REVISTA CIENTÍFICA
CONECTIVIDAD
Instituto Superior Tecnológico Rumiñahui

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

Artículo Científico

Análisis de la protección digital y del ciberacoso en las redes sociales con estudiantes universitarios en Puebla, México

Analysis of Digital Protection and Cyberbullying on Social Media Among University Students in Puebla, Mexico

Luis Enrique Colmenares-Guillen[1], Edgar Genaro Olea Vidal[2]

[1] Benemérita Universidad Autónoma de Puebla, enrique.colmenares@correo.buap.mx, Puebla - México
[2] Benemérita Universidad Autónoma de Puebla, edgar.oleav@alumno.buap.mx, Puebla - México

Autor para correspondencia: enrique.colmenares@correo.buap.mx

RESUMEN

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) en la educación superior postpandemia ha transformado las interacciones sociales digitales. Sin embargo, esta expansión sostenida ha propiciado la emergencia de conductas de violencia en línea entre pares, como el ciberacoso. En este contexto, el objetivo de esta investigación es analizar la relación entre la Protección de datos digitales y la participación de los estudiantes en conductas de ciberacoso. Para esta investigación, se realizó un enfoque cuantitativo correlacional y diseño no experimental, transversal y ex post facto, aplicando encuestas digitales a 354 alumnos de la Facultad de Ciencias de la Computación de la BUAP. El análisis de los resultados, realizado con SPSS, indicó niveles altos de protección digital ($M = 3.18$, $DE = 0.54$) con una baja incidencia de ciberacoso ($M = 0.25$, $DE = 0.32$), revelando a la ciberagresión como predictor principal del fenómeno ($\beta = 0.779$, $p < 0.001$). Asimismo, se identificó una dinámica bidireccional y relacional entre los roles de cibervíctima ($\beta = 0.469$, $p < 0.001$; $R^2 = 0.230$) y ciberagresor ($\beta = 0.468$, $p < 0.001$; $R^2 = 0.231$). Se concluye que el ciberacoso en esta facultad depende principalmente de factores relacionales y conductuales, y su prevención requiere de una formación multidisciplinaria que integre ética digital y competencias socioemocionales.

Palabras clave: Ciberacoso; Protección Digital; Educación Superior; Redes Sociales.

ABSTRACT

The development of Information and Communication Technologies (ICT) in post-pandemic higher education has transformed digital social interactions. However, this continuous expansion has led to the emergence of online peer-to-peer violence, such as cyberbullying. In this context, the objective of this study is analyses the relationship between digital data protection and student participation in cyberbullying. For this study, a quantitative correlational approach was used, employing a non-experimental, cross-sectional, and ex post facto design, with digital surveys applied a sample of 354 students from the BUAP School of Computer Science. Analysis of the results, conducted using SPSS, indicated high levels of digital protection ($M = 3.18$, $SD = 0.54$) with a low incidence of cyberbullying ($M = 0.25$, $SD = 0.32$), revealing cyberaggression as the primary predictor of the phenomenon ($\beta = 0.779$, $p < 0.001$). Likewise, a bidirectional and relational dynamic was identified between the roles of cybervictim ($\beta = 0.469$, $p < 0.001$; $R^2 = 0.230$) and cyberaggressor ($\beta = 0.468$, $p < 0.001$; $R^2 = 0.231$). The conclusion is that cyberbullying in this college depends primarily on relational and behavioral factors, and prevention requires multidisciplinary training that integrates digital ethics and social-emotional skills.

Keywords: Cyberbullying; Digital Protection; Higher Education; Social Media.

Derechos de Autor

Los originales publicados en las ediciones electrónicas bajo derechos de primera publicación de la revista son del Instituto Superior Tecnológico Universitario Rumiñahui, por ello, es necesario citar la procedencia en cualquier reproducción parcial o total. Todos los contenidos de la revista electrónica se distribuyen bajo una licencia de Creative Commons Reconocimiento-NoComercial-4.0 Internacional.

Citar como:

Colmenares-Guillén, L. E., & Olea Vidal, E. G. (2026). Análisis de la protección digital y del ciberacoso en las redes sociales con estudiantes universitarios en Puebla, México. *CONECTIVIDAD, 7(2), e548.* https://doi.org/10.37431/conectividad.v7i2.548

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

1. INTRODUCCIÓN

El desarrollo creciente de las Tecnologías de la Información y la Comunicación (TIC) ha modificado de manera significativa los procesos de interacción social, académica y comunicativa en la educación superior. En el contexto universitario, los entornos virtuales han adquirido relevancia en el desarrollo de actividades académicas de los estudiantes, que interactúan constantemente y coordinan actividades con las redes sociales, plataformas digitales y sistemas de mensajería instantánea. Investigaciones recientes (Arif et al., 2024; Marrero-Sánchez & Vergara-Romero, 2023) señalan que este crecimiento sostenido en la sociabilidad digital ha favorecido la creación de nuevas formas de interacción, como los memes, que han propiciado a su vez la emergencia y consolidación de conductas de violentas en línea como el ciberacoso.

Alismaiel (2023) define el ciberacoso como una forma de violencia escolar ejercida por miembros de la comunidad educativa mediante el uso de TIC con el propósito de intimidar, humillar, amenazar o aislar socialmente a la víctima, enfatizando la agresión entre pares como carácter propio de este fenómeno. Esta conducta se manifiesta con insultos, amenazas, difusión de rumores, exclusión deliberada, humillación pública o divulgación de contenido ofensivo en plataformas digitales (Gallegos et al., 2025). Con respecto al acoso tradicional, el ciberacoso posee características particulares, por ejemplo, que se realiza de manera anónima, la permanencia del contenido ofensivo en línea, la rápida difusión de las agresiones y el alcance potencialmente ilimitado de la audiencia, factores que intensifican el impacto de la agresión sobre la víctima (Zhu et al., 2021).

