Neutrosophic Computing and Machine Learning, Vol. 42, 2026

University of New Mexico

Diseño de un modelo de gestión de riesgos empresariales basado en principios criminológicos y técnicas criminalísticas para fortalecer el gobierno corporativo.

Design of a business risk management model based on criminological principles and forensic techniques to strengthen corporate governance.

Emilio Josué Ochoa Semeria[1], Domenica Melissa Ochoa Semeria[2]

[1]Licenciatura En Criminologia Y Criminalistica, Universidad Tecnológica Latinoamericana En Linea(Utel) México, Master En Administración De Empresas (Mba), Eidhi International University (Estados Unidos Y México), ochoajosue483@gmail.com, **https://orcid.org/0009-0002-4178-2769**

[2]Médico, Universidad Católica De Cuenca, Posgradista De Psiquiatria En Curso, Universidad De Cuenca. domeochoa97@gmail.com , https://orcid.org/0009-0000-6212-4947

Resumen.

El gobierno corporativo enfrenta actualmente desafíos crecientes derivados del incremento de fraudes, corrupción y delitos empresariales que vulneran la integridad organizacional y la confianza de los stakeholders. Los modelos tradicionales de gestión de riesgos, aunque útiles para identificar riesgos operativos y financieros, presentan limitaciones significativas para anticipar, detectar y mitigar conductas delictivas intencionadas, al carecer de perspectivas criminológicas y técnicas criminalísticas que permitan comprender las motivaciones, modos de operación y evidencias asociadas a estos fenómenos. La presente investigación tuvo como objetivo diseñar un modelo de gestión de riesgos empresariales que integre principios criminológicos y técnicas criminalísticas para fortalecer el gobierno corporativo en organizaciones públicas y privadas. Metodológicamente, el estudio se desarrolló bajo un enfoque mixto, de tipo propositivo, con un diseño no experimental transversal. Se emplearon métodos analíticos, sistémicos, deductivos y comparativos, y se aplicaron técnicas de revisión documental, entrevistas a expertos y encuestas dirigidas a directivos, auditores y especialistas en riesgos, criminología y criminalística. Como resultado principal se obtuvo un modelo estructurado en siete etapas —identificación de riesgos, perfil criminológico, análisis criminalístico, valoración del riesgo, controles preventivos, monitoreo y mejora continua—, integrado por cinco componentes estratégicos: gobierno corporativo y cultura ética; factores criminológicos y perfil del delincuente; técnicas de investigación forense y evidencia digital; gestión administrativa y control interno; y herramientas tecnológicas de inteligencia artificial y alertas tempranas. Se concluye que la integración de la criminología y la criminalística en la gestión de riesgos empresariales permite una identificación más temprana y precisa de riesgos delictivos, fortalece la capacidad de investigación y sanción de irregularidades, y contribuye a una cultura organizacional más ética y resiliente frente a amenazas internas y externas. El modelo propuesto constituye un aporte original que supera los enfoques tradicionales de cumplimiento normativo, al incorporar una visión integral del riesgo delictivo que abarca desde la prevención hasta la investigación y la mejora continua.

Palabras clave: Gobierno Corporativo, Gestión De Riesgos Empresariales, Criminología Corporativa, Criminalística Forense, Compliance, Prevención Del Fraude.

Abstract

Corporate governance currently faces growing challenges derived from the increase in fraud, corruption, and corporate crimes that undermine organizational integrity and stakeholder trust. Traditional risk management models, although useful for identifying operational and financial risks, have significant limitations in anticipating, detecting, and mitigating intentional criminal conduct, as they lack criminological perspectives and forensic techniques to understand the motivations, modus operandi, and evidence associated with these phenomena. This research aimed to design a corporate risk management model that integrates criminological principles and forensic techniques to strengthen corporate governance in public and private organizations. Methodologically, the study was developed under a mixed approach, of a propositional type, with a non-experimental cross-sectional design. Analytical, systemic, deductive, and comparative methods were employed, and documentary review techniques, expert interviews, and surveys directed at managers, auditors, and specialists in risk, criminology, and forensic science were applied. The main result obtained was a model structured in seven stages — risk identification, criminological profile, forensic analysis, risk assessment, preventive controls, monitoring, and continuous improvement— integrated by five strategic components: corporate governance and ethical culture; criminological factors and offender profile; forensic investigation techniques and digital evidence; administrative management and internal control; and technological tools of artificial intelligence and early warning systems. It is concluded that the integration of criminology and forensic science into corporate risk management allows for earlier and more accurate identification of criminal risks, strengthens the capacity for investigation and sanctioning of irregularities, and contributes to a more ethical and resilient organizational culture against internal and external threats. The proposed model constitutes an original contribution that surpasses traditional regulatory compliance approaches by incorporating a comprehensive view of criminal risk that ranges from prevention to investigation and continuous improvement.

