“CIBERSEGURIDAD Y EL USO DE DISPOSITIVOS ELECTRÓNICOS EN ESTUDIANTES DE EDUCACIÓN SUPERIOR. CASO DE ESTUDIO”

“CYBERSECURITY AND THE USE OF ELECTRONIC DEVICES AMONG HIGHER EDUCATION STUDENTS. CASE STUDY”

Clara Guadalupe Pozo Hernández[1]; Raúl Saed Reascos Pinchao[2]; Rocío Alexandra Menodoza Villamar[3]

Universidad Laica Eloy Alfaro de Manabí[1,2,3]

clara.pozo@uleam.edu.ec[1]; raul.reascos@uleam.edu.ec[2]; rocio.menodoza@uleam.edu.ec[3]

Clara Guadalupe Pozo Hernández código Orcid1 https://orcid.org/0000-0001-6186-1099

Raúl Saed Reascos Pinchao código Orcid 2 https://orcid.org/0000-0002-7903-4312

Rocío Alexandra Menodoza Villamar código Orcid 3 https://orcid.org/0000-0002-1277-7162

Recibido: 10 de noviembre de 2025 / Aprobado: 29 de diciembre de 2025

RESUMEN

Los dispositivos móviles, como smartphones, tables y laptops, son herramientas fundamentales para los estudiantes universitarios, tanto para la comunicación como para el desarrollo de sus actividades académicas. Sin embargo, su uso masivo involucra riesgos significativos en ciberseguridad. Este estudio tuvo como objetivo identificar y evaluar los riesgos cibernéticos en los dispositivos de los estudiantes de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión El Carmen, aplicando una encuesta estructurada a 317 estudiantes obtenidos a partir de una población de 1,785. Los resultados más relevantes corresponden a vulnerabilidades detectadas en los dispositivos móviles de los estudiantes principalmente por sus comportamientos al momento de utilizar sus dispositivos, así se obtuvo que un 80% acepta solicitudes de amistad de desconocidos, exponiéndose a perfiles falsos; el 75% abre correos de origen desconocido, aumentando el riesgo de phishing; y el 75% comparte información personal en redes sociales, facilitando el mal uso de sus datos. Por otro lado, se identificaron buenas prácticas: el 85% descarga aplicaciones solo de fuentes confiables, el 82% considera que sus contraseñas son seguras y el 78% evita otorgar permisos innecesarios a las apps. Estos

hallazgos evidencian la necesidad de reforzar la educación en ciberseguridad, promoviendo prácticas seguras para proteger la información personal y reducir la exposición a amenazas digitales. La implementación de programas de formación y campañas de sensibilización podría mejorar significativamente la seguridad digital en la comunidad universitaria.

PALABRAS CLAVES: ciberseguridad, amenaza, vulnerabilidad, seguridad informática

ABSTRACT

Mobile devices, such as smartphones, tablets, and laptops, are essential tools for university students, both for communication and for developing their academic activities. However, their widespread use entails significant cybersecurity risks. This study aimed to identify and assess cyber risks on the devices of students at the Universidad Laica Eloy Alfaro de Manabí (ULEAM), El Carmen Extension, by administering a structured survey to 317 students drawn from a population of 1,785. The most relevant findings relate to vulnerabilities detected in students' mobile devices, primarily due to their behavior when using their devices. It was found that 80% accept friend requests from strangers, exposing themselves to fake profiles; 75% open emails from unknown sources, increasing the risk of phishing; and 75% share personal information on social media, facilitating the misuse of their data. On the other hand, good practices were identified: 85% download apps only from trusted sources, 82% consider their passwords to be secure, and 78% avoid granting unnecessary permissions to apps. These findings highlight the need to strengthen cybersecurity education, promoting safe practices to protect personal information and reduce exposure to digital threats. The implementation of training programs and awareness campaigns could significantly improve digital security in the university community.

