REVISTA DE LA ACADEMIA NEOLONESA DE CIENCIAS PENALES

Año. 01 No. 02. Julio-diciembre 2025

Monterrey, Nuevo León
Julio 2025

Ciberseguridad y conductas delictivas. Un panorama criminalístico desde el perfil del suboficial del ejército colombiano

Cybersecurity and Criminal Conduct: A Criminological Perspective from the Profile of a Colombian Army Non-Commissioned Officer

Lina María Rivera Alturo[1]
ORCID 0009-0008-6695-679X
Sussy Alejandra Hernández García[2]
ORCID 0000-0002-7819-6459

Fecha de recibido: 07 de abril de 2025 / Fecha de aprobación: 20 de junio de 2025

Resumen

En la era digital, la ciberseguridad es un pilar fundamental para proteger la información, un activo primordial para ciudadanos, gobiernos y el Ejército Nacional. Este análisis documental explora la intrínseca relación entre la ciberseguridad y las conductas delictivas que proliferan con la creciente dependencia de las Tecnologías de la Información y la Comunicación (TIC), impulsadas por la Cuarta Revolución Industrial. La criminalística tradicional ha trascendido la escena física para converger con el ciberespacio, ahora un dominio operativo vital para la infraestructura crítica militar, presentando desafíos sin precedentes debido a la sofisticación y velocidad de amenazas como el ransomware, el phishing y los ataques DDoS. En este contexto, la formación del Tecnólogo en Criminalística es crucial. Un currículo pertinente, basado en metodologías activas, debe prepararlos para identificar no solo los delitos, sino también el modus operandi de los ciberdelincuentes. Paralelamente, la investigación subraya los profundos y a menudo subestimados perjuicios psicológicos de los delitos informáticos. El ciberacoso, el fraude y el robo de identidad pueden provocar ansiedad, depresión, Trastorno de Estrés Postraumático (TEPT) y un grave deterioro del bienestar emocional. El estudio concluye que es imperativo un enfoque integral que combine la capacitación especializada del personal militar, la prevención mediante la educación digital y un robusto sistema de apoyo psicológico y legal para las víctimas, garantizando así la seguridad en el ciberespacio.

Palabras Clave

Conductas delictivas, ciberseguridad, Informática forense, criminalística, formación.

Abstract

In the digital age, cybersecurity stands as a fundamental pillar for protecting information, a primary asset for citizens, governments, and the National Army. This documentary analysis explores the intrinsic relationship between cybersecurity and the criminal behaviors that proliferate due to a growing reliance on Information and Communication Technologies (ICT), driven by the Fourth Industrial Revolution. Traditional criminology has transcended the physical realm to converge with cyberspace, which is now a vital operational domain for critical military infrastructure. This shift presents unprecedented challenges due to the sophistication and speed of threats like ransomware, phishing, and DDoS attacks. In this context, the training of Criminology Technologists is crucial. A relevant curriculum, based on active methodologies, must prepare them not only to identify crimes but also to understand the modus operandi of cybercriminals. Concurrently, the research highlights the profound and often underestimated psychological harm caused by cybercrime. Cyberbullying, fraud, and identity theft can lead to anxiety, depression, Post-Traumatic Stress Disorder (PTSD), and a severe decline in emotional well-being. The study concludes that a comprehensive approach is imperative, one that combines specialized training for military personnel, prevention through digital education, and a robust system of psychological and legal support for victims, thereby ensuring security in cyberspace

Key words

Criminal behavior, cybersecurity, forensic computing, criminalistics, training.

[1] Ingeniera de Sistemas, Magister en Educación y Docencia, Docente de la Escuela Militar de Suboficiales "Sargento Inocencio Chincá", lmrivera18@gmail.com
[2] Trabajadora Social, Especialista en Gerencia Social, Maestrante en Gerencia Social y Desarrollo Integral, Docente de la Escuela Militar de Suboficiales "Sargento Inocencio Chincá", trabajosocialsussy@gmail.com

