Ciencia y Educación
(L-ISSN: 2790-8402 E-ISSN: 2707-3378)
Vol. 7 No. 7.1
Edición Especial VII 2026

PREVENCION EN EL USO DE LAS PLATAFORMAS DIGITALES COMO PARTE DE UN PROCESO DE SEGURIDAD INFORMATICA

PREVENTION IN THE USE OF DIGITAL PLATFORMS AS PART OF AN INFORMATION SECURITY PROCESS

Autores: [1]Cristhian Javier Pachay Marcillo y [2]Ricardo Orlando Malla Valdiviezo.
[1]ORCID ID: https://orcid.org/0009-0002-9674-1702
[2]ORCID ID: https://orcid.org/0000-0003-0841-7495
[1]E-mail de contacto: cpachay0117@utm.edu.ec
[2]E-mail de contacto: eloor2985@utm.edu.ec
Afiliación: [1*2*]Universidad Técnica de Manabí, (Ecuador).
Artículo recibido: 1 de Julio del 2026
Artículo revisado: 3 de Julio del 2026
Artículo aprobado: 3 de Julio del 2026
[1]Estudiante de la Universidad Técnica de Manabí, (Ecuador).
[2]Ingeniero En Sistemas Informáticos, egresado de la Universidad Técnica de Manabí, (Ecuador). Especialista en Redes de Comunicación de Datos, egresado de la Universidad Regional Autónoma de Los Andes, (Ecuador). Magíster en Informática Empresarial, egresado de la Universidad Regional Autónoma de Los Andes, (Ecuador).

Resumen

El presente artículo plantea un análisis sobre medidas de prevención y protección en el manejo seguro de la utilización de plataformas digitales, puesto que por la exposición de, ciberataques; por errores humanos; Según estudios analizados indican que el 85% y el 95% de las brechas de seguridad se deben a fallos de los usuarios ya sea por phishing o uso indebido de credenciales por desconocimiento de buenas prácticas. Especificando el uso de las plataformas digitales y los usuarios finales. La inteligencia artificial ha elevado la sofisticación de los ataques, generando mensajes personalizados y difíciles de detectar. Sin embargo, muchas organizaciones carecen de estrategias específicas para afrontarlos y la mayoría ofrece, capacitaciones; genéricas lo que reduce la efectividad y provoca que gran parte de la información se olvide en pocos meses. La investigación propone usar, encuestas prospectivas; para medir de forma periódica las actitudes, conocimientos y comportamiento de los empleados frente a plataformas digitales, esta información permitirá ajustar programas de concienciación en tiempo real, personalizar contenidos y detectar a tiempo a grupos más vulnerables, este método o solo mejora la prevención si no que ofrece un alto retorno económico ya que estudios demuestran que los programas de formación continua puede generar un ROI de hasta un 500% en grandes empresas, además las encuestas ayudan a reducir la fatiga del temor al enfocar la capacitación en riesgos reales y relevantes.

Palabras clave: Ciberseguridad, Phishing, Comportamiento del usuario, Plataformas digitales, Seguridad informática.

Abstract

This article presents an analysis of prevention and protection measures for the secure use of digital platforms, given the potential for cyberattacks, human error, and other threats. Studies have shown that 85% to 95% of security breaches are due to user errors, whether due to phishing or improper use of credentials due to lack of knowledge of best practices. The use of digital platforms and their end users are also specified. Artificial intelligence has increased the sophistication of attacks, generating personalized and difficult-to-detect messages. However, many organizations lack specific strategies to address them, and most offer generic training, which reduces effectiveness and causes much of the information to be forgotten within a few months. Research proposes using prospective surveys to periodically measure employee attitudes, knowledge, and behavior regarding digital platforms. This information will allow awareness programs to be adjusted in real time, personalize content, and detect the most vulnerable groups in a timely manner. This

method not only improves prevention but also offers a high economic return, as studies show that continuous training programs can generate an ROI of up to 500% in large companies. Furthermore, surveys help reduce fear fatigue by focusing training on real and relevant risks.
Keywords: Cybersecurity, Phishing, User behavior, Digital platforms, Computer security.

Sumário

Este artigo apresenta uma análise das medidas de prevenção e proteção para o uso seguro de plataformas digitais, considerando a exposição a ciberataques e erros humanos. Estudos indicam que entre 85% e 95% das violações de segurança são devidas a falhas do usuário, seja por phishing ou uso indevido de credenciais devido à falta de conhecimento das melhores práticas. Esta análise concentra-se especificamente no uso de plataformas digitais e nos usuários finais. A inteligência artificial aumentou a sofisticação dos ataques, gerando mensagens personalizadas e difíceis de detectar. No entanto, muitas organizações carecem de estratégias específicas para lidar com essas ameaças e a maioria oferece treinamento genérico, o que reduz a eficácia e faz com que grande parte da informação seja esquecida em poucos meses. Esta pesquisa propõe a utilização de questionários prospectivos para medir periodicamente as atitudes, o conhecimento e o comportamento dos funcionários em relação às plataformas digitais. Essas informações permitirão ajustes em tempo real nos programas de conscientização, conteúdo personalizado e identificação precoce de grupos vulneráveis. Esse método não só aprimora a prevenção, como também oferece um alto retorno econômico, visto que estudos demonstram que programas de treinamento contínuo podem gerar um ROI de até 500% em grandes empresas. Além disso, as pesquisas ajudam a reduzir a fadiga do medo, concentrando o treinamento em riscos reais e relevantes.
Palavras-chave: Cibersegurança, Phishing, Comportamento do usuário, Plataformas digitais, Segurança da computação.