Keywords: Corporate Governance, Enterprise Risk Management, Corporate Criminology, Forensic Science, Compliance, Fraud Prevention.

1. Introducción

El gobierno corporativo se ha consolidado como un pilar fundamental para la sostenibilidad y el buen funcionamiento de las organizaciones en el contexto económico actual [1]. Este concepto, que abarca el sistema de relaciones entre la dirección, el consejo de administración, los accionistas y los grupos de interés, proporciona la estructura y los procesos a través de los cuales se dirigen las organizaciones y se supervisa su desempeño [1][2]. Los principios de transparencia, rendición de cuentas, equidad y responsabilidad que sustentan el gobierno corporativo son esenciales para generar confianza entre los inversores y la sociedad en general [1][2]. Una buena gobernanza no solo facilita el acceso a financiación y promueve la innovación, sino que también contribuye a la resiliencia de las corporaciones y, por extensión, a la estabilidad de la economía en su conjunto [1].

A pesar de la creciente sofisticación de los sistemas de control interno y de los marcos normativos, el fraude corporativo y los delitos empresariales han experimentado un incremento preocupante a nivel global [3]. Las organizaciones se enfrentan a amenazas cada vez más diversas y sofisticadas, que van desde el fraude financiero tradicional hasta los delitos informáticos y la corrupción a gran escala [3][4]. Estudios recientes indican que el 89% de los casos de fraude ocupacional corresponden a la apropiación indebida de activos, una modalidad que, aunque no siempre acapara los titulares, representa pérdidas económicas millonarias para las empresas [4]. La complejidad de los entornos empresariales actuales, caracterizados por la interconexión global y la digitalización, ha creado nuevas vulnerabilidades y ha amplificado el impacto de las conductas ilícitas [5][6]. Los delitos de cuello blanco, que incluyen desde el desvío de fondos hasta la falsificación de estados financieros, no solo generan pérdidas económicas directas, sino que erosionan la confianza institucional, dañan la reputación corporativa y pueden comprometer la supervivencia de las organizaciones [4][5][7].

Los modelos tradicionales de gestión de riesgos, si bien han demostrado ser útiles para identificar y mitigar riesgos operativos y financieros, presentan limitaciones significativas cuando se enfrentan a la complejidad de los delitos empresariales [8][9]. Estos enfoques suelen adoptar una perspectiva fragmentada o sectorial, asu-

miendo que los riesgos son fenómenos aislados que pueden gestionarse de manera independiente, lo que resulta inadecuado para abordar amenazas que a menudo son sistémicas e interconectadas [8][9]. Además, los modelos tradicionales tienden a ser reactivos y se centran en el control posterior, en lugar de anticiparse a las conductas ilícitas. En muchas ocasiones, se basan en el supuesto de que los riesgos son eventos discretos y predecibles, lo que les impide captar la naturaleza dinámica y adaptativa de los esquemas de fraude y corrupción [5][10]. La falta de una comprensión profunda de los factores criminológicos que motivan y facilitan el delito en el contexto empresarial deja a las organizaciones expuestas a los denominados "eventos cisne negro" y a amenazas que no se ajustan a los patrones de riesgo predefinidos [5][9][10].

