REVISTA DE CIENCIAS FORENSES DE HONDURAS

Artículo original

TRABAJO ORIGINAL

Impacto percibido por las víctimas de estafas electrónicas en Tegucigalpa, Honduras

Perceived impact by victims of electronic scams in Tegucigalpa, Honduras

Donnie Rene López Ramírez[1*]: https://orcid.org/0000-0002-4004-4628

Luis Gerardo Reyes Flores[1]: https://orcid.org/0000-0002-5399-2766

[1]*Universidad Nacional de la Policía de Honduras. Dirección de Investigación Científica y Comunicaciones. Tegucigalpa, Honduras.*

**Correspondencia a:* donnierene@gmail.com

Palabras clave

Ciberdelitos, Ciberseguridad, Estafa electrónica, Víctimas del crimen, Percepción social.

Keywords

Cybercrime, Cybersecurity, Electronic fraud, Victims of crime, Social perception.

Citar como

López Ramírez D, Reyes Flores LG. Impacto percibido por las víctimas de estafas electrónicas en Tegucigalpa, Honduras. Rev. cienc. forenses Honduras. 2025; 11(2): 7-15. doi:10.5377/rcfh.v11i2.22411.

Historia del artículo

Recepción: 24 -7- 2025

Aprobación: 12 -2- 2026

Declaración de relaciones actividades financieras y conflictos de interés

Ninguna

Se contó con la autorización institucional para la recolección de la información.

Se obtuvo el consentimiento informado de los participantes, no se sometió al Comité de Bioética.

Agradecimientos

No se declaran.

Uso de herramientas de IA

No se declaran.

RESUMEN

Objetivo: Comprender el impacto a nivel económico y emocional en los afectados de estafas electrónicas.

Introducción: los ciberdelitos y estafas electrónicas son actividades delictivas comunes en nuestra sociedad debido al uso cotidiano de páginas digitales o sus redes sociales para actividades particulares y de negocios. Se estima que a nivel mundial millones de personas al año son víctimas de ciberdelitos, lo que tiene un impacto no solo a nivel económico, sino también psicológico. En Honduras aún no se conoce su prevalencia, ni el impacto en las víctimas

Metodología: enfoque cuantitativo, tipo descriptivo-correlacional, en el que se utilizó un instrumento tipo encuesta para la recolección de datos la cual fue aplicada a personas que interpusieron denuncia durante los meses de octubre a diciembre del 2024 en la Unidad Investigativa Contra Delitos Informáticos de la Policía Nacional de Honduras. El instrumento constaba de tres dimensiones (impacto emocional, confianza en compras en línea e impacto financiero), evaluadas mediante un total de 12 doce preguntas (ítems); cada una diseñada para medir el impacto emocional en la confianza para realizar compras en línea y el impacto financiero en las víctimas de estafas electrónicas, la muestra fue no probabilística por conveniencia, con 188 participantes.

Resultados: El 40% experimentó una mezcla de frustración e ira al sentirse engañada, además 53% perdió la confianza en las plataformas digitales para realizar compras o pagos de servicios o productos, mientras un 45% reportaron haber sufrido una pérdida económica además de la sensación de impotencia ante la posibilidad que los responsables quedaran impunes.

Conclusión: Las víctimas de estafas electrónicas participantes; son personas jóvenes, sin distingos por sexo que sufrieron afectaciones emocionales y económicas, adicionalmente se observó una disminución en la confianza de los afectados al momento de realizar compras de productos en línea.

ABSTRACT

Objective: Understanding the economic and emotional impact on victims of online scams.

Introduction: Cybercrimes and electronic scams are a common criminal activity in contemporary society due to the widespread daily use of digital platforms or social media for personal activities or business. This study analyzed the perceived impact on individuals who were victims of cybercrimes in the city of Tegucigalpa, Honduras.

Methodology: Quantitative approach, with a descriptive correlational design which used a survey as instrument to collect data, it was administered to individuals who filed complaints during the last quarter of 2024 in the Cybercrime Investigative Unit of Honduras National Police. This 12 items instrument measured three dimensions: emotional impact, trust in on line transactions and finally financial impact on cybercrime victims, a convenience nonprobability sample of 188 participants was used.

