Capítulo 8

Los límites de la libertad individual y colectiva: prevención y garantías frente al ciberdelito

Octavio Quintero Avila
Universidad Autónoma de Nuevo León, México
oquinteroa@uanl.edu.mx
https://orcid.org/0000-0003-3922-9964

Juan Antonio Caballero Delgadillo
Universidad Autónoma de Nuevo León, México
juan.caballerodlg@uanl.edu.mx
https://orcid.org/0000-0001-9439-5696

Introducción

La consolidación del espacio digital como entorno privilegiado para la socialización, la expresión y el desarrollo personal, ha transformado radicalmente las nociones clásicas de libertad. Este ecosistema sociotécnico, caracterizado por la conectividad global y la desmaterialización de las relaciones sociales, ha generado nuevas tensiones entre los derechos individuales y las responsabilidades colectivas, especialmente ante el auge de fenómenos delictivos que encuentran en el ciberespacio un terreno fértil para su proliferación.

Desde el enfoque filosófico-jurídico, la libertad no puede entenderse únicamente como ausencia de coerción, sino como un equilibrio dinámico entre la autonomía personal y el interés colectivo por preservar la seguridad, la dignidad y la paz social (Koch, 2024). Esta redefinición es crucial en contextos digitales donde los límites de la libertad se difuminan entre el anonimato, la ubicuidad y la hiperconectividad.

En términos criminológicos, el ciberdelito representa un campo emergente de tensiones normativas. Wall (2007) lo definió como un conjunto de actividades ilícitas facilitadas por tecnologías digitales, cuya complejidad trasciende los marcos del derecho penal tradicional. Jaishankar (2017) amplió esta visión al incluir fenómenos como el ciberacoso, el hacking ético y los delitos sexuales virtuales, subrayando la necesidad de integrar dimensiones tecnosociales, espaciales y temporales en su análisis.

La criminología, por tanto, enfrenta el reto de trasladar sus teorías al ciberespacio, adecuando modelos clásicos a entornos deslocalizados, asincrónicos y altamente dinámicos. Teorías como la de las actividades rutinarias (Cohen y Felson, 1979) han sido reconfiguradas bajo esquemas como la Cyber-Routine Activity Theory (Vakhitova, 2025), la cual propone que los encuentros entre víctimas y agresores no requieren coincidencia física, sino condiciones de convergencia digital.

Asimismo, enfoques situacionales como la prevención del delito mediante el diseño ambiental (CPTED, en inglés) han sido proyectados al

entorno digital. Jeffery (1972) propuso que la oportunidad es una condición necesaria para la comisión del delito, influida por factores del entorno. En estudios recientes, estos principios han sido validados mediante simulaciones de vigilancia virtual y control de accesos digitales (Quintero Avila, 2025), reforzando la aplicabilidad del enfoque ambiental al ciberespacio.

En este contexto, la ciberseguridad se concibe como una responsabilidad compartida. Kikerpill (2021) introduce el concepto de "esferas internas de protección", señalando que los individuos informados y empoderados constituyen la primera línea de defensa contra los ciberdelitos. La libertad, entonces, no es incompatible con la seguridad, sino su condición ética y operativa cuando se ejerce con conciencia, información y garantías jurídicas.

Este análisis integral del ciberdelito exige, además, una perspectiva desde la paz. Garantizar la seguridad digital sin recurrir a modelos de vigilancia masiva o control coercitivo exige un enfoque preventivo que priorice la protección de los derechos humanos y fomente entornos digitales inclusivos, éticos y pacíficos (Yang y Fan, 2025; Akar, 2025).

Los estudiantes universitarios constituyen una población estratégica para este análisis. Su exposición intensiva al ciberespacio, combinada con una conciencia parcial sobre los riesgos y medidas de autoprotección, los convierte en blanco frecuente de ciberdelincuentes. De acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI, 2023), n = 18 400 000 personas usuarias de internet en México (20,9 %) reportaron haber sido víctimas de ciberacoso. Esta afectación fue más frecuente en mujeres. Las formas más comunes fueron contacto mediante identidades falsas ($n \approx$ 6 609 600; 35,9 %), mensajes ofensivos ($n \approx$ 6 127 200; 33,3 %) y envío de contenido sexual no solicitado ($n \approx$ 4 784 000; 26,0 %), siendo Facebook y WhatsApp las plataformas predominantes.

