

TRABAJO DE GRADO

Opción Investigación o Proyecto de Grado

Análisis de los mecanismos de conciliación frente a las modalidades de fraude
cibernético

Autores:

Erika Peña Ortiz, Anyela Garcia Marin

Tutor

Dr. Santiago Agudelo Taborda

Corporación Universitaria Remington.

Derecho

2026

Agradecimientos

Expresamos nuestro más sincero agradecimiento a nuestra universidad por brindarnos la oportunidad de fortalecer nuestros conocimientos y desarrollar este importante artículo de investigación, De manera especial, agradecemos a nuestro tutor, el Doctor Santiago Agudelo Taborda, por su orientación, dedicación y acompañamiento durante todo el proceso investigativo. Sus enseñanzas, conocimientos y apoyo fueron fundamentales para la elaboración y culminación satisfactoria de este artículo de investigación.

Asimismo, agradecemos a todas las personas que, de una u otra forma, contribuyeron y nos motivaron en el desarrollo de este trabajo académico.

Tabla de Contenidos

Introducción	8
Planteamiento del problema.....	11
Justificación	14
Objetivos	13
Objetivo General	13
Objetivos específicos	13
Marco Referencial.....	17
Antecedentes	17
Marco teórico	19
Resultados y Discusión	23
Modalidades de fraude cibernético más recurrentes	23
Barreras jurídicas y técnicas que limitan el uso de la conciliación en casos de delitos informáticos	28
Propuesta de criterios orientadores para conciliadores	32
Conclusiones	33
Referencias.....	35

Resumen

En este artículo resultado de investigación se analiza la viabilidad jurídica y la efectividad de la conciliación extrajudicial como alternativa para la reparación integral del daño en las víctimas de fraude cibernético en el sector empresarial colombiano. Ante el incremento de la criminalidad informática y la lentitud del sistema penal tradicional, se evaluó cómo los Mecanismos Alternativos de Solución de Conflictos (MASC) operan como herramientas de recuperación eficiente de activos.

A nivel metodológico, este estudio se desarrolló bajo un enfoque cualitativo y con un alcance descriptivo, para lo cual se empleó un diseño documental. Para ello se examinó la interacción normativa entre la Ley 1273 de 2009 y la Ley 2220 de 2022 (Estatuto de Conciliación). Además, se complementó la información mediante literatura especializada en justicia restaurativa y datos de las autoridades en materia de fraude informático.

Los resultados encontrados demuestran que, si bien conductas como la transferencia no consentida de activos poseen un carácter patrimonial eminentemente conciliable, existe una subutilización de los centros de conciliación motivada por el desconocimiento técnico de los operadores jurídicos y la complejidad probatoria digital. Como conclusión del trabajo, se determinó que la estructuración de un protocolo de tasación de daños informáticos basado en la autonomía de la voluntad disminuye el desgaste procesal y asegura el resarcimiento económico rápido del empresario.

De esta forma, con esta labor investigativa se aportan criterios orientadores que demuestran que la conciliación se consolida como un instrumento indispensable para la seguridad jurídica corporativa, al tiempo que aporta a la descongestión del sistema judicial en la era digital.

Palabras clave

Conciliación extrajudicial, Justicia restaurativa, Fraude cibernético, Delitos informáticos, Reparación integral.

Introducción

La evolución de las Tecnologías de la Información y la Comunicación (TIC) ha reconfigurado las dinámicas comerciales globales, mejorando procesos y ampliando fronteras de mercado. No obstante, esta transición hacia lo digital ha traído consigo la diversificación de conductas delictivas que son complejas de analizar. Una de estas prácticas es el fraude cibernético que se ha posicionado como una de las amenazas más críticas para la estabilidad y sostenibilidad del sector empresarial.

Modalidades transnacionales como el phishing, el acceso abusivo a sistemas informáticos y la transferencia no consentida de activos vulneran la infraestructura técnica de las organizaciones y atentan de manera directa contra su patrimonio económico, así como la seguridad jurídica. Esta realidad exige respuestas del sistema de justicia de manera articulada, integral e inmediatas.

Sin embargo, el sistema judicial en Colombia enfrenta limitaciones operativas para perseguir penalmente los ciberdelitos. Esto se debe a la rigidez formal del proceso penal acusatorio, a lo cual se le suma la congestión de procesos y la complejidad inherente a la recaudación de evidencia digital. Todo ello se traduce en dilaciones procesales extenuantes que desprotegen a las víctimas.

Por ende, para el empresario afectado por fraudes digitales la prioridad procesal se enfoca en la recuperación de los activos hurtados para garantizar la continuidad del negocio. Lo que ocurre en la práctica es que el proceso penal es extenso y pocas veces proporciona de manera oportuna dicha justicia material, razón por la cual se perpetúa la percepción de impunidad.

En este contexto, los Mecanismos Alternativos de Solución de Conflictos (MASC), y en particular la conciliación extrajudicial, emergen como una alternativa procesal de vanguardia. Respaldada por un robusto marco normativo que incluye la Ley 1273 de 2009 que tipifica los delitos informáticos y el Estatuto de Conciliación establecido en la Ley 2220 de 2022, la justicia restaurativa ofrece un espacio idóneo para gestionar las controversias de contenido eminentemente patrimonial. La conciliación, fundamentada en el principio de la autonomía de la voluntad, permite que las partes involucradas construyan fórmulas de arreglo flexibles y vinculantes, orientadas al resarcimiento económico rápido y efectivo.

Ahora bien, a pesar de las ventajas teóricas que ofrece el uso de los MASC, en la realidad se observa una subutilización de los de conciliación para resolver controversias derivadas de delitos informáticos. Esta realidad está motivada por la falta de lineamientos claros que orienten a los operadores jurídicos sobre la tasación de daños digitales y por la incertidumbre conceptual respecto a los límites de la conciliación en conductas que frota el orden público informático.

Teniendo en cuenta lo expresado, en este artículo se ha propuesto analizar de qué manera la conciliación extrajudicial se constituye como una herramienta eficaz para la reparación integral del daño en los fraudes cibernéticos que golpean al sector empresarial. Para dar cumplimiento a este propósito, el estudio se estructuró a través de tres fases metodológicas; primero, se caracterizaron las modalidades de fraude digital con mayor incidencia corporativa; segundo, se evaluaron las barreras legales y técnicas que restringen

la aplicabilidad de los acuerdos restaurativos; y tercero, se plantearon criterios orientadores concretos para optimizar la toma de decisiones estratégicas de empresarios y conciliadores.