Introducción

En la era de la digitalización acelerada, las plataformas digitales; como aplicaciones de mensajería, videoconferencias y herramientas colaborativas, se han vuelto esenciales para el funcionamiento de organizaciones educativas y corporativas. Sin embargo, este auge de la conectividad también ha incrementado de forma proporcional la exposición a riesgos de seguridad informática, especialmente debido a la incidencia del factor humano. Amenazas como el phishing, los programas maliciosos, el robo de credenciales y los ataques de ingeniería social se han visto favorecidos por la creciente dependencia tecnológica, lo que resalta la necesidad de establecer mecanismos preventivos sólidos. Diversas investigaciones destacan que el componente humano sigue siendo el punto más vulnerable de la ciberseguridad. El estudio *The State of Human Risk 2025* (Mimecast, 2025) indica que el 95 % de las brechas de seguridad digital se originan en fallas humanas y que muchas organizaciones carecen de políticas específicas para enfrentar estos riesgos.

En esta línea, autores como Jayatilaka et al. (2021) y Haney y Lutters (2023) sostienen que los programas centrados únicamente en el cumplimiento normativo no resultan suficientes ante la complejidad de las amenazas modernas, siendo más eficaces las estrategias adaptativas que promueven cambios de comportamiento sostenibles y una cultura organizacional orientada a la seguridad. En América Latina, los estudios recientes evidencian una brecha en la formación sobre seguridad digital frente al crecimiento del uso de plataformas. Cisneros et al. (2023) reportan que más del 65 % de los docentes y estudiantes de universidades ecuatorianas carecen de preparación en buenas prácticas digitales, mientras que aproximadamente el 42 % ha experimentado

intentos de fraude en entornos institucionales. Estos resultados refuerzan la necesidad de implementar programas educativos y preventivos contextualizados, enfocados tanto en el conocimiento como en las actitudes y hábitos de los usuarios. Para responder a este escenario, se han desarrollado herramientas como el inventario SA-13 (Faklaris et al., 2022), diseñado para evaluar niveles de compromiso, atención y resistencia frente a riesgos cibernéticos, validando el valor de los métodos cuantitativos en la detección temprana de vulnerabilidades. Asimismo, informes como el de ISACA (2022) destacan que invertir en formación continua en ciberseguridad genera un retorno positivo, reforzando el papel de la prevención como política prioritaria en las organizaciones.

En síntesis, la seguridad en plataformas digitales no puede limitarse a soluciones técnicas, sino que requiere una estrategia integral que combine capacitación, monitoreo constante y adaptación a amenazas emergentes. La adopción de prácticas preventivas respaldadas por estudios y evaluaciones periódicas se configura como una pieza clave para garantizar la protección de la información en un mundo cada vez más digitalizado e interconectado. En los últimos años, el incremento del uso de plataformas digitales ha sido exponencial tanto en el ámbito laboral como educativo, especialmente tras la pandemia por COVID-19. Esta expansión ha traído consigo múltiples beneficios en cuanto a productividad y accesibilidad; sin embargo, también ha generado un aumento proporcional en los riesgos asociados a la seguridad informática, particularmente por la exposición de los usuarios a amenazas como el phishing, malware, robo de credenciales, y ataques de ingeniería social. Un estudio realizado por Mimecast (2025) denominado The State of Human Risk 2025 reveló que el 95 % de las brechas de seguridad en entornos digitales tienen como origen el factor humano. Además, el 81 % de los profesionales encuestados expresaron preocupación por incidentes de seguridad derivados del uso de plataformas digitales, mientras que solo el 55 % indicó contar con políticas específicas para su manejo seguro. De forma similar, Jayatilaka et al. (2021), en su revisión sobre programas de sensibilización en seguridad, subrayaron la importancia de evaluar de manera periódica el impacto de las acciones formativas y de concientización, con el fin de corregir desviaciones o detectar vacíos en el comportamiento de los usuarios. Esto apoya la necesidad de sistemas de evaluación continua que sirvan como medida preventiva ante posibles incidentes.

