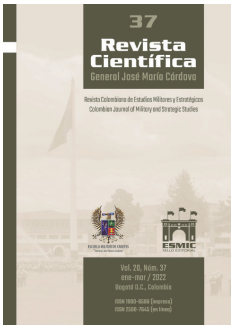

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú

Edwin Hernán Ramírez Asís
https://orcid.org/0000-0002-9918-7607
ehramireza@unasam.edu.pe
Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú

Roger Pedro Norabuena Figueroa
https://orcid.org/0000-0003-3731-9843
rnorabuenaf@unmsm.edu.pe
Universidad Nacional Mayor de San Marcos, Lima, Perú

Ricardo Enrique Toledo Quiñones
https://orcid.org/0000-0003-4834-5959
rtoledoq@unasam.edu.pe
Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú

Patricia Raquel Henostroza Márquez Mázmela
https://orcid.org/0000-0002-1816-1617
patricia.henostroza@pucp.pe
Pontificia Universidad Católica del Perú, Lima, Perú

Citación APA: Ramírez Asís, E. H., Norabuena Figueroa, R. P., Toledo Quiño-nes, R. E., & Henostroza Márquez Mázmela, P. R. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú. *Revista Científica General José María Córdova, 20*(37), 209-224. https://dx.doi.org/10.21830/19006586.791

Publicado en línea: 1.º de enero de 2022

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL

Miles Doctus

Revista Científica General José María Córdova
(Revista Colombiana de Estudios Militares y Estratégicos)
Bogotá D.C., Colombia

Volumen 20, número 37, enero-marzo 2022, pp. 209-224
https://dx.doi.org/10.21830/19006586.791

Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de Perú

Validation of a cybercrime awareness scale in Peruvian university students

Edwin Hernán Ramírez Asís y Ricardo Enrique Toledo Quiñones
Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú

Roger Pedro Norabuena Figueroa
Universidad Nacional Mayor de San Marcos, Lima, Perú

Patricia Raquel Henostroza Márquez Mázmela
Pontificia Universidad Católica del Perú, Lima, Perú

Resumen. Este artículo presenta un análisis para clasificar los indicadores de conciencia sobre ciberdelito en los estudiantes de tres universidades de Perú mediante un cuestionario de veinte ítems medidos con la escala Likert, que fue aplicado a un total de 372 estudiantes mediante Google Forms. El análisis factorial exploratorio se aplicó a los datos recopilados, que dieron lugar a cuatro factores denominados: 1) conciencia sobre *phishing*, 2) conciencia sobre el *spamming*, 3) eficacia del *software* antivirus, y 4) *bullying* en la web. La escala de conciencia sobre el ciberdelito demostró que tiene una consistencia interna adecuada de ,892 del alfa de Cronbach para el instrumento general y las alfas de las subescalas van desde ,782 a ,861. Así, se logra determinar la validez y fiabilidad de la escala propuesta.

Palabras clave: análisis factorial; *bullying*; cibercrimen; jóvenes; *phishing*; seguridad de los datos

Abstract. This article presents an evaluation to classify cybercrime indicator awareness in students of three universities in Peru. To this end, it applied a twenty-item Likert scale questionnaire using Google Forms to a total of 372 students. Exploratory factor analysis was applied to the data collected, resulting in four factors: 1) phishing awareness, 2) spamming awareness, 3) antivirus software effectiveness, and 4) web bullying. The cybercrime awareness scale showed adequate internal consistency, presenting .892 in Cronbach's alpha for the overall instrument and a range from .782 to .861 in the subscales' alphas, thus, making it possible to determine the validity and reliability of the proposed scale.

Keywords: bullying; cybercrime; data security; factor analysis; phishing; youngsters

Sección: Inteligencia y Logística • Artículo de investigación científica y tecnológica

Recibido: 9 de abril de 2021 • Aceptado: 5 de septiembre de 2021

Contacto: Edwin Hernán Ramírez Asís ehramireza@unasam.edu.pe

Introducción

En la pandemia mundial actual, los estudiantes en todo el mundo han obligado a las instituciones académicas a adoptar un nuevo esquema de educación a través de la enseñanza en línea (García, 2020). Los esfuerzos que ello ha implicado requieren que los estudiantes utilicen las tecnologías de información y comunicación (TIC) como teléfonos celulares, computadoras y conexión a internet para conectarse con sus docentes, sus lecciones y sus compañeros de la universidad (Alcántara, 2020). Sorprendentemente, alrededor del 16 % de personas carecen de habilidades en las TIC, aun a pesar de su exposición a internet. Goel (2014) menciona que incluso a los internautas todavía les resulta difícil aprender con las TIC, aunque a nivel básico las utilicen. Esta situación genera varios escenarios de problemas que pueden obstaculizar la calidad del aprendizaje en línea.

Las generaciones actuales han vivido tremendas mejoras en los patrones de comunicación, pero probablemente las generaciones venideras contarán con mejores esquemas de interacción hombre-máquina (Padilla-Carmona et al., 2016; Silva et al., 2020). Los jóvenes ahora residen en mundos virtuales donde los datos y todo tipo de conocimiento se comparten, invitan y excluyen, comprenden y articulan (Yah, 2020). Estas formas modernas de contacto transforman las relaciones, y hace que las áreas de intimidad, tan ansiosamente cuidadas por nuestras generaciones, tiendan a ser más exhibidas ahora. Por ello, es en estos espacios donde las personas deberíamos probar la formación y práctica de valores (Ferro-Veiga, 2020).