La criminología y la criminalística ofrecen un conjunto de herramientas y perspectivas que pueden complementar y enriquecer significativamente los enfoques tradicionales de gestión de riesgos [11][12]. La criminología corporativa, al analizar las causas, los patrones y las motivaciones del delito en el ámbito organizacional, permite comprender por qué y cómo se cometen los delitos empresariales [5][11]. Teorías como la de la elección racional o la de las actividades rutinarias proporcionan marcos explicativos para anticipar las conductas delictivas y diseñar estrategias de prevención más efectivas [11][12]. Por otro lado, la criminalística aplicada al entorno empresarial, que incluye la auditoría forense y el análisis de evidencia digital, proporciona las técnicas necesarias para investigar, documentar y demostrar la ocurrencia de delitos, fortaleciendo así la capacidad de respuesta y sanción de las organizaciones [12][13]. La integración de estos enfoques permite pasar de una gestión de riesgos basada en el cumplimiento normativo a una gestión más integral, que abarca desde la prevención hasta la investigación y la mejora continua [5][11][12].

A pesar del creciente reconocimiento de la utilidad de la criminología y la criminalística en el ámbito empresarial, existe un vacío científico significativo en la integración sistemática de estos campos en los modelos de gestión de riesgos. Si bien existen marcos normativos como el COSO ERM, la ISO 31000 y las normas de compliance como la ISO 37301 y la ISO 37001, estos no incorporan de manera explícita y estructurada los principios criminológicos y las técnicas criminalísticas [2][10]. La mayoría de los enfoques actuales se centran en el control interno y en el cumplimiento de las normas, sin abordar las causas profundas del comportamiento delictivo ni ofrecer herramientas específicas para la investigación forense en el contexto corporativo [5][12]. Esta carencia limita la capacidad de las organizaciones para anticipar, detectar y responder eficazmente a las amenazas delictivas, dejando un espacio que la presente investigación busca cubrir [5][11].

La justificación de esta investigación radica en la necesidad de proporcionar a las organizaciones un modelo de gestión de riesgos que integre de manera coherente y operativa los principios criminológicos y las técnicas criminalísticas. Se pretende superar las limitaciones de los modelos tradicionales, ofreciendo un enfoque que no solo se anticipe a los riesgos delictivos, sino que también fortalezca la capacidad de investigación y sanción de irregularidades. La creciente sofisticación de los delitos empresariales y el incremento de las exigencias regulatorias en materia de prevención de fraudes y corrupción hacen que esta integración sea no solo oportuna, sino necesaria para fortalecer el gobierno corporativo y proteger los intereses de todas las partes involucradas [3][5][13]. En consecuencia, el objetivo general de esta investigación es diseñar un modelo de gestión de riesgos empresariales que integre principios criminológicos y técnicas criminalísticas para fortalecer el gobierno corporativo en organizaciones públicas y privadas.

2. Fundamentación teórica.

2.1 Gobierno corporativo

El gobierno corporativo se define como el sistema de reglas, prácticas y procesos mediante los cuales las organizaciones son dirigidas y controladas [1]. Este concepto abarca las relaciones entre la dirección, el consejo de administración, los accionistas y los grupos de interés, estableciendo la estructura a través de la cual se fijan los objetivos de la empresa y se determinan los medios para alcanzarlos y supervisar su cumplimiento [1][2]. La importancia del gobierno corporativo radica en su capacidad para generar confianza entre los inversores y la sociedad, reducir los riesgos operativos y legales, y mejorar la calidad de las decisiones estratégicas [1]. El sistema de gobierno corporativo especifica la distribución de derechos y responsabilidades entre los participantes de la organización y establece las reglas y procedimientos para la toma de decisiones, protegiendo así a los accionistas y demás grupos de interés frente a posibles conductas indebidas por parte de la dirección [3].

