Profs. y Crims. Juan Rodríguez, Jesús Oduber, Karin Arbach, Laura Bastidas, Áurea Esther Grijalva, Solbey Morillo, Neelie Pérez, Marina Rezende. *Hacking* en adolescentes de América Latina: Aplicación empírica de la Teoría de la Acción Situacional. 91-138. Revista Cenipec. 37. 2025. Enero - Diciembre. ISSN: 0798-9202

Prof. Juan Antonio Rodríguez
Prof. Jesús Oduber
Prof.ª Karin Arbach
Crim. Laura Bastidas
Prof.ª Áurea Esther Grijalva
Prof.ª Solbey Morillo
Crim. Neelie Pérez
Prof.ª Marina Rezende

Hacking en adolescentes de América Latina: Aplicación empírica de la Teoría de la Acción Situacional

Recepción: 13/10/2025 **Aceptación:** 21/12/2025.

Prof. Juan Antonio Rodríguez
jarodrig@ula.ve
https://orcid.org/0000-0003-4111-1666
Prof. Jesús Oduber
jesusangeloduber@gmail.com
https://orcid.org/0009-0009-4547-852X
Universidad de los Andes
Mérida-Venezuela
Profa. Karin Arbach
k_arbach@hotmail.com
https://orcid.org/0000-0003-1753-46903
Universidad Nacional de Córdoba
Córdoba - Argentina
Crim. Laura Bastidas
laurambzf@gmail.com
https://orcid.org/0009-0004-9573-6412
Programa de Doctorado en Derecho
Universidad Católica Andrés Bello
Caracas - Venezuela
Profa. Áurea Esther Grijalva
aurea.grijalva@academicos.udg.mx
https://orcid.org/0000-0001-8399-4247
Centro Universitario de Ciencias Sociales y Humanidades
Universidad de Guadalajara
Guadalajara - México
Profa. Solbey Morillo
solbey.morillo@gmail.university
https://orcid.org/0000-0002-2129-1121
International Bridge University
Miami - Estados Unidos
Crim. Neelie Pérez
perezneelie@gmail.com
https://orcid.org/0000-0001-6372-037X
Programa de Doctorado en Ciencias Sociales
Universidad Central de Venezuela
Caracas - Venezuela
Profa. Marina Rezende
mbazon@ffclrp.usp.br
https://orcid.org/0000-0002-8037-8710
Universidad de São Paulo
São Paulo - Brasil

Hacking en adolescentes de América Latina: Aplicación empírica de la Teoría de la Acción Situacional

Resumen

Este estudio analiza la Teoría de la Acción Situacional como marco explicativo del *hacking* juvenil con datos del *ISRD-4* (n = 9.645) de cinco países latinoamericanos. Los análisis de regresión muestran que la propensión individual al *hacking* y la exposición a entornos digitales criminógenos aumentan de forma independiente este tipo de prácticas. Los análisis de interacción revelan que el efecto de la exposición criminógena sobre este ciberdelito se potencia con mayores niveles de propensión individual. Los resultados respaldan esta teoría, aunque señalan desafíos empíricos, teóricos y metodológicos en su aplicación al espacio virtual.

Palabras clave: *hacking*, teoría de la acción situacional, *ISRD-4*, adolescencia.

Hacking among Latin American adolescents: An empirical application of Situational Action Theory

Abstract

This study analyzes Situational Action Theory as an explanatory framework for young people's hacking with data from five Latin American countries (n = 9,645). Regression analyses show that individual propensity to hacking and the exposure to digital criminogenic environments independently increase this type of activity. Analyses of interactions show that the effect on this cybercrime of exposure to criminogenic environments is strengthened by higher levels of individual propensity. The results support the theory, at the same time highlighting empirical, theoretical and methodological challenges to applying it to virtual space.

Key words: hacking, Situational Action Theory, ISRD-4, adolescence.

Le hacking chez les adolescents d'Amérique latine: Application empirique de la théorie de l'action situationnelle

Résumé

Cette étude examine la théorie de l'action situationnelle comme cadre explicatif du hacking juvénile à partir des données de l'ISRD-4 (n = 9 645) recueillies dans cinq pays d'Amérique latine. Les analyses de régression indiquent que la propension individuelle au hacking et l'exposition à des environnements numériques criminogènes accroissent indépendamment la probabilité de s'engager dans ce type de pratiques. Les analyses d'interaction montrent en outre que l'effet de l'exposition criminogène sur cette forme de cyberdélinquance se renforce à mesure que le niveau de propension individuelle augmente. Les résultats apportent un soutien empirique à la théorie, tout en mettant en évidence des défis empiriques, théoriques et méthodologiques liés à son application aux espaces virtuels.

Mots clés: *hacking*, théorie de l'action situationnelle, ISRD-4, adolescence.

Hacking em adolescentes latino-americanos: Uma aplicação empírica da Teoria da Ação Situacional

Resumo

Este estudo analisa a Teoria da Ação Situacional como um arcabouço explicativo para o *hacking* juvenil, utilizando dados do *ISRD-4* (n = 9.645) de cinco países da América Latina. Análises de regressão mostram que a propensão individual ao *hacking* e a exposição a ambientes digitais criminogênicos aumentam, de forma independente, esse tipo de atividade. Análises de interação revelam que o efeito da exposição criminogênica sobre esse cibercrime é amplificado por níveis mais elevados de propensão individual. Os resultados corroboram essa teoria, embora destaquem desafios empíricos, teóricos e metodológicos em sua aplicação ao espaço virtual.

Palavras chave: *hacking*, Teoria da Ação Situacional, *ISRD-4*, adolescência.

1.- Introducción[1]

El rápido crecimiento que han experimentado las Tecnologías de la Información y la Comunicación (TIC) en las últimas décadas ha incidido en múltiples dominios de la vida social. Esto ha cambiado de forma notable no solo las dinámicas interpersonales y laborales, sino también la manera en que se origina y manifiesta un número importante de conductas delictivas y antinormativas tanto en el mundo físico como en el virtual (Aiken *et al*., 2024; Alves y Miró, 2024). Un buen ejemplo de estos cambios es el fenómeno del *hacking* que, en casos específicos, como se precisará a continuación, puede constituir un delito de intrusión informática, el cual ha generado gran interés en el campo de las ciencias sociales y de algunas disciplinas tecnológicas (Back *et al*., 2018; Bossler y Burruss, 2011; Chng *et al*., 2022; Grabosky, 2016; Holt, 2023; Wall, 2001).

En términos generales, el *hacking* puede entenderse como una acción intencional orientada a acceder, utilizar o alterar sistemas, redes, programas o dispositivos informáticos ajenos (Aiken *et al*., 2024; Bossler y Burruss, 2011; Chng *et al*., 2022; Fox y Holt, 2021; Kim *et al*., 2024). En determinadas circunstancias, como ocurre con el *hacking* de 'sombrero blanco' o ético y en ciertas formas exploratorias, esta práctica puede ser una herramienta de uso autorizado, legal y muy útil para mejorar la ciberseguridad (Gopalsamy y Dastageer, 2025; Noordegraaf y Weulen, 2023). Sin embargo, muchas veces se usa indebidamente con propósitos maliciosos o dañinos y sin ningún tipo de consentimiento o autorización previa (p. ej., *hacking* de 'sombrero negro', *cracking*, etc.), convirtiéndola en una forma de conducta infractora que, según el país, puede tener carácter ilícito, constituyendo un hecho punible[2] (Bossler y Burruss, 2011; Grabosky, 2016; Lee y Holt, 2020; Maras *et al*., 2024; Yar, 2005). En

[1] Este artículo forma parte del Proyecto de Investigación «El estudio de la delincuencia juvenil autoinformada: aplicación de la encuesta *ISRD*-4 a adolescentes venezolanos», bajo el código D-495-23-09-B, financiado por el Consejo de Desarrollo Científico, Humanístico, Tecnológico y de las Artes (CDCHTA) de la Universidad de Los Andes. Mérida-Venezuela.

[2] Esta práctica forma parte de lo que McGuire y Dowling (2013) llaman delitos 'ciberdependientes' (*cyber-dependent crimes*), es decir, aquellos que solo pueden cometerse a través de sistemas informáticos, los cuales funcionan como herramientas e igualmente como objetivo del delito.

este sentido, los 'hackers' o 'piratas informáticos' forman una población o grupo muy heterogéneo con éticas, motivaciones, métodos y capacidades técnicas muy diversas que incluyen, entre otros, a aficionados sin formación tecnológica formal, asesores en ciberseguridad, 'hacktivistas', individuos con una alta competencia digital vinculados a redes delictivas organizadas o, incluso, adolescentes animados por la curiosidad o la búsqueda de reconocimiento[3] (Back *et al*., 2018; Bossler y Burruss, 2011; Chng *et al*., 2022; Lee y Holt, 2020; Romagna y Leukfeldt, 2023; Yar, 2005).

Precisamente un fenómeno que ha generado interés dentro de la denominada 'cibercriminología' (Jaishankar, 2010) es el del *hacking* juvenil (Aiken *et al*., 2024; Fox y Holt, 2021; Holt *et al*., 2021; Kim *et al*., 2024; Lee y Holt, 2020). Aunque la evidencia empírica relacionada sigue siendo parcial y, de algún modo, limitada (Savka, 2025), los estudios realizados hasta el momento presentan un panorama preocupante sobre la continua participación de los adolescentes en el delito de intrusión informática o de acceso indebido a sistemas (Fox y Holt, 2021). En la realidad norteamericana, por ejemplo, los resultados obtenidos por Marcum *et al*. (2014) en ciertas zonas de Estados Unidos demuestran que un 13% de los adolescentes reveló haber accedido sin autorización a cuentas de Facebook y un 12% a sitios web restringidos. En el contexto europeo, se estima que cerca del 17% de los adolescentes entre 16 y 19 años ha participado en alguna forma de *hacking* con fines maliciosos (Aiken *et al*., 2024), una cifra que es coherente con los hallazgos obtenidos por la *National Crime Agency* (2024) en relación con menores británicos de 10 a 16 años. Estos datos nos permiten pensar que este fenómeno no responde a especificidades temporales, culturales y geográficas concretas, y que, en cambio, se trata de una forma persistente de comportamiento juvenil a nivel global.

En el ámbito latinoamericano, el panorama presenta una mayor complejidad. La región ha sido señalada no solo como receptor constante

[3] Véase Chng *et al*. (2022) para una descripción más precisa de las principales tipologías y categorías de 'hackers' (p. ej., principiantes, profesionales, 'hacktivistas', ladrones de bajo perfil, facilitadores del delito, etc.), tanto en función de sus intenciones y motivaciones (p. ej., curiosidad, notoriedad, venganza, ideología, etc.) como de sus habilidades técnicas (p. ej., habilidades bajas, medias y altas).

de ataques cibernéticos[4] (Flor-Unda *et al*., 2023; Vergara, 2024), sino también como un lugar donde se originan amenazas digitales, en el que coinciden dinámicas de ciberespionaje, activismo digital y delincuencia organizada (Kshetri, 2013; Solar, 2023). Esta realidad se presenta dentro de un proceso de digitalización progresivo en América Latina; aunque, cabe agregar, que asimétrico y desigual, caracterizado por brechas respecto a regiones con mejores infraestructuras digitales (p. ej., América del Norte o Europa) y entre los propios países de América Latina y al interior de cada uno de ellos (PNUD, 2024). En este escenario, el estudio concreto del *hacking* juvenil, ya sea de naturaleza ilícita o no, sigue siendo muy limitado (véase, por ejemplo, Lee y Holt, 2020; Udris, 2016; Vepsäläinen *et al*., 2025). Aún son insuficientes las investigaciones empíricas que profundicen en su ocurrencia, aspectos etiológicos y consecuencias sociales o legales. En tal sentido, resulta necesario desarrollar investigaciones criminológicas que estudien sistemáticamente los factores y mecanismos causales subyacentes al acceso indebido a dispositivos o programas informáticos practicado por adolescentes dentro de América Latina. Esta necesidad no se debe solo a una deficiente base teórico-empírica, sino también a la urgencia de entender con mayor precisión y rigurosidad la complejidad del fenómeno para aportar evidencia que contribuya al diseño de estrategias de prevención y control más eficaces (Fox y Holt, 2021; Lee y Holt, 2020; Onwuadiamu, 2025; Savka, 2025; Schiks *et al*., 2024).