Particularmente preocupa resulta la situación de los adolescentes. De acuerdo con los datos del módulo sobre ciberacoso (MOCIBA) (INEGI, 2023): n = 3 300 000 jóvenes de 12 a 17 años (25,7 %) reportaron haber vivido alguna forma de ciberacoso entre julio de 2022 y agosto de 2023. Esta cifra incluye a $n \approx$ 1 958 000 mujeres (29,5 %) y $n \approx$ 1,342,000

hombres (22,2 %). Además, $n \approx 697\ 300$ adolescentes (5,5 %) recibieron insinuaciones sexuales no consentidas, con un mayor impacto en mujeres ($n \approx 477\ 380$; 8,9 %) que en hombres ($n \approx 123\ 030$; 2,3 %). Aproximadamente $n \approx 710\ 000$ adolescentes (5,6 %) fueron víctimas de envío de fotos o videos sexuales no solicitados, siendo el 8,5 % mujeres y el 2,8 % hombres. Finalmente, $n \approx 1\ 300\ 000$ adolescentes (9 9 %) recibieron mensajes ofensivos y $n \approx 930\ 000$ (7,1 %) fueron criticados por su apariencia o clase social, con una mayor prevalencia entre mujeres (10,1 %) que hombres (4,3 %).

Estas cifras revelan un patrón preocupante: la existencia entre la conciencia del riesgo y la adopción de medidas preventivas. Por ejemplo, en un estudio aplicado en Purdue, aunque el 72 % de estudiantes identificó amenazas como el *phishing* o el *malware*, solo el 25 % implementó prácticas básicas de seguridad (Hazarika, 2025). Investigaciones en Nigeria y Arabia Saudita reflejan patrones similares: los estudiantes poseen niveles medios de conciencia, pero bajos niveles de autoprotección digital (Eroğlu Yalın y Şahin Başfırıncı, 2018). En Ghana, se ha observado una correlación entre el uso intensivo del entorno digital y comportamientos adictivos en universitarios (Tachie-Menson et al., 2025). Además, Singh y Kumar (2023) reportaron una correlación negativa significativa ($r = -0{,}729$, $p < 0{,}01$) entre competencia digital y victimización cibernética, demostrando que una mayor alfabetización digital disminuye el riesgo de victimización.

En este marco, la presente investigacion tiene como finalidad analizar los límites entre la libertad individual y colectiva frente al ciberdelito, desde un enfoque interdisciplinario que articule lo jurídico, lo criminológico y lo educativo. A partir de una muestra de estudiantes universitarios, se exploran las percepciones de seguridad digital, con el propósito de formular estrategias que fortalezcan la protección de los derechos fundamentales sin comprometer la libertad digital. Particularmente, se busca comprender cómo influye la percepción de seguridad en la implementación de medidas individuales de autoprotección, así como el papel que desempeña la confianza institucional en la configuración de comportamientos responsables en línea.

Metodología

Se trata de un estudio descriptivo, transversal y cuantitativo, orientado a evaluar la percepción de riesgo digital frente al ciberdelito en estudiantes de una escuela nivel media superior privado del municipio de Monterrey, Nuevo León. La población objetivo fue $N = 4\,916$ alumnos matriculados. Se aplicó un muestreo no probabilístico por conveniencia, obteniéndose una muestra de $n = 378$.

La percepción de riesgo digital se midió con una escala de ocho ítems, desarrollada y validada por el Observatorio Universitario de Ciberdelitos. Tras alojar la encuesta en Microsoft Forms (tiempo promedio de respuesta 7 min 29 s, periodo de recolección 73 días) y exportar los datos en formato CSV, las respuestas se analizaron en Jamovi Desktop 2.6.44 (macOS).

Cada participante valoró en escala tipo Likert 1-5 ("1 = Muy poco" a "5 = Muchísimo") su nivel de preocupación ante los siguientes escenarios de ciberdelito:

1. Robo de criptomonedas
2. *Hackeo* de cuentas en redes sociales o correo electrónico
3. Fraude al vender bienes/servicios en línea
4. Uso de dispositivos falsificados (*hardware*/*software* malicioso)
5. Infección con virus o *malware*
6. Suplantación de identidad
7. *Hackeo* bancario
8. Fraude con tarjeta de crédito/débito
9. Fiabilidad interna

Se calculó el alfa de Cronbach para comprobar la homogeneidad interna de la escala. El coeficiente global resultó $\alpha = 0{,}994$, indicando excelente consistencia.