Tabla de contenido

Introducción

En la amplia y confusa red de la era digital, la ciberseguridad emerge como un pilar fundamental, trascendiendo las esferas individuales y organizacionales. La información, establecida como activo primordial tanto para la ciudadanía como para el desarrollo de las actividades gubernamentales y del Ejército Nacional, demanda una atención prioritaria. Desde la perspectiva de la tecnología en Criminalística de campo de la Escuela Militar de Suboficiales, el presente análisis documental y descriptivo explora la intrínseca relación entre la ciberseguridad y las conductas delictivas que proliferan en la era posmoderna, dando lugar a la aparición constante de amenazas y vulnerabilidades. La creciente e innegable dependencia de las Tecnologías de la Información y la Comunicación (TIC) ha configurado un escenario propicio para la materialización de un espectro cada vez más amplio de actividades ilícitas perpetradas en el ciberespacio.

La formación en Seguridad Informática e Informática Forense dentro del currículo académico no solo busca la identificación de delitos informáticos, sino que profundiza en el reconocimiento de las conductas delictivas subyacentes. Comprender el modus operandi de los ciberdelincuentes, quienes encuentran un número creciente de víctimas en el ciberespacio, se ha convertido en una necesidad apremiante para garantizar la seguridad y la soberanía en el contexto colombiano.

Los delitos informáticos, también conocidos como cibercrímenes, se han convertido en una amenaza creciente en la sociedad digital actual. Aunque sus consecuencias materiales y económicas son evidentes, no deben subestimarse los profundos perjuicios psicológicos que pueden ocasionar en las víctimas. Estas secuelas, muchas veces invisibles, afectan la salud mental, el bienestar emocional y la calidad de vida de quienes las sufren.

Revisión de literatura

La Criminalística y su convergencia con el ciberespacio

Tradicionalmente, la criminalística se ha definido como la disciplina científica encargada de descubrir, identificar, interpretar y evaluar los indicios y evidencias de un hecho delictivo, con el fin de comprobar su existencia, identificar a los responsables, recolectar pruebas y reconstruir los sucesos (Bosquet, 2015). Sin embargo, la naturaleza cambiante del crimen ha llevado a esta disciplina a trascender la escena física y expandirse significativamente al entorno digital, tal como lo

evidencian los trabajos de Casey (2011) sobre evidencia digital y Carrier (2005) en relación con el proceso forense digital.

La interconexión global impulsada por la globalización y la innovadora Cuarta Revolución Industrial ha convertido el ciberespacio en un nuevo frente para la criminalidad en el siglo XXI, a partir de la comunicación en masas y su difusión en internet como lo revela (Castells, 2000) en su análisis de la sociedad red, termino usado para describir las nuevas formas de comunicación, generando desafíos considerables debido a la creciente sofisticación de las amenazas digitales. Entre estos desafíos, destaca la búsqueda de una definición exacta de "cibercrimen" con implicaciones tanto para el ámbito legal como para los procedimientos de la criminalística. Siguiendo a Cuadra (2010), este se define como las actividades ilícitas llevadas a cabo mediante recursos informáticos y electrónicos, que vulneran la integridad, la confidencialidad o la accesibilidad de la información de individuos o entidades, particularmente en el ciberespacio.

La rápida evolución tecnológica y la creciente digitalización de la vida cotidiana han propiciado una significativa transformación en el panorama de los delitos informáticos. Entre los más relevantes se encuentran, el ransomware, el phishing, hackeo de sistemas informáticos, los ataques de denegación de servicio (DDoS) y el malware. Estas actividades ilícitas, que comparten el uso de la tecnología con fines maliciosos y la explotación de vulnerabilidades, generan un impacto considerable a nivel económico, social y político, presentando desafíos inherentes a su investigación

El Ciberespacio como un dominio operativo en la infraestructura crítica militar

El ciberespacio se ha consolidado como un dominio operativo de vital importancia dentro de la infraestructura crítica militar de Colombia. Esta nueva dimensión de la guerra y la seguridad exige una comprensión profunda de sus características y vulnerabilidades. Según Manzano (2018), "el ciberespacio trasciende las fronteras físicas, permitiendo la proyección de poder y la ejecución de operaciones a distancia con una velocidad y un alcance sin precedentes". Esta capacidad de operar sin las limitaciones geográficas tradicionales introduce desafíos significativos para la defensa nacional, ya que los ataques pueden originarse desde cualquier lugar del mundo y dirigirse a sistemas esenciales para la operatividad militar, al igual que en tiempo, determinando la toma de decisiones en cuestión de segundos de ejecución.