El interés del presente estudio es analizar la conducta de *hacking* en una muestra de jóvenes provenientes de cinco países latinoamericanos (Argentina, Brasil, Colombia, México y Venezuela) participantes en la última edición del 'Estudio Internacional de la Delincuencia Autoinformada' (*ISRD-4*, por sus siglas en inglés). Para este análisis se adopta la Teoría de la Acción Situacional

[4] En el año 2020, por ejemplo, se llegó a registrar cerca de 750.000 incidentes diarios de *malware* en países como Brasil, México y Colombia (Flor-Unda *et al*., 2023). Como dato adicional, según Vergara (2024) América Latina y el Caribe constituye la región con el mayor crecimiento de incidencias o eventos cibernéticos dados a conocer públicamente (ciberdelito visible) a través de fuentes abiertas (p ej., medos de comunicación, plataformas digitales, prensa especializada, etc.) a nivel mundial. Entre 2014 y 2023, la tasa promedio de crecimiento anual alcanzó el 25%, superior a la media mundial que registró 21%. Este patrón se asocia a una alta exposición digital, déficits de protección en ciberseguridad y una rápida digitalización -aún no completamente desarrollada (PNUD, 2024)-, que en conjunto aumentan los niveles de vulnerabilidad y riesgo cibernético en la región.

(en adelante, TAS) propuesta por Wikström y su equipo (Wikström, 2004; Wikström, 2010; Wikström *et al*., 2012; Wikström *et al*., 2024), porque ofrece una perspectiva analítica integral para la interpretación del comportamiento transgresor, entendido como el resultado de la combinación de factores personales y ambientales que interactúan en situaciones concretas de acción. En sí, esta investigación propone una prueba empírica de esta teoría al estudio de prácticas de *hacking* en población juvenil, pretendiendo con los siguientes objetivos: (i) contrastar su capacidad explicativa frente a ciberdelitos[5] y a realidades culturales diferentes a las habitualmente exploradas, y (ii) aportar al desarrollo de una criminología cibernética y situacional en el contexto latinoamericano.

1.1.- La TAS: principios básicos y explicación del *hacking* en entornos digitales

La TAS es un modelo que describe, explica y predice el comportamiento delictivo o transgresor desde un enfoque multidimensional (Wikström *et al*., 2012). Una de sus ventajas está en la capacidad de articular, en una misma estructura teórica, factores de tipo individual y ambiental. Esto permite una comprensión más integral y sistémica de los procesos que pueden llevar a una persona a transgredir normas sociales o legales interpretadas, en el marco de esta teoría, como manifestaciones de moralidad (Wikström, 2004; Wikström, 2010). En términos generales, esta teoría afirma que la conducta delictiva, o cualquier otra forma de transgresión de normas morales, se origina por el efecto conjunto de: (i) la *propensión individual al delito* (entendida como la disposición a ver y escoger la conducta infractora como una opción posible según los niveles de moralidad personal y la capacidad de ejercer el autocontrol)[6] y (ii) la

[5] Fox y Holt (2021) definen el 'ciberdelito' como 'el uso indebido de la tecnología con fines delictivos' (p. 944).

[6] La *moralidad individual* hace referencia al conjunto de creencias, normas y emociones (como la culpa o la vergüenza) que funcionan como un factor mediante el cual la persona evalúa moralmente las posibles opciones de conducta disponibles en una situación concreta. Y, por su parte, la noción de *autocontrol* se centra en la capacidad de la persona para resistirse a ciertos estímulos situacionales (tentaciones y provocaciones), manteniendo la coherencia entre sus acciones y su moralidad interna. En la TAS, el autocontrol se concibe tanto como un rasgo relativamente estable como la capacidad situacional de gestión moral frente a determinadas condiciones del entorno (Wikström, 2010; Wikström *et al*., 2012).

exposición a entornos criminógenos (definidos como aquellos ambientes donde la motivación situacional, es decir, tentaciones o provocaciones, sus normas morales y los mecanismos de disuasión actúan sobre la percepción y elección de las posibles conductas)[7] (Wikström *et al*., 2012; Wikström *et al*., 2024).

El postulado central de la TAS sostiene que la acción delictiva resulta -aunque no necesariamente se determina- cuando coinciden, en una situación específica, la propensión individual al delito y una exposición significativa a un entorno criminógeno (lo que la teoría denomina hipótesis PEA [Propensión x Exposición → Acción]) (Wikström *et al*., 2012; Wikström *et al*., 2018). Es esta interacción la que desencadena el *proceso de percepción-elección* o *proceso situacional* (→), definido como una secuencia en la que la persona, a raíz de una determinada motivación, reconoce y contempla las posibles opciones de actuación disponibles, las evalúa a través del filtro moral y, a continuación, toma una decisión (delictiva o no) que puede estar determinada por controles internos y externos (Wikström, 2010; Wikström *et al*., 2012; Wikström *et al*., 2018). Este proceso bietápico, considerado el núcleo explicativo de la TAS, se basa entonces en la idea de que ni los factores personales ni los contextuales operan de forma aislada. La conducta infractora (según la hipótesis PEA inherente al *modelo situacional*) no ocurre solo porque existan oportunidades criminógenas en el ambiente, ni porque el individuo presente cierta predisposición, sino porque, en la concurrencia de ambos elementos, se configura la percepción de que delinquir o transgredir las normas constituye una opción posible, elegible y, en determinados casos, ejecutable.

Si bien la formulación original de la TAS se ha centrado por lo general en formas tradicionales de delincuencia *offline* (véase Hardie y Rose, 2025;

[7] La *motivación* en forma de tentaciones surge cuando una oportunidad es compatible con los deseos, propósitos o intereses personales y en forma de provocación cuando interferencias externas generan conflicto, frustración o malestar individual. El *componente normativo del contexto* (*contexto moral*) representa el grado en que los valores y normas morales junto a ciertas expectativas de comportamiento son visibles y compartidas en dicho entorno. En el caso de la *disuasión*, esta se entiende como la percepción subjetiva del riesgo asociado a las consecuencias negativas, ya sean formales o informales, derivadas del quebrantamiento de las normas relativas al contexto (Wikström, 2010; Wikström *et al.*, 2012).

Pauwels *et al*., 2018), algunos desarrollos posteriores han sugerido la posibilidad de extender su aplicabilidad a dinámicas propias del ciberespacio (p. ej., Choi y Yun, 2019; Hu *et al*., 2024; Hwang *et al*., 2021; Kabiri *et al*., 2020; Kabiri y Hosseinzadeh, 2025; Lee y Jung, 2025; Shadmanfaat *et al*., 2020; Vepsäläinen *et al*., 2025). En dinámicas concretas como las del *hacking* juvenil, la versión clásica de esta teoría diría que la decisión de actuar delictivamente surge de la interacción entre la propensión individual (es decir, una estructura moral que no identifica este delito cibernético como incorrecto, junto con un limitado autocontrol) y la exposición a un escenario criminógeno, que en este caso puede involucrar dimensiones tanto físicas como virtuales, en la que las reglas morales del entorno son permisibles hacia este tipo de prácticas y no existe un control formal ni informal efectivo. Esta interacción influye en cómo algunos adolescentes perciben la situación, haciendo que definan moralmente la acción del *hacking* ilegítimo como aceptable, lo que condiciona su selección como una opción factible.

Ahora bien, pese al evidente interés que ha producido en algunos países el fenómeno del *hacking* ilegal perpetrado por adolescentes, resultan aún escasos los estudios que, desde la criminología, lo aborden mediante la aplicación rigurosa y sistemática de sus marcos teóricos tradicionales (p. ej., Bekkers *et al*., 2025a; Bossler y Burruss, 2011; Kim *et al*., 2024; Fox y Holt, 2021; Marcum *et al*., 2014; Vlckova y Burianek, 2025). En este sentido, la TAS ha sido utilizada de forma limitada para el análisis de la delincuencia *online* (Hardie y Rose, 2025) y, con mucha menos frecuencia, para explicar fenómenos específicos como el intrusismo informático o *hacking* ilegal juvenil (Vepsäläinen *et al*., 2025). No obstante, merece una atención especial la propuesta de Pérez (2017), quien plantea una reformulación de la TAS orientada al estudio de los entornos digitales, conocida como *Situational Action Theory Revised for the Internet* (*SAT-RI*, por sus siglas en inglés). Sin pretender, hasta cierto punto, reemplazar el marco original, esta adaptación busca ajustarlo a las singularidades del ciberespacio, incorporando factores, conceptos y procesos causales que no habían sido considerados en su diseño inicial, permitiendo de este modo, según su autor, una interpretación más adecuada de las actividades delictivas en espacios virtuales.

La *SAT-RI* plantea tres aspectos que podrían resultar relevantes para el análisis de la TAS clásica en el mundo cibernético. En primer lugar, propone una reconceptualización del entorno de acción, al entender Internet no como una simple extensión del espacio físico, sino como un escenario 'autónomo', regido por sus propios códigos, normas y valores que influyen en las oportunidades y condiciones del *hacking* y de otros delitos digitales. En segundo lugar, incorpora al modelo revisado la presencia de guiones de neutralización específicos del ciberespacio, así como diversas distorsiones cognitivas y narrativas de carácter estructural o cultural que se articulan con la *propensión individual al ciberdelito* (moralidad e intención delictiva) y con formas de exposición al contexto ambiental de Internet. De este modo, la *SAT-RI* permite explicar cómo personas que, en entornos físicos, actúan conforme a la ley, pueden justificar e implicarse en prácticas ilícitas *online* como el *hacking*. Finalmente, este modelo subraya el papel de ciertas características estructurales inherentes a la 'arquitectura de Internet' (como, por ejemplo, la accesibilidad, el anonimato, la asincronía, la ubicuidad, la existencia de redes y comunidades virtuales o la ausencia de controles formales eficaces), las cuales operan como condiciones situacionales que alteran de manera significativa tanto el autocontrol como la percepción de oportunidades (en términos de costos y beneficios) para cometer *hacking* ilegal.

Por otra parte, en estudios sobre el *hacking* juvenil que no adoptan directamente el marco teórico de la TAS (como es el caso de la *SAT-RI*), se observa también una atención recurrente a variables clave del modelo original. Por ejemplo, diversas investigaciones han coincidido en que un bajo nivel de autocontrol (manifestado, entre otras formas, mediante la impulsividad o la búsqueda de riesgos), combinado con otros factores individuales como la disposición y actitud favorable hacia el delito, normas propias que favorecen el *hacking* malicioso o experiencias previas de delincuencia fuera de línea, así como con factores contextuales como los vínculos familiares débiles, la supervisión parental deficiente o la fuerte influencia de amigos o compañeros infractores, ya sean virtuales o presenciales, aumenta significativamente la probabilidad de que los jóvenes se vean involucrados en actividades de acceso informático ilegal (Back *et*

al., 2018; Bekkers *et al*., 2025a; Fox y Holt, 2021; Holt y Steinmetz, 2021; Holt *et al*., 2020; Kim *et al*., 2024; Lee y Holt, 2020; Marcum *et al*., 2014; Udris, 2016)[8]. Cabe destacar, además, que varios de los factores ya abordados por la TAS clásica adquieren nuevas orientaciones interpretativas en algunas de estas investigaciones.

Sumado a esto, la *SAT-RI* y otras propuestas centradas en el *hacking* han adoptado variables que son, o podrían llegar a ser, de interés para un análisis del planteamiento original de Wikström en circunstancias específicas del ciberespacio. Por ejemplo, mientras que Aiken *et al.* (2024) y Martineau *et al*. (2024) insisten en el papel central de las normas morales internalizadas y los contextos situacionales (un enfoque afín con el marco clásico de la TAS), Palmieri *et al.* (2021) añaden una perspectiva biotemperamental al vincular predisposiciones neuropsicológicas, como la sensibilidad individual ante la recompensa y el castigo, con el funcionamiento del autocontrol y la respuesta frente a la disuasión. En entornos digitales, donde las señales de castigo son menos visibles debido al anonimato y a la ausencia de consecuencias inmediatas, dichas disposiciones pueden condicionar los procesos que incentivan y controlan la conductua, por ejemplo, reduciendo la inhibición ante riesgos percibidos de sanción y potenciando la búsqueda de recompensas inmediatas. Asimismo, el trabajo de Gordon y Ma (2003) añade una dimensión relevante al introducir la noción de mecanismos de justificación moral, posteriormente integrada (como formas de neutralización) en la *SAT-RI* y en otras investigaciones empíricas sobre el *hacking* (p, ej., Bossler, 2021; Connolly *et al*., 2025), e incluso extendida al análisis de fenómenos como el ciberacoso (Hu *et al*., 2024). En determinados entornos digitales, ciertas justificaciones o racionalizaciones morales funcionan como mecanismos cognitivos que modulan la influencia de emociones morales como la culpa, facilitando que el individuo tome la decisión de transgredir las normas en estos espacios.

En correspondencia con Pérez (2017) y Palmieri *et al.* (2021), Smith (2024) propone además ampliar los modelos teóricos tradicionales incorporando

[8] Aunque también se debe señalar que Gordon y Ma (2003) no encontraron evidencia de una asociación entre autocontrol e intención de *hackin*g, y Guo y Wang (2024) lo consideran un predictor de baja relevancia para este tipo de ciberdelito.