La expansión de la tecnología a través de los dispositivos móviles y las redes sociales conduce a desarrollar un ambiente ideal para múltiples formas de ciberdelincuencia y la distribución de información ilícita en internet. Zúñiga (2018) plantea que el público en general no es lo suficientemente consciente de la gravedad de los delitos cibernéticos ni conoce cómo prevenirlos. Esto crea problemas y desafíos que, según Vajagathali et al. (2019), incluyen la coerción cibernética, la descarga ilegal, la piratería informática y la piratería de *software*, entre otros delitos calificados como ciberdelincuencia. Esta es una amenaza significativa en todos los ámbitos, incluyendo la defensa nacional, el orden estatal y los derechos de privacidad (Fernández & Martínez, 2018). Lamentablemente, los informes que circulan en la web presentaron a algunos estudiantes, profesionales y celebridades de la televisión acosados por los ciberdelincuentes.

En este sentido, las tecnologías experimentan mejoras y desarrollos constantes, y son una parte cada vez más importante de nuestra vida cotidiana y del funcionamiento de las instituciones (Martínez, 2020). Pero estos desarrollos aumentan las posibilidades del ciberdelito, ya que internet ahora es una de las tecnologías más utilizadas y uno de los principales canales de solicitud de información y negocios. Asimismo, impulsado por el Ambisyon Natin 2040, que promueve la visión de moldear a los estudiantes para que se desenvuelvan en el mundo real con mayores competencias, se hace necesario aprender y aplicar habilidades de TIC (López et al., 2019). Así, este artículo presenta una investi-

gación centrada en la exploración de los factores de conciencia sobre el ciberdelito desde la percepción de los estudiantes universitarios, utilizando un análisis factorial exploratorio que se centra en el análisis de los factores subyacentes de una escala de conciencia sobre el ciberdelito construido en equipo. El propósito central del análisis es evaluar las propiedades psicométricas de la escala de conciencia sobre ciberdelito en los estudiantes universitarios, con el fin de mostrar su relevancia y confiabilidad.

Marco teórico

Existen estudios que incluyen como factores relacionados con la ciberdelincuencia la falta de formación y educación adecuadas, y un bajo nivel de conciencia sobre el ciberdelito (Goel, 2014; Fuster-Guillén et al., 2020); la falta de legislación inclusiva y poco conocimiento sobre las políticas de seguridad en internet en las organizaciones (Pons, 2017), y el perfil sexual (Senthilkumar & Easwaramoorthy, 2017). Igualmente, una encuesta realizada por Muniandy et al. (2017) reveló un comportamiento insatisfactorio de los participantes hacia la ciberseguridad. En palabras de Potgieter (2019), los estudiantes deben estar preparados y conscientes de la intervención de protección de datos para evitar ser víctimas de la ciberdelincuencia. Al respecto, las campañas de conocimiento pueden desarrollar una cultura de seguridad proactiva de la información (Da Veiga, 2016). Sin embargo, es bastante desafortunado que el ciberdelito se haya convertido en un concepto culturalmente aceptado; la gente ha comenzado a cometer un delito y practicar esta técnica. Por lo tanto, se requiere con urgencia examinar y monitorear este fenómeno, especialmente en el contexto de la nueva normalidad de la educación superior en el país, que requiere que los estudiantes y profesores utilicen internet y otras infraestructuras digitales para transferir cualidades y aprendizaje (Tossi, 2017).

En general, las amenazas de internet se pueden dividir en dos grupos diferentes. En primer lugar, los desafíos a los derechos legales existentes, cuya característica proviene de la aplicación de tecnología emergente (Ferro-Veiga, 2020); y en segundo lugar, las amenazas a, por ejemplo, las propias infraestructuras electrónicas, que tienen el objetivo de modificar o evitar el funcionamiento habitual de los sistemas de información. Estos son los peligros que surgen del uso de *software* espía (rastreadores) y de vigilancia automatizada (*cookies*, *software* espía). Dichos eventos se presentan comúnmente en actividades como el acceso no autorizado, la distribución de programas informáticos peligrosos y la denegación intencional de accesos al servicio en internet que perturban los servicios disponibles y pueden provocar daños a los portales de las organizaciones que operan con sus clientes y usuarios a través de internet (Barrios, 2017).

Así mismo, los instrumentos implementados por los ciberdelincuentes se han desarrollado más o igual que el avance tecnológico, similar a los virus informáticos. Lenhart et al. (2015) indican que los ciberdelincuentes corrompieron inicialmente las computadoras de sus víctimas al portar virus a través de medios de almacenamiento de datos, mientras

que en la actualidad el delito cibernético se realiza mediante internet (Tejo et al., 2021). El uso de internet se ha expandido en los últimos cinco años, lo cual ha generado un aumento constante en la cantidad de eventos de ciberdelitos.

Por otro lado, Cumbreras (2020) aporta sobre las modalidades de robo por parte de los ciberdelincuentes. En las primeras fases de las amenazas de internet, los atacantes cibernéticos tienden a piratear las redes de bases de datos para obtener acceso a ellas. Por lo tanto, los autores de robos informáticos y delitos cibernéticos se dan cuenta de que el dinero está en cuentas bancarias, así que principalmente quieren piratear las computadoras utilizadas para las interacciones entre el usuario y la banca. El segundo delito más común es el fraude de identidad para las empresas y las personas. El tercer delito más común es el acceso abusivo a los sistemas de información. En cuarto lugar, existen transferencias patrimoniales no consensuadas, comportamientos delictivos que permiten robar dinero al atacante o transferir valiosos activos financieros de las víctimas. Al respecto, según López et al. (2018), los principales tipos de ciberdelitos y los aspectos en los que se debe crear conciencia sobre ciberdelito son: conciencia sobre el *phishing*, conciencia sobre el *spamming*, eficacia del *software* antivirus y *bullying* en la web.

