas actuales en ciberseguridad de los socios mediante una evaluación inicial basada en instrumentos validados; (2) desarrollar una aplicación web interactiva que cumpliera con los estándares de accesibilidad WCAG 2.1 (20), integrando audio-descripciones, navegación por teclado y contenido multimodal; (3) capacitar a los socios mediante talleres presenciales en el laboratorio de APRODVICH, utilizando la aplicación y materiales de apoyo adaptados; (4) medir el impacto de la intervención comparando los resultados de la evaluación inicial con una evaluación final; y (5) socializar los resultados con la comunidad académica y la asociación beneficiaria. Este artículo presenta los resultados de esta intervención, cuyo impacto se ha medido a través de un diseño cuasi-experimental con pre y post prueba, demostrando una mejora sustancial en los conocimientos, comportamientos y autoconfianza digital de los participantes, y validando un modelo de enseñanza inclusivo y replicable.

MATERIALES Y MÉTODOS

La presente investigación se enmarcó en un enfoque mixto, combinando métodos cuantitativos y cualitativos, y se estructuró siguiendo una metodología de Investigación Basada en Diseño (IBD) o Design-Based Research (DBR), integrada con un diseño cuasi-experimental de pre-prueba y post-prueba para un solo grupo. Este enfoque permitió, por un lado, evaluar la efectividad de la intervención y, por otro, mejorar iterativamente la solución tecnológica y pedagógica en su contexto real de uso.

El estudio se desarrolló en cuatro fases principales secuenciales: (1) Justificación y diagnóstico, (2) Preparación y diseño de la solución, (3) Ejecución de la intervención, y (4) Análisis de resultados. Para las fases 1 y3 se aplicó el componente cuasi-experimental, al medir el nivel de conocimiento en ciberseguridad de los participantes antes y después de la intervención educativa en la asociación.

La población que es el objetivo del estudio estuvo formada por la totalidad de 30 socios activos de la Asociación Provincial de Discapacitados Visuales de Chimborazo (APRODVICH) de la ciudad

de Riobamba, Ecuador. Se trabajó con un censo de los 30 socios, lo que otorga alta validez interna a los resultados. Los participantes presentaban diversos grados de discapacidad visual, tales como: ceguera total o baja visión. Los resultados muestran un rango de edad predominante entre 26 y 40 años (70%) como los muestra la Figura 2. Todos los participantes eran usuarios habituales de dispositivos digitales, principalmente teléfonos inteligentes (80%), y dependían de tecnologías de apoyo como lectores de pantalla (80%) o asistentes de voz (20%) para su interacción digital con estos dispositivos.

Las actividades de: diagnóstico, recolección de datos y ejecución de los talleres se desarrollaron en las instalaciones de APRODVICH en su laboratorio de computación. Este lugar que resultaba familiar y accesible para los socios fue clave para garantizar su comodidad y la validez del estudio.

La intervención se centró en el uso de una aplicación web educativa, cuya portada se muestra en la Figura 1, desarrollada específicamente para el proyecto, y en talleres presenciales de capacitación.

Se diseñó y desarrolló una aplicación web progresiva (PWA), alojada en el dominio de la asociación (https://aprodvich.com). Esta aplicación estuvo estructurada en tres módulos interactivos basados en los resultados del diagnóstico inicial: "La llave maestra" que son las contraseñas seguras, "Detector de mentiras" que es la seguridad en redes sociales y detección de fraudes y "Mi círculo de confianza" referente a la privacidad de datos. Para garantizar el cumplimiento de las WCAG 2.1 nivel AA (11), se aplicaron técnicas específicas: uso de HTML semántico y atributos ARIA para lectores de pantalla, navegación completa por teclado con indicador de foco visible, y contenido multimodal con audio-descripciones y retroalimentación sonora. La conformidad se verificó mediante herramientas automáticas (WAVE, AChecker, Lighthouse), inspección heurística (14) con el método Barrier Walkthrough y pruebas de usabilidad con los participantes piloto utilizando lectores de pantalla NVDA, VoiceOver y TalkBack en dispositivos móviles y computadoras.

Para la recolección de datos, se utilizaron dos instrumentos principales.

El primero fue un cuestionario estructurado aplicado de forma oral y asistida a los 30 socios, el cual sirvió como evaluación diagnóstica inicial denominado como pre-test. Este cuestionario recogió información sobre su perfil demográfico, el uso de tecnología, herramientas de accesibilidad usada por los socios, sus experiencias previas con amenazas digitales, el nivel de conocimiento autopercibido en ciberseguridad y las preferencias de aprendizaje que tienen los socios encuestados. Los resultados de esta encuesta con un 80% sin conocimientos y el 70% como víctimas de estafas, permitieron establecer la línea base del proyecto y definir los contenidos de la capacitación.

El segundo instrumento fue un cuestionario de evaluación final denominado como post-test, aplicado también de forma oral tras la intervención. Este cuestionario incluyó preguntas para medir la adquisición de conocimientos específicos sobre contraseñas seguras, detección de phishing y privacidad, los cambios en comportamientos digitales, la usabilidad y accesibilidad de la aplicación web, y la percepción de los participantes sobre la metodología y su impacto en la

autonomía y confianza digital. Las preguntas abiertas permitieron recoger valiosa información cualitativa.

La validación de los instrumentos de recolección de datos se realizó mediante juicio de expertos y una prueba piloto. Los cuestionarios, basados en una adaptación accesible del instrumento Cybersecurity Attitudes, Behaviors, and Knowledge (CAB-K), fueron revisados por tres especialistas del equipo de investigación: dos con experiencia en accesibilidad web y tecnologías de apoyo, y uno en ciberseguridad. Estos evaluaron la claridad, pertinencia y adecuación del lenguaje. Con base en sus observaciones, se ajustaron los ítems para simplificar la terminología y contextualizar los ejemplos. Posteriormente, se realizó una prueba piloto con tres socios de APRODVICH no incluidos en la muestra final, lo que permitió verificar la correcta interpretación oral de las preguntas y el formato de entrevista asistida, refinando así el protocolo de aplicación. En cuanto al desarrollo tecnológico, se implementó una aplicación web progresiva (PWA) utilizando HTML5, CSS3, JavaScript (ES6) y el framework Vue.js para la gestión reactiva de la interfaz, mientras que el backend se desarrolló con Node.js y Express, con almacenamiento en PostgreSQL.

Se impartieron 6 talleres presenciales en el laboratorio de APRODVICH, con una duración total de 12 horas distribuidas en varias sesiones. Los talleres, liderados por los investigadores y con el apoyo de estudiantes de la carrera de Desarrollo de Software, siguieron una metodología práctica y guiada (aprender haciendo), la cual fue preferida por el 90% de los socios en el diagnóstico inicial. Durante las sesiones de los talleres, los participantes interactuaron directamente con la aplicación web en computadoras y realizaron ejercicios prácticos supervisados por los estudiantes participantes del instituto.