'variables tecnológicas', lo que ayuda a explicar por qué, entre otras razones, personas con una motivación delictiva orientada a la gratificación pueden incurrir en ciberdelitos como el *hacking* cuando el entorno ambiental de Internet lo facilita. De hecho, uno de los aportes más relevantes de todos estos autores radica, en buena medida, en mostrar cómo 'condiciones estructurales' del ciberespacio afectan la relación clásica entre percepción, decisión y acción. En relación con esto, la literatura también muestra que la expectativa de sanción o castigo actúa de forma ambivalente en ámbitos digitales: mientras que la disuasión legal parece tener un efecto limitado, la censura o desaprobación social proveniente de padres o amigos cercanos al adolescente ejerce un impacto más importante en el acceso informático ilegal (un hallazgo que también fue identificado por Patchin e Hinduja [2018] en el caso del ciberacoso). Esto apunta a que, al menos en jóvenes, como sugieren estos resultados, las formas informales de control parecen ser más efectivas que el castigo institucionalizado o formal, incluido cuando existe riesgo de su aplicación (Aiken *et al*., 2024).

Por último, desde un 'enfoque de interdependencia', algunos estudios revisados sobre el *hacking* asociado a adolescentes, tienden a abandonar las explicaciones lineales para proponer modelos más complejos que expliquen la acción recíproca entre persona y ambiente. Este patrón, además, ha sido observado en otros delitos digitales, como el ciberacoso (Lee y Jung, 2025; Lee *et al*., 2021; Liu *et al*., 2020; Shadmanfaat *et al*., 2020) o la piratería digital (Choi y Yun, 2019). En el ámbito del *hacking*, Palmieri *et al*. (2021) sostienen que, por ejemplo, el sistema BIS (*Behavioral Inhibition System*, o Sistema de Inhibición Conductual), responsable de contener las conductas infractoras ante señales de castigo, puede ver afectada su eficacia cuando el entorno altera la percepción de peligro o riesgo. Este sería el caso del ciberespacio, donde el anonimato, como ya se indicó, actúa en ciertos niveles de Internet como un elemento que distorsiona la evaluación del riesgo y, por lo tanto, debilita el funcionamiento de dicho sistema. Los autores describen este proceso como un modelo de moderación situacional, en el cual determinadas características del espacio digital no solo influyen, sino que transforman la acción de este factor individual inhibitorio. En esta dirección, Smith (2024) propone un

marco integrador según el cual factores de diversa naturaleza (individuales, como rasgos personales o motivaciones; sociales, incluyendo la presión de grupo o la influencia de la 'subcultura hacker'; y tecnológicos, como el acceso o el anonimato) convergen e interactúan de manera dinámica, ofreciendo así una explicación más completa y precisa de este ciberdelito. Este enfoque se ve reforzado por los hallazgos de Martineau *et al*. (2024), quienes, a partir del análisis de narrativas cualitativas, identifican una trayectoria evolutiva del *hacking* ilícito (comprendida en tres fases: inicio, continuación y abandono) vinculada, en cada etapa, a la compleja interacción entre variables contextuales (p. ej., violencia doméstica, baja supervisión familiar, participación en 'foros de hackers', etc.) e individuales (p. ej., dificultades académicas, deficiente autocontrol, uso de técnicas de neutralización, etc.) que actúa como un amplificador del riesgo.

En síntesis, aunque el entorno digital introduce dinámicas singulares y la aplicación de la TAS al acceso indebido a sistemas informáticos ha sido limitada, la evidencia empírica disponible sugiere que varios de sus predictores y mecanismos de interrelación podrían tener un potencial explicativo muy valioso para esta conducta. Esta afirmación encuentra fundamento en algunos de los estudios señalados que, aun sin adoptar explícitamente la TAS, coinciden en destacar la importancia, por ejemplo, del autocontrol, las normas morales (individuales o ambientales) o el castigo informal, en consonancia con los supuestos centrales del modelo.

2.- El presente estudio

Si bien la TAS presenta una aceptable capacidad explicativa frente a la delincuencia tradicional u *offline*, su aplicación empírica a comportamientos ilícitos o indebidos en entornos digitales sigue siendo muy reducida (Hardie y Rose, 2025; Pauwels *et al*., 2018; Vepsäläinen *et al*., 2025). Este déficit es más marcado en el contexto de América Latina, donde los estudios criminológicos que analizan prácticas delictivas juveniles en el ciberespacio son casi inexistentes. No obstante, la TAS se plantea como una teoría general capaz de explicar la conducta delictiva y problemática en poblaciones adolescentes, también en diferentes continentes y en escenarios digitales (Kabiri, 2025; Kabiri y Hosseinzadeh, 2025; Vepsäläinen *et al*.,

2025), aun cuando su formulación original se orientó al análisis de acciones específicas del mundo físico. En tal sentido, la presente investigación parte de un problema concreto: la insuficiente comprobación empírica de la capacidad explicativa de la TAS respecto a prácticas delictivas en el espacio virtual (Hardie y Rose, 2025), particularmente en adolescentes pertenecientes a nuestra región.

Considerando todo lo expuesto, este artículo analiza en qué medida los factores y procesos planteados por la TAS explican la implicación de adolescentes latinoamericanos en prácticas de *hacking* ilegal. De ello se derivan dos cuestiones operativas: si la propensión individual al delito y la exposición criminógena a contextos digitales de riesgo predicen efectivamente esta conducta, y si dicha implicación depende de la interacción entre estos dos conceptos. Así, el propósito general de este estudio es evaluar la capacidad explicativa de la TAS en el espacio virtual, a partir de datos de cinco países latinoamericanos incluidos en la cuarta edición del *ISRD-4* (Marshall *et al*., 2022).

Con este propósito, decidimos examinar empíricamente uno de los postulados centrales de la TAS, según el cual la conducta delictiva se explica por la interacción entre individuo y ambiente. Aunque esta formulación, base de la hipótesis PEA (PxE→A), ha sido desarrollada principalmente para interpretar delitos del mundo físico, su aplicación al *hacking* permite explorar hasta qué punto los patrones de heterogeneidad interindividual propuestos por esta teoría (Hirtenlehner y Mesko, 2025) también operan en ambientes virtuales. Para comenzar a profundizar en esto, el primer objetivo se centra en analizar los efectos directos e independientes sobre esta conducta de dos de los constructos principales de la TAS: la propensión individual y la exposición a entornos criminógenos. En este estudio, la primera hipótesis plantea que:

> H1: La frecuencia de las prácticas de *hacking* entre los adolescentes de la muestra se incrementa a medida que aumenta tanto la *propensión individual al hacking* como la *exposición a entornos digitales criminógenos*, considerando el efecto específico de cada uno de estos predictores sobre la conducta.

El segundo objetivo aborda un nivel complejo de interacción (moderación simple) de orden individual (Hirtenlehner y Mesko, 2025; Kennedy, 2024), para evaluar si la fuerza del efecto del entorno digital criminógeno en la variable explicada depende del nivel de propensión al ciberdelito del adolescente, tal como lo plantea la TAS para los delitos del mundo *offline*. Desde esta perspectiva, se examina si quienes presentan una mayor predisposición al *hacking* (esto es, una moralidad individual más débil y un menor autocontrol) muestran una mayor vulnerabilidad a los contextos en línea criminógenos. Este enfoque conduce, en consecuencia, a plantear la siguiente hipótesis:

> H2: El efecto de la exposición al entorno digital criminógeno en los niveles de *hacking* incrementa a medida que aumenta la propensión individual hacia esta conducta. De tal manera que el efecto de la exposición a este entorno sobre la frecuencia de *hacking* será más acentuado entre los adolescentes con alta propensión individual, mientras que entre aquellos con baja propensión dicho efecto será mínimo o, incluso, nulo.

En suma, este estudio evalúa empíricamente una de las principales hipótesis interactivas de la TAS en una muestra multinacional de adolescentes latinoamericanos, un contexto poco explorado en la literatura. A diferencia de los estudios previos sobre esta teoría centrados en poblaciones juveniles europeas (p, ej., Kennedy, 2024; Kroneberg y Nägel, 2024), asiáticas (p. ej., Alruwaili, 2019; Kokkalera *et al*., 2020; Liu *et al*., 2020) y norteamericanas (p. ej., Ishoy y Blackwell, 2018), esta investigación aborda un vacío crítico tanto en la validez intercultural y generalización de la TAS, como en la comprensión de la ciberdelincuencia juvenil en América Latina. Así, se busca aportar evidencia sobre la aplicabilidad y eficacia del modelo clásico de Wikström en fenómenos cibernéticos como, por ejemplo, el *hacking* ilegal, ampliando la perspectiva sobre las dinámicas digitales en jóvenes de nuestra región.

3.- Método

3.1.- Participantes

La muestra estuvo conformada por 10.538 adolescentes escolarizados entre octavo y undécimo año de bachillerato, provenientes de instituciones

públicas y privadas ubicadas en dos ciudades (una mediana y otra grande) de Argentina, Brasil, Colombia, México y Venezuela. Todos los participantes formaron parte de la cuarta edición del estudio internacional *ISRD* (Marshall *et al*., 2022). Tras aplicar criterios de filtrado por edad, limitando la muestra a estudiantes entre 13 y 18 años, así como de otros parámetros destinados a mejorar la calidad de los datos (p. ej., inconsistencias en la información suministrada y valores atípicos), se configuró una muestra final de 9.645 casos (X_{edad} = 15,10; DT = 1,35) compuesta en un 52,3% por adolescentes del género femenino y en un 47,7% del género masculino[9]. La participación fue completamente voluntaria y se contó en cada país con el consentimiento informado de los adolescentes, previa autorización de los responsables institucionales correspondientes para la aplicación del instrumento.

3.2.- Medidas

3.2.1.- Variable dependiente

Hacking. La conducta de *hacking*[10] se empleó como variable dependiente y se evaluó mediante un único ítem que preguntaba si, en los últimos 12 meses, el encuestado había 'hackeado' o ingresado en una cuenta privada o en algún computador para adquirir datos, obtener el control de una cuenta o borrar información. Coherente con la estructura de medición del *ISRD-4* para los ciberdelitos (abuso basado en imágenes, incitación al

[9] Los participantes identificados como 'no binario' no se incluyeron en los análisis por su baja representación en la muestra (1,6%), lo que impide estimaciones estadísticas fiables para comparaciones entre categorías de sexo/género. Esta decisión se tomó especialmente para asegurar la validez y estabilidad de los modelos de regresiones.

[10] Aunque medido en este estudio mediante autoinforme, se destaca que el *hacking* está tipificado penalmente en los cinco países estudiados siempre que el acceso a sistemas informáticos se realice ´sin autorización', con sanciones o medidas previstas según los marcos normativos aplicables en cada uno de ellos. Está tipificado en el Artículo 153-bis del Código Penal argentino, el Artículo 154-A del Código Penal brasileño, los Artículos 269 A al 269 J del Código Penal colombiano, el Artículo 211 (bis 1, bis 2 y bis 4) del Código Penal Federal mexicano y el Artículo 6 de la Ley Especial contra los Delitos Informáticos de Venezuela. Esta referencia confirma que la medida de *hacking* usada refleja una infracción jurídicamente definida y comparativamente equivalente, cuya detección por los organismos de control formal traería, si el acceso no es autorizado, consecuencias legales. Desde la perspectiva de la TAS, tal delimitación es importante, ya que ubica esta conducta dentro del dominio de las acciones delictivas moral y jurídicamente establecidas, condición necesaria para analizar las causas y procesos postulados por esta teoría.

odio *online*, ciberfraude y *hacking*) y con el resto de conductas antinormativas autoinformadas, se solicitó además reportar la frecuencia con la que se había incurrido en esta conducta, indicador que se empleó en los análisis estadísticos de este estudio por su mayor potencial de variación. Valores más altos en esta medida significan una participación más frecuente en esta forma de delito cibernético.

3.2.2.- Variables independientes y de control

Moralidad individual. En este estudio, la moralidad individual se operacionalizó a través de creencias morales específicamente referidas al *hacking*. Estas creencias se midieron mediante un único ítem que evaluaba, en una escala de cuatro puntos, qué tan malo consideraban los adolescentes que una persona de su edad 'hackeara' una computadora o descubriera la contraseña de una cuenta ajena para obtener o borrar datos (Marshall *et al*., 2022). Las opciones de respuesta iban desde 'Muy mal' [1] hasta 'Nada mal' [4], es decir, esta última opción se asocia con un sentido de moralidad individual más débil. Para los análisis, las puntuaciones originales fueron transformadas en puntuaciones *z*, lo que permitió estandarizar la medida y facilitar su interpretación comparativa en los modelos estadísticos.