A continuación, se presentan las estadísticas por ítem, incluidas sus medias y las correlaciones ítem-total:

Tabla 1

Estadísticas de fiabilidad de cada ítem de la escala de percepción de riesgo digital

Ítems	Media	Correlación del elemento con otros	Alfa de Cronbach
Robo de criptomonedas	2,98	0,943	0,995
Hackeo de cuentas redes/email	3,66	0,959	0,993
Fraude al vender bienes/ servicios	3,51	0,984	0,992
Dispositivos falsificados	3,46	0,985	0,992
Infección con virus	3,55	0,979	0,992
Suplantación de identidad	3,49	0,983	0,992
Hackeo bancario	3,38	0,981	0,992
Fraude con tarjeta	3,36	0,978	0,992

Procedimiento y consideraciones éticas

Previo a la aplicación del cuestionario se obtuvo consentimiento informado, en el que se explicó a los participantes el propósito del estudio, la voluntariedad de su colaboración, la no recolección de nombres ni datos personales identificativos y la confidencialidad absoluta de sus respuestas. La encuesta se difundió y completó dentro de las instalaciones de la universidad, garantizando un entorno controlado y cómodo para los alumnos.

Criterios de inclusión. Estudiantes mayores de 18 años, matriculados en la escuela y que otorgaron su consentimiento.

Criterios de exclusión. Menor de 18 años o no estar matriculado en la institución durante el periodo de estudio. No haber otorgado el consentimiento informado (registro sin confirmación expresa). Respuestas duplicadas, detectadas por coincidencia de dirección de correo electrónico

Tamaño de la muestra

Para asegurar representatividad con un nivel de confianza del 95 % $(Z = 1{,}96)$ proporción esperada $p = 0{,}50$ y margen de error $e = 0$. se utilizó la fórmula para población finita:

$$n = \frac{N \cdot Z^2 \cdot p(1-p)}{e^2 \cdot (N-1) + Z^2 \cdot p(1-p)}$$

Procesamiento de datos

Los datos recolectados se exportaron desde Microsoft Forms en formato CSV y, antes de su análisis, se adaptaron manteniendo los ítems de Likert con códigos numéricos de 1 a 5 y recodificando las respuestas binarias a 0 (No) y 1 (Sí). A continuación, todas las variables se cargaron en Jamovi Desktop 2.6.44 (macOS), donde se evaluó la fiabilidad interna de la escala de percepción de riesgo mediante el cálculo del alfa de Cronbach $(\alpha = 0{,}994)$, se obtuvieron estadísticas descriptivas (media, desviación estándar e intervalo de confianza al 95 % para cada ítem) y se llevaron a cabo comparaciones de grupo: pruebas T de muestras independientes para la variable sexo y ANOVA. Adicionalmente, se planificaron análisis de correlación entre percepción de riesgo. Este proceso metodológico garantiza la validez interna del instrumento y la solidez de los resultados, permitiendo abordar de manera coherente los límites de la libertad digitales desde una perspectiva criminológico-metodológica.

Resultados

La tabla 2 muestra que los estudiantes perciben un riesgo moderado-alto ante la mayoría de las modalidades de ciberdelito, con medias que oscilan entre M = 2,98 (SD = 1,38; 95 % CI [2,84, 3,12]) para el robo de criptomonedas y M = 3,66 (SD = 1,19; 95 % CI [3,54, 3,78]) para el hackeo de cuentas en redes/email. En particular, la preocupación por la infección con

virus (M = 3,55, SD = 1,17; 95 % CI [3,43, 3,67]) y la suplantación de identidad (M = 3,49, SD = 1,23; 95 % CI [3,37, 3,62]) se sitúan también por encima del punto medio de la escala, lo que sugiere que los estudiantes internalizan estas amenazas como restricciones a su autonomía digital.

Este patrón de percepción refleja los límites de la libertad en entornos digitales: aunque los usuarios disfrutan de acceso constante y anonimato, reconocen la necesidad de contramedidas para preservar su seguridad y dignidad en espacios hiperconectados. El rango relativamente estrecho de los intervalos de confianza respalda la consistencia de estas valoraciones en la muestra, lo cual apoya la idea de que la percepción colectiva de riesgo actúa como un freno operativo sobre las prácticas de libertad digital.