Los datos cuantitativos y cualitativos recogidos en las evaluaciones pre y post intervención fueron tabulados y analizados utilizando técnicas de estadística descriptiva. Se calcularon frecuencias y porcentajes para las variables categóricas con el objetivo de conocer el nivel de conocimiento, tipos de prácticas adoptadas, y valoraciones de usabilidad. Para evaluar la importancia del cambio en los conocimientos de los socios se compararon los porcentajes de respuestas correctas en las preguntas clave de los dos cuestionarios indicados. Los datos cualitativos provenientes de las preguntas abiertas fueron analizados mediante una categorización por temas para identificar los patrones y las percepciones sobre la experiencia de usuario y el impacto alcanzado del proyecto.

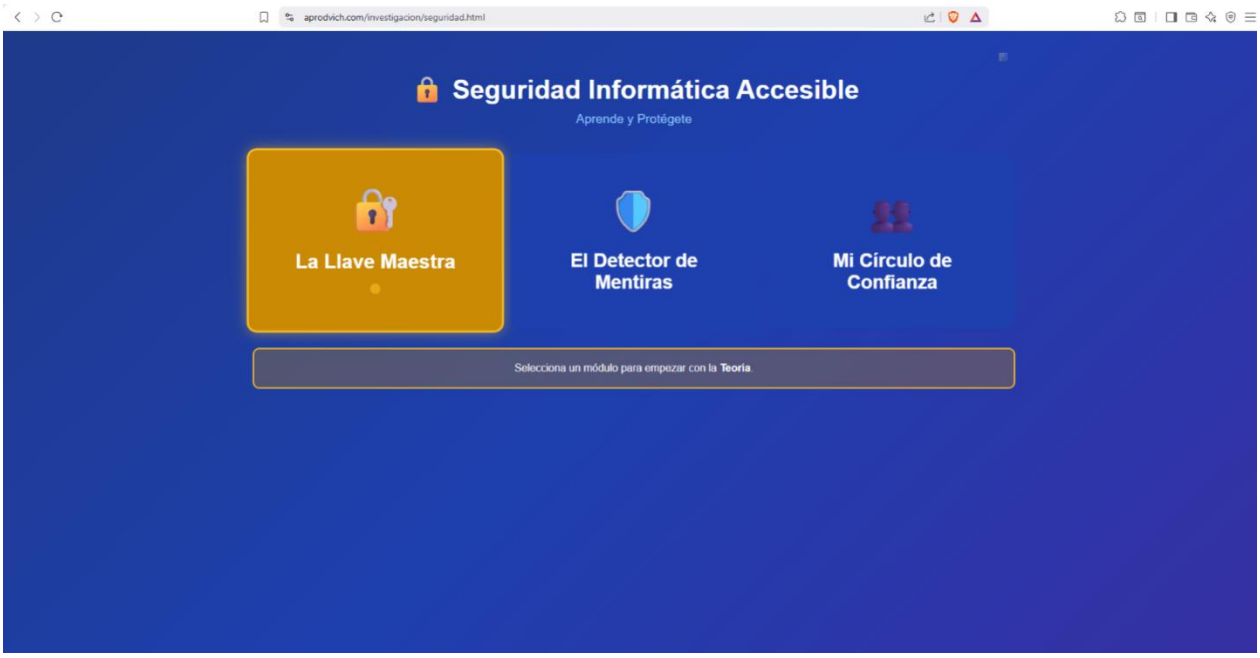

Figura 1. Principal Interfaz de la aplicación web desarrollada.

Fuente: https://aprodvich.com/investigacion/seguridad.html.

Nota: *"Herramienta desarrollada para la capacitación y evaluación"*

RESULTADOS

Los resultados que se presentan a continuación se derivan del análisis de los datos recolectados mediante los cuestionarios aplicados a los 30 socios de APRODVICH antes (pre-test) y después (post-test) de la intervención educativa. El análisis integra tanto datos cuantitativos sobre conocimientos y comportamientos, como datos cualitativos sobre la experiencia de usuario y la percepción de impacto.

1. Caracterización Inicial de los socios y Línea Base

Los datos recogidos en la evaluación diagnóstica permitieron definir el perfil de los beneficiarios y fijar el punto de partida del proyecto. Todos los 30 socios encuestados manifestaron hacer uso cotidiano de dispositivos digitales; entre ellos, el teléfono inteligente constituye el recurso principal para ocho de cada diez participantes. En cuanto a las ayudas técnicas para acceder a la información, la mayoría (80%) emplea lectores de pantalla, mientras que el restante 20% utiliza asistentes de voz. Uno de los hallazgos más relevantes de esta fase inicial es que el 80% de los participantes había enfrentado dificultades previas para acceder a cursos o contenidos digitales, situación atribuida directamente a la falta de accesibilidad de dichos recursos.

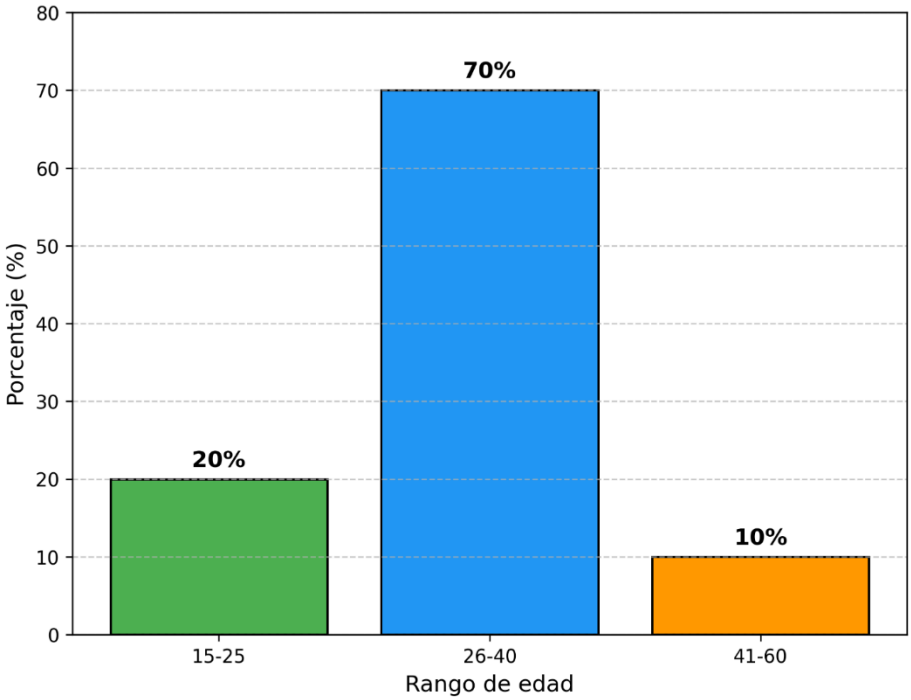

Figura 2. Distribución por rango de edad de los participantes.

Fuente: Análisis de resultados de la Encuesta inicial.