A*utocontrol*. Este concepto de capturó mediante seis ítems adaptados de la Escala de Grasmick *et al*. (Marshall *et al*., 2022), incluyendo tres ítems sobre impulsividad (p. ej., 'Actúo en el momento sin detenerme a pensar') y tres sobre tendencia al riesgo (p. ej., 'Algunas veces hago cosas arriesgadas para divertirme'). Las respuestas se recogieron con una escala Likert de cinco puntos (1 = 'Totalmente en desacuerdo'; 5 = 'Totalmente de acuerdo'). Tras sumar los seis ítems, donde puntuaciones más altas significan un menor nivel de autocontrol, el índice total fue estandarizado mediante puntuaciones *z*. La escala mostró una consistencia interna adecuada (α de Cronbach = .77) según los criterios orientativos propuestos por Nunnally y Barnstein (1994).

Propensión individual al hacking. Debido a que la propensión al delito es el resultado del efecto conjunto de la moralidad individual y el autocontrol según la TAS, se sumaron las puntuaciones *z* de ambas variables para

crear una medida con la cual estimar la disposición personal al *hacking*. Puntajes más altos representan una mayor propensión, reflejando una combinación de débil moralidad y bajo autocontrol.

Exposición a entornos digitales criminógenos. Este constructo se midió mediante un índice orientado a captar los estilos de vida y rutinas *online* de los estudiantes, asumiendo que, al igual que ocurre en el mundo físico (Engström, 2018), los distintos usos de Internet generan niveles diferenciados de exposición criminógena (Dolliver y Love, 2015; Kaakinen *et al*., 2021). Con esta variable se cuantifica la frecuencia con la que se visitan espacios virtuales de riesgo o peligrosos asociados en la literatura con mayores medios y oportunidades criminógenas (Alves y Miró, 2024; Bekkers *et al*., 2025c; Brewer *et al*., 2018; Carcelén *et al*., 2025; Ferrara *et al*., 2021; Hawdon *et al*., 2020; Livingstone y Stoilova, 2021; Meldrum *et al*., 2026; Savoia *et al*., 2021; Sirola *et al*., 2024; Temara, 2024; Tomazic y Bessa, 2017). En concreto, se preguntó con qué frecuencia los participantes: (i) navegan en la *Deep Web* o *Darknet*[11], (ii) ingresan a sitios prohibidos para menores de edad y (iii) realizan apuestas en línea. Cada ítem se respondió en una escala de seis categorías, desde 'Nunca' (1) hasta 'Varias veces por hora' (6).

Atendiendo a los estudios relativos a la TAS sobre exposición criminógena *offline* basados en el concepto de estilo de vida arriesgado (*Risky lifestyle*) (p. ej., ver Hirtenlehner y Mesko, 2025; Pauwels *et al*., 2018), se mantuvo una estructura aditiva en esta medida, ya que los tres ítems representan facetas complementarias de actividades y rutinas de riesgo asociadas al uso de Internet[12]. Para obtener un índice general, estos ítems también fueron

[11] La *deep web* o 'red profunda' se refiere a una parte de Internet con contenidos no indexados por motores de búsqueda, mientras que la *darknet* constituye un subconjunto de ella, integrada por redes estratégicamente ocultas (Gallo, 2025; Meldrum *et al*., 2026). El acceso a la *darknet* requiere de herramientas de anonimato como *TOR* (*The Onion Router*) o *I2P* (*Invisible Internet Project*), que cifran y encaminan el tráfico para preservar la identidad del cibernauta (Botchkovar *et al*., 2025; Meldrum *et al*., 2026; Sirola *et al*., 2024; Temara, 2024). En algunos de los países incluidos en este estudio, ambos términos son utilizados de forma indistinta por los adolescentes, pese a sus diferencias técnicas.

[12] Conviene señalar que esta medida no captura la relación del encuestado con amigos o compañeros involucrados en actividades de *hacking* aun cuando la encuesta del *ISRD-4* dispone de este indicador. Dado que la literatura especializada demuestra que las medidas de iguales están afectadas por importantes problemas de identificación (incluida, por ejemplo, la imposibilidad de distinguir

estandarizados mediante puntuaciones *z* y posteriormente sumados. Un análisis preliminar de fiabilidad revela una consistencia interna moderada (α de Cronbach = .53), coherente con valores reportados en medidas agregadas que capturan comportamientos de baja prevalencia y heterogéneos (p. ej., Svensson y Pauwels, 2010). Los valores más altos de esta variable corresponden a un mayor nivel de exposición a entornos criminógenos en Internet.

*Término de Interacción Propensión*Exposición.* Este representa la probabilidad de que se produzca el *hacking*, calculada como el producto de la multiplicación de las puntaciones de Propensión individual al *hacking* y Exposición a entornos digitales criminógenos. Esta medida (Propensión*Exposición) refleja el riesgo de involucrarse en conductas como el *hacking* como resultado de la combinación de características personales y contextuales (hipótesis PEA), específicamente dentro del contexto digital.

Variables sociodemográficas. Se incorporó a los análisis la variable género (codificada como 0 = mujer y 1 = hombre) y la variable edad medida por los años de encuestado. La Tabla 1 resume los descriptivos de todas las variables de estudio.

Tabla 1. Descriptivos de las principales variables de estudio

Variables	N	Media	DE	Mínimo	Máximo
Hacking (Frecuencia, log.)	9333	.04	.23	0	3
Moralidad individual (puntuación *z*)	9521	.00	1.00	-.64	3.55
Autocontrol (puntuación *z*)	9294	.00	1.00	-2.26	2.24
Propensión individual al *hacking* (puntuación *z*)	9232	.00	1.51	-3.00	6.00
Exposición a entornos digitales criminógenos (puntuación *z*)	9291	-.01	2.15	-1.00	12.00
Interacción Propensión*Exposición (PxE)	8982	.88	4.10	-29.00	71.00
Sexo (1= hombre)	9444	.48	-	-	-
Edad	9182	15.10	1.35	13	18

rigurosamente la selección y el contagio [Shalizi y Thomas, 2011], los efectos del *reflection problem* [Manski, 1993] y los sesgos asociados al uso de percepciones autorreportadas sobre la conducta de los amigos [Helms *et al.*, 2014]), se decidió descartar este tipo de indicador de riesgo y privilegiar otras aproximaciones contextuales, centradas en dominios y oportunidades de Internet favorables para la acción digital. No obstante, al igual que las medidas basadas en estilos de vida empleadas en las investigaciones TAS previas (Pauwels *et al*., 2018), el índice confeccionado en este estudio ofrece una aproximación válida y conceptualmente coherente al grado de exposición recurrente a oportunidades criminógenas en el ambiente digital.

3.3.- Procedimiento analítico

La estrategia de análisis se diseñó para responder de manera coherente a la hipótesis PxE derivada de la TAS y a las características de los datos. Dada la evidente asimetría de la variable dependiente frecuencia de *hacking* se aplicó una transformación logarítmica (asimetría original = 11,49; asimetría variable transformada = 6,49) con el fin de atenuar la heterocedasticidad y aproximar la normalidad de los errores (aunque se llevaron a cabo análisis adicionales en la escala original para verificar la consistencia de los hallazgos), una práctica usada en otros estudios criminológicos con variables de conteo altamente sesgadas (p. ej., Hardie, 2019; Hirtenlehner y Hardie, 2016; Hirtenlehner y Treiber, 2017). Después de esta transformación, se realizaron análisis descriptivos iniciales y correlaciones (Pearson) para examinar la estructura asociativa entre los conceptos centrales de la TAS (propensión individual al *hacking* [y sus factores constitutivos] y exposición a entornos digitales criminógenos) y la conducta de *hacking*.

A continuación, se procedió a explorar la interacción PxE mediante un análisis comparativo de medias orientado a examinar las diferencias en la frecuencia de *hacking* entre cuatro grupos formados por la combinación de niveles altos y bajos (dicotomizados por la mediana) de propensión individual al *hacking* y exposición contextual. Esta estrategia, coherente con estudios anteriores (p. ej., Hirtenlehner y Mesko, 2025), permite un examen exploratorio del posible patrón de interacción subyacente (p. ej., mayor ocurrencia de *hacking* cuando coinciden altos niveles de propensión y altos niveles de exposición). Dado que las distribuciones continuaban mostrando asimetrías y violaciones parciales de homocedasticidad, el contraste entre los cuatro grupos se realizó mediante la prueba *H* de Kruskal-Wallis. Asimismo, se construyó también un primer gráfico de interacción exploratorio (Y = media log. transformada de *hacking*; X = niveles de exposición; líneas = niveles de propensión), que permite visualizar si la pendiente de la relación entre exposición y *hacking* varía sistemáticamente según los niveles de propensión, lo cual constituye la esencia de la hipótesis interactiva PxE.

Sobre la base de lo anterior, se desarrollaron los análisis multivariantes posteriores. Así, para estimar los efectos directos e independientes y los

interactivos se optó por un enfoque de regresiones MCO con dos modelos comparativos. El primero incluyó los dos predictores teóricos clave, controles básicos (edad y sexo) y errores estándar robustos por clúster (una decisión metodológica motivada por la naturaleza del diseño muestral del *ISRD-4*) estimados mediante PROCESS v.5.0. El segundo modelo añadió, además de los predictores y controles previos, el término de interacción. Este modelo permite evaluar si el efecto de los factores contextuales sobre la conducta de *hacking* varía según el nivel de propensión individual, asumida en todos los análisis como el moderador. Además de verificar la significación estadística de la interacción PxE, se profundizó en su forma o naturaleza (fuerza y dirección). Para ello se aplicó con el apoyo de PROCESS v.5.0, un Análisis de Pendientes Simples (*Simple Slopes Analysis*) con 10.000 réplicas *bootstrap*, siguiendo el procedimiento de Hayes (2018). Esto permitió estimar cómo varían los efectos condicionales de la exposición criminógena sobre la variable respuesta según los niveles (bajos, medios y altos) de propensión individual al *hacking*[13]. Finalmente, para contrastar si las pendientes asociadas a los efectos condicionales se diferencian estadísticamente entre sí, se aplicó la prueba *Z* propuesta por Paternoster *et al.* (1998), creada originalmente para evaluar la igualdad de coeficientes de regresión estimados en (sub)muestras comparables. Todos los análisis se realizaron en SPSS v.26.

4.- Análisis de datos

4.1.- Correlaciones bivariadas

Las correlaciones producto-momento presentadas en la Tabla 2 evidencian asociaciones conformes a las expectativas teóricas, mostrando patrones coherentes entre los predictores individuales y contextuales y la frecuencia de *hacking* en el marco de la TAS. Consistente con este enfoque, el *hacking* se relaciona positivamente (aunque la fuerza de esta primera asociación no es tan intensa) con el autocontrol (r[9005] = .10, p <.001), la moralidad individual (r[9225] = .22, p <.001), y, de manera también

[13] Los adolescentes se clasificaron en tres grupos según su propensión individual: niveles bajos (≤ 1 DE por debajo de la media), niveles medios (entre − 1 DE y + 1 DE) y niveles altos (≥ 1 DE por encima de la media).

relevante, con la propensión individual al *hacking* (r[8951] = .22, p <.001)[14], demostrando que una moralidad débil y un bajo autocontrol se asocian con una mayor implicación en esta conducta. Por su parte, el contacto con entornos digitales criminógenos muestra (con menor intensidad) una asociación estadística con la frecuencia de *hacking* en la dirección esperada. El producto del término PxE, también muestra una relación significativa con la variable respuesta (r[8713] = .11, p <.001), lo que indica que la interacción entre predisposiciones individuales y exposición a ambientes digitales de riesgo incrementa la implicación en esta conducta. Este importante hallazgo apoya la idea central del enfoque PxE y define, a partir de aquí, el eje analítico que guiará la evaluación detallada de los efectos interactivos en los siguientes pasos.