KEYWORDS: Cybersecurity, threat, vulnerability, computer security

INTRODUCCIÓN

La adopción masiva de dispositivos móviles (smartphones, tablets y laptops) en la educación superior ha redefinido los procesos de enseñanza-aprendizaje durante la última década. Estos dispositivos no solo facilitan el acceso a recursos educativos y plataformas digitales, sino que se han convertido en herramientas esenciales para la comunicación académica, la colaboración y la gestión de información (Hwang & Tsai, 2011). No obstante, esta dependencia tecnológica expone a los estudiantes a un entorno digital crecientemente complejo, donde la protección de datos personales y académicos emerge como un desafío urgente.

Las ciber amenazas ponen en evidencia las vulnerabilidades en el sector educativo, expuestas cada vez más a phishing, rasonware, robo de identidad (Sánchez et al., 2020). Investigaciones recientes revelan que los estudiantes universitarios usan con mucha frecuencia redes públicas y utilizan de forma prolongada aplicaciones, convirtiéndolos en blancos fáciles de ataques (Livingstone et al., 2021). Además, la situación se agrava cuando existe baja formación en ciberseguridad, haciendo que riesgos como exposición de datos sensibles o descarga de códigos maliciosa a los dispositivos sean más frecuentes

Considerando esta problemática, el presente estudio busca evaluar los riesgos de ciberseguridad derivados al uso de dispositivos móviles por los estudiantes de la ULEAM-Extensión El Carmen, con la finalidad de obtener evidencia de las vulnerabilidades y posibles riesgos a los cuales están expuestos. Para ello se analizan los comportamientos en el uso de dispositivos al momento de interactuar en redes sociales, intercambiar información a través de correos electrónicos, descargar y utilizar aplicaciones, considerando que es en estos espacios donde se concentran amenazas como el secuestro de cuentas, filtración de datos, malware. También se evalúan comportamientos seguros adoptados por los usuarios como configuración de seguridad, métodos de bloqueo y conocimientos generales sobre ciberseguridad. Finalmente, con base a los hallazgos, se proponen medidas para mitigar los efectos negativos de posibles riesgos y estrategias que en el caso de una institución educativa se podrían adoptar para formar en sus estudiantes una culturad protección de su información y datos sensibles.

La relevancia de esta investigación radica en su enfoque preventivo: al identificar y abordar los comportamientos de riesgo desde una perspectiva práctica, se espera reducir incidentes como el robo de identidad o el malware, que afectan tanto a individuos como a las instituciones. Esto cobra especial urgencia en un escenario donde el 74% de los ciberataques se vinculan a errores

humanos (Verizon Business, 2023), lo que convierte a la educación en ciberseguridad en una competencia transversal indispensable para la era digital.

Marco Teórico de la Investigación

Ciberseguridad y Seguridad Informática

La ciberseguridad es un área de la seguridad informática que abarca los mecanismos encaminados a proteger la información que se genera, procesa, transmite y almacena utilizando dispositivos electrónicos, de riesgos y amenazas como malware, pishing, ransomware, entre otros digitales (Stallings & Brown, 2018). En la actualidad a crecido su importancia especialmente en entornos educativos, donde los estudiantes manejan información sensible académica principalmente en sus dispositivos móviles. Según el NIST (2021), combinar tecnología de protección, aplicación de políticas de seguridad claras y capacitación continua es esencial para disminuir los efectos negativos de riesgos de seguridad informática. La falta de conocimientos en ciberseguridad aumenta la exposición a posibles fraudes, secuestro de identidad, pérdida de datos. En el entorno móvil la ciberseguridad implica salvaguardar información personal, credenciales académicas y datos sensibles almacenados en los dispositivos (ISO/IEC 27001, 2022).

La ciberseguridad implica la aplicación de buenas prácticas que incluye entre otras el uso de contraseñas seguras, autenticación multifactor y la descarga de aplicaciones de sitios oficiales. La adopción de marcos de seguridad como el proporcionado por ISO 27001 proporcionan un manejo adecuado de la información de forma segura, garantizando protección tanto a usuarios como infraestructura.