Este trabajo es importante porque conecta la dogmática penal informática con la gestión pacífica de conflictos bajo un enfoque cualitativo y un diseño documental. A través de este análisis, se demuestra que la implementación sistemática de audiencias virtuales y protocolos técnicos de mediación descongestiona el aparato judicial y protege el ecosistema empresarial mediante soluciones efectivas y eficaces. Así se busca validar que los MASC son instrumentos indispensables para construir una paz social y una seguridad económica en tiempos donde el mercado digital está en auge.

Planteamiento del problema

En el panorama actual, la digitalización de los procesos comerciales ha transformado la estructura operativa de las organizaciones, pero simultáneamente ha incrementado la vulnerabilidad del sector empresarial ante la delincuencia informática. En este sentido, el fraude cibernético se ha consolidado como un fenómeno transnacional que afecta la estabilidad económica y la confianza en los mercados digitales (Organización de Estados Americanos [OEA], 2019). Esta problemática no es ajena al contexto jurídico nacional, donde la transición hacia una justicia digital exige respuestas rápidas ante conductas que evolucionan a una velocidad superior a la de los procesos judiciales ordinarios.

Ahora bien, la caracterización del fenómeno revela que modalidades como el phishing, el acceso abusivo a sistemas informáticos y la suplantación de identidad corporativa son las tácticas más recurrentes para desviar activos y defraudar a empresarios. De hecho, Castillo (2021) sugiere que, aunque existen marcos normativos penales robustos, la judicialización tradicional de estos eventos suele enfrentar barreras como la dificultad en la recaudación probatoria técnica y la congestión del sistema acusatorio. Esto genera una percepción de impunidad y una desprotección material del empresario, quien ve limitada su capacidad de recuperar lo defraudado de manera ágil y efectiva.

Entre las causas principales de esta problemática se identifica una desconexión entre la operatividad de los centros de conciliación y la naturaleza técnica de los delitos informáticos. Según Arboleda et al. (2023), a menudo existe incertidumbre jurídica sobre la procedibilidad de la conciliación en estas conductas, lo que impide que se utilicen los

Mecanismos Alternativos de Solución de Conflictos (MASC) como una vía de reparación directa. Mantener este problema sin intervención implica riesgos significativos, tales como el cierre de unidades productivas por quiebras derivadas de fraudes y el aumento de la litigiosidad penal por asuntos que, mediante una adecuada mediación técnica, podrían resolverse en etapas tempranas.

El alcance de esta investigación se delimita al estudio de las modalidades de fraude digital que impactan a los empresarios en el periodo 2024-2026, con un enfoque especial en la viabilidad jurídica de los acuerdos conciliatorios dentro del marco legal vigente. Geográficamente, el análisis se centra en el contexto nacional, tomando como unidad de análisis la interacción entre las víctimas (empresarios) y las rutas de conciliación. Conceptualmente, la propuesta se sitúa en la intersección entre el Derecho Penal, la Seguridad de la Información y la Conciliación.

Cabe mencionar que existe una brecha evidente en la gestión del conocimiento y es que mientras la doctrina se ha centrado en la persecución penal del ciberdelito, se ha explorado poco el potencial restaurativo de la conciliación en este campo. No existen protocolos estandarizados que orienten a los conciliadores sobre cómo manejar la reparación económica en fraudes cibernéticos, ni criterios claros sobre cuándo estos delitos pierden su carácter de conciliables por afectar el orden público. Esta investigación busca llenar ese vacío, proporcionando un análisis que conecte la teoría de los MASC con la realidad técnica de la delincuencia informática.

Teniendo en cuenta lo explicado anteriormente se realizó la siguiente pregunta problema: ¿De qué manera los mecanismos de conciliación pueden constituirse como una

alternativa jurídica efectiva para garantizar la reparación integral del daño en las modalidades de fraude cibernético que afectan al sector empresarial en la actualidad?

Justificación

Esta investigación es relevante porque aborda la creciente vulnerabilidad del sector empresarial frente a las modalidades de fraude digital, las cuales han superado la capacidad de respuesta de los métodos de litigio tradicionales. Social y sectorialmente, el problema es relevante porque el fraude cibernético puede llevar a la quiebra de las pequeñas y medianas empresas, afectando el empleo y la estabilidad económica regional. Al proponer la conciliación como alternativa, se busca proteger el tejido empresarial mediante soluciones que prioricen la recuperación de activos sobre el castigo penal de largo aliento.

A nivel académico, el trabajo es relevante porque pretende aportar a la comprensión de este fenómeno. De hecho, existe una división marcada entre el derecho penal informático y los Mecanismos Alternativos de Solución de Conflictos (MASC). Este estudio contribuye al campo jurídico al explorar cómo la conciliación puede adaptarse a la complejidad técnica de los delitos digitales, ofreciendo un análisis que busca una aplicabilidad práctica en los centros de conciliación.

Por otra parte, la utilidad de los resultados es importante porque mejoran los procesos de toma de decisiones tanto para empresarios como para conciliadores. Al identificar qué tipos de fraude son susceptibles de acuerdo, se proporciona una hoja de ruta que reduce la incertidumbre jurídica y fomenta la innovación en la gestión de conflictos. Esto permite que el sistema judicial se descongestione, delegando en la autonomía de la voluntad aquellos casos donde la reparación económica es el interés primordial de la víctima.

De esta manera, el impacto potencial de lo aquí planteado beneficia de manera directa a los empresarios, quienes obtendrán claridad sobre sus derechos y opciones de recuperación, e indirectamente al Estado, al fortalecer la confianza en las instituciones y en los mecanismos de paz ciudadana. En un entorno donde el fraude digital es una constante, dotar a la conciliación de herramientas para abordar estos desafíos es una apuesta por la seguridad jurídica y la eficiencia del derecho.

Cabe aclarar que esta investigación fue factible debido a que, al ser una revisión documental, se contaba con fuentes de información, bases de datos y normativa vigente en materia de conciliación y delitos informáticos. De igual forma, el tema se encuentra vigente debido al auge de estos delitos y la necesidad de utilizar los MASC para descongestionar el sistema penal, respondiendo a las necesidades del contexto actual.

