
A

Más allá de lo técnico: la criminología como eje indispensable en la comprensión y prevención del cibercrimen

Beyond the technical: criminology as an indispensable axis in understanding and preventing cybercrime

Carlos Avendaño[1]

Resumen

El presente artículo analiza la necesidad de una formación interdisciplinaria en materia de cibercrimen, argumentamos que el enfoque tecnocrático dominante (centrado casi exclusivamente en aspectos técnicos de la ciberseguridad) resulta insuficiente para comprender y prevenir el delito informático contemporáneo. A través de una revisión teórica y un diagnóstico de la situación formativa en la región, se discute la perspectiva predominantemente técnica y se destacan aportes clave desde la criminología como ciencia social. En particular, se examinan los marcos teóricos y enfoques analíticos de la criminología cultural, la criminología cyborg y la cibercriminología, evidenciando cómo estas perspectivas amplían la comprensión del cibercrimen al incorporar dimensiones sociales, culturales y humanas usualmente ignoradas. El estudio se basa en la revisión de la literatura académica y documentos de política educativa. Los resultados revelan vacíos importantes en la formación profesional en ciberseguridad desde

1. Magister en Criminología. Universidad

un punto de vista social y crítico. Por ejemplo: escasa atención a las motivaciones y comportamientos de los ciberdelincuentes, o a las implicaciones sociales de los delitos informáticos, así como una marcada desconexión entre las disciplinas tecnológicas y las ciencias sociales. En la discusión se proponen orientaciones para una agenda de formación interdisciplinaria que integre contenidos de criminología, sociología, psicología y ética en los programas de ciberseguridad, con el objetivo de formar profesionales capaces de abordar el cibercrimen de manera holística. Se concluye enfatizando que superar el enfoque técnico dominante e incorporar la perspectiva criminológica y sociocultural no solo enriquecerá la comprensión, investigación y respuesta al cibercrimen en América Latina.

Palabras clave: Cibercrimen, Interdisciplinariedad, Criminología cultural, Criminología cyborg, Cibercriminología, Formación profesional, Enfoque técnico.

Abstract

This article analyzes the need for interdisciplinary training in the field of cybercrime, arguing that the dominant technocratic approach (focused almost exclusively on the technical aspects of cybersecurity) is insufficient to understand and prevent contemporary cybercrime. Through a theoretical review and an assessment of the current state of training in the region, the predominantly technical perspective is discussed, and key contributions from criminology as a social science are highlighted. In particular, the theoretical frameworks and analytical approaches of cultural criminology, cyborg criminology, and cybercriminology are examined, showing how these perspectives broaden the understanding of cybercrime by incorporating social, cultural, and human dimensions that are often overlooked. The study is based on a review of academic literature and educational policy documents. The results reveal significant gaps in professional cybersecurity training from a social and critical standpoint. For example: limited attention to the motiva-

tions and behaviors of cybercriminals, or to the social implications of cybercrime, as well as a marked disconnection between technological disciplines and the social sciences. The discussion proposes guidelines for an interdisciplinary training agenda that integrates content from criminology, sociology, psychology, and ethics into cybersecurity programs, with the goal of preparing professionals capable of addressing cybercrime in a holistic manner. The conclusion emphasizes that overcoming the dominant technical approach and incorporating criminological and sociocultural perspectives will not only enrich the understanding, research, and response to cybercrime in Latin America.

Keywords: *Cybercrime, Interdisciplinarity, Cultural Criminology, Cyborg Criminology, Cybercriminology, Professional Training, Technical Approach.*

Introducción

En las últimas décadas, el auge de las tecnologías digitales ha generado un incremento sostenido de los delitos informáticos a nivel global. América Latina no escapa a esta tendencia: cada vez más actividades delictivas se cometen a través de internet, planteando nuevos desafíos para la seguridad pública y la justicia penal (López Gorostidi, 2022). Históricamente, la respuesta institucional y formativa frente al delito informático ha estado dominada por un enfoque tecnocrático, es decir, por perspectivas centradas principalmente en los aspectos técnicos de la ciberseguridad (infraestructura digital, criptografía, ingeniería de sistemas, etc.). En la práctica, ello se traduce en que la mayoría de los programas académicos y capacitaciones profesionales relacionados con el cibercrimen han enfatizado la formación en informática y tecnología, prestando comparativamente poca atención a las dimensiones humanas y sociales del fenómeno (Chen et al., 2023). Si bien las competencias técnicas son imprescindibles para prevenir y contrarrestar ataques[2], existe el riesgo de reducir el problema del cibercrimen a una mera cuestión tecnológica, dejando de lado preguntas fundamentales: ¿Quiénes son los ciberdelincuentes cuáles son sus motiva-

2. Por ejemplo: el fortalecimiento de cortafuegos, el software de seguridad y la pericia forense digital.

ciones? ¿Qué subculturas o dinámicas sociales favorecen ciertas conductas ilícitas en línea? ¿Cómo influye el contexto sociocultural en la definición de qué es delito en el mundo digital? Estas interrogantes, y otras, remiten a un campo de conocimientos que trasciende lo técnico y se adentra en lo social y criminológico.

Diversos autores han señalado que las amenazas a la seguridad ciudadana en el ciberespacio son múltiples y aún poco estudiadas desde una perspectiva social (K.-S. Choi & Toro-Álvarez, 2017). Mientras los delitos informáticos aumentan, la acción policial y la capacidad de investigación en la esfera digital permanecen rezagadas, y solo una fracción de los cibercrímenes llega a ser detectado o reportada a las autoridades (K.-S. Choi & Toro-Álvarez, 2017). En paralelo, la investigación académica sobre delitos cibernéticos ha sido limitada en comparación con la dedicada a la delincuencia tradicional (K.-S. Choi & Toro-Álvarez, 2017). Esto ha generado brechas significativas entre lo que sabemos y lo que ignoramos a cerca de los delincuentes informáticos. En otras palabras, enfrentamos un fenómeno criminal en rápida evolución, pero carecemos de marcos teóricos y evidencia empírica robusta para comprenderlo y abordarlo de manera integral. Ante esta realidad, diversos especialistas proponen expandir el enfoque analítico más allá de lo técnico, incorporando métodos y teorías de las ciencias sociales, particularmente de la criminología, entendida como la ciencia que estudia el crimen en sus causas, dinámicas y controles, al estudio del cibercrimen (Chen et al., 2023).

Este artículo se enmarca en dicha discusión y busca construir un estado del arte crítico sobre la formación en cibercrimen, enfatizando la necesidad de superar el modelo tecnocrático dominante. En concreto, se argumenta que la perspectiva criminológica con su bagaje teórico sobre comportamientos desviados, contextos culturales, motivaciones de los ofensores y estructuras de control social, es indispensable para enriquecer la comprensión y la prevención del delito informático. Para sustentar esta tesis, en la sección teórica se presentan tres corrientes emergentes de la criminología que ofrecen valiosos aportes en el contexto digital: la criminología cultural, la criminología cyborg y la cibercriminología. Cada una de ellas aporta marcos conceptuales y enfoques analíticos innovado-

res para analizar fenómenos como la piratería informática, el ciberacoso, el fraude en línea o la delincuencia organizada en la red; todas convergen en destacar que el **factor humano-cultural** es tan importante como el tecnológico a la hora de entender el cibercrimen (Yar, 2018). Posteriormente, se describe la metodología empleada para diagnosticar las vacancias en la formación profesional vigente en materia de ciberseguridad, con especial foco en América Latina. A continuación, en la sección de resultados, se exponen hallazgos sobre las deficiencias formativas desde la perspectiva social y crítica. Por ejemplo: planes de estudio que relegan contenidos de ciencias sociales, o profesionales de seguridad con escaso conocimiento en criminología y comportamiento delictivo. En la discusión, se analizan las implicaciones de dichos hallazgos y se proponen lineamientos para una agenda de formación interdisciplinaria capaz de responder a los desafíos complejos del cibercrimen contemporáneo en la región. Finalmente, las conclusiones sintetizan los argumentos y resaltan la urgencia de una aproximación integradora en la enseñanza y práctica de la ciberseguridad.