Giumetti & Kowalski (2024) consideran el acoso tradicional, se restringe a contextos y espacios específicos, como la escuela o el trabajo, el ciberacoso se realiza en cualquier momento y lugar, acompañando a la víctima incluso dentro de espacios considerados seguros. Esta disponibilidad constante, dificulta que la persona afectada eluda las agresiones, lo cual genera la sensación de indefensión y vulnerabilidad. Karayol et al. (2025) identificaron roles de agresor, víctima y observador, en dinámicas de violencia digital ejercidas en redes sociales y aplicaciones de mensajería instantánea con estudiantes universitarios. Además, se ha observado que dichos roles no son estáticos, ya que una misma persona experimenta distintos niveles de participación en función de las circunstancias y contextos de la interacción digital.

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

Desde el ámbito de la salud mental, se han documentado síntomas de ansiedad, depresión, estrés, ideación suicida y alteraciones psicosomáticas (Usuga Jerez et al., 2023); mientras en el plano académico se observan dificultades de concentración, descenso en el rendimiento, abandono de actividades escolares y desmotivación hacia los estudios, a sí mismo, diversos autores advierten que el impacto del ciberacoso es más severo que el del acoso tradicional, debido al anonimato del agresor y a la continuidad de las agresiones en el tiempo (Ibrahim et al., 2024; Patchin & Hinduja, 2006).

En México, al menos un 20.4% (19.4 millones de personas) de la población de 12 o más reporta haber sido víctima de ciberacoso. De estos, un 23.5% de los hombres y el 28% de las mujeres de entre 20 y 29 años reportaron haber sido víctimas en 2025, observándose un aumento significativo en la población masculina con respecto al año anterior (22.1%) y un decremento para las mujeres (31.1%) Instituto Nacional de Estadística y Geografía [INEGI], (2025); Instituto Nacional de Estadística y Geografía [INEGI], (2026). Por otro lado, en el escenario postpandemia en el ámbito universitario en México, Vallejos-Parás et al. (2026) identificaron sobre una población de 863 estudiantes un 23% de frecuencia en conductas de ciberacoso. A su vez, documentaron dinámicas de socialización digital como la lectura de rumores en internet y el envío masivo de memes ofensivos o burlones como las agresiones más frecuentes entre pares universitarios.

En este escenario, las competencias digitales adquieren una relevancia particular para la comprensión y prevención del ciberacoso. Actualmente, estas competencias trascienden el simple dominio técnico de herramientas tecnológicas y abarcan conocimientos, habilidades y actitudes relacionadas con la comunicación responsable, la seguridad digital, la gestión de la identidad en línea, el pensamiento crítico y la convivencia ética en los entornos virtuales. De acuerdo con el Marco Europeo de Competencia Digital para la Ciudadanía (DigComp) (Vuorikari et al., 2022) las competencias digitales se clasifican en cinco áreas principales: alfabetización en información y datos; comunicación y colaboración; creación de contenido digital; seguridad y resolución de problemas.

La competencia Protección de datos digitales y privacidad online (Amador Alarcón et al., 2024) representa el conjunto de conocimientos, habilidades y prácticas orientadas a resguardar la información personal en entornos digitales, valorando la capacidad del individuo para identificar

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

riesgos relacionados con la exposición de datos personales, configurar adecuadamente los parámetros de privacidad, utilizar contraseñas seguras, gestionar permisos de acceso y adoptar conductas preventivas frente a posibles amenazas digitales. Desde esta perspectiva, el desarrollo de competencias digitales determina un factor protector frente a conductas de riesgo en línea, favoreciendo formas más seguras y responsables de participación en los espacios digitales (Marrero-Sánchez & Vergara-Romero, 2023; Uygun, 2025).

El objetivo de esta investigación es analizar la relación entre la competencia Protección de datos digitales y privacidad online con la participación de los estudiantes en conductas de agresión y victimización en ciberacoso en estudiantes de la Facultad de Ciencias de la Computación de la Benemérita Universidad Autónoma de Puebla (BUAP).

2. MÉTODOS

2.1. Diseño

La presente investigación tiene un enfoque cuantitativo de alcance correlacional y diseño no experimental de corte transversal. No se manipularon las variables y la recolección de datos se realizó en un único momento temporal con el fin de describir las variables y analizar su asociación (Hernández Sampieri & Mendoza Torres, 2018). Como variable independiente se tiene la competencia Protección de datos digitales y privacidad online, y por variables dependientes, la ciberagresión y la cibervictimización. Como variables de control o comparación se consideraron sexo, edad, carrera, semestre, red social de mayor uso, tiempo de conexión y configuración de cuentas.

2.2. Participantes

La muestra estuvo conformada por 354 estudiantes de la Facultad de Ciencias de la Computación de la BUAP, y se tiene evidencia empírica contextualizada en una población con un alto dominio técnico de las TIC. El muestreo fue de tipo no probabilístico por conveniencia, debido a la accesibilidad de los participantes y a las condiciones de aplicación del instrumento. Se incluyeron estudiantes de distintos semestres y programas académicos para lograr una mayor representatividad dentro de la facultad, sin excluir por edad o sexo. Se excluyó a aquellos participantes de la prueba piloto para evitar sesgos por familiarización con la prueba.