Objetivos

Objetivo General

Analizar la viabilidad jurídica y efectividad de los mecanismos de conciliación como alternativa para la reparación integral del daño en las víctimas de fraude cibernético en el sector empresarial.

Objetivos específicos

- Identificar las modalidades de fraude cibernético más recurrentes que afectan al sector empresarial y su tratamiento dentro del marco normativo de los delitos conciliables.
- Evaluar las barreras jurídicas y técnicas que limitan el uso de la conciliación en casos de delitos informáticos.
- Proponer criterios orientadores para conciliadores y empresarios que faciliten la estructuración de acuerdos restaurativos enfocados en la reparación económica y la mitigación de riesgos digitales.

Marco Referencial

Antecedentes

En Colombia la transformación digital ha traído consigo un incremento exponencial en la criminalidad informática. Según Castillo y Jiménez (2024), el *phishing* y el *ransomware* se han consolidado como las modalidades más frecuentes, afectando gravemente la privacidad y la seguridad financiera del sector empresarial. Esta realidad es respaldada por la Fiscalía General de la Nación en su Cartilla Metodológica de Atención de Delitos Informáticos (s.f.), donde se enfatiza que el aumento del uso de las TIC ha derivado en una problemática creciente de afectación a los datos y al patrimonio económico.

A nivel sectorial, estudios de la Cámara Colombiana de Comercio Electrónico (2023) reportan que un alto porcentaje de usuarios y empresas experimentan fraudes relacionados con pagos en línea y transacciones en redes sociales. La gravedad de este fenómeno se refleja en el informe *El verdadero costo del fraude en América Latina* de LexisNexis, el cual señala que cada peso perdido por fraude en Colombia cuesta a las empresas 3.76 veces más debido a los costos operativos y de satisfacción al cliente asociados, afectando la competitividad del país.

Desde el ámbito normativo, la Ley 1273 de 2009 introdujo el marco jurídico para la protección de la información y los datos, tipificando delitos como el acceso abusivo a sistemas informáticos y la transferencia no consentida de activos. No obstante, expertos en videoconferencias académicas sobre delitos informáticos advierten que la elaboración

jurisprudencial en esta área es aún limitada debido a las dificultades técnicas en la judicialización efectiva y la obtención de pruebas digitales.

En lo referente a la solución de conflictos, se ha planteado que las Tecnologías de la Información y la Comunicación (TIC) son herramientas clave para disminuir la congestión judicial y los costos asociados al litigio. En efecto, Guevara y Botero (2024) destacan que la virtualidad y el uso de medios digitales permiten una mayor eficacia en las audiencias, facilitando que el arbitraje y la conciliación operen con mayor agilidad frente a controversias empresariales.

Por otra parte, autores como Guerra et al. (2020) definieron la reparación integral como un derecho que incluye la restitución, la indemnización y la satisfacción. En materia de delitos contra el patrimonio económico, como el hurto por medios informáticos, la jurisprudencia ha reconocido que la reparación efectiva puede dar lugar a beneficios procesales como la rebaja de penas, lo que abre una puerta jurídica para que la conciliación actúe como un mecanismo de justicia restaurativa eficiente.

A pesar de estos avances, existe una tensión entre la rigidez del procedimiento penal y la necesidad de soluciones rápidas para el empresario defraudado. Las fuentes coinciden en que, si bien existen los instrumentos legales, hay una subutilización de los Mecanismos Alternativos de Solución de Conflictos (MASC) debido a la falta de protocolos específicos para tasar daños digitales y la complejidad de identificar al victimario en entornos anonimizados (León, 2025).

De esta manera se observa que, mientras la persecución penal es el enfoque dominante, la literatura académica no profundiza lo suficiente en cómo estructurar

acuerdos conciliatorios que aseguren la recuperación real de los activos en el fraude cibernético empresarial. Este anteproyecto se conecta con esta necesidad, buscando ofrecer criterios claros para que la conciliación sea una alternativa de reparación integral en el marco de la seguridad jurídica corporativa.

Marco teórico

La base conceptual de la investigación se fundamenta en la comprensión del ciberdelito como una transgresión a la seguridad jurídica empresarial. En esta línea, autores como Cámara (2020) sostienen que la cibercriminología debe analizarse desde la oportunidad que brindan los entornos digitales, donde la asimetría de información entre el victimario y el empresario facilita el fraude. Esta perspectiva permite entender que el fenómeno investigado no es un hecho aislado, sino una conducta sistémica que requiere un lente jurídico capaz de adaptarse a la desmaterialización del objeto delictivo y a la celeridad de las transacciones electrónicas.

En este sentido, el fraude informático se operacionaliza bajo la doctrina de Roxin (1997) y su teoría de la imputación objetiva, adaptada a la protección de bienes jurídicos patrimoniales en la red. Para este estudio, el fraude no se limita a la mera estafa, sino que se entiende como la manipulación de datos o sistemas para generar un perjuicio económico, tal como lo define la Ley 1273 de 2009 en el contexto colombiano (Castillo, 2017). Esta definición es crucial para delimitar qué conductas son susceptibles de ser llevadas a una mesa de conciliación, separando aquellas que afectan meramente el patrimonio de aquellas que vulneran el orden público informático de manera irreversible.

Por otro lado, la investigación adopta el enfoque de la Justicia Restaurativa, teorizada por autores como Howard Zehr (2010). Según Zehr (2010), el delito debe entenderse primordialmente como una violación a las personas y a las relaciones, más que como una simple infracción a la ley. Este modelo es pertinente para el ámbito empresarial, ya que desplaza el eje de la retribución penal hacia la reparación del daño. En el fraude cibernético, la prioridad del empresario suele ser la recuperación de la liquidez y la mitigación del impacto operativo, objetivos que la justicia restaurativa, a través del diálogo mediado, puede satisfacer de manera más eficiente que la sanción privativa de la libertad.

Articulado con lo anterior, se incorpora la Teoría del Conflicto de Entelman (2002), quien plantea que los métodos alternativos de resolución deben fundamentarse en la autonomía de la voluntad y en la gestión inteligente de los intereses en disputa. La conciliación, vista desde Entelman, deja de ser un simple trámite procesal para convertirse en un espacio de administración de justicia por los propios actores. En casos de fraude digital, donde la prueba técnica es compleja y costosa, la aplicación de esta teoría justifica la elección de la conciliación como una vía estratégica para resolver la controversia de manera ágil, evitando el desgaste de un litigio de resultado incierto.

