Comunicación para el XIV Congreso Español de Criminología

Título:
Ciberdelincuencia juvenil y Modelo del Triple Riesgo Delictivo: análisis empírico de factores personales, sociales y situacionales en jóvenes con formación tecnológica

Autores:
Abel González (Universidad a Distancia de Madrid)
Marleen Weulen Kranenbarg (Vrije Universiteit Amsterdam)

Resumen

La ciberdelincuencia de tipo dependiente representa una amenaza creciente en el panorama delictivo juvenil, caracterizada por el uso de tecnologías de la información para atacar sistemas informáticos. A pesar del incremento de estudios sobre criminalidad digital, son escasas las investigaciones centradas en los factores de riesgo que explican las trayectorias delictivas específicas en jóvenes con conocimientos técnicos. Esta comunicación aplica el Modelo del Triple Riesgo Delictivo (TRD) de Redondo (2008, 2015) a una muestra de alto riesgo (N = 725) de estudiantes en programas formativos de informática. A partir del análisis de autorreportes sobre conductas como el hacking técnico, el uso o creación de herramientas técnicas (malware, ataques DDoS) y el uso indebido del acceso no autorizado, se exploran los riesgos personales, sociales y de oportunidad asociados a cada tipo de ciberdelito. Los resultados muestran que la victimización y la pertenencia a grupos de iguales infractores son factores comunes a todas las categorías delictivas, mientras que otras variables —como el conocimiento técnico, la supervisión parental o el uso intensivo de foros y videojuegos— presentan relaciones específicas según el tipo de conducta. El estudio valida empíricamente los principios del modelo TRD y propone líneas de prevención diferenciadas para subgrupos de jóvenes ofensores en entornos digitales.

Palabras clave: ciberdelincuencia juvenil, Modelo del Triple Riesgo Delictivo, factores de riesgo, hacking, jóvenes tecnológicamente capacitados, prevención criminológica

---

Introducción

Desde los trabajos pioneros de Yar (2005), la ciberdelincuencia juvenil ha sido señalada como un fenómeno emergente con profundas implicaciones para la criminología contemporánea. A pesar de ello, las investigaciones centradas específicamente en los delitos ciberdependientes —aquellos que requieren competencias técnicas para vulnerar sistemas— han sido escasas en comparación con los delitos ciberasistidos o convencionales. Esta laguna teórica y empírica es especialmente visible en la ausencia de estudios que incorporen marcos teóricos integradores capaces de explicar el origen y evolución de estas conductas.

El presente trabajo busca contribuir al conocimiento sobre la ciberdelincuencia juvenil técnica a través del **Modelo del Triple Riesgo Delictivo (TRD)**, un enfoque meta-teórico desarrollado por Redondo (2008, 2015) que integra explicaciones sobre factores personales, sociales y situacionales. Aplicado hasta ahora en contextos principalmente presenciales, su aplicación al ámbito digital permite avanzar en la comprensión de cómo se construyen las trayectorias delictivas juveniles en entornos virtuales.

Para ello, se ha empleado una muestra de alto riesgo compuesta por **725 estudiantes de entre 12 y 25 años**, todos ellos inscritos en programas de formación en informática. La investigación se basa en la autodeclaración de conductas delictivas ciberdependientes, excluyendo prácticas básicas como el acceso por adivinación de contraseñas, para centrarse en comportamientos técnicamente avanzados: hacking sofisticado, creación y uso de malware, ataques DDoS, defacement, y manipulación o robo de datos.

El objetivo central de este estudio es doble:

1. Clasificar y analizar los factores de riesgo personales, sociales y de oportunidad asociados a distintos tipos de delitos ciberdependientes.
2. Evaluar la utilidad del modelo TRD como herramienta explicativa y predictiva en el campo de la cibercriminalidad juvenil.

