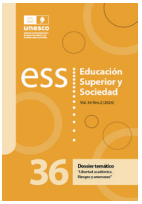


REVISTA EDUCACIÓN SUPERIOR Y SOCIEDAD
2024, Vol.36 Nro.2 (jul. - dic.), pp. 316-344
https://doi.org/10.54674/ess.v36i2.917
e-ISSN: 26107759
Recibido 2023-07-01 | **Revisado** 2023-08-12
Aceptado 2024-10-14 | **Publicado** 2024-12-27

7. Acoso cibernético a universitarios creadores de contenido: análisis y medidas de prevención en Bolivia

Cyberbullying to Students of University Content Creators: Analysis, Prevention Recurses in Bolivia

José Gunnar Zapata Zurita *

* Universidad Mayor de San Simón, Cochabamba, Bolivia

RESUMEN

Este artículo se centra en el acoso cibernético a creadores de contenido universitario en Cochabamba, Bolivia. Se busca identificar los delitos cometidos contra estos estudiantes, los patrones de comportamiento delictivo y las medidas preventivas adoptadas por las universidades. La metodología empleada es mixta, combinando 864 encuestas a estudiantes de la Universidad Mayor de San Simón, la Universidad Católica Boliviana "San Pablo" y la Escuela Militar de Ingeniería "Mariscal Antonio José de Sucre". Además, se realizaron entrevistas a responsables de sistemas y seguridad informática, creadores de contenido y autoridades policiales, durante noviembre y diciembre de 2023. Se analiza la prevalencia del acoso, desde solicitudes de información personal hasta hackeo de cuentas, resaltando la vulnerabilidad de estos creadores. Los hallazgos subrayan la necesidad de concienciación sobre seguridad cibernética y la importancia de la colaboración entre universidades y creadores de contenido para desarrollar estrategias de prevención integrales. Se enfatiza la urgencia de revisar y actualizar la legislación boliviana en materia de acoso cibernético, así como la necesidad de una respuesta eficaz por parte de las autoridades judiciales. El artículo destaca la importancia de un enfoque multidisciplinario y colaborativo que combine medidas tecnológicas, educativas, legales y recursos comunicativos para crear un entorno digital más seguro. Este estudio es un paso importante para entender y combatir el acoso cibernético en Bolivia, y puede servir como base para futuras investigaciones y políticas en esta área.

Palabras clave: Acoso; estudiante; universidad; protección de datos; medios sociales

Cyberbullying to Students of University Content Creators: Analysis, Prevention resources in Bolivia

ABSTRACT

This paper focuses on cyberbullying among university content creators in Cochabamba, Bolivia. It seeks to identify the crimes committed against these students, the patterns of criminal behavior, and the preventive measures adopted by universities. The methodology used is mixed, combining 864 surveys of students from the Universidad Mayor de San Simón, the Universidad Católica Boliviana "San Pablo," and the Escuela Militar de Ingeniería "Mariscal Antonio José de Sucre. In addition, interviews were conducted with responsible individuals in systems and computer security, content creators, and law enforcement authorities during November and December 2023. This paper analyzes the prevalence of bullying, from requests for personal information to account hacking, highlighting the vulnerability of these creators. The findings emphasize the need for awareness of cybersecurity and the importance of collaboration between universities and content creators to develop comprehensive prevention strategies. It underscores the urgency of reviewing and updating Bolivian legislation on cyberbullying, as well as the need for an effective response from judicial authorities. The article highlights the importance of a multidisciplinary and collaborative approach that combines technological, educational, legal, and communicative measures to create a safer digital environment. This study is an important step in understanding and combating cyberbullying in Bolivia and may serve as a basis for future research and policies in this area..

Keywords: Bullying; students; university; data protection; social media

Cyberbullying para universitários criadores de conteúdo: análise e medidas de prevenção na Bolívia

RESUMO

Este artigo foca no cyberbullying entre criadores de conteúdo universitário em Cochabamba, Bolívia. Busca-se identificar os crimes cometidos contra esses estudantes, os padrões de comportamento criminoso e as medidas pre-

ventivas adotadas pelas universidades. A metodologia utilizada é mista, combinando 864 pesquisas com estudantes da Universidad Mayor de San Simón, da Universidad Católica Boliviana "San Pablo" e da Escuela Militar de Ingeniería "Mariscal Antonio José de Sucre". Além disso, foram realizadas entrevistas com responsáveis por sistemas e segurança da informação, criadores de conteúdo e autoridades policiais durante novembro e dezembro de 2023. Analisa-se a prevalência do bullying, desde pedidos de informações pessoais até hacking de contas, destacando a vulnerabilidade desses criadores. Os resultados enfatizam a necessidade de conscientização sobre segurança cibernética e a importância da colaboração entre universidades e criadores de conteúdo para desenvolver estratégias abrangentes de prevenção. Sublinha-se a urgência de revisar e atualizar a legislação boliviana sobre cyberbullying, bem como a necessidade de uma resposta eficaz por parte das autoridades judiciais. O artigo destaca a importância de uma abordagem multidisciplinar e colaborativa que combine medidas tecnológicas, educacionais, legais e comunicativas para criar um ambiente digital mais seguro. Este estudo é um passo importante para entender e combater o cyberbullying na Bolívia e pode servir como base para futuras pesquisas e políticas nesta área..

Palavras-chave: Assédio; estudantes; universidade; proteção de dados; mídia social.

Cyberharcèlement parmi les créateurs de contenu universitaire : analyse et mesures de prévention en Bolivie

RÉSUMÉ

Cet article se concentre sur le cyberharcèlement parmi les créateurs de contenu universitaire à Cochabamba, en Bolivie. Il vise à identifier les crimes commis contre ces étudiants, les schémas de comportement criminel et les mesures préventives adoptées par les universités. La méthodologie utilisée est mixte, combinant 864 enquêtes auprès des étudiants de l'Universidad Mayor de San Simón, de l'Universidad Católica Boliviana «San Pablo» et de l'Escuela Militar de Ingeniería «Mariscal Antonio José de Sucre ». De plus, des entretiens ont été menés avec des responsables des systèmes et de la sécurité informatique, des créateurs de contenu et des autorités policières pendant novembre et décembre 2023. On analyse la prévalence du harcèlement, des demandes d'informations personnelles au piratage de comptes, mettant en évidence la vul-

nérabilité de ces créateurs. Les résultats soulignent la nécessité de sensibiliser à la cybersécurité et l'importance de la collaboration entre les universités et les créateurs de contenu pour développer des stratégies de prévention globales. Il met en avant l'urgence de réviser et de mettre à jour la législation bolivienne sur le cyberharcèlement, ainsi que le besoin d'une réponse efficace des autorités judiciaires. L'article met en lumière l'importance d'une approche multidisciplinaire et collaborative combinant des mesures technologiques, éducatives, légales et communicatives pour créer un environnement numérique plus sûr. Cette étude est une étape importante dans la compréhension et la lutte contre le cyberharcèlement en Bolivie et peut servir de base pour de futures recherches et politiques dans ce domaine.

Mots clés: Brimade ; étudiante ; université ; Protection des données ; Médias sociaux.

1. INTRODUCCIÓN

En Bolivia, el 67,5% de la población tiene acceso a internet, lo que equivale a aproximadamente 7.3 millones de personas. De este porcentaje, el 95% de las personas mayores de 14 años tiene acceso a internet móvil, 68% se conecta a redes con frecuencia y el 45% busca entretenimiento o farándula en internet (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, 2017). Considerando a los creadores de contenido, su papel está centrado en individuos que comparten contenido a través de sus dispositivos móviles.

Esta investigación parte de un caso en particular. Camila Hidalgo Ayllón, estudiante y creadora de contenido, fue víctima de acoso cibernético o ciberacoso (acoso virtual) y ciber hostigamiento durante su etapa escolar. El conflicto surgió a partir de la difusión de un fotomontaje, creado por un compañero de su escuela, que superpuso el rostro de Hidalgo en una fotografía de contenido sexual, propia de la pornografía infantil. El acusado no proporcionó una explicación de sus acciones y diversos de sus compañeros difundieron tal imagen. Hidalgo tardó más de un año en descubrir lo ocurrido y, ante la desidia demostrada por las autoridades de su colegio, decidió presentar una querella formal ante la Defensoría de la Niñez y Adolescencia del Gobierno Autónomo Municipal de Cochabamba contra el agresor y quienes deliberadamente difundieron tal imagen. El caso aún no ha sido resuelto como corresponde, por limitaciones legales e informáticas.