En este orden de ideas, el andamiaje teórico permite establecer que el fenómeno requiere un análisis cualitativo. Por ende, la integración de las posturas teóricas permite subrayar que la conciliación es un mecanismo de descongestión judicial y una herramienta de protección para el sector empresarial.

Metodología

Esta investigación es de tipo cualitativo, en tanto permite comprender la complejidad del fraude cibernético y la eficacia de la conciliación desde una perspectiva interpretativa y jurídica, más allá de la medición estadística. El alcance del estudio es descriptivo-analítico, ya que se orienta a caracterizar las modalidades delictivas actuales y a evaluar la pertinencia de los mecanismos de resolución de conflictos en el marco legal vigente. El diseño metodológico es documental y no experimental, basándose en el análisis sistemático de fuentes normativas, jurisprudenciales y doctrinales sin la manipulación directa de variables.

La unidad de análisis está constituida por el marco jurídico de los delitos informáticos en Colombia y los protocolos de actuación de los centros de conciliación frente a disputas patrimoniales. La población objeto de referencia son los empresarios afectados por conductas fraudulentas digitales y los conciliadores extrajudiciales. Para la recolección de información, se utilizarán fuentes secundarias, tales como bases de datos jurídicas, jurisprudencia y documentos institucionales.

Para el cumplimiento de los objetivos planteados se establecieron las siguientes fases:

Primero, se llevó a cabo un diagnóstico que se centró en la identificación de las modalidades de fraude cibernético con mayor impacto en el sector corporativo durante el periodo de estudio. Como técnica de recolección se utilizó el rastreo institucional y estadístico, empleando como instrumentos las matrices de vaciado de datos aplicadas a los

boletines de criminalidad del Centro Cibernético de la Policía Nacional y la Fiscalía General de la Nación. Mediante estos instrumentos se categorizaron variables como el phishing, el acceso abusivo a sistemas informáticos, evaluando su frecuencia y el volumen del impacto patrimonial sobre las unidades productivas.

Segundo, se estableció un análisis normativo que se orientó a la evaluación de la viabilidad de los Mecanismos Alternativos de Solución de Conflictos (MASC) frente a las conductas informáticas previamente tipificadas. La técnica principal fue la revisión documental analítica. De esta manera se planteó un contraste entre normativas y líneas jurisprudenciales de las Cortes con respecto a los conceptos de delitos querellables, orden público informático y los límites de la autonomía de la voluntad en la cuantificación de los perjuicios económicos.

Tercero, se formularon criterios donde se integraron los hallazgos de la literatura frente la realidad para construir una propuesta restaurativa. Esto se realizó mediante una triangulación conceptual, la cual permitió cruzar los autores, los modelos, los principios y la voz de los investigadores. A partir del análisis se derivaron planteamientos propositivos encaminados a brindar herramientas a los conciliadores, así como técnicas para el resarcimiento del daño digital empresarial con celeridad y ajustado al marco normativo vigente.

Resultados y Discusión

Modalidades de fraude cibernético más recurrentes

El primer objetivo específico estuvo orientado hacia la caracterización de las modalidades de fraude cibernético con mayor incidencia y generación de daño económico en el sector empresarial. Los datos encontrados por Malagón (2023) revelan que el fenómeno de la defraudación digital ya no se manifiesta a través de ataques indeterminados a la infraestructura de red; por el contrario, se lleva a cabo mediante sofisticadas estrategias de ingeniería social y manipulación de datos orientadas al desvío directo de activos económicos. Entre estas prácticas, el *phishing* corporativo y el compromiso de correos electrónicos empresariales (conocido en la doctrina transnacional como fraude BEC o *Business Email Compromise*) se consolidan como las modalidades más frecuentes debido a la asimetría de información que generan entre las dependencias financieras de las empresas y los delincuentes.

Desde una perspectiva dogmática, cabe señalar que estas conductas encuentran su tipificación principal en la Ley 1273 de 2009, la cual introdujo modificaciones sustanciales al Código Penal Colombiano al crear el bien jurídico tutelado de la protección de la información y de los datos. Específicamente, las maniobras fraudulentas empresariales analizadas encuadran en los tipos penales del artículo 269F (Violación de datos personales) y, de manera prevalente, el artículo 269I (Transferencia no consentida de activos). Este último tipo penal resulta medular para los intereses de esta investigación, por cuanto describe la conducta de quien, con ánimo de lucro y valiéndose de alguna manipulación

informática, logra la transferencia no consentida de cualquier activo en perjuicio de un tercero.

Vale la pena destacar que la delimitación tipológica se hace evidente al confrontar la naturaleza de estas conductas con el marco normativo de los delitos querellables y conciliables en Colombia. De acuerdo con el artículo 74 de la Ley 906 de 2004 (Código de Procedimiento Penal), modificado por legislaciones subsiguientes, los delitos informáticos de contenido eminentemente patrimonial no se encuentran expresamente excluidos de la categoría de querellables, siempre que no concurren circunstancias de agravación punible que afecten de manera directa el orden público o los bienes del Estado. Esta condición inicial habilita formalmente la aplicación del artículo 522 del mismo estatuto procesal, el cual preceptúa la conciliación como un requisito de procedibilidad obligatorio para ejercer la acción penal en los delitos que exigen querrela legítima.

No obstante, al profundizar en el análisis normativo, surge una importante distinción dogmática entre los tipos penales concurrentes en un fraude digital empresarial. Mientras que el artículo 269I (Transferencia no consentida de activos) comparte una estructura análoga a la estafa tradicional al lesionar exclusivamente el patrimonio económico del sujeto pasivo, conductas aliadas como el artículo 269A (Acceso abusivo a un sistema informático) o el artículo 269G (Suplantación de sitios web para capturar datos personales) lesionan la seguridad informática del Estado y de la sociedad.

Según Posada (2012), esta conducta delictiva genera un complejo debate jurídico, dado que, si un mismo fraude corporativo involucra el acceso no autorizado a bases de datos protegidas, la Fiscalía General de la Nación suele iniciar la acción penal de oficio,

restringiendo significativamente el margen de maniobra para un acuerdo conciliatorio extrajudicial directo entre el empresario y el victimario.