Este enfoque ofrece una visión más matizada de la delincuencia cibernética técnica, permitiendo avanzar desde estrategias de prevención genéricas hacia intervenciones diferenciadas en función de las características del infractor y del tipo delictivo. A lo largo de esta comunicación se presentarán los fundamentos teóricos del modelo TRD, los métodos utilizados, los principales hallazgos empíricos y sus implicaciones teóricas y prácticas.

Marco teórico y revisión de la literatura

1. La ciberdelincuencia juvenil: una problemática emergente y diferenciada

La ciberdelincuencia juvenil ha cobrado protagonismo en las dos últimas décadas, tanto en los discursos mediáticos como en las políticas públicas. Sin embargo, desde el ámbito académico, su tratamiento ha estado frecuentemente limitado a enfoques parciales o descriptivos (Yar, 2005; Rokven et al., 2018). En particular, los **delitos ciberdependientes**, aquellos que requieren habilidades técnicas para vulnerar sistemas informáticos (hacking, desarrollo de malware, ataques DDoS), han sido frecuentemente agrupados con delitos ciberasistidos (como el acoso en línea o el sexting), impidiendo una adecuada caracterización etiológica (Virgara & Whitten, 2023).

Estudios recientes, como los de Loggen, Moneva y Leukfeldt (2023), insisten en la necesidad de disgregar estas categorías para evitar errores metodológicos y explicativos. El presente trabajo sigue esta orientación y propone una diferenciación interna dentro de la ciberdelincuencia dependiente, en función del tipo de conocimiento técnico implicado y del modo en que se articulan los factores de riesgo en los perfiles juveniles. Esta distinción se revela especialmente relevante a la hora de entender la diversidad de trayectorias delictivas en entornos digitales y sus implicaciones preventivas.

2. El Modelo del Triple Riesgo Delictivo (TRD) como marco integrador

El **Modelo del Triple Riesgo Delictivo (TRD)** fue formulado por Redondo (2008, 2015) con el objetivo de integrar, desde una perspectiva meta-teórica, distintos enfoques explicativos del comportamiento delictivo. A diferencia de modelos centrados exclusivamente en factores individuales o estructurales, el TRD parte de la interacción dinámica de tres niveles de riesgo:

- **Riesgo personal**: hace referencia a características individuales como la impulsividad, la baja empatía, la adicción, el escaso autocontrol o la precocidad del comportamiento antisocial.
- **Riesgo social**: alude a factores relacionales y de socialización, como la exposición a pares delincuentes, la desestructuración familiar, el bajo apego escolar o la escasa supervisión parental.
- **Riesgo situacional u oportunidad**: vinculado a contextos específicos que facilitan o estimulan la comisión del delito, como la disponibilidad de objetivos, la ausencia de guardianes o la exposición frecuente a entornos criminógenos.

El modelo se basa en tres principios clave:

1. **Convergencia intra-riesgo**: acumulación de factores de riesgo dentro de una misma dimensión que intensifican la probabilidad delictiva.
2. **Interacción entre niveles**: la combinación de riesgos personales y sociales genera una disposición criminógena que se actualiza cuando concurren oportunidades situacionales.
3. **Efecto mariposa criminógeno**: pequeños cambios en una dimensión pueden desencadenar efectos desproporcionados en otras, alterando el curso del desarrollo delictivo.

Este modelo ha demostrado capacidad explicativa en investigaciones sobre delincuencia juvenil tradicional (Pérez Ramírez, 2012), ciberacoso (González García, 2016), y trayectorias de desistimiento (Farrington & Piquero, 2005), pero su aplicación a la cibercriminalidad técnica juvenil sigue siendo escasa. El presente trabajo pretende contribuir a esa línea.

3. Estado actual de la investigación empírica

Diversos estudios han identificado factores asociados a la ciberdelincuencia juvenil, aunque la mayoría se centran en el hacking genérico o el uso de contraseñas adivinadas (Wissink et al., 2023), sin diferenciar niveles de sofisticación técnica. Desde la perspectiva del TRD, una revisión de estos estudios permite clasificar los hallazgos en las siguientes categorías:

- **Riesgos personales**: baja autoestima, adicción al ordenador, escaso autocontrol, fascinación por la tecnología, alto nivel de conocimiento en TIC, victimización previa y comportamientos antisociales tempranos (Loggen et al., 2023).
- **Riesgos sociales**: pertenencia a comunidades hacker, baja vinculación escolar, supervisión parental débil o ausente, desempleo juvenil y alto estatus socioeconómico (Weulen Kranenbarg et al., 2022).