Esta situación pone de manifiesto aspectos preocupantes: el riesgo que enfrentan los adolescentes populares en entornos educativos, la negligencia de determinadas instituciones educativas y las autoridades al no proporcionar el apoyo adecuado a la víctima, y la importancia de la cobertura mediática en la visibilización y prevención de estos delitos. Estas experiencias al ser frecuentes involucran el desarrollo de una investigación científica sobre el acoso cibernético a estudiantes bolivianos, con el fin de prevenir situaciones similares y promover una mayor justicia y asesoramiento para las víctimas.

Bajo esta premisa, este subtítulo parte de un estado de la cuestión y una revisión a la legislación boliviana, con referencia al acoso cibernético y los ciberdelitos. Posteriormente, son presentados el problema y los objetivos de investigación.

1.1. Estado de la cuestión

El término "cyberbullying" engloba acciones que ponen en peligro la vida de una persona, como acoso con comentarios malintencionados, creación de cuentas falsas en redes sociales, estafas informáticas y sextorsión.

Partiendo desde una mirada a la problemática señalada, en España, el investigador Meseguer González (2013) describe la evolución de los métodos utilizados por los delincuentes cibernéticos y los desafíos que enfrentan las autoridades policiales y judiciales de aquel país para combatirlos. Sugiere, además que, la implementación de soluciones de inteligencia avanzada puede ayudar a disminuir el impacto de los ciberataques y ahorrar costos significativos; concluyendo que los ciberdelitos pueden ocurrir en cualquier lugar del mundo y formular leyes para contrarrestarlos es sumamente complicado pero imprescindible.

Bajo esta mirada, los españoles Martínez Atienza y Fernández Bermejo (2020) subrayan la necesidad de adaptar la legislación a los avances tecnológicos y promover la cooperación internacional para abordar eficazmente esta problemática en el reino español.

De manera complementaria, la investigadora española Jiménez Rozas (2022) profundiza en el alcance global de los ciberdelitos, señalando cómo eventos como la pandemia de COVID-19 han exacerbado esta problemática. Destaca la importancia de una respuesta institucional efectiva para combatir este fenómeno, incluyendo la necesidad de una legislación robusta y mecanismos de denuncia ágiles. Jiménez, también, pone de relieve los desafíos en la comunicación y sensibilización del público en general sobre los riesgos del cibercrimen, especialmente en el contexto de entidades financieras.

En la literatura latinoamericana, investigadores como el colombiano Manjarrés Bolaño (2012), profundizan en los tipos de delitos informáticos y la legislación existente en la región. Sobre tal problemática, el investigador dominicano, Abreu Valencia (2022), destaca la importancia de comprender los riesgos asociados a la dependencia de las sociedades occidentales de los sistemas informáticos y electrónicos, así como la necesidad de fortalecer la cooperación internacional en la lucha contra el cibercrimen en la República Dominicana.

Retornando a Colombia, Herrera-López *et al.* (2023) investigaron la producción bibliográfica referida a la temática señalada para determinar los valores de prevalencia. Analizaron 234 artículos, identificando que la mayoría aborda el *bullying*, con escasa atención al *ciberbullying*. Se destaca la prevalencia del mencionado delito, con estudios que reportan cifras entre el 20% y el 30%, mientras que para el ciberbullying se reconocen valores entre el 2.5% y el 42.5%. Estos resultados reflejan tendencias de investigación a nivel global y sugieren una reducción en la brecha tecnológica entre Latinoamérica y los países desarrollados, aunque también evidencian un bajo impacto de las publicaciones y una contribución limitada al cuerpo teórico de estos fenómenos.

La investigadora argentina Mercol (2022) aborda la necesidad de concientizar sobre los ciberdelitos, especialmente en el ámbito bancario. La autora propone estrategias y temáticas para desarrollar campañas de sensibilización, destacando la importancia de una comunicación efectiva en la prevención de estos delitos. Los investigadores colombianos Escobar Martínez y Rojas (2016) señalan que los ciberdelincuentes aprovechan la omnipresencia de los dispositivos electrónicos y las aplicaciones web para perpetrar sus ataques. Desde Argentina, Salgado et al. (2019) amplían este panorama, al destacar la necesidad de una mayor conciencia y protección por parte de los usuarios.

La investigadora chilena Rosa Barroso Toledo (2011) aborda la problemática de la pornografía infantil en Internet y su relación con el avance de las nuevas tecnologías. La autora analiza cómo el surgimiento de los delitos informáticos ha facilitado la aparición, masificación, distribución y comercialización de este tipo de contenido.

En Ecuador, Santillán Molina *et al*. (2021) investigan cómo la evolución de las tecnologías de la información ha generado un aumento en los delitos cibernéticos que afectan los derechos fundamentales de las personas, especialmente desde el año 2000 con la proliferación de las redes sociales y el robo de identidad. Según los autores, en el mencionado país, la falta de legislación específica dificulta la

persecución de estos delitos informáticos, que incluyen cibercrimen, terrorismo, ataques, guerra y espionaje, siendo los cibercriminales expertos en acceder a información sensible desde lugares estratégicos para perpetrar sus acciones. La ausencia de sanciones y la falta de restricciones al acceso a dispositivos electrónicos en centros penitenciarios contribuyen a la reincidencia en delitos cibernéticos, lo que subraya la necesidad urgente de actualizar la legislación y fortalecer la capacidad de investigación y persecución de estos crímenes en el país.

Es relevante considerar los estudios del Centro Universitario de Ciencias Económico Administrativas (CUCEA) de la Universidad de Guadalajara, en particular la investigación realizada por Prieto Quezada *et al*. (2015), que examina la incidencia de maltrato presencial y ciberacoso entre estudiantes universitarios en México. Los resultados muestran que la violencia sigue presente en la educación superior, manifestándose a través de insultos, amenazas y el robo de contraseñas como formas comunes de acoso virtual. Asimismo, se destaca el papel de las redes sociales, especialmente Facebook, como plataformas que amplifican el maltrato originado en las aulas.

A pesar de la creciente conectividad, el estudio revela una disminución en la calidad de las interacciones, lo que favorece un entorno propicio para la violencia digital. Se concluye que la educación universitaria no garantiza necesariamente mejores relaciones interpersonales, pues la violencia no solo persiste, sino que en algunos casos se intensifica entre los estudiantes.

Considerando la narrativa de los jóvenes que han vivido violencia en las escuelas, Prieto Quezada *et al.* (2017) desarrollaron una investigación sobre la violencia cibernética en el ámbito universitario. Se presentan las formas invasivas y dañinas del acoso por medio de las Tecnologías de la Información y la Comunicación (TIC), debido a la inmediatez y el alcance masivo de la información. El análisis teórico y epistemológico del fenómeno del acoso en redes, presentado en el estudio, describe el origen, evolución y manifestaciones actuales, como el ciberbullying, la difusión de fotos y videos humillantes y el robo de contraseñas. Subraya la vulnerabilidad de los adolescentes y jóvenes, principales víctimas de estas prácticas tanto en México como en El Salvador, donde a pesar de sus diferencias, ambas naciones comparten preocupaciones sobre la violencia y el acoso en entornos físicos y virtuales.

La investigación ha enfatizado la necesidad de visibilizar el acoso en el entorno educativo y propone la implicación activa de la comunidad escolar como actor clave para abordar el problema. En ambos países, la preocupación por

el ciberacoso resalta la urgencia de desarrollar estrategias integrales de intervención. El estudio concluye que, aunque la tecnología ha abierto nuevas vías para la violencia, también ofrece oportunidades para combatirla, por lo que se hace un llamado a educadores, políticos y profesionales de la salud a adoptar un enfoque conjunto y holístico para prevenir y enfrentar el ciberacoso.

Conforme lo señalado previamente, la preocupación en torno a la problemática de la violencia en las unidades educativas es cada vez mayor. Por ello, sucedieron diversas investigaciones que, el Consejo Mexicano de Investigación Educativa (COMIE), presentó el Estado de Conocimiento sobre tales estudios, en el período 2002 al 2011, bajo la coordinación de Furlán Malamud y Spitzer Schwartz (2013), que ofrece un análisis profundo de la evolución de la investigación sobre violencia escolar en México.

La publicación comienza con una revisión internacional de los enfoques globales expuestos en las investigaciones sobre la violencia en las escuelas, en los que se destacan estudios clave sobre convivencia, disciplina y violencia en el entorno escolar. Se posiciona a la convivencia escolar como un campo emergente de investigación educativa, desarrollando análisis sobre distintos tipos de convivencia (inclusiva, democrática, pacífica) y su impacto en la calidad de vida escolar. En cuanto a la disciplina, se documenta el crecimiento sostenido en los estudios sobre disciplina e indisciplina, señalando cómo la violencia ha ganado relevancia en la investigación educativa.