Results: 40% of victims experienced a strong feeling of anger and frustration, demonstrating an intense emotional response on being deceived. Likewise, 53% of participants lost trust in digital platforms for buying products or paying for services, while 45 % of participants reported that they suffered economic loss along with a feeling of helplessness at the possibility that the perpetrators might go unpunished.

Conclusion: Cybercrime victims in Tegucigalpa where young adults, without distinction between sexes, that suffered deep emotional distress and substantial financial losses, furthermore a notable decrease on victims' trust in making online purchasing and acquiring products was observed.

INTRODUCCIÓN

Debido al auge informático y a la interconectividad facilitada por la internet hay un surgimiento de nuevas modalidades de crimen ligados a la tecnología y al uso masivo de las redes sociales, lo que facilita las estafas electrónicas o los ciberdelito, que se perpetran a través de la web u otro tipo de redes[1,2]. En su mayoría los ciberdelitos son planificados considerando elementos de ingeniería social la cual se refiere a las técnicas que los hackers utilizan para engañar al usuario con el motivo de robarle información personal y llevarlo a huecos de su seguridad [3] y realizar estafas de productos o servicios utilizando las redes sociales. En Honduras este tipo de delitos incrementó, especialmente durante y después de la pandemia de la COVID-19 por el aumento del uso de la internet y la compra de productos en línea [4].

Estas actividades ilícitas no solo generan a las víctimas pérdidas económicas significativas, sino que también las afectan en múltiples formas como la psicológica, social y emocional [5]. Por ello en nuestro contexto toma relevancia conocer cómo operan estas modalidades delictivas y como impactan a las víctimas. En años recientes los ciberdelitos y específicamente las estafas electrónicas han crecido considerablemente a nivel mundial con grandes pérdidas económicas que proyectadas alcanzan los seis billones de dólares anuales, lo que acentúa la necesidad de contramedidas eficaces6, por su parte en Latinoamérica la situación es preocupante debido a vulnerabilidades estructurales y por la rápida adopción tecnológica tanto a nivel organizacional como individual, lo que incrementó la proliferación de fraudes y ataques cibernéticos. Asimismo, la baja conciencia sobre ciberseguridad, la falta de estándares y software especializados, brechas de seguridad y la falta de capacitación y especialización profesional [7].

Honduras carece de una ley enfocada en la ciberseguridad como tal, existiendo preocupación en cuanto a la protección de datos personales, ya que muchas empresas privadas manejan y recopilan información sin controles adecuados, no obstante, instituciones públicas y privadas tratan de implementar métodos de verificación[8] para dificultar el hacking [9]; en contraste los cibercriminales pueden clonar, falsificar o robar perfiles fácilmente en las redes

sociales debido al gran número de usuarios activos y a la facilidad para acceder a la información de los usuarios[10]; la condición de perfil público en redes sociales expone información personal de estos[11], siendo la privacidad de los datos personales un tema sensible[12]. Otro aspecto a mencionar son las compras en línea sin verificación de la seguridad y confiabilidad del sitio web, donde se da acceso a la información personal pudiendo ser vulnerada[13].

En el caso particular de Honduras la ausencia de una política nacional de ciberseguridad constituye una potencial vulnerabilidad por lo que en años recientes el gobierno ha renovado su estrategia de seguridad nacional para incluir la ciberdelincuencia y fortalecer las instituciones encargadas de velar por la seguridad nacional[14]. La Policía Nacional de Honduras creó una unidad especializada, para investigar denuncias relacionadas al ciberdelito; siendo la ciberestafa una de las más comúnmente denunciada. El código penal hondureño establece en el Art.365, que: *"Comete estafa quien, con ánimo de lucro, utiliza engaño suficiente para producir error en otro y le induce a realizar un acto de disposición en perjuicio propio o ajeno"*[15].

Este estudio tuvo por objetivo describir el impacto percibido por las víctimas de estafas electrónicas y explorar posibles relaciones entre variables, como el impacto emocional, confianza en los servicios en línea y el impacto en la economía personal.

