UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

Revista VÍNCULOS
Ciencia, Tecnología y Sociedad
Un Enlace hacia el Futuro

Recibido: 4 de febrero 2026 / Aceptado: 18 de mayo 2026

VALIDACIÓN ESCALA SOBRE SEGURIDAD Y PRIVACIDAD DIGITAL PARA UNIVERSITARIOS

DIGITAL SECURITY AND PRIVACY SCALE VALIDATION FOR UNIVERSITY STUDENTS

Carlos Arturo Torres Gastelú[1], Carlos Torres Real[2]

Resumen:

En este documento se describe el proceso de diseño y validación de la escala de percepción titulada SEPID, creada para medir la seguridad y privacidad digital en estudiantes universitarios. La escala tipo Likert desarrollada contiene cuatro dimensiones: actitud hacia la gestión de la seguridad y privacidad, medidas preventivas de privacidad, medidas preventivas de seguridad y eventos vividos en contra de la integridad a su identidad digital. Se aplicó a 539 estudiantes inscritos en tres universidades públicas mexicanas. Se realizó un análisis factorial exploratorio (AFE) y análisis factorial confirmatorio (AFC) para determinar su validez. Como parte de los resultados, se obtuvo un alfa de Cronbach de 0.747 y un índice Kaiser-Meyer-Olkin (KMO) de 0.838 global para las cuatro subescalas. La versión final contiene 22 ítems agrupados en cuatro factores. La escala SEPID cuenta con un nivel aceptable de confiabilidad y validez para medir la seguridad y privacidad digital en estudiantes universitarios.

Palabras claves: estudiante universitario, internet, medición, medios sociales, protección de datos.

Abstract

This paper describes the design and validation of the SEPID scale, developed to assess digital security and privacy perception among university students. This Likert-type instrument comprises four dimensions: attitudes toward security and privacy management, privacy preventive measures, security preventive measures, and adverse events affecting digital identity integrity. The study surveyed 539 students enrolled in three Mexican public universities. Both Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) were conducted to establish validity. Results yielded a global Cronbach's alpha of 0.747 and a Kaiser-Meyer-Olkin (KMO) index of 0.838 across the subscales. The final version consists of 22 items grouped into four factors. Consequently, the SEPID scale demonstrates acceptable reliability and validity for assessing digital security and privacy in university students.

Keywords: university student; internet; measurement; social media; data protection.

1 Doctor en Ciencias de la Administración, UNAM, México, Veracruz. Afiliación institucional: Universidad Veracruzana, México. Correo electrónico personal e institucional e-mail: torresgastelu@gmail.com, ctorres@uv.mx. ORCID: https://orcid.org/0000-0003-2527-9602

2 Licenciado en Pedagogía, Universidad Veracruzana, México, Veracruz. Afiliación institucional: Universidad Veracruzana, México. Correo electrónico personal e institucional e-mail: ctorresreal@hotmail.com, zS20005102@estudiantes.uv.mx. ORCID: https://orcid.org/0000-0003-3500-7803

1. Introducción

La integración progresiva de las Tecnologías de la Información y Comunicación (TIC) en el ámbito de la educación superior ha redefinido los procesos de enseñanza-aprendizaje, ofreciendo oportunidades sin precedentes para el acceso al conocimiento y la colaboración. Sin embargo, esta digitalización también ha expuesto a los estudiantes universitarios y a las instituciones a un panorama creciente de amenazas cibernéticas. La omnipresencia de la conectividad y el intercambio de información digital hacen que la comprensión de la seguridad y privacidad en este colectivo sea no solo relevante, sino imperativa.

Estudios recientes han documentado un aumento significativo de ciberataques dirigidos específicamente a estudiantes universitarios, afectando sus sistemas de información y comprometiendo datos sensibles. La protección de esta información es de vital importancia, no solo para salvaguardar la seguridad y el bienestar individual de los estudiantes, sino también para mantener la confianza en las instituciones educativas y en la integridad de sus sistemas.

Se observa una dinámica particular en este grupo demográfico, que podría denominarse la paradoja de la madurez digital. Los estudiantes universitarios, al ser en gran medida nativos digitales, se caracterizan por una alta familiaridad y un uso extensivo de las plataformas y herramientas tecnológicas en su vida diaria. Esta inmersión digital podría llevar a la suposición de una competencia inherente en el manejo de la seguridad y privacidad en línea. No obstante, la literatura científica revela una discrepancia notable: a pesar de su destreza en el uso de la tecnología, a menudo carecen de una comprensión profunda de los riesgos asociados y de la aplicación efectiva de medidas de protección [1].

Esta brecha entre el uso generalizado y la conciencia de seguridad crea una vulnerabilidad inherente que subraya la urgencia y la justificación de este estudio. La implicación de esta paradoja es clara: la educación en ciberseguridad debe ir más allá de la mera instrucción sobre el uso de la tecnología y centrarse en una alfabetización digital en seguridad que aborde de manera específica las brechas de conocimiento y comportamiento.

Partiendo de lo anterior, se propone revisar en este documento las cuatro dimensiones propuestas: actitud hacia la gestión de la seguridad y privacidad, medidas preventivas de privacidad, medidas preventivas de seguridad y eventos vividos en contra de la integridad a su identidad digital. Para ello, se plantea la siguiente pregunta de investigación: ¿Qué nivel de confiabilidad y validez posee la escala SEPID para medir la seguridad y privacidad digital en estudiantes universitarios? El objetivo de la investigación fue describir el proceso de confiabilidad y validez de la escala SEPID. Se parte de la hipótesis de que dicho instrumento reúne los criterios de confiabilidad y validez necesarios para ser utilizada en estudiantes universitarios.