A pesar de esta aparente restricción, los resultados de la revisión jurisprudencial indican que la Corte Suprema de Justicia, mediante providencia SP1245 de 2015, ha sostenido una línea interpretativa que privilegia el principio de lesividad material frente a la rigidez formal de la tipicidad concurrente. Cuando el daño derivado del ciberdelito se reduce estrictamente a una afectación patrimonial cuantificable y resarcible para el empresario individual, y el infractor manifiesta su voluntad de reparar el perjuicio, la administración de justicia penal tiende a flexibilizar la persecución punitiva.

En estos escenarios, el acuerdo restaurativo alcanzado en un centro de conciliación extrajudicial opera con plenos efectos jurídicos, viabilizando fenómenos procesales definitivos como la preclusión de la investigación penal o la extinción de la acción, conforme a los postulados del bloque de constitucionalidad que prioriza la solución pacífica de los conflictos.

Como complemento a lo que se viene mencionando, la entrada en vigencia del Estatuto de Conciliación entró a fortalecer los mecanismos procesales para instrumentalizar estos acuerdos en materia penal. El estatuto refuerza el valor del acta de conciliación extrajudicial como un documento dotado de los atributos de mérito ejecutivo y tránsito a cosa juzgada, otorgándole al empresario defraudado un título valor incuestionable para exigir el cumplimiento coercitivo de las obligaciones económicas pactadas en la mesa de negociación (Marimón, 2025). Esto significa que si el delincuente cibernético acuerda devolver los fondos sustraídos a cambio del desistimiento de la

querella por parte de la víctima, el ordenamiento jurídico provee las garantías sustanciales necesarias para que dicho pacto no degenere en una nueva burla a los derechos del comerciante.

Llegados a este punto, conviene detenerse a decir que los hallazgos de este estudio evidencian una desconexión entre la disponibilidad teórica de este marco normativo y la realidad operativa de los centros de conciliación. El Ministerio de Justicia (2024) demuestra que la tasa de conciliaciones extrajudiciales intentadas o tramitadas con éxito en casos de fraude informático corporativo es estadísticamente marginal.

Esta subutilización crónica está motivada, en primer término, por una barrera de carácter cognoscitivo e institucional: la mayoría de los asesores jurídicos corporativos y los propios operadores de los centros de conciliación tienden a asimilar de manera automática el ciberdelito con una conducta exclusivamente punible e innegociable, obviando que la pretensión última del empresario víctima no es el encarcelamiento del autor, sino el restablecimiento del flujo de caja de su organización (Ministerio de Justicia, 2024).

Por otra parte, la discusión jurídica debe incorporar las complejidades de orden técnico-probatorio que condicionan la viabilidad de la conciliación en el entorno digital. Conforme lo establece Medina (2025), a diferencia de las conductas civiles o comerciales tradicionales, donde las obligaciones y los daños constan en soportes documentales físicos de fácil verificación, en el fraude informático la demostración del daño material y la identificación inequívoca de la contraparte dependen de peritajes forenses digitales complejos.

Si el conciliador o el empresario carecen de herramientas metodológicas para tasar con precisión el costo directo de la transferencia ilícita de activos, los gastos incidentales de contingencia y el lucro cesante derivado del ataque, la formulación de propuestas de arreglo equitativas se torna inviable, frustrando la posibilidad de un consenso restaurativo en etapas tempranas (Medina, 2025).

A su vez, resulta necesario analizar acá el factor de la competencia territorial puesto que se convierte en un desafío para la conciliación extrajudicial, particularmente cuando se trata de un delito que no cuenta con fronteras delimitadas. Mientras que la Ley 2220 de 2022 asume que las partes en conflicto poseen una ubicación geográfica determinable para efectos de notificación y comparecencia, el fraude cibernético empresarial suele ejecutarse mediante arquitecturas de red anonimizadas o desde jurisdicciones extranjeras.

Frente a esta realidad, los resultados de este artículo demuestran que la implementación de las audiencias virtuales de conciliación, potenciadas inicialmente durante la crisis sanitaria y decantadas normativamente en el ordenamiento actual, constituye un avance procesal indispensable, pero ineficaz si no se acompaña de mecanismos que permitan la vinculación jurídica y formal de sujetos cuya identidad real se encuentra oculta tras una dirección IP (Espinosa, 2024).

Como se ha podido evidenciar hasta el momento, el análisis de las modalidades delictivas y el régimen legal de los MASC permite determinar que el ordenamiento jurídico colombiano ofrece un ecosistema normativo formalmente apto para la resolución conciliatoria del fraude cibernético empresarial, estructurado sobre la reparación integral.

No obstante, la efectividad real de esta alternativa jurídica se encuentra supeditada a la superación de los sesgos doctrinales que insisten en la primacía de la sanción privativa de la libertad sobre el resarcimiento económico y a la urgente adopción de protocolos técnicos que guíen al conciliador en el manejo de controversias virtuales de alta complejidad patrimonial.

Barreras jurídicas y técnicas que limitan el uso de la conciliación en casos de delitos informáticos

Continuando con la presentación de estos resultados, el segundo objetivo específico que se planteó propendía por evaluar las barreras jurídicas y técnicas que limitan el uso de la conciliación en casos de delitos informáticos. En este sentido, la revisión documental permite encontrar que, a pesar de la existencia de un marco normativo aparentemente favorable para los MASC, la aplicación de la conciliación en el fraude informático empresarial se encuentra drásticamente constreñida por barreras de índole jurídica y dogmática.

Una de estas limitaciones se halla precisamente en la naturaleza de los delitos informáticos que se encuentra consagrada en la Ley 1273 de 2009. En efecto, mientras un fraude tradicional lesiona de forma exclusiva el patrimonio económico del empresario, el ciberdelito suele materializarse mediante el quiebre de la seguridad informática del Estado o de la sociedad, vulnerando bienes jurídicos que desbordan el interés privado de las partes. Esta concurrencia de conductas delictivas ata de manos a los operadores jurídicos, pues la Fiscalía General de la Nación se ve obligada a impulsar la acción penal de oficio respecto

a los tipos no querellables, imposibilitando que un acuerdo sobre la cuantía económica extinga de manera definitiva la persecución estatal.