Teorización: aportes criminológicos al estudio del cibercrimen

Limitaciones del enfoque técnico dominante

Antes de adentrarnos en las corrientes criminológicas, conviene explicar por qué el enfoque tecnicista actual resulta limitado. Bajo el paradigma tecnocrático, el cibercrimen se concibe primordialmente como un problema de vulnerabilidades informáticas y de ausencia de controles tecnológicos adecuados. En consecuencia, la solución suele buscarse mediante más y mejor tecnología: firewalls más avanzados, algoritmos criptográficos más robustos, herramientas de monitoreo y respuesta a incidentes, etc. Si bien estas medidas son esenciales, numerosos analistas señalan que no podemos abordar eficazmente el fenómeno criminal en línea sin entender también a las personas involucradas (delincuentes y victimas) y el entorno social en que operan (Chen et al., 2023). Por ejemplo, muchos ataques ci-

bernéticos explotan el llamado "factor humano" mediante **ingeniería social** (engaños, phishing, manipulación psicológica), algo que escapa a las meras soluciones técnicas. Del mismo modo, el surgimiento de comunidades de ciberdelincuentes y mercados ilegales en la "dark web" responde a dinámicas de grupo, valores culturales y redes de confianza entre delincuentes, aspectos que difícilmente se comprenden solo desde la óptica de la informática.

En la literatura especializada se reconoce cada vez más que el cibercrimen es un fenómeno complejo y multidimensional, que requiere un enfoque integral. Por ello, diversos campos (desde la psicología hasta la sociología, pasando por el derecho y la ciencia política) aportan piezas importantes del rompecabezas (Chen et al., 2023). La criminología, en particular, ofrece un marco teórico sobre el comportamiento delictivo y sus causas inherentes a complejas relaciones sociales. Así, mientras la informática y la ingeniería de seguridad enseñan cómo proteger un sistema, la criminología ayuda a comprender por qué alguien lo ataca, cómo evoluciona una carrera criminal en línea y qué factores socioculturales influyen en esas conductas. Como señala Giever (2018), ya no tenemos el lujo de mantener barreras entre los expertos en TI y los especialistas en seguridad ciudadana: es imprescindible un enfoque "balanceado" que aproveche todas las disciplinas pertinentes (Giever, 2018). Esta visión integrada permitirá diseñar tácticas y estrategias de prevención y protección más completas. Por ejemplo, se pueden combinar medidas técnicas con programas de educación digital para potenciales víctimas, o realizar intervenciones sociales dirigidas a poblaciones en riesgo de delinquir en línea.

Desde una perspectiva crítica, el predominio histórico del enfoque técnico refleja también cierta **"visión reduccionista"** del delito informático, a veces concebido simplemente como una traslación de delitos tradicionales al medio digital. Durante mucho tiempo, la respuesta académica fue aplicar teorías criminológicas clásicas al nuevo entorno sin cuestionar si este introducía cambios cualitativos. Se asumía que teorías como la actividad rutinaria, el control social o la asociación diferencial podrían explicar la ciberdelincuencia igual que explican robos o fraudes convencionales (Arroyo, 2020). En efecto, se han utilizado modelos tradicionales para abordar el

cibercrimen como la teoría de las actividades rutinarias, usada para entender la convergencia en tiempo y espacio de delincuentes motivados, víctimas apropiadas y ausencia de eficaces guardianes o protectores en entornos digitales (Miró Llinares, 2011). Estas aplicaciones han sido útiles hasta cierto punto. Sin embargo, varios autores señalan que el ciberespacio posee características únicas, como la anonimidad, la desinhibición online, la atemporalidad y la ausencia de fronteras físicas, que desafían supuestos de las teorías convencionales. Por ello, además de adaptar teorías existentes, han emergido nuevos enfoques criminológicos específicos para el entorno digital. A continuación, se presentan tres de estos enfoques: la criminología cultural, la criminología cyborg y la cibercriminología. Cada uno de ellos aporta una lente particular para analizar el cibercrimen y, a la vez, todos coinciden en subrayar la importancia de factores no técnicos (culturales, identitarios, socioeconómicos, etc.) en el fenómeno delictivo de internet.

Criminología Cultural y cibercultura del crimen

La criminología cultural es una rama de la criminología crítica que estudia el crimen considerando su dimensión de creación de significado, su relación con la cultura y los símbolos, y las emociones que rodean tanto las conductas desviadas como el control social. Surgida en los años 1990 con autores como Jeff Ferrell, Keith J. Hayward y Jock Young, esta perspectiva enfatiza que el delito no puede separarse de los valores culturales, las subculturas y las representaciones mediáticas. En el contexto del cibercrimen, la criminología cultural ofrece un marco invaluable para entender, por ejemplo, la subcultura hacker, las comunidades de crakers, o fenómenos como el "trolleo" y la toxicidad en línea, donde la transgresión adquiere significados lúdicos o contestartarios. (Avendaño et al., 2025; López Gorostidi, 2022)

Hayward (2012), uno de los referentes de esta corriente, invita explícitamente a utilizar la criminología cultural para explicar el comportamiento de los delincuentes en el ciberespacio (López Gorostidi, 2022). En su trabajo sobre las "cinco espacialidades de la criminología cultural", Hayward intro-

duce conceptos como convergencia y telepresencia aplicados al cibercrimen (López Gorostidi, 2022). La convergencia alude por un lado, a la convergencia tecnológica o unificación de plataformas de comunicación que facilitan nuevos delitos, y por otro, a la convergencia de actores en línea, delincuentes y víctimas que nunca se encontrarán en el mundo físico, pero coinciden virtualmente (Hayward, 2012). La telepresencia, por su parte, se refiere a la capacidad de estar "presentes" en lugares lejanos mediante medios digitales, lo cual expande el alcance de ciertas conductas delictivas (por ejemplo, un abusador puede acosar a víctimas en otros países en tiempo real, o un delincuente informático penetrar sistemas remotos) (Hayward, 2012). Estas nociones ponen de relieve la dimensión espacial y simbólica del cibercrimen: Internet crea espacios sociales nuevos donde las reglas tradicionales se difuminan, permitiendo interacciones criminales mediadas por avatares, identidades ficticias y contextos virtuales. La criminología cultural propone analizar esos espacios no solo en términos técnicos, sino entendiendo las prácticas culturales que allí emergen.

Un aporte concreto de la criminología cultural es considerar el cibercrimen como aporte de la vida diaria digital y de las culturas juveniles contemporáneas. Majid Yar (2018) argumenta que hasta ahora ha habido poca aplicación concretada de los conceptos de la criminología cultural al estudio del crimen en internet, y a su vez la propia criminología cultural no ha reflexionado suficiente sobre cómo las nuevas formas de comunicación en línea transforman la cultura (Yar, 2018). Este autor aboga por un dialogo más estrecho entre criminología cultural y "cibercriminología", de modo que la primera se adapte a la realidad electrónicamente mediada por la vida social contemporánea, y la segunda incorpore la importancia de la producción y consumo de significados en moldear el delito en línea (Yar, 2018). Por ejemplo, comprender qué significado encuentran ciertos jóvenes en realizar actos de hacking ¿es una forma de rebeldía, de juego, de construcción más efectivas que solo mejorar la seguridad del sistema? La criminología cultural sugiere usar métodos cualitativos (como la etnografía digital, la observación participante en foros o la netnografía) para adentrarse en la cibercultura del delito y captar las narrativas y símbolos que la rodean (Conescrim, 2025).

Desde la perspectiva formativa nos podemos preguntar ¿qué implica integrar la criminología cultural en la enseñanza sobre cibercrimen? La respuesta es clara, en primer lugar, incorporar contenidos que aborden el crimen como fenómeno cultural: teorías de la construcción social del delito, estudios de subculturas delincuenciales, análisis de los medios digitales y su rol en amplificar miedos o glorificar ciertas conductas (piénsese en la figura del hacker justiciero de la ficción). También fomentar en los estudios habilidades de análisis cualitativo e interdisciplinario. Por ejemplo: interpretar discursos en redes sociales, entender la estética y jerga de comunidades "underground online", para complementar sus habilidades técnicas. La criminología cultural aporta una mirada holística que vincula el cibercrimen con las dinámicas culturales de la sociedad red, y su integración en la formación puede producir profesionales más conscientes del contexto sociocultural en el que operan los delincuentes y víctimas digitales.

Criminología cyborg: repensando la intersección humano-tecnología

Otro enfoque innovador es la llamada criminología cyborg, propuesta por Jorge Ramiro Pérez (Pérez Suárez, 2017). El término cyborg evoca la fusión del humano y máquina; aplicado a la criminología, implica estudiar el delito en un mundo donde la frontera entre lo humano y lo tecnológico es cada vez más difusa. Este paradigma parte de la premisa de que la revolución digital ha transformado profundamente nuestras interacciones sociales, nuestra identidad e incluso nuestras conductas, creando una nueva ecología del delito. La criminología cyborg busca ampliar el horizonte disciplinar incorporando una visión verdaderamente socio-técnica del crimen, tomando elementos de la antropología, la filosofía de la tecnología y la teoría crítica.