METODOLOGÍA

Estudio cuantitativo no experimental, de corte transversal que se realizó en Tegucigalpa, Distrito Central, Honduras, en un contexto urbano proclive a la ocurrencia de ciberdelitos y estafas electrónicas, dada la convergencia de factores tales como: limitantes en la seguridad digital, mínima alfabetización digital y desconocimiento de procedimientos de denuncia. La población fue de carácter indeterminada conformada por habitantes de la ciudad de Tegucigalpa, mayores de edad, línea y que interpusieron sus denuncias durante octubre y noviembre del 2024 ante la Unidad Investigativa contra Delitos Informáticos de la Dirección Policial de Investigación (DPI) de Tegucigalpa. La muestra fue no probabilística por conveniencia, conformada por 188 participantes que voluntariamente aceptaron participar en el estudio.

Para el proceso de recolección de datos, se diseñó un instrumento tipo encuesta, que se muestra en la **Cuadro 1**, consistente de 12 preguntas evaluadas en una escala de 1 al 5, donde 1 es totalmente en desacuerdo y 5 es muy de acuerdo, los cuales se establecieron mediante un análisis factorial exploratorio (AFE)[16], realizado para examinar la estructura subyacente del instrumento reduciendo la dimensionalidad en los ítems y agrupándolos en factores coherente en tres dimensiones:

1.-Impacto emocional en las víctimas de estafas electrónicas, con un total de tres preguntas relacionadas a este aspecto.

2.-Impacto en la confianza en los medios electrónicos, con un total de cinco preguntas en relación a este aspecto.

3.-Impacto económico auto percibido, con un total de cuatro preguntas relacionadas a este aspecto.

Además, se aplicó el modelo de rotación varimax[17] lo que facilitó la interpretación de los factores al maximizar la varianza explicada con cargas factoriales que oscilaron entre 0.458 y 0.901 lo cual indica una relación fuerte entre los ítems y sus respectivas dimensiones.

El instrumento fue sometido a validación por jueces expertos; profesionales policiales especializados en el área de investigación criminal, para verificar la validez de contenido y del constructo, lo que introdujo mejoras en la redacción de los ítems. Previo a la aplicación del instrumento, se obtuvo el consentimiento informado de todos los participantes, explicándoseles los objetivos del estudio, el carácter voluntario y anónimo de su

participación y el uso exclusivo de su información con fines académicos. Se garantizó la confidencialidad de las respuestas, asegurando que ningún dato pudiera ser asociada a una persona o denuncia en particular.

Los datos fueron procesados en el programa estadístico Statistical Package for the Social Sciences (SPSS)[18], versión 25 y Jamovi [19] versión 2.4 y se realizaron análisis de estadística descriptiva[20]. Una vez recolectada la información se calculó un alfa de Cronbach cuya puntuación fue de 0.87 indicando una alta consistencia en el conjunto de reactivos.

Se realizó un análisis correlacional para examinar la relación entre los principales constructos del estudio: Impacto emocional, Confianza en plataformas digitales e Impacto económico. Se aplicó el coeficiente de Correlación de Spearman (rs)[21], debido a que en el análisis preliminar de los datos se corroboró una distribución no paramétrica (p- valor < 0.05), además para interpretar el grado de correlación se utilizaron los rangos establecidos por Martínez y Col.[22].

RESULTADOS

El cuadro 1 muestra los resultados expresados en porcentaje de los descriptivos de los reactivos del instrumento de impacto percibido por las víctimas de estafas electrónicas.

De los 188 participantes el 63% eran jóvenes entre 18 a 33 años, asimismo, el nivel de educación predominante fue la secundaria con el 68.1%, mostrando un equilibrio de género (55% hombres, 45% mujeres). La distribución de los datos demográficos (sexo, nivel educativo y rango de edad) de los participantes se muestra en el **Cuadro 2**.