Más adelante, la publicación presenta los hallazgos sobre casos de bullying y otras formas de violencia que han permitido visibilizar fenómenos como el uso de drogas, intentos suicidas y discriminación, destacando la relación entre el clima escolar y la recurrencia del maltrato. Se ha identificado la falta de mecanismos institucionales adecuados para enfrentar el problema, lo que permite que el bullying persista en los centros educativos. Complementariamente, se identifica y advierte sobre la presencia de casos emergentes de ciber-bullying, y la relación entre el consumo de drogas y la violencia escolar.

El impacto de esta publicación desembocó en la actualización del estado de conocimiento, correspondiente al período 2012-2021, bajo la coordinación de Furlán Malamud, Prieto Quezada y Ochoa Reyes. Este nuevo volumen profundiza el análisis de los enfoques teóricos y metodológicos sobre la convivencia escolar, la disciplina y las distintas formas de violencia en los entornos educativos. Presenta cómo en el período delimitado, las investigaciones sobre estos temas han crecido significativamente, y cómo la pandemia de COVID-19 ha

influido profundamente en la forma en que se entienden y abordan las relaciones en el entorno escolar.

Los hallazgos del estudio presentan a la convivencia escolar como un área de estudio en construcción, dentro de las investigaciones educativas, en lugar de ser una temática emergente. Las investigaciones cualitativas y cuantitativas analizadas exponen la incidencia de factores como la inclusión, la democracia y el clima escolar. Asimismo, se examinan los enfoques sobre disciplina, considerando un cambio hacia perspectivas más inclusivas y basadas en los derechos humanos, dejando atrás modelos punitivos. Las investigaciones revisadas resaltan la importancia de la participación de las comunidades escolares en la construcción de ambientes de paz.

En referencia a la violencia, se identifican hallazgos sobre el bullying, el ciberacoso y la narcoviolencia, mostrando un incremento en los estudios sobre estos temas, especialmente en niveles educativos superiores. De esta manera, se evidencia que estos casos se vinculan con problemáticas de la salud mental, el consumo de drogas y la discriminación de género.

Considerando ambos volúmenes (Estado del Conocimiento sobre Convivencia, Disciplina y Violencia en las Escuelas 2002-2011 y posterior de 2012-2021) se identifican diferencias en la consideración de los enfoques investigativos y las temáticas abordadas. Mientras que el primer libro se centra en establecer las bases conceptuales sobre violencia, convivencia y disciplina, con un enfoque inicial en la violencia escolar y el bullying como fenómenos emergentes, el informe más reciente integra las problemáticas como el ciber-bullying y la violencia institucional, de una manera integral. Por otro lado, el impacto de la pandemia de COVID-19 en las dinámicas escolares ha introducido un nuevo eje de análisis en el segundo libro, resaltando la forma en que la crisis sanitaria mundial ha amplificado las desigualdades y los desafíos en la convivencia y violencia en el entorno educativo. Los resultados presentados de ambas publicaciones manifiestan una finalidad de contribuir a mejorar la eficacia de las políticas educacionales que son implementadas en México y el mundo.

Considerando el contexto boliviano, Velasco Rojas (2022) presenta una investigación que demanda una mayor atención y acción por parte de las autoridades y la sociedad en su conjunto para hacer frente a la problemática de los delitos informáticos, como el acoso cibernético. La falta de una legislación específica sobre ciberdelitos y la ausencia de mecanismos ágiles y eficientes para la denuncia y sanción de los delitos informáticos son desafíos que deben

abordarse con urgencia. Velasco recomienda el desarrollo de estrategias integrales que garanticen la protección de los ciudadanos en el entorno digital y promuevan la colaboración entre instituciones nacionales e internacionales para enfrentar este problema de manera efectiva.

Finalmente, Medrano Salamanca (2023) aborda de manera exhaustiva todas las formas de ciberbullying o ciberacoso en el sistema educativo boliviano, considerando los diversos tipos de ciberacoso que han surgido con la evolución de la tecnología y el uso inadecuado de dispositivos. Se destaca la importancia de la supervisión por parte de padres, maestros y unidades educativas para garantizar la seguridad de los menores. Además, se propone un proyecto de ley que busca modificar el parágrafo I, Artículo 152 de la Ley 548 "Código Niño, Niña y Adolescente", estableciendo nuevas medidas de protección en el sistema educativo.

El análisis exhaustivo de diversos autores respecto al ciberdelito y sus implicaciones revela la urgente necesidad de adaptar la legislación y fortalecer los mecanismos de protección en entornos digitales. Las investigaciones subrayan la complejidad de combatir los delitos informáticos en un contexto globalizado y tecnológicamente avanzado. Destacan la importancia de promover la cooperación internacional y el desarrollo de estrategias integrales para prevenir y sancionar estos actos delictivos. Por otro lado, existen propuestas de modificación legislativa que demuestran el compromiso por garantizar la seguridad y protección de los ciudadanos. Por tanto, es imperativo que las autoridades y la sociedad en su conjunto asuman una postura proactiva y colaborativa para abordar esta problemática en Bolivia y a nivel mundial.

1.2. El acoso cibernético y los "ciberdelitos" en la legislación boliviana

La presente investigación aborda temáticas de gran relevancia, particularmente en lo que respecta a los aspectos legales del acoso cibernético, también conocido como ciber-bullying. Este fenómeno, considerado un delito en Bolivia, requiere un entendimiento profundo de las penalizaciones correspondientes antes de su estudio detallado.

Es esencial destacar que la Constitución Política de Estado de Bolivia (CPE), en su artículo 130, establece un mecanismo legal para la Acción de Proteger la Privacidad. Este mecanismo ofrece a las personas que han experimentado una vulneración de su privacidad en las redes la posibilidad de resguardar sus datos.

El Código Penal boliviano establece las penalizaciones para los delitos contra el honor, la dignidad de las personas, incluyendo el acoso cibernético. Este código establece las medidas para resarcir daños a las víctimas a través de una medida de la justicia restauradora, sanción pecuniaria o privación de libertad, dependiendo de la gravedad del caso.

Las disposiciones específicas relacionadas con los delitos informáticos y el acoso cibernético son: el artículo 281 que, aborda la difusión e incitación al racismo o la discriminación, imponiendo penas para aquellos que promuevan ideas discriminatorias. Además, se establecen sanciones para delitos contra la dignidad y el honor de las personas, como la difamación (Artículo 282), calumnia (Artículo 283), injuria (Artículo 287) y ofensas a la memoria de difuntos, entre otros. Estos artículos incluyen las publicaciones en redes y plataformas digitales, difundiendo información falsa.

La Ley 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación (TIC) establece sanciones económicas y penales para delitos informáticos. Quienes cometan delitos en el entorno digital enfrentan distintas medidas punitivas y deben indemnizar a las víctimas. La intrusión ilegal en dispositivos o redes informáticas resulta en una pena de dos a cuatro años de cárcel y una compensación económica. La captación ilícita de información digital conlleva una privación de libertad de uno a tres años, además de una indemnización. La destrucción o modificación dolosa de datos digitales se penaliza con entre uno y cinco años de prisión, junto con una reparación económica. El sabotaje digital es castigado con una pena de entre cinco y diez años de cárcel. Por último, el espionaje en sistemas digitales se condena con una pena de tres a seis años de prisión, más la obligación de indemnizar los daños causados.

Además de establecer sanciones para los delitos informáticos, la Ley 164 también establece medidas de protección para los ciudadanos. Estas incluyen el derecho a la privacidad y la protección de datos personales, el derecho a la seguridad de los sistemas informáticos, y el derecho a la información y la educación sobre los delitos informáticos.

La Ley 348 Integral para Garantizar a las Mujeres una Vida Libre de Violencia incorpora disposiciones significativas para proteger contra la violencia cibernética, especialmente en casos de feminicidio y diversas formas de violencia contra las mujeres. Esta legislación establece condiciones para la protección legal de las víctimas de violencia, aplicables también a situaciones en línea.

Por otro lado, la Ley 045 Contra el Racismo y Toda Forma de Discriminación busca prevenir y sancionar actos de racismo y discriminación, incluso aquellos

que ocurren en entornos digitales. Aunque esta ley aborda la discriminación y el racismo en línea, su aplicación requiere pruebas sólidas ante un tribunal de justicia, lo que representa un desafío adicional para las víctimas de conductas antisociales.