Según Pérez Suárez (2017), los postulados iniciales de una criminología cyborg serán los siguientes: a) una criminología que considere el impacto de las tecnologías digitales en todas las facetas del comportamiento

humano, estudiando la relación emocional que se forja entre personas y la tecnología (especialmente Internet); b) una criminología que examine las nuevas formas de delito creadas por la proliferación de la tecnología y la interfaz hombre/maquina, así como conductas desviadas o actitudes disfuncionales asociadas (adicción a la red, obsesión, fenómenos de desigualdad como la brecha digital de género, desviaciones sexuales en línea, conductas patológicas, suicidios vinculados al mundo virtual, etc.); c) una criminología que incorpore un discurso antropológico, filosófico, social, psicológico, sexual, crítico y cultural sobre nuestra relación con las máquinas, y d) una criminología orientada a desarrollar y probar teorías específicamente criminológicas para explicar el cibercrimen dentro de este nuevo marco (Pérez Suárez, 2017). La criminología cyborg propone representar al crimen considerando al ser humano como un ente híbrido inmerso en entornos tecnológicos, donde las herramientas digitales son extensiones de la agencia humana.

Este enfoque se inspira en ideas posmodernas como las de Donna Haraway (1984), quien en su "Manifiesto Cyborg" sostuvo que las distinciones rígidas entre humano, máquina y organismo se habían borrado en la sociedad contemporánea (Pérez Suárez, 2017). Aplicado al delito, ello sugiere que problemas que antes considerábamos puramente "sociales" ahora deben entenderse en un continuum socio-técnico. Por ejemplo: la personalidad de un ciberdelincuente podría analizarse considerando cómo interactúa con los medios digitales: ¿le proporciona Internet una suerte de máscara o "avatar" que libera comportamientos antisociales que no manifestaría cara a cara? ¿le genera la conectividad permanente una desensibilización hacia las víctimas? ¿Cómo influye la arquitectura criminógena de la red (estructuras como la dark web, la posibilidad de anonimato, la criptografía) en facilitar u obstaculizar ciertas conductas? La criminología cyborg estudia estas cuestiones, proponiendo que incluso la mera exposición a internet puede ser criminógena en sí misma esto es, que estar inmerso en lo digital modifica la propensión del individuo al delito (Pérez Suárez, 2017).

Al integrar múltiples enfoques provenientes de diversas disciplinas como la antropología, la filosofía y otras, desafía la segmentación tradicional del conocimiento en la formación profesional. Adoptar esta pers-

pectiva requiere preparar a los futuros expertos en ciberseguridad para que desarrollen una comprensión que trascienda lo meramente técnico. Esto implica incluir en su formación contenidos como la filosofía de la tecnología, con debates éticos sobre la inteligencia artificial y la vigilancia, la psicología digital, centrada en los impactos cognitivos y conductuales del uso intensivo de pantallas, la antropología digital, que analiza la transformación de las comunidades humanas en contextos virtuales, y los estudios de género y tecnología, particularmente relevantes para examinar fenómenos como la sextorsión o el acoso en línea. La idea es formar profesionales que comprendan al "usuario" no solo como un elemento a proteger en términos de ciberseguridad, sino como un ser humano complejo cuyas interacciones con las tecnologías pueden dar lugar a nuevas formas de riesgo y de delito.

Un ejemplo concreto donde la perspectiva cyborg resulta útil es el fenómeno de la ciberdelincuencia ligada a patologías y adicciones. Mientras el abordaje tradicional podría clasificar ciertos comportamientos (como la producción de malware por diversión, o el doxing) simplemente como adicción a internet, alteraciones en la empatía mediadas por la pantalla, o la creación de identidades virtuales desconectadas de la responsabilidad social. Entender estos factores puede influir en cómo se estructuran los programas de rehabilitación de ciberdelincuentes o las campañas de concientización en el uso sano de la tecnología.

Podemos decir que la criminología cyborg expande el análisis del cibercrimen al terreno de la interacción humano-tecnología, proponiendo un enfoque verdaderamente interdisciplinario. Su inclusión en el estado del arte refuerza la argumentación de este artículo: para enfrentar el delito cibernético contemporáneo, debemos formar expertos capaces de navegar tanto las complejidades técnicas como las humanas, conscientes de que en el mundo digital "la máquina es parte de nosotros" y, por ende, la solución al crimen digital también debe integrar a la máquina en la ecuación social del delito (Pérez Suárez, 2017).

Cibercriminología: integración de criminología y tecnología

El tercer enfoque a discutir, es la cibercriminología o criminología cibernética, entendida como una especialización de la criminología enfocada específicamente en los delitos cometidos en el ciberespacio. A diferencia de la criminología cultural o cyborg (que supone marcos teóricos particulares), la cibercriminología se plantea más bien como un campo interdisciplinario en sí mismo, que aplica métodos ciminológicos al estudio de la delincuencia informática. Algunos autores la definen como la convergencia entre criminología e informática, abarcando tanto la prevención y estudio de los delitos en línea como la comprensión de las formas en que la tecnología afecta la conducta delictiva. K. Jaishanka (2011), uno de los pioneros en delimitar este campo, la describe como la ciencia que estudia la ciberdelincuencia y el comportamiento delictivo en el ciberespacio, para comprender su etiología, desarrollar teorías específicas y proponer medidas de prevención y control (Jaishankar, 2011).

La necesidad de la cibercriminología surge, como se mencionó, de las lagunas en la comprensión del fenómeno que dejaron las aproximaciones tradicionales. Los académicos reconocen que el accionar policial en el ciberespacio ha sido insuficiente, que pocas víctimas denuncian los ataques informáticos, y que la población general subestima el impacto de los ciberdelitos (K.-S. Choi & Toro-Álvarez, 2017). Esta situación dificulta construir lo que algunos llaman la "ecuación del crimen" en el mundo digital, pues faltan datos y teorías sólidas sobre cómo, por qué y quiénes cometen delitos en línea. La cibercriminología viene a llenar ese vacío, sistematizando el estudio del modus operandi de los ciberdelincuentes, sus perfiles, las motivaciones y los factores situacionales que facilitan los delitos en entornos virtuales.

Una contribución importante de la cibercriminología ha sido adaptar y probar teorías criminológicas en el nuevo dominio digital. Al ser un campo nuevo, inicialmente muchos investigadores recurrieron a teorías del mun-

do físico para explicar los delitos en el ciberespacio (Arroyo, 2020). Entre las más utilizadas se encontraron la teoría del aprendizaje social, la del control social, la teoría general de la tensión, la teoría de los vínculos sociales, la teoría de la disuasión y la teoría de las actividades rutinarias (TAR) (Arroyo, 2020; Garrido, 2012). Estas teorías aportaron ciertas claves: por ejemplo, la TAR sugiere que la ocurrencia de un delito requiere de la convergencia en tiempo y espacio de un ofensor motivado, una víctima adecuada y la ausencia de guardianes eficaces; al trasladar esto al ciberespacio, se analizaron situaciones como usuarios desprotegidos (sin antivirus, sin educación digital) que son "presas fáciles" para delincuentes motivados en ausencia de regulaciones o vigilancia (guardianes) en línea. Sin embargo, también se identificó la necesidad de teorías nativas del entorno digital. Jaishankar (2008) propuso la Teoría de la Transacción Espacial (Space Transtition theory), que postula que personas que son conformistas en el espacio físico pueden exhibir comportamientos delictivos en el ciberespacio debido a la flexibilidad de identidad, anonimato y ausencia de disuasión efectiva en línea. Aunque esta teoría ha generado debate, representa un esfuerzo por explicar fenómenos propios de Internet, como por qué individuos "comunes" incurren en discursos de odio o piratería cuando están tras pantalla.

La cibercriminología también enfatiza el uso de metodologías empíricas para obtener datos sobre ciberdelito. Por ejemplo: estudios victimológicos mediante encuestas en línea para estimar la cifra oculta de ciertos delitos (como el ciberacoso o las estafas amorosas en "dating apps"), análisis de redes sociales para mapear redes de ciberdelincuencia organizada, y experimentos en laboratorios de seguridad para observar comportamientos ante señuelos digitales. Al aplicar estas metodologías, se han podido identificar patrones y factores causales de las desviaciones en el ciberespacio (K. Choi, 2015), información con la cual los académicos pueden sugerir políticas públicas y estrategias preventivas informadas por evidencia.

En términos formativos, la cibercriminología se plasma en programas académicos que combinan cursos de informática, seguridad de la información y derecho penal con cursos de criminología, justicia criminal y ciencias forenses digitales. Un ejemplo fuera de América Latina es la carrera de "Cyber Criminology" ofrecida por la universidad Estatal de Florida (FSU),

donde el plan de estudios entrelaza asignaturas de ciencia computacional (programación, redes, técnicas de hacking ético) con asignaturas de criminología (teorías del delito, justicia penal, métodos de investigación social). Del mismo modo universidades en México, Colombia y Brasil han desarrollado programas focalizados en ciberseguridad y análisis de delitos digitales. No obstante, su orientación sigue siendo predominantemente técnica, sin integrar desarrollos teóricos recientes de la criminología, ni perspectivas críticas sobre criminalización digital, privacidad y derechos humanos en el ciberespacio.