Destacó una concentración significativa (22 a 59%) de respuestas en las categorías 4 "de acuerdo" y 5 "totalmente de acuerdo", mostrando que las víctimas del ciberdelito auto perciben impacto en múltiples dimensiones como ser a nivel emocional, confianza y hábitos financieros. Asimismo, los hallazgos señalan que las víctimas enfrentan sentimientos de frustración, pérdida de confianza en el entorno digital y cambios significativos en los hábitos de consumo y seguridad en línea.

Los resultados muestran impacto en diversas áreas: el 40 % reportó ira constante hacia los perpetradores. Mientras que a nivel emocional el 51% sintió frustración por no recuperar lo perdido.

Con respecto a la confianza en realizar compras en internet, las respuestas revelaron que el 53% manifestó perdida de la confianza en plataformas digitales y el mismo porcentaje de los participantes manifestaron temor a compartir información personal incluso en sitios que consideraban seguros, el 59% de los participantes expresó haber cambiado sus hábitos o comportamientos a la hora de cotizar o comprar productos en internet.

En relación al impacto financiero sufrido por las víctimas de este tipo de delitos el 45% reportó un impacto económico significativo, otro aspecto a considerar en este ámbito es que, un 37% incurrió en gastos adicionales para servicios de protección de identidad y asesorías legal tras haber sido víctimas de ciberdelitos; a su vez, un 37% expresó haber recortado gastos esenciales debido a las pérdidas financieras sufridas.

El análisis factorial exploratorio realizado, (**ver Cuadro 3**) para medir el impacto percibido en víctimas de ciberdelitos o estafas electrónicas permitió identificar tres factores principales que agrupan las variables evaluadas:

- impacto emocional (I_Emoc_)
-confianza (Conf_L_)
-impacto económico (I_Econ)

El análisis factorial en relación a las dimensiones estudiadas indicó que el perjuicio económico ocasionado por las pérdidas financieras directas y las dificultades para recuperar los fondos constituyen un componente principal y claramente identificable de la victimización por ciberdelitos.

Cuadro 1: Descriptivo de los reactivos del instrumento de impacto percibido por las víctimas de ciberestafas expresados en porcentaje.

	1=Totalmente en desacuerdo	2.=En desacuerdo	3=Ni de acuerdo ni en desacuerdo	4.-De acuerdo	5.-Muy de acuerdo
1.Siento ira o frustración constante hacia los perpetradores del ciberdelito o estafas electrónicas.	2%	3%	17%	38%	40%
2.Siento frustración por la incapacidad de poder recuperar lo perdido como consecuencia del ciberdelito.	3%	0%	16%	51%	30%
3.Experimento sentimientos de vergüenza o culpa por haber sido víctima de un ciberdelito.	9%	5%	19%	36%	31%
4.He perdido confianza en las plataformas digitales para realizar compras o pagos de servicios o productos.	6%	6%	13%	53%	22%
5.La inseguridad digital disminuyó la confianza en negocios en línea, de venta de productos o servicios en línea.	5%	5%	12%	53%	25%
6.Dudo en compartir información personal en línea, incluso en sitios en línea que antes consideraba seguros.	4%	3%	10%	53%	30%
7.Creo que no se debe confiar en la identidad de las personas o entidades con las que interactúo en línea.	2%	4%	12%	52%	30%
8.La pérdida financiera que sufrí ha afectado mi economía.	6%	6%	18%	45%	25%
9.Incurrí en gastos adicionales por servicios de protección de identidad y asesoría legal tras el incidente.	7%	12%	21%	37%	23%
10.He recortado esenciales debido a las pérdidas financieras sufridas por el ciberdelito.	10%	11%	20%	37%	22%
11.Después de haber sido víctima tuve un impacto negativo en mis ahorros.	6%	9%	16%	45%	24%
12.He cambiado mis hábitos en línea al cotizar/comprar productos en internet.	4%	4%	11%	59%	22%

Fuente: Elaboración propia.