Nota: *"El perfil etario de la población"*

En cuanto a ciberseguridad, el 80% de los socios declaró no tener ningún conocimiento, y solo un 20% reportó un nivel básico. Ningún participante se autopercibió en un nivel intermedio o avanzado, esta información se muestra en la Figura 2. Esta falta de conocimiento se traduce en una alta exposición al riesgo: el 70% afirmó haber sufrido directamente o conocer casos de estafas digitales o problemas de seguridad. A pesar de esta vulnerabilidad, el 90% de los encuestados consideró importante aprender ciberseguridad y manifestó su disposición a participar en el proyecto, validando la pertinencia y la demanda de la intervención.

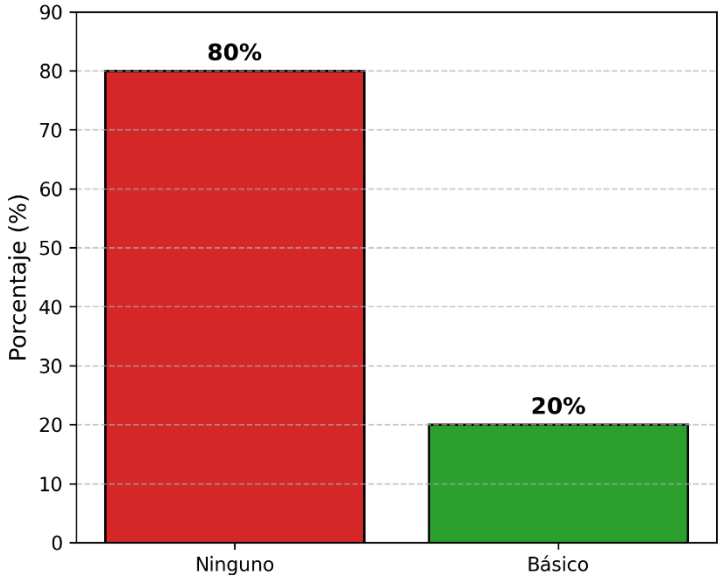

Figura 3. Nivel de conocimiento autopercibido en ciberseguridad.

Fuente: Análisis de resultados de la Encuesta inicial.

Nota: *"Punto de partida del proyecto y necesidad de intervención."*

2. Adquisición de Conocimientos en Ciberseguridad

La comparación de los resultados del pre-test y el post-test muestra una mejora sustancial y generalizada en los conocimientos de los participantes.

En cuanto al nivel de conocimiento autopercibido, se observó una transformación radical. Mientras que en la evaluación inicial el 80% de los socios se ubicaba en la categoría de "ningún conocimiento", tras la intervención, el 70% se autopercibió en un nivel "intermedio" y el 10% en un nivel "avanzado". El 20% restante se mantuvo en un nivel "básico", lo que indica que ningún participante se quedó en la categoría de "ningún conocimiento" después de la capacitación, esta información se puede visualizar en la Figura 3.

Para valorar la apropiación de los contenidos fundamentales se examinaron las respuestas a las preguntas específicas incluidas en el cuestionario posterior a la intervención; una síntesis de estos resultados se presenta en la Figura 5. En lo relativo al módulo de contraseñas seguras, los participantes evidenciaron un manejo sólido de los criterios esenciales. Así, el 93,3% reconoció acertadamente la conveniencia de "incluir números" como parte de una contraseña robusta, mientras que el 90% identificó la "longitud" como otro atributo clave. Otros aspectos igualmente valorados fueron la "combinación de mayúsculas y minúsculas" (83,3%) y la "omisión de información personal" (80%). El criterio que registró una menor frecuencia de mención fue el de emplear una clave "diferente para cada cuenta" (66,7%), lo que señala un aspecto que podría reforzarse en futuras ediciones de la formación. En conjunto, el 81,1% de los socios identificó en promedio cada uno de los elementos esenciales para construir una contraseña segura.

En la Figura 6 se evidencia la actitud de los socios frente a una situación simulada de estafa (phishing) a través de un mensaje de texto bancario, el 100% de las respuestas de los socios se alinearon con conductas de seguridad. La acción de protección inmediata "No hacer clic" en el enlace fue mencionada por el 70% de los participantes, mientras que un 50% indicó que "consultaría con alguien de confianza" y un 40% optaría por "verificar contactando directamente al banco por un medio oficial". Este resultado es particularmente relevante si se contrasta con el dato inicial del 70% que reportó haber sido víctima o conocer casos de estafas.

En cuanto a las estrategias para proteger la privacidad en entornos de redes sociales, los participantes señalaron con claridad diversas acciones preventivas. La conducta más frecuentemente reportada fue “no compartir el número de identificación personal”, mencionada por el 80% de los encuestados. En segundo lugar, con un 70%, se situó la opción de “configurar la privacidad de las publicaciones para que solo sean visibles para amigos”; mientras que “revisar quién puede acceder a la información personal” fue indicada por el 60% de los socios. Estos hallazgos evidencian una comprensión específica sobre la importancia de resguardar los datos personales, aspecto que constituye uno de los tres ejes temáticos prioritarios definidos en el proyecto.

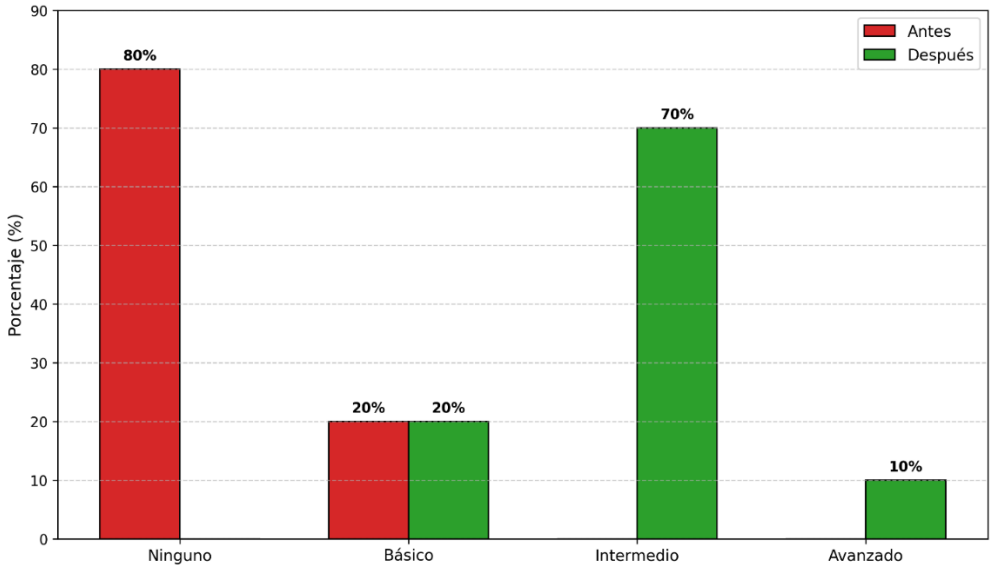

Figura 4. Comparación a nivel de conocimientos antes y después de la intervención.

Fuente: Análisis de resultados de la Encuesta inicial y final.