Las personas que cometen este tipo de delitos se denominan piratas informáticos, y normalmente son profesionales inteligentes y de alto nivel informático (Sancho, 2017). El aumento en el número de computadoras y dispositivos móviles inteligentes en todo el mundo, así como el aumento de la conectividad de redes integradas en casi todos los países a través de internet, han propiciado el aumento de los piratas informáticos (Ferro-Veiga, 2020). La seguridad de los datos, por otro lado, tiene tres piedras angulares: secreto, integridad y disponibilidad (Cujabante et al., 2020). El primero es la privacidad en referencia al valor que se logra al tener los datos reservados solo para los usuarios dentro de una red de bases de datos; la integridad tiene el objetivo de mantener intactas todas las pruebas, y la disponibilidad permite que el material pueda estar accesible en cualquier momento para su consulta.

Metodología

Esta investigación exploratoria cuantitativa utiliza un marco de validez predictiva para examinar los factores de conciencia sobre el ciberdelito entre los estudiantes peruanos de la Universidad Nacional Santiago Antúnez de Mayolo, la Universidad San Pedro y la Universidad Católica Los Ángeles de Chimbote en Perú. Los jóvenes entre 15 y 25 años usan con mayor frecuencia los medios digitales para realizar compras por internet, por lo que tienen una mayor predisposición a ser víctimas del ciberdelito. Dado que esta población se encuentra en su mayoría estudiando en las universidades, se considera dicha muestra como idónea para poder validar el instrumento utilizado en este estudio. El método también profundiza en la evaluación de la fiabilidad de los factores derivados con referencia al valor alfa de Cronbach mínimo del ,70, un total de 372 encuestados de

cuatro facultades (ciencias empresariales, ingeniería, ciencias de la salud y educación). Se adquirieron las autorizaciones necesarias antes de la recopilación de datos. Asimismo, se informó a los estudiantes sus derechos y el contenido del cuestionario, por lo que suscribieron un consentimiento informado.

Debido a la falta de instrumentos disponibles en internet, el equipo investigador se vio obligado a hacer una recolección cualitativa de artículos para ser incluidos en el instrumento a través del modo de *crowdsourcing* en línea en Facebook con una pregunta "¿Cómo sería su conciencia hacia el ciberdelito y su impacto en su educación?" Se derivó un total de sesenta respuestas cualitativas, las cuales se analizaron mediante procedimientos de codificación. Surgieron cuatro categorías principales de ciberdelito basadas en el análisis de contenido de las respuestas: ciberdelito contra individuos, contra la propiedad, contra una organización y contra la sociedad. Por lo tanto, se construyó una escala de 20 ítems sobre el conocimiento del ciberdelito. Este instrumento contiene declaraciones sometidas a una adecuada validación entre tres expertos, y posteriormente se distribuyó entre los 372 encuestados utilizando un formulario electrónico a través de Google Forms.

Al analizar los datos, se codificaron todas las respuestas con 1 para totalmente en desacuerdo; 2, en desacuerdo; 3, neutral; 4, de acuerdo, y 5, totalmente de acuerdo. Entre las 372 respuestas se utilizó la opción buscar y reemplazar de Microsoft Excel, y luego se exportó el archivo en el *software* SPSS versión 26 para su análisis. Se comprobaron los datos en busca de respuestas perdidas (Quezada, 2019).

Para el primer objetivo, se utilizó el análisis de componentes principales con una gran muestra, establecida como una salvaguarda para establecer la consistencia del resultado (Supo & Zacarías, 2020). Para el segundo objetivo, dado que en la investigación se optó por descubrir las diferencias significativas de perfil sobre los factores derivados, se ejecutó la prueba de análisis de varianza multivariante bidireccional mediante SPSS V26 con el perfil como variables independientes y las puntuaciones de los factores como variables dependientes. Para el tercer objetivo de examinar el poder del instrumento en la predicción de la conciencia del delito cibernético, se empleó un análisis de función discriminante.

Resultados

Factores de concienciación sobre la ciberdelincuencia

El primer análisis de factores exploratorios se llevó a cabo con la escala de 20 ítems para medir la conciencia sobre el ciberdelito. Como el tamaño de la muestra es de 372, se llevó a cabo una prueba preliminar que involucró las pruebas de Kaiser-Mayer-Olkin (KMO) y Bartlett. La medida general de KMO de adecuación de muestreo fue de ,659 y la prueba de esfericidad de Bartlett fue inferior a ,05. Con base en estos resultados, se logra definir que el análisis factorial en la muestra estudiada es correcto. Utilizando el análisis de com-

ponentes principales a través de métodos de rotación Varimax se obtuvo una solución de cuatro factores (valores propios superiores a 1), que explicó aproximadamente el 65 % de la varianza total. Los 20 ítems se incluyeron debido a que su carga factorial era superior a ,600 (Ledesma et al., 2019), lo que muestra una validez adecuada de la escala.

Después de analizar los elementos incluidos en cada componente, los cuatro factores son: conciencia sobre el *phishing* (autovalor = 5,284, α = ,861), conciencia sobre el *spamming* (autovalor = 2,892, α = ,799), eficacia percibida del *software* antivirus (autovalor = 2,576, α = ,782) y *bullying* en la web (autovalor = 1,981, α = ,839). En la Tabla 1 también se muestran los resultados del cálculo del alfa de Cronbach, que nos permite identificar si una escala es o no confiable. Para el caso del instrumento analizado, se aprecia que los cuatro factores tienen niveles adecuados de fiabilidad, ya que todos son superiores al ,70 (Supo & Zacarías, 2020).