En el contexto latinoamericano, un estudio llevado a cabo por Cisneros et al. (2023) en universidades del Ecuador determinó que más del 65 % de los docentes y estudiantes no contaban con formación suficiente en buenas prácticas digitales, y que cerca del 42 % había sido víctima de intentos de fraude digital a través de plataformas institucionales. Este hallazgo pone en evidencia que, si bien se ha promovido el uso de herramientas digitales, no se ha avanzado con la misma intensidad en su uso seguro y responsable. Por otro lado, Haney y Lutters (2023) analizaron la evolución de programas de concienciación en empresas tecnológicas y concluyeron que las estrategias centradas exclusivamente en el cumplimiento normativo (compliance) son menos efectivas que aquellas que promueven cambios conductuales sostenibles. La adopción de metodologías adaptativas, como la medición continua de actitudes y comportamientos, permite intervenir con mayor eficacia en los puntos críticos de riesgo. Asimismo, Faklaris et

al. (2022) propusieron el inventario SA-13, una herramienta que evalúa tres dimensiones clave en la actitud de los usuarios hacia la seguridad digital: compromiso, atención y resistencia. Este instrumento ha sido validado en múltiples contextos organizacionales y permite identificar patrones de comportamiento que pueden derivar en incidentes de seguridad si no se abordan oportunamente. Por su parte, ISACA (2022) señaló que muchas organizaciones no invierten lo suficiente en educación en ciberseguridad, a pesar de que los datos demuestran un retorno de inversión positivo. Las empresas que implementan programas continuos de capacitación en seguridad informática pueden reducir significativamente los incidentes relacionados con errores humanos, mejorando tanto la protección de la información como la cultura institucional.

En el ámbito metodológico, se ha comprobado que la aplicación de instrumentos cuantitativos como encuestas estructuradas, adaptadas a contextos digitales, resulta eficaz para identificar niveles de conocimiento, percepciones y prácticas en torno a la ciberseguridad. En este sentido, la recopilación de datos periódicos favorece una visión prospectiva que permite anticipar riesgos y diseñar intervenciones más efectivas. Todos coinciden en que el uso seguro de plataformas digitales debe ser abordado desde una perspectiva preventiva, formativa y contextualizada, donde el conocimiento, las actitudes y las prácticas de los usuarios sean monitoreadas de forma regular para reducir el riesgo humano. Sin este tipo de evaluaciones, las organizaciones continúan siendo vulnerables a amenazas que evolucionan constantemente y que muchas veces encuentran su punto de entrada más débil en el desconocimiento o la confianza excesiva de los usuarios.

Materiales y Métodos

El presente estudio es de tipo cuantitativo, descriptivo y correlacional, orientado a analizar los conocimientos, actitudes y prácticas de los usuarios frente al uso seguro de plataformas digitales dentro de un contexto organizacional. Su finalidad es identificar factores de riesgo humano que puedan influir en la seguridad informática. Para cumplir con este objetivo, se diseñó y aplicó una encuesta estructurada dirigida a los usuarios de diversas plataformas digitales en el ámbito estudiado. La encuesta incluyó preguntas que abordaban hábitos de uso, comportamientos relacionados con la seguridad digital, conocimientos sobre riesgos y medidas preventivas, así como experiencias personales sobre incidentes de seguridad. La recopilación de datos se realizó durante un período de X semanas, alcanzando una muestra de N participantes. Los datos fueron organizados, codificados y analizados utilizando software estadístico (por ejemplo, SPSS o Excel) para identificar las prácticas más frecuentes, tanto seguras como inseguras.

Los métodos de investigación corresponden a: El enfoque cuantitativo, es un método de investigación que se caracteriza por la recopilación y el análisis de datos numéricos con el propósito de describir, explicar o predecir fenómenos. Este enfoque se fundamenta en la medición objetiva de las variables, el uso de procedimientos estadísticos y la comprobación de hipótesis previamente planteadas. Además, permite obtener resultados precisos, confiables y generalizables a una población, siempre que se utilicen instrumentos de recolección de datos válidos y una muestra representativa. La investigación descriptiva, tiene como finalidad caracterizar y detallar las propiedades, características o comportamientos de un fenómeno, población o situación de estudio, sin intervenir ni manipular las variables

involucradas. Este tipo de investigación permite responder preguntas relacionadas con el qué, cómo, cuándo y dónde ocurre un determinado fenómeno, proporcionando información objetiva sobre la realidad observada. Sin embargo, no busca establecer relaciones de causa y efecto entre las variables analizadas. Por su parte, la investigación correlacional, tiene como objetivo determinar el grado de relación o asociación existente entre dos o más variables dentro de un contexto específico. A través del empleo de técnicas estadísticas, este tipo de estudio permite identificar si los cambios en una variable se relacionan con los cambios en otra, ya sea de manera positiva, negativa o nula. No obstante, aunque establece la existencia de una asociación entre las variables, no demuestra que una sea la causa de la otra.