Los principios del gobierno corporativo constituyen los pilares sobre los que se asienta una buena gobernanza [1][4]. La transparencia exige que las empresas proporcionen información oportuna y precisa sobre todos los asuntos materiales relacionados con su actividad, incluyendo la situación financiera, el desempeño, la estructura de propiedad y la remuneración de los directivos [4]. Este principio busca garantizar que los grupos de interés tengan acceso a la información necesaria para evaluar el desempeño de la organización, sin comprometer los secretos comerciales [4][5]. La rendición de cuentas implica que los responsables de la gestión y los miembros del consejo respondan por sus acciones y decisiones ante la empresa y sus accionistas, actuando siempre en el mejor interés de la organización [1][4]. La equidad asegura el tratamiento justo de todos los accionistas, protegiendo especialmente los derechos de los accionistas minoritarios y de los inversores extranjeros, garantizando que todos los accionistas de la misma clase reciban el mismo trato [4][5]. La responsabilidad, por su parte, implica la obligación de considerar los intereses de todas las personas afectadas por las actividades de la empresa, observando los estándares éticos de las sociedades en las que operan y dando voz a los grupos de interés en los procesos de toma de decisiones [4][5].

Las buenas prácticas de gobierno corporativo han sido codificadas en diversos marcos internacionales que sirven como referencia para las organizaciones públicas y privadas [4][6]. Los Principios de Gobierno Corporativo del G20 y la OCDE, revisados por última vez en 2023, constituyen el estándar global más reconocido en esta materia, ofreciendo recomendaciones sobre los derechos de los accionistas, el papel de los inversores institucionales, la divulgación y transparencia corporativa, las responsabilidades de los consejos de administración y la sostenibilidad y resiliencia de las empresas [6][7][8]. Estos principios, aunque no vinculantes, han sido adoptados por 52 economías y han servido de base para el desarrollo de marcos normativos en numerosos países [7]. La transparencia y la rendición de cuentas se han consolidado como elementos centrales de estos estándares, especialmente relevantes para las empresas que buscan acceder a los mercados de capitales y para las organizaciones que manejan recursos públicos [6].

2.2 Gestión de riesgos empresariales

La gestión de riesgos empresariales se define como el conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al riesgo [19]. Este concepto ha evolucionado desde enfoques tradicionales fragmentados hacia modelos integrales que reconocen la interconexión de las amenazas y su impacto en el logro de los objetivos estratégicos [19]. A diferencia de la gestión de riesgos financieros, que se centra en riesgos específicos como los de mercado, crédito o liquidez, la gestión de riesgos empresariales adopta una perspectiva holística que abarca riesgos operativos, estratégicos, de cumplimiento y reputacionales [19]. Esta visión integrada permite a las organizaciones no solo mitigar amenazas, sino también capitalizar las oportunidades que surgen de la incertidumbre [20].

Los tipos de riesgos que enfrentan las organizaciones son diversos y pueden clasificarse en varias categorías [19]. Los riesgos financieros incluyen aquellos derivados de fluctuaciones en los mercados, como los riesgos de tasa de interés, tipo de cambio y precio de commodities [20]. Los riesgos operativos surgen de fallas en procesos internos, personas o sistemas, abarcando desde errores en la cadena de suministro hasta fraudes internos y ciberataques [19]. Los riesgos estratégicos se relacionan con decisiones que afectan la dirección de la organización, como la entrada a nuevos mercados o el desarrollo de productos innovadores [20]. Los riesgos de cumplimiento y reputacionales están vinculados al incumplimiento de normas legales o a daños a la imagen corporativa [19]. La complejidad del entorno empresarial actual, caracterizado por la globalización y la digitalización, ha multiplicado las fuentes de riesgo y ha hecho indispensable una gestión más sofisticada [20].

El modelo COSO ERM (Enterprise Risk Management – Integrating with Strategy and Performance), publicado en 2017 por el Committee of Sponsoring Organizations of the Treadway Commission, constituye uno de los marcos de referencia más influyentes en la gestión de riesgos empresariales [21]. Este marco supera la versión anterior de 2004 al enfatizar la integración de la gestión de riesgos con la estrategia y el desempeño organizacional [21]. El modelo se estructura en cinco componentes interrelacionados: gobernanza y cultura, estrategia y establecimiento de objetivos, desempeño, revisión y revisión, e información, comunicación y reporte [21]. Cada componente contiene un conjunto de principios que orientan la implementación efectiva del ERM, totalizando veinte principios que abarcan desde la supervisión del riesgo por parte del consejo hasta la comunicación de información sobre riesgos en toda la organización [21]. El marco COSO enfatiza que el riesgo debe considerarse no como un elemento aislado, sino como un factor integrado en la planificación estratégica y en la ejecución de las operaciones diarias [22].