2.3. Instrumentos

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

En este apartado se describen los instrumentos de acuerdo con su orden de aplicación. El primero fue el cuestionario sociodemográfico. El cual constó de 7 ítems exploratorios sobre edad, sexo, carrera, semestre, red social mayor utilizada, tiempo promedio de conexión y configuraciones de perfiles de redes sociales.

El segundo cuestionario, el de protección de datos digitales y privacidad online (Amador Alarcón et al., 2024), diseñado para medir los conocimientos, habilidades y actitudes, que están asociados con esta competencia mediante 13 ítems con escala de respuesta tipo Likert de 1 a 4, en donde 1 = *totalmente en desacuerdo* y 4 = *muy de acuerdo.* Aunque este cuestionario está elaborado para el nivel medio superior, se revisó su pertinencia para el nivel superior y no se modificaron los ítems.

Por último, el Test de Ciberbullying, TCB (Garaigordobil, 2013), retomado de Martínez Ramón et al. (2020) en la creación de un instrumento diseñado para evaluar ciberacoso entre pares en educación superior. El TCB evalúa la frecuencia que se experimentan, observan o ejercen 15 conductas de ciberacoso, con un total de 45 ítems con cuatro opciones de respuesta: 0 = *nunca*, 1 = *casi nunca*, 2 = *en ocasiones* y 3 = *siempre*. Este instrumento fue seleccionado por su alta consistencia interna en la medición del ciberacoso. El instrumento fue creado para poblaciones de 12 a 18 años; sin embargo, tras la aplicación de la prueba piloto, no se identificaron problemas de comprensión que hicieran necesaria su adaptación a estudiantes universitarios. Posterior a dicha aplicación del piloto, se decidió eliminar la subescala de Ciberobservación, sin afectaciones que comprometieran la consistencia interna del instrumento.

Se conservó el formato original de respuesta para ambas escalas (0-3 y 1-4), con un total de 50 ítems, sociodemográficos incluidos. El instrumento final fue digitalizado mediante Google Forms y distribuido mediante código QR.

2.4. Piloto

Antes de la aplicación definitiva, se realizó una prueba piloto con una muestra de 83 estudiantes, de los cuales 3 se abstuvieron de responder, lo que dejó una muestra piloto final de 80 estudiantes. Esta cantidad se justifica metodológicamente de manera que un tamaño muestral de esta magnitud en una prueba piloto identifica errores de forma, además de realizar análisis preliminares tanto de consistencia interna (Alfa de Cronbach), como estadísticos descriptivos

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

para reducir el margen de error en la estimación de la fiabilidad del instrumento (Díaz Muñoz, 2020; Silva Medina, 2024).

Con base en la retroalimentación recibida por la muestra sobre la extensión del instrumento y los resultados de los análisis preliminares, se eliminó la subescala de *ciberobservación* para centrar el estudio en los roles de *cibervíctima* y *ciberagresor.* Su eliminación no supuso una afectación para la confiabilidad del instrumento, ya que el alfa de Cronbach es superior de 0.9 para ambas subescalas. Los resultados de los análisis de consistencia interna y de análisis estadísticos se muestran a continuación en Tabla 1 y Tabla 2. Los participantes del piloto no se incluyeron en la muestra final.

Tabla 1. Coeficiente Alfa de Cronbach de la encuesta piloto.

Escala / Subescala	N ítems	α Cronbach
Protección de datos digitales	13	0.918
Cibervictimización	15	0.900
Ciberagresión	15	0.996
Ciberobservación	15	0.932
Ciberacoso – Total	45	0.935

Tabla 2. Estadísticos descriptivos de la encuesta piloto.

Variable	N	Media (M)	Desviación estándar (DE)	Mínimo	Máximo
Ciberacoso total	80	0.51	0.46	0	3
Cibervictimización	80	0.35	0.41	0	3
Ciberagresión	80	0.74	1.18	0	3
Ciberobservación	80	0.43	0.51	0	3
Protección de datos digitales	80	3.07	0.72	1	4

Al finalizar la aplicación de la prueba piloto, se acercaron tres estudiantes para solicitar orientación y apoyo para casos de ciberacoso y extorsión, lo que manifiesta la importancia de atender las necesidades de participantes en situaciones sensibles como el ciberacoso. Se decidió incluir al final del formulario un directorio de apoyo y rutas de atención institucional para quienes lo necesitaran. A su vez, la participación fue voluntaria, anónima y confidencial, y se informó a los participantes de su derecho a retirarse en cualquier momento sin consecuencias. No se solicitaron datos de identificación directa, la información se analizó de forma agregada y solo el equipo de investigación tuvo acceso a ella.

2.5. Análisis de datos

Los análisis de datos se realizaron con el software IBM SPPS Statistics 26. Primero, se calcularon

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

la consistencia interna de los instrumentos mediante el α de Cronbach y ω de McDonald, y los estadísticos descriptivos utilizando frecuencias, porcentajes, medias y desviaciones estándar. Posteriormente, se ejecutó un análisis correlacional para determinar la relación entre variables, seguido del coeficiente de correlación de Spearman y del análisis de regresión lineal múltiple con el objetivo de identificar los factores que explican la incidencia de ciberacoso. Se finalizó con una serie de análisis no paramétricos para evaluar diferencias entre grupos.