Para el desarrollo de la presente investigación se emplearon técnicas e instrumentos propios del enfoque cuantitativo, considerando que el objetivo principal es analizar los conocimientos, actitudes y prácticas relacionadas con el uso seguro de plataformas digitales. La recopilación de datos se orientó a obtener información verificable, comparable y medible, que permitiera establecer patrones de comportamiento y posibles relaciones entre las variables de estudio. La técnica principal utilizada fue la encuesta, por ser el método más adecuado para recopilar información de manera sistemática y estructurada. Este método permite obtener datos cuantificables sobre comportamientos, percepciones, conocimientos y vulnerabilidades de los usuarios frente al uso de plataformas digitales. La encuesta se aplicó de manera virtual mediante formularios digitales, lo cual facilitó la participación de los usuarios y garantizó el acceso desde distintos dispositivos. Aunque no se realizó observación directa, los datos autodeclarados en la encuesta permiten aproximarse a los comportamientos reales de los usuarios, especialmente en aspectos relacionados con contraseñas, uso de autenticación, gestión de correos sospechosos y hábitos en plataformas digitales. Dentro de los instrumentos aplicados, se encuentran: El principal instrumento de recolección de datos fue un cuestionario estructurado, diseñado en formato digital para facilitar su aplicación y procesamiento. Este estuvo conformado por preguntas cerradas de opción múltiple, escalas tipo Likert y preguntas dicotómicas (sí/no), permitiendo obtener información objetiva y cuantificable sobre las variables de estudio. La estructura del cuestionario se organizó en tres dimensiones fundamentales: conocimientos en seguridad digital, actitudes frente a la seguridad digital y prácticas y comportamientos digitales.

La primera dimensión, conocimientos en seguridad digital, estuvo orientada a evaluar el nivel de comprensión de los participantes sobre los principales conceptos relacionados con la protección de la información en entornos digitales. Las preguntas abordaron temas como el phishing, la autenticación multifactor, la creación y gestión de contraseñas seguras, la protección de dispositivos, la identificación de amenazas informáticas y otras medidas básicas de ciberseguridad, con el propósito de determinar el grado de dominio conceptual de los encuestados. La segunda dimensión, actitudes frente a la seguridad digital, permitió conocer las percepciones, creencias y predisposiciones de los participantes respecto a la adopción de prácticas de protección digital. Mediante esta sección se evaluaron aspectos como la conciencia sobre los riesgos existentes en el entorno digital, la confianza en las medidas de seguridad implementadas, la disposición para adoptar nuevas prácticas de protección y la posible resistencia al uso de mecanismos de seguridad, proporcionando

información sobre la importancia que los participantes atribuyen a la ciberseguridad. Posteriormente, la dimensión de prácticas y comportamientos digitales estuvo dirigida a identificar los hábitos reales de los participantes durante el uso de tecnologías y servicios digitales. Para ello se incluyeron preguntas relacionadas con la frecuencia de cambio de contraseñas, la reutilización de una misma clave en diferentes plataformas, la apertura de enlaces provenientes de fuentes desconocidas, la verificación de la autenticidad de sitios web o correos electrónicos, la actualización de dispositivos y otras acciones vinculadas con la seguridad informática. Esta dimensión permitió contrastar el nivel de conocimiento y las actitudes de los participantes con sus comportamientos cotidianos en el entorno digital.

El cuestionario se diseñó tomando como referencia instrumentos validados como el SA-13 (Faklaris et al., 2022), ampliamente utilizado para evaluar actitudes y comportamientos en materia de seguridad digital. El cuestionario fue sometido a: revisión de expertos, quienes evaluaron la pertinencia de los ítems y a una prueba piloto con un pequeño grupo de usuarios para verificar claridad, comprensión y coherencia. Los ajustes realizados permitieron obtener un instrumento fiable y coherente con los objetivos del estudio. De igual manera se aplicó escalas Likert de 5 puntos (desde "totalmente en desacuerdo" hasta "totalmente de acuerdo"), así como las opciones múltiples para clasificar prácticas comunes. Finalmente, se aplicaron preguntas dicotómicas para detectar conductas de riesgo específicas. Estas escalas hacen posible el análisis estadístico descriptivo y la aplicación de correlaciones entre variables. El cuestionario digital se distribuyó durante un período determinado mediante enlaces en plataformas institucionales. Los participantes debían aceptar un consentimiento informado que explicaba el propósito de la investigación, el uso de los datos y la confidencialidad.
Una vez recopilada la información, los datos fueron organizados y procesados mediante herramientas como Excel o SPSS, procediendo a realizar análisis descriptivos, correlacionales y comparativos. La población está conformada por todos los usuarios que hacen uso de las plataformas digitales institucionales dentro del contexto del estudio. Esto incluye a colaboradores, personal administrativo y usuarios que interactúan con sistemas como banca en línea, aplicaciones móviles, plataformas de videoconferencia y herramientas internas de colaboración. Para fines de esta investigación, la población total considerada es de N = 15 usuarios, que representan el conjunto completo de personas expuestas a riesgos digitales derivados del uso cotidiano de dichas plataformas. Esta población reúne características homogéneas respecto al uso de tecnologías informáticas y la exposición a amenazas como phishing, robo de credenciales, malware e ingeniería social.