Tabla 2

Estadísticos descriptivos de los ítems de percepción de riesgo digital

Ítems	N	Media	Inferior	Superior	DE
Fraude con tarjeta	378	3,36	3,24	3,49	1,24
Hackeo bancario	378	3,38	3,26	3,51	1,24
Suplantacion de identidad	378	3,49	3,37	3,62	1,23
Infeccion con virus	378	3,55	3,43	3,67	1,17
Disposotivos falsificados	378	3,46	3,34	3,58	1,19
Fraude al vender bienes/servicios	378	3,51	3,39	3,62	1,17
Hackeo de cuentas redes/*email*	378	3,66	3,54	3,78	1,19
Robo de criptomonedas	378	2,98	2,84	3,12	1,38

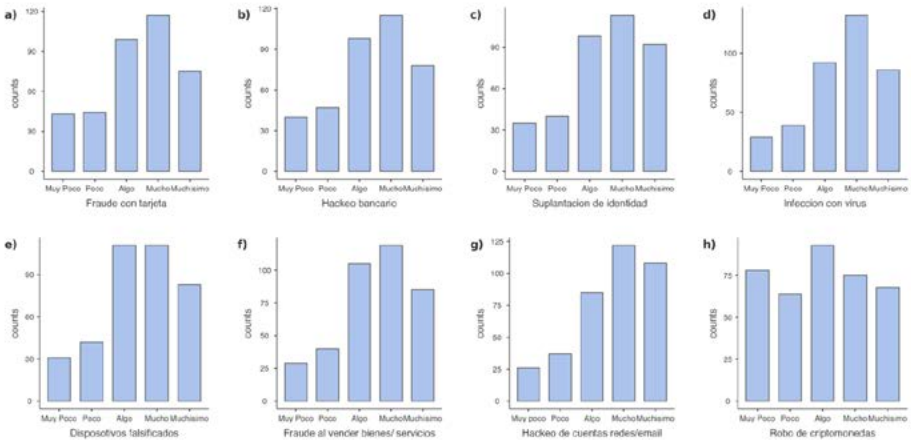
Nota. El CI de la media supone que las medias muestrales siguen una distribución T con N-1 grados de libertad. Intervalo de confianza al 95 %.

En la figura 1 se observa que, para la mayoría de los ítems, las categorías Algo (3) y Mucho (4) concentran la mayoría de las respuestas, lo que evidencia una percepción de riesgo moderado-alto entre los estudiantes.

Por ejemplo, los histogramas *b* y *g* muestran más de 100 respuestas en Mucho para hackeo bancario y hackeo de cuentas, respectivamente, mientras que *h* (robo de criptomonedas) presenta una distribución más desplazada hacia Algo y Poco. Este patrón respalda el argumento de que los estudiantes perciben como especialmente amenazantes las intrusiones sobre datos financieros y de acceso (tarjetas, cuentas) y en menor medida los incidentes de criptomonedas, lo cual delimita de manera diferenciada los límites de la libertad digital en función del tipo de ciberdelito.

Figura 1

Distribuciones de frecuencia de las respuestas a los ocho ítems de percepción de riesgo digital

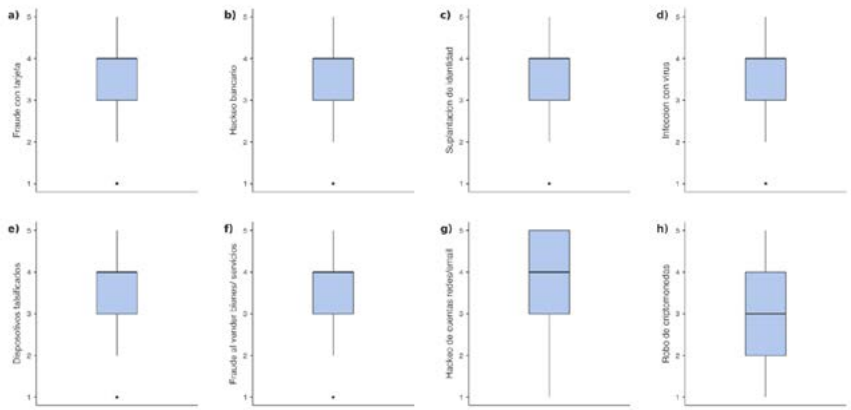


En la figura 2 se aprecia que, para todos los ítems, la mediana se sitúa entre Algo y Mucho (valores 3-4), confirmando una percepción global de riesgo moderado-alto; además, el rango intercuartílico de la mayoría de las cajas se extiende de 3 a 4 puntos, lo que indica una dispersión central reducida en la valoración de las diferentes amenazas. En cada diagrama aparece al menos un valor atípico hacia 1 (Muy poco), lo que sugiere que un pequeño porcentaje de estudiantes percibe un riesgo muy bajo. El ítem "Robo de criptomonedas" muestra una caja más alargada y bigotes más extensos, reflejando una mayor heterogeneidad en la preocupación por