Nota: *“Demuestra visualmente el impacto de la capacitación”*

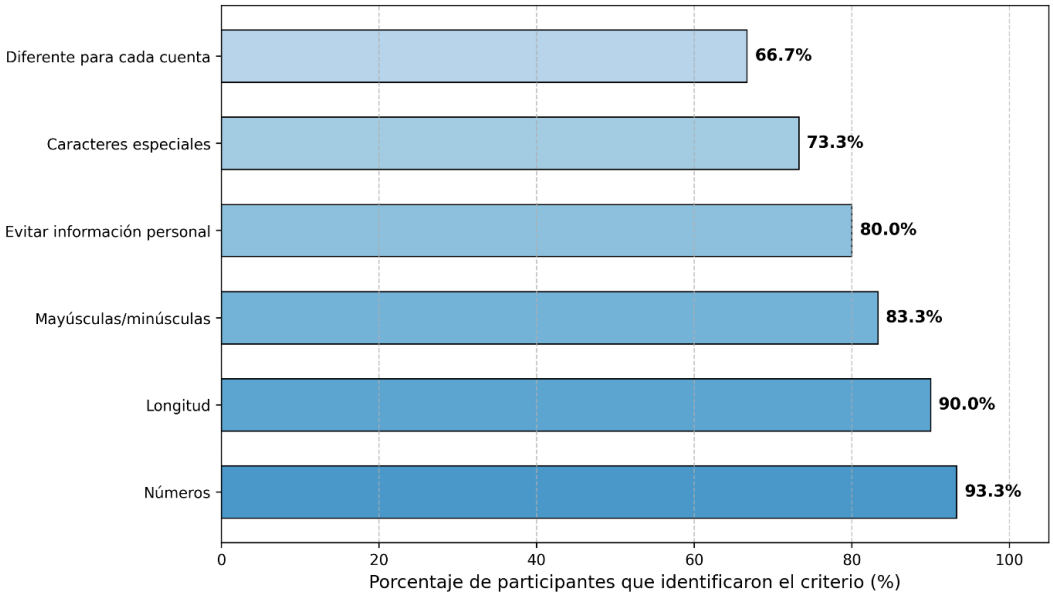

Figura 5. Criterios de contraseñas seguras identificados por participante.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Muestra los aspectos del módulo de contraseñas mejor asimilados"*

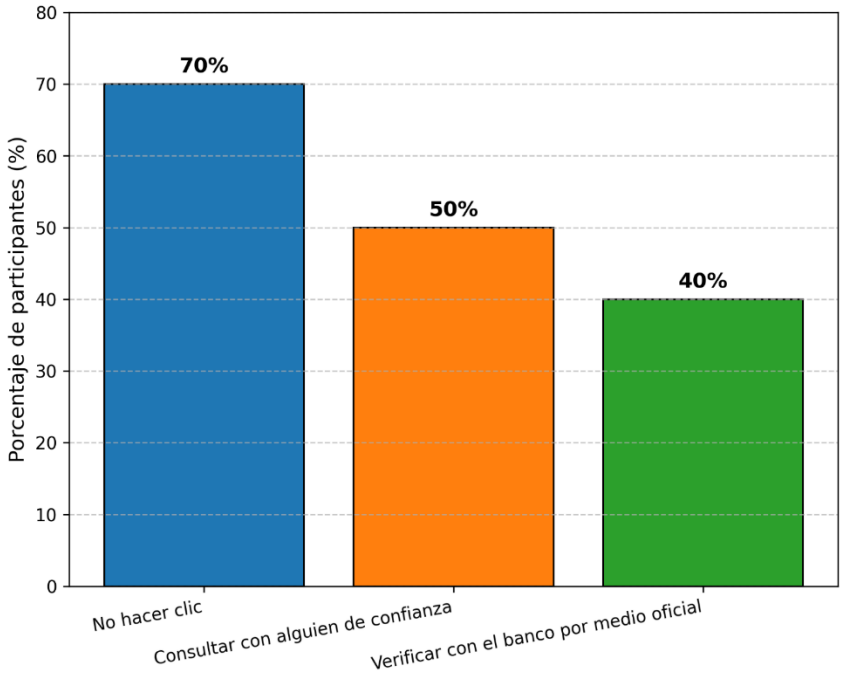

Figura 6. Conductas de seguridad frente a una estafa simulada.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Visualiza la internalización de conductas preventivas, un cambio conductual clave"*

3. Cambios en comportamientos y prácticas digitales

Uno de los indicadores de impacto más significativos es la transferencia del conocimiento a la acción. La evaluación final reveló que la gran mayoría de los participantes modificó sus comportamientos digitales como resultado de la capacitación.

Como se aprecia en la Figura 7, el 80% de los socios manifestó haber comenzado a emplear contraseñas más robustas y distintas para cada servicio a partir del inicio de la capacitación. En igual porcentaje (80%), los participantes señalaron que ahora revisan los mensajes de apariencia sospechosa antes de darles crédito, una modificación conductual de especial relevancia para la prevención de fraudes. Por otra parte, el 70% de los encuestados indicó que había ajustado las opciones de privacidad en sus redes sociales y que actúa con mayor cautela al compartir información en línea. Resulta particularmente significativo que ningún participante (0%) declarara no haber introducido cambio alguno, lo que refleja que la formación incidió de manera transversal en las prácticas digitales cotidianas de todo el grupo.

En coherencia con estos cambios, al preguntarles si se sentían más preparados para identificar y evitar estafas, el 90% de los participantes respondió "Sí, mucho más preparado". Un 6.7% adicional se sintió "un poco más preparado", sumando un 96.7% de socios que aumentaron su percepción de preparación frente a las amenazas digitales como lo demostramos en la Figura 8.

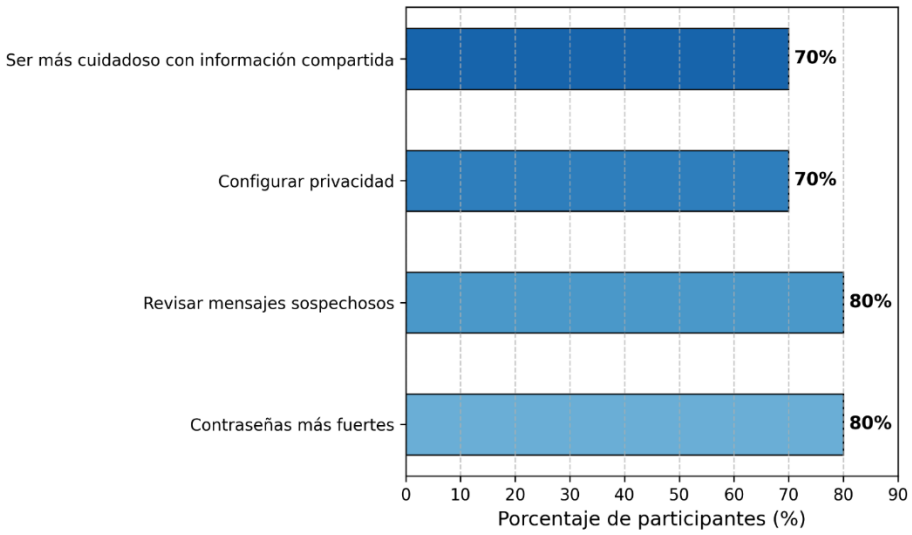

Figura 7. Prácticas de seguridad adoptadas después de la capacitación.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Demuestra que el conocimiento se tradujo en acciones concretas."*

Figura 8. Percepción de preparación para identificar y evitar estafas.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Refuerza el impacto en la autoconfianza preventiva."*

4. Evaluación de la herramienta tecnológica y la metodología pedagógica

La aplicación web desarrollada cuya portada se muestra en la Figura 1 y la metodología de taller práctico fueron ampliamente valoradas por los usuarios, validando las elecciones de diseño del proyecto.