- **Riesgos situacionales**: uso intensivo de videojuegos, foros de programación, ausencia de reglas parentales claras, acceso frecuente a tecnologías y entornos digitales sin vigilancia (Rokven et al., 2018).

A pesar de estas evidencias, la mayoría de estudios no han aplicado marcos teóricos integradores ni han diferenciado adecuadamente los tipos de ciberdelitos. Ello limita su capacidad predictiva y dificulta la elaboración de estrategias preventivas ajustadas. De ahí la relevancia del presente estudio, que se propone aplicar el TRD a una muestra de jóvenes con formación técnica, para identificar configuraciones de riesgo diferenciadas según el tipo de conducta ciberdelictiva.

4. Justificación del presente estudio

El estudio que aquí se presenta pretende superar tres limitaciones de la literatura previa:

1. **Falta de diferenciación interna**: no todos los ciberdelitos técnicos son iguales en términos de habilidad, motivación o patrón de riesgo. Este estudio distingue entre hacking técnico, uso de herramientas técnicas (como malware y DDoS), y uso indebido del acceso no autorizado.
2. **Ausencia de modelos teóricos sólidos**: se utiliza el TRD como marco integrador, capaz de ordenar y explicar los factores implicados en las trayectorias ciberdelictivas.
3. **Enfoque empírico con muestra de alto riesgo**: se emplea una muestra amplia (N=725) de estudiantes con formación en informática, considerados de alto riesgo, lo que mejora la validez externa y la utilidad de los resultados para intervenciones específicas.

Metodología

1. Diseño y enfoque

La presente investigación se enmarca en un diseño cuantitativo de carácter transversal, con análisis secundario de datos recogidos en el marco del proyecto internacional *Understanding Cybercriminal Behaviour among Young People*, financiado por el Home Office del Reino Unido. Se ha seguido una estrategia de análisis empírico multivariado orientada a identificar relaciones significativas entre factores de riesgo —clasificados según el Modelo del Triple Riesgo Delictivo (TRD)— y conductas ciberdependientes autorreportadas por jóvenes en formación técnica.

2. Muestra

La muestra se compone de **725 estudiantes** (26% mujeres), con edades comprendidas entre **12 y 25 años** (M = 16,62; DT = 1,99), procedentes de centros educativos con programas en **informática y tecnologías de la información**. La muestra fue seleccionada intencionalmente como grupo de alto riesgo en función de su afinidad con el ámbito tecnológico, lo que incrementa la probabilidad de exposición a oportunidades cibercriminógenas y el desarrollo de competencias técnicas asociadas a delitos ciberdependientes.

Los centros educativos participantes incluyen ocho instituciones de formación terciaria, tres escuelas de educación secundaria de nivel superior y una de nivel inferior. Todos los centros imparten formación técnica especializada en informática. La recogida de datos se realizó en dos oleadas consecutivas mediante cuestionarios autoaplicados en el aula.

3. Variables dependientes

Las **variables dependientes** se definieron a partir de las respuestas autorreportadas en la segunda oleada del estudio, focalizándose exclusivamente en conductas **ciberdependientes técnicamente sofisticadas**. Se excluyeron conductas simples como el acceso por adivinación de contraseñas.

A través de un **análisis factorial de componentes principales con rotación varimax**, se identificaron tres categorías empíricas de ciberdelitos técnicos:

- **Hacking técnico**: incluye accesos no autorizados mediante aplicaciones técnicas, exploits o inyecciones SQL.
- **Uso o creación de herramientas técnicas**: incluye ataques DDoS (propios o en colaboración) y uso o desarrollo de malware.
- **Uso indebido del acceso no autorizado**: comprende la copia ilegal de datos, vandalismo digital, manipulación de sistemas o defacement de sitios web.