Es importante destacar que, si bien la normativa boliviana no diferencia específicamente los ciberdelitos de otras conductas antisociales en una ley exclusiva, estos pueden ser tratados dentro del marco penal existente; sin embargo, en el caso del acoso y otros delitos cibernéticos relacionados, las víctimas enfrentan dificultades para presentar pruebas ante las fiscalías y tribunales debido al anonimato, perfiles falsos y otros obstáculos que dificultan la obtención de evidencia. Estos desafíos agravan aún más la situación de las víctimas de tales delitos en línea.

1.3. El problema y los objetivos de la investigación

En el contexto de la temática "Intervenciones escolares ante las ciber conductas antisociales", se ha seleccionado como objeto de estudio: Los casos de acoso cibernético (ciberbullying) a estudiantes universitarios que son creadores de contenido y las medidas de prevención del implementadas por las universidades.

La delimitación geográfica se establece en los municipios de Cochabamba, con un período definido desde noviembre hasta diciembre de 2023. La población bajo estudio son los creadores de contenido en las plataformas de Facebook y TikTok que están cursando estudios de grado en las siguientes universidades ubicadas en la ciudad de Cochabamba: Universidad Mayor de San Simón-UMSS (1832), Universidad Católica Boliviana "San Pablo"-UCB (1966) y la Escuela Militar de Ingeniería "Mariscal Antonio José de Sucre"-EMI (1955).

La población objetivo son los creadores de contenido inscritos en universidades bolivianas con sede en Cochabamba, como la UMSS, la UCB y la EMI, sin embargo, no existe un censo específico de esta población. Conforme la gestión establecida y conforme fuentes oficiales de las universidades mencionadas, en la UMSS hubo 76.209 estudiantes inscritos, en la UCB 3.371, y en la EMI 2.031.

Los objetivos de esta investigación son:

- Establecer los delitos contra los universitarios que son creadores de contenido y los patrones recurrentes en el comportamiento de los perpetradores de delitos, según criterio de los estudiantes universitarios.

- Identificar los recursos informáticos y comunicativos disponibles en las universidades investigadas y las medidas de prevención contra el acoso cibernético (ciberbullying) implementadas por creadores de contenido universitarios.

2. MATERIALES Y MÉTODOS

El ciberacoso, que incluye el hostigamiento e intimidación en plataformas digitales, es un problema que afecta de manera significativa a aquellos con diferentes formas de pensar y aprender. Este fenómeno puede manifestarse de diversas maneras, como la difusión de contenido humillante o amenazante, la suplantación de identidad y el acoso verbal, extendiéndose a través de redes sociales, mensajes, juegos en línea y más, lo que representa un riesgo para la integridad de las víctimas (UNICEF, 2022).

Este delito puede implicar acciones específicas contra la privacidad, como la divulgación de datos y el ciberhostigamiento. La divulgación de datos implica la revelación de información privada obtenida de manera confidencial, mientras que el ciberhostigamiento busca humillar a la víctima mediante la difusión de contenido humillante a través de medios digitales (Marín-Cortés & Linne, 2021).

La suplantación de identidad también puede estar relacionada con el ciberacoso, manifestándose a través de ataques como el IP spoofing, el email spoofing, el facial spoofing y el robo de cuentas en redes sociales (Pandove *et al.*, 2010). Estos ataques buscan engañar a los usuarios para obtener acceso no autorizado o robar información personal (Zapata Molina, 2012).

Finalmente, otras formas de ciberacoso incluyen la sextorsión y el acoso íntimo, que abarcan prácticas como la pornovergüenza, el porno no consentido, la pornovenganza y el acoso persistente. Estas formas de ciberacoso tienen como objetivo humillar o dañar a la víctima mediante la difusión de contenido íntimo sin consentimiento o el acecho persistente a través de medios digitales (Acurio del Pino, 2014).

Por otro lado, es importante destacar que los patrones recurrentes de acoso cibernético se manifiestan a través de la repetición compulsiva de comportamientos, cambios disruptivos repentinos o progresivos, y efectos a largo plazo en la salud mental y el bienestar de las víctimas (IIDH, 2014).

Para combatir estas amenazas, se utilizan recursos informáticos de seguridad, que son herramientas y técnicas diseñadas para proteger sistemas y datos contra amenazas cibernéticas. Estos recursos incluyen antivirus, firewalls, sistemas

de detección de intrusos, cifrado de datos, autenticación de usuarios y copias de seguridad (Kizza, 2017).

Considerando lo anterior, los recursos comunicativos para la seguridad informática pueden ser elementos clave en la prevención y detección de ciberacoso y otros delitos informáticos, considerando las experiencias en seguridad informática para contrarrestar amenazas híbridas (Nussipova et al, 2023). Estos recursos pueden generar procesos de comunicación efectivos, educación sobre seguridad digital, campañas de concienciación y protocolos de actuación ante incidentes de seguridad.

Por lo expuesto, la presente investigación se enmarca en una investigación básica que adopta un enfoque metodológico mixto, centrado en los hechos fenoménicos, considerando las variables de investigación: Delitos, patrones recurrentes, recursos informáticos y recursos comunicativos.

El diseño metodológico propone la aplicación de técnicas de encuestas a 864 estudiantes de las mencionadas universidades, complementadas con entrevistas estructuradas a creadores de contenido: Por la UMSS, Camila Hidalgo y Sarah Sanabria; de la UCB, Alejandro Alcócer y de la EMI, Rodny Sehuenca.

El personal administrativo de universidades con responsabilidades en seguridad informática entrevistado fue el siguiente: En la UMSS, el Ing. Boris Alfaro, jefe del Departamento de Tecnologías de la Información y Comunicación (DTIC), desempeña estas funciones. En la EMI, el My. (Ing.) Camilo Ríos es el encargado de la Unidad de Sistemas y Tecnología (UST). Ambos, entrevistados, junto con el Mgr. Mario Antezana, responsable de la Unidad de Tecnologías de la Información de la Facultad de Humanidades y Ciencias de la Educación de la UMSS (UTI).

Finalmente, se incluyen los resultados de una entrevista estructurada a Tnl. Enrique Reynaga, jefe de la División Cibercrimen de la Fuerza Especial de Lucha Contra el Crimen de la ciudad de La Paz (FELCC).

3. RESULTADOS

El análisis de los resultados de la investigación es presentado, considerando los objetivos de la investigación.

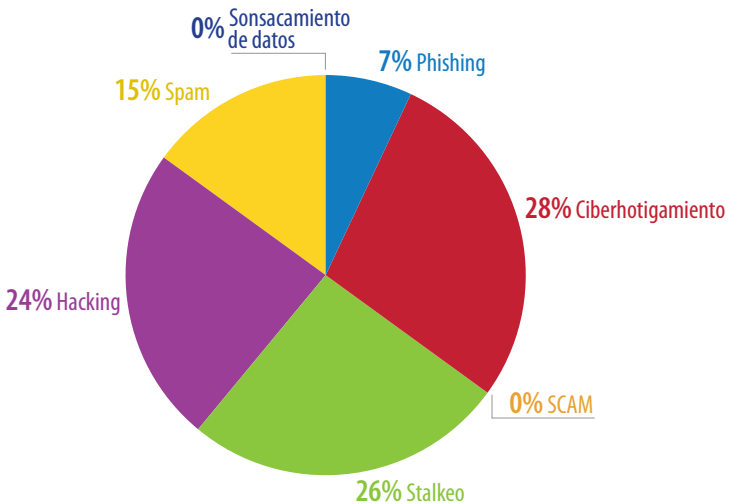
3.1. Delitos y patrones recurrentes en el comportamiento de los perpetradores

Con base en los testimonios de los estudiantes de las universidades "UMSS", "UCB" y la "EMI" consultados, se identificaron los delitos más frecuentes que se

cometen, tanto en cantidad como en porcentaje, siendo el ciberhostigamiento el más recordado (28%). Ellos expresan sus temores a ser víctimas de esta y otras formas de acoso, debido a las consecuencias que conllevan estos delitos.

Sarah Sanabria, una estudiante que ha sido víctima de cyber-bullying, señala haber sido "hostigada, intimidada, acechada, atacada, humillada y amenazada" por seguidores de figuras políticas debido a sus "críticas y sátiras hacia [los] ídolos electorales". En su caso, ella identifica a los "guerreros digitales" como sus agresores, en desmedro de su libertad de pensamiento y expresión. Los autodenominados "guerreros digitales" representan a un colectivo de personas afines al Movimiento al Socialismo (MAS), principal fuerza política en Bolivia, quienes han desarrolladas campañas coordinadas de desinformación para desacreditar a la oposición y posicionar la candidatura Luis Arce, actual presidente del país (Chequea Bolivia, 2024).