En Argentina se encuentra la Licenciatura en Criminología y Ciberdelitos (UADE), un programa pionero en la región que se define como una ciencia multidisciplinaria para formar profesionales especializados en prevención, ciberseguridad, evidencia digital y evaluación de conductas delictivas, combinando competencias de seguridad informática con conocimientos de criminología y ciencias forenses (UADE, s. f.). Estos esfuerzos académicos responden precisamente a la demanda de expertos híbridos, capaces de "hablar el idioma" tanto de los ingenieros de sistemas como de los operadores de justicia criminal.

A nivel de posgrado en Argentina podemos mencionar a la Especialización en Seguridad Informática – Universidad de Buenos Aires (UBA): centrada exclusivamente en aspectos técnicos de protección de sistemas y redes. Carece de formación en criminología, prevención de delitos o análisis del comportamiento criminal en entornos digitales, lo cual limita su alcance interdisciplinario. En segundo lugar, la Maestría en Ciberseguridad y Redes – Universidad Nacional de La Plata (UNLP) y Maestría en Ciberdefensa y Seguridad – Universidad de Buenos Aires (UBA): orientadas principalmente al ámbito técnico-militar y a la protección de infraestructuras críticas, sin integración de marcos criminológicos ni análisis de las dinámicas sociales y jurídicas del cibercrimen. De igual modo a la Especialización en Seguridad Informática – Universidad Nacional de la Defensa (UNDEF): ofrece una sólida formación técnica en defensa informática, pero sin un enfoque preventivo ni incorporación de perspectivas criminológicas contemporáneas.

La cibercriminología representa la institucionalización de un abordaje interdisciplinario del delito informático. Sus marcos teóricos van desde la adaptación de modelos clásicos hasta la creación de teorías nuevas, y sus propuestas formativas abogan por derribar las barreras entre facultades de computación, derecho y ciencias sociales. El reconocimiento de la cibercriminología como campo legítimo es un indicador claro de que la académica está respondiendo a la necesidad de comprender el cibercrimen de manera integral. Para América Latina, donde el desarrollo de programas especializados apenas comienza, la adopción de este enfoque podría acelerar la formación de talento humano capaz de enfrentar con mayor eficacia los desafíos emergentes en el programa delictivo digital.

Tabla 1.

Enfoques criminológicos para el estudio del cibercrimen.

Enfoque	Definición	Aportes clave	Ejemplo de aplicación
Criminología Cultural	Estudia el crimen como fenómeno cultural, analizando significados, símbolos y emociones en contextos digitales.	- Análisis de subculturas hacker - Significado social del ciberdelito - Estética de la transgresión digital	Análisis de memes como vehículo de ciberacoso
Criminología Cyborg	Examina la fusión humano-tecnológica y su impacto en el comportamiento delictivo.	- Efectos psicológicos de la mediación tecnológica - Adicciones digitales y delito - Identidades virtuales	Perfilamiento de stalkers digitales
Cibercriminología	Campo interdisciplinario que aplica métodos criminológicos al estudio específico del delito digital.	- Teorías adaptadas al ciberespacio - Metodologías de investigación digital - Perfiles criminales en línea	Investigación de redes de fraude en darkweb

Fuente: Elaboración propia basada en Yar (2018), Pérez Suárez (2017) y Jaishankar (2011)

Metodología

El presente estudio adopta un enfoque cualitativo y exploratorio, centrado en la revisión documental y el análisis crítico de fuentes secundarias (Marín, 2004). Se llevó a cabo una búsqueda exhaustiva de literatura académica tanto en inglés como en español relacionada con la intersección entre cibercrimen, criminología y educación. Dado el interés en enfoques interdisciplinarios y críticos, se puso especial atención en publicaciones recientes que abordan las limitaciones de los planteamientos tradicionales y propusieran marcos teóricos innovadores, como la criminología cultural, cyborg o cibercriminología. Asimismo, se revisaron informes institucionales y planes de estudio relevantes en el contexto latinoamericano para diagnosticar el estado actual de la información en ciberseguridad/cibercrimen.

La metodología se estructuró en dos fases principales:

- **Fase 1: revisión teórica y construcción del estado del arte.** En esta etapa se analizaron textos clave para cada una de las perspectivas criminológicas identificadas. Por ejemplo, para criminología cultural se revisó literatura de criminología crítica y estudios sobre cibercultura del delito; para criminología cyborg, se consultaron trabajos fundacionales (incluyendo la tesis doctoral de Pérez Suárez y escritos derivados); para cibercriminología, se revisaron artículos que definieran el campo y exploran teóricos, conceptos y enfoques analíticos de dichas corrientes, sirviendo de base para la sección de teorización del artículo. También se extrajeron de estas fuentes las propuestas formativas o implicaciones educativas que sugerían, cuando las hubiera, con el fin de incorporarlas a la discusión.

- **Fase 2: Diagnóstico de la formación profesional en cibercrimen/ciberseguridad.** Se recopilaron datos sobre programas académicos existentes en América Latina relacionando si incluían componentes interdisciplinarios. Esto se hizo mediante la revisión de planes

de estudio publicados en sitios web universitarios por ejemplo: el plan de la Licenciatura en Criminología y Ciberdelitos de la UADE, o la Maestría en Ciberseguridad propuesta por el BID-UC3M (Nowersztern et al., 2021). Adicionalmente, se consultaron informes de organismos regionales (como el Banco Interamericano de Desarrollo y la Organización de los Estados Americanos) sobre la brecha de talento en ciberseguridad y recomendaciones de capacitación, buscando referencias a la necesidad de habilidades no técnicas. En esta fase también se incluyó el análisis de literatura gris-blogs especializados, artículos de opinión de expertos latinos- que comentaran la situación formativa o la praxis de la seguridad digital desde un enfoque social [por ejemplo, entradas como "La ciberdelincuencia desde una perspectiva multidisciplinar y social"(*La ciberdelincuencia desde una perspectiva multidisciplinar y social*, 2024)]

No se realizaron encuestas ni entrevistas directas debido a la naturaleza exploratoria y el alcance regional del estudio. En su lugar, el diagnóstico se basó en comparar la información documental recopilada con los planeamientos teóricos identificados en la fase 1, para detectar brechas o alineamientos.

El análisis de la información se efectuó mediante técnicas de análisis de contenido cualitativo. Se elaboró una matriz donde se volcaron, por un lado, las categorías teóricas derivadas de las perspectivas criminológicas como la importancia de factores culturales, necesidad de enfoque socio-técnico, relevancia de teorías específicas, entre otras; y, por otro lado, las observaciones sobre currículos y políticas formativas en América Latina como la presencia/ausencia de cursos de criminología, interdisciplinariedad declarada en la misión de los programas. Esto permitió identificar patrones, tales como la recurrente ausencia de ciertos contenidos en los planes de estudio o la presencia de iniciativas aisladas que se alinean con la agenda interdisciplinaria propuesta.

La metodología combinó la revisión bibliográfica crítica con el análisis documental de casos y políticas educativas. Si bien la dependencia de la información disponible públicamente y la subjetividad en la interpretación, resulta adecuado para el objetivo del trabajo: generar una síntesis argu-

mentativa y fundamentada que sirva de base para propuestas de mejora curricular. Los hallazgos de esta metodología se presentan en la siguiente sección.

Resultados: Vacancias en la formación profesional y desconexiones disciplinares

Del análisis realizado emergen evidencias claras de vacancias en la formación profesional en materia de cibercrimen/ciberseguridad, particularmente en lo referente a la incorporación de perspectivas sociales y criminológicas en América Latina. A continuación, se sintetizan los resultados en torno a tres ejes: a) la prevalencia de un currículo técnico y la escasa presencia de contenidos de ciencias sociales en programas de ciberseguridad; b) la separación institucional entre disciplinas, es decir carreras de informática vs criminología, y la falta de espacios de convergencia; c) las implicaciones de estas brechas en la práctica profesional y en la capacidad de respuesta al cibercrimen en la región.