1.1. Estudios relacionados

Sobre la dimensión actitud hacia la gestión de la seguridad y privacidad, el nivel de conciencia sobre ciberseguridad entre los universitarios es variado. De acuerdo con el estudio realizado por López et al. [2] en México, se halló que, "en general, la mayoría de los estudiantes parecen ser conscientes de los riesgos", aunque sus actitudes oscilan desde una confianza cautelosa hasta una franca desconfianza hacia el manejo de sus datos por terceros. Esta heterogeneidad indica que algunos estudiantes confían moderadamente en las medidas de seguridad existentes, mientras que otros desconfían abiertamente de cómo se manipulan sus datos personales. No obstante, incluso entre quienes expresan confianza, se detectan ideas contradictorias que revelan falta de certeza o comprensión incompleta del tema.

Las investigaciones sugieren que muchos usuarios, incluidos estudiantes, tienden a relegar la seguridad informática a un segundo plano de interés [3], enfocándose más en la comodidad o la conectividad que en protegerse activamente. Este desinterés relativo puede deberse a la percepción de que "nada malo me va a pasar" (sesgo de invulnerabilidad) o a que consideran engorrosas las medidas de seguridad.

Los propios estudiantes reconocen sus carencias: casi todos concuerdan en que las universidades "deben reforzar la educación en seguridad de la información" dentro de su formación. En un estudio realizado en China con 1.710 universitarios, casi el 100% manifestó que la universidad necesita fortalecer la enseñanza en seguridad informática, evidenciando de que no están suficientemente preparados [4]. Esta demanda de capacitación, sumada a la evidencia de actitudes descuidadas, sugiere que muchos estudiantes estarían dispuestos a mejorar su gestión de seguridad y privacidad si recibieran orientación formal al respecto.

Respecto a la dimensión medidas preventivas de privacidad, un problema común es la tendencia a compartir información en exceso (oversharing). Investigaciones sistemáticas sobre comportamientos de riesgo digital identifican el "compartir más información de la necesaria" como uno de los hábitos riesgosos frecuentes entre usuarios jóvenes [5]. Esto incluye publicar datos personales sensibles, fotografías íntimas o detalles privados en entornos en los que terceros no confiables pueden acceder.

Por ejemplo, se ha observado que es habitual que los estudiantes universitarios mantengan un número elevado de "amigos" o seguidores en redes sociales que en realidad no conocen personalmente. Un análisis reportó que aproximadamente una quinta parte de los contactos en Facebook de un usuario típico podrían ser personas desconocidas [6], quienes sin embargo tienen acceso a sus fotos e información compartida (p. ej., etiquetas en imágenes, actualizaciones de estado). Este hecho

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

expone a los jóvenes a riesgos, ya que individuos fuera de su círculo de confianza pueden explotar esos datos.

Con respecto a la dimensión medidas preventivas de seguridad, la literatura evidencia que muchos estudiantes universitarios no siguen prácticas óptimas de ciberseguridad, lo que aumenta su vulnerabilidad técnica frente a ataques. Uno de los hallazgos más consistentes es la debilidad en las prácticas de contraseñas. Diversos estudios reportan que los jóvenes tienden a usar contraseñas débiles, repetidas en múltiples cuentas o a compartirlas con otros.

Una encuesta internacional concluyó que "todos los estudiantes seguían siendo débiles en sus prácticas de contraseña", revelando problemas como uso de contraseñas cortas o predecibles, y falta de actualización periódica [4]. Asimismo, una revisión sistemática en Brasil identificó el compartir las contraseñas como uno de los comportamientos de riesgo más comunes entre usuarios de entornos digitales [5].

Por otro lado, algunos reportes que señalan que el spam y los archivos maliciosos son problemas recurrentes que enfrentan los universitarios en línea: en un estudio, el tipo de problema más común mencionado fue el spam recibido en sus correos o mensajes [4], lo cual suele ser la puerta de entrada a intentos de phishing o malware. La negligencia en la verificación de adjuntos de email es otro comportamiento de riesgo identificado en usuarios: muchos no revisan la legitimidad de archivos o enlaces antes de hacer clic [5], lo que los deja expuestos a fraudes o infecciones.

Al revisar las medidas de seguridad que sí aplican los estudiantes, se observa disparidad. Por un lado, la mayoría usa algún nivel de protección antivirus o software de seguridad básico si sus dispositivos lo traen preinstalado, pero no siempre de forma activa o consistente. Por ejemplo, un estudio halló que los estudiantes varones tenían ligeramente mejores hábitos en cuanto a mantenimiento del dispositivo (actualizaciones, uso de herramientas técnicas) que las mujeres, mientras que estas mostraban más precaución en contextos sociales en línea.

Esto sugiere que ciertos subgrupos podrían enfocarse más en unas medidas que en otras. En general, sin embargo, ningún grupo destacó por prácticas de seguridad sobresalientes, evidenciando que incluso los estudiantes de áreas técnicas presentaban deficiencias importantes. Un hallazgo interesante de ese estudio en China fue que los estudiantes de primer año tuvieron puntajes mejores en ciertos hábitos de seguridad (dispositivo, navegación web) que los alumnos de años superiores [4]. Esto podría indicar que las nuevas generaciones llegan con mayor familiaridad en algunas herramientas, o bien que con el tiempo los estudiantes se confían y relajan sus prácticas.