Dispositivos Móviles en el Ámbito Universitario

Los dispositivos móviles, como smartphones, tablets y laptops, se han convertido en herramientas indispensables para la vida académica, facilitando el acceso a plataformas educativas, bibliotecas virtuales y comunicación entre estudiantes y docentes. Su portabilidad

y conectividad permiten el aprendizaje ubicuo, rompiendo barreras geográficas y temporales en la educación superior (García-Peñalvo et al., 2020). Sin embargo, esta dependencia tecnológica también los convierte en blancos frecuentes de ciberataques, especialmente cuando se utilizan redes Wi-Fi públicas sin protección (ENISA, 2023). Además, el uso de aplicaciones no verificadas para fines académicos incrementa el riesgo de infecciones por malware, comprometiendo datos personales e institucionales.

El uso de dispositivos móviles actualmente es imprescindible en el proceso de enseñanza-aprendizaje para la aplicación de metodologías innovadoras, que facilitan el trabajo colaborativo. Sin embargo, la falta de conocimiento sobre ciberseguridad por parte de estudiantes general vulnerabilidades críticas como el phishing y el robo de credenciales (Symantec, 2023). Otros estudios revelan que cerca del 70% de estudiantes no cifran la información sensible que almacenan en sus dispositivos exponiéndose a filtraciones de datos (NIST, 2021). Por estas razones las universidades deben integrar planes de capacitación en sus planes educativos, que combinen tecnología, normativas y concienciación para un uso responsable.

Vulnerabilidades en Dispositivos Móviles

Vulnerabilidad es una debilidad que presenta un sistema ante posibles amenazas, el uso constante y fácil de dispositivos móviles incrementa también su nivel de exposición a riesgos. ENISA (2023), en su informe Threat Lanscape 2023, resalta que la forma más efectiva de mantener dispositivos móviles protegidos es mediante la actualización continua de sus sistemas operativos, de esta forma disminuye la vulnerabilidad y exposición riesgos como malware, ransomware, acceso no autorizado, también recomienda configurar actualización automática como estrategia de seguridad móvil.

En 2023, Kaspersky dio a conocer que aproximadamente el 23% de aplicaciones que se pueden descargar de sitios no oficiales contienen algún tipo de Código malicioso, con su consecuente peligro para los dispositivos móviles. Por otro lado, el mismo informe indica que las aplicaciones legítimas suelen solicitar al Usuario conceder muchos permisos para acceder a funcionalidades de las mismas, otra forma de exposición peligrosa (Kaspersky, 2023).

OWASP Mobile Top 10 (2023) revela que los principales riesgos son el almacenamiento inseguro de datos y la falta de cifrado en comunicaciones. Del informe publicado por Internet Safety Labs, se obtiene que el 78% de aplicaciones educativas compartieron información personal de estudiantes con terceros principalmente con empresas de publicidad y análisis de datos, observándose así la vulnerabilidad de las plataformas educativas (Internet Safety Labs, 2024).

Otro factor a considerar en ciberseguridad es la conexión a redes. El reporte del NIST (2021) expone que un 40% de usuarios en contextos universitarios utilizan por lo general redes Wi-Fi públicas, exponiendo sus dispositivos a ataques como man-in-the middle. Técnicas como redes falsas y el sniffing de paquetes son especialmente efectivas en entornos académicos (He et al., 2020). Estas debilidades sumadas a la falta de configuración de seguridad aumentan la posibilidad de riesgos.

Principales Amenazas a Dispositivos Móviles

Siendo los dispositivos móviles un medio de comunicación masiva y continua, están por lo tanto expuestos a diversas amenazas y peligros, algunos de los más comunes son:

Malware Móvil: Programa malicioso creado con intención de dañar dispositivos móviles, su objetivo es infiltrase, dañar o controlar estos dispositivos, poniendo en riesgo su privacidad, funcionamiento y seguridad de la información almacenada (Gómez & Hernández, 2024, p. 102)

***Phishing/Smishing*:** Técnica que utiliza mensajes de texto (SMS) para engañar a sus víctimas, con el objetivo de obtener información personal o instalar software malicioso en sus dispositivos, Phishing por su parte es una técnica de ingeniería social que a través de la comunicación electrónica engaña a los usuarios para que revelen información sensible (Martínez Santander, Cruz Gavilanes, Cruz Gavilanes & Álvarez Lozano, 2017, p. 120).

