Tipo de artículo: Artículo original

Evaluación de habilidades docentes de Ciberseguridad para la Prevención de Riesgos Cibernéticos en IES

Evaluation of Cybersecurity teaching skills for the Prevention of Cyber Risks in HEIs

Karen Estacio Corozo[*] **https://orcid.org/0000-0002-6394-2455**

[1] Instituto Superior Tecnológico ARGOS. Ecuador. Correo electrónico: k_estacio@tecnologicoargos.edu.ec

*** Autor para correspondencia: k_estacio@tecnologicoargos.edu.ec**

Resumen

La investigación tiene como objetivo evaluar la comprensión y percepción de la ciberseguridad entre docentes, enfocándose en la prevención de ataques de malware, ingeniería social y hábitos de protección de información confidencial. Se utilizó una metodología descriptiva cuantitativa con una muestra de 61 docentes de modalidad virtual. La encuesta, fue validada por expertos en Tecnologías de la Información, evaluó el reconocimiento y consecuencias de ciberataques. Los resultados revelaron una distribución uniforme en la identificación de información confidencial, resaltando la importancia de proteger datos específicos. La mayoría reconoció riesgos de compartir información, sin embargo, hubo brechas en la percepción de consecuencias como el chantaje y la extorsión. En ingeniería social, se señaló la necesidad de mejorar la comprensión, y en protección contra malware, hubo desconocimiento sobre ransomware y sus consecuencias. En conclusión, la investigación resalta la importancia de fortalecer la ciberseguridad en la educación y propone medidas para mejorar la identificación de amenazas y habilidades de prevención. Estos hallazgos mencionan la necesidad de una mayor formación en ciberseguridad en el entorno educativo, contribuyendo a mitigar riesgos y proteger la información sensible de forma más efectiva.

Palabras clave: malware, ransomware, phishing, ciberseguridad en la educación, ingeniería social

Abstract

The research aims to assess the understanding and perception of cybersecurity among teachers, focusing on the prevention of malware attacks, social engineering, and habits for protecting confidential information. A descriptive quantitative methodology was employed with a sample of 61 teachers in virtual mode. The survey, validated by experts in Information Technologies, evaluated the recognition and consequences of cyber attacks. The results revealed a uniform distribution in identifying confidential information, emphasizing the importance of safeguarding specific data. While the majority acknowledged the risks of sharing information, there were gaps in the perception of consequences such as blackmail and extortion. In social engineering, there was a noted need for improved understanding, and in malware protection, there was a lack of awareness regarding ransomware and its consequences. In conclusion, the research underscores the importance of enhancing cybersecurity in education and proposes measures to improve threat identification and prevention skills. These findings highlight the necessity for increased cybersecurity training in the educational environment, contributing to risk mitigation and more effective protection of sensitive information.

Keywords: *malware, ransomware, phishing, cybersecurity in education, social engineering*

Recibido: 22/12/2023
Aceptado: 24/02/2024
En línea: 01/03/2024

Introducción

La evolución y mayor acceso a internet, las comunicaciones y las tecnologías móviles han facilitado transacciones en línea, generando una creciente cantidad de datos digitales almacenados en servidores locales y en la nube. En las últimas décadas se ha visto una creciente dependencia de las tecnologías de la información y la comunicación (TIC) e Internet en varios sectores de la sociedad (Garrido Antón & García-Collantes, 2022). Con esta creciente dependencia de la tecnología, también ha habido un aumento de las amenazas cibernéticas y los delitos cibernéticos. Para resguardar estos datos y mitigar delitos cibernéticos derivados de actividades ilícitas en línea, entidades responsables de información crítica, han invertido significativamente en ciberseguridad (Khader et al., 2021). A pesar de fortalecer las infraestructuras, se ha subestimado la inversión en concientización de seguridad entre los usuarios, dejándolos como el eslabón más vulnerable de la cadena de seguridad de la información.