En cualquier caso, la concientización y capacitación se revelan fundamentales: un experimento en México demostró que, tras una charla formativa en ciberseguridad, los alumnos incrementaron su percepción de conocimiento en seguridad informática y mostraron mayor conciencia sobre la necesidad de realizar respaldos periódicos de su información. Antes de la intervención, muchos no solían hacer copias de seguridad frecuentes; después, valoraron más esta medida preventiva básica [3]. Esto indica que educar a los estudiantes en buenas prácticas (como gestionar contraseñas robustas, actualizar sus sistemas, usar autenticación de dos pasos, hacer backups, etc.) sí puede traducirse en mejoras conductuales.

Pese a algunas señales positivas, los estudios coinciden en que las prácticas de seguridad de los universitarios son en general insuficientes para el entorno de amenazas actual. Además de las contraseñas débiles y la falta de actualización ya mencionadas, otros comportamientos riesgosos incluyen: no bloquear la sesión o el equipo al dejarlo desatendido (muchos estudiantes confían demasiado en su entorno cercano y dejan sus laptops o cuentas abiertas en bibliotecas, por ejemplo) [5], y no tener copia de sus datos importantes (lo que agrava el impacto si sufren un ataque de ransomware o un fallo del equipo).

Es importante destacar que conforme los jóvenes avanzan en edad y uso de la tecnología, enfrentan riesgos mayores: se ha observado que la incidencia de problemas de ciberseguridad aumenta con la edad dentro del grupo juvenil. Los universitarios, al usar internet más extensamente que escolares de niveles inferiores, "enfrentan más problemas de seguridad" y son más propensos a ser blanco de ataques [4].

Por ello, instituciones y expertos enfatizan la necesidad de inculcar hábitos sólidos: cosas tan sencillas como mantener los dispositivos y antivirus actualizados, desconfiar de enlaces/adjuntos sospechosos, usar contraseñas fuertes y únicas, activar el doble factor de autenticación, y evitar redes públicas sin protección, pueden mitigar significativamente los riesgos [7,3,8].

En suma, el nivel de higiene cibernética de los estudiantes universitarios deja margen de mejora. Muchos jóvenes reconocen que no cuentan con preparación suficiente para protegerse en línea y esperan aprender más al respecto [4]. Como respuesta, algunas universidades han comenzado a incluir talleres o cursos sobre seguridad digital para sus alumnos, buscando cubrir esta necesidad formativa [3]. Los resultados preliminares son alentadores: cuando se les brinda conocimientos y herramientas, los estudiantes tienden a adoptar medidas preventivas antes ignoradas. Esto sugiere que la brecha no es de apatía total, sino principalmente de desconocimiento y hábito, factores que pueden modificarse con educación continua.

En el caso de la dimensión eventos vividos en contra de la integridad a su identidad digital, la investigación sugiere que una mayoría de estudiantes universitarios no ha sido víctima directa de ciberataques graves –al menos no a su conocimiento–,

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

pero una proporción significativa sí ha enfrentado algún tipo de incidente digital. En un estudio realizado con estudiantes de informática en México, se preguntó a los participantes si habían sido víctimas de un ciberataque y qué había sucedido. Los resultados mostraron que el 44% respondió a la pregunta, y dentro de ese grupo la mayoría (14 de 22 estudiantes) indicó que no había sufrido ningún ataque.

Esto sugiere que una porción importante (aproximadamente el 64% del total, considerando también quienes no respondieron) no reporta experiencias de vulneración digital significativas o no está consciente de haberlas sufrido. De hecho, varios estudiantes expresaron incertidumbre con respuestas como "no sé", evidenciando "una posible falta de conocimiento para identificar ciberataques". Esta falta de conciencia implica que algunos podrían haber sido atacados sin darse cuenta (por ejemplo, si su información fue robada pero no detectaron indicios).

No obstante, un grupo menor sí reportó vivencias concretas de ataques. Entre los incidentes narrados por estudiantes se contaron casos de robo de cuentas de redes sociales (por medio de enlaces maliciosos o técnicas de phishing) y problemas financieros más serios como la clonación de tarjetas bancarias para efectuar fraudes. Estos sucesos ilustran el espectro de gravedad: desde pérdidas de acceso a perfiles online (que afectan su identidad digital en redes) hasta daños económicos reales.

En tales casos, la reacción de los estudiantes fue sobre todo reactiva: algunos lograron mitigar el daño de manera proactiva, por ejemplo recuperando sus cuentas comprometidas mediante procesos de verificación, o transfiriendo fondos rápidamente al detectar un cargo fraudulento en su cuenta. Sin embargo, incluso entre quienes actuaron diligentemente tras el ataque, sus testimonios revelan que "no estaban adecuadamente preparados para prevenir este tipo de situaciones" [2]. Es decir, respondieron una vez ocurrido el incidente, pero no contaban con medidas preventivas de antemano (como autenticación de doble factor en sus cuentas o alertas bancarias configuradas) que pudieran haber impedido o limitado el ataque.

Además de ataques dirigidos a obtener información o dinero, los estudiantes enfrentan eventos que comprometen su identidad digital en términos de reputación y bienestar. Un evento común son las estafas en línea y engaños. Por ejemplo, estudiantes universitarios que han sido expuestos a intentos de fraude vía phishing (correos o mensajes engañosos).