este tipo de ciberdelito, mientras que en "*Hackeo* de cuentas" e "Infección con virus" la parte superior de la caja se acerca más a 5 y los bigotes se prolongan hacia valores altos, señalando que un número considerable de estudiantes asigna puntajes elevados a estas amenazas. En conjunto, estos patrones refuerzan la idea de que las vulneraciones sobre datos y accesos financieros actúan como límites efectivos a la autonomía digital de los alumnos, en tanto que los riesgos emergentes presentan percepciones más dispares, ilustrando cómo los "límites de la libertad" se configuran de manera diferencial según la naturaleza del ciberdelito.

Figura 2

Diagramas de caja de la percepción de riesgo digital para cada modalidad de ciberdelito



Se realizaron pruebas T de Student para muestras independientes con el fin de comparar la percepción de riesgo digital entre mujeres $(n = 221)$ y hombres $(n = 157)$. Dado que las pruebas de Levene indicaron heterogeneidad de varianzas en todos los casos $(p < 0{,}05)$, se emplearon los valores de t corregidos por desigualdad de varianzas. Como muestra la tabla 3, todas las diferencias fueron altamente significativas $(p < 0{,}001)$, con puntuaciones medias sistemáticamente superiores en el grupo masculino. Por ejemplo, en el ítem "Robo de criptomonedas" las mujeres registraron $M = 2{,}00$ $(\text{DE} = 0{,}85)$ frente a $M = 4{,}34$ $(DE = 0{,}64)$ en los hombres,

$t\ (376) = -29{,}3$, $p < 0{,}001$, $d = 3{,}06$; y en "art. de cuentas" las medias fueron 2,93 $(DE = 0{,}98)$ y 4,69 $(DE = 0{,}47)$, respectivamente, $t\ (376) = -20{,}8$, $p < 0{,}001$, $d = 2{,}17$. El efecto más reducido, aunque aún de gran magnitud, se observó en "Infección con virus" $(t = -20{,}1,\ d = 2{,}10)$, y el patrón se mantuvo para todos los escenarios evaluados.

Estos resultados revelan una brecha de género significativa en la percepción de las amenazas digitales: los varones perciben sistemáticamente mayores riesgos que las mujeres.

Tabla 3

Prueba T para muestras independientes

Ítems		Estadístico	gl	*p*		Tamaño del efecto
Robo de criptomonedas		−29,3[a]	376	<,001		−3,06
Hackeo de cuentas redes /*email*		−20,8[a]	376	<,001		−2,17
Fraude al vender bienes/ servicios		−21,7[a]	376	<,001		−2,26
Dispositivos falsificados	T de Student	−22,9[a]	376	<,001	D de Cohen	−2,39
Infección con virus		−20,1[a]	376	<,001		−2,10
Suplantación de identidad		−22,0[a]	376	<,001		−2,30
Hackeo bancario		−22,7[a]	376	<,001		−2,37
Fraude con tarjeta		−22,4[a]	376	<,001		−2,34

[a] La prueba de Levene significativa $(p < 0{,}05)$ sugiere que las varianzas no son iguales.

Nota. H_a μFemenino ≠ μMasculino.

Como pone de relieve la tabla 4, en todos los escenarios de ciberdelito los hombres $(n = 157)$ registran medias y medianas claramente superiores a las de las mujeres $(n = 221)$. Por ejemplo, en el ítem "Robo de criptomonedas" los varones alcanzan una media de $M = 4{,}34$ $(Mdn = 4{,}00; SD = 0{,}64; SE = 0{,}051)$, frente a $M = 2{,}00$ $(Mdn = 2{,}00; SD = 0{,}845; SE = 0{,}057)$ en el grupo femenino. De igual modo, "Hackeo de cuentas" muestra $M = 4{,}69$ $(Mdn = 5{,}00; SD = 0{,}465; SE = 0{,}037)$ en hombres, frente a $M = 2{,}93$ $(Mdn = 3{,}00; SD = 0{,}984; SE = 0{,}066)$ en mujeres. Esta brecha de aproximadamente dos a dos puntos y medio en la escala Likert se repite en todos los ítems, poniendo de manifiesto diferencias sistemáticas en la percepción del riesgo digital.