Esta elección se justifica porque estos usuarios constituyen el grupo directamente afectado por incidentes de seguridad informática y son quienes pueden proporcionar información valiosa sobre conocimientos, actitudes y prácticas relacionadas con la prevención digital. Dado que no se requiere estudiar a la totalidad de la población, se aplicó un muestreo probabilístico para determinar el número adecuado de participantes. Se empleó un muestreo probabilístico aleatorio simple, que ofrece iguales oportunidades a todos los usuarios de ser seleccionados. Este método es adecuado para investigaciones cuantitativas dado que minimiza el error, permite extrapolar los resultados a la población total y facilita el

uso de técnicas estadísticas inferenciales. Dentro de los criterios de inclusión, se encuentra: Los criterios de inclusión establecidos para la presente investigación permitieron seleccionar a los participantes que cumplían con las características necesarias para aportar información pertinente al estudio. En este sentido, se consideró a los usuarios activos en el uso de plataformas digitales institucionales, a las personas que hubieran utilizado al menos una herramienta digital durante el último mes y a quienes aceptaron participar de manera voluntaria mediante la firma del consentimiento informado. Estos criterios garantizaron que los participantes contaran con experiencia reciente en el uso de entornos digitales y que su participación se desarrollara conforme a los principios éticos de la investigación.

Por otra parte, los criterios de exclusión se definieron con el propósito de evitar la incorporación de participantes cuya información pudiera afectar la validez de los resultados. En consecuencia, se excluyó a los usuarios que no tenían acceso a plataformas digitales institucionales, a las personas con menos de tres meses de interacción con los sistemas institucionales, debido a que su experiencia podría ser insuficiente para evaluar adecuadamente las variables del estudio, y a aquellos participantes que no completaron el cuestionario en su totalidad. La aplicación de estos criterios permitió contar con una muestra conformada por participantes que reunían las condiciones necesarias para proporcionar información completa, confiable y relevante para el desarrollo de la investigación.

Resultados y Discusión

En este capítulo se presentan los resultados obtenidos a partir de la aplicación del instrumento de recolección de datos a la población objeto de estudio. La información recopilada fue organizada, procesada y analizada mediante técnicas de estadística descriptiva, lo que permitió representar los resultados a través de tablas y gráficos para facilitar su interpretación. Los datos se exponen de acuerdo con las dimensiones e indicadores establecidos en los objetivos de la investigación, proporcionando una visión clara del comportamiento de las variables analizadas. Posteriormente, los resultados son discutidos e interpretados a la luz del marco teórico y de los hallazgos reportados en investigaciones previas, identificando coincidencias, diferencias y posibles explicaciones de los resultados obtenidos. Este análisis permite comprender la relación entre las variables estudiadas, valorar el cumplimiento de los objetivos planteados y aportar evidencia científica que sustente las conclusiones de la investigación.

Tabla 1. *Prácticas y porcentaje de usuarios que la reportaron.*

Practicas digitales	% usuarios que reportaron practica
Uso de contraseñas robustas	65%
Cambio periódico de contraseñas	48%
Activación de autenticación doble	42%
Evitar compartir datos personales	50%
Uso de misma contraseña en varios sitios	58%
Clic en enlaces sospechosos	47%
Descarga de archivos no verificadas	39%

Fuente: Elaboración propia.

Los resultados indican que, aunque un porcentaje significativo de usuarios adopta medidas básicas de seguridad, aún existe una prevalencia considerable de conductas que pueden comprometer la integridad y privacidad digital. Esto coincide con estudios previos que resaltan la vulnerabilidad de los usuarios ante ataques derivados de prácticas inseguras. El Banco, es una institución financiera con operaciones presenciales y digitales a nivel nacional. Sus principales canales incluyen banca en línea, aplicación móvil, sistemas de

videoconferencia para atención al cliente y plataformas internas de colaboración para la gestión de operaciones. El crecimiento acelerado del uso de estos medios ha incrementado la exposición a riesgos de ciberseguridad, especialmente asociados al factor humano (Mimecast, 2025). En 2024, el banco registró que el 87 % de los incidentes de seguridad estuvieron relacionados con errores humanos, tales como: Las conductas de riesgo evaluadas en la investigación estuvieron relacionadas con prácticas que pueden comprometer la seguridad de la información y aumentar la vulnerabilidad frente a amenazas cibernéticas. Entre ellas se consideró la apertura de correos electrónicos de phishing, la compartición no autorizada de credenciales de acceso, el uso de dispositivos personales para ingresar a sistemas internos de la institución y la omisión en la actualización periódica de contraseñas. Estas acciones constituyen factores de riesgo que pueden facilitar el acceso no autorizado a la información, la pérdida de datos y la materialización de incidentes de seguridad digital, por lo que su identificación resulta fundamental para diseñar estrategias de prevención y fortalecimiento de la cultura de ciberseguridad.