La norma ISO 31000:2018, titulada "Risk management – Guidelines", ofrece un enfoque complementario y de aplicación general para cualquier tipo de organización, independientemente de su tamaño o sector [23]. Esta norma, revisada para simplificar su lenguaje y hacerla más accesible, se fundamenta en la idea de que la gestión del riesgo es parte de la gobernanza y el liderazgo, y es fundamental para cómo se gestiona la organización en

todos los niveles [23]. Sus principios clave incluyen la creación y protección de valor, la integración en los procesos organizacionales, la consideración de factores humanos y culturales, y la mejora continua [23]. La norma establece que la gestión del riesgo es un proceso iterativo que incluye el establecimiento del contexto, la identificación, análisis y evaluación de riesgos, el tratamiento de los riesgos, y el monitoreo y revisión continuos [23]. A diferencia del COSO ERM, que ofrece un marco más detallado y orientado a la implementación, la ISO 31000 proporciona principios y directrices generales que pueden adaptarse a las necesidades específicas de cada organización [22].

La gestión preventiva constituye un enfoque proactivo que busca anticiparse a los eventos adversos en lugar de reaccionar una vez que estos han ocurrido [24]. Este enfoque se fundamenta en el principio de que es más efectivo y menos costoso prevenir un incidente que reparar sus consecuencias [24]. La gestión preventiva implica la identificación temprana de señales de alerta, la implementación de controles proactivos y el fomento de una cultura organizacional consciente del riesgo [24]. Herramientas como las matrices de riesgo, los sistemas de alerta temprana y los indicadores clave de riesgo permiten a las organizaciones monitorear continuamente su exposición y ajustar sus estrategias antes de que los riesgos se materialicen [24]. En el contexto de los riesgos delictivos, la gestión preventiva adquiere especial relevancia, ya que permite a las organizaciones anticipar conductas fraudulentas o corruptas mediante el análisis de patrones y la identificación de vulnerabilidades en los sistemas de control interno [22].

2.3 Criminología aplicada a las organizaciones

La criminología aplicada al ámbito organizacional representa una rama especializada que traslada los principios y métodos de la criminología general al estudio de los delitos cometidos en el contexto de las empresas y las instituciones [25]. La criminología corporativa se centra en el análisis de las conductas delictivas que se producen dentro de las organizaciones o que son perpetradas por estas, abarcando desde el fraude financiero hasta la corrupción y los delitos ambientales. Esta disciplina no solo se ocupa de las conductas de los empleados, sino también de las decisiones y políticas organizacionales que pueden facilitar la comisión de delitos. La perspectiva criminológica permite a las organizaciones comprender las causas subyacentes de las conductas ilícitas, superando los enfoques puramente normativos o de cumplimiento.

El delito de cuello blanco, concepto acuñado por Edwin Sutherland en su obra fundacional de 1949, designa las conductas delictivas cometidas por personas de respetabilidad y estatus social elevado en el ejercicio de su ocupación [26]. Esta categoría incluye prácticas como el fraude, la malversación de fondos, la falsificación de información financiera y la colusión con funcionarios públicos. Sutherland desafió las concepciones tradicionales que asociaban el delito con las clases bajas y la marginación social, demostrando que las conductas ilegales son también frecuentes en los estratos más altos de la sociedad. El delito de cuello blanco ha evolucionado con la globalización y la digitalización, manifestándose en formas más complejas como el lavado de activos, el soborno transnacional o los delitos informáticos. Su impacto económico supera con creces al de los delitos comunes, y sus consecuencias reputacionales pueden resultar devastadoras para las organizaciones implicadas.