La creciente dependencia de la infraestructura crítica militar colombiana en sistemas interconectados la expone a una gama diversa de amenazas cibernéticas. Autores como Arquilla y Ronfeldt (2001) señalan que "la guerra en red y los conflictos de baja intensidad se caracterizan por el uso estratégico de la información y la tecnología para desestabilizar al adversario". En este contexto, la protección de redes de comunicación, sistemas de control de armamento, inteligencia y logística se vuelve fundamental. Cualquier vulnerabilidad explotada en estos sistemas podría tener consecuencias catastróficas para la seguridad y la soberanía nacional, afectando la capacidad de respuesta ante amenazas convencionales y no convencionales.

En este sentido, la investigación criminal sobre el ciberespacio se vuelve esencial para desarrollar estrategias de defensa cibernética robustas y adaptativas. Singer y Friedman (2014) enfatizan la necesidad de "comprender la naturaleza evolutiva de las amenazas cibernéticas y la importancia de la colaboración entre los sectores público y privado para fortalecer la resiliencia cibernética". El análisis de las capacidades ofensivas y defensivas en el ciberespacio, así como la identificación de las principales vulnerabilidades y la implementación de medidas preventivas y reactivas, son aspectos cruciales para garantizar la seguridad y la operatividad de la infraestructura militar de un Ejército globalizado

El Rol del Tecnólogo en Criminalística en la Era Digital y el Auge de los Ciberataques

La integración pedagógica de las Tecnologías de la Información y la Comunicación (TIC) y la Inteligencia Artificial (IA) no solo como herramientas, sino como elementos constitutivos del proceso de aprendizaje, permitirá a los futuros tecnólogos desarrollar la alfabetización digital y las competencias necesarias para interactuar eficazmente con la evidencia digital y las nuevas formas de criminalidad. Siemens (2005) en su teoría del conectivismo, postula que el aprendizaje ya no reside únicamente en el individuo, sino que se extiende a través de redes y tecnologías, enfatizando la importancia de la capacidad para construir y navegar estas redes; Un currículo pertinente para esta era debe ser flexible, adaptable y centrado en el estudiante, promoviendo el aprendizaje autónomo y colaborativo.

Basándose en las ideas de Knowles (1980) sobre la andragogía, el aprendizaje de adultos debe reconocer sus experiencias previas y fomentar la autogestión del aprendizaje. La incorporación de metodologías activas, como el aprendizaje basado en problemas (ABP), el estudio de casos reales de ciberataques y simulaciones forenses digitales permitirá a los alumnos aplicar los conocimientos teóricos en contextos prácticos y desarrollar habilidades de pensamiento crítico y toma de decisiones, proporcionar retroalimentación adaptativa, optimizando así la adquisición de competencias especializadas en el ámbito de la criminalística digital.

En el contexto del perfil profesional militar, donde la criminalística emerge como un eje transversal fundamental, el syllabus de Seguridad Informática e Informática Forense profundiza en conceptos y resultados de aprendizaje esenciales; Estos se orientan a la identificación no solo de los delitos informáticos, sino también de aquellas conductas delictivas subyacentes que revelan el modus operandi de los criminales, la velocidad y la naturaleza transfronteriza de los ciberataques contemporáneos, Schick (2020) destaca cómo la falsificación y la desinformación, impulsadas por la tecnología, emergen como resultados frecuentes de las actividades delictivas en el ciberespacio.

Dada la creciente victimización en el ciberespacio y el papel fundamental de la Cuarta Revolución Industrial en la reconfiguración del poder gubernamental hacia el dominio digital (Schwab, 2020), el enfoque transversal del tecnólogo en criminalística de la Escuela Militar de Suboficiales se convierte en una herramienta esencial para comprender y neutralizar las amenazas que afectan las actividades militares. Por ello, una capacitación rigurosa del personal militar en estos aspectos críticos resulta indispensable para el ejercicio de sus funciones.