Gráfico 1. *Delitos identificados por los estudiantes*



Fuente: Elaboración propia.

Contrariamente a estos resultados, los delitos con mayor índice de denuncias son la estafa y la extorsión. Según el Tnl. Enrique Reynaga, jefe de la División Cibercrimen de FELCC, "los ciberdelincuentes hackean cuentas y crean falsos trabajos. Abusan económicamente de la población y los extorsionan con fo-

tografías y vídeos íntimos si no hacen lo que se les exige". Por tanto, la mayoría de los estudiantes conocen estos delitos por sus propias vivencias o las de sus amigos, así como por las denuncias informadas por la Policía Nacional. Este resultado es respaldado por los responsables de sistemas de las universidades.

El 54% de los universitarios encuestados señalaron que han sufrido el hackeo de sus cuentas de redes o correo electrónico, por lo menos, una vez. Ellos consideran que quienes cometen estos delitos son hackers, intrusos o atacantes, mientras los usuarios acceden a sus cuentas personales de e-mail y redes, a través de los sistemas de Internet públicos o propios de su universidad o de unidades universitarias (UMSS). Conforme el 65% de los encuestados, las razones para el suceso de este delito radican en un desconocimiento de los recursos de seguridad, por parte de las víctimas, además de la insuficiencia de los recursos de seguridad disponibles en Bolivia.

Rodny Sehuenca, un estudiante entrevistado, considera que, a medida que los universitarios desempeñan un papel cada vez más importante en la creación y difusión de contenido en línea, es imperativo implementar medidas de seguridad digital más sólidas y programas educativos que los equipen con las habilidades necesarias para proteger su información personal y salvaguardar la integridad de su trabajo creativo. "La seguridad pasa por la educación para proteger las cuentas", manifiesta. Esta referencia es corroborada por Sanabria, cuyo testimonio fue compartido previamente.

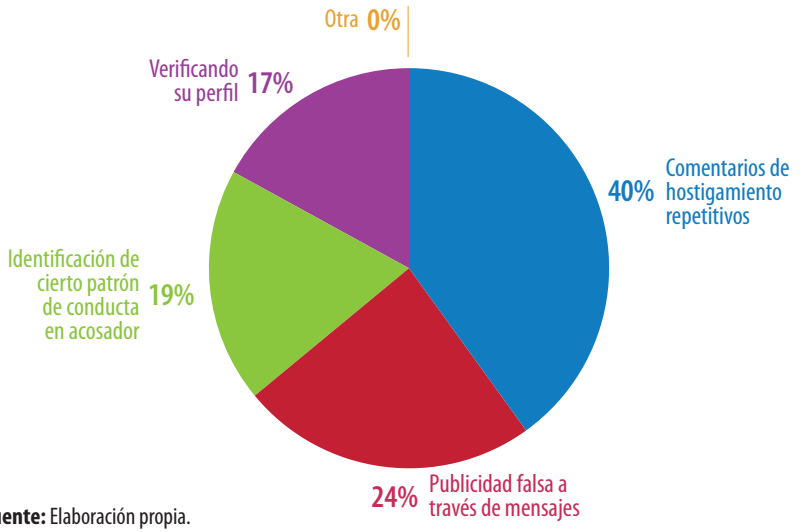
Conforme los entrevistados, "nadie está absuelto de sufrir un ciberataque, pero puede proteger su información para no ser parte de las numerosas víctimas". Según los resultados de las boletas de encuesta, las medidas para proteger sus cuentas son: "No compartir información personal abiertamente" (37%), "configurar el perfil de redes como privado" (35%) y el "uso de contraseñas complejas" (26%). Sobre medidas de seguridad, se analizarán datos más adelante.

Por otro lado, los patrones de los ciber-acosadores son actividades rutinarias realizadas por estos y la aparición de un suceso desencadenante como un objetivo disponible, pero todo esto está determinado por un esquema que se forma el infractor en su mente como resultados de actividades realizadas cotidianamente (Andresen, 2014). De acuerdo con los encuestados, el patrón más comúnmente identificado en los perpetradores de ciberdelitos es la emisión repetitiva de comentarios hostiles. Estos hallazgos ofrecen una perspectiva detallada sobre las percepciones de los participantes respecto a los patrones predominantes en los autores de delitos cibernéticos.

Según los estudiantes consultados, los comentarios de hostigamiento reiterados son el aspecto más destacado de tales; vinculados a sobre todo a temas político-electorales. Como fue señalado previamente por Sanabria, una de las entrevistadas, colectivos como los "guerreros digitales" y otros simpatizantes, no solo de los partidos políticos nacionales, sino de los frentes electorales de la UMSS.

Cabe aclarar que, conforme el artículo 92 de la Constitución Política del Estado Plurinacional de Bolivia, las universidades públicas son autónomas frente a la gestión de otras entidades públicas, por lo que tienen una libre administración de sus recursos y sistema de gobierno universitario. La gobernanza universitaria sucede a partir de un sistema de cogobierno docente estudiantil, donde las instancias del poder legislativo sostienen una representación paritaria entre docentes y estudiantes, accediendo a tales, por medio de elecciones anuales. Bajo esta premisa, es común que, en tiempos electorales, circulen por redes, panfletos y publicaciones que desacrediten a los candidatos o a sus seguidores.

Gráfico 2. *Patrones recurrentes identificados en los acosadores*



Fuente: Elaboración propia.

Los estudiantes consultados de la UMSS advierten que los comentarios de hostigamiento son frecuentes durante los períodos electorales universitarios. Los estudiantes consultados en la UCB y EMI, donde no existen el sistema de cogobierno, manifiestan que tales comentarios suceden en espacios deno-

minados "de confesionario", siendo comunidades cerradas en la red de Instagram®, sobre todo, donde los estudiantes emiten impresiones y referencias a sus docentes y otros compañeros. Cuando un comentario es compartido, "se vuelve viral" y sale de tales comunidades afectando a los implicados, conforme Alejandro Alcócer, un estudiante entrevistado.

Respecto a la identificación de los agresores, el encargado de la UST indica que, la EMI detecta ciberataques mediante el análisis de bitácoras, las cuales reflejan el comportamiento de los usuarios en sus plataformas. Dichas bitácoras facilitan la identificación de Protocolos de Internet (IPs) que intentan obtener acceso de manera reiterada mediante una avalancha de ataques para conseguir contraseñas, las cuales son posteriormente bloqueadas; sin embargo, no pueden identificar a los equipos de dónde emergen los comentarios de hostigamiento publicados en las redes. Al respecto, los entrevistados de la UMSS coinciden en que es "prácticamente imposible" identificar a los autores de los comentarios de hostigamiento en redes, dado que la mayoría de estos provienen de perfiles falsos.

3.2. Recursos informáticos y comunicativos

Conforme el encargado de la Unidad de Sistemas y Tecnología (UST), la EMI gestiona los recursos para los ciberataques, que incluyen al acoso, mediante el uso de diversas herramientas, incluyendo copias de seguridad. Estas copias se almacenan en discos adicionales y el uso de Redes Privadas Virtuales (VPNs) se ha intensificado, especialmente durante la pandemia de COVID-19. Actualmente, la universidad planea implementar una nueva aplicación para facilitar la comunicación entre el personal administrativo y docente, evitando así interferencias de otras aplicaciones.

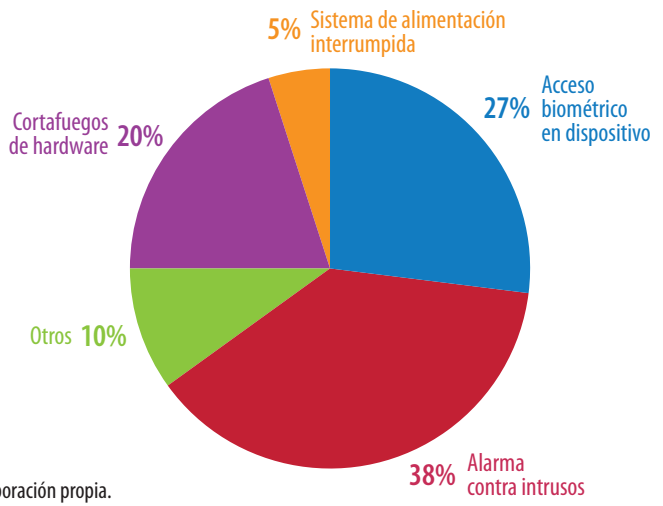
En la UMSS, el jefe del DTIC menciona que, para gestionar los delitos informáticos, incluyendo el "ciberacoso", mantienen copias de seguridad, preferentemente en ubicaciones seguras fuera del departamento mencionado. Además, utilizan herramientas como Snort®[1] o Suricata®2[2] para analizar el tráfico de red y prevenir amenazas. La institución tiene políticas de seguridad que cubren aspectos como la seguridad de los usuarios finales, accesos físicos y procedimientos de respaldo y seguridad. Al igual que la EMI, la UMSS utiliza VPNs y firewalls[3].