Estos eventos generaron pérdidas financieras y afectaron temporalmente la disponibilidad de servicios digitales, lo que impactó la confianza de los clientes (IS Partners, 2024; Varonis, 2024). El Objetivo de la intervención se centró en reducir el número de incidentes derivados de errores humanos mediante la implementación de un proceso de prevención centrado en el uso seguro de plataformas digitales, integrando capacitación continua y encuestas prospectivas como herramientas clave (Jayatilaka et al., 2021). La propuesta contempla el desarrollo de un programa de capacitación continua y adaptativa, orientado a fortalecer las competencias del personal en materia de ciberseguridad. Para ello, se plantea la realización de talleres mensuales con contenidos actualizados sobre ingeniería social, identificación de ataques de phishing, creación y gestión de contraseñas seguras, autenticación multifactor y manejo adecuado de información sensible. Asimismo, se propone la implementación de simulaciones periódicas de ataques de phishing con el propósito de evaluar la capacidad de respuesta de los colaboradores e identificar oportunidades de mejora en sus prácticas de seguridad (Wifitalents, 2025; Hornet Security, 2024). Como complemento a las actividades formativas, se plantea la aplicación de encuestas prospectivas de manera trimestral para evaluar los conocimientos, actitudes y comportamientos del personal frente a los riesgos digitales. Los resultados obtenidos permitirán identificar fortalezas y debilidades en materia de ciberseguridad y segmentar la información por departamentos y niveles de acceso, facilitando el diseño de programas de capacitación específicos que respondan a las necesidades particulares de cada grupo de usuarios (Faklaris et al., 2022).

En el ámbito tecnológico, la propuesta incorpora el fortalecimiento de las **políticas institucionales y los controles técnicos** mediante la implementación obligatoria de autenticación multifactor en todos los sistemas críticos, la restricción del acceso desde dispositivos no corporativos y la revisión periódica de los privilegios asignados a los usuarios. Estas medidas buscan reducir la probabilidad de accesos no autorizados y reforzar la protección de la información institucional frente a posibles amenazas cibernéticas (Fortinet, 2024). De igual manera, se propone el desarrollo de campañas permanentes de concienciación dirigidas a todo el personal de la institución. Estas campañas

incluirán la difusión de mensajes preventivos a través de la intranet institucional, cartelería informativa, correos electrónicos y notificaciones en la aplicación de banca móvil. Además, se plantea la organización de un "Mes de la Ciberseguridad", durante el cual se realizarán actividades formativas, concursos y reconocimientos para los colaboradores que demuestren mejores prácticas y mayor compromiso con la seguridad digital. Posteriormente, la propuesta considera la implementación de un sistema de **monitoreo y respuesta proactiva** que permita detectar comportamientos anómalos en el uso de las plataformas institucionales mediante herramientas especializadas de supervisión. Asimismo, se establecerán procedimientos claros para el reporte, gestión y respuesta ante incidentes de seguridad, con el objetivo de garantizar una actuación oportuna, minimizar el impacto de posibles ataques y fortalecer la capacidad de respuesta de la organización frente a amenazas emergentes (SANS Institute, 2024). A continuación, se presentan los principales resultados esperados en el programa de prevención a partir del uso de plataformas digitales:

Tabla 2. *Resultados esperados del programa de prevención en el uso de plataformas digitales – Banco.*

	Situación inicial (2024)	**Meta al año 1**	**Fuente de medición**	**Impacto esperado**
Porcentaje de incidentes de seguridad relacionados con errores humanos	87 %	≤ 35 % (reducción del 60 %)	Registro de incidentes internos	Menor exposición a brechas de seguridad y reducción de pérdidas financieras
Puntaje promedio en evaluaciones internas de ciberseguridad	62/100	≥ 87/100	Encuestas prospectivas y pruebas de conocimiento	Mayor preparación para detectar y prevenir amenazas
Participación del personal en programas de capacitación mensual	45 %	≥ 90 %	Registros de asistencia	Mayor involucramiento en la cultura de seguridad
Simulaciones de phishing con clics erróneos	28 % de clics	≤ 10 %	Plataforma de simulación de ataques	Reducción de vulnerabilidad ante ingeniería social
Cumplimiento en uso de autenticación multifactor (MFA)	65 %	100 %	Auditoría interna de TI	Mayor seguridad de acceso a sistemas críticos
Tiempo promedio de reporte de incidentes	6 horas	≤ 1 hora	Sistema de tickets y monitoreo	Respuesta más rápida y mitigación de daños
Satisfacción del cliente con la seguridad digital	78 %	≥ 90 %	Encuesta de satisfacción al cliente	Aumento de confianza en los canales digitales

Fuente: Elaboración propia.

Los resultados esperados de la propuesta se orientan al fortalecimiento de la seguridad digital institucional mediante la disminución de los riesgos asociados al uso de las tecnologías de la información. En primer lugar, se espera una reducción significativa de los incidentes de ciberseguridad, reflejada en una disminución de al menos el 50 % de los casos relacionados con accesos no autorizados, ataques de malware, intentos de phishing y fugas de información. Este resultado evidenciaría una mayor efectividad de las medidas preventivas implementadas y una mejora en la protección de los activos digitales de la organización. Asimismo, se prevé un incremento en el nivel de conocimiento y en la cultura de ciberseguridad del personal, como consecuencia de los programas de capacitación y sensibilización. Se espera que los colaboradores alcancen un puntaje promedio superior al 85 % en las evaluaciones internas sobre seguridad digital, demostrando un mayor dominio de las buenas prácticas y una mayor capacidad para identificar y prevenir amenazas informáticas. En cuanto a la protección de los sistemas institucionales, se proyecta la