2.6. Consentimiento Informado

De acuerdo con el código ético del psicólogo (Del Carmen Ángeles Calderón et al., 2009) y la ley de protección de datos (Presidencia de la República, 2010), previo a la aplicación de los instrumentos, se informó a los participantes sobre el objetivo de la investigación, sobre la recopilación de los datos, sin registro del correo electrónico y sobre el tratamiento que se les daría a los datos recopilados, a los cuales tuvo acceso sólo el equipo de investigación. Se les informó que la participación sería libre y voluntaria y previo a iniciar con el cuestionario, se les administró un consentimiento informado.

3. RESULTADOS

El análisis de la fiabilidad de los instrumentos mostró una consistencia interna adecuada. La escala de Protección de datos digitales obtuvo α = 0.848 y ω = 0.846. La subescala cibervictimización obtuvo α = 0.889 y un ω = 0.886 y la de ciberagresión obtuvo α = 0.925 y un ω = 0.923. La escala total ciberacoso obtuvo α = 0.918 y ω = 0.916. Los valores superiores a 0.80 indican una fiabilidad fuerte, mientras que valores cercanos o superiores a 0.90 indican una consistencia interna excelente. En la Tabla 3 se visualizan los resultados de los datos analizados.

Tabla 3. Coeficientes de Alfa de Cronbach y Omega de McDonald de los instrumentos.

Escala / Subescala	N ítems	α Cronbach	ω McDonald
Protección de datos digitales	13	0.848	0.846
Cibervictimización	15	0.889	0.886
Ciberagresión	15	0.925	0.923
Ciberacoso – Total	30	0.918	0.916

Los resultados de la encuesta muestran que el grupo predominante por edad fue de 17 a 20 años, con una mayor representación de hombres. La red social más utilizada registrada fue TikTok, en cuanto al tiempo promedio de conexión, el grupo predominante fue el de 4 – 6 h, y en la configuración de redes sociales, la mayoría reportó tener configuración privada. Ver Tabla 4.

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

Tabla 4. Resultados de dimensión Datos Demográficos.

Dimensión 1: Datos Demográficos							
Edad	17 – 20 (44.6%)	21 – 23 (38.7%)	24 – 26 (9.9%)	27 – 29 (4.5%)	Otra (2.3%)		
Sexo	Hombre (74.3%)	Mujer (23.7%)	Prefiero no decirlo (2%)				
Carrera	Lic. Cs. Datos (4.2%)	Lic. Cs. Computación (19.5%)	Ing. TICs (15%)	Ing. Cs. Computación (61.3%)			
Semestre	1 – 2 (7.4%)	3 – 4 (29.9%)	5 – 6 (33.1%)	7 – 8 (20.6%)	9 – 10 (9%)		
Red Social	TikTok (37.9%)	Instagram (29.4%)	WhatsApp (9.9%)	Facebook (4.8%)	X (Twitter) (2%)	YouTube (15%)	Otra (1.1%)
Tiempo de Conexión	1 – 3h (36.4%)	4 – 6h (50.3%)	7 – 9h (11%)	10 o más h (2.3%)			
Configuración Red Social	Pública (39.5%)	Privada (60.5%)					

Las variables principales del estudio se muestran en la Tabla 5. Los estudiantes reportaron un nivel alto de protección digital (M = 3.18, DE = 0.54; rango posible mínimo 1 – máximo 4). En contraste, los puntajes de ciberacoso fueron bajos, tanto en cibervictimización (M = 0.39, DE = 0.45) como en ciberagresión (M = 0.11, DE = 0.29; rango posible mínimo 0 – máximo 3).

Tabla 5. Estadísticos descriptivos de variables principales.

Variable	N	Media (M)	Desviación estándar (DE)	Mínimo	Máximo
Protección digital	354	3.18	0.54	1	4
Ciberacoso	354	0.25	0.32	0	3
Cibervictimización	354	0.39	0.45	0	3
Ciberagresión	354	0.11	0.29	0	3

Sobre la prevalencia del ciberacoso, se consideró que un estudiante participaba en un rol cuando reportó al menos una conducta con valor de respuesta mayor a 0 (*nunca*). Bajo este criterio, el 85% (n = 301) fue clasificado como cibervíctima y el 47.5% (n = 168) como ciberagresor. El 44.4% (n = 157) de la muestra presentó ambos roles, el 40.7% solo presentó el rol de cibervíctima, el 3.1 % solo el de ciberagresor y el 11.9% reportó ninguno de los anteriores como se muestra en la Tabla 6. La ciberagresión fue más frecuente en hombres (55.1%) que en mujeres (25%), sin diferencias significativas en cibervictimización, con 86.7% en hombres y 78.6% en mujeres. El 17.2% de la muestra reportó al menos una conducta con valor 4 (*siempre*). Las correlaciones no paramétricas de Spearman entre las variables del estudio se presentan en la Tabla 7. Los resultados identificaron correlaciones positivas significativas entre cibervictimización

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

y ciberagresión (ρ = .415, p < .001), lo que sugiere una relación consistente entre ambas variables.

Tabla 6. Prevalencia de los roles de ciberacoso.

Categoría	n	%
Cibervíctima	301	85.0
Ciberagresor	168	47.5
Ambos roles	157	44.4
Solo víctima	144	40.7
Solo agresor	11	3.1
Algún rol	312	88.1
Ninguno	42	11.9

Tabla 7. Matriz de correlaciones de Spearman.

Variable	1	2	4
Protección digital	—		
Cibervictimización	-.058	—	
Ciberagresión	-.150**	.415**	—

Por otro lado, se observó una relación negativa débil entre los factores de protección digital y la conducta agresora (ρ = -.150, p = .005), lo que evidencia un efecto modulador limitado.