Aunque muchos no caen en la trampa, otros sí han llegado a proporcionar datos sensibles creyendo en comunicados falsos de bancos o servicios, comprometiendo su identidad financiera. Según datos globales, en 2021 alrededor de 16.6% de los internautas experimentaron fraudes en línea y 6.6% sufrieron el robo de sus cuentas o contraseñas en un periodo de seis meses [4]. Si bien estas cifras incluyen a la población general, los universitarios –por su alta actividad digital– están entre los más afectados.

Un punto relevante es que la vivencia de un incidente que atenta sobre su seguridad y privacidad digital, suele despertar mayor consciencia y cambio de actitud. Muchos estudiantes solo toman en serio ciertas medidas después de haber sido víctimas. Por ejemplo, un joven que pierde el acceso a su cuenta por un hacker probablemente aprenderá a usar contraseñas más fuertes o activar la verificación en dos pasos tras esa experiencia. De igual modo, quienes sufren ciberacoso pueden ajustar sus configuraciones de privacidad o ser más selectivos con lo que comparten a futuro.

En este sentido, las experiencias negativas funcionan como lecciones personales. Sin embargo, idealmente no se debería depender del "aprendizaje por golpe": la formación preventiva busca que los estudiantes se protejan antes de ser víctimas. Desafortunadamente, la investigación muestra que una parte de los estudiantes no imagina el alcance de los riesgos hasta que estos se materializan.

Como se mencionó, aquellos que "no están seguros si fueron atacados" revelan una peligrosa falta de alfabetización digital que los mantiene en situación vulnerable. Es urgente, según los expertos, incorporar contenidos de ciberseguridad y protección de la identidad digital en los currículos académicos para subsanar estas falencias [2]. Solo así podrá evitarse que la primera toma de conciencia ocurra tras un evento dañino.

2. Metodología

Se trata de un tipo de estudio cuantitativo, no experimental y transversal que pretende identificar las medidas preventivas para preservar la protección de la información que realizan los individuos cuando están conectados a la red, así como la actitud que toman éstos hacia la gestión de su protección y los eventos vividos en contra de la integridad a su identidad digital.

2.1. Participantes

El instrumento fue aplicado de manera presencial en tres universidades públicas mexicanas alcanzando una muestra de 539 estudiantes seleccionados de manera aleatoria a conveniencia del investigador. Se trata de una muestra no probabilística con la participación de 6 licenciaturas. El instrumento se aplicó en la mayoría de los semestres. La composición de la muestra por sexo fue de 62.9% mujeres y 37.1% hombres. La distribución por edad, reveló que el 24.2% de los estudiantes tenían entre 18 y 19 años, el 42.4% entre 20 y 21 años, el 19.1% entre 22 y 23 años, el 5.9% entre 24 y 25 años, y el 8.3% eran mayores de 25 años.

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

2.2. Instrumento

Se aplicó un instrumento conformado por 41 ítems valorado mediante una escala Likert de cinco opciones que van desde muy en desacuerdo, en desacuerdo, indiferente, de acuerdo, muy de acuerdo.

2.3. Procedimiento

La recolección de datos cumplió con las normas éticas solicitando la autorización a las autoridades mediante la expedición de un oficio solicitando el apoyo para su aplicación. Los jefes de las diferentes licenciaturas proporcionaron un listado de horarios, días y maestros. También enviaron un correo a los maestros solicitando su apoyo. Antes de la aplicación, se les explicó el propósito del estudio y se les pidió que llenaran el consentimiento informado de los participantes, en el cual proporcionaron sus nombres y firmas. De la misma manera, se les indicó que se trataba de un estudio sin fines de lucro donde se respetaría la confidencialidad y el anonimato de sus respuestas.

2.4. Análisis de datos

Para la validación del instrumento se ejecutó el Análisis Factorial Exploratorio (AFE) mediante la identificación de los componentes principales y sus correspondientes pruebas de Alpha de Cronbach. En tanto, para el Análisis Factorial Confirmatorio (AFC) se emplearon índices de ajuste para evaluar el modelo teórico propuesto y su congruencia con los datos observados. Estas pruebas fueron realizadas con dos herramientas de Software: SPSS versión 25 y AMOS versión 23.

3. Resultados y discusión

A continuación, se presentan los análisis descriptivos, análisis de fiabilidad, análisis factorial exploratorio, análisis factorial confirmatorio y el apartado de discusión.

3.1. Análisis descriptivos

Se realizaron análisis descriptivos como evidencia de la normalidad univariada en la distribución de los puntajes de los ítems. En la Tabla 1 se muestran los valores de medias (M), desviaciones estándar (DE), asimetría y curtosis de todos los ítems que componen el cuestionario SEPID. Los valores de asimetría y curtosis sugieren la existencia de normalidad univariada en la distribución de los puntajes de los ítems, debido a que los valores de asimetría y curtosis se consideran aceptables, al encontrarse en los rangos de -3 a +3 y de -10 a +10, respectivamente [9,10].