Respecto a la usabilidad y accesibilidad de la herramienta desarrollada, el 70% de los participantes valoró la experiencia de uso con sus lectores de pantalla o mediante teclado como "muy fácil"; otro 20% la calificó como "fácil", aunque señaló haber enfrentado alguna dificultad menor. En conjunto, el 90% de los usuarios reportó una experiencia positiva, lo que evidencia que la adopción de los criterios establecidos en las WCAG 2.1 contribuyó de manera efectiva a la usabilidad del sistema. Solo un 3,3% de los encuestados indicó no haber podido utilizar la aplicación. Estos resultados se presentan de manera sintética en la Figura 9.

La claridad de la información también recibió una alta valoración. El 80% de los encuestados indicó que "todo fue muy claro", y un 10% adicional que "la mayoría de las cosas fueron claras", sumando un 90% de satisfacción en este aspecto. Este dato es especialmente relevante si se recuerda que, antes del proyecto, el 80% de los socios había tenido dificultades para acceder a cursos por falta de accesibilidad como lo resume la Figura 10.

En lo referente a la metodología de enseñanza, el 80% de los participantes consideró que el "taller práctico con guía" constituyó el formato más adecuado para su aprendizaje. El restante 20%

también lo valoró positivamente, aunque expresó el deseo de disponer de más tiempo para la práctica individual. Ningún participante manifestó preferencia por otro tipo de formato, lo que respalda plenamente la elección metodológica realizada a partir del diagnóstico inicial, en el que el 90% de los socios ya había manifestado su inclinación por este enfoque.

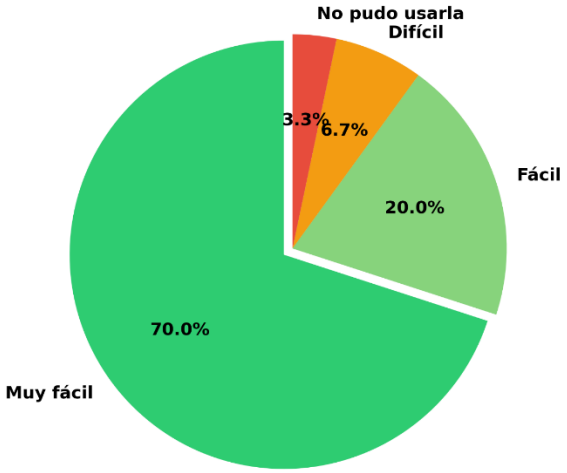

Figura 9. Usabilidad y accesibilidad de la aplicación web.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Valida el cumplimiento del objetivo de desarrollar una herramienta accesible."*

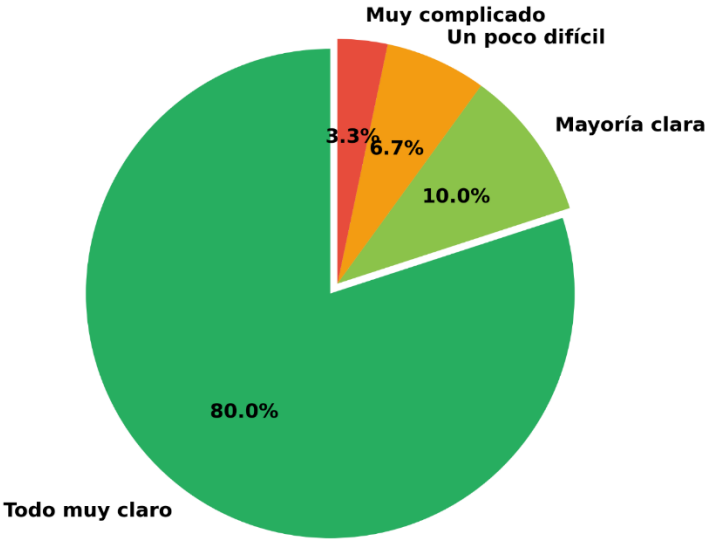

Figura 10. Claridad de la información recibida en los detalles.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Confirma la efectividad del diseño pedagógico y la adecuación del lenguaje."*

5. Impacto en la confianza, autonomía y proyección futura

Más allá de los conocimientos y comportamientos, el proyecto generó un impacto profundo en la dimensión personal de los participantes, reflejado en su autoconfianza y sentido de autonomía.

En relación con la percepción de autonomía y confianza para el uso de internet y la protección de información personal, ocho de cada diez participantes afirmaron sentirse “mucho más seguros y autónomos” tras la capacitación, mientras que un 16,7% adicional señaló sentirse “un poco más seguro”. De modo que el 96,7% de los socios experimentó algún grado de incremento en su empoderamiento digital. Por otra parte, para el 60% de los encuestados la relevancia de la ciberseguridad en su vida cotidiana se tornó “mucho más importante de lo que pensaban” luego de la intervención. Una síntesis de estos hallazgos se presenta en la Figura 11.

El elevado grado de satisfacción con el proyecto quedó reflejado en la disposición a recomendar la experiencia, tal como se ilustra en la Figura 12. Nueve de cada diez participantes manifestaron que “definitivamente” recomendarían este tipo de formación a otras personas con discapacidad visual de su entorno, y el restante 10% respondió “probablemente sí”. Ninguno de los socios se mostró indeciso o en desacuerdo con la recomendación.

Al consultar a los socios sobre los temas que desearían abordar en futuras instancias formativas, el interés manifestado por los socios se orientó hacia la continuidad de su aprendizaje en áreas de aplicación práctica. Los tópicos con mayor aceptación fueron “compras seguras en línea y banca electrónica” y “protección de dispositivos móviles y aplicaciones”, cada uno con el 70% de las preferencias, seguidos por “detección de estafas por teléfono y mensajes de voz” (60%). Esta información se resume gráficamente en la Figura 13. Dichas preferencias sientan las bases para la sostenibilidad del proyecto y el diseño de nuevas fases de capacitación.