Currículos dominados por lo técnico

La revisión de planes de estudio universitarios y cursos de capacitación en Latinoamérica muestra que, salvo contadas excepciones, los programas dedicados a seguridad informática, ciberdefensa o ciberseguridad ponen un énfasis casi excluyente en competencias técnicas, pero no incluyen explícitamente cursos sobre criminología, psicología del delincuente o sociología del crimen. De hecho, la incorporación de módulos legales se justifica en muchos programas como una forma de tener una "visión global, no exclusivamente técnica" de la ciberseguridad (Nowersztern et al., 2021), lo que sugiere que inicialmente incluso la dimensión jurídica estaba subrepresentada. En muchos casos, los únicos contenidos "no técnicos" en estos programas son los referidos a legislación (delitos informáticos

tipificados en el código penal, regulación de evidencia digital) un componente importante, sin duda, pero que por sí solo no cubre la comprensión socio-criminológica del fenómeno. En contraste, los programas de criminología y criminalística tradicionales en la región apenas comienzan a incluir unidades sobre ciberdelito, y cuando lo hacen suelen limitarse a la descripción de tipos penales o a nociones básicas de informática, sin profundizar en metodologías de investigación digital.

Esta situación redunda en que los graduados en ciberseguridad carecen de formación para analizar el comportamiento delictivo, mientras que los graduados en criminologías jurídicas carecen de competencias técnicas para entender cómo se comete el delito en la práctica digital. Un ejemplo paradigmático es el de las fuerzas policiales: los especialistas en delitos informáticos suelen provenir de la rama de ingeniería o informática forense, dominan las herramientas de análisis de evidencia digital pero no necesariamente han recibido instrucción en teorías criminológicas que les ayuden, por ejemplo: a perfilar a un ciberagresor sexual o a entender dinámicas de bandas de ciberdelincuentes. Por el contrario, investigadores o peritos con background en criminología pueden tener entrenamiento en perfilación criminal, pero si no comprenden conceptos técnicos (como funcionamiento de malware, enrutamiento de redes, blockchain, etc.) les será difícil aplicar sus conocimientos al mundo digital. Esta dicotomía apareció reflejada en varios documentos consultados: por ejemplo, Giever (2018) subraya que durante demasiado tiempo se han mantenido barreras entre los encargados de la seguridad IT y los encargados de la seguridad física/tradicional, lo cual obstaculiza la protección integral de los activos y la persecución efectiva del delito (Giever, 2018)

Fragmentación disciplinar e institucional

Los resultados indican que la estructura institucional académica en la región suele replicar la separación entre campos, con escasas instancias de convergencia. Las facultades o departamentos de computación tratan el tema de seguridad desde una óptica de ingeniería, mientras que las facul-

tades de ciencias sociales o derecho pueden ofrecer alguna materia electiva sobre "criminalidad informática" sin mayor profundidad técnica. Esta fragmentación se refleja también en la disponibilidad de fuentes y datos: no se identificaron fácilmente estudios empíricos latinoamericanos que combinen datos técnicos con variables sociocriminológicas en el análisis del cibercrimen (como sí ocurre en otros contextos donde surgen equipos de investigación multidisciplinarios. Un hallazgo relevante fue la identificación de programas pioneros de corte interdisciplinario, pero que son aún excepcionales. Además del mencionado programa de UADE en Argentina (UADE, s. f.), destaca la creación de diplomados o certificaciones conjuntas entre instituciones tecnológicas y policiales (por ejemplo, cursos en convenio entre universidades tecnológicas y ministerios de seguridad), de igual manera las propuestas de posgrado. Sin embargo, estos suelen enfocarse en capacitación técnica de fuerzas del orden juristas, más que en formar tecnólogos con perspectiva social.

La encuesta de necesidades conducida por el BID antes de elaborar su programa de maestría reveló que la mayoría de universidades latinoamericanas priorizaba contenidos técnicos por encima de otros, y solo una minoría destacó la necesidad de incluir aspectos organizacionales o humanos en la curricula. Aunque esa maestría incorpora un módulo de "Concienciación y formación" y otro de "Marco legal y ciberdelitos", dichos módulos complementarios son limitados en horas respecto al núcleo duro técnico. Esto ilustra la mentalidad imperante: se reconoce la importancia de lo interdisciplinario en el discurso, pero la práctica curricular queda relegado a algunos complementos.

Un aspecto adicional de la desconexión disciplinar es la falta de investigación aplicada desde las ciencias sociales al fenómeno del cibercrimen en el contexto latinoamericano. Los resultados de la revisión bibliográfica muestran que la mayor parte de las teorías y modelos criminológicos para internet provienen de académicos de Norteamérica, Europa o Asia. En Latinoamérica, la producción criminológica ha tratado en volcarse al escenario digital, concentrándose tradicionalmente en delitos convencionales (violencia, narcotráfico, etc.). Esto genera un vacío de referentes teóricos locales y posiblemente de contenido en los programas educativos: los docentes pueden no contar con suficiente literatura en español o con

estudios de casos regionales para enseñar sobre cibercrimen desde un ángulo social. No obstante, se observan señales de cambio: por ejemplo, la publicación de libros como "El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio" (Miró Llinares, 2012) abrió camino en el debate hispano; la Revista Criminología y Sociedad en países como México ha dedicado números al tema; y eventos académicos recientes incluyen simposios sobre cibercriminología. Estos desarrollos, aunque incipientes podrían alimentar mejoras curriculares en el futuro.

Implicaciones de los vacíos formativos

Las consecuencias de esta situación se manifiestan en distintos niveles. Desde el punto de vista de la política pública y la estrategia de seguridad, la falta de especialistas con visión interdisciplinaria dificulta la elaboración de planes integrales contra el cibercrimen. Por ejemplo, un país puede invertir en actualizar sus infraestructuras y equipo de ciberseguridad (lo técnico) pero descuidar la capacidad de fiscales, jueces y policías en la comprensión de las dinámicas del ciberespacio o en la atención adecuada a víctimas de delitos en línea. De hecho, informes regionales señalan que Latinoamérica muestra rezagos en capacidades institucionales frente al cibercrimen; la posición de la mayoría de países en índices globales de ciberseguridad es intermedia o baja (Nowersztern et al., 2021), en parte debido a brechas en formación y coordinación.

En el terreno operativo, entrevistados indirectos (a través de análisis de testimonios en prensa y foros profesionales) apuntan a problemas como: investigaciones que fracasan por desconocimiento de patrones criminales (más allá de la pura evidencia técnica), iniciativas de prevención que no logran convocar a la ciudadanía por no considerar factores culturales (por ejemplo, campañas anti-phishing que no se adaptan a la idiosincrasia local), o iniciativas legales que carecen de sustento empírico sobre el comportamiento de los delincuentes informáticos. Un ejemplo concreto observado es la proliferación de estafas cibernéticas aprovechando la pandemia de COVID-19; muchos países de la región reaccionaron con alertas

técnicas, pero pocos emprendieron estudios sobre el perfil sociopsicológico de los estafadores o sobre por qué ciertas poblaciones cayeron más en los engaños. Información que sería valiosa para afinar las respuestas educativas.

Por otro lado, a nivel educativo, los estudiantes y profesionales en formación parecen percibir la necesidad de complementar su perfil. En algunos programas de ingeniería en sistemas se ha empezado a recomendar a los alumnos tomar cursos electivos de ciencias sociales, y viceversa, estudiantes de criminología muestran interés en certificaciones técnicas. No obstante, esta autointegración depende en gran medida de iniciativas personales. La falta de una ruta formativa establecida que combine ambos mundos puede desalentar a quienes ven la intersección: por ejemplo, un estudiante de criminología que quisiera especializarse en cibercrimen encuentra pocas opciones de posgrado en la región para hacerlo (podría optar por criminología tradicional, o por seguridad informática, pero no algo que las una, salvo contadas excepciones), las propuestas que hay priorizan perfiles técnicos. Esta ausencia de oferta formativa estructurada fue confirmada al no hallarse programas de maestría en cibercriminología en universidades latinoamericanas a diferencia de Europa o EEUU. Donde ya existen incluso Grados en Criminología con especialidad en Ciberdelincuencia (ESDEG, s. f.).

Se evidencia un desfase entre el modelo formativo imperante y las necesidades reales para enfrentar el cibercrimen. El currículo sigue dominado por lo técnico; las estructuras académicas reflejan silos disciplinares; y ello redunda en profesionales parcial o insuficientemente equipados para comprender integralmente el fenómeno. Esta brecha formativa constituye en sí misma un riesgo, pues mientras la delincuencia evoluciona rápidamente, la capacitación de quienes deben combatirla lo hace a un ritmo más lento y fragmentado. La siguiente sección discutirá cómo encarar estas deficiencias y propondrá lineamientos para reconducir la formación hacia un paradigma verdaderamente interdisciplinario y crítico, aprovechando las perspectivas teóricas exploradas anteriormente.