La falta de concientización sobre la amenaza de los ataques a la ciberseguridad es uno de los factores que contribuyen al creciente número de ataques relacionados con Internet (Hart et al., 2020; Stankov & Gotseva, 2020; Yan et al., 2021). Una de las firmas fabricantes de antivirus Kaspersky (2023), afirma que prácticamente todos los géneros de ataques informáticos incorporan elementos de ingeniería social. Por ejemplo, los correos electrónicos de "phishing" y las estafas de virus, que exhiben un marcado componente social, pretenden persuadir a los usuarios de su autenticidad, con el objetivo de obtener información personal o datos corporativos, por más insignificantes que estos puedan parecer puede dejar desastrosas consecuencias.

El impacto del ransomware en universidades del Reino Unido, como el caso de Portsmouth, tuvo que cerrar parcialmente el campus tras un ataque que dejó inoperativos sus sistemas informáticos (Beardsley, 2023). Los perpetradores de ataques cibernéticos no siempre buscan rescates monetarios, sino que centran sus esfuerzos en interrumpir la prestación de servicios de aprendizaje. Específicamente, los hackers se enfocan en perturbar el acceso a sistemas de información importantes, que posibilitarían a los docentes presentar material, a los estudiantes, enviar tareas o acceder a recursos de apoyo exclusivos en formato digital dentro de la red institucional (Chowdhury et al., 2022).

A pesar de que, la concientización de ciberseguridad para los empleados es esencial, no aborda completamente la formación de habilidades necesaria para fortalecer la defensa de las empresas contra ciberataques. Es importante que las empresas realicen inversiones significativas en el desarrollo de habilidades de ciberseguridad en todos los niveles

de su fuerza laboral y liderazgo. Esta inversión no solo puede disminuir la carga financiera generada por episodios de ciberataques, sino que también contribuye a preservar la confianza del consumidor en sus marcas (Adams & Makramalla, 2015), por lo tanto, se debe instaurar de manera precisa los fundamentos de la ciberseguridad, la formación interna en prácticas sólidas de ciberseguridad a quienes forman parte de la institución educativa como un factor importante para prevenir ataques y asegurar la continuidad educativa, la seguridad de la información asegura la confidencialidad, disponibilidad e integridad de los datos mediante la implementación y gestión de controles apropiados. Esto implica considerar diversas amenazas y reducir al mínimo las consecuencias de posibles incidentes de seguridad. (Estacio, 2023).

El objetivo de la presente investigación es evaluar en un grupo de docentes que forman parte de un Instituto Superior Tecnológico (IST), de entornos de formación en línea, la comprensión, percepción e identificación de amenazas como malware, ingeniería social y hábitos de protección de información confidencial.

Materiales y métodos

El ciberdelito ha surgido como una de las principales amenazas para la economía global. Para las empresas, los costos y las pérdidas asociadas con el ciberdelito son significativos, abarcando desde la corrupción y destrucción de datos hasta el robo de fondos, propiedad intelectual, información personal y financiera. Además, se incluyen la interrupción del negocio tras un ciberataque, el deterioro de la reputación empresarial, la pérdida de productividad, entre otros impactos negativos (FGE, 2021).

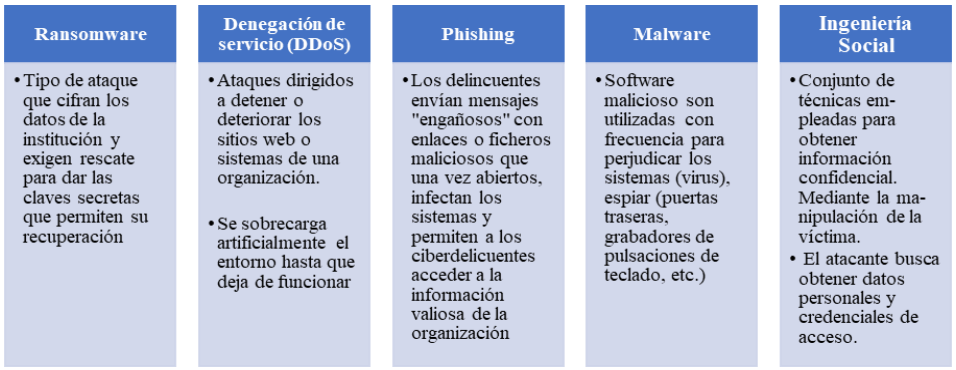

Figura 1. Tipos de cibrecrimen
Fuente: Elaboración propia a partir de (Kaspersky, 2023; Telefónica, 2023)