Tabla 4

Estadísticos descriptivos de la percepción de riesgo digital por sexo

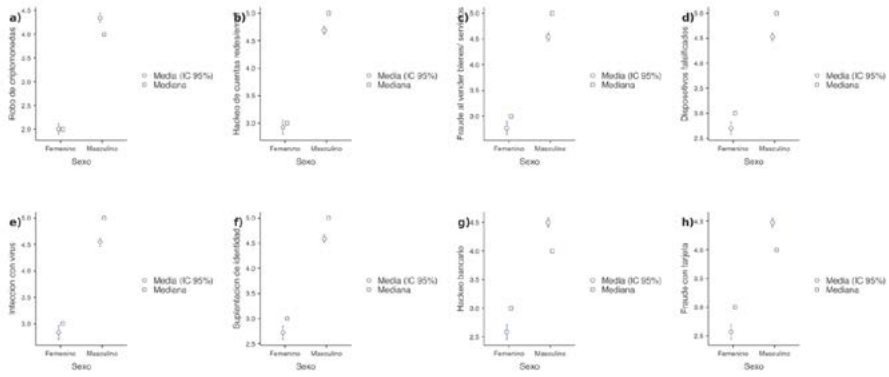
Ítems	Grupo	N	Media	Mediana	DE	EE
Robo de criptomonedas	Femenino	221	2,00	2,00	0,845	0,0568
	Masculino	157	4,34	4,00	0,638	0,0509
Hackeo de cuentas redes/email	Femenino	221	2,93	3,00	0,984	0,0662
	Masculino	157	4,69	5,00	0,465	0,0371
Fraude al vender bienes/servicios	Femenino	221	2,77	3,00	0,932	0,0627
	Masculino	157	4,54	5,00	0,500	0,0399
Dispositivos falsificados	Femenino	221	2,70	3,00	0,911	0,0613
	Masculino	157	4,53	5,00	0,501	0,0400
Infección con virus	Femenino	221	2,84	3,00	0,977	0,0657
	Masculino	157	4,55	5,00	0,499	0,0398

Ítems	Grupo	N	Media	Mediana	DE	EE
Suplantación de identidad	Femenino	221	2,72	3,00	0,978	0,0658
	Masculino	157	4,59	5,00	0,494	0,0394
Hackeo bancario	Femenino	221	2,59	3,00	0,967	0,0650
	Masculino	157	4,50	4,00	0,502	0,0400
Fraude con tarjeta	Femenino	221	2,57	3,00	0,977	0,0657
	Masculino	157	4,48	4,00	0,501	0,0400

La figura 3 grafica las medianas con sus intervalos de confianza al 95 % para cada grupo y confirma que el IC de la mediana masculina acota siempre entre $[4{,}0;\ 5{,}0]$, mientras que el femenino se sitúa en $[2{,}0;\ 3{,}0]$. La escasa superposición entre estos intervalos respalda la relevancia práctica de la brecha observada. En conjunto, tanto la tabla 4 como la figura 3 evidencian que los hombres internalizan un mayor grado de preocupación y, por ende, una mayor "autolimitación" de su libertad digital ante las amenazas cibernéticas. Estos resultados subrayan la importancia de incorporar la perspectiva de género en las estrategias de prevención y en los modelos teóricos de la Cyber Routine Activity al diseñar intervenciones de seguridad en el ciberespacio.

Figura 3

Medianas con sus intervalos de confianza



Discusión de resultados

Los resultados de este estudio se inscriben en una línea creciente de investigación que vincula la percepción de riesgo con la adopción y gestión de tecnologías emergentes en contextos universitarios. Por ejemplo, Oc et al. (2024) examinaron la adopción de herramientas de inteligencia artificial generativa por parte de 353 estudiantes en entornos de evaluación y hallaron que la percepción de riesgo actúa como un freno significativo en la intención de uso, mientras que la confianza y la pericia tecnológica facilitan la implementación de dichas innovaciones. Este hallazgo resuena con nuestros datos, donde las amenazas financieras y de acceso (hackeos, fraudes) fueron las que motivaron mayores puntajes de preocupación.

Asimismo, Morman y Brisco (2024) investigaron la percepción de riesgos en entornos de colaboración asistida por computadora con un grupo de 25 estudiantes de posgrado, encontrando que, incluso entre usuarios habituados a plataformas avanzadas, emergen brechas de percepción según experiencias previas y competencias digitales. Su descripción de distribución heterogénea de respuestas coincide con la variabilidad observada en nuestro ítem de "Robo de criptomonedas", donde la dispersión fue mayor y los valores atípicos más frecuentes.