Las tres categorías fueron transformadas en variables dicotómicas, codificadas como 1 si el participante reportó haber cometido al menos una de las conductas correspondientes en los últimos 4 meses, y 0 en caso contrario.

4. Variables independientes

En consonancia con el Modelo TRD, se organizaron las variables independientes en tres bloques: **riesgos personales, sociales y de oportunidad**. En la medida de lo posible, se emplearon variables de la primera oleada para evitar problemas de causalidad inversa.

a) Riesgo personal (6 variables)

- **Edad**: en años cumplidos (ola 1).
- **Adicción al ordenador**: escala de 6 ítems adaptada de la *Game Addiction Scale* (Lemmens et al., 2015), $\alpha = .74$.
- **Conocimiento técnico en TIC**: número de respuestas correctas en un test de 5 preguntas sobre competencias informáticas (ola 2).
- **Bajo autocontrol**: escala de Grasmick et al. (1993), $\alpha = .72$ (ola 2).
- **Victimización previa**: dicotómica; haber sido víctima de hackeo, malware o trampas en videojuegos (ola 2).
- **Competencia social en línea**: escala de 4 ítems adaptada de Lemmens et al. (2011), $\alpha = .81$.

b) Riesgo social (4 variables)

- **Tiempo a solas en casa**: número de horas sin supervisión un día entre semana (ola 1).
- **Satisfacción con la formación en TIC**: escala de 2 ítems, $\alpha = .71$.

- **Diálogo con docentes sobre actividades informáticas**: escala de acuerdo de 1 a 5.
- **Pares infractores**: dicotómica; tener amigos (presenciales u online) que hayan cometido conductas ciberdependientes.

c) Riesgo de oportunidad (3 variables)

- **Reglas parentales**: media de dos escalas (offline y online) sobre supervisión y normas parentales (α = .77 y .88 respectivamente).
- **Reglas escolares**: media de escalas sobre normativa y control escolar offline y online (α = .78 y .80).
- **Actividades online de riesgo**: dicotómica; pasar más de 1 h/día en foros o programación, o más de 3 h/día en videojuegos.

5. Estrategia analítica

Dado que las variables dependientes son dicotómicas, se aplicaron **modelos de regresión logística binaria**. Para cada una de las tres categorías delictivas se estimaron:

1. Un modelo por separado para cada bloque de riesgo (personal, social y de oportunidad).
2. Un modelo final con todas las variables significativas de los bloques anteriores.

La capacidad explicativa de los modelos se evaluó mediante el **pseudo R^2 de Nagelkerke** y la significación de los coeficientes se estableció con valores $p < .05$, .01 y .001.

6. Consideraciones éticas

La investigación original fue autorizada por los comités éticos correspondientes y siguió principios de consentimiento informado, anonimato y protección de datos. La presente explotación secundaria de datos se ha realizado con fines académicos, sin acceso a información identificable, y siguiendo los principios éticos del Código Deontológico de la European Society of Criminology.

Resultados

1. Prevalencia y tipologías de ciberdelincuencia técnica

Los resultados muestran que, excluyendo las conductas simples de hacking por adivinación de contraseñas, **el 36%** de los encuestados admitió haber cometido al menos un delito ciberdependiente en los cuatro meses anteriores a la encuesta. La distribución por categorías revela los siguientes niveles de prevalencia:

- **Uso indebido del acceso no autorizado**: 27,3%
- **Hacking técnico**: 17,9%
- **Uso o creación de herramientas técnicas**: 10,5%

Estos datos reflejan una importante presencia de ciberdelincuencia técnica entre jóvenes en formación tecnológica, con diferencias notables en función de la sofisticación de la conducta.