Ítems	M	DE	Asimetría	Curtosis	Ítems	M	DE	Asimetría	Curtosis
ACE1	4.63	0.858	-2.862	8.209	MES22	4.25	0.944	-1.437	2.004
ACE2	4.35	0.962	-1.856	3.396	MES23	3.96	1.147	-1.153	0.611
ACE3	4.51	0.826	-1.996	4.304	MES24	4.39	0.937	-1.809	3.161
ACE4	2.37	1.267	0.646	-0.622	MES25	3.29	1.490	-0.382	-1.264
ACE5	3.66	1.075	-0.641	-0.315	MES26	4.17	0.992	-1.192	0.961
ACE6	4.23	0.945	-1.421	1.860	MES27	3.87	1.204	-0.933	0.027
ACE7	3.38	1.305	-0.471	-0.908	MES28	3.93	1.095	-0.935	0.262
ACE8	3.67	1.009	-0.639	0.073	MES29	4.28	0.961	-1.519	2.186
ACE9	2.35	1.463	0.593	-1.140	MES30	3.65	1.374	-0.690	-0.782
ACE10	2.54	1.416	0.321	-1.272	MES31	3.90	1.255	-1.002	-0.014
ACE11	3.92	1.177	-0.948	0.074	ECI32	2.31	1.455	0.701	-0.965
MEP12	4.07	1.099	-1.179	0.720	ECI33	2.79	1.470	0.165	-1.349
MEP13	4.20	1.062	-1.401	1.317	ECI34	1.96	1.342	1.195	0.063
MEP14	4.10	1.170	-1.217	0.513	ECI35	1.97	1.340	1.165	0.007
MEP15	4.46	1.047	-2.088	3.527	ECI36	2.04	1.361	1.066	-0.221
MEP16	4.09	1.124	-1.232	0.772	ECI37	2.58	1.532	0.332	-1.449
MEP17	3.75	1.229	-0.797	-0.256	ECI38	2.11	1.396	0.958	-0.479
MEP18	4.15	1.045	-1.365	1.474	ECI39	1.87	1.263	1.331	0.569
MEP19	4.05	1.070	-1.298	1.287	ECI40	2.02	1.260	1.029	-0.099
MEP20	3.54	1.303	-0.528	-0.805	ECI41	2.08	1.337	0.939	-0.441
MEP21	3.80	1.108	-0.799	0.016					

Nota. ACE = Actitud hacia la gestión de la seguridad y privacidad; MEP = Medidas preventivas de privacidad; MES = Medidas preventivas de seguridad; ECI = Eventos vividos en contra de la integridad a su identidad digital.

Tabla 1. Medias, desviaciones estándar, asimetría y curtosis de los 41 ítems iniciales de SEPID.

Fuente: elaboración propia.

Por consiguiente, todos los ítems muestran normalidad univariada en sus puntajes. Por otro lado, el ítem ACE3 fue el que presentó menor variabilidad en sus opciones de respuesta (alrededor de las opciones tres y cuatro), al tener la menor desviación estándar (0.82), con media de 4.51. Por su parte, el ítem ECI37 fue el de mayor variabilidad (alrededor de las opciones tres y cuatro), al obtener la desviación estándar más alta (1.53), alrededor de la media de 2.58.

3.2. Análisis de fiabilidad

Para la confiabilidad de las subescalas, se realizó la prueba de alfa de Cronbach empleando el software SPSS® versión 25 (Ver Tabla 2). Se observa que el valor del alfa de Cronbach global del instrumento fue alto (0.845).

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Dimensiones	Número de ítems	Alfa de Cronbach
Actitud hacia la gestión de la seguridad y privacidad.	11	0.649
Medidas preventivas de privacidad	10	0.861
Medidas preventivas de seguridad	10	0.748
Eventos vividos en contra de la integridad a su identidad digital	10	0.875
Total	**41**	**0.845**

Tabla 2. Alfa de Cronbach de las dimensiones y global del instrumento SEPID.

Fuente: elaboración propia.

Escala	KMO	X^2	gl	X^2/gl	% de var	factores	ítems
ACE	0.74	1055.24	55	19.18	41.9%	2	11
MEP	0.87	2045.07	45	45.44	57.7%	2	10
MES	0.82	1089.58	45	24.21	45.9%	2	10
ECI	0.91	2266.29	45	50.36	59.4%	2	10

Nota. ACE = Actitud hacia la gestión de la seguridad y privacidad; MEP = Medidas preventivas de privacidad; MES = Medidas preventivas de seguridad; ECI = Eventos vividos en contra de la integridad a su identidad digital.

Tabla 3. Resultados del AFE de las subescalas que componen el cuestionario Seguridad y privacidad digital en estudiantes universitarios.

Fuente: elaboración propia.

3.3. Análisis factorial exploratorio (AFE)

Se realizó un AFE deductivo, con un método de extracción de componentes principales con rotación Varimax, empleando el software estadístico SPSS en su versión 25. El criterio de exclusión fue aquellos ítems con cargas factoriales menores a 0.30 y aquellos que presentaban cargas mayores a este valor en dos factores [11]. Para el caso de la subescala de Actitud hacia la gestión de la seguridad y privacidad (ACE), el índice Kaiser, Meyer y Olkin (KMO) fue normal, de 0.74, y la prueba de esfericidad de Bartlett resultó significativa (X2= 1055.24, p < 0.000). Se obtuvo que una solución de dos factores que explicó 41.9% de la varianza total de los puntajes.