Por último, Setyadi et al. (2025) demostraron mediante un modelo SEM-PLS con 385 estudiantes indonesios que la alfabetización digital y la gestión de riesgos influyen de manera moderada pero significativa en el rendimiento en entornos de aprendizaje modernos, remarcando el rol de la resiliencia estudiantil frente a amenazas cibernéticas

Este enfoque sistémico refuerza la idea de que nuestra escala de percepción de riesgo no solo mide un fenómeno acotado a la preocupación, sino que se conecta con competencias tecnológicas y estrategias preventivas de amplio alcance.

En conjunto, estas aportaciones recientes amplían nuestro marco teórico de "límites de la libertad", al mostrar que la percepción de riesgo digital integra dimensiones psicológicas, tecnológicas e institucionales.

La brecha de género (tabla 3 y figura 3), lejos de ser un hallazgo aislado, se enmarca en una realidad global donde la experiencia, la confianza y la formación determinan la manera en que estudiantes internalizan las restricciones a su autonomía digital. Este panorama subraya la urgencia de diseñar programas de prevención y alfabetización diferenciados, que consideren tanto las amenazas emergentes como las dinámicas particulares de cada grupo demográfico.

Conclusiones

La presente investigación tuvo por objetivo analizar los límites entre la libertad individual y colectiva frente al ciberdelito desde un enfoque interdisciplinario que integra lo jurídico, lo criminológico y lo educativo. Mediante la aplicación de una escala de ocho ítems en una muestra de 378 estudiantes universitarios, se constató que la percepción de riesgo digital se sitúa mayoritariamente en niveles moderado-alto (M entre 2,98 y 3,66), lo que pone de relieve un freno práctico a la autonomía en entornos hiperconectados. La excelente consistencia interna de la escala ($\alpha = 0{,}994$) y la estrechez de los intervalos de confianza respaldan la fiabilidad de estos indicadores. Adicionalmente, la brecha de género hallada, con puntuaciones masculinas sistemáticamente superiores a las femeninas en todas las modalidades de ciberdelito, evidencia que la valoración de las amenazas está modulada por factores sociodemográficos y experiencias previas.

Los resultados que mejor dan cuenta de cómo la percepción de riesgo actúa como límite a la libertad individual y colectiva son, en primer lugar, los estadísticos descriptivos de la tabla 2, que muestran medias moderado–alto para cada modalidad de ciberdelito, indicando que los estudiantes ya internalizan restricciones a su autonomía digital. En segundo lugar, la brecha de género revelada por la tabla 3 y los descriptivos de grupo (tabla 4 y figura 3), donde los hombres perciben riesgos significativamente mayores que las mujeres ($p < 0{,}001$, $d > 2{,}0$), ejemplifica cómo esos límites no son uniformes sino modulados por factores sociodemográficos. Finalmente,

los diagramas de caja de la figura 2 (medianas en 3-4 y bigotes estrechos) confirman la consistencia de esa autolimitación colectiva ante las amenazas digitales. En conjunto, estas evidencias corroboran que la percepción de riesgo constituye un freno operativo a la libertad de acción en el ciberespacio, cumpliendo así el objetivo central de la investigación.

Desde el punto de vista teórico, estos resultados validan la aplicación de la Cyber-Routine Activity Theory y del CPTED digital, al mostrar cómo la percepción de oportunidad delictiva y las condiciones ambientales guían las rutinas de seguridad de los usuarios. En términos prácticos, la identificación de los escenarios de mayor preocupación (fraudes financieros, accesos no autorizados y *malware*) proporciona una base empírica para priorizar acciones formativas en alfabetización digital, promoviendo competencias específicas en contramedidas tecnológicas (por ejemplo, autenticación multifactor y gestión de contraseñas) y estrategias de vigilancia situacional.

Como limitaciones, cabe mencionar el carácter transversal del estudio y el muestreo por conveniencia, lo que restringe la generalización de los resultados. Futuros trabajos podrían adoptar diseños longitudinales para evaluar la evolución de la percepción de riesgo a lo largo del tiempo y explorar, de manera experimental, la eficacia de intervenciones educativas basadas en simulaciones de ataque y formación en ciberseguridad. Asimismo, se recomienda ampliar el análisis a variables como la confianza institucional y las conductas concretas de autoprotección, con el fin de construir un modelo integrado de *libertad digital responsable* que oriente la formulación de políticas públicas y protocolos académicos en el ámbito de la seguridad y la criminología del ciberespacio.