Tabla 1. Cargas factoriales según en el análisis de componentes principales

Declaraciones sobre el ciberdelito	Carga factorial	Autovalores	% de varianza	Factores
Creo que es difícil identificar un sitio web fraudulento.	,789	5,284	28,789	Conciencia sobre el *phishing* (α = ,861)
Me importa comprar el mejor *software* antivirus.	,786			
Sé cuáles son los datos de mi tarjeta que no debería ingresar en ningún sitio web sospechoso.	,767			
Conozco algunas de las leyes sobre ciberdelitos.	,757			
Me protejo del ciberdelito.	,684			
En general, no confío en los sitios web que me piden que ingrese datos sobre mi tarjeta bancaria.	,671			
Cuando estoy en línea, identifico claramente mi espacio permisible y prohibido a los demás.	,653			
Creo que estoy protegido de los ciberdelitos.	,791	2,892	14,873	Conciencia sobre el *spamming* (α = ,799)
Creo que descargar cualquier archivo de cualquier sitio web siempre es seguro.	,766			
Haría clic en cualquier enlace que reciba por correo electrónico/SMS.	,692			
Creo que soy capaz de identificar un correo electrónico o sitio web fraudulento.	,625			

Continúa tabla...

Declaraciones sobre el ciberdelito	Carga factorial	Autovalores	% de varianza	Factores
Creo que un ciberdelito solo afecta el espacio virtual.	,811	2,576	12,968	Eficacia del *software* antivirus (α = ,782)
Creo que los antivirus son suficientes para protegerme de un delito cibernético.	,768			
Utilizo otros métodos distintos del *software* antivirus para protegerme de los ciberdelitos.	,745			
Haría clic en los archivos con alerta de antivirus.	,693			
Cuento con antivirus pagado oficialmente.	,652			
Confío en cualquier sitio web que me pida que introduzca los datos de mi cuenta bancaria.	,791	1,981	8,972	*Bullying* en la web (α = ,839)
Creo que las grandes empresas son las únicas víctimas del ciberdelito.	,787			
Creo que solo las personas con mucho dinero son las únicas víctimas del ciberdelito.	,746			
He experimentado ser víctima de un delito cibernético.	,648			

Fuente: Elaboración propia

Prueba entre los niveles de perfiles destacados y los factores derivados

El análisis multivariado de la varianza (Manova) se utilizó en el análisis de los factores demográficos seleccionados, con el sexo y la facultad a la que pertenece el estudiante como las variables independientes. Las cuatro dimensiones de la conciencia sobre ciberdelito (CSC) se introdujeron como variables dependientes.

Se empleó la prueba M de Box de igualdad de las matrices de covarianza para probar la suposición sobre el uso de Manova. Los hallazgos indican una diferencia estadísticamente significativa en las matrices de covarianza, de ahí el uso de traza de Pillai para una prueba multivariante, y la prueba Scheffe para múltiples comparaciones establecidas en ,001.

El resultado del Manova encontró diferencias estadísticamente significativas en los cuatro factores de CSC y las facultades (traza de Pillai = ,683, F [3, 372] = 11,144, p < ,001,

η2 = ,236). El sexo se encontró no significativo (traza de Pillai = ,071, F [3, 372] = 2,890, *p* > ,001, η2 = ,236), y el efecto de interacción del sexo y las facultades fue significativo (traza de Pillai = ,242, F [3, 372] = 3,235, *p* < ,001, η2 = ,087). Estos hallazgos implican que el sexo afecta la conciencia del ciberdelito de los estudiantes universitarios alrededor de un 23,60 %, mientras que la interacción entre el sexo y la facultad afecta la puntuación de factores en alrededor de un 8,70 %.

Además, la Tabla 2 refleja la importancia de la prueba de los factores que utilizan los efectos entre sujetos de sexo-facultad. Los resultados encontraron que el factor 4 (*bullying* en la web) es la variable más relevante entre las cuatro dimensiones para comparar entre facultades en alrededor de 10,5 % (MS = 4,668, F [3, 372] = 7,459, *p* < ,001, η2 = ,105).

Tabla 2. Significación de la prueba de Scheffe del factor 4 comparando entre facultades

Facultades		Diferencia de medias	*P*	Interpretación
Ingeniería	Ciencias económicas	,842	,017	Significativo
	Ciencias de la salud	,146	,876	No significativo
	Educación	,088	,943	No significativo
Ciencias empresariales	Ciencias de la salud	–,691	,036	Significativo
	Educación	–,730	,074	No significativo
Ciencias de la salud	Educación	–,049	,866	No significativo

Sexo-facultad (*p* = ,000); factor 4 (*p* = ,000) significativo.

Fuente: Elaboración propia

La prueba de Scheffe reveló diferencias significativas en el conocimiento del ciberdelito en términos del factor 4 (*bullying* en la web) para estudiantes de la facultad de ingeniería y ciencias empresariales (diferencia de medias = ,837, *p* = ,017), y los encuestados de la facultad de ciencias empresariales y la facultad de ciencias de la salud (diferencia de medias = –,691, *p* = ,036). Del mismo modo, el resultado mostró que los estudiantes de la facultad de ingeniería tienen mejor conciencia del ciberdelito en comparación con otras facultades. En comparación, los de la facultad de ciencias empresariales retrataron la conciencia más deficiente sobre el ciberdelito.

Predicción de las capacidades de la escala de conciencia sobre el ciberdelito

Los resultados del análisis discriminante de la función se observan en la Tabla 3 después de emplear el análisis de corrección de Bonferroni, que reveló tres funciones discriminantes.

La primera función explica el 74,60 % de la variación, R^2 canónico = ,728; el segundo explica el 21,3 % de la varianza, R^2 canónico = ,502; mientras que el tercero explica solo el 4,10 %, R^2 canónico = ,247. En combinación, estas funciones discriminatorias identificaron diferencias significativas en la conciencia sobre ciberdelito de los estudiantes universitarios, χ^2 (15) = 214,606, p = ,000. Después de eliminar la primera función, la segunda función también mostró diferencias significativas en la conciencia de ciberdelito de los grupos, χ^2 (8) = 68,378, p = ,000. Sin embargo, después de eliminar la primera y segunda función, la tercera función no identifico diferencias significativas en la conciencia de ciberdelito de los grupos, χ^2 (3) = 12,228, p = ,007. Por lo tanto, la herramienta no había mostrado discriminación entre los estudiantes de diferentes facultades.