Perjuicios psicológicos y delitos informáticos: Una conexión profunda y preocupante

En la era digital, los delitos informáticos han emergido como una amenaza significativa, no solo por sus repercusiones económicas, sino también por el profundo impacto psicológico que generan en las víctimas. El ciberacoso, una forma de violencia que se perpetra a través de medios digitales, ha demostrado tener consecuencias devastadoras en la salud mental de quienes lo padecen. Este artículo investigativo explora las diversas manifestaciones del ciberacoso, sus efectos psicológicos y las estrategias para mitigar su impacto.

Teniendo presente que, el auge de las tecnologías de la información y la comunicación (TIC) ha generado un incremento significativo en la incidencia de los delitos informáticos. Más allá de las pérdidas económicas directas, estos crímenes producen un profundo impacto psicológico en las víctimas, afectando su bienestar emocional, social y físico (Kowalski & Limber, 2007). Este artículo revisa la literatura científica para comprender la naturaleza y magnitud de este impacto, identificando las áreas de mayor vulnerabilidad y las estrategias de intervención más efectivas.

Tipos de delitos informáticos y sus consecuencias psicológicas

Diversos tipos de cibercrimen provocan daño psicológico significativo:

1. Ciberacoso (Cyberbullying): El acoso online, caracterizado por la intimidación, amenazas y humillación a través de medios digitales, se asocia con altos niveles de ansiedad, depresión, baja autoestima y aislamiento social (Smith et al., 2008). En casos extremos, puede llevar a ideación suicida (Hinduja & Patchin, 2010).
2. Fraudes cibernéticos: Las estafas online, como el phishing o el robo de identidad, generan estrés, ira, culpa, vergüenza y, en algunos casos, TEPT (Trastorno de Estrés Postraumático) (Dutton y Greene, 2010). La pérdida financiera y la violación de la privacidad contribuyen al impacto psicológico.
3. Robo de identidad: La usurpación de la identidad personal produce una profunda sensación de vulnerabilidad, desconfianza y miedo a perder el control de la propia vida. Las consecuencias financieras y legales se suman al daño psicológico (Eaton et al., 2013).
4. Difusión no consentida de contenido íntimo (Revenge Porn): La publicación sin consentimiento de imágenes o videos privados causa un daño psicológico devastador, incluyendo vergüenza, humillación, depresión, ansiedad y problemas en las relaciones interpersonales (Campbell et al., 2016).

Las manifestaciones psicológicas del ciberacoso pueden desencadenar una variedad de síntomas psicológicos en las víctimas. Según Ortega y Carrascosa (2018), las víctimas de ciberbullying experimentan malestar psicológico significativo, que se intensifica con la duración del acoso. Este malestar se manifiesta en forma de ansiedad, depresión, estrés, ira, miedo, vergüenza y culpa. Además, estudios indican que las víctimas pueden desarrollar síntomas físicos como dolores de cabeza, fatiga y problemas digestivos (Garaigordobil, 2011).

La victimización en línea también puede llevar al aislamiento social, cambios en los hábitos de sueño y alimentación, disminución del rendimiento académico o laboral, abuso de sustancias y conductas autolesivas (Psicólogos de México, s.f.). Estos efectos no solo deterioran la calidad de vida de las víctimas, sino que también pueden tener consecuencias a largo plazo en su bienestar emocional y social.

Esto, teniendo presente que, los factores que aumentan la vulnerabilidad psicológica pueden incrementar la susceptibilidad de los individuos a los efectos psicológicos del ciberacoso. La edad es un factor determinante; niños, adolescentes y jóvenes son más propensos a sufrir estos efectos debido a su etapa de desarrollo emocional y social (Díaz-Aguado, 2024). Además, las personas con baja autoestima, problemas de ansiedad o depresión son más vulnerables a los impactos psicológicos de estos delitos (Córdova Cedeño et al., 2023).

Las experiencias previas de acoso o violencia también pueden aumentar la susceptibilidad de una persona a los efectos psicológicos del ciberacoso. Quienes han sido víctimas en el pasado pueden experimentar una reactivación de traumas anteriores, intensificando su respuesta emocional y dificultando su recuperación (Redondo et al., 2022).