En el ámbito ecuatoriano, los Institutos Superiores Tecnológicos (IST) son considerados parte fundamental dentro del Sistema de Educación Superior, regidos por las disposiciones normativas emanadas del Consejo de Educación Superior (CES). En particular, en la provincia de Guayas, se ha identificado un total de 32 IST, 5 entidades de carácter público y 27 de naturaleza privada. Este panorama destaca la diversidad y relevancia de estas instituciones en el contexto educativo, evidenciando su importante papel en la formación técnica y tecnológica en la región (CES, 2023).

Aunado a lo mencionado, se realizó una investigación de tipo descriptivo con enfoque cuantitativo y diseño transversal, la selección de la muestra fue no probabilística por conveniencia, por facilidad de acceso al público objeto, escogiendo una IST del sector privado de la provincia del Guayas. Esta muestra estaba compuesta por 61 docentes de diferentes áreas del conocimiento que imparten clases en modalidad virtual.

Se desarrolló una encuesta con el propósito de evaluar el nivel de conciencia en ciberseguridad entre los docentes que participan en entornos virtuales de aprendizaje. La encuesta se enfocó en identificar las vulnerabilidades clave en la seguridad de la información que podrían dar lugar a ser víctimas de ciberdelitos (Figura 1).

La redacción de las diez preguntas (Tabla 1) que conforman la encuesta se llevó a cabo mediante una exhaustiva revisión bibliográfica, el cuestionario fue sometido a un proceso de validación mediante la revisión de cuatro expertos seleccionados por sus amplios conocimientos y experiencia en el campo de Tecnologías de la Información. Esta fase de validación se llevó a cabo con el propósito de afinar la pertinencia, claridad conceptual, redacción y terminología del contenido de la encuesta antes de entrar en la fase de recolección de datos.

En la Figura 2 se presenta la estructura de la rúbrica de validación. Esta rúbrica fue compartida con los expertos durante una reunión virtual, donde se proporcionaron explicaciones detalladas sobre los aspectos a tener en cuenta para cada una de las diez preguntas del cuestionario. La evaluación se realizó mediante una escala de valoración de Likert que abarcó desde 1 hasta 5.

Calificación							
1 = Inaceptable 2 = Deficiente 3 = Regular 4 = Bueno 5 = Excelente							
Pertinencia: La pregunta es relevante y adecuada para medir los aspectos específicos que se desean analizar. **Claridad Conceptual:** Las pregunta está formulado de manera que el encuestado pueda entender fácilmente lo que se está preguntando, evitando ambigüedades o malentendidos. **Redacción y Terminología:** Lredacción de la pregunta es clara y coherente, así como el uso adecuado de la terminología específica del campo de estudio.							
	Contenido		**Evaluación**				
Item	**Criterio**	**Observaciones**	**1**	**2**	**3**	**4**	**5**
1	Pertinencia		☐	☐	☐	☐	☐
	Claridad Conceptual		☐	☐	☐	☐	☐
	Redacción y Terminología		☐	☐	☐	☐	☐

Figura 2. Rúbrica de validación de contenido del cuestionario mediante el juicio de expertos
Fuente: Elaboración propia a partir de (Escobar-Pérez & Cuervo-Martínez, 2008; Penfield & Giacobbi, Jr., 2004)

Una vez recopilada las rubricas de validación de los expertos se procedió a utilizar V de Aiken, un índice utilizado en la validación de instrumentos de medición, como cuestionarios o escalas. Este índice, denotado como "V" (fórmula 1) ofrece una medida descriptiva del nivel de relevancia del contenido de un ítem, es decir, qué tan adecuado es un elemento específico para medir lo que se pretende evaluar (Penfield & Giacobbi, Jr., 2004).