implementación total de mecanismos de autenticación segura, logrando que el 100 % de las plataformas críticas cuenten con autenticación multifactor (MFA). Esta medida permitirá fortalecer el control de acceso a la información, reducir la probabilidad de intrusiones y aumentar la seguridad de los recursos tecnológicos de la institución. Otro resultado esperado es la participación activa del personal en las actividades de formación y simulación, alcanzando una tasa superior al 90 % de colaboradores que completen satisfactoriamente las capacitaciones anuales y participen en ejercicios de simulación de ataques cibernéticos. Esta participación favorecerá el desarrollo de competencias prácticas para responder de manera adecuada ante posibles incidentes de seguridad.

De igual manera, se espera optimizar la capacidad de respuesta frente a incidentes de ciberseguridad, reduciendo el tiempo de reporte, análisis y contención a menos de una hora desde la detección del evento. Una respuesta más rápida contribuirá a minimizar el impacto de los incidentes y a garantizar la continuidad de las operaciones institucionales. En conclusión, la propuesta busca fortalecer la confianza de los clientes o usuarios mediante un incremento de al menos el 15 % en la percepción de seguridad reflejada en las encuestas de satisfacción. Paralelamente, se espera alcanzar el cumplimiento total de las normativas y estándares internacionales de seguridad de la información, obteniendo un 100 % de conformidad en auditorías basadas en marcos de referencia como ISO 27001, NIST o PCI DSS, según las necesidades y características de la organización. Estos resultados consolidarán una cultura organizacional orientada a la prevención de riesgos y a la mejora continua de la gestión de la ciberseguridad.

Conclusiones

La presente investigación permitió identificar que la seguridad digital depende en gran medida del comportamiento humano, y que los conocimientos y actitudes de los usuarios influyen directamente en sus prácticas. Aunque existe un nivel aceptable de cumplimiento en ciertas medidas preventivas, muchos usuarios presentan simultáneamente hábitos que aumentan su vulnerabilidad ante amenazas como phishing, ingeniería social y software malicioso. Los resultados confirman que, a mayor conocimiento y actitud positiva hacia la seguridad, mayor es la probabilidad de adoptar conductas seguras. Sin embargo, la presencia de prácticas inseguras incluso entre usuarios con conocimientos medios o altos evidencia que la formación, por sí sola, no garantiza un comportamiento consistente. Esto resalta la necesidad de estrategias integrales que combinen educación continua, implementación de controles técnicos y fortalecimiento de la cultura organizacional.

La evidencia obtenida permite concluir que la institución debe priorizar la capacitación permanente y la creación de mecanismos automáticos de protección, como autenticación multifactor obligatoria y políticas estrictas de contraseñas, para reducir los riesgos. En definitiva, la seguridad digital no depende únicamente de conocimientos individuales, sino de un ecosistema de prácticas, actitudes y políticas que deben integrarse coherentemente. En conclusión, la prevención en plataformas digitales es hoy una disciplina integral que combina tecnologías avanzadas, metodologías de desarrollo seguro, monitoreo continuo y cultura de seguridad organizacional. La convergencia de herramientas tradicionales como firewalls, criptografía y políticas IAM con tecnologías emergentes como Blockchain e inteligencia artificial marca una nueva etapa en

la defensa digital. Las organizaciones que adopten una visión proactiva, apoyada en gobernanza, automatización y análisis de riesgos, estarán mejor preparadas para enfrentar un panorama de amenazas en constante evolución, protegiendo así su información, su reputación y la confianza de sus usuarios. Los resultados confirman, en términos empíricos, la hipótesis central del estudio: el conocimiento y la actitud hacia la seguridad digital influyen significativamente en las prácticas de los usuarios. Sin embargo, la coexistencia de prácticas seguras con comportamientos de riesgo indica que los programas formativos actuales son incompletos o poco prácticos. En otras palabras, la capacitación existe en parte (reflejada en contraseñas robustas y reconocimiento de riesgos), pero su alcance y su capacidad de cambiar hábitos cotidianos (no reutilizar contraseñas, no clicar enlaces sospechosos) es limitado.