Por esta razón, es fundamental que las víctimas de ciberacoso reciban apoyo psicológico especializado para procesar el trauma, desarrollar estrategias de afrontamiento y recuperar su bienestar emocional. La atención psicológica puede incluir terapia cognitivo-conductual, intervenciones basadas en la resiliencia y programas de apoyo grupal (Ortega & Carrascosa, 2018).

Además del apoyo psicológico, es importante que las víctimas conozcan sus derechos y opciones legales para denunciar el delito y buscar justicia. La asesoría legal puede empoderar a las víctimas, ayudándolas a recuperar el control sobre su vida y a prevenir futuras situaciones de acoso (Fundación Impulsando Vida, s.f.).

La participación en grupos de apoyo con otras víctimas puede ser beneficiosa para compartir experiencias, recibir apoyo emocional y encontrar estrategias de afrontamiento. Estos grupos proporcionan un entorno seguro donde las víctimas pueden expresar sus sentimientos y aprender de las experiencias de los demás (Redondo et al., 2022).

Todo esto, teniendo presente que, la prevención del ciberacoso y sus efectos psicológicos requiere un enfoque integral que incluya educación en seguridad digital, promoción del uso responsable de las tecnologías de la información y la comunicación (TIC), y la creación de entornos seguros en línea. Es fundamental educar a las personas sobre los riesgos cibernéticos, las medidas de seguridad que pueden tomar y cómo prevenir ser víctimas de delitos informáticos (Fundación Impulsando Vida, s.f.).

Fomentar el uso responsable de las TIC, especialmente entre niños y adolescentes, es crucial para prevenir conductas de riesgo. Esto incluye enseñar habilidades de comunicación asertiva, empatía y resolución de conflictos, así como promover valores de respeto y tolerancia en el entorno digital (Díaz-Aguado, 2024).

Es importante denunciar los delitos informáticos a las autoridades para que puedan ser investigados y se haga justicia. La denuncia no solo ayuda a proteger a la víctima, sino que también contribuye a la identificación y sanción de los agresores, disuadiendo futuras conductas delictivas (Córdova Cedeño et al., 2023).

Fomentar la creación de entornos seguros en línea donde las personas puedan interactuar e intercambiar información sin temor a ser víctimas de cibercrimen es esencial. Esto implica la implementación de políticas de moderación efectivas en las plataformas digitales, así como la promoción de una cultura de respeto y responsabilidad en el uso de las TIC (Redondo et al., 2022).

Metodología y métodos

La presente investigación adoptó un enfoque metodológico mixto, combinando elementos cualitativos y cuantitativos para obtener una comprensión integral de las problemáticas relacionadas con los ciberdelitos y las conductas delictivas en el entorno digital desde la perspectiva de los suboficiales del Ejército Colombiano. La fase cualitativa se centra en explorar las percepciones, experiencias y desafíos que enfrentan estos suboficiales en relación con la ciberseguridad y la investigación criminalística digital; con la aplicación de entrevistas semiestructuradas con suboficiales con experiencia en áreas relevantes, así como con formadores.

Paralelamente, la dimensión cuantitativa de la investigación para la identificación de patrones, tendencias y la frecuencia de ciertos tipos de ciberdelitos o conductas delictivas que involucran elementos digitales en el contexto militar colombiano. Aplicando un cuestionario estructurado y diseñado con preguntas cerradas y escalas de Likert, a una muestra representativa de suboficiales.

Esta triangulación de la información nos ofrece una comprensión más completa del fenómeno investigado, generando divergencia o complementariedad en la evaluación de los hallazgos de ambos enfoques, la interpretación y discusión de los resultados se realizaron en el contexto del perfil del suboficial del Ejército Colombiano y su rol en la criminalística dentro del entorno operativo y formativo militar.