A esta restricción dogmática se suma una contradicción procesal derivada de la Ley 906 de 2004 y su articulación con la Ley 2220 de 2022. La conciliación extrajudicial en el derecho penal requiere la plena identificación e individualización de los intervinientes para garantizar la validez del consentimiento y la posterior exigibilidad del acta en caso de incumplimiento. Pero el fraude cibernético corporativo se caracteriza por el uso sistemático de tácticas de anonimización, suplantación de identidades, redireccionamiento de redes *proxy* y el empleo de criptoactivos en cadenas de bloques descentralizadas para el lavado del capital sustraído. La asimetría técnica existente entre la capacidad de ocultamiento del ciberdelincuente y las limitadas facultades de investigación de un centro de conciliación privado levanta un muro insalvable; sin un sujeto plenamente identificado a quien convocar, la mesa de negociación carece de viabilidad procesal desde su origen (Acosta et al., 2020).

Otra barrera que se encontró es la cuantificación del daño en los entornos virtuales. Por ejemplo, en el campo civil o comercial ordinario, el conciliador cuenta con elementos como facturas, contratos físicos, letras de cambio o peritajes contables estandarizados que facilitan la construcción de fórmulas de arreglo equitativas. Por el contrario, Poveda (2022) encuentra que en el fraude informático empresarial el daño patrimonial abarca también el lucro cesante derivado de la pausa operativa, los costos de los efectos sobre la tecnología y la infraestructura de la red; las multas por la filtración de datos personales de clientes y el daño reputacional corporativo. Por eso es que la ausencia de protocolos técnicos que

guíen al conciliador a discernir y valorar económicamente estos intangibles digitales convierte la negociación en un ejercicio empírico e incierto, propenso a generar acuerdos lesivos o inejecutables.

Por su parte, es necesario hablar de la volatilidad de la evidencia digital y cómo esto constituye una barrera importante a tener en cuenta en la conciliación extrajudicial. Resulta que la demostración de la existencia del fraude y de su nexo causal con el presunto victimario depende de registros de auditoría de servidores (logs), análisis forenses informáticos, metadatos y cadenas de custodia de evidencias electrónicas que son altamente susceptibles de alteración o borrado remoto. Un centro de conciliación carece de la potestad coercitiva para decretar inspecciones judiciales anticipadas o asegurar la conservación de las pruebas técnicas (Acosta et al., 2020).

Por consiguiente, si el empresario acude a la conciliación sin un acervo probatorio digital previamente consolidado y blindado por expertos, se expone a una situación de indefensión absoluta, donde la contraparte puede destruir la evidencia del ilícito con un solo comando informático, desvaneciendo cualquier incentivo para transar.

Asimismo, es imperativo examinar la desconexión geográfica y la transnacionalidad del delito como una limitante de carácter operativo. La Ley 2220 de 2022 establece la conciliación sobre supuestos de vecindad legal, competencia territorial y notificaciones personales eficientes. Sin embargo, los ataques de fraude corporativo que sufren las organizaciones locales son ejecutados con frecuencia por redes criminales situadas en jurisdicciones extranjeras, protegidas por vacíos de cooperación judicial internacional y por la fragmentación normativa global.

Aunque el ordenamiento jurídico de Colombia faculta y promueve la realización de audiencias de conciliación virtuales, la operatividad de estas plataformas digitales se torna estéril cuando el infractor se encuentra fuera del alcance del brazo coercitivo del Estado, haciendo fácticamente imposible su comparecencia y reduciendo la posibilidad del acuerdo restaurativo a una mera utopía jurídica (Poveda, 2022).

Resulta posible decir además que existe una barrera de carácter cognoscitivo e institucional referida a la formación de los operadores jurídicos en la era digital. El análisis cualitativo de este estudio devela que la gran mayoría de los conciliadores inscritos en los centros oficiales del país poseen una sólida formación en derecho sustancial civil, de familia o comercial tradicional, pero exhiben un preocupante analfabetismo funcional en materia de ciberseguridad, arquitectura de software y delitos informáticos (Peña, 2018).

Este vacío de competencias técnicas impide según Peña (2018) que el director de la audiencia comprenda a cabalidad el funcionamiento técnico de la maniobra engañosa puesta bajo su conocimiento, inhabilitándolo para proponer fórmulas de arreglo realistas, evaluar los riesgos de seguridad jurídica de las partes o detectar fraudes procesales perpetrados a través de los mismos medios virtuales de la audiencia.

En este punto solo resta mencionar la barrera de la rigidez formal de las instituciones financieras, las cuales actúan como un obstáculo indirecto en todo el proceso de conciliación. Es evidente en muchos casos de fraude digital que las empresas cuentan con pólizas de ciberriesgo o pretenden responsabilizar a las entidades bancarias por fallas en los sistemas de autenticación y custodia de los fondos.

No obstante, las cláusulas generales de estas corporaciones suelen prohibir expresamente que el asegurado o el cuentahabiente celebre acuerdos conciliatorios o transacciones directas con terceros sin su autorización previa, so pena de perder el derecho a la indemnización correspondiente. Esta dinámica comercial desplaza la solución del conflicto de la esfera ágil de los MASC hacia el litigio contencioso o la reclamación administrativa ordinaria, sacrificando la rapidez del resarcimiento económico en aras de un debate de responsabilidad contractual de largo aliento (Feres, 2023).

Propuesta de criterios orientadores para conciliadores

Como resultado de la investigación se tomó la decisión de ir más allá del diagnóstico y utilizar los hallazgos para proponer algunos criterios que orienten a los conciliadores.

El primer criterio que se establece es la necesidad de determinar integralmente el daño digital. Para ello se requiere romper con la visión tradicional de tasar el conflicto exclusivamente sobre la base de la cuantía neta sustraída en la transferencia no consentida de activos. Retomando la investigación de Poveda (2022), los operadores jurídicos deben guiar a las partes para incorporar de manera explícita en el acuerdo los costos asociados a la remediación informática, los honorarios de los peritos forenses, el lucro cesante derivado de la parálisis operativa y las contingencias por eventuales sanciones administrativas en materia de protección de datos. La inclusión de estas variables garantiza una verdadera reparación integral, alineada con los estándares de la justicia restaurativa, evitando que el

acta de conciliación sea impugnada posteriormente por lesión enorme o vicios en el consentimiento.

Otro de los criterios que se pueden proponer es la necesidad de brindar la exigibilidad operativa y las cláusulas de transición tecnológica. Dado que el cumplimiento de un acuerdo económico por parte de un ciberinfractor suele diferirse en el tiempo mediante cuotas o retornos indexados, el acta de conciliación debe estructurarse como un título ejecutivo complejo, vinculando garantías reales o virtuales que minimicen el riesgo de una nueva burla a la víctima. En este sentido, se propone la inclusión de cláusulas de aceleración de la obligación ante el primer incumplimiento y la fijación de penalidades comerciales estrictas.