***Aplicaciones Maliciosas*:** Son programas o software creados con la finalidad de oacionar daño a un Sistema o dispositivo, mediante la infiltración no autorizada comprometiendo la seguridad del mismo. Estas aplicaciones conocidas como malware pueden incluir virus, gusanos, troyanos, entre otros (Barrera & Salazar, 2024, p. 58).

***Pérdida o Robo Físico*:** Se refiere a la pérdida, sustracción no autorizada de dispositivos que contienen información relevante para una organización o usuario, incluye computadoras, discos, servidores, memorias, cuya seguridad es fundamental para garantizar la seguridad digital y su pérdida puede comprometer la confidencialidad, disponibilidad e integridad de la información (ENISA, 2020).

Explotación de Permisos: Es el uso indebido de permisos otorgados sea a usuarios o aplicaciones que gracias a exceso de privilegios tengan permiso para realizar acciones dañinas a un dispositivo o aplicación, esto pude deberse al otorgar permisos excesivos, o malas configuraciones de seguridad que dejan vulnerable el dispositivo ante posibles atacantes (Rivera & González, 2023, p. 75).

***Ingeniería Social*:** Hadnagy (2021) define la ingeniería social como "el arte de manipular a las personas para que divulguen información confidencial o realicen acciones que comprometan la seguridad de los sistemas" (p. 37)

METODOLOGÍA

La presente investigación tiene enfoque cuantitativo, se basa en análisis estadístico de los datos obtenidos e una encuesta estructurada realizada a estudiantes universitarios con la finalidad de evaluar prácticas de seguridad al utilizar sus dispositivos móviles, que pueden estar asociadas a riesgos de ciberseguridad.

Para el diseño metodológico se consideró medir variables asociadas al comportamiento de los usuarios en relación al uso de sus dispositivos móviles, tales como, métodos de Bloque, configuración de seguridad, conocimiento sobre fundamentos de ciberseguridad, manejo de redes sociales, acceso de redes públicas, instalación de nuevas aplicaciones. Se emplearon técnicas estadísticas para medir la frecuencia y encontrar patrones sean estos de seguridad o riesgo. El enfoque cuantitativo permite cuantificar la magnitud de vulnerabilidades de los dispositivos en función de los controles implementados por los usuarios.

Diseño De la Investigación

La investigación ha sido realizada empleando un diseño no experimental, y transversal ya que se aplicó una encuesta para conocer en un momento determinada las prácticas de seguridad

digital de estudiantes universitarios en el uso de dispositivos móviles.

Diseño Instrumental:

El instrumento utilizado fue un cuestionario estructurado conformado por 26 preguntas cerradas de escala dicotómica (Si/No) y preguntas de opción múltiple. El instrumento abordó cuatro ejes asociados a comportamientos de estudiantes al utilizar sus dispositivos, estos fueron: protección física, controles de acceso, configuraciones de seguridad, manejo de credenciales y uso de redes sociales. La finalidad del instrumento fue diagnosticar las vulnerabilidades y posibles riesgos para proporcionando una base cuantitativa sólida para el desarrollo de intervenciones educativas focalizadas.

Unidad de Análisis

El estudio se aplicó a los estudiantes de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, según datos proporcionados por la secretaría General 1875, como se muestra en la Tabla 1.

Tamaño de la muestra

Para determinar el tamaño de muestra representativo de la población estudiantil (N=1,875) en la investigación sobre prácticas de ciberseguridad móvil, se aplicó la fórmula para poblaciones finitas con proporciones conocidas, dado que se trabajó con variables categóricas (prácticas de seguridad: Sí/No). El cálculo se realizó bajo los siguientes parámetros:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2 \cdot (N-1) + Z^2 \cdot p \cdot q}$$

Donde:

n: Tamaño de la muestra (**317**).