El KMO de la subescala de Medidas preventivas de privacidad (MEP) fue notable al alcanzar un valor de 0.87, y la prueba de esfericidad de Bartlett resultó significativa (X2= 2045.07, p < 0.000). Se obtuvo una solución con dos factores que explican 57.7% de la varianza total de los puntajes. Para la subescala de Medidas preventivas de seguridad (MES) el KMO fue notable de 0.82, y la prueba de esfericidad de Bartlett resultó significativa (X2= 1089.58, p < 0.000). Se obtuvo una solución de dos factores que resulta 45.9% de la varianza total de los puntajes

El KMO de la subescala de Eventos vividos en contra de la integridad a su identidad digital (ECI) fue muy notable al alcanzar un valor de 0.91, y la prueba de esfericidad de Bartlett resultó significativa (X2= 2266.29, p < 0.000). Se obtuvo una solución con dos factores que explican 59.4% de la varianza total de los puntajes (Ver Tabla 3).

3.4. Análisis factorial confirmatorio (AFC)

A fin de corroborar la asociación de factores obtenida en el AFE, se llevó a cabo el AFC tomando como criterio base la teoría del instrumento y los análisis factoriales congruentes con el diseño de las subescalas. Además, se consideró el mínimo de tres ítems por factor. Para tal fin, se empleó el método de estimación de máxima verosimilitud para determinar la bondad de ajuste empírica del modelo.

Como resultado del AFC, se eliminaron los ítems que no se asociaron con los factores del modelo [12,13]. De esta forma, se obtuvieron los modelos de medida por cada escala que cumplieron con los índices de bondad de ajuste, a fin de confirmar la sustentabilidad empírica del modelo.

Los índices considerados fueron**:** el índice ji al cuadrado sobre grados de libertad o relativa (X2/gl), la raíz cuadrada de residual estandarizada (SRMR), el índice de bondad de ajuste ajustado (AGFI), el índice de ajuste comparativo (CFI) y, finalmente, el error de la raíz cuadrada de la media de aproximación (RMSEA). Estos índices se consideran aceptables si sus valores superan los criterios de ajuste establecidos, que son (X2/gl > 1**;** CFI y AGFI > 0.95**;** SRMR < 0.08 y RMSEA < 0.06 [14,15,16]. A continuación, se presentan los resultados obtenidos en los índices de bondad de ajuste para cada una de las subescalas (Ver Tabla 4).

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Modelo	Chi-cuadrado X^2	*gl*	X^2 relativa (X^2/gl)	CFI	SRMR	RMSEA	AGFI
ACE	2.523	2	1.261	.996	.019	.022	.988
MEP	30.079	8	3.760	.974	.045	.072*	.952
MES	11.961	5	2.392	.983	.027	.051	.973
ECI	38.344	14	2.739	.984	.026	.057	.960

Nota. ACE = Actitud hacia la gestión de la seguridad y privacidad; MEP = Medidas preventivas de privacidad; MES = Medidas preventivas de seguridad; ECI = Eventos vividos en contra de la integridad a su identidad digital.

*Marca los índices que no cumplen con los criterios de bondad de ajuste del modelo.

Tabla 4. Índices de los modelos para medir las subescalas del cuestionario Seguridad y privacidad digital en estudiantes universitarios.

Fuente: elaboración propia.

Igualmente como resultado del AFC, se obtiene que las subescalas ACE, MES y ECI son las únicas validadas por la totalidad de sus índices de bondad de ajuste. Mientras tanto, en la escalas MEP no se satisfacen los criterios de ajuste en uno de sus índices, el RMSEA, lo cual se desestima, ya que se pueden considerar validadas por sus cuatros índices restantes. Una vez validadas las escalas, se presentan sus respectivos modelos de medida, de los cuales los correspondientes a las subescalas ACE, MES y ECI, contemplan un modelo unidimensional, el resto de ellos resultaron modelos de dos factores, con al menos dos variables observables por componente. Por lo tanto, para la subescala MEP se llegó a un modelo de 6 ítems (MEP18, MEP19, MEP21, MEP13, MEP14 y MEP15) (Ver Figura 1).

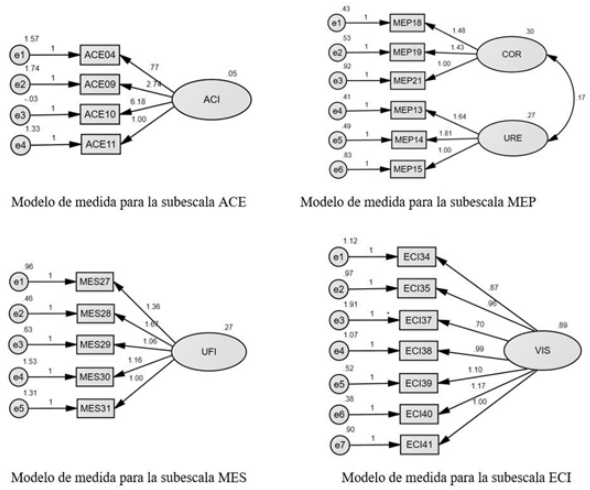

Figura 1. Modelos de medida de la escala Seguridad y privacidad digital en estudiantes universitarios (subescalas ACE, MEP, MES y ECI).

Fuente: elaboración propia

3.5. Discusión

Al realizar el contraste de los resultados del presente trabajo con los estudios previos, se identifica que cada una de las dimensiones de la escala presentan elementos similares de otros instrumentos de la temática. Sobre la dimensión Actitud hacia la gestión de la seguridad y privacidad (ACE), la escala SEPID establece ítems sobre el conocimiento de los riegos de seguridad y privacidad digital.