$$V = \frac{\bar{x} - l}{k} \quad (1)$$

Donde "V" representa el índice de V de Aiken, $\overline{"x"}$ representa la media aritmética de las puntuaciones del criterio de cada pregunta dentro del cuestionario, "l" el nivel más bajo de la calificación en la escala, en la rúbrica fue 1 (Figura 2), "k" representa el rango en la escala de calificaciones (denotado por k = 5 - 1) basándose en la calificación de cada juez experto.

$$L = \frac{2nkV + z^2 - z\sqrt{4nkV(1-V) + z^2}}{2(nk + z^2)} \quad (2)$$

$$U = \frac{2nkV + z^2 + z\sqrt{4nkV(1-V) + z^2}}{2(nk + z^2)} \quad (3)$$

En las Ecuaciones 2 y 3, para el calcular el intervalo de confianza, "z" corresponde al valor de una distribución normal estándar, de modo que la distribución se encuentra entre –z y z, se utilizó un intervalo de confianza del 95%, donde z = 1.96.

Para llevar a cabo este cálculo de las ecuaciones, se empleó la herramienta de software Excel. Este proceso se desglosó en tres etapas de los intervalos, representadas como "A" (mediante la fórmula 6), "B" (a través de la fórmula 7) y "C" (utilizando la fórmula 8).

$$L = \frac{A - B}{C} \quad (4)$$

$$U = \frac{A + B}{C} \quad (5)$$

Donde:

$$A = 2nkV + z^2 \quad (6)$$

$$B = \sqrt{4nkV(1-V) + z^2} \quad (7)$$

$$C = 2(nk + z^2) \quad (8)$$

El promedio del índice V de Aiken, arrojó un resultado de 0.88, indicando un nivel alto de validez para el instrumento. La utilización de un intervalo de confianza del 95% para el valor de Vp fortalece la confiabilidad del resultado obtenido, proporcionando una medida más completa de la variabilidad posible alrededor del valor promedio, otorgando una perspectiva más robusta de la validez de la encuesta.

Posterior a la validación del cuestionario, se procedió a ejecutar la fase de recolección de datos, se obtuvo consentimiento por parte de las autoridades de IST. La aplicación del cuestionario fue en línea, utilizando Google Forms, el enlace fue compartido con los 61 docentes vía correo electrónico institucional y los datos resultantes fueron analizados estadísticamente mediante Microsoft Excel. Este procedimiento simplificó la obtención de información esencial para el análisis en el contexto de este estudio. El enlace al cuestionario fue enviado a los participantes mediante sus correos electrónicos institucionales, proporcionándoles información detallada sobre el propósito de la investigación. Se obtuvo el consentimiento informado antes de su participación, garantizando la privacidad de las respuestas recopiladas.

Tabla 1. Preguntas utilizadas para la encuesta.

Ítem	Pregunta	Sección
1	Seleccione la información que considere que debe ser confidencial	Protección contra Phishing
2	¿En qué medida concuerda usted con la afirmación de que compartir información confidencial podría acarrear consecuencias negativas?	Ingeniería Social Protección contra Phishing
3	Seleccione la (s) consecuencia (s) de compartir información sensible	Ingeniería Social Protección contra Phishing
4	¿Cómo describirías la ingeniería social?	Ingeniería Social
5	¿Con cuál de las siguientes situaciones relacionarías a la ingeniería social?	Ingeniería Social
6	¿Con qué frecuencia abre archivos adjuntos en su correo electrónico de remitentes desconocidos?	Protección contra Phishing
7	¿Con qué frecuencia abre archivos adjuntos que recibe en sus redes sociales de remitentes desconocidos?	Protección contra Phishing
8	¿Cuál (es) de las siguientes opciones describiría a un malware?	Protección de Malware
9	Seleccione los tipos de malware que conoce:	Protección de Malware
10	¿A través de qué medio considera usted que se puede propagar un malware?	Protección de Malware

Fuente: Elaboración propia a partir de (Choi, 2013; Garba et al., 2021; Khader et al., 2021; Kraus et al., 2023; Nagarajan et al., 2012; Zaqueu & Mawela, 2023)

Resultados y discusión

En la fase de análisis de resultados se elaboraron tablas de distribución de frecuencia, como también gráficos estadísticos que representen las variables cualitativas nominales categóricas que atañen a la problemática identificada. Se presentarán los resultados analizando cada sección detallada en el instrumento de recolección de datos, iniciando con protección contra phishing e ingeniería social por su similar uso de señuelos. La Tabla 2 hace referencia a una pregunta de selección múltiple relacionada a la identificación de información confidencial, se observan una

distribución uniforme en los resultados destacando los datos de tarjetas de crédito o débito con 19% y datos financieros de la institución con 18%.