Discusión: Hacia una agenda de formación interdisciplinaria en cibercrimen

Los hallazgos anteriores plantean un panorama desafiante, pero al mismo tiempo iluminan áreas de oportunidad claras para reorientar la formación en cibercrimen. La discusión se centrará en dos aspectos: primero, la relevancia de integrar las perspectivas criminológicas (cultural, cyborg, cibercriminología) en la práctica formativa y profesional, evidenciando los beneficios que ello traería al campo; segundo, propuestas concretas para una agenda educativa interdisciplinaria, adaptada al contexto latinoamericano, que subsane los vacíos identificados y potencie la respuesta regional al delito informático.

Integración de perspectivas criminológicas: del dicho al hecho

A lo largo del artículo se ha argumentado teóricamente a favor de incluir visiones de criminología cultural, cyborg y cibercriminología en el abordaje del cibercrimen. Aquí conviene traducir esas ideas al terreno práctico de la formación y el desempeño profesional. ¿Qué ganarían los especialistas en seguridad digital al incorporar estas ópticas? ¿cómo se vería reflejado en su labor cotidiana?, y a la inversa, ¿qué aportan estas perspectivas a la criminología general desde la experiencia del ciberespacio?

Enfoque cultural en la práctica: imaginemos a un analista de ciberseguridad encargado de diseñar una campaña corporativa para concientizar a empleados sobre riesgos de phishing. Con una orientación puramente técnica, probablemente se limitaría a explicar los mecanismos del phishing y las recomendaciones de no clicar enlaces sospechosos. Con una perspectiva cultural, ese analista podría enriquecer la campaña entendiendo

las narrativas que usan los atacantes (por ejemplo, aprovechar épocas de aguinaldo con temas de bonos, o temores comunes como el de perder la cuenta bancaria) y las vulnerabilidades culturales (tendencia a confiar en correos institucionales, etc.). Podría segmentar el mensaje según subculturas dentro de la organización (no es lo mismo concienciar a personal de TI que al área administrativa) y emplear símbolos e historias relevantes para cada grupo. Haría una prevención más eficaz al resonar con la realidad social del público objetivo. A escala macro, incluir la criminología cultural en políticas públicas implicaría considerar cómo fenómenos como los pánicos morales en torno al cibercrimen pueden influir en la legislación, o cómo ciertas representaciones mediáticas del "hacker malo" versus el "hacker justiciero" afectan la percepción pública y la colaboración con autoridades. Profesionales formados con esta lente estarían mejor preparados para navegar esas dinámicas simbólicas.

Enfoque cyborg en la práctica: Considérese ahora un investigador policial trabajando un caso de ciberacoso (cyberbullying) entre adolescentes. Más allá de recolectar evidencia digital, un agente con formación en criminología cyborg entendería que el acoso en línea no es simplemente una réplica virtual del acoso escolar tradicional, sino que tiene peculiaridades: la persistencia del acoso (27/7 el joven no puede refugiarse en casa), la amplificación por audiencia invisible (otros pueden unirse anónimamente), la posible desinhibición de los ofensores al no ver directamente el daño causado, etc. Integraría conocimientos de psicología sobre el efecto de la mediación tecnológica en la empatía, y sabría que la víctima experimenta esa agresión en espacios (redes sociales, chats) que forman parte integral de su identidad juvenil. Por tanto, propondría medidas de intervención que combine lo tecnológico (por ejemplo, moderación algorítmica, bloqueo de cuentas agresoras) con lo psicosocial (terapia tanto para la víctima como para los agresores, involucrando a padres y docentes en ambos mundos, físico y digital). Así, el profesional cyborg actúa en ambos frentes, entendiendo que la realidad virtual es realidad en términos de consecuencias. Este mismo razonamiento se puede aplicar a casos como ciberdelitos con motivaciones emocionales (celos que derivan en espionaje digital a la pare-

ja, etc.), donde lo importante es ver la continuidad entre la conducta offline y online más que separarlas.

Enfoque de cibercriminología en la práctica: Finalmente, pensemos en un analista de inteligencia financiera investigando movimientos sospechosos relacionados con fraude electrónico. Un perfil técnico quizás se enfocaría en seguir la pista del dinero y las herramientas usadas (malware de troyano bancario, transferencia a cuentas mulas, etc.) Un análisis con formación en cibercriminología además se haría preguntas como: ¿Está este fraude vinculado a alguna red criminal organizada trasnacional? ¿Qué patrones de comportamiento muestran los defraudadores en casos similares? ¿Existen "comunidades de aprendizaje" delictivo (foros clandestinos) de donde pudo surgir esta modalidad de ataque? Por ejemplo, podría reconocer modus operandi repetidos que apuntan a un mismo actor, cruzar datos reconocer modus operandi repetidos que apuntan a un mismo actor, o cruzar datos con información criminológica ¿los perpetradores en países X suelen reclutar cómplices jóvenes desempleados para actuar como intermediarios? Este conocimiento integrado le permitiría colaborar mejor con sociólogos o criminólogos en la elaboración de perfiles de grupos criminales y con ingenieros en cómo interrumpir técnicamente sus operaciones. Es la materialización del "equipo interdisciplinario" que Giver sugería: expertos de TI, de negocios, de criminología trabajando juntos con un lenguaje común (Giever, 2018).

Las perspectivas criminológicas aportan profundidad contextual a la labor contra el cibercrimen. Los profesionales ya no actúan a ciegas respecto al quién y por qué del delito, sino que integran esa comprensión a sus estrategias. Esto redunda en soluciones más robustas: prevención focalizada, investigación más astuta, sanciones y rehabilitación más adecuadas. Además, desde el lado de la criminología, incorporar estas experiencias tecnológicas enriquece la disciplina, obligándola a innovar teorías (como se hizo con la transición espacial, etc.) y actualizar metodologías como el uso del Big Data en estudios del crimen, la etnografía digital, entre otros. En el fondo, se trata de derribar el mito de que lo "virtual" es un terreno ajeno a las ciencias sociales: lo virtual es profundamente social. Integrar criminología en cibercrimen es un reconocimiento de ese hecho.

Propuesta para una agenda formativa integradora

A partir de lo discutido, es posible delinear una serie de recomendaciones concretas para avanzar hacia una formación interdisciplinaria en cibercrimen. Estas propuestas están pensadas principalmente para el contexto latinoamericano, considerando sus estructuras académicas y desafíos particulares, pero pueden tener relevancia más amplia. Se organizan en torno a: a) nivel curricular con respecto al diseño de programas y contenidos, b) nivel pedagógico, es decir, métodos de enseñanza-aprendizaje, y c) nivel institucional y de política pública con alianzas, certificaciones y marcos de referencia.

A) Reformulación curricular y contenidos: se propone que universidades e instituciones de formación incorporen itinerarios interdisciplinarios en sus ofertas educativas. Por ejemplo, en las carreras de informática o ingeniería en sistemas, crear concentraciones o minors en criminología/ciencias sociales aplicadas a la ciberseguridad. Esto implicaría introducir asignaturas como: Sociología del Ciberespacio, Criminología del Cibercrimen, Psicología del Comportamiento Online, Ciberdelitos y Derecho Penal, Ética y Tecnología, entro otras. Estas materias deben impartirse con rigor equivalente a las técnicas, idealmente con docentes provenientes de las ciencias sociales (posiblemente co-titulares por facultades de criminología o humanidades). De igual manera, en las carreras de criminología o derecho penal, incluir cursos de Fundamentos de Seguridad de la Información, Tecnologías emergentes y delitos, Investigación forense digital y talleres prácticos donde los estudiantes aprendan. Por ejemplo, cómo se recolectan y analizan evidencias electrónicas. Para los programas de postgrado, se sugiere la creación de maestrías especializadas en cibercriminología. Estas podrían estructurarse con un núcleo común (mitad de materias en seguridad informática, mitad en criminología y derecho), complementando con seminarios avanzados que integren ambos campos (estudios de caso integrales, laboratorios de ciberinvestigación simulada). La experiencia de

FSU en EE.UU. puede servir de modelo, adaptando los contenidos a las problemáticas locales por ejemplo: énfasis en delitos prevalentes en LATAM como fraudes financieros, ataques a infraestructuras críticas, etc.

Un componente clave del currículo integrado debe ser el aprendizaje basado en problemas reales, donde los estudiantes de distintas disciplinas trabajen juntos. Se puede implementar laboratorios o clínicas de cibercrimen en las universidades, en que equipos mixtos (estudiantes de computación, de criminología, de derecho) analicen conjuntamente un escenario. Por ejemplo: un ejercicio en el que simulan la investigación de un delito informático de principio a fin, desde la detección técnica del incidente hasta la identificación del sospechoso, pasando por el análisis de su motivación y la preparación de casos para juicio. Estas experiencias rompen la barrera mental entre campos y preparan a los alumnos para colaborar en su vida profesional.