Tabla 3. Análisis de funciones discriminante

Función	λ de Wilks	% de varianza	Correlación canónica	df	χ2	*P*	Interpretación
1 a través de 3	,330	74,6	,728	15	214,606	,000	Significativo
2 a través de 3	,702	21,3	,502	8	68,378	,000	Significativo
3	,939	4,1	,247	3	12,228	,007	No significativo

Fuente: Elaboración propia

Hay varias maneras en que la conciencia sobre el ciberdelito se puede utilizar para mejorar la experiencia de aprendizaje digital de los estudiantes. Dicha conciencia sirve como una herramienta que mide los niveles de seguridad y el impacto del ciberdelito en los estudiantes de varias facultades. Esto facilitará una comprensión holística de las experiencias de los estudiantes y ayudará a identificar cuáles de los cuatro factores tienen el mayor impacto en la experiencia de seguridad de los estudiantes. En general, esta herramienta se puede utilizar para comparar los índices de conciencia sobre el ciberdelito de las universidades sobre los cuatro factores. Por lo tanto, se puede replicar.

Discusión

Factor 1: conciencia sobre *phishing*

Esta primera dimensión de la escala de conciencia sobre el ciberdelito, que describe el 28,789 % de los elementos, contiene siete elementos: "Creo que es difícil identificar un sitio web fraudulento", con una carga factorial de ,798, seguido de "Me importa comprar el mejor *software* antivirus", con una carga factorial de ,768. Los estados de cuenta retratan casos sobre transacciones en línea que requieren información confidencial como tarjetas bancarias y espacios privados, con cargas de factoriales entre ,767 y ,653.

Estos hallazgos están relacionados con lo reportado por Cheng et al. (2020), que indica que los estilos de vida en línea de los usuarios son el componente clave del ciberdelito. Nagalingam et al. (2015) revelaron un bajo nivel de conciencia sobre los intentos de *phishing* con factores primos, incluyendo el pasar por alto, la falta de conciencia sobre la banca en línea y la negligencia personal. Por su parte, en un estudio de encuesta, Díaz et al. (2020) mostraron cómo alrededor del 59 % de los estudiantes que han abierto un correo electrónico de *phishing* hicieron clic en su enlace fraudulento, y una asociación significativa entre varios factores demográficos y la susceptibilidad de un estudiante a un ataque de *phishing*. Quiroz-Zambrano y Macías-Valencia (2017), a través de una herramienta de concienciación sobre la información, dieron a conocer que los hombres comienzan a llevar el conocimiento con seguridad a través de la autoenseñanza, mientras que las mujeres tienden a preferir el crédito académico e interactuar en sus círculos sociales. De igual forma, Espinoza-Sánchez (2019) señaló la falta de recursos para combatir y salvaguardar a los estudiantes contra la ciberdelincuencia.

Por consiguiente, estos hallazgos y estudios relacionados resaltan la urgencia de que el sector educativo promueva el diseño de sistemas altamente seguros y proporcione capacitación en ciberseguridad a los estudiantes antes de involucrarlos en cualquier plataforma de educación digital. Dar a los estudiantes las habilidades y conocimientos sobre cómo protegerse contra las amenazas cibernéticas y los intentos de *phishing* les permitirá saber lo que deben hacer en el futuro.

Factor 2: conciencia sobre el *spamming*

Esta segunda dimensión de la escala de conciencia sobre el ciberdelito describe el 14,873 % de los elementos. La escala contiene cuatro elementos: "Creo que estoy protegido de los ciberdelitos", con una carga factorial de ,791, seguido de "Creo que descargar cualquier archivo de cualquier sitio web siempre es seguro", con una carga factorial de ,766. El resto de las instrucciones muestran casos de reventado de enlaces e invitaciones innecesarias, con cargas factoriales entre ,692 y ,625.

En un estudio realizado por Dada et al. (2019), se mostró que alrededor del 14,3 % del tráfico de correo electrónico monitoreado en 2019 es un spam, lo que conduce a una mala conciencia del usuario, como hacer clic en el enlace recibido creyendo que es un correo electrónico legítimo del proveedor. Esto, según Asghar et al. (2020), aumentará el miedo de la gente a entrar a sitios web y otros servicios. Suárez (2018) descubrió una proporción muy pequeña de participantes que reconocieron dos objetos sospechosos en relación con los encuestados que detectaron solo uno. Además, Roy et al. (2020) indicaron en su estudio el grave problema causado por spam a personas, organizaciones y proveedores de servicios. A pesar de la alta conciencia de las personas hacia el spam, todavía puede pasar debido a descuentos prometedores y precios baratos u ofertas especiales (Sancho, 2017; Tejo et al., 2021).

Esto permite reconocer que el spam es un problema que contribuye a fomentar diversas actividades ilegales en el sector educación. Los resultados de estudios relacionados indican la naturaleza degenerativa pero creciente del estado de los correos electrónicos estafa en todo el mundo. En suma, es necesario educar a los estudiantes en identificar estafas por correo electrónico y seguir prácticas preventivas ampliamente reconocidas, como nunca seguir un enlace dentro de un correo electrónico no especificado, o nunca compartir ninguna información personal.

Factor 3: eficacia del *software* antivirus

La tercera dimensión de la escala de conciencia sobre el ciberdelito, que describe el 12,968 % de los elementos, contiene cinco elementos: "Creo que un ciberdelito solo afecta el espacio virtual", con una carga factorial de ,811, seguido de "Creo que los antivirus son suficientes para protegerme de un ciberdelito", con una carga factorial de ,768, y "Utilizo otros métodos distintos del *software* antivirus para protegerme de los ciberdelitos", con una carga factorial de ,745. Estas declaraciones retratan la necesidad de utilizar un *software* antivirus y de conectar las opciones "permitidas" para aplazarse a sí mismo en la confirmación o evitar ser atacado por los ciberdelincuentes.