N: Población total (**1,875** estudiantes).

Z: Valor Z de la distribución normal para un **95% de confianza** (**1.96**).

p: Proporción esperada de la variable crítica (conservadora: **0.5**, máxima variabilidad).

q: 1−p1−*p* (**0.5**).

e: Margen de error aceptado (**5%** o **0.05**).

Se aplicó muestreo estratificado proporcional por carrera, garantizando representatividad (n=317; error 5%, confianza 95%).

Tabla 1

Distribución de la muestra por carreras de la ULEAM- Extensión El Carmen

CARRERAS	frecuencia	Porcentaje	Porcentaje Acumulado
ADMINISTRACIÓN DE EMPRESAS	18	5,68	5,68
AGRONEGOCIOS	15	4,73	10,41
AGROPECUARIA	80	25,24	35,65
AUDITORÍA Y CONTROL DE GESTIÓN	11	3,47	39,12
CONTABILIDAD Y AUDITORÍA	19	5,99	45,11
EDUCACIÓN BÁSICA	60	18,93	64,04
EDUCACIÓN INICIAL	21	6,62	70,66
ENFERMERÍA	19	5,99	76,66
FINANZAS	17	5,36	82,02
PSICOLOGÍA EDUCATIVA	12	3,79	85,80
SOFTWARE	15	4,73	90,54
TECNOLOGIAS DE LA INFORMACIÓN	30	9,46	100,00
TOTAL	317	100	

Nota: Datos proporcionados por secretaría General extensión El Carmen

Técnica de recolección de datos

La recolección de datos se realizó mediante encuestas físicas (cuestionarios impresos) aplicadas directamente a los estudiantes de la ULEAM, Extensión El Carmen una vez recibida la aprobación de los coordinadores de carrera. El proceso fue ejecutado por 25 estudiantes de la carrera de Tecnologías de la Información, quienes recibieron capacitación previa para garantizar estandarización en la aplicación. La información de las fichas fue registrada en un archivo de Excel compartido y validado por los docentes responsables del proceso.

Se logró una muestra válida de 317 encuestas con datos completos, representativos de la población objetivo. La participación de estudiantes de Tecnologías de la Información como encuestadores aseguró precisión técnica en la explicación de términos relacionados con ciberseguridad

RESULTADOS

Los resultados obtenidos en el presente estudio corresponden a comportamientos de seguridad practicados estudiantes universitarios al momento de utilizar sus dispositivos móviles, tales como métodos de bloqueo, configuraciones de seguridad y principales comportamientos de riesgo.

Tabla 2

Métodos de Bloqueo de Pantalla

Método de Bloqueo	Sí	No	% Sí
Algún método de bloqueo	336	43	88.7%
Contraseña	102	277	26.9%
PIN	148	231	39.0%
Huella	227	152	59.9%
Reconocimiento facial	114	265	30.1%
Patrón	108	271	28.5%

La Tabla 2, muestra los resultados obtenidos en relación a métodos de bloqueo utilizados por los estudiantes, estos datos revelan que mientras el 88.7% de los estudiantes utiliza algún método de bloqueo, existe una marcada preferencia por métodos biométricos (huella digital 59.9%, reconocimiento facial 30.1%) sobre opciones más seguras como contraseñas (26.9%) o PIN (39.0%). Este comportamiento en la población ULEAM-Extensión El Carmen se debe a que los estudiantes, frecuentemente acceden a sus dispositivos entre clases, prefieren métodos rápidos como la huella digital. Además, que existe la creencia errónea de que la biometría es inviolable, cuando en realidad dispositivos de gama media - comunes en esta población - son vulnerables a spoofing básico. Mientras solo el 28.5% usa patrones, método que balancea seguridad y conveniencia, pero requiere entrenamiento.

Otro aspecto importante al momento de mantener los dispositivos seguros, son las configuraciones de seguridad, la Tabla 3 presenta las principales acciones tomadas por los estudiantes en esta área.