Tabla 2. Correlaciones bivariadas entre las variables centrales da la TAS

Variables	1	2	3	4	5	6	7
1. *Hacking* (Frecuencia, log.)	-						
2. Moralidad individual (puntuación *z*)	.22***	-					
3. Autocontrol (puntuación *z*)	.10***	.15***	-				
4. Propensión individual al *hacking* (puntuación *z*)	.22***	.76***	.76***			-	
5. Exposición a entornos digitales criminógenos (puntuación *z*)	.10***	.20***	.22***	.27***			
6. Interacción Propensión*Exposición (PxE)	.11***	.21***	.08***.	.19***	.42***	.	
7. Sexo (1= hombre)	.03**	.10***	.06***	.11***	.22***	.06***	
8. Edad	.00 n.s.	-.02 n.s.	.02 n.s.	.00 n.s.	.03**	-.01 n.s.	.01 n.s.

n.s.: no significativo
*p ≤.05; **p ≤.01; ***p ≤.001

4.2.- Análisis de interacción preliminares

Como segundo paso, tras identificar una correlación estadísticamente significativa entre el término de interacción PxE y el logaritmo de la frecuencia de *hacking*, se examinó con mayor detalle el patrón subyacente mediante un análisis de diferencias de medias. La Tabla 3 muestra que las

[14] Las correlaciones de casi todos los predictores se mantienen en rangos aceptables, con valores elevados únicamente entre moralidad y propensión (r[9232] = .76, p <.001) y entre autocontrol y propensión (r[9232] = .76, p <.001), resultado que es lógicamente consistente con la composición o configuración de esta última variable. No obstante, debido a que los VIF no superan 1.07 (O'Brien, 2007), la multicolinealidad no representa un problema relevante en este estudio.

combinaciones entre la propensión individual y la exposición criminógena configuran perfiles claramente diferenciados de implicación en *hacking*. El nivel más bajo se observa en el grupo baja propensión/baja exposición (M = .01), mientras que el más elevado corresponde al grupo alta propensión/alta exposición (M = .09). Los grupos de nivel medio presentan una tendencia coherente con una variación progresiva, y la prueba de Kruskal-Wallis confirma la existencia de diferencias estadísticamente significativas entre las cuatro condiciones ($H_{(3)}$ = 203.98, p <.000)[15]. En conjunto, este patrón respalda en un principio el supuesto central de la TAS, según el cual la conducta infractora tiende a intensificarse cuando se combinan disposiciones personales favorables a la transgresión y entornos caracterizados por presentar determinadas características criminógenas.

Tabla 3. Medias de *hacking* por categorías de propensión individual al *hacking* y exposición a entornos digitales criminógenos

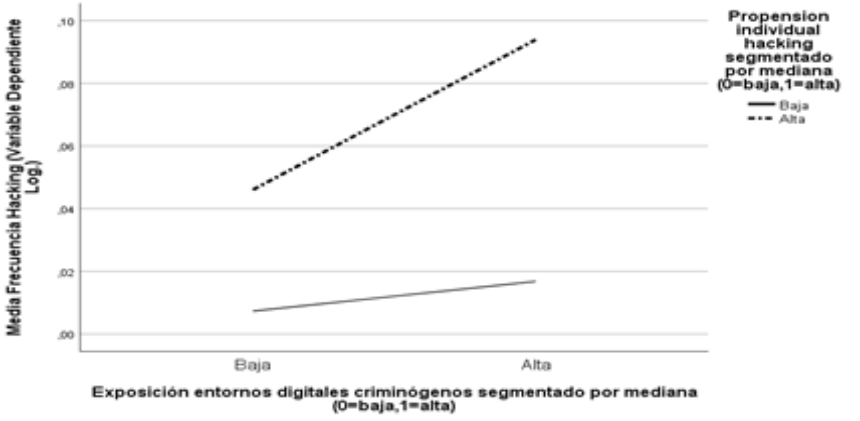
Propensión individual al *hacking*	Exposición a entornos digitales criminógenos	Media (DE) de frecuencia de *hacking*
Baja	Baja	.01 (.09)
Baja	Alta	.02 (.14)
Alta	Baja	.05 (.24)
Alta	Alta	.09 (.36)

n = 8.713

La Figura 1 confirma visualmente esta lógica interactiva. La pendiente vinculada al incremento en la exposición al entorno criminógeno se intensifica de manera considerable en el grupo de adolescentes más propensos al *hacking*; en cambio, entre los adolescentes menos propensos, dicho aumento no produce una variación relevante. La diferencia entre ambas líneas apunta hacia este posible efecto de moderación: el ambiente digital favorable a la transgresión ejerce una influencia más marcada sobre el *hacking* en aquellos adolescentes que manifiestan una alta predisposición hacia este tipo de prácticas. Este patrón empírico apoya nuevamente el postulado PEA.

[15] Las diferencias entre grupos se evaluaron mediante la prueba de Kruskal-Wallis y se corroboraron adicionalmente con un análisis de varianza que arrojó resultados consistentes ($F_{(3)}$=67,96, p <.000).

Figura 1. Exploración gráfica de la interacción entre propensión individual al *hacking* y exposición a entornos digitales criminógenos



Nota: Propensión individual al *hacking* y exposición a entornos digitales criminógenos se dicotomizaron en la mediana.

4.3.- Regresión MCO con términos de interacción y análisis de pendientes simples

En este tercer paso, y con base en las diferencias de medias y el primer gráfico de interacción presentados en el paso exploratorio, se analiza la significación estadística de los efectos interactivos encontrados anteriormente mediante dos modelos de regresión MCO presentados en la Tabla 4. En el Modelo 1, tanto la propensión individual al *hacking* (B = .03, t = 9.02, p <.001) como el contacto con entornos digitales criminógenos (B = .01, t = 3.26, p <.001) presentan efectos positivos y estadísticamente significativos en la variable respuesta, mientras que el género y la edad no alcanzan significación estadística. Interpretados en términos del logaritmo de la frecuencia anual de *hacking*, estos coeficientes representan incrementos aproximados de 3% (propensión) y de 1% (exposición) en la frecuencia esperada por cada aumento de una unidad en los respectivos predictores. Aunque la varianza explicada es modesta (R^2 = .05), los patrones observados son coherentes con la propuesta teórica de la TAS y robustos dado el tamaño muestral (n = 8.159). En definitiva, los resultados del Modelo 1 respaldan la primera hipótesis (H1),

al mostrar que tanto la propensión individual como la exposición criminógena a entornos digitales incrementan significativamente la frecuencia de *hacking*, es decir, ambos constructos actúan como predictores independientes de la variable respuesta.

Tabla 4. Predictores TAS de la frecuencia de *hacking* juvenil (MCO con errores estándar robustos por clúster)

	Modelo 1 B (CR) [t][a]	**Modelo 2** B (CR) [t]
Propensión individual al *hacking*	.03(.00) [9.02]***	.03(.00) [9.17]***
Exposición a entornos digitales criminógenos	.01(.00) [3.26]***	.00(.00) [2.00]*
Propensión*Exposición (Hipótesis PEA)	-	.00(.00) [3.19]***
Género	n.s.	n.s.
Edad	n.s.	n.s.
R^2 ajustado	.05	.06
N	8.159	8.159

[a]B = coeficientes de regresión, errores estándar robustos por clúster (entre paréntesis) y t-ratio [entre corchetes]. Variable dependiente: número de veces al año en que se incurrió en *hacking* (transformación logarítmica). Los predictores, propensión individual al *hacking* y exposición a entornos digitales criminógenos, están estandarizados en función de la escala *z* y el término de interacción es el producto de ambos predictores estandarizados.
*$p \leq .05$; **$p \leq .01$; ***$p \leq .001$; n.s.= no significativo

Por su parte, el Modelo 2 pone a prueba la H2 mediante la inclusión del término de interacción Propensión*Exposición en la ecuación, cuyo coeficiente resulta positivo y altamente significativo (B = 0.00, t = 3.19, $p < .001$). En esta fase del análisis, el objetivo no es aún caracterizar los efectos condicionales que serán tratados más adelante, sino determinar si la interacción identificada en los análisis previos mantiene significación estadística cuando se controla por los efectos principales de los dos

predictores teóricos y por el género y edad. El incremento de la varianza explicada ($R^2 = .06$) es un indicio de que el término multiplicativo añade cierta capacidad explicativa a la ecuación, aunque la magnitud de los efectos principales sea baja dada la escala logarítmica de la variable respuesta. En consecuencia, estos resultados constituyen inicialmente evidencia que apoya la Hipótesis 2, en tanto la interacción entre propensión individual y exposición a entornos digitales criminógenos constituye un componente estadísticamente significativo del proceso P×E postulado por la TAS.

Esto justifica metodológicamente la necesidad de desarrollar un análisis más concreto de los efectos moderadores observados. O, dicho de otro modo, proporciona la base empírica para examinar, en el paso siguiente, cómo la exposición a escenarios criminógenos en Internet se relaciona con el *hacking* según los distintos niveles de propensión.

En tal sentido, los resultados presentados en la Tabla 5 demuestran que el efecto condicionado de la exposición a entornos digitales criminógenos sobre la ocurrencia de *hacking* aumenta de manera progresiva a medida que incrementa la propensión individual. En concreto, entre los adolescentes de baja propensión, el efecto del contexto digital sobre el *hacking* fue prácticamente nulo y no significativo ($B = .001$, $SE = .001$, n.s.), es decir, no existe una relación estadísticamente significativa entre la exposición contextual y el *hacking* en este grupo. En el nivel medio, el efecto adquiere significación y una magnitud moderada ($B = .003$, $SE = .001$, $p \leq .01$). Finalmente, en el nivel de mayor propensión, el efecto alcanza una magnitud superior ($B = .012$, $SE = .004$, $p \leq .001$), mostrando un cambio claro y significativo en la pendiente. El remuestreo *bootstrap* (10.000 iteraciones) respalda la estabilidad y robustez de estas estimaciones.

En conjunto, estos resultados indican que, mientras los entornos *online* criminógenos apenas ejercen influencia entre los adolescentes que presentan baja propensión, su capacidad explicativa aumenta considerablemente conforme la propensión individual crece, resultando consistente con una relación de moderación. Estos resultados proporcionan evidencia de acuerdo con la segunda hipótesis planteada y con los postulados centrales de la TAS.

Tabla 5. Efectos condicionales de la exposición a entornos digitales criminógenos según niveles de propensión individual al *hacking* (MCO con errores estándar robustos por clúster)

	B (CR)[a]
Efectos condicionales de la exposición a entornos digitales criminógenos en:	
Niveles bajos de propensión individual al *hacking* (- 1 DT)	.001(.001) n.s.
Niveles medios de propensión individual al *hacking* (- 1 DT y + 1 DT)	.003 (.001)*
Niveles altos de propensión individual al *hacking* (+ 1 DT)	.012 (.004)***
Test de igualdad	*Z*[b]
Niveles bajos/Niveles medios	-1.41 [d] n.s.
Niveles medios/Niveles altos	-2.18**
Niveles bajos/Niveles altos	-2.67***

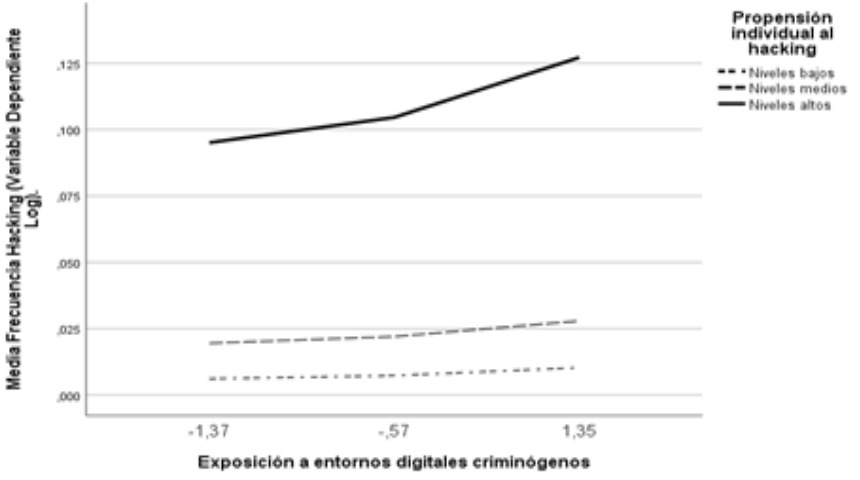
[a]B = coeficientes de regresión y errores estándar robustos por clúster entre paréntesis. Variable dependiente: número de veces al año en que se incurrió en *hacking* (transformación logarítmica). Bootstrap N remureos =10.000.
[b]*Z* = valores *Z*; **p* ≤.05; ***p* ≤.01; ***p ≤.001; n.s.= no significativo.

La Figura 2 aporta evidencia complementaria al mostrar pendientes de regresión claramente diferenciadas entre los niveles de propensión individual al *hacking*. La línea correspondiente al grupo de niveles altos presenta una inclinación considerablemente mayor que las de los grupos de niveles medios y bajos, reflejando diferencias claras en respuesta al tipo de contexto.

Las pruebas *Z* de diferencias de coeficientes (Paternoster *et al*.,1998) corroboran este patrón (ver Tabla 5), revelando contrastes significativos entre niveles bajos vs. altos ($Z = -2.67$, $p < .001$) y medios vs. altos ($Z = -2.18$, $p < .01$), mientras que la comparación bajos vs. medios no alcanza significación.

En conjunto, estos hallazgos confirman que el impacto del contexto digital criminógeno se intensifica precisamente entre los adolescentes con mayor propensión al *hacking*, reforzando la naturaleza interactiva propuesta en H2 y subrayando que el riesgo asociado a la exposición criminógena en el ciberespacio es especialmente crítico entre los adolescentes con niveles más altos de propensión individual.