Sobre la prevención de otros delitos informáticos, como los ciberataques, se destaca el uso de firewalls y la actualización de software en la UMSS, conforme

el jefe de la DTIC. Los ataques más frecuentes en los sitios web de la UMSS son el *phishing*, el *malware* y los ataques de denegación de servicio (DDoS). El DTIC recibe de 1 a 2 reportes anuales, y sigue un protocolo específico en caso de robo de cuentas en redes sociales, que incluye cambiar contraseñas, activar la verificación en dos pasos y notificar a la institución afectada y a la policía nacional. El responsable de la UST menciona que la técnica de phishing es común, y que la EMI utiliza la prueba CAPTCHA[4] y correos electrónicos para contrarrestarla.

Al respecto, la mayoría de los estudiantes encuestados (62%) desconoce el uso de recursos informativos para la protección contra ciberdelitos, en particular, contra el acoso cibernético. En cuanto a la seguridad de hardware, software y red, la mayoría relativa de los encuestados (38%) utiliza como recurso preferido, las alarmas contra intrusos. Los estudiantes consultados señalan que, a pesar de conocer diversos recursos, no los utilizan porque los recursos más efectivos conllevan un pago por licencia de activación, siendo su costo, según los encuestados, relativamente caro. Otra dificultad para los estudiantes es el idioma de los recursos, desconociendo el inglés.

Gráfico 3. *Recursos informáticos contra los delitos conocidos por los universitarios*



Fuente: Elaboración propia.

Los recursos comunicativos, que incluyen diversas acciones y mecanismos tanto verbales como no verbales, son fundamentales para facilitar una interac-

ción efectiva. Estos recursos, que abarcan desde conductas intencionales hasta espontáneas, contribuyen al intercambio de información y al establecimiento de un ambiente emocional positivo. Sin embargo, se ha identificado que la mayoría de los estudiantes encuestados carece de información oportuna y adecuada sobre el uso correcto de estas herramientas para la comunicación.

En el contexto de la concientización sobre ciberdelitos, considerando la opinión de los responsables de seguridad informática de la UMSS y EMI, ambas universidades implementan acciones comunicativas para informar a los universitarios sobre los peligros de los delitos en Internet. A pesar de reconocer la preferencia de los estudiantes por las redes, estas instituciones señalan limitaciones debido a la cantidad de usuarios; sin embargo, consideran que redes como WhatsApp y Facebook son efectivas para la transmisión de esta información.

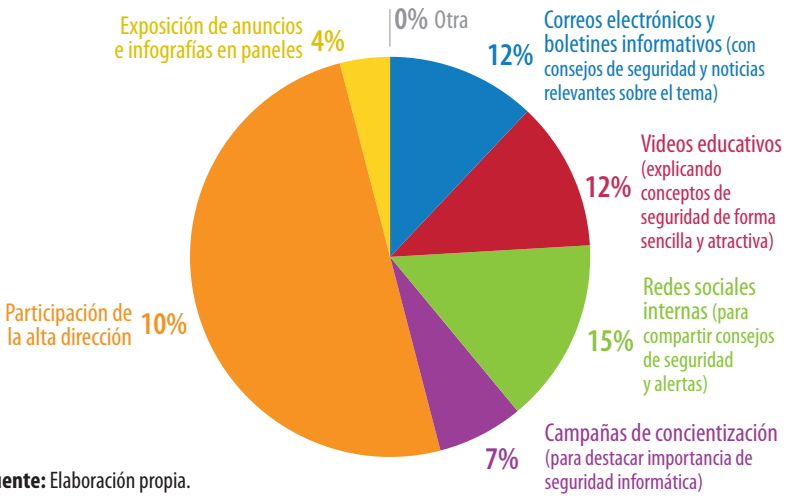
El responsable de la Unidad de Sistemas y Tecnología (UST) de la EMI destaca la importancia de utilizar aplicaciones probadas por el mercado para la seguridad informática, así como la necesidad de evitar el uso excesivo de plugins en el sistema operativo. Los estudiantes consultados señalan que instalan aplicaciones aceptando condiciones que no comprenden, reconociendo una actitud parsimoniosa al respecto, ya que el contenido aceptado no es analizado en su totalidad debido a su extensión. Este aspecto denota que, los recursos comunicativos empleados no son suficientes para los estudiantes.

Para el jefe del Departamento de Tecnologías de la Información y Comunicación (DTIC) de la UMSS, el análisis de patrones recurrentes es esencial para la detección de ciberataques. Por lo tanto, se realizan publicaciones y campañas informativas a docentes, personal administrativo y estudiantes sobre seguridad cibernética. Las infografías sobre medidas de seguridad tienen un mayor impacto en el público universitario, según el entrevistado. Además, se llevan a cabo talleres de seguridad informática como parte de la concientización sobre el manejo adecuado de las redes. Consultando a los estudiantes de esta universidad, arguyen que tales recursos son limitados porque no llegan a la totalidad de la población estudiantil, siendo de 76.190 universitarios (UMSS, 2023).

Según las encuestas realizadas, los estudiantes identifican que los recursos comunicativos más importantes para preservar la seguridad informática son los correos electrónicos y boletines informativos, seguidos por publicaciones en redes, videos educativos y, sobre todo, la participación de la alta dirección. La razón de tal preferencia radica en el criterio de que los mensajes enviados a

los correos electrónicos no solo informan, sino que educan, partiendo de contenido relevante. La participación de la alta dirección de la universidad en la difusión de estos mensajes y recursos comunicacionales refleja, para los estudiantes, un compromiso institucional con la seguridad informática.

Gráfico 4. *Recursos comunicativos para ciberseguridad preferidos por los estudiantes*



Fuente: Elaboración propia.

La preferencia señalada por los estudiantes a los mensajes en correos electrónicos ingresa en contradicción con la frecuencia de ingreso a los mismos. Según los responsables de seguridad informática de ambas universidades, el ingreso de los estudiantes a las casillas electrónicas es relativa y no frecuente, en comparación al acceso a las redes. Por lo cual, se debe emplear recursos complementarios en estas últimas.

3.3. Medidas para prevenir el acoso cibernético asumidas por los creadores de contenido en Cochabamba, Bolivia

Dentro del ámbito de su expresión creativa, los estudiantes universitarios entrevistados han optado por asumir roles como creadores de contenido, motivados por la recepción positiva de sus publicaciones, las cuales han sido ampliamente vistas, compartidas y comentadas. Esta experiencia los ha llevado a consolidarse en dicho rol. En sus relatos, los entrevistados afirman que aplican

diversas medidas para prevenir el ciberacoso y el ciberhostigamiento.

Los universitarios Sanabria y Sehuencia mencionan que, personalmente, utilizan medidas de seguridad como la instalación de aplicaciones de antivirus y contraseñas seguras. Además, ambos señalaron que colaboran con organizaciones para impartir talleres y charlas en escuelas, universidades y comunidades sobre el uso responsable de las Tecnologías de la Información y Comunicación (TIC), así como para prevenir el ciberacoso. Asimismo, llevan a cabo campañas en redes sociales para difundir información sobre las consecuencias de estas conductas y ofrecen consejos para prevenirlas y enfrentarlas. Sanabria destaca que dedica ciertas publicaciones a informar a sus seguidores sobre herramientas tecnológicas para su seguridad. Alcócer coincide con esta idea, por lo que se dedica a enseñar a las personas a limitar la visibilidad de sus publicaciones, a desactivar comentarios para evitar mensajes ofensivos y bloquear a usuarios que acosen o intimiden. De esta manera, todos los entrevistados manifiestan estar comprometidos con mantener un entorno digital seguro, eliminando comentarios ofensivos, discriminatorios o que inciten al odio, y reportando casos de ciberacoso y ciberhostigamiento a las plataformas digitales correspondientes.

Estas acciones, equiparables a estrategias de responsabilidad social empresarial, reflejan la preocupación de los creadores de contenido por la ciberseguridad, dado que los riesgos y peligros en la navegación y visitas de sitios pueden afectar a su audiencia. En el caso específico de Camila Hidalgo, mencionado anteriormente, es preciso enfrentar a los perpetradores de delitos en las redes y evitar que, otras personas, sean víctimas del acoso cibernético.