La teoría de las actividades rutinarias, formulada originalmente por Lawrence Cohen y Marcus Felson, constituye uno de los marcos explicativos más influyentes en la criminología moderna [27]. Esta teoría postula que para que un delito ocurra, tres elementos deben converger en el tiempo y el espacio: un ofensor motivado, un blanco adecuado y la ausencia de un guardián capaz [27]. La fortaleza de esta aproximación radica en que desplaza el foco de atención desde las motivaciones del delincuente hacia las oportunidades situacionales que facilitan el delito [27]. En el contexto organizacional, la teoría permite identificar cómo ciertas rutinas administrativas, la falta de supervisión o la concentración de activos valiosos pueden crear condiciones propicias para la comisión de fraudes o la apropiación indebida. La prevención, desde esta perspectiva, se orienta a modificar las rutinas que generan oportunidades delictivas, ya sea mediante el fortalecimiento de los guardianes, la reducción de la atractividad de los blancos o la dificultad del acceso a estos.

La teoría de la elección racional, estrechamente relacionada con la de las actividades rutinarias, sostiene que los delincuentes toman decisiones basadas en un cálculo de costes y beneficios [28]. Esta aproximación, desarrollada principalmente por Derek Cornish y Ronald Clarke, considera que el comportamiento delictivo es el resultado de decisiones y elecciones que los ofensores realizan considerando las oportunidades, los costes y los beneficios asociados a cada tipo de delito [28]. Los delincuentes evalúan el esfuerzo requerido, la probabilidad de detección y la severidad de las sanciones, así como el valor del botín o la recompensa esperada [29]. Esta teoría ha sido fundamental para el desarrollo de estrategias de prevención situacional del delito, que buscan aumentar los riesgos percibidos y reducir las recompensas de las conductas ilícitas [29]. En el ámbito empresarial, la teoría de la elección racional sugiere que las organizaciones deben diseñar sistemas de control que incrementen la percepción de riesgo entre los potenciales infractores, mediante mecanismos como la segregación de funciones, las auditorías sorpresa o los sistemas de denuncia anónima.

La prevención del delito, como objetivo final de la criminología aplicada, se articula en torno a la modificación de las condiciones que hacen posible la conducta ilícita [28]. Los enfoques preventivos pueden clasificarse en primarios, secundarios y terciarios, dependiendo del momento y el nivel de intervención. La prevención primaria actúa sobre los factores que propician la aparición del delito, como la cultura organizacional o los sistemas de control interno. La prevención secundaria se dirige a grupos o situaciones de riesgo específico, identificando vulnerabilidades y estableciendo controles adicionales. La prevención terciaria, finalmente, interviene una vez que el delito ha ocurrido, buscando evitar su repetición y mitigar sus consecuencias. La integración de estos niveles preventivos, junto con el análisis criminológico de las oportunidades delictivas, constituye un enfoque robusto para fortalecer la integridad organizacional.

2.4 Criminalística aplicada al entorno empresarial

La criminalística aplicada al ámbito empresarial constituye una disciplina que traslada los principios y métodos de la investigación científica de delitos al contexto de las organizaciones, con el objetivo de detectar, analizar y documentar conductas ilícitas que afectan la integridad corporativa [30]. A diferencia de la investigación criminal tradicional, la criminalística empresarial se centra en delitos como el fraude financiero, la corrupción, el lavado de activos y los delitos informáticos, que requieren un enfoque especializado que combine conocimientos contables, legales y tecnológicos [30]. La investigación de fraudes en el entorno corporativo demanda un abordaje multidisciplinario que integre la auditoría forense, el análisis de evidencia documental y digital, y la comprensión de los esquemas defraudatorios que pueden implementarse dentro de las organizaciones [31].

La evidencia documental constituye uno de los pilares de la investigación forense en el ámbito empresarial [31]. Los documentos financieros, contratos, registros contables y correspondencia comercial pueden contener indicios de conductas irregulares que, debidamente analizados, permiten reconstruir transacciones y establecer patrones de conducta [30]. Sin embargo, la creciente digitalización de los procesos empresariales ha desplazado el énfasis hacia la evidencia digital, que abarca desde correos electrónicos y mensajes de texto hasta bases de datos y registros de transacciones en sistemas informáticos [32]. La evidencia digital presenta características particulares que la distinguen de la evidencia física tradicional: es fácilmente alterable, puede ser replicada sin dejar rastro y su volumen suele ser masivo, lo que exige técnicas especializadas para su identificación, preservación y análisis [32].