Cuadro 2: Datos demográficos de los participantes, n=188

Variable	Categoría	Frecuencia	%
Sexo	Hombre	104	55
	Mujer	84	45
Nivel educativo	Primaria	6	3,2
	Secundaria	128	68,1
	Universitario	49	26,1
	Ninguno	5	2,7
Edad	18-33 años	119	63
	34-48 años	49	26
	49-65 años	20	11

A su vez, la confianza en el uso de plataformas digitales se ve severamente afectada tras el delito y apunta directamente a una pérdida significativa de la confianza para realizar transacciones o compartir información en línea posterior a la experiencia fraudulenta, indicando además que las consecuencias emocionales son un componente inherente a este tipo de delitos.

Se obtuvo un índice de 0.547, lo que indica que se encontró una correlación positiva (rs=0.547 entre el impacto emocional y la pérdida de confianza en las víctimas de este tipo de delito financiero. Esto sugiere que, a mayor impacto emocional (estrés, ansiedad, etc.), menor es la confianza en instituciones, negocios en línea, sistemas o procesos relacionados con la ciberseguridad.

También se observó una correlación positiva moderada entre el impacto emocional y el impacto económico(rs=0.478). Esto implica que, a medida que aumenta la percepción de pérdidas económicas, el impacto emocional también tiende a intensificarse.

Además, se observó una correlación positiva moderada entre la pérdida de confianza en las compras en línea y el impacto económico (rs=0.378). Las víctimas que experimentaron mayores pérdidas económicas también reportaron una disminución significativa en su confianza hacia mecanismos de protección, entidades financieras o vendedores de productos en línea.

DISCUSIÓN

Las personas víctimas de estafas en internet se ven afectadas en tres áreas principales: el aspecto emocional, el económico y la confianza.

El estudio mostró que ser víctima de estafas en línea afecta significativamente el aspecto emocional en las personas, con emociones negativas como el miedo y la angustia, así como sentimientos de culpa que predominaron entre los afectados. Estos hallazgos son consistentes con el estudio realizado por Lusthaus[23], quien estableció que el anonimato en línea crea un gran déficit de confianza que hace que las transacciones asociadas a ciberdelincuencia sean muy inestables. Nuestros hallazgos reflejan la otra cara de esa inestabilidad: cuando la transacción fraudulenta se completa, el déficit de confianza no se resuelve, sino que se transfiere y amplifica en la víctima, traduciéndose en ira, frustración y desconfianza permanente.

Cuadro 3: Análisis factorial de las dimensiones estudiadas

Factor	Factor			Unicidad
	Impacto económico	Confianza en plataformas digitales	Impacto emocional	
I_Emoc_4			0.818	0.427
I_Emoc_5			0.675	0.514
I_Emoc_6			0.639	0.454
Conf_L_9		0.693		0.511
Conf_L_10		0.816		0.423
Conf_L_11		0.876		0.269
Conf_L_12		0.458		0.604
I_Econ13	0.680			0.422
I_Econ14	0.578			0.499
I_Econ16	0.875			0.265
I_Econ17	0.901			0.275
I_Econ18	0.502			0.776

Un alto porcentaje de los participantes reportó sentimientos negativos constantes hacia los perpetradores, lo que concuerda con estudios previos realizados por Bada y Nurse[24] en el que la frustración, ira e indignación son emociones constantes tras haber sufrido la pérdida económica, además de experimentar sentimientos de culpa y vergüenza, como lo muestra gran parte de los encuestados que acudieron a interponer la denuncia a las autoridades policiales.

Realizando una comparación con el estudio de Fenge y Lee[25], que afirma que la victimización por ciberdelitos tiene un mayor impacto negativo en el bienestar emocional para casos centrados en la persona, conocidos y víctimas no compensadas y un menor impacto en los afectados de ingresos más altos, el presente estudio no midió estas variables, pero sí evidenció la afectación emocional en las víctimas participantes.

Conclusiones

Las víctimas de las estafas electrónicas son personas jóvenes, con un nivel educativo en su mayoría de educación media, sin distinción de sexo. Adicionalmente manifestaron impactos auto percibidos a nivel emocional, económico y una evidente pérdida de confianza en los medios digitales y redes sociales que ofrecen servicios de compra y venta de productos o servicios.