Por tanto, es esencial destacar que la prevención del acoso cibernético (ciberbullying) es una responsabilidad compartida. Los creadores de contenido, las plataformas digitales, las familias y las instituciones educativas deben colaborar para crear un entorno digital seguro e inclusivo para todos.

4. DISCUSIÓN Y CONCLUSIONES

La investigación realizada sobre el acoso cibernético y los delitos en línea entre los creadores de contenido universitarios en Bolivia revela una serie de hallazgos significativos que merecen atención y acción por parte de las instituciones educativas, las autoridades y la sociedad en general. Estos hallazgos no solo proporcionan una comprensión más profunda de la naturaleza y el al-

cance del problema, sino que también sugieren posibles vías para abordarlo de manera más efectiva.

Los resultados de la investigación, obtenidos a través de encuestas y entrevistas, revelan que los universitarios creadores de contenido son particularmente vulnerables a delitos como el hackeo de cuentas, la difusión no autorizada de contenido íntimo y el acoso reiterado en redes sociales. Se evidenció que creadores de contenido, aunque no se dedican exclusivamente a esta actividad, han experimentado diversas formas de acoso cibernético. La prevalencia de estas experiencias, que incluyen desde solicitudes de información personal hasta hackeo de cuentas y amenazas de publicación de contenido íntimo, resalta la urgencia de abordar este problema. Esta situación demanda no solo una actualización legislativa, sino también la implementación de políticas públicas que promuevan la prevención del acoso cibernético en todos los espacios, especialmente en el entorno académico.

La naturaleza cambiante del entorno digital y la relativa inexperiencia de determinados usuarios en materia de seguridad cibernética pueden dejar a los creadores de contenido vulnerables a diversas formas de acoso y delitos en línea. Esto destaca la necesidad de una mayor concienciación y educación sobre la protección de la privacidad y la seguridad en línea.

Asimismo, este artículo visibilizó los vacíos legales y tecnológicos que existen en Bolivia en torno a la protección de los usuarios en línea. La falta de mecanismos ágiles para la denuncia de ciberdelitos y la ausencia de una legislación que penalice de manera efectiva estas conductas ponen a las víctimas, en este caso, los estudiantes universitarios, en una situación de desprotección.

Los patrones de conducta de los criminales cibernéticos, recurriendo a cuentas anónimas, perfiles falsos, proporcionan información valiosa sobre las tácticas y motivaciones detrás de los ataques en línea. La comprensión de estos patrones puede ayudar a anticipar y prevenir futuros ataques, así como a identificar y enjuiciar a los perpetradores.

El uso de recursos informáticos como firewalls y VPNs por parte de las instituciones universitarias para combatir los ciberdelitos es una medida crucial; sin embargo, las limitaciones asociadas con el gran número de usuarios y la falta de conciencia sobre seguridad cibernética subrayan la necesidad de una mayor inversión en infraestructura y educación en este ámbito.

Los recursos comunicativos, como los mensajes y boletines digitales enviados a los correos electrónicos, deben complementarse con publicaciones en las re-

des y con campañas de concienciación institucional. La difusión de información sobre seguridad cibernética y la promoción de prácticas seguras en línea pueden contribuir significativamente a la protección de los usuarios. Así como la incorporación de la temática como transversal en los planes de estudios de programas y carreras universitarias.

La adopción de medidas de prevención por parte de los creadores de contenido, como el uso de antivirus y contraseñas seguras y su voluntad para impartir talleres, difundir información y ofrecer consejos prácticos demuestra que la lucha contra los delitos cibernéticos no solo es responsabilidad de las instituciones y las autoridades, sino también de los propios usuarios. Este compromiso individual refuerza la importancia de una participación consciente de todos los actores en la construcción de un entorno digital seguro.

A pesar de lo señalado, esta investigación revela la necesidad de una mayor conciencia y capacitación en seguridad cibernética entre los creadores de contenido y la población en general. Si bien, determinados entrevistados muestran un compromiso activo en la promoción de la seguridad en línea, la mayoría carece de una comprensión profunda de las medidas de protección necesarias para prevenir el acoso cibernético y otros delitos digitales. Esto resalta la importancia de programas educativos y campañas de sensibilización más amplias para abordar esta brecha de conocimiento y mejorar la protección en línea para todos los usuarios.

Se recomienda una mayor colaboración entre las universidades y los creadores de contenido para desarrollar e implementar campañas integrales de prevención del acoso cibernético y los delitos en línea. Estas pueden recibir el apoyo de organizaciones sociales, entidades públicas o empresas privadas para la formulación de estrategias de responsabilidad social empresarial y de concientización social, incluyendo la organización de talleres y campañas de sensibilización, así como la promoción de prácticas seguras en línea a través de plataformas digitales.

Dentro de la discusión planteada en esta publicación, es fundamental llevar a cabo una revisión exhaustiva y una actualización de la legislación boliviana para abordar de manera específica el problema del acoso cibernético. Esta revisión debe incluir la tipificación clara y precisa de este tipo de delito, así como el establecimiento de mecanismos de denuncia y sanción que sean ágiles y eficientes. Además, es esencial garantizar la protección de las víctimas, asegurando que cuenten con el respaldo necesario para enfrentar estas situaciones.

Además, se requiere una mayor agilidad por parte de las instituciones pertinentes, como la fiscalía general del Estado Plurinacional y las diversas instancias del Órgano Judicial, en la consideración de los casos de acoso cibernético. Esto implica la implementación de medidas que permitan identificar a los infractores, incluso en casos de cuentas falsas o anonimato en línea.

La prevención del acoso cibernético y los delitos en línea es una responsabilidad compartida que requiere un enfoque multidisciplinario y colaborativo. Con una combinación de medidas tecnológicas, educativas y legales, es posible crear un entorno digital más seguro e inclusivo para todos.

Por lo expuesto, la investigación realizada para este artículo puede contribuir a establecer una base fundamental para el diseño de políticas públicas que no solo prevengan el acoso cibernético en las universidades, sino que también garanticen la atención integral a las víctimas y promuevan la colaboración entre entidades educativas, tecnológicas y judiciales para su disminución. Por tanto, el enfoque, en su construcción, debe ser integral y multidisciplinario, combinando elementos tecnológicos, educativos y legales. La incorporación de las conclusiones y recomendaciones de esta investigación en la agenda política puede conducir a la formulación de políticas públicas que enfrenten de manera proactiva el acoso cibernético, protejan a las víctimas y promuevan un uso responsable y seguro de las tecnologías digitales.

REFERENCIAS

Abreu Valencia, F. A. (2022). La cooperación internacional en materia de cibercrimen y evidencia digital. *Saber y Justicia*, 1(21), 30-53.

Acurio del Pino, S. (2014). Delitos Informáticos: Generalidades. En *Delitos Informáticos 1* (pp. 1-17). Organización de los Estados Americanos. https://lc.cx/hyp3pb

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación. (2017). Encuesta Nacional de Opinion sobre Tecnologías de Información y Comunicación. https://lc.cx/sT6oV2

Alba, C. A. (2020). Acoso escolar, ciberacoso y las nuevas tecnologías de la información y la comunicación. *Revista Cubana de Medicina General Integral, 36(3),* 1-9. https://lc.cx/0oMV4M

Andresen, M. A. (2014). *Environmental Criminology: Evolution, Theory, and Practice*. Taylor & Francis.

Barroso Toledo, R. (2011). Los delitos en internet: Un enfoque desde la pornografía infantil en la red. *Revista F@ro*, 13, 101-114. https://bit.ly/3E0YVo9

Belisario Méndez, A. N. (2014). *Análisis de métodos de Ataques de Phishing*. Biblioteca Digital FCE. https://lc.cx/0yE0WY

Campos Freire, F., Rivera Rogel, D., & Rodríguez Hidalgo, C. (2014). La presencia e impacto de las universidades de los países andinos en las redes sociales digitales. *Revista Latina de Comunicación Social*, (69), 571–592. https://doi.org/10.4185/RLCS-2014-1025

Cano-Pita, G. E., & García-Mendoza, M. J. (2018, 5 de enero). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *Dominio de las Ciencias*, 4(1), 1-14. https://doi.org/10.23857/dc.v4i1.762

Cerezo Ramírez, F., & Rubio Hernández, F. J. (2017). Medidas relativas al acoso escolar y ciberacoso en la normativa autonómica española. Un estudio comparativo. *Revista Electrónica Interuniversitaria de Formación del Profesorado*, 20(1), 113-126. https://doi.org/10.6018/reifop/20.1.253391

Chequea Bolivia. (2020). *Guerreros del MAS tramaron estrategias coordinadas de desinformación para influir en los votantes*. Chequea Bolivia. https://lc.cx/nfSaxt