Referencias bibliográficas

Akar, S. G. M. (2025). Students' disengagement in online courses: validity and reliability of an instrument. *Journal of Education and Learning*, *19*(1), 506-514. https://doi.org/10.11591/edulearn.v19i1.21733

Cohen, L. E., y Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589

Eroğlu Yalın, B., y Şahin Başfırıncı, Ç. (2018). Cybersecurity Perceptions of University Students in Turkey. *Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi*, *8*(2), 2-14. https://bit.ly/46qjS6O

Hazarika, H. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria*, *0*(0). https://doi.org/10.1177/09557490251340833

INEGI. (2023). *Módulo sobre ciberacoso (MOCIBA) 2023*. https://bit.ly/46qjUeW

Jaishankar, K. (2017). *Routledge Handbook of International Crime and Justice Studies*. Routledge.

Jeffery, C. (1972). Crime Prevention Through Environmental Design. *Criminology*, *10*(2), 191. https://doi.org/10.1111/j.1745-9125.1972.tb00553.x

Kikerpill, K. (2021). The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. *Kybernetes*, *50*(4), 1015-1026. https://doi.org/10.1108/K-06-2020-0335

Koch, H. (2024). Planning, Democracy and Collective Freedom. *Erasmus Journal for Philosophy and Economics*, *17*(2), 146-173. https://doi.org/10.23941/EJPE.V17I2.857

Lee, J. J., Go, M.-H., Kim, Y.-K., Joo, M., Seo, J., Oh, H., Kauh, J., y Lee, K. (2020). A Multi-Component Analysis of CPTED in the Cyberspace Domain. *Sensors*, *20*(14). https://doi.org/10.3390/s20143968

Miró Llinares, F. (2013). La victimización por cibercriminalidad social: un estudio a partir de la teoría de las actividades cotidianas en el

ciberespacio. *Revista Española de Investigación Criminológica*, *11*. https://doi.org/10.46381/reic.v11i0.77

Morman, B., y Brisco, R. (2024). Students' perception of risks in computer-supported collaborative design teams. *Proceedings of the Design Society*, *4*, 2925-2934. https://doi.org/10.1017/pds.2024.296

Oc, Yusuf, Gonsalves, Chahna, y Quamina, La Toya. (2024). Generative AI in Higher Education Assessments: Examining Risk and Tech-Savviness on Student's Adoption. *Journal of Marketing Education, 47*(2), 138-155. https://doi.org/10.1177/02734753241302459

Quintero Avila, O. (2025). Análisis espacial del delito: violencia de género en Monterrey, Nuevo León. En O. Quintero Avila y J. A. Caballero Delgadillo (eds.), *Perspectivas criminológicas*: *en la inteligencia criminal estratégica* (vol. 1, pp. 63-104). Tirant Humanidades.

Setyadi, A., Pawirosumarto, S., Damaris, A., y Dharma, R. (2025). Risk management, digital technology literacy, and modern learning environments in enhancing learning innovation performance: A framework for higher education. *Education and Information Technologies*, *30*, 15095-15123. https://doi.org/10.1007/s10639-025-13380-4

Singh, R., y Kumar, A. (2023). Examining the Relationship Between Digital Competence and Cybercrime Victimization Among University Students. *ĀmnĀyikĪ, 23*(2). https://bit.ly/47OywXJ

Tachie-Menson, A., Essel, H. B., Essuman, M. A., Nunoo, F. K. N., Appau, E., Akuteye, A. D., Boadi, E. A., y Quaye, N. T. (2025). Relationship Between Digital Nativity and Internet Addiction Among University Students in Ghana. *F1000Research*, *14*(139). https://doi.org/10.12688/f1000research.156283.1

Vakhitova, Z. I. (2025). *Cyber-Routine Activity Theory*. Oxford University Press.

Wall, D. S. (2007). *Cybercrime*: *The Transformation of Crime in the Information Age*. Polity Press.

Yang, Y.-F., y Fan, C.-C. (2025). Evaluating the effectiveness of Virtual Reality (VR) technology in safety management and educational training: an empirical study on the application and feasibility of digital training systems. *Interactive Learning Environments*, *33*(6), 3804-3832. https://doi.org/10.1080/10494820.2025.2454434