2. Riesgos personales: predictores diferenciados

Los modelos de regresión logística para **riesgos personales** indican una capacidad explicativa del 13% para el hacking técnico, del 8% para el uso de herramientas técnicas y del 8% para el uso indebido del acceso. Las principales conclusiones son:

- **Victimización previa**: predictor significativo y robusto para las tres categorías delictivas (OR > 2.0 en todos los modelos).
- **Adicción al ordenador**: asociada significativamente con el hacking técnico (OR = 2.49) y el uso indebido del acceso (OR = 1.91), pero no con el uso de herramientas técnicas.
- **Conocimiento técnico (IT-knowledge)**: se relaciona únicamente con el hacking técnico (OR = 1.50), lo que refuerza la especificidad de este comportamiento.
- **Bajo autocontrol**: únicamente significativo en el modelo de uso indebido del acceso (OR = 1.59), sugiriendo su relevancia en contextos de impulsividad y oportunidad.
- **Competencia social en línea**: débilmente relacionada con el uso indebido del acceso en el modelo aislado, pero pierde significación al controlar por otras variables.

3. Riesgos sociales: rol de la supervisión y los pares

El bloque de **riesgos sociales** explica entre el 6% y el 7% de la varianza en las conductas delictivas. Se observan patrones consistentes y específicos:

- **Pares infractores**: variable predictora clave en las tres categorías. Su presencia incrementa significativamente la probabilidad de cometer ciberdelitos, con odds ratios superiores a 2.0 en todos los modelos finales.
- **Tiempo en casa sin supervisión**: asociado exclusivamente al uso de herramientas técnicas (OR = 1.24), lo que subraya el papel del aislamiento como facilitador de conductas técnicamente ejecutadas.
- **Satisfacción con la educación en TIC** y **diálogo con docentes**: no presentan efectos estadísticamente significativos al incluirse en los modelos finales, aunque el diálogo muestra un efecto positivo marginal en el hacking técnico.

4. Riesgos de oportunidad: reglas y rutinas digitales

Los **riesgos de oportunidad** presentan un patrón menos homogéneo y más débil en comparación con los personales y sociales, con un poder explicativo que oscila entre el 3% y el 9%. Destacan:

- **Actividades online de riesgo**: asociadas significativamente con el hacking técnico (OR = 4.29) y el uso de herramientas técnicas (OR = 3.14). También aparecen en el modelo inicial de uso indebido del acceso, pero pierden significación al introducir los demás riesgos.

- **Reglas parentales**: su ausencia se relaciona negativamente con el hacking técnico (OR = 0.68), mostrando un efecto protector del control informal. No es significativa para las otras dos categorías.
- **Normativa escolar**: no presenta significación en ninguno de los modelos.

5. Modelos integrados: patrones de convergencia

Los **modelos finales integrados** muestran diferentes configuraciones de riesgo:

- **Hacking técnico**:
  - Factores personales: victimización, adicción al ordenador, conocimiento en TIC.
  - Social: pares infractores.
  - Oportunidad: actividades online de riesgo, ausencia de reglas parentales.
  - Pseudo R^2: 0.17
- **Uso o creación de herramientas técnicas**:
  - Personal: victimización.
  - Social: pares infractores, tiempo sin supervisión.
  - Oportunidad: actividades online de riesgo.
  - Pseudo R^2: 0.13
- **Uso indebido del acceso no autorizado**:
  - Personal: victimización, adicción al ordenador, bajo autocontrol.
  - Social: pares infractores.
  - Oportunidad: no significativa.
  - Pseudo R^2: 0.11

Estos hallazgos refuerzan la hipótesis de que **la combinación de factores personales y sociales tiene mayor peso explicativo** que los factores situacionales, aunque estos últimos resultan relevantes en los comportamientos más técnicos y planificados.

Análisis comparado y discusión de los resultados

1. Confirmación de factores comunes: victimización y pares infractores

Uno de los hallazgos más robustos del presente estudio es la **consistencia de dos predictores** a lo largo de las tres categorías de ciberdelito técnico: la **victimización previa** y la **pertenencia a grupos de iguales infractores**. Este patrón sugiere una **dinámica circular** entre victimización y delincuencia, tal como ha sido descrito en el marco de la criminología del desarrollo (Farrington, 2019).