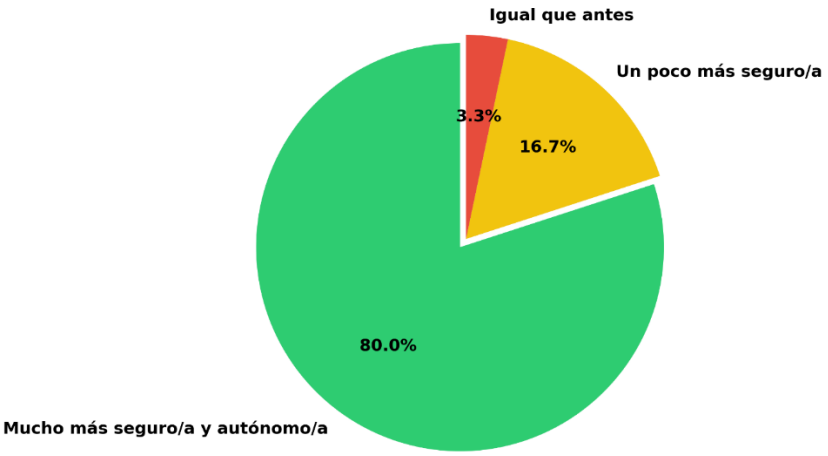

Figura 11. Aumento de la confianza y autonomía digital.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *“Impacto humano más profundo del proyecto.”*

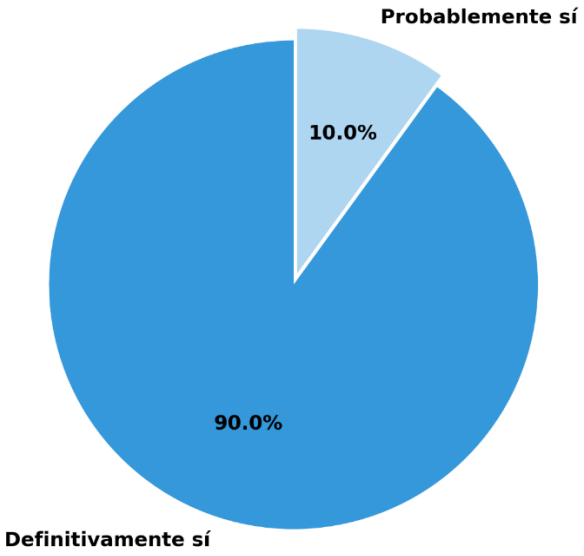

Figura 12. Disposición a recomendar la capacitación.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Muestra la satisfacción general y el valor percibido por los participantes."*

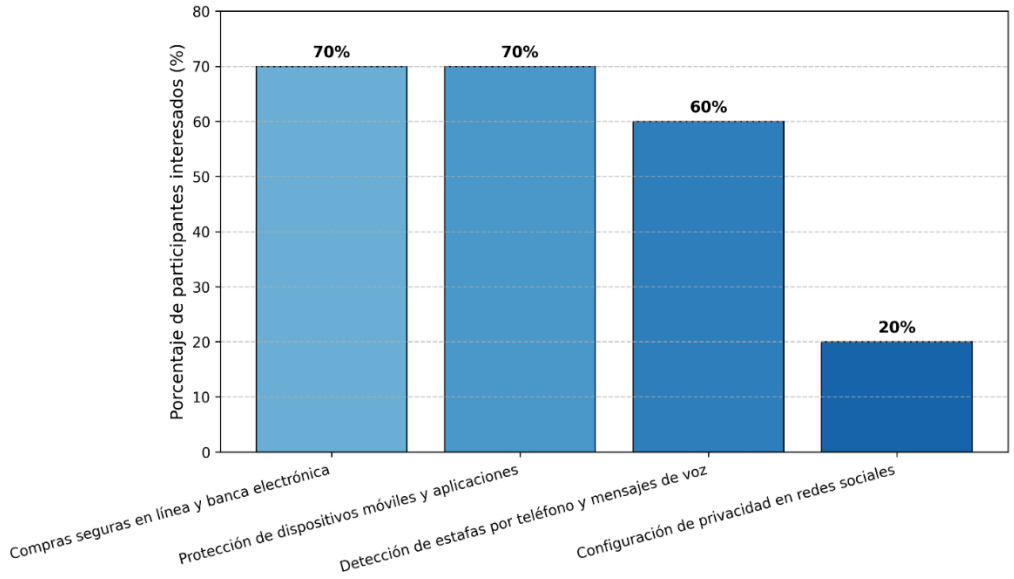

Figura 13. Temas de interés para futuras capacitaciones.

Fuente: Análisis de resultados de la Encuesta final.

Nota: *"Traza la hoja de ruta para la sostenibilidad del proyecto."*

DISCUSIÓN

Los resultados obtenidos en este estudio confirman el impacto positivo y multidimensional de una intervención educativa en ciberseguridad, diseñada específicamente para ser accesible a personas con discapacidad visual (21). El análisis de los datos no solo evidencia una mejora significativa en los conocimientos técnicos de los participantes, sino que también revela una transformación en sus comportamientos digitales y un fortalecimiento de su autoconfianza y autonomía, abordando así la "doble vulnerabilidad" identificada en la literatura (2).

Entre los hallazgos más destacados se encuentra la constatación de que las barreras de accesibilidad representan el principal obstáculo para la inclusión digital de las personas con discapacidad visual. El contraste entre ambos datos es especialmente revelador: mientras que el 80% de los socios de APRODVICH reportó haber enfrentado dificultades previas para acceder a información formativa, tras la intervención el 90% calificó la aplicación como fácil o muy fácil de usar con sus lectores de pantalla. Esta evidencia respalda la necesidad de desarrollar herramientas fundamentadas en estándares como las WCAG 2.1 (6)(21). La alta usabilidad alcanzada no obedece al azar, sino que deriva de una implementación sistemática de técnicas de accesibilidad entre ellas, el uso de HTML semántico, la navegación plenamente operable por teclado y la provisión de alternativas textuales (5,8), lo que permitió que las tecnologías de apoyo cumplieran su función sin interferencias. Este logro contrasta con lo que ocurre en numerosos sitios web educativos y gubernamentales, los cuales, como señalan Acosta-Vargas et al. (7) y Laitano (9), siguen presentando barreras críticas, por ejemplo, contraste insuficiente o ausencia de etiquetas en formularios que perpetúan la exclusión.

La efectividad del modelo pedagógico empleado, centrado en talleres prácticos y guiados, también merece un análisis profundo. La preferencia del 90% de los participantes por este formato, manifestada en el diagnóstico inicial y ratificada en la evaluación final, respalda la idea de que el aprendizaje en adultos, especialmente en temas de seguridad, requiere un enfoque experiencial y contextualizado (5). La posibilidad de interactuar con la aplicación en un entorno controlado y con el acompañamiento de facilitadores permitió a los socios no solo "saber" qué es una contraseña segura (24), sino "saber hacerla" y aplicarla en sus dispositivos, cerrando así la brecha entre el conocimiento declarativo y la aplicación práctica. Este enfoque de "aprender haciendo" resultó clave para que el 80% de los participantes modificara efectivamente sus contraseñas y hábitos de navegación, un cambio conductual que es el fin último de cualquier programa de concienciación en seguridad.