B) Enfoques pedagógicos interdisciplinarios: más allá de qué enseña, es importante cómo se enseña. Promover la interdisciplinariedad significa también fomentar ciertas habilidades transversales. Se deben desarrollar en los estudiantes competencias de comunicación entre disciplinas: por ejemplo, que un ingeniero pueda explicar un concepto técnico en términos comprensibles para un abogado, y que un criminólogo pueda interpretar un informe técnico básico. Esto se logra incorporando actividades como debates interdisciplinarios en clase (un estudiante defiende la perspectiva técnica y otro la social sobre un mismo problema), proyectos de investigación tutelados por dos profesores de diferentes áreas, e incluso intercambios o rotaciones cortas por cursos de la otra disciplina.

Asimismo, la pedagogía debe incentivar el pensamiento crítico y ético frente a la tecnología. Los docentes podrían usar casos controversiales (como dilemas de privacidad vs vigilancia, o debates sobre la responsabilidad de redes sociales en delitos de odio) para que los estudiantes analicen no solo la solución técnica/legal sino las implicaciones morales y sociales. Esto entrena la sensibilidad necesaria para abordar la ciberseguridad de forma humanista. En la literatura se insiste en que la criminología crítica

exhorta a cuestionar las estructuras de poder y los discursos dominantes (Conescrim, 2025); trasladado a la educación, implica animar a los futuros profesionales a cuestionar, por ejemplo, si ciertas políticas de ciberseguridad podrían lesionar derechos, o si las narrativas tecnológicas ocultan exclusiones sociales.

Otro aspecto pedagógico es la actualización constante. Dado que el cibercrimen evoluciona rápidamente, los programas deben revisarse con mayor frecuencia que otras disciplinas tradicionales. Se sugiere establecer comités curriculares inter-facultades que se reúnan anualmente para incorporar novedades (tanto tecnológicas como criminológicas). Por ejemplo, en años recientes han cobrado importancia fenómenos como la desinformación en línea y la manipulación de redes sociales con fines delictivos (fraudes políticos etc.); estos temas deben encontrar cabida en cursos nuevos o módulos dentro de cursos existentes, para que los graduados salgan preparados en las fronteras emergentes del cibercrimen.

C) Institucionalización y políticas de apoyo: Para implementar cambios de esta envergadura, se requiere voluntad institucional. Una recomendación es que las universidades establezcan convenios de colaboración entre facultades de distintas áreas para codesarrollar programas. Por ejemplo: una alianza entre una Facultad de Ingeniería y una de Ciencias Sociales para ofertar conjuntamente un diplomado en "Cibercriminalidad y Sociedad". Esto facilita compartir recursos, profesores atraer un público variado. También se aconseja vincular actores extremos: agencias de gobierno, unidades de delitos informáticos de la policía, empresas de ciberseguridad y ONGs de derechos digitales. Su participación en consejos consultivos puede orientar los contenidos hacia necesidades reales y ofrecer plazas de prácticas profesionales interdisciplinarias (por ejemplo, que un estudiante de criminología realice pasantías en un CERT -Equipo de Respuestas a Emergencias Informáticas- o que uno de informática pase un tiempo en un observatorio de violencia digital de una ONG).

A nivel de políticas públicas educativas, organismos regionales como la OEA o el BID podrían desempeñar un papel catalizador. Así como han impulsado la creación de redes académicas en ciberseguridad (Red Cibe-

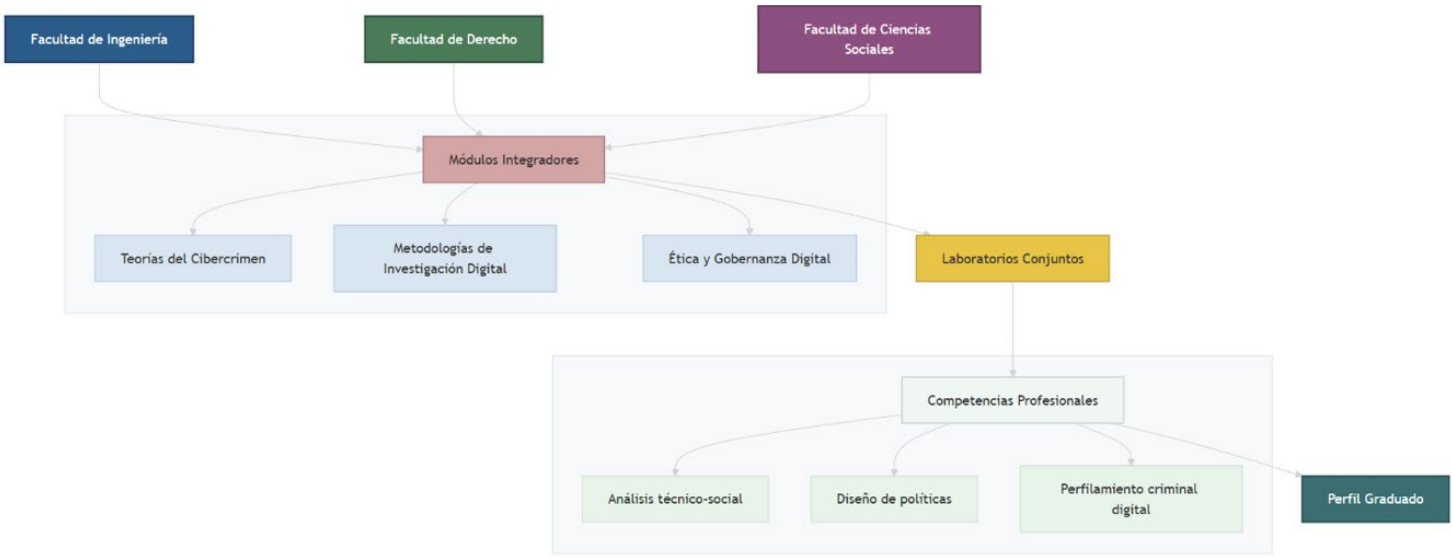
rreducación o Ciberlac) (Paz et al., 2023), podrían promover la integración de módulos sociales en estándares de competencias. Por ejemplo, que las certificaciones profesionales internacionales (tipo CISSP, CISM) incluyan en sus dominios de conocimiento principios básicos de criminología y comportamiento, o la creación de una certificación nueva en Cybercrime Analysis con enfoque interdisciplinario. Otra idea es desarrollar recursos educativos abiertos específicos: tal vez inspirados por el éxito del programa de maestría abierta BID-UC3M, se podría elaborar un complemento sobre criminología del cibercrimen de uso libre, que universidades de la región puedan adoptar para enriquecer sus cursos técnicos.

Dese la perspectiva del mercado laboral, señalemos que cada vez más empleadores valoran habilidades blandas y multidisciplinares en ciberseguridad. Grandes empresas y consultoras buscan analistas que entiendan el risk management no solo técnicamente sino en términos de impacto social y comportamiento humano. Si las universidades logran transmitir ese perfil híbrido, sus egresados tendrán ventaja comparativa. Por ende, conviene también difundir entre los estudiantes de la idea de que esta formación integrada mejora su empleabilidad y eficacia profesional.

También, es importante establecer mecanismos de evaluación y retroalimentación de estas iniciativas. Se podría, por ejemplo, hacer seguimiento a la cohorte de graduados de programas interdisciplinarios (como la UADE) para ver cómo se desempeñan en el campo, o recopilar feedback de empleadores. Los resultados positivos (casos de éxito en resolver problemas complejos gracias a su formación integral) servirán para convencer a más instituciones de replicar el modelo.

La agenda formativa integradora pasa por rediseñar currículos, adoptar pedagogías críticas y colaborativas, y asegurar respaldo institucional y político. No se trata simplemente de añadir un par de cursos sociales a una malla técnica (o viceversa), sino de una transformación holística en cómo concebimos la enseñanza sobre cibercrimen. Implica que los distintos actores educativos reconozcan que están formando a profesionales que operarían en un entorno donde lo tecnológico y lo social se entrelazan indisolublemente. La criminología cultural, la criminología cyborg y la cibercriminología nos han dado el sustento teórico para justificar este giro; ahora corresponde implementar los cambios necesarios para materializarlos.

Modelo de Formación Interdisciplinaria en Cibercrimen



Leyenda: Este diagrama muestra la convergencia curricular propuesta, donde las tres facultades contribuyen a módulos comunes que se operacionalizan en laboratorios prácticos, generando un perfil profesional integrado.