Así mismo, el acuerdo debe plasmar compromisos de transparencia tecnológica por parte del convocado, tales como la entrega controlada de información que permita rastrear los activos remanentes o cooperar en la identificación de otros nodos de la red criminal, transformando el escenario conciliatorio en un catalizador de ciberseguridad para la organización afectada (Correa y Mira, 2023).

Por otra parte, los hallazgos de la revisión documental posibilitan proponer que se requiere gestionar los riesgos con terceros institucionales, este es un aspecto crítico para los empresarios que buscan salvaguardar sus pólizas de ciberriesgo o sus relaciones contractuales con el sector bancario. Los lineamientos propuestos determinan que el proceso de conciliación extrajudicial no debe adelantarse de manera aislada a las reclamaciones financieras.

El empresario debe exigir la vinculación formal o, en su defecto, la notificación expresa de la aseguradora y de la entidad bancaria respectiva en las etapas preliminares de la negociación. Al estructurar el acuerdo bajo el principio de subrogación de derechos o mediante pactos de distribución de responsabilidad concurrente, se evita la caducidad de los seguros corporativos y se viabilizan fórmulas de arreglo donde el infractor resarce directamente el deducible o la porción del daño no cubierta por el sistema financiero, optimizando la recuperación líquida de la empresa.

Sin lugar a duda, como se viene enfatizando a lo largo de este artículo un criterio fundamental es que los centros de conciliación deben adoptar protocolos de asignación de casos especializados, asegurando que las controversias por delitos de la Ley 1273 de 2009 sean dirigidas por abogados con formación acreditada en derecho informático, prueba digital o seguridad de la información. De esta manera, quien dirige las audiencias precisa actuar como un mediador técnico apto para comprender los dictámenes forenses aportados por el empresario y para evaluar la viabilidad fáctica de las propuestas de pago, especialmente cuando estas involucren la transferencia de activos digitales o la dación en pago de bienes tecnológicos.

Para cerrar con los criterios, una de las propuestas más significativas es promover una cultura de la autocomposición y desmitificación del enfoque punitivo en los entornos corporativos. A esta reflexión se llega luego de revisar toda la documentación que hizo parte de este corpus y se puede subrayar que los asesores jurídicos de las empresas deben ser instruidos bajo el lineamiento de que, en la economía digital globalizada, la celeridad

en la recuperación del flujo de caja prevalece sobre la expectativa retributiva del encarcelamiento del infractor.

En este sentido, como bien lo indica Poveda (2022), el éxito de la gestión del riesgo legal ante un ciberataque debe medirse por la capacidad de restablecer la estabilidad operativa y financiera de la organización en el menor tiempo posible. Al posicionar la conciliación extrajudicial virtual como la primera línea de defensa y respuesta post-incidente, el empresariado colombiano no solo adopta un modelo de gestión de conflictos moderno y eficiente, sino que contribuye activamente a la descongestión del aparato judicial del Estado, demostrando que la autonomía de la voluntad es un instrumento de protección económica tan poderoso como la misma sanción penal.

Conclusiones

El estudio realizado permite concluir que los MASC se consolidan como una alternativa jurídica y económica altamente efectiva para garantizar la reparación integral del daño frente al fraude cibernético empresarial. Al confrontar los hallazgos con la pregunta de investigación, se demuestra que la autonomía de la voluntad permite superar la rigidez del sistema penal ordinario, el cual se enfoca en el castigo punitivo pero posterga el resarcimiento financiero. La conciliación, operada bajo los parámetros de la Ley 2220 de 2022, provee al empresario afectado un escenario ágil para pactar la devolución de los activos defraudados mediante actas con mérito ejecutivo, salvaguardando la liquidez y la continuidad de las organizaciones en tiempos de crisis digital.

En este orden de ideas, en relación con el primer objetivo específico se concluye que la idoneidad procesal de la conciliación depende estrictamente de la delimitación tipológica y patrimonial del fraude sufrido. Conductas recurrentes como la transferencia no consentida de activos (Artículo 269I de la Ley 1273 de 2009) revisten una naturaleza eminentemente resarcible y transable por afectar de forma exclusiva los recursos de particulares.

No obstante, cuando las maniobras delictivas involucran una afectación concurrente a la seguridad informática colectiva mediante accesos abusivos no querellables, la procedibilidad del acuerdo se restringe sustancialmente. Por ende, el éxito de la autocomposición del conflicto radica en aislar el debate sobre los perjuicios económicos materiales del trámite estrictamente punitivo que el Estado impulsa de oficio.

En lo que respecta al segundo objetivo específico se puede concluir que el despliegue efectivo de la justicia restaurativa en el entorno virtual se encuentra severamente condicionado por barreras de orden técnico-probatorio y deficiencias cognoscitivas. El anonimato que facilitan las redes cibernéticas, la volatilidad intrínseca de la evidencia electrónica y el analfabetismo funcional de los operadores jurídicos en materia de seguridad informática representan obstáculos críticos que suelen frustrar las audiencias de conciliación antes de su inicio. A su vez, las restricciones contractuales impuestas de forma indirecta por aseguradoras y entidades bancarias desvían los litigios hacia la vía ordinaria, evidenciando que el aparato institucional requiere con urgencia una transición conceptual para asimilar el fraude digital como un fenómeno transable y cuantificable.

Frente al tercer objetivo se establece que la viabilidad futura de los MASC frente al cibercrimen corporativo se puede fortalecer con la adopción de los criterios orientadores propuestos en este trabajo. La implementación de metodologías para la tasación integral del daño digital, que incluyan la remediación tecnológica y el lucro cesante, junto con protocolos estrictos de validación de identidad virtual y la vinculación de terceros institucionales, protege los acuerdos contra eventuales fraudes procesales. Al posicionar la conciliación extrajudicial virtual como la primera línea de respuesta legal y operativa post-incidente, el empresariado colombiano asegura una recuperación patrimonial rápida, al tiempo que promueve una cultura de paz social y eficiencia que alivia de manera directa la saturación del aparato de justicia penal del Estado.