En el caso de los jóvenes tecnológicamente capacitados, la **victimización digital** (por hackeos, trampas en videojuegos o malware) puede constituir una experiencia que genera aprendizaje, curiosidad o incluso motivación para ejercer represalias, en línea con el fenómeno del retaliatory hacking (Loggen et al., 2023). Esta observación refuerza la hipótesis de que, en el ciberespacio, las fronteras entre víctima y victimario son particularmente porosas, y la experiencia de victimización puede convertirse en un **precursor del comportamiento ofensivo**.

Por otro lado, la **influencia de los pares infractores**, tanto presenciales como virtuales, constituye una evidencia sólida del papel de la socialización en entornos técnicos. Esta relación concuerda con los postulados de la **Teoría del Aprendizaje Social** (Akers, 1998) y también con estudios previos sobre comunidades hacker juveniles, que actúan como espacios de legitimación, entrenamiento y transmisión de conocimientos (Steinmetz, 2015).

2. Diferencias según tipo delictivo: perfiles y trayectorias diferenciadas

El análisis comparado permite distinguir patrones específicos para cada categoría delictiva:

- El **hacking técnico** aparece vinculado a un perfil de alta especialización: jóvenes con **conocimientos TIC elevados**, **adicción al ordenador** y **hábitos digitales intensivos**, pero también con cierto grado de control sobre su conducta (el autocontrol no resulta significativo). La relevancia de variables como las **reglas parentales** o la ausencia de supervisión **sugiere que estas conductas requieren tiempo, planificación y oportunidad**, es decir, un entorno permisivo donde el joven pueda operar sin restricciones.
- En el caso del **uso o creación de herramientas técnicas**, como el malware o los ataques DDoS, el perfil es **más instrumental y situacional**. Aquí no se detecta asociación con la adicción o el conocimiento técnico elevado, lo que sugiere que estos comportamientos podrían apoyarse en herramientas prefabricadas o de fácil acceso. En cambio, destaca la influencia del **aislamiento físico (tiempo a solas)** y la **exposición a pares**, lo cual remite a escenarios donde **la falta de vigilancia y la presión grupal** actúan como desencadenantes.
- El **uso indebido del acceso no autorizado** se relaciona significativamente con **bajo autocontrol**, **adicción al ordenador** y **victimización**, pero **no con actividades digitales complejas ni con conocimiento técnico avanzado**. Este perfil apunta a una conducta **más impulsiva**, posiblemente reactiva, en la que el acceso no autorizado constituye una oportunidad casual más que una acción planificada. Esta categoría se asemeja a la **delincuencia oportunista**, donde el control inhibitorio y la motivación emocional juegan un papel clave.

3. Evaluación del Modelo del Triple Riesgo Delictivo (TRD)

La aplicación del TRD al ámbito de la ciberdelincuencia técnica juvenil permite extraer varias conclusiones relevantes:

- El principio de **convergencia intra-riesgo** se confirma, especialmente en el caso del hacking técnico, donde la combinación de varios factores personales (victimización, adicción, conocimientos TIC) incrementa notablemente la probabilidad de infracción.
- La **interacción inter-riesgo** también se evidencia: en los tres modelos finales aparecen al menos una variable personal y una social como predictores significativos, mientras que las situacionales refuerzan su efecto en las tipologías más técnicas. Esta dinámica sugiere que **la activación del comportamiento delictivo requiere una conjunción de condiciones personales, sociales y contextuales**.

- El principio del **efecto mariposa criminógeno** también se vislumbra en la forma en que pequeños cambios —por ejemplo, una menor supervisión o el acceso a foros técnicos— pueden desencadenar procesos de aprendizaje desviados y trayectorias delictivas sostenidas.