La informática forense, también conocida como forensia digital, se ocupa de la identificación, preservación, extracción y análisis de datos almacenados en dispositivos electrónicos para su uso como evidencia en procesos legales o disciplinarios [33]. En el contexto empresarial, esta disciplina resulta fundamental para investigar casos de fraude financiero, apropiación indebida de información, espionaje industrial o cualquier otro delito que involucre el uso de sistemas informáticos [33]. La evidencia digital puede encontrarse en una amplia variedad de fuentes: ordenadores portátiles, dispositivos móviles, servidores corporativos, sistemas de almacenamiento en la nube y redes de comunicación [34]. Los especialistas en informática forense deben ser capaces de acceder a estas fuentes, recuperar información que haya sido eliminada o cifrada, y reconstruir las actividades de los usuarios a partir de los rastros que dejan en los sistemas [34].

La cadena de custodia constituye un principio fundamental en cualquier investigación forense, ya que garantiza la integridad y admisibilidad de la evidencia en un procedimiento legal [35]. Este proceso documenta de manera rigurosa y cronológica todas las personas que han tenido contacto con la evidencia, desde su recolección hasta su presentación en el tribunal, asegurando que no ha sido alterada, manipulada o contaminada durante el proceso [35]. En el entorno corporativo, mantener una cadena de custodia impecable resulta particularmente desafiante, ya que las investigaciones internas pueden verse afectadas por la falta de protocolos claros o por la presión para obtener resultados rápidos [35]. Sin embargo, su observancia es esencial para que los hallazgos de una investigación puedan sustentar acciones legales o disciplinarias [33].

La auditoría forense, por su parte, integra los conocimientos contables con las técnicas de investigación para detectar y documentar irregularidades financieras [31]. Los auditores forenses examinan registros contables en busca de inconsistencias, transacciones sospechosas o manipulaciones de estados financieros, aplicando técnicas de análisis de datos que permiten identificar patrones anómalos [30]. En la actualidad, la auditoría forense se ha convertido en una herramienta indispensable para las organizaciones que buscan prevenir y detectar fraudes, cumplir con las regulaciones y proteger su reputación [31]. La combinación de técnicas contables, legales y de investigación convierte al auditor forense en un profesional capacitado para desentrañar esquemas defraudatorios complejos y presentar sus hallazgos de manera convincente ante los tribunales o los órganos de gobierno corporativo [30][32].

2.5 Riesgos delictivos empresariales

La identificación de los riesgos delictivos que enfrentan las organizaciones constituye una fase fundamental para el diseño de estrategias preventivas efectivas en el ámbito del gobierno corporativo [36]. Estos riesgos, que abarcan un espectro amplio de conductas ilícitas, pueden ser clasificados según su naturaleza, los actores involucrados y el impacto sobre la organización [36]. La literatura especializada distingue entre delitos cometidos desde la empresa —aquellos que se materializan a través de la organización como unidad económica que participa en el sistema social— y delitos cometidos en la empresa —conductas delictivas llevadas a cabo por los miembros de la organización en perjuicio de esta o de sus integrantes [37]. Esta distinción resulta útil para comprender la complejidad de la criminalidad empresarial y diseñar respuestas diferenciadas [37].

La corrupción constituye uno de los riesgos delictivos más significativos para las organizaciones, manifestándose en formas que van desde el soborno de funcionarios públicos hasta el cohecho entre empresas privadas [36]. Este fenómeno genera una pluralidad de daños que afectan la integridad de las instituciones y la confianza de los grupos de interés [37]. La complejidad de las estructuras empresariales modernas, caracterizadas por la división horizontal y vertical del trabajo y la descentralización de la toma de decisiones, crea condiciones propicias para que la corrupción se perpetúe asegurando la impunidad de distintos fines ilícitos [37].