Figura 2. Pendientes de regresión (MCO) del efecto de la exposición a entornos digitales criminógenos en el *hacking* diferenciadas por niveles de propensión individual



5.- Discusión y conclusiones

A partir de los datos comparativos de cinco países latinoamericanos integrantes del *ISRD-4*, este estudio examinó en qué medida la TAS explica las prácticas de *hacking* juvenil en ambientes digitales. Las diferentes pruebas y análisis estadísticos revelan un perfil consistente de resultados: la propensión individual al *hacking* y exposición a entornos digitales criminógenos operan como predictores significativos de la frecuencia de esta conducta, confirmando la primera hipótesis (H1).

Asimismo, los resultados indican que la exposición criminógena adquiere mayor peso a medida que aumenta la propensión individual, lo que valida la hipótesis de efectos interactivos (H2) y refuerza la idea central de la TAS según la cual las influencias ambientales se acentúan entre personas con mayor debilidad moral y menor autocontrol, es decir, más propensas al delito. No obstante, estos hallazgos requieren ser matizados a la luz de diversas consideraciones teóricas, empíricas y metodológicas.

En conjunto, los resultados confirman que el indicador de 'propensión individual al *hacking*' (concebida como la combinación entre creencias morales favorables a este tipo de prácticas y bajo autocontrol) actúa como un predictor significativo de la variable dependiente, en concordancia con la evidencia acumulada tanto en delitos *offline* como en ciberdelitos (véase Hardie y Rose, 2025; Pauwels, *et al*., 2018; Vepsäläinen *et al*., 2025). No obstante, este hallazgo precisa algunas consideraciones. Por un lado, el concepto de 'moralidad individual' suele capturarse en la mayoría de los estudios mediante indicadores de creencias morales sobre la conducta evaluada, junto con otros factores como las emociones morales (vergüenza y culpa), la internalización de la identidad moral o la empatía emocional (Hardie y Rose, 2025; Pauwels *et al*., 2018). Esta es una aproximación empírica útil, pero que deja por fuera componentes cognitivo-morales fundamentales, como las técnicas de neutralización, las cuales han sido identificadas en la literatura previa sobre delitos *online* como mecanismos que reinterpretan o atenúan las normas morales e influyen en la culpa moral (Bossler, 2021; Connolly *et al*., 2025; Gordon y Ma, 2003; Hu *et al*., 2024; Pérez, 2017). En función de estos hallazgos, se sugiere que las técnicas de neutralización podrían conceptualizarse como una dimensión adicional de la propensión individual en entornos digitales, dada su aparente capacidad explicativa en el ciberespacio (Schmitt *et al*., 2025).

Por otro lado, aunque la escala de 'bajo autocontrol' de Grasmick *et al*. (1993) mantiene correlaciones coherentes con la moralidad y con la frecuencia de *hacking*, lo que apoya observaciones anteriores (p. ej., Aiken *et al*., 2024; Back *et al*., 2018; Holt *et al*., 2020; Lee y Holt, 2020; Pérez, 2017; Udris, 2016), su capacidad predictiva parece ser más sólida en 'hackers' novatos o principiantes según los hallazgos de Bossler y Burruss (2011) y de Holt *et al*. (2021). Es decir, personas inexpertas, con habilidades técnicas básicas y amplios vínculos sociales, cuyas acciones suelen caracterizarse por métodos y formas simples de 'hackeo' y una búsqueda rápida de gratificación. Un patrón que, se podría especular, predomina probablemente en la muestra analizada en el presente estudio, dada la juventud de los participantes. En este sentido, se plantea la interrogante de si esta medida, derivada de la escala de Grasmick y su

equipo, resulta igualmente válida para poner a prueba la TAS en otros perfiles o subgrupos de 'hackers' como, por ejemplo, los identificados por Chng *et al*. (2022) en su investigación. O, por el contrario, si sería más apropiado recurrir a medidas de autocontrol que, por un lado, se basen en criterios diferentes a los utilizados en la clásica operacionalización de la *Teoría General del Delito* de Gottfredson y Hirschi (esto es, un rasgo fijo, estable y general asociado a la preferencia por conductas delictivas 'impulsivas, arriesgadas, de bajo esfuerzo e inmediata satisfacción'), o, por otro, se ajusten mejor a la concepción de la naturaleza situacional del autocontrol ante conflictos morales propuesta por la TAS (Hardie y Rose, 2025; Hasselhorn *et al*., 2025). Atender a estas cuestiones, es decir, qué dimensiones de la moralidad se incorporan y qué tipo de 'hacker' se captura con la medida de autocontrol, resulta esencial para precisar el verdadero alcance de la propensión individual en ambientes digitales[16].

La confirmación de la primera hipótesis también respalda la capacidad predictiva del constructo 'exposición a entornos digitales criminógenos', aunque su alcance explicativo requiere igualmente de algunas reflexiones. Por ejemplo, la exposición de los adolescentes a la *Darknet* implica acercarse a entornos donde operan grupos, comunidades o redes con normas morales que aceptan y promueven el acceso ilegítimo a sistemas informáticos y otro tipo de ciberdelitos (Botchkovar *et al*., 2025; Chrzanowska-Gancarz, 2022; Ferrara *et al*., 2021; Meldrum *et al*., 2026; Sirola *et al*., 2024; Smith, 2024). Estas comunidades, pese a su heterogeneidad estructural y organizativa (Romagna y Leukfeldt, 2023, 2025), mantienen códigos internos, creencias subculturales y estilos de interacción que orientan la conducta de sus miembros (Bekkers *et al*., 2025b; Bossler y Burruss, 2011). El control informal 'intragrupal' se ejerce, por ejemplo, mediante mecanismos simbólicos y relacionales tales como el

[16] Es muy importante considerar que la propensión individual no solo funciona como predictor de la conducta de *hacking*, sino que también podría orientar la selección de determinados entornos digitales, llevando a los adolescentes hacia espacios congruentes con sus propios valores y predisposiciones, donde los incentivos y oportunidades para este tipo de conductas se encuentran concentrados. De esta manera, incluso ante fuertes incentivos tecnológicos, las normas morales internas actúan como un filtro que modula tanto la acción delictiva como la exposición a situaciones de riesgo, reforzando la importancia de considerar la propensión individual como un factor que opera sobre la conducta de *hacking* concreta y la selección de contextos específicos.

prestigio o la reputación *online*, la sanción social y/o la exclusión de quienes no cumplen las normas pro-*hacking*, reforzando la internalización de definiciones, valores y conductas asociadas al intrusismo informático (Bossler y Burruss, 2011; Holt *et al*., 2012; Lee, 2018; Romagna y Leukfeldt, 2023, 2025; Sela, 2012). En paralelo, puede existir control y disuasión 'intergrupal' (p. ej., grupos de 'hackers éticos' vs. 'hacktivistas') que sancionan o desaprueban informalmente a quienes violan códigos generales de la comunidad, diferenciando las normas según orientación y objetivos del grupo (Romagna y Leukfeldt, 2023, 2025). Sumado a esto, la evidencia indica que, tanto la percepción subjetiva como las estrategias reales de detección y castigo formal por parte de las autoridades competentes en estos espacios o plataformas, suelen ser mínimas para un número significativo de delitos cibernéticos (Botchkovar *et al*., 2025; Meldrum *et al*., 2026; Ngo y Jaishankar, 2017; Pérez, 2017; Temara, 2024). En consecuencia, la percepción de criminogeneidad podría depender más de la estructura normativa y de los riesgos percibidos asociados a sanciones internas e informales (gestionadas comúnmente por moderadores o administradores de plataformas virtuales, líderes subculturales, amigos, iguales y/o adversarios [Romagna y Leukfeldt, 2025; Smith, 2024]), que de elementos externos de disuasión institucional.

Se reconoce que reducir la medición de la exposición criminógena a unas pocas variables basadas en conductas de riesgo digital simplifica en gran medida esta complejidad, dado que distintos microespacios (algunos completamente determinados por el anonimato) presentan variaciones en normas y eficacia de los mecanismos de control y disuasión tanto formales como informales. Precisamente, esta variabilidad normativa y de control es central en la TAS para definir la criminogeneidad de un entorno físico (Hardie y Rose, 2025), y todo parece indicar que esta lógica podría igualmente extenderse al mundo virtual. Por ello, aunque la medida compuesta de exposición constituye una aproximación útil, los resultados subrayan la necesidad de operacionalizaciones más sensibles y afinadas, que consideren, por ejemplo, distintos niveles de Internet (superficial vs. oculto), esquemas normativos internos y formas alternativas de control y sanción grupal (Romagna y Leukfeldt, 2025), así como otras formas de disuasión como la supervisión familiar (Bekkers *et al*., 2025b).

Asimismo, los análisis también muestran que el comportamiento 'hacker' de estos adolescentes se ajusta de manera consistente al principio de interacción central del mecanismo PEA (Wikström, 2009), según el cual la influencia de la exposición criminógena solo se activa cuando coincide con una propensión individual que permita definir la conducta como moralmente aceptable y factible. Así, los adolescentes con una inclinación moral contraria al ciberdelito analizado y con elevados niveles de autocontrol tienden a permanecer relativamente poco vulnerables a las circunstancias contextuales exploradas, mientras que quienes se hallan en rangos medios o altos de propensión individual parecen ser afectados con mayor facilidad por las condiciones criminógenas *online* en su proceso de percepción-elección. Este patrón reafirma la idea de la TAS (y de otras perspectivas paralelas sobre interdependencia enfocadas al ámbito digital [Palmieri *et al*., 2021; Smith, 2024]) de que las condiciones del entorno no operan como factores autónomos, sino como factores cuya eficacia depende de la agencia o características individuales del actor (y viceversa). No obstante, la magnitud moderada del efecto interactivo y las características de las medidas utilizadas (especialmente en la captación del contexto criminógeno y del bajo autocontrol) sugieren la necesidad de avanzar hacia operacionalizaciones más precisas, coherentes con los desafíos discutidos anteriormente.

Ahora bien, un hallazgo secundario, pero empíricamente relevante es que, a diferencia de lo reportado para el denominado 'norte global' (p. ej., Aiken *et al*., 2024; Marcum *et al*., 2014; National Crime Agency, 2024), el *hacking* juvenil en Latinoamérica presenta en este estudio una prevalencia mucho más baja (3,5%), siendo congruente con la evidencia previa del *ISRD* (Udris, 2016). Esta variación no resulta explicable solamente por artefactos metodológicos, sino que sugiere que, aunque el *hacking* adolescente constituye un fenómeno transnacional, su ocurrencia parece estar condicionada por las características operativas de Internet y por los niveles de digitalización asociados a la cultura y al desarrollo tecnológico de cada región (Chen *et al*., 2023; Vergara, 2024). Es decir, por ejemplo, el acceso diferencial a infraestructuras digitales según la ubicación geográfica, las formas culturalmente establecidas de socialización *online* y las normas que regulan la aceptabilidad (o no) de determinadas prácticas digitales guardan relación con la configuración de los factores y

procesos clave que hacen más o menos probables las conductas cibernéticas ilegales, incluido el *hacking* juvenil. Desde la perspectiva de la TAS, los resultados presentados en este trabajo son consistentes con la evidencia que indica que los mecanismos explicativos del delito mantienen su validez en distintas realidades sociales y culturales (Alruwaili, 2019; Kabiri, 2025; Kabiri y Hosseinzadeh, 2025; Kokkalera *et al*., 2020; Liu *et al*., 2020), dependiendo de la naturaleza de los contextos morales y las oportunidades de acción, tanto en espacios físicos como virtuales. Así, las variaciones culturales, socioeconómicas y tecnológicas entre regiones no solo parecen incidir en la prevalencia del *hacking* (Chen *et al*., 2023; Vergara, 2024), sino también en los factores individuales y situacionales que determinan si un delito cibernético es percibido y seleccionado como una alternativa viable de acción (Kokkalera *et al*., 2020; Vepsäläinen *et al*., 2025). En consecuencia, la comprensión de la variabilidad geográfica y cultural del ciberdelito desde la perspectiva de la TAS requiere de un mayor desarrollo de investigaciones comparadas que integren de manera explícita estos distintos niveles de análisis.