Por otro lado, para analizar los factores asociados a los roles de ciberagresor y cibervíctima, se ajustaron dos modelos de regresión lineal múltiple en los cuales se incorporaron la protección digital, el tiempo de conexión y la configuración de la cuenta como variables adicionales. En el primer modelo que se muestra en la Tabla 8. El modelo para ciberagresión fue significativo (F (4, 349) = 26.03, p < .001), con un coeficiente de determinación de la varianza de R^2 = .230, demuestra que la cibervictimización fue el único predictor significativo (β = .469, p < .001).

Tabla 8. Regresión lineal múltiple para ciberagresión.

Predictor	B	EE	β	t	p	IC 95 %
Cibervictimización	0.299	0.030	.469	9.92	<.001**	[0.239, 0.358]
Protección digital	-0.009	0.025	-.017	-0.35	.724	[-0.059, 0.041]
Tiempo conexión	0.024	0.019	.060	1.28	.201	[-0.013, 0.061]
Configuración cuenta	0.015	0.028	.025	0.53	.596	[-0.040, 0.070]

Nota. N = 354; F(4, 349) = 26.03, p < .001; R^2 = .230; R^2 ajustada = .221. Tiempo de conexión: 1 = 1–3 h, 2 = 4–6 h, 3 = 7–9 h, 4 = 10 h o más; configuración de la cuenta: 1 = pública, 2 = privada. IC 95 % = intervalo de confianza al 95 %.

El segundo modelo en la Tabla 9, la regresión lineal para predecir cibervictimización también fue significativo (F (4, 349) = 26.25, p < .001), con un coeficiente de determinación de R^2 = .231, en el cual encontró una asociación con la ciberagresión (β = .468, p < .001), que evidencia una relación recíproca entre ambas variables. Ninguna otra variable mostró asociaciones

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

significativas (valores de p > .20), esto en conjunto con los resultados, sugiere una dinámica bidireccional entre cibervictimización y ciberagresión, posicionando a ambas como elementos centrales en la comprensión del ciberacoso. Dado el diseño transversal del estudio, los resultados no permiten establecer el orden temporal entre roles ni su secuencia.

Tabla 9. Regresión lineal múltiple para cibervictimización.

Predictor	B	EE	β	t	p	IC 95 %
Ciberagresión	0.736	0.074	.468	9.92	<.001**	[0.590, 0.882]
Protección digital	-0.024	0.040	-.028	-0.59	.554	[-0.102, 0.055]
Tiempo conexión	0.032	0.030	.051	1.07	.285	[-0.027, 0.090]
Configuración cuenta	-0.043	0.044	-.047	-0.98	.328	[-0.130, 0.044]

Nota. N = 354; F(4, 349) = 26.25, p < .001; R^2 = .231; R^2 ajustada = .222. Tiempo de conexión: 1 = 1–3 h, 2 = 4–6 h, 3 = 7–9 h, 4 = 10 h o más; configuración de la cuenta: 1 = pública, 2 = privada. IC 95 % = intervalo de confianza al 95 %.

Respecto a la configuración de la cuenta, de acuerdo con los resultados mostrados en la Tabla 10, se encontraron diferencias en protección digital (p < .001), siendo mayor en cuentas privadas. En cambio, la conducta agresora (p = .048) fue mayor en cuentas públicas. No se encontraron diferencias en ciberacoso ni victimización.

Tabla 10. Diferencias por configuración de cuenta (Cuenta pública o privada).

Variable	U	p
Protección digital	11565	<.001*
Ciberacoso	13169	0.054
Cibervictimización	13391	0.090
Ciberagresión	13268	0.048*

Para concluir, se realizaron análisis no paramétricos para evaluar diferencias entre grupos. Se encontraron diferencias significativas según el sexo en ciberacoso (p = .003), victimización (p = .027) y conducta agresora (p < .001), siendo los hombres quienes presentaron mayores niveles en estas variables. No se observaron diferencias en protección digital. Los resultados se muestran en la Tabla 11.

Tabla 11. Diferencias por sexo.

Variable	U	p
Protección digital	11042	.996
Ciberacoso	8689	.003*
Cibervictimización	9289	.027*
Ciberagresión	7383	<.001*

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

4. DISCUSIÓN

Para la discusión, con respecto a la presencia de ciberacoso, se encontró una participación amplia con baja frecuencia de conductas de ciberacoso, lo que explica la baja media de las variables y su alta prevalencia, ya que, al considerarse cualquier respuesta distinta de "nunca", el 85.0 % de los estudiantes reportó al menos una conducta de cibervictimización y el 47.5% al menos una de ciberagresión. Estas cifras se consideran con la frecuencia: en el 31.9% de la muestra la frecuencia máxima como víctima fue "casi nunca", y el 17.2% reportó alguna conducta con frecuencia "siempre". Sin embargo, aplicando como criterio más estricto sólo la incidencia de conductas "en ocasiones" o "siempre", la prevalencia fue de 53.1 % para cibervictimización y 18.6 % para ciberagresión. Dichos valores superan el 33.5 % que reporta el INEGI (2026) población de nivel superior. En conjunto, los resultados en el contexto universitario sugieren que la exposición a conductas hostiles en línea es amplia, aunque menos recurrente. En INEGI (2026) registró una incidencia de 28% en mujeres y 23.5% en hombres en el grupo de edad de 20 a 29 años, lo que ofrece un marco de referencia relevante para contextualizar los resultados en cuestión de género.