Recomendaciones:

Dada la vulnerabilidad de las víctimas condicionada entre otras por un débil marco legal y el desconocimiento de los *modus operandi* de los criminales, se requiere la implementación de estrategias de prevención, mitigación y respuesta contra los ciberdelitos o estafas electrónicas; como la educación y concientización sobre aspectos importantes para reducir la vulnerabilidad, campañas informativas de parte de instituciones de seguridad sobre los tipos y estrategias más comunes de los estafadores, así como socializar canales de denuncia accesibles y eficaces

para que las autoridades policiales puedan proceder de manera más rápida contra los delincuentes.

Limitantes

Dentro de este aspecto cabe mencionar que este estudio presenta limitantes metodológicas que deben considerarse al interpretar sus hallazgos, en primer lugar el tiempo de respuesta en el llenado de las encuestas de los denunciantes fue extenso, lo que retrasó la recolección de la muestra. Además, al haberse centrarse exclusivamente en víctimas que denunciaron puede existir un sesgo de selección. Las personas que no denunciaron este tipo de delitos podrían experimentar impactos diferentes.

REFERENCIAS BIBLIOGRÁFICAS

1. Lakhani S. Perspectives on internet-based crimes. En: Sahni SP, Bhadra P, editores. Criminal Psychology and the Criminal Justice System in India and Beyond. Singapore: Springer; 2021 [citado 2025 ene 10]. Disponible en: https://doi.org/10.1007/978-981-16-4570-9_9

2. Valdez Alvarado AR. El Cibercrimen. Rev Inf Tecnol Soc. 2009 [citado 2025 ene 10]; (3):122-124. Disponible en: https://scholar.google.com/citations?view_op=view_citation&hl=es&user=PuUhHgcAAAAJ&citation_for_view=PuUhHgcAAAAJ:Tyk-4Ss8FVUC

3. López Grande CE, Guadrón RS. Ingeniería social: el ataque silencioso. Rev Tecnol ITCA-FEPADE. 2015 [citado 2025 feb 15];(8):38-45. Disponible en: https://core.ac.uk/outputs/80296691/?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

4. Abdul-Bar Méndez O. COVID-19 y cibercrimen[Tesis]. Elche: Universidad Miguel Hernández de Elche; 2021 [citado 2025 ene 8]. Disponible en: https://dspace.umh.es/bitstream/11000/25669/1/TFM-Abdul-Bar%20M%c3%a9ndez,%20Omar.pdf

5. Makarova EA, Makarova EL. Ciber-victimización y su impacto en el estado psicosomático de la víctima. IJCRSEE. 2023 [citado 2025 ene 8];11(2):231-245. Disponible en: https://www.ijcrsee.com/index.php/ijcrsee/article/view/2496

6. Alghamdi MI. A Descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. Int J Eng Res Technol. 2020 [citado 2025 ene 8];9(6):731-735. Disponible en: https://www.ijert.org/research/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide-IJERTV9IS060565.pdf

7. Flor-Unda O, Simbaña F, Larriva-Novo X, Acuña Á, Tipán R, Acosta-Vargas P. A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. Informatics. 2023 [citado 2025 ene 8]; 10(3):71. Disponible en: https://doi.org/10.3390/informatics10030071

8. Santos Montenegro MA, Barrios Miranda ÁS, González de Vinces PJ. El hacking como comportamiento típico en las nuevas formas de delincuencia organizada. Espirales Rev multidiscip investig.2019; 3(26): 60-70. Disponible en: https://doi.org/10.31876/re.v3i26.460

9. Tsikerdekis M, Zeadally S. Online deception in social media. Inf Sci Fac Publ. 2014 [citado 2024 nov 23]: 12. Disponible en: https://uknowledge.uky.edu/slis_facpub/12

10. Rohit M, Sharmila C. A secure user image privacy preserving technique to avoid clone attack in online social network. J Comput Theor Nanosci. 2020[citado 2025 ene 8];17(5):2304-2307. Disponible en: https://www.researchgate.net/publication/342333218_A_Secure_User_Image_Privacy_Preserving_Technique_to_Avoid_Clone_Attack_in_Online_Social_Network