Pese a los aportes teóricos y empíricos alcanzados por este estudio, resulta pertinente reconocer una serie de limitaciones que condicionan el alcance de sus conclusiones. En primer lugar, la baja prevalencia del comportamiento de *hacking* en la muestra introduce un posible sesgo hacia estimaciones conservadoras, lo que aconseja cautela en la generalización de los hallazgos. En segundo lugar, la operacionalización y medición de los factores contextuales presentó restricciones relevantes, al haberse circunscrito, por ejemplo, a una medida indirecta del nivel de exposición criminógena asociada en este caso a rutinas y estilos de vida arriesgados en Internet. Además, este estudio no incluyó variables relativas a la asociación con amigos o compañeros que practican *hacking* porque su análisis excedía las estrategias y el alcance centrado en interacciones que caracteriza este trabajo. Sin embargo, esta dimensión, como se ha comprobado en otros estudios, tiende a influir en la exposición (véase Hardie y Rose, 2025; Pauwels *et al*., 2018). En tercer lugar, aunque el proceso situacional de percepción-elección que conecta la propensión y la exposición criminógena con la acción fue mencionado a nivel teórico, el

presente estudio no logró someter a prueba empírica los mecanismos concretos a través de los cuales dicho proceso conduce al *hacking* ilegal, lo que constituye tal vez una posible limitación. En cuarto lugar, no se realizaron análisis de sensibilidad complementarios, aunque su utilidad ha sido señalada en la literatura para evaluar la robustez de los resultados cuando la variable dependiente (medida como frecuencia) presenta asimetrías que vulneran supuestos clave de las regresiones MCO (Serrano, 2018). Finalmente, aunque se dispuso de una muestra multinacional, no fue posible realizar comparaciones entre países debido a la escasa frecuencia de casos de *hacking* en cada uno de ellos, impidiendo examinar la variabilidad de los mecanismos explicativos en función de contextos culturales, normativos o tecnológicos específicos.

En función de estas limitaciones, se sugiere que futuras investigaciones avancen hacia el diseño de medidas más sólidas y válidas para captar los principales conceptos de la TAS, así como hacia una integración más profunda entre esta teoría y las particularidades sociales y técnicas del entorno digital. Esto requiere incorporar indicadores específicos asociados al ciberespacio y a los usuarios del mismo, como, por ejemplo, la percepción de anonimato y desinhibición en línea, las habilidades y conocimientos técnicos de los cibernautas, la exposición a entornos con baja vigilancia y escasa regulación formal y la participación en comunidades o foros *online* con normas y controles propios (Palmieri *et al.*, 2021; Pérez, 2017; Smith, 2024; Suler, 2004). A su vez, incluir el efecto del comportamiento problemático en Internet de las amistades en futuros análisis puede contribuir a una comprensión más amplia de los factores que explican por qué ciertos entornos digitales favorecen el *hacking* u otras formas de ciberdelito. Asimismo, sería relevante emplear métodos mixtos que combinen técnicas cuantitativas con aproximaciones cualitativas como las entrevistas o la etnografía digital, que permitan captar motivaciones, trayectorias y narrativas de los jóvenes involucrados. También se sugiere el uso de escenarios hipotéticos o viñetas como los empleados en estudios previos (p. ej., Pauwels, 2018; Rodríguez y Birkbeck, 2017; Rodríguez *et al*., 2022), que representen situaciones moralmente complejas o controvertidas, pero en este caso en entornos digitales. Este tipo de metodología permitiría analizar con mayor precisión el

proceso de percepción-elección mediante el cual la propensión individual y la exposición situacional se convierten en acción. Por último, tal como lo recomiendan Hardie y Rose (2025) y Vepsäläinen *et al*. (2025), se invita a realizar análisis comparativos entre países o regiones continentales con el fin de evaluar cómo factores estructurales, normativos y tecnológicos modulan los efectos y procesos teorizados por la TAS.

En consonancia con la evidencia que establece el inicio del *hacking* en edades tempranas (en torno a los 12 años) y su evolución hacia formas más graves al final de la adolescencia (Lee y Holt, 2020), este comportamiento ha sido explicado en ocasiones por los investigadores desde marcos como la *Teoría General del Delito*, la *Teoría de las Actividades Rutinarias* o la *Teoría del Aprendizaje Social* (Back *et al*., 2018; Bekkers *et al*., 2025a; Bossler y Burruss, 2011; Fox y Holt, 2021; Holt *et al*., 2021; Kim *et al*., 2024; Nodeland y Morris, 2020; Savka, 2025). En comparación con estas perspectivas, concluimos que los resultados del presente estudio indican que la TAS ofrece también un cuerpo teórico sólido, más integrado y empíricamente operativo para comprender el *hacking* juvenil en entornos digitales. Al parecer, no requiere de profundas modificaciones de sus procesos causales (tal como lo propone, por ejemplo, la *SAT-RI*), aunque sí de ciertas adaptaciones como se acaba de discutir. En particular, la contrastación empírica (parcial) de la hipótesis PEA, a partir de una muestra transnacional latinoamericana, demuestra que la interacción entre la propensión individual y la exposición criminógena a contextos digitales aumenta la probabilidad de este tipo de ciberdelitos. Esta evidencia contribuye a llenar un vacío relevante en una literatura dominada por estudios europeos y norteamericanos, reforzando la validez transcultural de la TAS desde la perspectiva del ciberespacio. Además de su aportación teórica, los hallazgos subrayan la relevancia de diseñar programas de prevención que integren simultáneamente las características del cibernauta y el entorno digital, orientando intervenciones específicas hacia los perfiles individuales de riesgo y los contextos en los que dichas propensiones se activan.

Referencias bibliográficas

Aiken, M; Davidson, J; Walrave, M; Ponnet, K; Phillips, K. y Farr, R. (2024). Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. *Forensic Sciences*, *4*, 24-41.

Alruwaili, N. (2019). *A test of Situational Action Theory in Saudi Arabia*. Tesis doctoral: Universidad de Salford.

Alves, B. y Miró, F. (2024). Digital life and crime trends in the global south: on the impact of increased Internet use on opportunities for crime. *Revista Española de Investigación Criminológica*, *22*(2), e863.

Back, S; Soor, S. y LaPrade, J. (2018). Juvenile Hackers: An Empirical Test of Self- Control Theory and Social Bonding Theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, *1*(1), 40-55.

Bekkers, L; Holt, T. y Leukfeldt, E. (2025a). The psychological correlates of cybercrime offending: Exploring the self-control/social learning relationship in serious cyber-dependent crime. *European Journal of Criminology*, *0*(0).

Bekkers, L; Holt, T. y Leukfeldt, E. (2025b). Exploring the factors that differentiate individual and group offenders in cyber-dependent crime. *Journal of Criminal Justice*, *101*, 102522.

Bekkers L; Holt, T. y Leukfeldt, E. (2025c). Online gaming as a criminological environment: exploring criminogenic needs and offending behaviors of gamers. *Journal of Criminal Psychology*, *0*(0).

Botchkovar, E; Antonaccio, O; Ballou, A. y Maimon, M. (2025). Crime and calculation: The decision-making of Dark Web actors. *Computers in Human Behavior*, http://dx.doi.org/10.2139/ssrn.5232168

Bossler, A. (2021). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice*, *46*(6), 911-934.

Bossler, A. y Burruss, G. (2011). The General Theory of Crime and Computer Hacking: Low Self-Control Hackers? En T. Holt y B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 38-67). IGI Global Scientific Publishing.

Brewer, R; Cale, J; Goldsmith, A. y Holt, T. (2018). Young people, the internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology*, *12*(1), 115-132.

Carcelén, S; Márquez, O. y Vilches, M. (2025). Online Risk Behaviours Among Adolescents: Identifying Areas of Digital Vulnerability. *Children & Society*, *0*, 1-15.

Chen, S; Hao, M; Ding, F; Jiang, D; Dong, J; Zhang, S; Guo, Q. y Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & Social Sciences Communications*, *10*(1), 71-10.

Chrzanowska-Gancarz, M. (2022). The dark side of the Internet and the ontological sense of safety. *Organization & Management*, *165*, 21-31.

Chng, S; Lu, H; Kumar, A. y Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 1-8.

Choi, J. y Yun, I. (2019). Do moral beliefs condition the impact of low self-control on digital piracy? *Deviant Behavior 42*(7), 837-849.

Connolly, L; Borrion, H. y Arief, B. (2025) Ransomware crime through the lens of neutralization theory. *European Journal of Criminology*, *22*(4), 534-556.

Dolliver, D. y Love, K. (2015). Criminogenic asymmetries in cyberspace: A comparative analysis of two tor marketplaces. *Journal of Globalization Studies 6*(2), 75-96

Engström, A. (2018). Associations between risky lifestyles and involvement in violent crime during adolescence. *Victims & Offenders*, *13*(7), 898-920.

Ferrara, P; Franceschini, G; Corsello, G; Mestrovic, J; Giardino, I; Vural, M; Pop, T; Namazova-Baranova, L. y Pettoello-Mantovani, M. (2021). The Dark Side of the Web — A Risk for Children and Adolescents Challenged by Isolation during the Novel Coronavirus 2019 Pandemic. *The Journal of Pediatrics*, *228*, 324-325.

Flor-Unda, O; Simbaña, F; Larriva-Novo, X; Acuña, Á; Tipán, R. y Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America, *Informatics*, *10*(3) 1-24.

Fox, B. y Holt, T. (2021). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior*, *48*(7), 943-963. https://doi.org/10.1177/0093854820969754

Gallo, F. (2025). La cara oculta de la Dark Web. un análisis volumétrico de la presencia de masi en freenet. *Revista de Derecho Penal y Criminología*, *34*, 371-386.

Gopalsamy, M. y Dastageer, K. (2025). The role of ethical hacking and AI in proactive cyber defense: Current approaches and future perspectives. *International Journal of Innovative Science and Research Technology*, *10*(2), 482-489.

Gordon, S. y Ma, Q. (2003). *Convergence of Virus Writers and Hackers: Fact or Fantasy*. Symantec Security. Disponible en: file:///C:/Users/

ACER/Downloads/silo.tips_inside-convergence-of-virus-writers-and-hackers-fact-or-fantasy-symantec-security-response-by-sarah-gordon-symantec-security-response.pdf

Grabosky, P. (2016). The evolution of cybercrime, 2006-2016. En J. Holt (Edit.), *Cybercrime through Aninterdisciplinary Lens* (pp. 29-50). Routledge.

Grasmick, H; Tittle, C. y Bursik, R. (1993). Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency*, *30*, 5-29.

Guo, S. y Wang, Y. (2024). Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system. *Computers in Human Behavior*, 152, 108079.

Hair, J; Anderson, R; Tatham, R. y Black, W. (2008). *Análisis multivariante*. Prentice Hall.

Hardie, B. (2019). Why monitoring doesn't always matter: The interaction of personal propensity with physical and psychological parental presence in a situational explanation of adolescent offending. *Deviant Behavior, 42*(3), 329-352.

Hardie, B. y Rose, C. (2025). What next for tests of the situational model of Situational Action Theory? Recommendations from a systematic review. *European Journal of Criminology*, *22*(3), 303-345.

Hasselhorn, F; Sattler, S; Kroneberg, C. y Seddig, D. (2025). The Self-Control Ability Scale: Measuring a Key Construct of Situational Action Theory. *Justice Quarterly*, *42*(7), 1321-1348. https://doi.org/10.1080/07418825.2024.2413584

Hawdon, J; Parti, K. y Dearden, T. (2020). Cybercrime in America amid COVID 19: the initial results from a natural experiment. *American Journal of Criminal Justice*. doi: https://doi.org/10.1007/s12103-020-09534-4

Hayes, A. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. The Guilford press.

Helms, S; Choukas-Bradley, S; Widman, L; Giletta, M; Cohen, G. y Prinstein, M. (2014). Adolescents misperceive and are influenced by high-status peers' health risk behaviors. *Developmental Psychology*, *50*(12), 2697-2714. https://doi.org/10.1037/a0038178

Hirtenlehner, H. y Hardie, B. (2016). On the Conditional Relevance of Controls: An Application of Situational Action Theory to Shoplifting. *Deviant Behavior 37*(3),315-31.

Hirtenlehner, H. y Mesko, G. (2025). Crime propensity and lifestyle risk: The interplay of personal morality and self-control ability in determining the significance of criminogenic exposure. *European Journal of Criminology*, 0(0).

Hirtenlehner, H. y Treiber, K. (2017) Can situational action theory explain the gender gap in adolescent shoplifting? Results from Austria. *International Criminal Justice Review, 27*(3), 165-187.

Holt, T; Strumsky, D; Smirnova, O. y Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber* Criminology, *6*(1). 891-903.

Holt, T. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior, 139*: 107493. https://doi.org/10.1016/j.chb.2022.107493.

Holt, T; Cale, J; Brewer, R. y Goldsmith, A. (2021). Assessing the role of opportunity and low self-control in juvenile hacking. *Crime and Delinquency*, *67*(5), 662-688.

Holt, T; Navarro, J; y Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime and Delinquency*, *66*(11), 1533-1555.

Holt, T. y Steinmetz, K. (2021). Examining the role of Power-Control Theory and Self-Control to account for computer hacking. *Crime & Delinquency*, *67*(10), 1491-1512. *https://doi.org/10.1177/0011128720981892*.

Hu, S; Lei, W; Zhu, H; y Hsu, C. (2024). Cyberbullying perpetration on social media: A situational action perspective. *Information & Management*, *61*(6), 104013.