Al analizar la variable ciberagresión, se encontró una desviación estándar que supera en más del doble a su media ($M = 0.11$, $DE = 0.28$), lo que sugiere que la agresión se concentra en una sola conducta. Al profundizar en este fenómeno, se identificó que la causa reside en el ítem 1 de la subescala ciberagresión ¿Has enviado mensajes ofensivos e insultantes mediante el teléfono móvil o Internet?, con un porcentaje de respuesta de 41,5%, con relación a los demás ítems que tienen un porcentaje medio de 5% y en el cual el 44% de los agresores lo reportaron como única conducta agresora. Dicho fenómeno se atribuye a dinámicas sociales de comunicación entre la comunidad universitaria, en la cual se observa la normalización de la violencia a nivel de mensaje y burla a través de memes (García Hernández et al., 2024).

Un hallazgo relevante radica en la correlación positiva entre cibervictimización y ciberagresión ($\rho = .415$, $p < .001$), lo que evidencia una importante intersección entre ambos constructos. Este resultado muestra la presencia de un traslape de roles que da lugar a perfiles híbridos como el de cibervíctima-ciberagresor o ciberagresor-cibervíctima. La magnitud de la correlación en este estudio refuerza la necesidad de comprender el ciberacoso no como categorías aisladas, sino

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

como un proceso dinámico de retroalimentación, donde la agresión surge como respuesta a experiencias previas de victimización (Buelga et al., 2020; Martínez-Ferrer et al., 2021).

Además, los modelos de regresión confirman la relación bidireccional entre variables cibervictimización y ciberagresión. Estos resultados refuerzan que la concepción del ciberacoso es una problemática relacional que representa que los roles se alternan según el contexto. Las conductas previas de ciberagresión equivalen al mayor predictor para la cibervictimización y viceversa. La presencia de estos factores ha complejizado su abordaje, por lo que se requiere que esta dinámica multicausal sea considerada en el desarrollo de estrategias de intervención (Vallejos-Parás et al., 2026; Walrave & Heirman, 2011).

Por otro lado, los resultados evidenciaron una relación significativa débil (ρ = -.150, p = .005) entre la conducta agresora y la variable protección digital. Lo cual, demuestra que para disminuir la incidencia de ciberacoso se necesitan estrategias que consideren la formación en competencias socioemocionales en conjunto con el desarrollo de habilidades para el dominio de las TIC y seguridad digital (Uygun, 2025; Vallejos-Parás et al., 2026; Wright, 2018).

Con respecto a las diferencias por sexo, los resultados mostraron que los hombres presentan mayores niveles de ciberacoso, cibervictimización y ciberagresión. Estos hallazgos coinciden con investigaciones recientes realizadas en población universitaria, donde hay diferencias significativas en la implicación de conductas en ciberacoso referente al sexo (Martínez-Monteagudo et al., 2021).

Asimismo, diversos estudios señalan que los hombres presentan una mayor participación en roles de agresión y agresión-victimización dentro de los entornos digitales. Desde esta perspectiva, las diferencias se explican a partir de patrones socioculturales asociados a la construcción de la masculinidad, los cuales favorecen formas más directas de expresión de la agresividad. Este hecho refuerza la idea que el ciberacoso constituye un fenómeno dinámico en el cual los individuos desempeñan simultáneamente o de manera alternada los roles de agresor y víctima (Herrera López et al., 2025).

De manera similar, en el uso de redes sociales, los resultados en esta investigación indican que existen diversas plataformas asociadas a la presencia de ciberacoso. Esto coincide con Gottschalk (2022), que señala como características principales la inmediatez de la comunicación,

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

la posibilidad del anonimato, la amplia difusión de contenido y el uso generalizado de las TIC que favorecen la aparición de conductas de ciberacoso, sin que sea determinante la red social.

Finalmente, en relación con la protección de datos digitales, se encontró que usuarios con cuentas privadas presentan mayores niveles de protección, lo cual coincide con Gómez Cruz (2023), que destacan la importancia de las configuraciones de privacidad y del control de la información personal que se comparte como medida para reducir la exposición a riesgos en entornos digitales, y que, en consecuencia, posee una incidencia indirecta en el ciberacoso.

Para afrontar el reto del ciberacoso, se necesitan estrategias que consideren factores sociales, relacionales, conductuales y tecnológicos, y que la protección digital y el desarrollo de una ética interaccional enfocada en espacios digitales sean pilares de esta comunicación virtual.

5. CONCLUSIONES

Las conclusiones de los resultados en la investigación demuestran la relación entre la incidencia de ciberacoso en el nivel de educación superior y los alcances reales de la protección digital como estrategia preventiva.

Los resultados confirman que el ciberacoso está ampliamente presente en la población universitaria, aunque con niveles bajos de frecuencia, valores que se observan en las medias de cibervictimización ($M = 0.39$, $DE = 0.45$) y ciberagresión ($M = 0.11$, $DE = 0.28$) y la prevalencia del ciberacoso (85% ($n = 301$) fue clasificado como cibervíctima y el 47.5% ($n = 168$) con base al criterio $n > 0$ "*nunca*"). Los valores de la media y la desviación estándar de la variable ciberagresión indican la presencia de conductas concretas de agresión recurrentes, con valores altos en casos como la comunicación entre pares por mensaje o llamada. Estos resultados afirman la incidencia de violencia normalizada a nivel comunicacional entre pares universitarios.