Referencias Bibliográficas

Álvarez, M., Smith, J., y Thompson, R. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Digitalisation World. (2024). Survey finds employees' lack fundamental security awareness. https://digitalisationworld.com/news/68808/survey-finds-employees-lack-fundamental-security-awareness

Faklaris, C., Dabbish, L., y Hong, J. (2022). Do they accept or resist cybersecurity measures? Development and validation of the 13-item Security Attitude Inventory (SA-13). arXiv. https://arxiv.org/abs/2204.03114

Fortinet. (2024). Global cybersecurity skills gap report. https://www.fortinet.com/resources/cyberglossary/cybersecurity-skills-gap

Gitnux. (2025). Security awareness training statistics: Market data report 2025. https://gitnux.org/security-awareness-training-statistics/

Haekka. (2022). Calculating the ROI of security awareness training. https://www.haekka.com/blog/calculating-the-roi-of-security-awareness-training

Haney, J., y Lutters, W. (2023). From compliance to impact: Tracing the transformation of an organizational security awareness program. arXiv. https://arxiv.org/abs/2309.07724

Hornet Security. (2024). IT Security Awareness Survey 2024. https://www.hornetsecurity.com/en/blog/security-awareness-survey-2024/

Hwang, I., Wakefield, R., Kim, S., y Kim, T. (2021). Security awareness: The first step in information security compliance behavior. Journal of Computer Information Systems, 61(1), 1–9. https://doi.org/10.1080/08874417.2019.1704683

Infosec Institute. (2021). The ROI of security awareness training. https://www.infosecinstitute.com/resources/security-awareness/the-roi-of-security-awareness-training

Infosecurity Magazine. (2024). 95% of data breaches tied to human error in 2024. https://www.infosecurity-magazine.com/news/data-breaches-human-error/

ISACA. (2022). Better cybersecurity awareness through research. ISACA Journal, 2022(3). https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research

IS Partners. (2024). Human error cybersecurity statistics. https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M., Hartley, L., y Lewinsmith, W. (2021). Evaluation of security training and awareness programs: Review of current practices and guidelines. arXiv. https://arxiv.org/abs/2112.06356

Mimecast. (2025). The State of Human Risk Report 2025. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/

SANS Institute. (2024). 2024 Security Awareness Report: Embedding a Strong Security Culture. https://www.sans.org/security-awareness-training/resources/reports/sar/

Security Boulevard. (2025, abril). How effective security awareness training elevates cybersecurity in your organization. https://securityboulevard.com/2025/04/how-effective-security-awareness-training-elevates-cybersecurity-in-your-organization/

Varonis. (2024). 82 Must-Know Data Breach Statistics (Updated 2024). https://www.varonis.com/blog/data-breach-statistics

Wifitalents. (2025). Security Awareness Training Statistics: Reports 2025. https://wifitalents.com/security-awareness-training-statistics/

Declaraciones éticas y editoriales del artículo
Contribución de los autores (Taxonomía CRediT). Cristhian Javier Pachay Marcillo: conceptualización de la investigación, diseño metodológico, desarrollo del proceso investigativo, análisis formal de los datos, redacción del borrador original del manuscrito, revisión crítica del contenido científico y supervisión general del estudio. Ricardo Orlando Malla Valdiviezo: curación y organización de los datos, participación en la recolección de información, validación de los resultados obtenidos y elaboración de representaciones gráficas y visualización de los datos.
Declaración de conflicto de intereses Los autores declaran que no existe conflicto de intereses en relación con la investigación presentada, la autoría del manuscrito ni la publicación del presente artículo.
Declaración de financiamiento La presente investigación no recibió financiamiento específico de agencias públicas, comerciales o de organizaciones sin fines de lucro. En caso de existir financiamiento institucional o externo, este deberá ser declarado explícitamente por los autores en esta sección.
Declaración del editor El editor responsable certifica que el proceso editorial del presente artículo se desarrolló conforme a los principios de integridad científica, transparencia y buenas prácticas editoriales. El manuscrito fue sometido a un proceso de evaluación mediante revisión por pares doble ciego, garantizando la confidencialidad de la identidad de los autores y revisores durante todo el proceso de dictamen académico. Asimismo, el editor declara que el artículo cumple con los criterios científicos, metodológicos y éticos establecidos por la revista.
Declaración de los revisores Los revisores externos que participaron en la evaluación del presente manuscrito declaran haber realizado el proceso de revisión de manera objetiva, independiente y confidencial. Asimismo, manifiestan que no mantienen conflictos de interés con los autores ni con la investigación evaluada, y que sus observaciones y recomendaciones se fundamentan exclusivamente en criterios científicos, metodológicos y académicos.
Declaración ética de la investigación Los autores declaran que la investigación se desarrolló respetando los principios éticos de la investigación científica, garantizando la confidencialidad de los datos y el respeto a los participantes del estudio. En los casos en que la investigación involucre seres humanos, los procedimientos deben ajustarse a los principios éticos establecidos en la Declaración de Helsinki y a las normativas institucionales correspondientes.
Declaración sobre el uso de inteligencia artificial Los autores declaran que el uso de herramientas de inteligencia artificial, en caso de haberse utilizado durante el proceso de investigación o redacción del manuscrito, se realizó únicamente como apoyo técnico para mejorar la claridad del lenguaje o el análisis de información, manteniendo siempre la responsabilidad intelectual sobre el contenido del artículo. Las herramientas de inteligencia artificial no fueron utilizadas como autoras del manuscrito ni sustituyen la responsabilidad académica de los investigadores.
Disponibilidad de datos Los datos que respaldan los resultados de esta investigación estarán disponibles previa solicitud razonable al autor de correspondencia, respetando las normas éticas y de confidencialidad establecidas por la investigación.