Hwang, K; Bock, G. y Kim, H. (2021). A Study of Cross-Border E-Consumers' Cunning Behavior from the Perspective of Situational Action Theory. *Asia Pacific Journal of Information Systems, 31*(4), 633-673.

Ishoy, G. y Blackwell, B. (2018). Situational Action Theory's Self-Control/Morality Interaction Effects and the Moderating Influence of Being Female: A Comparison of Property and Violent Offending Using a Sample of Juvenile Delinquents. *Feminist Criminology*, *14*(4), 391-419.

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology, 4(*1 y 2*)*, 2-31.

Kabiri, S. (2025). Hunting in the digital jungle. Exploring cyberstalking with higher order moderation in Situational Action Theory. *Journal of Criminal Justice*, *98*, 102400.

Kabiri, S. y Hosseinzadeh, M. (2025). Analysis of agency and structure in virtual platforms; Exploring cyberstalking through the lens of Situational Action Theory. *Interdisciplinary Studies in the Humanities*, *17*(2), 29-61.

Kabiri, S; Shadmanfaat, S; Samuels, K y Gallupe, O. (2020.) Does moral identity matter in situational action theory? Some evidence of Iranian fans' cyberbullying perpetration. *International Criminal Justice Review*, *30*(4), 406-420.

Kaakinen, M; Koivula, A; Savolainen, I; Sirola, A; Mikkola, M; Zych, I; Paek, H; y Oksanen, A. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. *Aggressive Behavior*, *47*(5), 530-543.

Kennedy, L. (2024). Prioritise propensity: A multi-method analysis of peer influence and school-based aggression. *Deviant Behavior, 45*(2), 139-168.

Kim, J; Leban, L. y Lee, Y. (2024). Theoretical explanations of the development of youth hacking'. *Crime & Delinquency*, *70*(8), 1971-1992.

Kokkalera, S; Marshall, C. y Marshall I. (2020). How exceptional is India? A test of situational action theory. *Asian Journal of Criminology, 15*(3), 195-218.

Kroneberg, C. y Nägel, C. (2024). When violence is not an option: Perceived choice sets and differential deterrability among adolescents in Germany. *Crime & Delinquency, 71*(9), 3128-3156.

Kshetri, N. (2013). Cybercrime and Cybersecurity in Latin American and Caribbean Economies. En Nir Kshetri (Edit.), *Cybercrime and Cybersecurity in the Global South* (pp. 135-151). Palgrave Macmillan.

Lee, B. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research, 11*(2), 563-584.

Lee, J. y Holt, T. (2020). Assessing the Factors Associated with the Detection of Juvenile Hacking Behaviors. *Frontiers in Psychology, 11*(840), 1-10.

Lee, S. y Jung, S. (2025). How Do Internal and External Control Factors Affect Cyberbullying? Partial Test of Situational Action Theory. *Behavioral Sciences*, *15*(7), 837.

Lee, S; Song, H y Park, J. (2021). Exploring Risk and Protective Factors for Cyberbullying and Their Interplay: Evidence from a Sample of South Korean College Students. *International Journal of Environmental Research and Public Health, 18*(24), 13415.

Livingstone, S. y Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-

Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

Liu, W; Qiu, G. y Zhang, S. (2020). Situational action theory and school bullying: Rethinking the moral filter. *Crime & Delinquency*, *68*(4), 572-593.

Manski, C. (1993). Identification of endogenous social effects: The reflection problem. *The Review of Economic Studies*, *60*(3), 531-542. https://doi.org/10.2307/2298123

Maras, K; Sweiry, A; Villadsen, A. y Fitzsimons, E. (2024). Cyber offending predictors and pathways in middle adolescence: Evidence from the UK Millennium Cohort Study. *Computers in Human Behavior*, *151*, 108011.

Marcum, C; Higgins, G; Ricketts, M. y Wolfe, S. (2014). Hacking in High School: Cybercrime Perpetration by Juveniles. *Deviant Behavior*, *35*(7), 581-591.

Mardia, K. (1970). Measures of multivariate skewness and kurtosis with applications. *Biometrika*, *57*(3), 519-530.

Marshall, I; Birkbeck, C; Enzmann, D; Kivivuori, J; Markina, A. y Steketee, M. (2022). *International Self-Report Delinquency (ISRD4) study protocol: Background, methodology, and mandatory items for the 2021/2022 survey.* Northeastern University.

Martineau, M; Spiridon, E. y Aiken, M. (2024). Pathways to Criminal Hacking: Connecting Lived Experiences with Theoretical Explanations. *Forensic Sciences*, *4*(4), 647-668.

McGuire, M. y Dowling, S. (2013). *Cybercrime: a review of the evidence*. Research report 75. Home Office.

Meldrum, R. C., Partin, R. D. y Lehmann, P. S. (2026). The role of criminal history, low self-control, and social learning variables in accessing the Dark Web. *Journal of Crime and Justice*, 1-28. https://doi.org/10.1080/0735648X.2026.2621153

National Crime Agency. (2024). *One in five children found to engage in illegal activity online*. 21 de Marzo. https://www.nationalcrimeagency.gov.uk/news/one-in-five-children-found-to-engage-in-illegal-activity-online

Ngo, F. y Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology*, *11*(1), 1-9.

Nodeland, B. y Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior, 41*(1), 41-56.

Noordegraaf, J. y Weulen, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*, *22*, 803-824. https://doi.org/10.1111/1745-9133.12650

Nunnally, J. y Bernstein, I. (1994). *Psychometric theory*. McGraw-Hill.

O'Brien, R. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity*, *41*(5), 673-690.

Onwuadiamu, G. (2025). Cybercrime in Criminology: A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology, 8*, 100136.

Palmieri, M; Shortland, N. y McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior, 120*, 106745.

Patchin, J. e Hinduja, S. (2018). Deterring teen bullying: Assessing the impact of perceived punishment from police, school, and parents. *Youth Violence and Juvenile Justice*, *16*(2), 190-207.

Paternoster, R; Brame, R; Mazerolle, P. y Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology*, *36*(4), 859-866.

Pauwels, L. (2018). Analysing the perception-choice process in situational action theory. A randomized scenario study. *European Journal of Criminology*, *15*(1), 130-147.

Pauwels, L; Svensson, R. y Hirtenlehner, H. (2018). Testing situational action theory: A narrative review of published studies between 2006 and 2015. *European Journal of Criminology*, *15*(1), 32-55.

Pérez, J. (2017). *We are cyborgs developing a theoretical model for understanding criminal behaviour on the Internet*. España: Criminología y Justicia.

Programa de las Naciones Unidas para el Desarrollo (PNUD). (2024, 4 de agosto). Conexiones perdidas: Una revolución digital incompleta en América Latina y el Caribe. https://www.undp.org/es/latin-america/blog/conexiones-perdidas-una-revolucion-digital-incompleta-en-america-latina-y-el-caribe

Rodríguez, J. A. y Birkbeck, C. (2017). La Teoría de la acción situacional: una prueba del proceso de percepción elección mediante la encuesta

factorial en Venezuela. *Revista de Derecho Penal y Criminología*, *18*, 265-304.

Rodríguez, J. A; Redondo, A; Belandría, J. y Garrido, N. (2022). El «filtrado moral» de la violencia física en conflictos de parejas íntimas. Una prueba parcial de la Teoría de la Acción Situacional en función del género. *Boletín Criminológico*, *28*, 1-34.

Romagna, M. y Leukfeldt, E. (2023). Becoming a hacktivist: examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime & Justice*, *47*(4), 511-529.

Romagna, M. y Leukfeldt, E. (2025). Hacktivism: From loners to formal organizations? Assessing the social organization of hacktivist networks. *Deviant Behavior*, *46*(9), 1104-1124,

Savka, A. (2025). Primary drivers for teenagers' illegal hacking, as evidenced by criminological literature from the past five years: A systematic literature review. *Essex Student Journal*, *17*(1), 1-17.

Savoia, E; Harriman, N; Su, M; Cote, T. y Shortland, N. (2021). Adolescents' Exposure to Online Risks: Gender Disparities and Vulnerabilities Related to Online Behaviors. *Journal of Environmental Research and Public Health*, *18*(11), 5786.

Schiks, J; van 't Hoff-de Goede, S. y Leukfeldt, R. (2023). An alternative intervention for juvenile hackers? A qualitative evaluation of the Hack_Right intervention. *Journal of Crime and Justice*, *47*(4), 492-510.

Schmitt, H. S; Sindermann, C. y Montag, C. (2025). Moral disengagement and low self-control make a versatile rulebreaker: A partial test of situational action theory across various manifestations of deviance. *Deviant Behavior*, *46*(12), 1551-1587.

Sela, R. (2012). Gangs and the Web: Gang members' online behavior. *Journal of Contemporary Criminal Justice*, *28*(4), 389-405.

Serrano, A. (2018). Crime contemplation and self-control: A test of Situational Action Theory's hypothesis about their interaction in crime causation. *European Journal of Criminology*. *15*(1) 93-110.

Shadmanfaat, S; Richardson D; Muniz C; Cochran; J; Kabiri, S. y Howell, J. (2020) Cyberbullying against rivals: Application of key theoretical concepts derived from Situational Action Theory. *Deviant Behavior, 44*(4), 336-355.

Shalizi, C. y Thomas, A. (2011). Homophily and contagion are generically confounded in observational social network studies. *Sociological Methods & Research, 40*(2), 211-239. https://doi.org/10.1177/0049124111404820

Sirola, A; Savolainen, I. y Oksanen, A. (2024). Who uses the dark web? Cross-national and longitudinal evidence on psychosocial, behavioral, and individual predictors. *Personality and Individual Differences, 227*, 112709.

Smith, T. (2024). Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimization in the Digital Realm. *International Journal of Cybersecurity Intelligence & Cybercrime, 7*(2), 54-70.

Solar, C. (2023). *Cybersecurity Governance in Latin America: States, Threats, and Alliances*. State University of New York Press.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, *7*(3), 321-326.

Svensson, R. y Pauwels, L. (2010). Is a Risky Lifestyle Always "Risky"? The Interaction Between Individual Propensity and Lifestyle Risk in Adolescent Offending: A Test in Two Urban Samples. *Crime & Delinquency*, *56*(4), 608-26.

Temara, S. (2024). The Dark Web and Cybercrime: Identifying Threats and Anticipating Emerging Trends. *International Journal of Advanced Engineering Research and Science (IJAERS), 11*(10) 80-93.

Tomazic, T. y Bessa, N. (2017). Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web. *Revija za kriminalistiko in kriminologijo*, *68*, 412-423.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: a cross-national study. *International Journal of Cyber Criminology*. *10*, 127-146.

Vlckova, T. y Burianek, J. (2025). The Role of Self-Control in Offline and Online Juvenile Delinquency: Insights from Czech Adolescents in the ISRD-4 Study. *Journal of Contemporary Criminal Justice*, 1-14.

Vepsäläinen, J; Kaakinen, M; Ellonen, N; Arbach, K; Bazon, M; Hazel, N; Kivivuori, J: Kokoravec, I; Langeland, C; Markina, A; Meško, G: Rodríguez, J. A; Valdimarsdóttir, M. y Oksanen, A. (2025). Cybercrime Correlates Among Adolescents in Europe and South America: A Cross-National Analysis Based on Situational Action Theory. *Journal of Contemporary Criminal Justice, 41*(4), 661-678.

Vergara, E. (2024). *Cybersecurity economics for emerging markets*. Banco Mundial. https://hdl.handle.net/10986/42130

Wall, D. (2001). Cyber crimes and the internet. En D. Wall (Ed.), *Crime and the Internet*, (pp. 1-17). Routledge.

Wikström, P-O. (2004). Crime as alternative: Towards a cross-level situation action theory of crime causation. En McCord (Ed.), *Beyond empiricism, institutions, and intentions in the study of crime* (pp. 1-37). Transaction.

Wikström P-O. (2009) Crime propensity, criminogenic exposure and crime involvement in early to mid adolescence. *Monatsschrift für Kriminologie und Strafrechtsreform* 92, 253-266.

Wikström, P-O. (2010). Explaining crime as moral actions. En S. Hitlin y S. Vaisey (Eds.), *Handbook of the Sociology of Morality* (211–239). Springer.

Wikström, P-O; Mann, R. y Hardie, B. (2018). Young people´s differential vulnerability to criminogenic exposure: Bridging the gap between people and place oriented approaches in the study of crime causation. *European Journal of Criminology*, *15*(1) 10-31.

Wikström, P-O; Oberwittler, D; Treiber, K. y Hardie, B. (2012). *Breaking Rules: The Social and Situational Dynamics of Young People's Urban Crime*. Oxford University Press.

Wikström, P-O; Treiber, K. y Roman, G. (2024). *Character, Circumstances, and Criminal Careers. Towards a Dynamic Developmental and Life-Course Criminology*. Oxford University Press.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal*, *44*, 387-399.