Otra aportación de este estudio es la relación bidireccional entre cibervictimización y ciberagresión, respaldada tanto por correlaciones significativas ($\rho = .415$, $p < .001$) como por modelos de regresión (cibervictimización predice ciberagresión, $\beta = .469$, $p < .001$, $R^2 = .230$; ciberagresión predice cibervictimización, $\beta = .468$, $p < .001$, $R^2 = .231$). De esta manera, los resultados demuestran que los estudiantes que han sido víctimas de ciberacoso presentan una mayor probabilidad de ejercer conductas agresivas y viceversa. Por ejemplo, estudiantes que reportaron recibir mensajes ofensivos (214, frecuencia $n > 1$) también reconocieron replicar

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

esta conducta (147, frecuencia n > 1). Este resultado demuestra que el ciberacoso opera como una dinámica relacional de retroalimentación en el cual los roles se intercambian según varíen las circunstancias, de tal manera que el agresor se convierta en víctima y la víctima en agresor.

Respecto a las competencias en protección de datos digitales, se reportaron niveles similares de victimización entre estudiantes con puntajes tanto altos como bajos en protección digital, lo que demuestra de manera independiente con respecto a la protección digital, existe una alta probabilidad de ser víctima de agresiones en línea, especialmente si se trata de interacciones sociales entre pares. Esta afirmación se refuerza al observar los resultados del análisis correlacional, que reporta una relación baja entre la competencia protección de datos digital, cibervictimización ($p = -.058$, $p = .005$) y ciberacoso ($p = -.095$, $p = .005$).

Con respecto a la relación de las variables protección de datos digital y ciberagresión, se identificó una relación negativa débil significativa ($\rho = -.150$, $p = .005$), lo que indica que los estudiantes que adoptan prácticas más cuidadosas durante la interacción digital se involucran menos en conductas de ciberagresión, revelando el papel de la protección digital como un regulador conductual durante las interacciones en línea y reforzando la importancia de diseñar una intervención de carácter multidisciplinario que contemple la formación integral del alumno en la adquisición de competencias tanto socioemocionales como tecnológicas.

Contribución de los Autores (CRediT): LECG: Conceptualización, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Supervisión, Validación, Visualización, Redacción - revisión y edición. EGOV: Curación de datos, Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original, Redacción - revisión y edición.

Conflicto de Intereses: Los autores declaran que no existen conflictos de intereses en esta publicación.

Declaración de Uso de Inteligencia Artificial: El autor LECG declara que utilizó una herramienta de inteligencia artificial (IA) en la corrección de estilo del artículo. La herramienta utilizada para este fin fue: COPILOT.

REFERENCIAS

Alismaiel, O. A. (2023). Digital Media Used in Education: The Influence on Cyberbullying Behaviors among Youth Students. *International Journal of Environmental Research and Public Health, 20*(2), 1370. https://doi.org/10.3390/ijerph20021370

Amador Alarcón, M. del P., Torres Gastelú, C. A., Lagunes Domínguez, A., & Medina Cruz, H. (2024). Diagnóstico sobre percepciones respecto a la competencia protección de datos digitales en estudiantes de educación media superior en México. *Revista del Centro de Investigación de la*

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

Universidad la Salle, *16*(62), 119–136. https://doi.org/10.26457/recein.v16i62.3900

Arif, A., Qadir, M. A., Martins, R. S., & Khuwaja, H. M. A. (2024). The impact of cyberbullying on mental health outcomes amongst university students: A systematic review. *PLOS Mental Health*, *1*(6), e0000166. https://doi.org/10.1371/journal.pmen.0000166

Buelga, S., Postigo, J., Martínez-Ferrer, B., Cava, M. J., & Ortega-Barón, J. (2020). Cyberbullying among adolescents: Psychometric properties of the CYB-AGS cyber-aggressor scale. *International Journal of Environmental Research and Public Health, 17*(9), 3090. https://doi.org/10.3390/ijerph17093090

Del Carmen Ángeles Calderón, A., Tavera, A. A., Becceril, M. F. B., Pérez, M. R. G., Meza, A. L., Montalvo, S. L., Otero, S. M., & Chaire, M. F. M. (2009). Código ético del psicólogo. *Huella de la Palabra, 3*. https://doi.org/10.37646/huella.vi3.511

Díaz-Muñoz, G. (2020). Metodología del estudio piloto. *Revista chilena de radiología, 26*(3), 100–104. https://doi.org/10.4067/S0717-93082020000300100

Gallegos, A., García Ampudia, L., Morales Córdova, H., Londoño-Celis, W., Velazco Mendoza, O. A., & Valencia, J. (2025). Cyberbullying in students: forms of aggression, risk factors, and educational responses in digital environments. *F1000Research*, *14*, 880. https://doi.org/10.12688/f1000research.168253.1

Garaigordobil, M. (2013). *Cyberbullying: Screening de Acoso entre Iguales.* TEA Ediciones, S.A.U. https://hogrefe-tea.com/recursos/Ejemplos/Cyberbullying_manual_extracto.pdf

García Hernández, K. J., Palmeros y Ávila, G., & Coeto Calcaneo, I. A. (2024). Dinámicas de convivencia y esparcimiento adoptadas por estudiantes universitarios en el contexto pospandemia. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *14*(28). https://doi.org/10.23913/ride.v14i28.1840

Giumetti, G. W., & Kowalski, R. M. (2024). Mattering Matters: Examining the Moderating Role of Mattering in Cyberbullying Victimization-Outcome Relationships Among College Students. *International Journal of Environmental Research and Public Health*, *21*(11), 1391. https://doi.org/10.3390/ijerph21111391