En un estudio empírico de Rodríguez et al. (2017) se reveló la ineficacia de un *software* antivirus comercial en la detección de todas las formas actuales de *malware*. Además, Sharif et al. (2019) descubrieron varios conceptos erróneos entre los expertos sobre el uso de *software* antivirus que pueden exponer a los usuarios a riesgos en términos de legitimidad, costo e interacción eco-web. Es bastante alarmante observar que la tasa de detección inicial de un virus recién creado es inferior al 7 % (Aminu et al., 2020). Schaik et al. (2017) encontraron que la mayoría de las organizaciones esperan un ataque sustancial antes de implementar políticas antivirus serias e instalar *software* de análisis de virus. Estos estudios revelaron que la mayoría de los productos antivirus en el mercado no podían mantenerse al día con la propagación del virus en internet.

No es un secreto que muchas personas han perdido información y han perdido una gran cantidad de tiempo tratando de recuperarse después de que un virus logró infectar sus computadoras. Esto implica la relevancia de invertir en *software* legítimo y herramientas educativas que mantendrán un ojo y oído para monitorear el acceso de archivos y conversaciones, especialmente en la digitalización del aula en la pandemia. Se debe recordar a los estudiantes que realicen análisis del equipo en busca de virus potenciales con frecuencia.

Factor 4: acoso a través de la ciberdelincuencia

La cuarta y última dimensión de la escala de conciencia sobre el ciberdelito, que describe el 8,972 % de los artículos, se calificó como "*bullying* en la web". Contiene cuatro elementos: "Confío en cualquier sitio web que me pida que entre en el detalle de mi cuenta bancaria", con la mayor carga de ,791, seguido de "Creo que las grandes empresas son las

únicas víctimas del ciberdelito", con una carga factorial de ,787, y "He experimentado ser víctima de un ciberdelito", con una carga factorial de ,648. Esto refleja la cultura existente del acoso en el mundo cibernético.

La literatura ha declarado varios casos de ciberacoso en todo el mundo. Por ejemplo, Lenhart et al. (2015) declaró un aumento del 87 % de los casos de ciberacoso entre los estudiantes de secundaria debido a su uso mejorado de dispositivos electrónicos. Rivadulla y Rodríguez (2019) mencionan que el uso de internet durante más de cuatro horas al día se asocia con una mayor probabilidad de ser víctima de ciberacoso. Por su parte, Marín-Cortés (2020) reveló que las estudiantes mujeres son víctimas más que los hombres a través de insultos y estar sujetas a rumores. Además, Méndez et al. (2019) describieron que solo cuatro de cada diez estudiantes reportarían que fueron ciberacosados, debido al anonimato del acosador. Además, la posibilidad de ser ridiculizados o restringidos en su uso de la tecnología afecta el rendimiento de los estudiantes (Larrañaga et al., 2018).

Dado el impacto significativo del ciberacoso, como se afirma en los hallazgos y estudios relacionados, los estudiantes tienen una mayor probabilidad de sufrir por esta causa y ver afectados sus estados de salud física y emocional, lo que puede convertirse en barreras para el funcionamiento adecuado del sistema universitario (Ramírez et al., 2020). En este sentido, dado que la apertura de clases se realiza a través de modos digitales, algunos alumnos se enfrentarán al acoso de otras personas en la web, sin tener ni idea de quiénes son. De hecho, esto implica la responsabilidad de cada institución académica, como las universidades, para abordar el impacto potencial del ciberacoso tanto en estudiantes ciberacosadores como víctimas.

Este estudio posee limitaciones notables, como las características de los estudiantes universitarios, ya que claramente no describe las percepciones de estudiantes en los otros niveles como primaria o secundaria. Por esa razón, se recomienda que futuras investigaciones puedan considerar la población de estudiantes de primaria o secundaria, debido a que, en la actualidad, esta población también es propensa a ser víctima de los ciberdelitos.

Conclusión

Con base en los resultados de este estudio, se concluye que el uso del análisis de componentes principales reveló cuatro factores válidos de conciencia sobre el ciberdelito según lo perciben los estudiantes universitarios: conciencia sobre el *phishing*, conciencia sobre el *spamming*, la eficacia percibida del *software* antivirus y el acoso en la web. La Manova bidireccional mostró que existe una interacción entre el sexo y la facultad a la que pertenece el estudiante cuando se relaciona con el factor 4 de ciberdelito llamado "*bullying* en la web". Además, entre los estudiantes de las cuatro facultades se encontraron diferencias significativas en la conciencia del ciberdelito, dado que los estudiantes de ingeniería tienen una mejor conciencia sobre ciberdelito respecto a las demás facultades. Por último, el resultado del análisis de funciones discriminatorias asegura que la escala desarrollada de conciencia

sobre ciberdelito puede servir para identificar y tomar medidas sobre el pensamiento del ciberdelito en estudiantes universitarios. En este sentido, se recomienda la aplicación de esta herramienta en la evaluación de la conciencia sobre ciberdelito de los estudiantes universitarios considerando los cuatro factores identificados, puesto que se logró determinar que esta escala evidencia validez y confiabilidad.

Finalmente, a pesar de las limitaciones del estudio por tratarse de una población homogénea en una ciudad peruana, es recomendable continuar con esta línea de investigación y ampliar el análisis a poblaciones de otros países. Otra alternativa es iniciar estudios en los trabajadores tanto del sector público como privado, puesto que también son una población que utiliza con mayor frecuencia el internet y, por tanto, corren el riesgo de ser víctimas del ciberdelito.