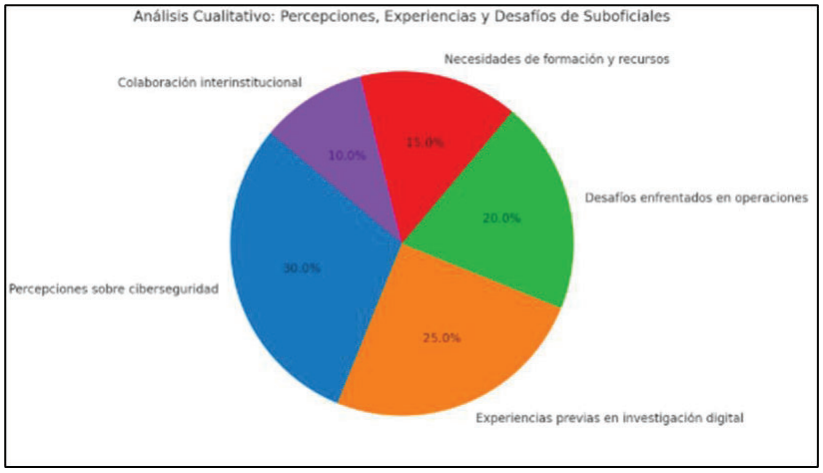

Figura 1. Identificación de categorías clave que surgieron de las percepciones, experiencias y desafíos expresados por los suboficiales.

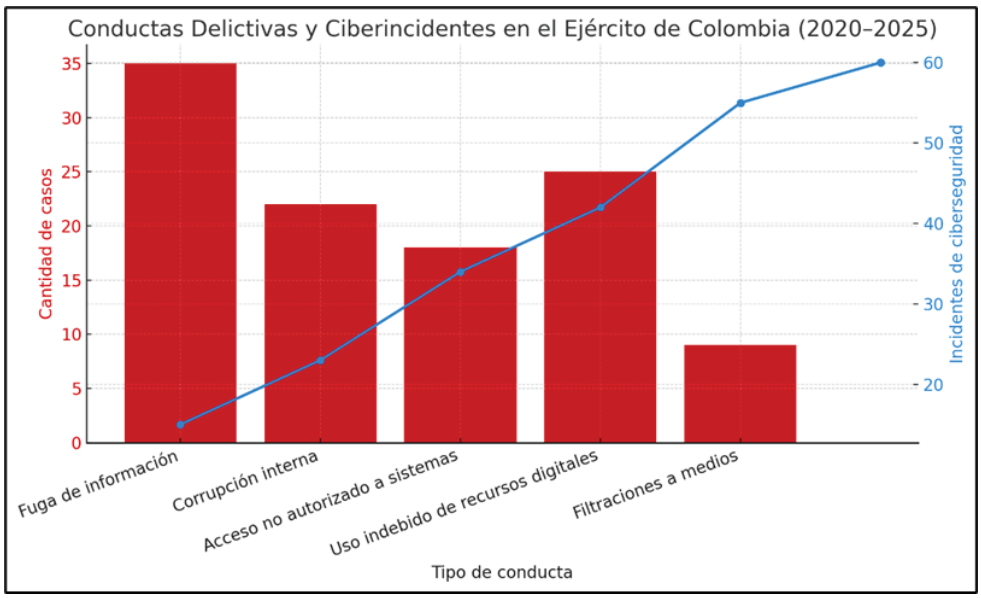

Figura 2. Conductas delictivas con la evolución de los incidentes de ciberseguridad en el Ejército de Colombia entre 2020 y 2025.

Resultados

la relevancia de la formación en criminalística tecnológica para la identificación de conductas delictivas en el contexto de la globalización y la Cuarta Revolución Industrial. Subraya cómo esta capacidad es crucial para enfrentar las crecientes y sofisticadas amenazas cibernéticas. Destaca la necesidad de una formación integral que combine los principios de la criminalística con las herramientas y técnicas del mundo digital, preparando a los futuros tecnólogos para ser actores clave en la lucha contra el cibercrimen.

Programas de capacitación especializados y certificaciones pueden equipar a los investigadores con las habilidades necesarias para enfrentar los desafíos tecnológicos y éticos. Belshaw (2019) sugiere que la formación debe ser integral, cubriendo aspectos técnicos, legales y éticos, para preparar a los profesionales para una práctica forense efectiva y responsable.

La conexión entre los delitos informáticos y los perjuicios psicológicos es profunda y preocupante. El ciberacoso, en particular, representa una amenaza significativa para la salud mental de las víctimas, afectando su bienestar emocional, social y físico. Abordar esta problemática requiere un enfoque integral y multisectorial que incluya la colaboración entre gobiernos, empresas, organizaciones civiles y la ciudadanía. Solo a través de esfuerzos coordinados y sostenidos se podrá crear un ciberespacio más seguro y proteger el bienestar emocional de las personas.