Desde una óptica más amplia, los hallazgos de este proyecto no solo se alinean con los de investigaciones precedentes, sino que los enriquecen. Coincidimos con Feng et al. (3) en que los usuarios con discapacidad visual son conscientes de los riesgos digitales; sin embargo, nuestras conclusiones van un paso más allá al evidenciar que, cuando se ponen a su disposición herramientas adecuadas y una formación pertinente, estas personas no solo logran reducir dichos riesgos, sino que también construyen un sentido de agencia y control sobre su identidad digital. El dato de que el 80% de los participantes haya reportado sentirse “mucho más autónomo” constituye un indicador inequívoco de que se ha logrado empoderar a un colectivo

históricamente dependiente. Por otra parte, nuestros resultados contradicen cualquier idea que atribuya la brecha digital en ciberseguridad a una supuesta desmotivación de este grupo: el 90% de los socios no solo demandó activamente la formación, sino que se involucró plenamente en ella, desvirtuando posibles sesgos acerca de una presunta pasividad de los usuarios con discapacidad.

A pesar de los resultados alentadores, es necesario reconocer las limitaciones del estudio. La principal es el tamaño de la muestra, limitada a 30 participantes de una única asociación en Riobamba. Si bien el carácter censal otorga validez interna a los hallazgos, estos no son generalizables sin precaución a toda la población con discapacidad visual en Ecuador o la región. Las particularidades culturales, socioeconómicas y de acceso a la tecnología de los socios de APRODVICH pueden diferir de las de otras personas con discapacidad visual en contextos rurales o de otras provincias. Otra limitación reside en el uso de cuestionarios auto-administrados de forma oral, los cuales, aunque necesarios por accesibilidad, pueden estar sujetos a sesgos de deseabilidad social. Sin embargo, la consistencia entre las respuestas a preguntas de conocimiento, las de cambio conductual y las observaciones de los facilitadores durante los talleres, refuerza la validez de los datos obtenidos.

Si bien los talleres y las pruebas de usabilidad se desarrollaron en el laboratorio de computación de APRODVICH, un entorno controlado que facilitó la interacción directa con los facilitadores y el acceso a los dispositivos, es necesario reconocer que este escenario puede diferir de las condiciones reales de uso en el hogar, donde los participantes enfrentan distracciones, limitaciones de conectividad y la ausencia de apoyo inmediato. Estudios previos en alfabetización digital para colectivos vulnerables han señalado que la transferencia de competencias desde un entorno supervisado hacia el contexto doméstico constituye un desafío metodológico relevante, pues factores como la motivación sostenida, la disponibilidad de recursos tecnológicos y el apoyo social pueden modular la efectividad a largo plazo de las intervenciones. Por tanto, futuras investigaciones deberían incorporar diseños longitudinales que evalúen la persistencia de los cambios conductuales en el entorno natural de los usuarios, así como el uso de estrategias de seguimiento remoto. En esta línea, se abre un campo prometedor para el desarrollo de módulos avanzados que aborden áreas de alta demanda, como la banca electrónica y las compras seguras en línea, cuya complejidad exige una progresión didáctica cuidadosa. Asimismo, la integración de técnicas de inteligencia artificial para la detección de fraudes en tiempo real, por ejemplo, mediante sistemas de alerta temprana que analicen patrones de mensajes sospechosos, así podría ofrecer una capa adicional de protección autónoma, especialmente diseñada para personas con discapacidad visual. Estas líneas no solo ampliarían el alcance del presente proyecto, sino que contribuirían a consolidar un ecosistema de herramientas inclusivas que trasciendan el ámbito formativo y se integren en la vida cotidiana de este colectivo.

En síntesis, los resultados de esta investigación ofrecen evidencia contundente de que es factible concebir y poner en práctica programas de alfabetización digital inclusivos que resultan efectivos. La intervención no solo contribuyó a fortalecer la seguridad digital de los 30 socios de APRODVICH, sino que dejó como resultado un modelo metodológico y tecnológico que, mediante las adaptaciones pertinentes, puede ser transferido a otras organizaciones que trabajan con

personas con discapacidad visual. El marcado interés expresado por los participantes en profundizar en temáticas como la banca electrónica o la protección de dispositivos traza una línea de trabajo clara para garantizar la sostenibilidad y escalabilidad de esta línea de investigación.

CONCLUSIONES

Los resultados obtenidos confirman que una intervención educativa en ciberseguridad, concebida bajo principios de accesibilidad universal, es capaz de producir mejoras sustanciales y cuantificables tanto en los conocimientos como en las conductas digitales de personas con discapacidad visual. El contraste entre las evaluaciones previas y posteriores a la intervención refleja un cambio notable: el 80% de los participantes que inicialmente declaró carecer de conocimientos en ciberseguridad transitó hacia niveles intermedios (70%) y avanzados (10%) luego del proceso formativo. Paralelamente, el 80% de los socios modificó sus prácticas de seguridad, adoptando contraseñas más robustas e incorporando hábitos de verificación ante posibles fraudes, lo que evidencia que se logró cerrar la distancia entre el saber declarativo y su aplicación efectiva en el contexto cotidiano.

La herramienta digital desarrollada, ajustada a los criterios establecidos en las WCAG 2.1 nivel AA, demostró ser eficaz y plenamente funcional para usuarios que dependen de lectores de pantalla y navegación mediante teclado. Nueve de cada diez participantes calificaron la experiencia de uso como positiva, considerada como fácil o muy fácil, lo que, valida la correcta implementación de técnicas de accesibilidad, entre ellas: el HTML semántico, las alternativas textuales descriptivas y la retroalimentación multimodal. Este logro adquiere mayor relevancia si se contrasta con la situación previa, en la que el 80% de los socios había enfrentado barreras de accesibilidad en otros entornos formativos; confirma, además, que la observación rigurosa de las pautas técnicas constituye un requisito ineludible y no una opción para garantizar la inclusión digital.

La metodología basada en talleres prácticos con guía, que desde el diagnóstico inicial contaba con la preferencia del 90% de los participantes, se consolidó como la más apropiada para el aprendizaje de adultos con discapacidad visual en materia de ciberseguridad. La estrategia de “aprender haciendo”, sumada al acompañamiento cercano de los facilitadores y al uso de la aplicación en un entorno controlado, permitió que los conocimientos se tradujeran en acciones concretas. Más allá de la adquisición de competencias técnicas, el 96,7% de los socios experimentó un incremento en su confianza y autonomía digital, lo que demuestra que el empoderamiento personal constituye un resultado tangible y fundamental en este tipo de intervenciones.

El modelo desarrollado en este proyecto, por su diseño basado en estándares abiertos y su enfoque metodológico validado, posee un alto potencial de replicabilidad y escalabilidad. El interés manifestado por los participantes en continuar su formación en temas como banca electrónica, protección de dispositivos móviles y detección de estafas (con un 70% y 60% de preferencia, respectivamente) traza una hoja de ruta clara para futuras fases. La sistematización de esta experiencia, junto con su comunicación a través de publicaciones científicas, permitirá que otras organizaciones dedicadas a la atención de personas con discapacidad visual tanto en el

ámbito nacional como regional puedan retomar y ajustar esta solución a sus propios contextos, contribuyendo de esta manera a construir una sociedad digital más equitativa e inclusiva.