Así, el TRD demuestra una notable **capacidad integradora**, permitiendo ordenar empíricamente los hallazgos en un marco que incluye postulados de teorías clásicas como el autocontrol, el aprendizaje social y las rutinas delictivas, pero con una articulación dinámica.

4. Implicaciones criminológicas y preventivas

El presente estudio plantea importantes implicaciones para la prevención y la intervención en jóvenes tecnológicamente capacitados:

- Es fundamental diferenciar entre **subtipos de infractores cibernéticos**, ya que no todos responden a los mismos factores ni presentan las mismas trayectorias. La aplicación de programas universales sería ineficaz frente a la heterogeneidad detectada.
- Para el **hacking técnico**, las estrategias deben centrarse en la canalización de habilidades técnicas hacia usos prosociales (p. ej., formación en ciberseguridad, competencias éticas, gamificación con retos legales). Este enfoque coincide con experiencias exitosas de **redireccionamiento de talentos**.
- Para quienes hacen **uso de herramientas técnicas**, es clave actuar sobre el **entorno social y la supervisión familiar**, promoviendo la mediación parental, el control digital razonable y el fortalecimiento de competencias familiares sobre entornos tecnológicos.
- En el caso del **uso indebido del acceso**, las intervenciones deben priorizar el desarrollo del **autocontrol, la empatía y la capacidad de detener conductas impulsivas**, junto con el monitoreo de la victimización.
- A nivel general, se recomienda el **diseño de programas preventivos basados en el TRD**, que combinen formación en habilidades socioemocionales, fortalecimiento del control informal y construcción de entornos digitales seguros.

Conclusiones, limitaciones y líneas futuras

1. Conclusiones generales

El presente estudio proporciona evidencia empírica relevante sobre la **estructura de factores de riesgo asociados a la ciberdelincuencia juvenil técnicamente especializada**, aplicando el Modelo del Triple Riesgo Delictivo (TRD) como marco teórico integrador. A partir de una muestra de alto riesgo compuesta por 725 estudiantes con formación en TIC, se ha demostrado que:

- La **victimización previa** y la **exposición a pares infractores** son predictores comunes y robustos en las tres tipologías delictivas.
- Existen **perfiles diferenciados** en función del tipo de conducta ciberdependiente: el hacking técnico responde a un patrón de especialización, el

uso de herramientas técnicas se vincula al aislamiento y la presión grupal, y el uso indebido del acceso parece más impulsivo y reactivo.
- El **TRD** permite organizar, explicar y comparar estas configuraciones de riesgo, mostrando un notable poder explicativo sin necesidad de recurrir a modelos exclusivos del mundo digital.

Estos hallazgos respaldan la idea de que la ciberdelincuencia juvenil, lejos de ser un fenómeno homogéneo o exclusivamente técnico, **responde a dinámicas personales, sociales y situacionales complejas**, que requieren un abordaje diferenciado y basado en la evidencia.

2. Limitaciones metodológicas

A pesar de sus aportes, este estudio presenta varias limitaciones:

- El uso de **datos autorreportados** puede dar lugar a sesgos de memoria, deseabilidad social o minimización del comportamiento delictivo.
- El diseño es **transversal**, lo que impide establecer relaciones causales firmes. Aunque se intentó mitigar este riesgo utilizando variables de la primera oleada, no puede descartarse bidireccionalidad.
- Las **variables de oportunidad** se midieron de forma indirecta y limitada. Faltan indicadores más específicos sobre la exposición a redes de distribución de herramientas delictivas, condiciones técnicas de acceso o dinámicas de anonimato digital.
- La muestra, aunque relevante, **no es representativa del conjunto de jóvenes**, sino de un segmento de alto riesgo. Esto mejora la validez interna pero reduce la generalización a poblaciones no técnicas.