Esto coincide con lo encontrado por López et al. [2] en su estudio, los autores muestran que los estudiantes parecen ser conscientes de los riesgos, aunque sus actitudes oscilan desde una confianza cautelosa hasta una franca desconfianza hacia el manejo de sus datos por terceros. Respecto a la dimensión Medidas preventivas de privacidad (MEP), la escala SEPID retoma ítems que involucran las prácticas y riesgos de privacidad digital. Lo cual se asemeja con lo encontrado por Nogueira et al. [5] en su estudio, identifican el "compartir más información de la necesaria" como uno de los hábitos riesgosos frecuentes entre usuarios jóvenes. Esto incluye publicar datos personales sensibles, fotografías íntimas o detalles privados en entornos en los que terceros no confiables pueden acceder.

Con respecto a la dimensión Medidas preventivas de seguridad (MES), la escala SEPID establece ítems sobre las prácticas y riesgos de ciberseguridad, Esto coincide con lo encontrado por Guo y Tinmaz [4] en su estudio, "todos los estudiantes seguían siendo débiles en sus prácticas de contraseña", revelando problemas como uso de contraseñas cortas o predecibles, y falta de actualización periódica.

Asimismo, el spam y los archivos maliciosos son problemas recurrentes que enfrentan los universitarios en línea: el tipo de problema más común mencionado fue el spam recibido en sus correos o mensajes, lo cual suele ser la puerta de entrada a intentos de phishing o malware.

Sobre la dimensión Eventos vividos en contra de la integridad a su identidad digital (ECI), la escala SEPID retoma ítems que involucran experiencias negativas en la red. Lo cual se asemeja con lo encontrado por López et al. [2] en su estudio, entre los incidentes narrados por estudiantes se contaron casos de robo de cuentas de redes sociales (por medio de enlaces maliciosos o técnicas de phishing) y problemas financieros más serios como la clonación de tarjetas bancarias para efectuar fraudes.

También, esto coincide con lo encontrado por Guo y Tinmaz [4] en su estudio, los estudiantes enfrentan eventos que comprometen su identidad digital en términos de reputación y bienestar. Un evento común son las estafas en línea y engaños. Por ejemplo, un porcentaje de universitarios ha sido expuesto a intentos de fraude vía phishing (correos o mensajes engañosos).

Aunque muchos no caen en la trampa, otros sí han llegado a proporcionar datos sensibles creyendo en comunicados falsos de bancos o servicios, comprometiendo su identidad financiera.

4. Conclusiones

Tras el análisis de las propiedades métricas de la escala SEPID, en la subescala ACE se excluyó el constructo Importancia de la Privacidad en Internet (IPI) por carecer de indicadores adecuados. Por otra parte, en la subescala MES se excluyó el constructo Impacto Uso Cuidadoso en Internet (UCI) por carecer de indicadores adecuados. En la subescala ECI se excluyó el constructo Control y Arrepentimiento en las Redes (CAR) por carecer de indicadores adecuados.

En cuanto a la confiabilidad, el alfa de Cronbach global de las cuatro subescalas fue aceptable (0.747), lo que indica que, en su conjunto, las subescalas miden el constructo para el cual fueron creadas. Tras los análisis aquí presentados, la escala queda conformada por cuatro factores y 22 ítems. Con lo anterior, se comprueba la hipótesis inicial, y se concluye que la escala SEPID posee niveles aceptables de confiabilidad para medir las medidas preventivas para preservar la protección de la información que realizan los individuos cuando están conectados a la red, así como la actitud que toman éstos hacia la gestión de su protección y los eventos vividos en contra de la integridad a su identidad digital.

Sería conveniente realizar una nueva aplicación con estudiantes de otras áreas de formación o de otros estados de México o países, además probar con estudiantes de nivel bachillerato o de posgrado. Lo que permitirá una mayor perspectiva y a su vez hacer una segunda validación del instrumento en otra población de estudio.

La revisión de la literatura evidencia que la seguridad y privacidad de los estudiantes universitarios es un tema de creciente importancia, con múltiples aristas interrelacionadas. En cuanto a la actitud, los estudiantes valoran en teoría su privacidad y comprenden que existen riesgos en el entorno digital, pero no siempre traducen esa preocupación en comportamientos seguros (brecha actitud-comportamiento).
Muchos jóvenes muestran conocimientos básicos sobre seguridad y privacidad digital, reflejado en un exceso de confianza cuando navegan en la web, así como un desconocimiento de los posibles riesgos. Esto conecta con la necesidad crítica de fortalecer la cultura y educación en ciberseguridad en el ámbito universitario, para transformar actitudes pasivas en actitudes proactivas.

Respecto a las medidas preventivas de privacidad, los estudiantes han adoptado algunas buenas prácticas –como restringir el acceso a sus perfiles y ser más cuidadosos con lo que comparten–, reflejando que la privacidad sí les importa. Sin embargo, estas medidas suelen ser parciales: se observa una tendencia a sobreexponerse (ya sea por hábitos de socialización digital o por ignorar configuraciones avanzadas), lo cual deja flancos abiertos en su protección. Aún es común que mantengan gran parte de su vida digital accesible a terceros no confiables, voluntaria o involuntariamente. En el plano de las medidas de seguridad técnica, la situación es preocupante.