Agradecimientos

Los autores desean agradecer a la Universidad Nacional Santiago Antúnez de Mayolo, la Universidad San Pedro y la Universidad Católica Los Ángeles de Chimbote por su apoyo en la realización de este artículo.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Edwin Hernán Ramírez Asís es doctor en administración, magíster en ciencias económicas y licenciado en administración. Es profesor investigador reconocido por el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica de Perú. Sus intereses de investigación son el comportamiento organizacional y los sistemas de seguridad y salud ocupacional.

https://orcid.org/0000-0002-9918-7607 - Contacto: ehramireza@unasam.edu.pe

Roger Pedro Norabuena Figueroa es doctor y licenciado en estadística, especialista en modelos de ecuaciones estructurales. Es investigador y docente principal en la Universidad Nacional Mayor de San Marcos, Lima (Perú). Realiza investigaciones multidisciplinarias en el modelo de predicción de comportamiento humano.

https://orcid.org/0000-0003-3731-9843 - Contacto: rnorabuenaf@unmsm.edu.pe

Ricardo Enrique Toledo Quiñones es doctor en economía, magíster en ciencias económicas con mención en gestión empresarial y licenciado en administración. Especialista en gestión y dirección de proyectos de inversión. Es investigador y docente principal de la

Facultad de Administración y Turismo de la Universidad Nacional Santiago Antúnez de Mayolo (Perú).

https://orcid.org/0000-0003-4834-5959 - Contacto: rtoledoq@unasam.edu.pe

Patricia Raquel Henostroza Márquez Mázmela es magíster en administración estratégica de empresas y licenciada en administración. Especialista en riesgos financieros por la Universidad Peruana de Ciencias Aplicadas (Perú). Certificada como analista de inversiones por la Bursen de la Bolsa de Valores de Lima, Perú. Es docente de Centrum de la Pontificia Universidad Católica del Perú.

https://orcid.org/0000-0002-1816-1617 - Contacto: patricia.henostroza@pucp.pe

Referencias

Alcántara Santuario, A. (2020). Educación superior y COVID-19: una perspectiva comparada. En H. Casanova (Ed.), *Educación y pandemia: una visión académica* (pp. 75-82). Universidad Nacional Autónoma de México. https://bit.ly/3wHtwyX

Aminu, S. A., Sufyanu, Z., Sani, T., & Idris, A. (2020). Evaluating the effectiveness of antivirus evasion tools against windows platform. *Fudma Journal of Sciences, 4*(1), 112-119. https://bit.ly/3mQo7Tb

Asghar, M. Z., Ullah, A., Ahmad, S., & Khan, A. (2020). Opinion spam detection framework using hybrid classification scheme. *Soft Computing, 24*(5), 3475-3498. https://doi.org/10.1007/s00500-019-04107-y

Barrio, M. (2017). *Ciberdelitos: amenazas criminales del ciberespacio*. REUS Editorial.

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior, 108*, 106311. https://doi.org/10.1016/j.chb.2020.106311

Cujabante, X. A., Bahamón, M. L., Prieto, J. C., & Quiroga, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357-377. http://dx.doi.org/10.21830/19006586.588

Cumbreras, M. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad, 16*, 151-162. https://bit.ly/3pL9WR4

Dada, E., Bassi, J., Chiroma, H., Adetunmbi, A., & Ajibuwa, O. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon, 5*(6), e01802. https://doi.org/10.1016/j.heliyon.2019.e01802

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24*(2), 139-151. http://dx.doi.org/10.1108/ICS-12-2015-0048

Díaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia, 44*(1), 53-67. https://doi.org/10.1080/01611194.2019.1623343

Espinoza-Sánchez, J. F. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. *La Razón Histórica: Revista Hispanoamericana de Historia de las Ideas Políticas y Sociales, 44*, 153-173. https://bit.ly/2PRhPFn

Fernández, D., & Martínez, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia*. Thomson Reuters Aranzadi.

Ferro-Veiga, J. M. (2020). *Seguridad informática: aspectos generales y especiales* [ebook]. S. d.

Fuster-Guillén, D., Ocaña, Y., Salazar, D., & Ramírez, E. (2020). Human development and family integration: Study from the comprehensive service of the elderly in Peru. *Revista Venezolana de Gerencia, 25*(90), 477-490. https://doi.org/10.37960/rvg.v25i90.32392

García Aretio, L. (2020). COVID-19 y educación a distancia digital: preconfinamiento, confinamiento y posconfinamiento. *RIED. Revista Iberoamericana de Educación a Distancia, 24*(1), 9-32. https://doi.org/10.5944/ried.24.1.28080

Goel, U. (2014). Awareness among B. Ed teacher training towards Cyber-crime. A Study. *Learning Community. An International Journal of Educational and Social Development, 5*(2-3), 107-117. https://bit.ly/3sTxTHR

Larrañaga, E., Navarro, R., & Yubero, S. (2018). Factores socio-cognitivos y emocionales en la agresión del ciberacoso. *Comunicar: Revista Científica de Comunicación y Educación*, 26(56), 19-28. https://doi.org/10.3916/C56-2018-02

Ledesma, R. D., Ferrando, P. J., & Tosi, J. D. (2019). Uso del análisis factorial exploratorio en RIDEP. Recomendaciones para autores y revisores. *Revista Iberoamericana de Diagnóstico y Evaluación–e Avaliação Psicológica, 52*(3), 173-180. https://doi.org/10.21865/RIDEP52.3.13

Lenhart, A., Duggan, M., Perrin, A., Stepler, R., Rainie, L., & Parker, K. (2015). *Teens, social media & technology overview 2015*. Pew Research Center. https://pewrsr.ch/3dQVPT0