El ciberacoso representa una grave amenaza para la salud mental de las víctimas, con consecuencias que pueden perdurar a lo largo del tiempo. Es imperativo que la sociedad, las instituciones educativas y las autoridades trabajen

conjuntamente para prevenir estos delitos, brindar apoyo a las víctimas y promover un entorno digital seguro y respetuoso.

Referencias bibliográficas

Arquilla, J., & Ronfeldt, D. (2001). Networks and netwars: The future of terror, crime, and militancy. RAND Corporation.

Bosquet, S. (2015). Criminalística forense. Tirant lo Blanch.

Campbell, R., et al. (2016). Revenge Pornography: A Review of the Literature. [Insert Journal Information]

Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Córdova Cedeño, J. J., Briones Ponce, M. E., & Delgado Cobeña, E. I. (2023). El ciberacoso y la estabilidad psicológica: estudio con adolescentes de Rocafuerte, Manabí, Ecuador. Revista PSIDIAL: Psicología y Diálogo de Saberes. https://doi.org/10.33936/psidial.v1i2.4351

Cuadra, A. (2010). Virtualidad y conocimiento. ELAP Escuela latinoamericana de estudios de posgrado y políticas públicas.

Díaz-Aguado, M. J. (2024). El ciberacoso aumenta la desconexión moral y la sensación de impunidad. El País. https://elpais.com/educacion/2024-12-15/maria-jose-diaz-aguado-catedratica-de-psicologia-evolutiva-el-ciberacoso-aumenta-la-desconexion-moral-y-la-sensacion-de-impunidad.html

Dutton, MA, y Greene, R. (2010). Resiliencia y victimización criminal. Revista de Estrés Traumático: Publicación oficial de la Sociedad Internacional para el Estudio del Estrés Traumático , 23 (2), 215-222.

Eaton, NR, Krueger, RF, Markon, KE, Keyes, KM, Skodol, AE, Wall, M., ... y Grant, BF (2013). Estructura y validez predictiva de los trastornos internalizantes. Revista de psicología anormal , 122 (1), 86.

Fundación Impulsando Vida. (s.f.). Cyberacoso: Consecuencias, prevención y conciencia digital. https://impulsandovida.org/article/cyberacoso-consecuencias-prevencion-y-conciencia-digital

Garaigordobil, M. (2011). Cibervictimización. Wikipedia. https://es.wikipedia.org/wiki/Cibervictimizaci%C3%B3nciencias.uautonoma.cl+2es.wikipedia.org+2psicologosdemexico.com+2

Hinduja, S., & Patchin, J. W. (2010). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Corwin Press.

Knowles, M. S. (1980). The modern practice of adult education: From pedagogy to andragogy. Cambridge Adult Education Company.

Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. Journal of adolescent health, 41(6), S22-S30.

Manzano, J. C. (2018). Ciberseguridad: Un enfoque estratégico para la defensa nacional. Editorial Segura.

Ortega, J., & Carrascosa, L. (2018). Malestar psicológico y apoyo psicosocial en víctimas de ciberbullying. International Journal of Developmental and Educational Psychology, 2(1), 357-366. https://www.redalyc.org/journal/3498/349856003038/html/redalyc.org

Psicólogos de México. (s.f.). La victimización en la era digital: acoso cibernético y sus consecuencias psicológicas. https://www.psicologosdemexico.com/la-victimizacion-en-la-era-digital-acoso-cibernetico-y-sus-consecuencias-psicologicas/psicologosdemexico.com

Redondo, J., Luzardo-Briceño, M., García-Lizarazo, K. L., & Inglés, C. J. (2022). Impacto psicológico del ciberbullying en estudiantes universitarios: un estudio exploratorio. Revista Colombiana de Ciencias Sociales.

https://revistas.ucatolicaluisamigo.edu.co/index.php/RCCS/article/view/2061revistas.ucatolicaluisamigo.edu.co

Schick, N. (2020). Deepfakes: The coming infocalypse. Hachette UK.

Schwab, K. (2020). La cuarta revolución industrial. Futuro hoy, 1(1), 06-10.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.