Tabla 2. Tipo de información que el encuestado considera de tipo confidencial

Tipo de Información	Frecuencia	Porcentaje
Cédula de identidad	46	14.8
Dirección	47	15.2
Número de teléfono	40	12.9
Datos de sus tarjetas de crédito o débito	59	19.0
Datos financieros de la institución	56	18.1
Patentes	22	7.1
Registros médicos	40	12.9
Desconoce la respuesta	0	-
Total	310	100.0

Así mismo el 82% de los encuestados está de acuerdo con la afirmación de que compartir información confidencial puede traer consecuencias negativas como lo muestra la Tabla 3, frente a un 18% que no está de acuerdo.

Tabla 3. ¿En qué medida concuerda usted con la afirmación de que compartir información confidencial podría acarrear consecuencias negativas?

Tipo de Información	Frecuencia	Porcentaje
Totalmente de acuerdo	43	70.5
De acuerdo	7	11.5
Medianamente en desacuerdo	2	3.3
Totalmente en desacuerdo	9	14.8
Total	61	100.0

En relación con las implicaciones derivadas de la divulgación de información confidencial, los participantes resaltan como aspectos significativos los riesgos de chantaje y extorsión, con un porcentaje del 20%, seguido por la preocupación por el robo de información, que alcanza el 18% (Tabla 4).

Tabla 4. Tipo (s) de consecuencia (s) derivada (s) de compartir información confidencial

Tipo de Consecuencia	Frecuencia	Porcentaje
Robo de información	44	18.7
Fraude	41	17.4
Chantaje y extorsión	47	20.0

Pérdida de privacidad	38	16.2
Pérdida de reputación	24	10.2
Pérdida de dinero	41	17.4
Total	235	100.0

Tan solo el 44.3% de los participantes logró identificar y brindar una definición precisa del concepto de ingeniería social, como se ilustra en la Figura 3. Con el objetivo de ampliar la fundamentación y establecer una conexión indirecta entre el concepto de ingeniería social y, a su vez, el phishing, se formuló la pregunta que contextualiza la ingeniería social mediante ejemplos de situaciones y escenarios sociales reales, como se presenta en la Figura 4. En este sentido, el 20% de los participantes asocia la ingeniería social con la acción de "Recibir un correo electrónico solicitando información personal", mientras que el 19% la vincula con la recepción de "Un mensaje urgente solicitando la confirmación de datos personales". No obstante, un 15% manifestó desconocer la respuesta.

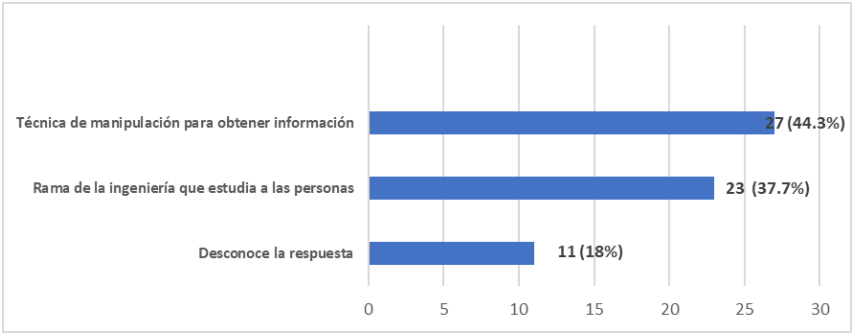

Figura 3. ¿Cómo describirías la ingeniería social? (selección múltiple)