Conclusiones

El análisis desarrollado a lo largo de este artículo conduce a una conclusión central: enfrentar los desafíos del cibercrimen contemporáneo exige superar el paradigma tecnocrático y avanzar hacia una formación interdisciplinaria que integre plenamente la perspectiva de las ciencias sociales (en particular la criminología) con la experticia técnica en ciberseguridad. La evidencia recopilada muestra que la aproximación dominante, enfocada casi exclusivamente en aspectos tecnológicos, es insuficiente para comprender la complejidad del delito en la era digital y, por ende, limita la efectividad de su prevención y control. Los ciberdelitos no ocurren en el vacío, sino en un entramado de significados culturales, interacciones humanas y configuraciones sociotécnicas que requieren ser abordados con herramientas analíticas más amplias.

A través de la construcción de un estado del arte crítico, destacamos cómo la criminología, en sus vertientes cultural, cyborg y cibernética, aporta marcos teóricos y enfoques analíticos cruciales para enriquecer la comprensión del cibercrimen. La criminología cultural nos recuerda que detrás de cada delito informático hay un contexto de valores, identidades y subculturas (desde la figura mítica del hacker hasta las comunidades clandestinas en la darknet) que otorgan sentido a esas conductas desviadas; ignorar esa dimensión es perder de vista el porqué profundo de muchos ataques. La criminología cyborg, por su parte, nos impulsa a repensar las fronteras entre lo humano y lo tecnológico, entendiendo que en la sociedad conectada los comportamientos delictivos son fruto de esa hibridación, y que soluciones efectivas surgirán de abordar simultáneamente los aspectos técnicos y humanos. Finalmente, la cibercriminología confirma la necesidad de un enfoque integrador, aplicando métodos empíricos y teorías adaptadas al ciberespacio para llenar las lagunas de conocimiento y guiar con base científica las políticas contra el cibercrimen.

El diagnóstico de la calidad latinoamericana puso de manifiesto que persisten importantes vacíos formativos: currícula desequilibradas hacia lo técnico, escasez de programas verdaderamente multidisciplinarios y una desconexión entre comunidades profesionales. Sin embargo, también identificamos esfuerzos emergentes y el reconocimiento creciente, tanto en el ámbito académico como en el laboral, de que un perfil híbrido es indispensable. En este sentido, las propuestas de agenda formuladas que abarcan reformas curriculares, innovaciones pedagógicas y articulación institucional, ofrecen una hoja de ruta para iniciar la transición hacia un nuevo modelo educativo. Un modelo donde un ingeniero de un "*script kiddie*", y donde un criminólogo sepa lo que es un ataque de "*SQL injection*" o cómo funciona la criptografía de clave pública; en definitiva, donde formemos profesionales completos para problemas complejos.

Para los países de América Latina, adoptar una formación interdisciplinaria en cibercrimen no es solo un imperativo académico, sino una pieza estratégica en su desarrollo digital y seguridad ciudadana. La región se encuentra en un punto de inflexión en materia de transformación digital, acelerada por la pandemia y la expansión de la economía digital. Esto amplía

la superficie de exposición a ciberdelitos, desde ataques a infraestructuras críticas hasta fraudes masivos y desinformación. Responder a estas amenazas requerirá equipos de trabajo capaces de entender al ciberdelincuente tan bien como entienden la tecnología que este explota. Como señala un informe, "comprender los aspectos legales de la ciberseguridad ayuda a tener una visión global, no exclusivamente técnica" (Nowersztern et al., 2021, p. 41); podríamos extender esa afirmación diciendo que comprender los aspectos humanos y criminológicos completa esa visión global de la seguridad digital.

En conclusión, integrar la criminología (y con ella, las ciencias sociales) en la formación contra el cibercrimen promete beneficios sustanciales: generar un conocimiento más profundo del fenómeno, habilita intervenciones más creativas y efectivas, y forma una fuerza laboral más versátil y preparada. Los obstáculos para ello (inercias institucionales, silos disciplinarios, recursos limitados) pueden superarse gradualmente con coordinación de esfuerzos entre academia, gobiernos y sector privado. Este artículo buscó sentar bases conceptuales y prácticas para impulsar ese cambio. Se espera que sus argumentos y recomendaciones contribuyan a que la próxima generación de especialistas en ciberseguridad en América Latina sea, ante todo, interdisciplinaria y crítica, equipada no solo con las últimas herramientas tecnológicas sino también con la comprensión sociocultural necesaria para navegar el complejo y fascinante universo del cibercrimen contemporáneo.

Referencias

Arroyo, S. C. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente(*). 60, 470-512.

Avendaño, C., Hidalgo, R., Torres, Y., & Sarraute, M. M. (2025). Fronteras Digitales y Violencia de Género: Un Estado del Arte en América Latina. Editorial EDP University. https://editorialedpuniversity.com/wp-content/uploads/2025/03/Libro-Fronteras-Digitales-y-Violencia-de-Genero.pdf

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1), 1-10. https://doi.org/10.1057/s41599-023-01560-x

Choi, K. (2015). Cybercriminology and digital investigation. LFB Scholarly Publishing.

Choi, K.-S., & Toro-Álvarez, M. (2017). Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Securidad Digital (Cybercriminology: Guide for Cybercrime Investigation and Best Practices in Digital Security). Fondo Editorial Universidad Santiago Nariño.

Conescrim. (2025, marzo 23). Entrevista a Jorge Ramiro Pérez Suárez: Criminología, consejos para estudiantes y proyectos que inspiran. Consejo Nacional de Estudiantes de Criminología. https://conescrim.es/conescrim/entrevista-jorge-ramiro-perez-suarez/

ESDEG. (s. f.). Maestría en Ciberseguridad y Ciberdefensa. Escuela Superior de Guerra. Recuperado 12 de mayo de 2025, de https://esdegue.edu.co/es/maestria-en-ciberseguridad-y-ciberdefensa

Garrido, V. (2012). Perfiles criminales: Un recorrido por el lado oscuro del ser humano. Ariel.

Giever, D. (2018). An Argument for Interdisciplinary Programs in Cybersecurity. International Journal of Cybersecurity Intelligence & Cybercrime, 1(1), 69-73. https://doi.org/10.52306/2578-3289.1004

Haraway, D. (1984). Manifiesto Ciborg: El sueño irónico de un lenguaje común para las mujeres en el circuito integrado. http://repositorio.ciem.ucr.ac.cr/jspui/handle/123456789/81

Hayward, K. J. (2012). Five Spaces of Cultural Criminology. British Journal of Criminology, 52(3), 441-462. https://doi.org/10.1093/BJC/AZS008

Jaishankar, K. (2008). Space transition theory of cyber crimes. En F. Schmallager & M. Pittaro (Eds.), Crimes of the Internet (pp. 283-301). Prentice Hall.

Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (0 ed.). Routledge. https://doi.org/10.1201/b10718

La ciberdelincuencia desde una perspectiva multidisciplinar y social. (2024, febrero 20). https://lasendadelcriminologo.com/la-ciberdelincuencia-desde-una-perspectiva-multidisciplinar-y-social/

López Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. Revista chilena de derecho y tecnología, 11(1), 121-146. https://doi.org/10.5354/0719-2584.2022.60913

Marín, M. E. G. (2004). Estrategias de investigación social cualitativa: El giro de la mirada. La Carreta Editores.

Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología, 13, 07:1-07:55.

Miró Llinares, F. (2012). El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons. https://www.academia.edu/7865754/El_Cibercrimen_Fenomenolog%C3%ADa_y_criminolog%C3%ADa_de_la_delincuencia_en_el_ciberespacio

Nowersztern, A., Paz, S., Kagelmacher, D., Berenfus, F. C., Libedinsky, P., Ribagorda, A., Tapiador, J., Fuentes, J. M. D., & González, L. (2021). Programa formativo en ciberseguridad para América Latina y el Caribe. IDB Publications. https://doi.org/10.18235/0003659

Paz, S., Belarte, G., & García-Belebguer, G. (2023, febrero 22). Red Ciberlac impulsa la formación de profesionales en ciberseguridad. Gobernarte. https://blogs.iadb.org/administracion-publica/es/como-red-ciberlac-impulsa-la-formacion-de-profesionales-en-ciberseguridad-en-america-latina-y-el-caribe/

Pérez Suárez, J. R. (2017). We Are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet. Criminología y Justicia.

UADE. (s. f.). LICENCIATURA EN CRIMINOLOGÍA Y CIBERDELITOS. UADE Home. Recuperado 9 de mayo de 2025, de https://www.uade.edu.ar/facultad-de-ciencias-juridicas-y-sociales/licenciatura-en-criminologia-y-ciberdelitos/

Yar, M. (2018). Toward a Cultural Criminology of the Internet. En K. F. Steinmetz & M. R. Nobles (Eds.), Technocrime and Criminological Theory (pp. 116-132). Routledge, Taylor & Francis Group. https://www.academia.edu/35641761/Yar_Toward_a_Cultural_Criminology_of_the_Internet_2018_pdf