Tabla 3

Configuraciones de Seguridad

Práctica	Sí	No	% Sí
Antivirus instalado	174	205	45.9%
Sistema operativo actualizado	334	45	88.1%
Conexión a WiFi públicas	132	247	34.8%
Otorga permisos innecesarios a apps	83	296	21.9%
Descarga apps de fuentes confiables	323	56	85.2%
Realiza copias de seguridad	266	113	70.2%
Desactiva redes inalámbricas cuando no las usa	242	137	63.9%
Verificación en dos pasos	197	182	52.0%
Cifrado de datos	198	181	52.2%
Borrado remoto activado	105	274	27.7%

Los resultados revelan un patrón de comportamiento de seguridad dual entre los estudiantes universitarios analizados, donde coexisten prácticas responsables con vulnerabilidades críticas. El 88.1% mantiene su sistema operativo actualizado y el 85.2% descarga aplicaciones de fuentes confiables, indicando efectividad de las actualizaciones automáticas en dispositivos modernos, conciencia básica sobre seguridad en descargas y posible influencia de advertencias institucionales sobre software pirata. Solo 45.9% usa antivirus, porcentaje preocupante considerando que el 34.8% se conecta a WiFi públicas (vector común de ataques) y el el 21.9% otorga permisos innecesarios al utilizar aplicaciones. En relación a protección de datos personales se observa que el 52.2% usa cifrado de datos. A pesar del riesgo pérdida o robo de dispositivos (solo 27.7% tiene borrado remoto)

Tabla 4

Comportamientos de Riesgo

Práctica	Sí	No	% Sí
Abre correos de desconocidos	285	94	75.2%
Usa mismas contraseñas en varias apps	216	163	57.0%

Actualiza contraseñas con frecuencia	214	165	56.5%

Considera sus contraseñas seguras	312	67	82.3%
Conoce qué es malware	147	232	38.8%
Sabe proteger su información	122	257	32.2%

La tabla 4 presenta los comportamientos de riesgo considerados en este estudio, los resultados revelan que el 75.2% abre correos de remitentes desconocidos este comportamiento, asociado al *phishing*, es especialmente riesgoso en el contexto universitario, donde los estudiantes reciben comunicaciones institucionales frecuentes. Solo 38.8% conoce qué es malware Esta cifra explica parcialmente por qué el 45.9% no usa antivirus. El 57% reutiliza contraseñas y 56.5% no las actualiza con frecuencia, estas prácticas, combinadas con el uso de WiFi públicas (34.8%, Tabla 3), incrementan el riesgo de Ataques de credential stuffing (uso de credenciales robadas en múltiples plataformas), si las contraseñas son similares a las de sus cuentas universitarias.

DISCUSIÓN

Los resultados de la investigación revelan datos sobre prácticas comunes de estudiantes universitarios al utilizar dispositivos móviles, mismas que en algunos casos representan vulnerabilidad ante riesgos de seguridad informática.

Existe una alta adopción de métodos de bloqueo con un 88,7%, los dispositivos modernos especialmente smartphones de gama media/alta exigen configurar un método de bloqueo durante la configuración inicial (Android desde la versión 9, iOS desde el iPhone 5s), coincide con estudios como el de *NIST (2021),* donde el 85% de usuarios jóvenes activan bloqueo por recomendaciones del sistema.

El método biométrico es el más integrado en dispositivos asequibles de allí que un 59,9% tenga preferencia por utilizar el bloqueo de huella digital. Según *FIDO Alliance (2022),* el 68% de usuarios considera la huella más segura que contraseñas, además el de desbloqueo promedio es 1.2 segundos.

Se evidencia un bajo uso de patrón (28.5%), investigaciones de *USENIX Security (2020)* demuestran que el 60% de patrones pueden adivinarse observando marcas de dedos en la pantalla, por otra parte, fabricantes como Samsung y Xiaomi ya no lo recomiendan en sus guías de seguridad móvil (2024) este método de bloqueo.