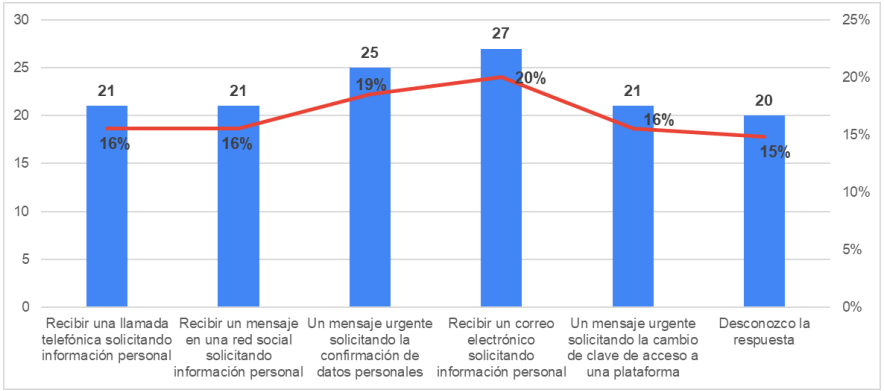

Figura 4. ¿Con cuál (es) de las siguientes situaciones relacionarías a la ingeniería social?

La mayoría de los participantes (62.3%) indicaron que nunca abren archivos adjuntos en su correo electrónico cuando provienen de remitentes desconocidos (Tabla 5). Solo un pequeño porcentaje (3.3%), esto sugiere una tendencia hacia la precaución al gestionar archivos adjuntos de origen desconocido.

Tabla 5. ¿Con qué frecuencia abre archivos adjuntos en su correo electrónico de remitentes desconocidos?

Tipo de Frecuencia	Frecuencia	Porcentaje
Nunca	38	62.3
Casi nunca	14	23.0
De vez en cuando	6	9.8
Casi siempre	1	1.6
Siempre	2	3.3
Total	61	100.0

La sección posterior, centrada en la protección contra el malware, tiene como objetivo identificar de medidas preventivas ante el malware. Se busca evaluar la percepción de riesgos vinculados a la apertura de archivos adjuntos maliciosos y promover la implementación de programas antivirus como salvaguarda para dispositivos móviles y computadoras contra amenazas de malware y virus.

La Figura 5 presenta los resultados obtenidos en relación con conceptos asociados a la definición de malware mediante una pregunta de opciones de selección múltiple. Un destacado 43% de los encuestados asocia el término "malware" con un software malicioso, mientras que el 13% lo vincula con el robo de información. Un reducido 3% manifiesta desconocer la respuesta.

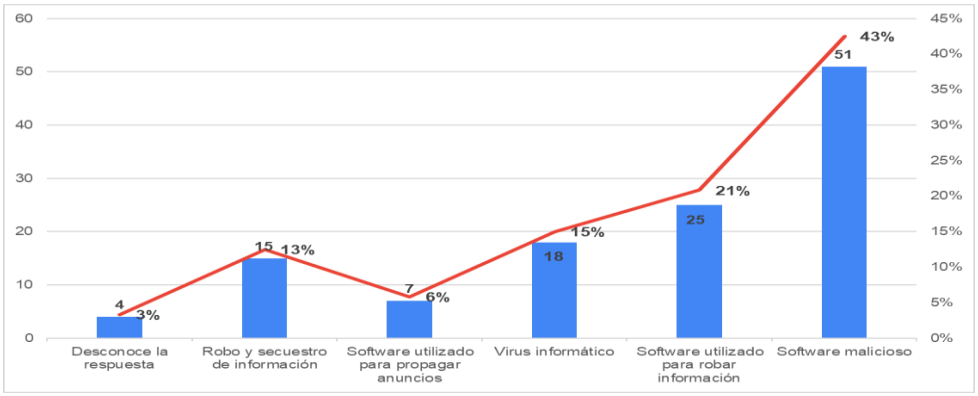

Figura 5. ¿Cuál (es) de las siguientes opciones describiría a un malware?

Después de analizar las nociones relacionadas con el concepto de malware, se instó a los participantes para que identificaran los tipos de malware que reconocen entre una lista de opciones de selección múltiple (Figura 6). El 25.3% eligió troyanos, únicamente el 10.8% seleccionó ransomware, a pesar de ser este último uno de los tipos de malware más peligrosos debido a sus significativas repercusiones operativas y económicas. Cabe destacar que un 4.8% indicó desconocer la respuesta.