Chilano, M. B. (2022). *La problemática del grooming en la Argentina: análisis de las estrategias y tácticas de las ONGs*. Grado Cero, 1-16. https://lc.cx/ctDihR

Coppola, M. (2023, 14 de noviembre). Seguridad informática: qué es, tipos y características. HubSpot. https://lc.cx/61pRIJ

Echeverría Echeverría, R., Paredes Guerrero, L., Evia Alamilla, N. M., Carrillo Trujillo, C. D., Kantún Chim, M. D., Batún Cutz, J. L., & Quintal López, R. (2019, 12 de marzo). Caracterización del hostigamiento y acoso sexual, denuncia y atención recibida por estudiantes universitarios mexicanos. *Revista de Psicología*, 27(2), 1-18. https://doi.org/10.5354/0719-0581.2018.52307

Escobar Martínez, J. I., & Quinto Rojas, L. C. (2016). Vulnerabilidad en dispositivos móviles con sistema operativo Android. *Cuaderno Activa*, 7(1), 55–65. https://lc.cx/l0yl9F

Fernández Bermejo, D., & Martínez Atienza, G. (2020). *Ciberdelitos*. Experiencia. https://lc.cx/POApfo

Furlán Malamud, A., & Spitzer Schwartz, T. C. (Coords.). (2013). *Convivencia, disciplina y violencia en las escuelas 2002-2011*. ANUIES, Dirección de Medios Editoriales: Consejo Mexicano de Investigación Educativa.

Furlán Malamud, A. J., Prieto Quezada, M. T., & Ochoa Reyes, N. E. (Coords.). (2024). *Convivencia, disciplina y violencia en las escuelas, 2012-2021* (Vol. 6, Serie Estados del Conocimiento 2012-2021; Área Temática 15). Consejo Mexicano de Investigación Educativa A. C.

Guerrero Álvarez, D. E. (2020). *Analisis del Ciberdelincuente en el derecho penal ecuatoriano*. Artículo Científico de Magister en Derecho, mención Derecho Penal y Criminología. Universidad Uniandes. 1-24. https://lc.cx/pZyP2F

Ballesteros, M.C., & Hernández, J.A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, (47), 209-234. https://lc.cx/o0Y410

Herrera-López, M., Romera, E. M., & Ortega-Ruiz, R. (2023). Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico. *Revista Colombiana de Psicología*, 32(2), 1-22.

Instituto Interamericano de Derechos Humanos. (2014). *Prevención del acoso escolar: Bullying y ciberbullying*. IIDH.

Jiménez Rozas, J. (2022). Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y nuevas problemáticas. [Trabajo de fin de Grado. Grado en Criminología. Curso académico 2021-2022]. Universidad de Salamanca. https://lc.cx/8FiM84

Kizza, J. M. (2017). *Guide to Computer Network Security* (4th ed.). Springer Cham. https://doi.org/10.1007/978-3-319-55606-2

Manjarrés Bolaño, I. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*, 5(9), 71-82

Marin-Cortes, A., & Linne, J. (2021). Una tipología del ciberacoso en jóvenes. *Revista Mexicana de Sociología*, 83(2), 331-356. https://lc.cx/RGNBTm

Medrano Salamanca, S. A. (2023). El ciberbullying en el sistema educativo boliviano: medidas de protección contra niñas, niños y adolescentes en la Ley 548. [Trabajo final de Diplomado en Derecho Penal y Procesal Penal, Universidad Mayor de San Simón]. DDigital - UMSS.

Mercol, G. (2022). *Educar e informar: estrategias de comunicación para prevenir estafas digitales*. Cuadernos del CIPeCo, 1-29.

Meseguer, J. (2013). Los nuevos modi operandi de los ciberdelincuentes durante la crisis económica. *Revista de Derecho UNED*, (12), 495-523. https://doi.org/10.5944/rduned.12.2013.11704

Nussipova, A., Khussainova, G., Kabilova, R., Kabilova, R., Aliyarov, E., & Nuralina, B. (2023). Information security communications strategy as a prerequisite to counteracting hybrid warfare: world experience [Estrategia de comunicaciones de seguridad de la información como requisito previo para contrarrestar la guerra híbrida: experiencia mundial]. *Revista Latina de Comunicación Social*, 82, 1-18. https://doi.org/10.4185/rlcs-2024-2134

Organización para la Cooperación y Desarrollo Económico. (2018). *Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental*. OCDE. https://doi.org/10.1787/9789264310681-es

Pandove, K., Jindal, A., & Kumar, R. (2010). Email Spoofing. *International Journal of Computer Applications*, 5(1), 27-30. https://doi.org/10.5120/881-1252

Prieto Quezada, M. T., Carrillo Navarro, J. C., & Lucio López, L. (2015). Violencia virtual y acoso escolar entre estudiantes universitarios: el lado oscuro de las redes sociales. *Innovación educativa*, 15(68), 33-47. https://lc.cx/ZhgJj2

Prieto Quezada, M. T., Carrillo Navarro, J. C., & Oliva, H.A (2017). *No te enredes en las redes. Análisis y narrativas del ciberacoso en educación superior*. ICTI

Salgado, C., Peralta, M., & Berón, M. (2019). Modelos y métodos de calidad: fortalecimiento de la seguridad en los sistemas de software. [Documento de trabajo]. Universidad Nacional de San Luis.

Santillán Molina, A. L., Delgado Rodríguez, R. N., & Guerrero Álvarez, D. E. (2021). Análisis del ciberdelincuente en el derecho penal ecuatoriano. [Tesis de maestría, Universidad de los Andes, Ambato, Ecuador]. DSpace de Uniandes. https://lc.cx/l29FYB

Torres, Á. C. (2022). *Ciberdelitos en el sector turístico: tipologías más habituales, prevención y la respuesta penal ante los mismos*. 1-32. https://lc.cx/WGez90

Torrico Villanueva, E. (2016). *Comunicación: De las matrices a los enfoques* (2.ª ed.). (G. L. M., Ed.). Punto de Encuentro.

Fondo de las Naciones Unidas para la Infancia/United Nations International Children's Emergency Fund. (2022). Ciberacoso: Qué es y cómo detenerlo. UNICEF. https://lc.cx/EkCBKa

Velasco Rojas, A. C. (2022). Análisis y prevención de los ciberdelitos en Bolivia. [Trabajo final de Diplomado en Derecho Penal y Procesal Penal, Universidad Mayor de San Simón]. DDigital - UMSS.

Villasís-Keever, M. Á., & Miranda-Novales, M. G. (2016). El protocolo de investigación IV: las variables de estudio. *Revista Alergia México*, 63(3), 199-206. https://doi.org/10.29262/ram.v63i3.199

Zapata Molina, L. P. (2012). Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de virtualización de libre distribución. *Ingenius*, 8, 1-18. https://doi.org/10.17163/ings.n8.2012.01

Zapata Zurita, J. G. (2017). *Sapere Aude: La información libre de la censura y libre del mercado*. Beau Bassin: EAE.

Zbairi Pardillio, N. E. (2015). El stalking como nueva forma de acoso: las limitaciones de la regulación y la intervención actuales. (Trabajo de fin de grado, Universitat Autònoma de Barcelona). http://surl.li/bnslcd

NOTAS

[1] Snort® es un Sistema de Detección de Intrusos (IDS) de código abierto, diseñado para identificar actividades sospechosas en redes. Realiza un análisis exhaustivo del tráfico de red, proporcionando monitoreo en tiempo real y registro de paquetes. Puede analizar protocolos y detectar contenido malicioso. Una de sus características destacadas es la capacidad de identificar huellas digitales del sistema operativo y emitir alertas correspondientes.

[2] Suricata®, al igual que Snort®, es un sistema de detección de intrusiones (IDS) de código abierto que detecta actividades sospechosas en redes mediante el análisis de tráfico. Suricata se distingue por su eficiente motor de detección basado en reglas, amplia compatibilidad con protocolos de red y sólida integración con otras herramientas de seguridad.

[3] Firewall es un sistema que supervisa y controla el tráfico de red, basándose en reglas de seguridad predefinidas. Actúa como una barrera entre las redes internas confiables y las externas no confiables, como Internet.

[4] CAPTCHA, acrónimo de 'Completely Automated Public Turing test to tell Computers and Humans Apart' (Prueba de Turing pública y automática para diferenciar entre computadoras y humanos), es un sistema de desafío-respuesta implementado para discernir entre usuarios humanos y bots en Internet. Su diseño y aplicación son fundamentales para mitigar el riesgo de actividades automatizadas no deseadas y garantizar la interacción humana genuina en la web.