En relación a prácticas de seguridad se obtiene que existe un alto porcentaje del sistema operativo con un 88,1 %, este resultado refleja un comportamiento positivo en cuanto a buenas prácticas básicas, lo cual es consistente con estudios recientes, según el *NIST (2023)*, el 80% de las brechas de seguridad en dispositivos móviles explotan vulnerabilidades para las cuales ya existían parches disponibles. El hecho de que la mayoría de los estudiantes mantenga sus dispositivos actualizados sugiere que están protegidos contra amenazas conocidas.

El 85,2% asegura que descarga aplicaciones de fuentes confiables, este indicador es alentador, ya que las tiendas oficiales (Google Play Store, Apple App Store) implementan revisiones de seguridad, investigaciones de *Kaspersky (2024)* muestran que las aplicaciones de tiendas no oficiales tienen 15 veces más probabilidades de contener código malicioso.

El borrado remoto de un dispositivo es una medida básica de seguridad, que protege la información en caso de pérdida o robo, sin embargo en el presente estudio apenas el 27,7% lo realiza, dato importante a considerar puesto que, según *IBM (2023)*, el 40% de las filtraciones en entornos educativos provienen de dispositivos perdidos o robados sin borrado remoto activado, muchos usuarios desconocen esta función o cómo activarla (*SANS Institute, 2022*), lo que sugiere la necesidad de capacitación específica.

Otro factor crítico detectado es el uso limitado de antivirus (45.9%), aunque los sistemas operativos móviles incluyen protecciones básicas, un antivirus añade una capa adicional de seguridad, el informe *Symantec (2024)* destaca que el malware móvil aumentó un 58% en el último año, especialmente en formas de spyware y ransomware.. Muchos usuarios asumen que las tiendas oficiales son 100% seguras, pero incluso estas pueden albergar aplicaciones maliciosas temporalmente (*OWASP, 2023*)

La investigación pone en evidencia un alto riesgo por apertura de correos sospechosos (75.2%) con bajo conocimiento de Malware (38.8%); estos resultados coinciden con datos de *Proofpoint (2024)*, donde el 78% de los ataques exitosos en educación comienzan con phishing. Esto es crítico porque, los correos maliciosos en móviles son más difíciles de identificar y la mayoría contienen enlaces a malware. Solo el **38.8%** sabe qué es malware, tiene relación con los resultados de McAfee (2024) en el que manifiesta que el **83%** de los usuarios móviles no reconoce señales de infección. Según *ENISA (2023)*, el 45% de las infecciones por malware en universidades provienen de archivos adjuntos en correos.

CONCLUSIONES

Los estudiantes universitarios evidencian una sobreestimación a la seguridad preestablecida en sus dispositivos, la falta de conocimiento en ciberseguridad hace que no den mayor importancia a la aplicación de medidas preventivas básicas como activación de borrado remoto, actualización de antivirus, dejando así desprotegida información importante y sensible que almacenan en sus dispositivos.

Los resultados de la investigación ponen en evidencia la necesidad de que en el ámbito educativo se incorpore educación sobre ciberseguridad, a fin de que los estudiantes creen conciencia de la importancia de proteger su información, creando de esta forma una cultura de manejo de información segura y así protegerse ante amenazas digitales, se propone realizar talleres al iniciar cada período académico con capacitaciones enfocadas en prácticas de seguridad básica como configuración correcta de antivirus, actualmente usado por el 45,9% , activación de borrado remoto, presente en apenas el 27,7% y gestión adecuada de permisos en aplicaciones.

Es fundamental realizar un monitoreo constante para evaluar el impacto de las intervenciones que se realicen, que permita la mejora continua con el incremento en aplicación de buenas prácticas en ciberseguridad por parte de los estudiantes; teniendo presente que la gestión de seguridad es un proceso continuo, puesto que la tecnología avanza y junto a ello aparecen nuevas amenazas y peligros de los que se deben proteger los sistemas.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera López, P. (2010). *Seguridad informática.* México: Editex.

Alvarez Basaldúa, L. D. (2005). *Seguridad en Informática.* México: Iberoamericana.