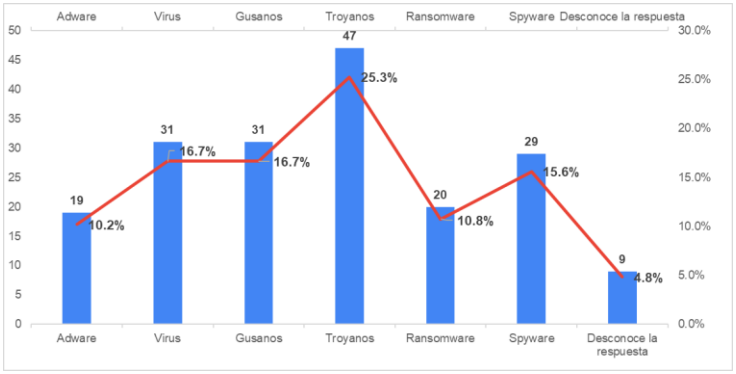

Figura 6. Tipos de malware que conoce el encuestado

Para culminar el análisis, la tabla 6 muestra los resultados de la interrogante donde se solicitó la identificación de los medios e instrumentos de propagación de malware. Destaca que el 30% mencionó la descarga desde internet, mientras que el 29.4% seleccionó archivos adjuntos de correo electrónico.

Tabla 6. ¿A través de qué medio considera usted que se puede propagar un malware?

Medio y/o instrumento de propagación	Frecuencia	Porcentaje
Archivos adjuntos de correo electrónico	47	29.4
Descargas de aplicaciones que no estén en las tiendas oficiales	32	20.0
Dispositivos USB infectados	29	18.1
Desconoce la respuesta	4	2.5
Descargas de Internet	48	30.0
Total	160	100.0

Conclusiones

Se concluye que los resultados de esta investigación ofrecen una visión integral sobre la conciencia y percepciones de los participantes en relación con la seguridad cibernética, en particular, en las áreas de protección contra phishing,

ingeniería social y malware. La distribución uniforme en la identificación de información confidencial, donde se destacan las tarjetas de crédito o débito y datos financieros de la institución, señala la importancia de abordar la protección de estos tipos de datos. Es alentador observar que la mayoría de los participantes está de acuerdo con la afirmación de que compartir información confidencial puede tener consecuencias negativas, lo que indica una comprensión general de los riesgos asociados. Sin embargo, existe una brecha en la percepción de las consecuencias específicas, ya que los participantes resaltan más los riesgos de chantaje y extorsión en comparación con el robo de información.

En el ámbito de la ingeniería social, los resultados subrayan la necesidad de mejorar la comprensión de este concepto, ya que menos de la mitad de los participantes pudo definirlo con precisión. La asociación con situaciones cotidianas, como recibir correos electrónicos solicitando información personal, revela la importancia de contextualizar los conceptos técnicos en la vida diaria. Es notable que la conciencia sobre ransomware, a pesar de ser una amenaza crítica, es relativamente baja. La baja identificación de este tipo de malware sugiere una necesidad de aumentar la concienciación sobre sus peligros potenciales.

El ámbito educativo continuará enfrentando una combinación peligrosa de ataques en aumento y redes vulnerables a menos que se tomen medidas inmediatas tanto por parte de las instituciones educativas como de los proveedores de tecnología. La falta de abordar aspectos fundamentales pone en riesgo la continuidad de la enseñanza y, en casos más graves, podría resultar en consecuencias financieras que obliguen al cierre de las instituciones educativas. Estos resultados subrayan la necesidad urgente de fortalecer la educación en ciberseguridad, no solo centrándose en amenazas técnicas específicas, sino también promoviendo una comprensión más profunda de las implicaciones y riesgos vinculados a la divulgación de información confidencial. Este estudio sienta las bases esenciales para el desarrollo de programas de concienciación y formación destinados a mejorar la postura de seguridad cibernética tanto a nivel individual como organizativo.