López, J., De Veyra, C., Geroy, L., Sales, R., Dizon, T., & Cutiongco, E. (2019). Envisioning the health research system in the Philippines by 2040: a perspective inspired by AmBisyon Natin 2040. *Acta Medica Philippina, 53*(3). https://doi.org/10.47895/amp.v53i3.148

López, A., López, L., & Yedra, R. (2018). Factores que contribuyen a la prevención de los delitos informáticos en el estado de Tabasco. *Gênero & Direito, 6*(3). https://doi.org/10.22478/ufpb.2179-7137.2017v6n3.37410

Marín-Cortés, A. (2020). Las fuentes digitales de la vergüenza: experiencias de ciberacoso entre adolescentes. *The Qualitative Report, 25*(1), 166-180. https://bit.ly/3dOUWKU

Martínez, E. E. (2020). Delitos cibernéticos. *Transregiones, 2*(2), 93-104. https://bit.ly/3dQW0h8

Méndez, I., Ruiz E., C., Martínez, J., & Cerezo, F. (2019). Ciberacoso según características sociodemográficas y académicas en estudiantes universitarios. *Revista Española de Pedagogía, 77*(273), 261-276. https://bit.ly/3t4ta3s

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity, 2017*, 800299. https://doi.org/10.5171/2017.800299

Nagalingam, V., Narayana, G., Rabiah, A., Nurazean, M., & Roslina, I. (2015). Identifying the level of user awareness and factors on phishing attempt among students. *Advanced Science Letters, 21*(10), 3243-3247. https://doi.org/10.1166/asl.2015.6520

Padilla-Carmona, M., Suárez-Ortega, M., & Sánchez-García, M. (2016). Inclusión digital de los estudiantes adultos que acceden a la universidad: análisis de sus actitudes y competencias digitales. *Revista Complutense de Educación, 27*(3), 1229-1246. https://doi.org/10.5209/rev_RCED.2016.v27.n3.47669

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO: Revista Latinoamericana de Estudios de Seguridad, 20*, 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Potgieter, P. (2019). The awareness behaviour of students on cyber security awareness by using social media platforms: a case study at Central University of Technology. En K. Njenga (Ed.), *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019* (vol. 12, pp. 272-280). Kalpa Publications in Computing. https://doi.org/10.29007/gprf

Quezada, N. (2019). *Metodología de la investigación*. Editorial Macro.

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(3), 676-688. https://bit.ly/3sUDEoV

Ramírez, E. H., Colichón, M. E., & Barrutia, I. (2020). Rendimiento académico como predictor de la remuneración de egresados en Administración, Perú. *Revista Lasallista de Investigación, 17*(2). https://bit.ly/3sMQOE6

Rivadulla López, J. C., & Rodríguez Correa, M. (2019). Ciberacoso escolar: experiencias y propuestas de jóvenes universitarios. *RIED. Revista Iberoamericana de Educación a Distancia, 22*(2), 179-201. https://doi.org/10.5944/ried.22.2.23541

Rodríguez, J. A., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. *URVIO: Revista Latinoamericana de Estudios de Seguridad, 20*, 63-79. http://dx.doi.org/10.17141/urvio.20.2017.2583

Roy, P. K., Singh, J. P., & Banerjee, S. (2020). Deep learning to filter SMS Spam. *Future Generation Computer Systems, 102*, 524-533. https://doi.org/10.1016/j.future.2019.09.001

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. *URVIO. Revista Latinoamericana de Estudios de Seguridad, 20*, 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559. https://doi.org/10.1016/j.chb.2017.05.038

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering, 263*(4), 042043. https://doi.org/10.1088/1757-899X/263/4/042043

Sharif, M., Roundy, K., Dell'Amico, M., Gates, C., Kats, D., Bauer, L., & Christin, N. (2019). A field study of computer-security perceptions using anti-virus customer-support chats. En *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (paper 78). https://doi.org/10.1145/3290605.3300308

Silva, D., Fuster, D., Norabuena, R., Ramírez, E., & Aguirre, A. (2020). Efectos del aprendizaje basado en problemas en la competencia instrumental traductora. *Apuntes Universitarios, 10*(3), 16-36. https://doi.org/10.17162/au.v10i3.455

Suárez, E. (2018). Algoritmo Machine Learnig en los sistemas de filtrado caso práctico SPAM de google en las cuentas de correo Institucionales de la FAFI. *Pro Sciences: Revista de Producción, Ciencias e Investigación, 2*(12), 17-23.

Supo, J., & Zacarías, H. (2020). *Metodología de la investigación científica: para las ciencias de la salud y las ciencias sociales*. Sincie.

Tejo-Machado, N., Rodrigues-Martinez-Basile, F., Cezar-Amate, F., & Ramírez-López, L. (2021). Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. *Revista Científica General José María Córdova, 19*(33), 181-203. http://dx.doi.org/10.21830/19006586.726

Tossi, A. A. (2017). Consideraciones sobre la ciberamenaza a la seguridad nacional. *Revista Política y Estrategia, 125*, 83-96. https://bit.ly/3Jrh1xY

Vajagathali, M., Navaneeth K., S., & Balaji N., B. (2019). Cyber crime awareness among college students in Mangalore. *Journal of Forensic Sciences & Criminal Investigation, 12*(1), 555828. https://bit.ly/3HjdoIG

Yah Santana, M. N. (2020). Incorporación de tecnologías digitales en los procesos de enseñanza-aprendizaje en escuelas secundarias. *Ixaya. Revista Universitaria de Desarrollo Social, 10*(19), 101-120. https://bit.ly/3Hvvqr1

Zúñiga, O. (2018). Educación y prevención en materia de protección de datos personales de niños, niñas y adolescentes en internet. *Estudios en Derecho a la Información, 5*(5), 59-79. https://bit.ly/3JyqILb