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México: Patria.

Barrera, J. S. (2024). *Seguridad informática y malwares: análisis de amenazas e implementación de contramedidas.* EMI.

Briceño, E. V. (2021). *Seguridad de la información.* Alzamora: Editorial Área de Innovación y Desarrollo,S.L.

CEP, E. (2019). *Auxiliar Administrativo (Turno Libre). Junta de Andalucía. Temario Vol. III.* Madrid: Editorial CEP S.L.

Chiriguayo Lozano, J. (2015). Comercio Electrónico: IMportancia de la Seguridad en las transacciones electrónicas, amenazas y soluciones a implementar. *Revista Empresarial, ICE-FEE-UCSG*, 8-14.

Cortés Hernández, A. (2019). Ingeniería social: Baiting. *Science*, 1-10.

Cruz Gavilanes, Y., & Martínez Santander, C. (2017). Ataques de ingeniería social. *Dominio de las ciencias*, 1-12.

Curi, O. E. (2018). *Auditoria en Sistemas.* Lima: OECP.

Forero, E. B. (2017). *Seguridad en redes.* Colombia: Areandino.

Gascó, E. (2013). *Seguridad Informática.* Madrid: Macmillan Iberia.

Gómez J.: Hernández, M. (2024). *Seguridad informática y Malwares - Análisis de amenazas e implementación de contramedidas* (3 ed.). (ENI, Ed.)

Gutiérrez Torres, D. (2017). *Comercio electrónico:creación y protección de un sitio web.* Medellin Colombia: Ediciones Unaula . Obtenido de https://elibro.net/es/ereader/uleam/164536?page=25.

Hadnagy, C. (2021). *Ingeniería Social: El arte del engaño.* Anaya Multimedia.

Hernández, M., & Baquero, L. (2020). *Ciclo de vida del desarrollo ágil de software seguro.* Bogotá, Colombia: Los Libertadores.

Larrocha, E. R. (2017). *Nuevas tendencias en los sistemas de información.* Madrid - España: Editorial Universitaria Ramón Areces,S.A.

Larrocha, E., & Cortiñas, P. (2017). *Nuevas tendencias en los sistemas de infromación.* Madrid: Universitaroa RAmón Areces.

Martínez Santander, C., Cruz Gavilanes, Y., & de la N., C. G. (s.f.). Seguridad por capas frenar ataques de smishing. *Dominios de las Ciencias, 4*(1), 115-130.

Mittnick, S. (2022). *Seguridad Cibernética. SEguridad en internet y protección para niños, adolescentes padres y profesionales.* Belbecub.

Murillo, Á., Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., . . . Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: Editorial Área de Innovación y Desarrollo, S.L.

Ovalle Vélez, K. (2019). *Repository.ucatolica.edu.co.* Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/24062/1/Ciberseguridad%20WiFi%20en%20Hogares.pdf

Palomar Delgado , D. (2019). *Introducción al comercio y negocio electrónico* . Edicones Universidad de Salamanca(España). Obtenido de http://hdl.handle.net/10366/139689

Pérez Sánchez, V. (2017). *Seguridad y salud.* Málaga: IC.

Postigo Palacios, A. (2020). *Seguridad Infromática.* Madrid: Ediciones Paraninfo.

Rivera, M., & González, J. (2023). *Seguridad informática: conceptos, estrategias y aplicaciones.* Tecnológica.

Robles Torrente, D. (2015). *Análisis de la seguridad privada.* Barcelona: UOC.

Romero, M., Figueroa, G., Vera, D., & Alava, J. (2018). *Introducción a la seguridad informática y sus vulnerabilidades.* Guayaquil: 3 Ciencias.

Sevilla, B. (2011). *Spam.* España: Facua.

Ujaen. (2018). *Guías de seguridad.* España: Universidad de Jaén. Obtenido de https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%203.%20Malware.pdf

Villalón Huerta, A. (2019). *Seguridad en Unix y redes. Versión 2.1.* España: Nau Llibres-Edicions Culturals Valencines, S.A.