REFERENCIAS BIBLIOGRÁFICAS

1. Barraga N. Discapacidad visual y aprendizaje. International Council for the Education of the Visually Handicapped; 1992. Disponible en: https://sid.usal.es/idocs/F8/FDO23237/disminuidos_visuales_y_aprendizaje.pdf
2. Ahmed T, Hoyle R, Connelly K, Crandall D, Kapadia A. Privacy Concerns and Behaviors of People with Visual Impairments. En: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (Internet). New York, NY, USA: Association for Computing Machinery; 2015 (citado 9 de marzo de 2026). p. 3523–32. (CHI '15). Disponible en: https://doi.org/10.1145/2702123.2702334
3. Lazar J, Feng J, Brooks T, Melamed G, Wentz B, Holman J, et al. The SoundsRight CAPTCHA: an improved approach to audio human interaction proofs for blind users. En: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2012. p. 2267-76. Disponible en: https://doi.org/10.1145/2207676.2208385
4. Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems, CHI '15, pages 3523-3532, 2015. Disponible en: https://dl.acm.org/doi/10.1145/2702123.2702334
5. Feng Y, Chen R, Ravichander A, Wilson S, Yao Y, Sadeh N. Understanding How to Inform Blind and Low-Vision Users about Data Privacy through Privacy Question Answering Assistants. En: Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23). Anaheim, CA: USENIX Association; 2023. p. 4661-78. Disponible en: https://dl.acm.org/doi/10.5555/3698900.3699016
6. Thoo YJ, Jeanneret Medina M, Froehlich JE, Ruffieux N, Lalanne D. A Large-Scale Mixed-Methods Analysis of Blind and Low-vision Research in ACM and IEEE. En: Proceedings of the 25th International ACM SIGACCESS Conference on Computers and Accessibility (Internet). New York, NY, USA: Association for Computing Machinery; 2023. (ASSETS '23). Disponible en: https://doi.org/10.1145/3597638.3608412
7. Yataco Marín RM. Tiflotecnología y el acceso a la información de las personas con discapacidad visual. Fénix Rev Bibl Nac Perú. 2022;(50):75-88. Disponible en: https://doi.org/10.51433/fenix-bnp.2022.n50.p76-90
8. Kane SK, Jayant C, Wobbrock JO, Ladner RE. Freedom to roam: A study of mobile device adoption and accessibility for people with visual and motor disabilities. En: Proceedings of the 11th international ACM SIGACCESS conference on Computers and accessibility. 2009. p. 115-22. Disponible en: https://doi.org/10.1145/1639642.1639663
9. Acosta-Vargas P, Acosta T, Lujan-Mora S. Framework for accessibility evaluation of hospital Websites. En: 2018 International Conference on eDemocracy eGovernment (ICEDEG). 2018. p. 9-15. Disponible en: DOI: 10.1109/ICEDEG.2018.8372368
10. Bigham JP, Jayant C, Ji H, Little G, Miller A, Miller RC, et al. VizWiz: nearly real-time answers to visual questions. En: Proceedings of the 23nd annual ACM symposium on User interface

software and technology. 2010. p. 333-42. Disponible en: https://doi.org/10.1145/1866029.1866080
11. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.1 (Internet). 2018 (citado 9 de marzo de 2026). Disponible en: https://www.w3.org/TR/WCAG21/
12. Patricia Acosta-Vargas, Belén Salvador-Acosta, Luis Salvador-Ullauri, William Villegas-Ch., and Mario Gonzalez. Accessibility in native mobile applications for users with disabilities: A scoping review. Applied Sciences, 11(12):5707, 2021. Disponible en: https://doi.org/10.3390/app11125707
13. Ali Abdolrahmani and Ravi Kuber. Should I trust it when I cannot see it? credibility assessment for blind web users. In Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility, ASSETS '16, pages 191-199, 2016. Disponible en: https://dl.acm.org/doi/abs/10.1145/2982142.2982173
14. Acosta-Vargas P, Salvador-Ullauri LA, Lujan-Mora S. A Heuristic Method to Evaluate Web Accessibility for Users With Low Vision. IEEE Access. 2019;7:125634-48. Disponible en: DOI: 10.1109/ACCESS.2019.2939068
15. Power C, Freire A, Petrie H, Swallow D. Guidelines are only half of the story: accessibility problems encountered by blind users on the web. En: Proceedings of the SIGCHI conference on human factors in computing systems. 2012. p. 433-42. Disponible en: https://doi.org/10.1145/2207676.2207736
16. García-Mireles G, Maldonado Vásquez AM, Morales-Trujillo ME. EvA-Web: Una herramienta para evaluar la accesibilidad de sitios web. SAHUARUS Rev Electrónica Matemáticas. 2021;5(2):45-57. Disponible en: https://doi.org/10.36788/sah.v5i2.103
17. Azenkot S, Rector K, Ladner R, Wobbrock J. PassChords: secure multi-touch authentication for blind people. En: Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility. 2012. p. 159-66. Disponible en: https://doi.org/10.1145/2384916.2384945
18. Khan S, Nazir S, Khan HU. Analysis of Navigation Assistants for Blind and Visually Impaired People: A Systematic Review. IEEE Access. 2021; 9: 26712 - 34. Disponible en: https://doi.org/10.1109/ACCESS.2021.3052415
19. Instituto Nacional de Estadística y Censos (INEC). Proyecciones de Población y Dificultades Funcionales 2022-2030: Resultados del VIII Censo de Población. Quito, Ecuador; 2024. Disponible en: https://www.ecuadorencifras.gob.ec/proyecciones-poblacionales/
20. Vigo M, Brown J, Conway V. Benchmarking web accessibility evaluation tools: measuring the harm of sole reliance on automated tests. En: Proceedings of the 10th International Cross-Disciplinary Conference on Web Accessibility. 2013. p. 1-10. Disponible en: https://doi.org/10.1145/2461121.2461124
21. Shinohara K, Wobbrock JO. In the shadow of misperception: Assistive technology use and social interactions. En: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011. p. 705-14. Disponible en: https://doi.org/10.1145/1978942.1979044
22. S. Abou-Zahra and M. Cooper. Wcag 2.0 test samplesrepository. In Universal Access in Human-Computer Interaction. Applications and Services, volume 5616 of LNCS, pages 619–

627. 2009. Disponible en: https://link.springer.com/book/10.1007/978-3-642-02713-0?page=4
23. Laitano MI. Accesibilidad web en el espacio universitario público argentino. Rev Esp Doc Cient. 2015;38(1):e079. Disponible en: http://dx.doi.org/10.3989/redc.2015.1.1136
24. Dosono B, Hayes J, Wang Y. "I'm stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. En: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (Internet). Ottawa: USENIX Association; 2015 (citado 10 de marzo de 2026). p. 151–68. Disponible en: https://doi.org/10.1145/3613904.3642233