Las rutinas básicas de ciberseguridad no están bien asentadas entre los universitarios. Prevalecen contraseñas débiles, dispositivos desactualizados, poca precaución ante amenazas comunes (phishing, malware) y almacenamiento imprudente de datos sensibles. Estos déficits los convierten en objetivos relativamente fáciles para atacantes oportunistas. La buena noticia es que existen intervenciones educativas puntuales que han demostrado mejorar significativamente la competencia digital en seguridad de los estudiantes – por ejemplo, capacitaciones que aumentan la frecuencia de backups o la comprensión de conceptos clave–.

Esto sugiere que, con el apoyo institucional adecuado, se puede cerrar la brecha de habilidades y fomentar hábitos de seguridad más sólidos en este colectivo. Finalmente, los eventos vividos por estudiantes nos recuerdan que las amenazas no son abstractas: una fracción no despreciable de universitarios ha sido víctima de algún tipo de ataque o abuso digital. Si bien muchos no han pasado por ello (o no lo saben), quienes sí lo han hecho corroboran con sus experiencias la gravedad potencial de no estar protegido –desde pérdidas económicas por fraude, hasta traumas por acoso o daños reputacionales duraderos–.

Estas vivencias confirman la urgencia de implementar las mejoras en actitud y medidas preventivas señaladas en las otras dimensiones.

ISSN 1794-211 X • e-lSSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2023). pp. 91-98. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

Además, ilustran un punto clave: la resiliencia digital de los estudiantes depende en gran medida de la preparación previa. Los que enfrentan mejor un incidente son usualmente aquellos que tenían algún plan de respuesta o conocimiento, mientras que los menos preparados sufren mayores estragos.

En conclusión, la literatura sugiere que garantizar la seguridad y privacidad de los estudiantes universitarios requiere un enfoque integral que abarque: (a) Concientización y actitud – fomentar en ellos un sentido de responsabilidad personal y escepticismo sano frente a los riesgos digitales; (b) Prácticas de privacidad – dotarlos de herramientas y recomendaciones claras para gestionar su información personal (configuraciones de privacidad, control de la huella digital, manejo de contenidos sensibles); (c) Prácticas de seguridad – inculcar hábitos técnicos de autoprotección (buenas contraseñas, actualizaciones, copias de seguridad, etc.) hasta convertirlos en parte de su rutina; y (d) Apoyo ante incidentes – protocolos y recursos de ayuda en las instituciones para cuando ocurran eventos, de modo que los estudiantes aprendan de ellos y reciban el soporte necesario.

Solo mediante esta aproximación multifacética se podrá mejorar la resiliencia de los universitarios en el mundo digital, asegurando que aprovechen la tecnología para su desarrollo académico y social sin comprometer su identidad ni su bienestar.

5. Referencias

[1] R. U. Azad. et al., "Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework", Global Knowledge, Memory and Communication, enero 2025.

[2] H. L. López. et al., "Percepción de la ciberseguridad entre estudiantes universitarios en entornos digitales: Un estudio en la Facultad de Informática Mazatlán", Revista De Tecnología E Innovación En Educación Superior, no. 11, pp. 72–95, diciembre 2024.

[3] R. V. Roque y C. M. Juárez, "Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios", Paakat: Revista de Tecnología y Sociedad, no. 14, pp. 1-13, agosto 2018.

[4] H. Guo y H. Tinmaz, "A survey on college students' cybersecurity awareness and education from the perspective of China", Journal for the Education of Gifted Young Scientists, vol. 11, no. 3, pp. 351-367, octubre 2023.

[5] A. R. Nogueira. et al., "Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital", Texto libre, vol. 17, pp. 1-17, agosto 2024.

[6] B. Castillejos. et al., "La seguridad en las competencias digitales de los millennials", Apertura, vol. 8, no. 2, pp. 54-69, octubre 2016.

[7] K. Jenab y S. Moslehpour, "Cyber Security Management: A Review", Business Management Dynamics, vol. 5, no. 11, pp. 16-39, mayo 2016.

[8] V. Stanciu y A. Tinca, "Students' awareness on information security between own perception and reality – an empirical study", Accounting and Management Information Systems, vol. 15, no. 1, pp. 112-130, marzo 2016.

[9] M. M. Griffin y T. D. Steinbrecher, "Large-Scale Datasets in Special Education Research" en International Review of Research in Developmental Disabilities, vol. 45. Nashville: Elsevier, 2013, pp. 351-367.

[10] R. B. Kline, "Principles and Practice of Structural Equation Modeling", 4a. ed. New York: The Guilford Press, 2016.

[11] R. F. DeVellis, "Scale Development. Theory and Applications". New York: SAGE Publications, 2012.

[12] B. B. Byrne, "Structural Equation Modeling with AMOS", 2a. ed. New York: Routledge Taylor & Francis Group, 2010.

[13] M. Á. Cea, "Análisis multivariable. Teoría y práctica en la investigación social". Madrid: Síntesis, 2004.

[14] T. A. Brown, "Confirmatory Factor Analysis for Applied Research", 2a. ed. New York: The Guilford Press, 2015.

[15] D. Hooper. et al., "Structural Equation Modelling: Guidelines for Determining Model Fit", Electronic Journal of Business Research Methods, vol. 6, no. 1, pp. 53-60, enero 2008.

[16] L. Hu y P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", Structural Equation Modeling: A Multidisciplinary Journal, vol. 6, no. 1, pp. 1-55, noviembre 1999.