Gómez Cruz, B. M. (2023). Lo digital es político: universitarias frente a la violencia digital hacia las mujeres. *Revista pueblos y fronteras digital*, *18*, 1–28. https://doi.org/10.22201/

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

cimsur.18704115e.2023.v18.640

Gottschalk, F. (2022). Cyberbullying: An overview of research and policy in OECD countries. *OECD Education Working Papers, No. 270.* OECD Publishing, Paris. https://doi.org/10.1787/f60b492b-en

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación : las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Herrera López, H. M., Sánchez Reina, M., Solarte Portilla, A. L., & Herrera Solarte, L. (2025). Cyberbullying en la universidad: un estudio descriptivo e instrumental con universitarios surcolombianos. *Informes Psicológicos*, *25*(1), 79–95. https://doi.org/10.18566/infpsic.v25n1a05

Ibrahim, F. M., Rashad Dabou, E. A., AbdelSamad, S., & Abuijlan, I. A. M. (2024). Prevalence of bullying and its impact on self-esteem, anxiety and depression among medical and health sciences university students in RAS Al Khaimah, UAE. *Heliyon*, *10*(3). https://doi.org/10.1016/j.heliyon.2024.e25063

Instituto Nacional de Estadística y Geografía [INEGI]. (2025). *Módulo sobre Ciberacoso (MOCIBA) 2024*. https://www.inegi.org.mx/programas/mociba/2024/

Instituto Nacional de Estadística y Geografía [INEGI]. (2026). *Módulo sobre Ciberacoso (MOCIBA) 2025.* https://www.inegi.org.mx/programas/mociba/2025/

Karayol, M., Murathan, T., Erdoğan, R., Akarsu, M., Baş, M., & Norman, G. (2025). Investigating the relationship between digital citizenship levels and cyberbullying attitudes of university students. *Frontiers in Psychology*, *16*. https://doi.org/10.3389/fpsyg.2025.1664397

Marrero-Sánchez, O., & Vergara-Romero, A. (2023). Digital competence of the university student. A systematic and bibliographic update. *Revista Amazonia Investiga*, *12*(67), 9–18. https://doi.org/10.34069/ai/2023.67.07.1

Martínez Ramón, J. P., Méndez, I., Ruiz-Esteban, C., & Cerezo Ramirez, F. (2020). Validation and reliability of the Questionnaire on Harassment among University Students (QAEU). *Revista Fuentes, 22*(1), 88–104. https://doi.org/10.12795/revistafuentes.2020.v22.i1.08

Martínez-Ferrer, B., León-Moreno, C., Suárez-Relinque, C., Del Moral-Arroyo, G., & Musitu-

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

Ochoa, G. (2021). Cybervictimization, Offline Victimization, and Cyberbullying: The Mediating Role of the Problematic Use of Social Networking Sites in Boys and Girls. *Psychosocial Intervention*, *30*(3), 155–162. https://doi.org/10.5093/PI2021A5

Martínez-Monteagudo, M. C., Aparisi, D., Delgado, B., León Antón, M. J., & Poveda Brotons, R. (2021). Ciberacoso en el ámbito universitario. Diferencias por sexo y curso académico. *Memorias del Programa de Redes-I3CE de calidad, innovación e investigación en docencia universitaria*, (Convocatoria 2020-21), 1435–1442. https://hdl.handle.net/10045/120808

Patchin, J. W., & Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169. https://doi.org/10.1177/1541204006286288

Presidencia de la República. (2010, 05 de julio). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Diario Oficial de la Federación [DOF]. (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Silva Medina, Y. (2024). El papel crucial de la prueba piloto dentro del proceso metodológico de investigación. En F. Cornejo Hernández y G. Sánchez López (Coordinadores) *Convivencia y Compementariedad Metodológica. Conceptos, Técnicas y Estrategias para el Estudio de lo Social* (77–93). ITESO, A.C. https://doi.org/10.31391/OPOB3342.6

Usuga Jerez, A. J., Lemos Ramírez, N. V., Gómez Camargo, M. F., & Adarme López, E. M. (2023). Ciberbullying durante la pandemia por covid-19: un estudio en adolescentes de Santander, Colombia. *Diversitas*, *19*(1), 95–108. https://doi.org/10.15332/22563067.9169

Uygun, D. (2025). The Relationship Between Digital Competence and Cyberbullying in Fourth-Grade Students. *TOJET: The Turkish Online Journal of Educational Technology, 24*(1), 72-80. https://files.eric.ed.gov/fulltext/EJ1466299.pdf

Vallejos-Parás, C., Andrade-Rosas, L.-A., & Echeverría-García, J. (2026). Cyberbullying among university students in the post-pandemic period: aggresive behaviors and prevention. *Revista Panamericana De Pedagogía, 41.* https://doi.org/10.21555/rpp.3467

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2, The Digital Competence framework for citizens: with new examples of knowledge, skills and attitudes.* Publications Office of

Fecha de recepción: 28 / 07 / 2026
Fecha de aceptación: 04 / 11 / 2026
Fecha de publicación: 19 / 11 / 2026

the European Union. https://data.europa.eu/doi/10.2760/115376

Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. *Children and Society*, *25*, 59–72. https://doi.org/10.1111/j.1099-0860.2009.00260.x

Wright, M. (2018). Cyberbullying Victimization through Social Networking Sites and Adjustment Difficulties: The Role of Parental Mediation. *Journal of the Association for Information Systems*, *19*(2), 113–123. https://doi.org/10.17705/1jais.00486

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health, 9*. https://doi.org/10.3389/fpubh.2021.634909