3. Propuestas para futuras investigaciones

Con base en los resultados y limitaciones señaladas, se proponen las siguientes líneas de investigación futura:

- **Estudios longitudinales** que permitan observar la evolución de los factores de riesgo y su interacción en el tiempo, siguiendo las trayectorias desde la experimentación hasta la desistencia.
- Incorporación de **técnicas mixtas** que combinen cuestionarios con entrevistas, análisis de redes sociales o estudios etnográficos en comunidades digitales.
- Diseño de **medidas más precisas de oportunidad**, considerando el tipo de acceso a herramientas, la naturaleza del entorno online, el tiempo de permanencia y los sistemas de anonimato utilizados.
- Investigaciones comparadas entre **diferentes perfiles de jóvenes infractores** (técnicos, no técnicos, híbridos) y entre **delitos ciberdependientes y ciberasistidos**, para explorar similitudes y divergencias desde el TRD.
- Análisis del impacto de variables como el **género, la identidad digital, la ideología o las motivaciones morales**, factores apenas explorados en el ámbito de la cibercriminalidad juvenil.

4. Implicaciones para la criminología y la prevención

Desde un punto de vista académico y aplicado, este estudio plantea varias implicaciones:

- Refuerza la validez del TRD como modelo útil para abordar no solo la criminalidad convencional, sino también las formas emergentes de delincuencia tecnológica.
- Invita a la criminología a **no desanclarse del factor humano**, incluso en contextos hiperconectados. Las decisiones delictivas en el ciberespacio siguen estando mediatizadas por la socialización, la personalidad, los contextos de oportunidad y las emociones.
- Requiere adaptar los programas preventivos y de intervención desde una **perspectiva segmentada y ecológica**, ajustada a los perfiles de riesgo detectados.
- Abre la posibilidad de desarrollar **programas específicos de redireccionamiento prosocial de habilidades tecnológicas** en contextos educativos, con enfoque preventivo y restaurativo.

- econocidas.

Referencias

1. Farrington, D. P. (2019). *The development of violence from age 8 to 61*. *Aggressive Behavior, 45*(4), 365–376. https://doi.org/10.1002/ab.21831
2. González García, A. (2016). Factores de riesgo en el ciberacoso: revisión sistemática a partir del modelo del triple riesgo delictivo (TRD). En J. M. Tamarit (Coord.), *Ciberdelincuencia y cibervictimización*. *Revista de Internet, Derecho y Política, 22*, 73–92.
3. Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378–395. https://doi.org/10.1007/s12103-011-9117-3
4. Lemmens, J. S., Valkenburg, P. M., & Gentile, D. A. (2015). The Internet Gaming Disorder Scale. *Psychological Assessment, 27*(2), 567–582. https://doi.org/10.1037/pas0000062
5. Loggen, R. J., Moneva, A., & Leukfeldt, R. (2023). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *PsyArXiv*. https://doi.org/10.31219/osf.io/ztfdw
6. Pérez Ramírez, M. (2012). *Riesgos personales, sociales y ambientales en la explicación del comportamiento antisocial: estudio empírico sobre el Modelo del Triple Riesgo Delictivo*. [Tesis doctoral, Universidad de Barcelona].
7. Redondo, S. (2008). Individuos, sociedades y oportunidades en la explicación y prevención del delito: modelo del Triple Riesgo Delictivo (TRD). *Revista Española de Investigación Criminológica, 6*. https://doi.org/10.46381/reic.v6i0.34
8. Redondo, S. (2015). *El origen de los delitos*. Tirant lo Blanch.
9. Rokven, J. J., Weijters, G., Beerthuizen, M., & van der Laan, A. M. (2018). Juvenile delinquency in the virtual world: Similarities and differences between

cyber-enabled, cyber-dependent and offline delinquents in the Netherlands. *International Journal of Cyber Criminology, 12*(1), 231–248. https://doi.org/10.5281/zenodo.1467690

10. Weulen Kranenbarg, M., Van der Toolen, Y., & Weerman, F. M. (2022). *Understanding cybercriminal behaviour among young people: Results from a longitudinal network study among a relatively high-risk sample*. Vrije Universiteit Amsterdam. https://research.vu.nl/en/publications/understanding-cybercriminal-behaviour-among-young-people