11. Zhu J, Zhang S, Singh L, Yang GH, Sherr M. Generating risk reduction recommendations to decrease vulnerability of public online profiles. En: 2016

International Conference on Advances in Social Networks Analysis and Mining (ASONAM); San Francisco, CA, USA. IEEE; 2016 [citado 2025 ene 8]: 411-416. Disponible en: https://doi.org/10.1109/ASONAM.2016.7752267

12. Zarei K. Fake identity & fake activity detection in online social networks based on transfer learning[Tesis]. Paris: Institut Polytechnique de Paris; 2022 [citado 2025 ene 8]. Disponible en: https://theses.hal.science/tel-03936643

13. Mendoza E. Ciberestafas: amenaza creciente que proviene de países de Sudamérica. Heraldo. 2024 may 24: Tegucigalpa. [citado 2025 ene 8]. Disponible en: https://www.elheraldo.hn/tegucigalpa/ciberestafas-amenaza-creciente-proviene-paises-sudamerica-CE19488468

14. Raudales Centeno CM. La brecha existente en la ciberseguridad en Honduras. Innovare. 2017 [citado 2025 mar 13];6(2):58-73. Disponible en: https://www.camjol.info/index.php/INNOVARE/article/view/5571

15. Honduras. Decreto 144-83, Código Penal. Tegucigalpa: Poder Judicial; 1984 [actualizado 2019; decreto 130-2017]. Disponible en: https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

16. Watkins MW. Exploratory factor analysis: a guide to best practice. J Black Psychol. 2018 [citado 2025 ene 8]; 44(3):219-246. Disponible en: https://journals.sagepub.com/doi/epub/10.1177/0095798418771807

17. Rohe K, Zeng M. Vintage factor analysis with varimax performs statistical inference. J R Stat Soc Series B Stat Methodol. 2023 [citado 2025 ene 8]; 85(4):1037-1060. Disponible en: https://doi.org/10.1093/jrsssb/qkad029

18. IBM Corp. IBM SPSS Statistics para Windows. Versión 25.0. Armonk (NY): IBM Corp; 2021 [citado 2025 ene 8]. Disponible en: https://www.ibm.com/analytics/spss-statistics-software.

19. The Jamovi project. Jamovi . Versión 2.5. 2024 [citado 2025 ene 8]. Disponible en: https://www.jamovi.org

20. Orçan F. Comparison of Cronbach's alpha and McDonald's omega for ordinal data: Are they different?. Int J Assess Tools Educ. 2023 [citado 2025 ene 8];10(4):709-722. Disponible en: https://doi.org/10.21449/ijate.1271693

21. Schober P, Boer C, Schwarte LA. Correlation coefficients: appropriate use and interpretation. Anesth Analg. 2018 [citado 2024 dic 22];126(5):1763-1768. Disponible en: https://doi.org/10.1213/ANE.0000000000002864

22. Martínez Ortega RM, Tuya Pendás LC, Martínez Ortega M, Pérez Abreu A, Cánovas AM. El coeficiente de correlación de los rangos de Spearman caracterización. Rev Habanera Cienc Méd. 2009 [citado 2025 ene 8];8(2). Disponible en: https://www.redalyc.org/pdf/1804/Resumenes/Resumen_180414044017_1.pdf

23. Lusthaus J. Trust in the world of cybercrime. Global Crime. 2012 [citado 2024 dic 12];13(2):71-94. Disponible en: https://doi.org/10.1080/17440572.2012.674183

24. Bada M, Nurse JRC. The social and psychological impact of cyber attacks. En: Benson V, Mcalaney J. editores. Emerging cyber threats and cognitive vulnerabilities Academic Press. 2020 [citado 2025 ene 8]. p. 73-92. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/B9780128162033000046

25. Fenge LA, Lee S. Comprensión de los riesgos de las estafas financieras como parte de la prevención del maltrato a personas mayores. Br J Soc Work. 2018 [citado 2024 dic 11];48(4):906-923. Disponible en: https://psycnet.apa.org/record/2018-37606-003