Agradecimientos

Se añaden los nombres de personas que contribuyeron a la investigación pero que no se consideran como parte del colectivo de autores. Se incluyen los nombres de instituciones o proyectos que proporcionaron facilidades para la realización de la investigación tanto materiales, logísticas o financieras.

Conflictos de intereses

El autor no posee conflictos de intereses.

Contribución de los autores

1. Conceptualización: Karen Estacio Corozo
2. Curación de datos: Karen Estacio Corozo
3. Análisis formal: Karen Estacio Corozo
4. Investigación: Karen Estacio Corozo
5. Metodología: Karen Estacio Corozo
6. Administración del proyecto: Karen Estacio Corozo
7. Recursos: Karen Estacio Corozo
8. Software: Karen Estacio Corozo
9. Validación: Karen Estacio Corozo
10. Visualización: Karen Estacio Corozo
11. Redacción – borrador original: Karen Estacio Corozo
12. Redacción – revisión y edición: Karen Estacio Corozo

Financiamiento

La investigación no requirió fuente de financiamiento externo.

Referencias

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review.

Beardsley, T. (2023, febrero 9). Security vulnerabilities make the education sector a risky business. OPEN ACCESS GOVERNMENT. Disponible en: https://www.openaccessgovernment.org/security-vulnerabilities-education-sector-risky-business/152902/

CES. (2023). Transformando la Educación Superior. Consejo de Educación Superior. Disponible en: https://www.ces.gob.ec/?page_id=1543

Choi, M. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. Disponible en: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1027&context=wisp2012

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. Computers & Security, 113, 102551. Disponible en: https://doi.org/10.1016/j.cose.2021.102551

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). VALIDEZ DE CONTENIDO Y JUICIO DE EXPERTOS: UNA APROXIMACIÓN A SU UTILIZACIÓN. 6(1).

Estacio Corozo, K. (2023). Modelo de evaluación madurez de gestión de seguridad de la información en centros de datos: Information Security Assessment Model for Data Centers. Cumbres, 9(1), p. 39-50. Disponible en: https://doi.org/10.48190/cumbres.v9n1a3

FGE. (2021). Perfil Criminológico: El Rol De La Administración De Justicia Y La Cooperación internacional En La Lucha Contra La Ciberdelincuencia. Disponible en: https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Garba, A. A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F., & Alim, S. (2021). An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia. 04.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security, 95, 101827. Disponible en: https://doi.org/10.1016/j.cose.2020.101827

Kaspersky. (2023). Ingeniería social: Definición. Kaspersky daily. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. Information, 12(10), 417. Disponible en: https://doi.org/10.3390/info12100417

Kraus, L., Švábenský, V., Horák, M., Matyás, V., Vykopal, J., & Celeda, P. (2023). Want to Raise Cybersecurity Awareness? Start with Future IT Professionals. Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1, p. 236-242. Disponible en: https://doi.org/10.1145/3587102.3588862

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), p. 256-262. Disponible en: https://doi.org/10.1109/CYBER.2012.6392562

Penfield, R. D., & Giacobbi, Jr., P. R. (2004). Applying a Score Confidence Interval to Aiken's Item Content-Relevance Index. Measurement in Physical Education and Exercise Science, 8(4), p. 213-225. Disponible en: https://doi.org/10.1207/s15327841mpee0804_3

Stankov, I., & Gotseva, D. (2020). An Overview of Security and Risk Management in Business Intelligence Systems. 2020 III International Conference on High Technology for Sustainable Development (HiTech), 1-5. https://doi.org/10.1109/HiTech51434.2020.9363990

Telefónica. (2023, marzo 29). Cibercrimen, una amenaza constante para todo tipo de empresas. Telefónica Tech. Disponible en: https://telefonicatech.com/blog/cibercrimen-una-amenaza-constante-para-todo-tipo-de-empresas

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. Computers in Human Behavior, 121, 106791. Disponible en: https://doi.org/10.1016/j.chb.2021.106791

Zaqueu, P., & Mawela, T. (2023). Factors Contributing to Cybersecurity Awareness, Education and Training. p. 69-78. Disponible en: https://doi.org/10.29007/l4ph