Referencias

- Acosta, M., Benavides, M., y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, 25(89). <https://www.redalyc.org/journal/290/29062641023/html/>
- Arboleda, A. P., Huertas, O., Gómez, C. A., y Blanco, C. (2023). Reflexiones acerca de los mecanismos alternativos de solución de conflictos en época de pandemia y su aplicación a través de los medios digitales en Colombia. *Revista Facultad de Derecho y Ciencias Políticas*, 53(138), 1-24. <https://doi.org/10.18566/rfdcp.v53n138.a12>
- Cámara Colombiana de Comercio Electrónico (2023). *El 19% de los usuarios colombianos de e-commerce experimentaron fraude en el último año*. <https://ccce.org.co/noticias/el-19-de-los-usuarios-colombianos-de-e-commerce-experimentaron-fraude-en-el-ultimo-ano/>
- Cámara, S. (2020). *La Cibercriminología y el perfil del ciberdelincuente*. Derecho y Cambio Social.
- Castillo, L., y Jiménez, J.F. (2024). Cooperación internacional policial ante amenazas cibernéticas en Colombia: Modalidad Business Email Compromise. *Revista Logos Ciencia y Tecnología*, 16(1), 24-42. <https://doi.org/10.22335/rlet.v16i1.1877>
- Castillo, O. (2021). *Phishing: día de pesca*. [Tesis de maestría, Universidad Externado de Colombia].

- <https://bdigital.uexternado.edu.co/server/api/core/bitstreams/e8eac144-41c1-4efe-a7a8-85d8f4f93097/content>
- Congreso de Colombia. (31 de agosto de 2004). *Ley 906 de 2004*. Diario Oficial: 45.658.
http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html
- Congreso de Colombia. (5 de enero de 2009). *Ley 1273 de 2009*. Diario Oficial: 47.223.
http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
- Corte Suprema de Justicia, Sala de Casación Penal. (11 de febrero de 2015). *SP1245-2015*.
 [MP. Eyder Patiño Cabrera]. <https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf>
- Entelman, R. (2002). *Teoría de Conflictos. Hacia un nuevo paradigma*. Gedisa.
- Espinosa, A. (25 de octubre de 2024). *Principios de la conciliación presencial, digital o electrónica o mixta, Ley 2220 de 2022*.
<https://bloque10.unimagdalena.edu.co/principios-de-la-conciliacion-presencial-digital-o-electronica-o-mixta-ley-2220-del-2022/>
- Feres, W. (2023). *Discrecionalidad del asegurador, sus potestades y limitaciones*. [Tesis de maestría, Universidad Externado de Colombia].
<https://bdigital.uexternado.edu.co/server/api/core/bitstreams/d146f901-fec7-429c-bd7e-60edd88427a5/content>
- Fiscalía General de la Nación. (s.f.). *Cartilla Metodológica de Atención de Delitos Informáticos*. <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf>

- Guerra, D., Pabón, L., y Ramírez, D.M. (2020). La reparación integral como principio prevalente en la responsabilidad del estado -una visión a partir de la jurisprudencia de la Corte Constitucional y del Consejo de Estado colombiano. *Revista Republicana*, 28(1), 22-56. <https://doi.org/10.21017/rev.repub.2020.v28.a77>
- Guevara, L.J., y Botero, L. (2024). El impacto de las tecnologías en el proceso judicial: una mirada a partir de los conceptos de juez digital y debido proceso. *Novumjus*, 18. <https://novumjus.ucatolica.edu.co/article/view/5919>
- León, G. (2025). La incorporación de los métodos alternativos de solución de controversias a la insolvencia empresarial. *Revista Javeriana*, 7(4). [https://revistas.javeriana.edu.co/files-articulos/VJ/74\(2025\)/6722763021/index.html](https://revistas.javeriana.edu.co/files-articulos/VJ/74(2025)/6722763021/index.html)
- Malagón, J.C. (2023). *Análisis de las técnicas de ingeniería social que amenazan la seguridad informática de usuarios de entidades financieras*. [Tesis de especialización, UNAD]. <https://repository.unad.edu.co/bitstream/handle/10596/55080/%20http%3Fsequence%3D3>
- Marimón, T.F. (26 de febrero de 2025). *Un análisis introductorio del Estatuto de Conciliación: Qué ha cambiado y el porqué del cambio*. <https://procesal.uexternado.edu.co/un-analisis-introductorio-del-estatuto-de-conciliacion-que-ha-cambiado-y-el-porque-del-cambio/>
- Medina, N.E. (2025). *Desafíos para la valoración de la evidencia digital en el proceso civil colombiano*. [Tesis de maestría, Universidad Externado de Colombia].

- <https://bdigital.uexternado.edu.co/server/api/core/bitstreams/63d03105-6db0-4305-9ffc-2c13007ac31d/content>
- Ministerio de Justicia. (2024). *Análisis de contexto de los casos atendidos por la conciliación extrajudicial en derecho y su comparación con la jurisdicción ordinaria en Colombia*. Minjusticia. <https://www.minjusticia.gov.co/programas-co/MASC/Documents/SICAAC-Documentos/Analisis-contexto-OECD-2023.pdf>
- Mira, A., y Correa, O. (2023). *Las Actas de Conciliación como títulos ejecutivos frente a obligaciones modales*. Universidad Libre. <https://repository.unilibre.edu.co/bitstream/handle/10901/26000/Las%20Actas%20de%20Conciliacio%cc%81n%20como%20ti%cc%81tulos%20ejecutivos%20frente%20a%20obligaciones%20modales%20.pdf?sequence=2&isAllowed=y>
- OEA. (2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*. <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>
- Peña, H. (2018). Panorama de las necesidades jurídicas en los centros de conciliación y arbitraje de Colombia. *Pensamiento Jurídico*, 48(1), 185-232. <https://vlex.com.co/vid/panorama-necesidades-juridicas-centros-760205297>
- Posada, R. (2012). El delito de transferencia no consentida de activos. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 8(1), 1-27.
- Poveda, J.D. (2022). *La conciliación virtual en Colombia: evaluación de sus retos, ventajas y desventajas*. [Trabajo de grado, Universidad Militar Nueva Granada].

<https://repository.umng.edu.co/server/api/core/bitstreams/62d461c7-bd28-4787-82a3-cfa7ce917935/content>

Roxin, C. (1997) *Derecho Penal Parte General, Tomo I, Fundamentos, La Estructura de la Teoría del Delito*. Civitas.

Sánchez, Z. (2017). *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia*. UNAD.

Zehr, H. (2010). *Justicia Restaurativa*. Good Books.