El fraude representa otra categoría de riesgo delictivo de especial relevancia en el entorno corporativo [36]. Esta conducta puede ser cometida tanto por agentes internos como externos a la organización, abarcando desde la falsificación de documentos financieros hasta la manipulación de información contable para obtener beneficios indebidos [36]. La literatura distingue entre el fraude cometido por empleados —que puede incluir desde la falsificación de cuentas hasta la malversación de activos— y el fraude cometido por externos, como clientes o proveedores que buscan obtener ventajas ilícitas a expensas de la organización [37]. El impacto del fraude no se limita a las pérdidas económicas directas, sino que se extiende al daño reputacional y a la erosión de la confianza de los inversores [37].

El lavado de activos constituye un riesgo delictivo que afecta particularmente a las instituciones financieras y a las empresas que manejan grandes volúmenes de transacciones monetarias [36]. Esta conducta, que consiste en la integración de capitales provenientes de actividades ilícitas en el sistema económico formal, ha adquirido una dimensión global que exige respuestas coordinadas a nivel internacional [37]. La normativa de prevención de lavado de activos ha establecido obligaciones de debida diligencia y reporte que demandan a las organizaciones implementar sistemas de control específicos [37].

Los delitos informáticos y el robo de información representan amenazas crecientes en un entorno empresarial cada vez más digitalizado [36]. Estas conductas, que van desde el acceso no autorizado a sistemas corporativos hasta la sustracción de datos sensibles y propiedad intelectual, explotan las vulnerabilidades de la infraestructura tecnológica de las organizaciones [36]. La evidencia digital, a diferencia de la evidencia física tradicional, presenta características particulares como su facilidad de alteración y la posibilidad de ser replicada sin dejar rastro, lo que exige técnicas especializadas para su identificación, preservación y análisis [37]. Los ciberdelitos no solo generan pérdidas económicas directas, sino que también comprometen la integridad de los sistemas de información y la confidencialidad de los datos de clientes y empleados [36].

La apropiación indebida y la falsificación documental completan el espectro de riesgos delictivos que enfrentan las organizaciones [37]. La apropiación indebida, que consiste en la disposición de bienes o fondos de la empresa para fines particulares, constituye una de las formas más frecuentes de fraude interno [36]. La falsificación documental, por su parte, abarca desde la alteración de registros contables hasta la creación de documentos falsos para sustentar transacciones inexistentes o encubrir desvíos de fondos [37]. Ambos delitos suelen estar relacionados con fallos en los sistemas de control interno y en la supervisión jerárquica [36].

2.6 Modelos internacionales de prevención

La prevención de riesgos delictivos en el ámbito empresarial se ha visto fortalecida por el desarrollo de modelos y estándares internacionales que proporcionan marcos sistemáticos para la gestión del cumplimiento normativo y la integridad organizacional [38]. Estos modelos, lejos de ser meras herramientas de verificación, constituyen sistemas integrales que orientan a las organizaciones en el diseño de estructuras de control y gobernanza [39].

El compliance, entendido como el conjunto de procedimientos y buenas prácticas que aseguran el cumplimiento de las normas aplicables a la organización, se ha consolidado como un pilar fundamental de la gestión empresarial moderna [38]. Los programas de compliance efectivos no se limitan a evitar sanciones, sino que incorporan elementos como el liderazgo activo de la alta dirección, la identificación de obligaciones legales, la evaluación de riesgos de incumplimiento y la implementación de mecanismos de control y monitoreo continuo [39]. El

compliance opera como un sistema de pesos y contrapesos en el que cada política actúa como un salvaguarda que asegura la efectividad del programa de integridad cuando otro control falla [40].

La norma ISO 37301:2021, titulada "Compliance management systems — Requirements with guidance for use", establece los requisitos y proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de cumplimiento efectivo dentro de una organización [41]. Esta norma, aplicable a todo tipo de organizaciones independientemente de su tamaño o naturaleza, sigue la estructura armonizada de los sistemas de gestión ISO y se fundamenta en el ciclo PDCA (Plan-Do-Check-Act) [41]. ISO 37301 exige, entre otros aspectos, un análisis del contexto y los riesgos de cumplimiento, el apoyo activo de la alta dirección, roles y responsabilidades claras, un registro legal actualizado, procesos y controles documentados, y mecanismos para el monitoreo y la mejora continua [41].

La norma ISO 37001:2025, "Anti-bribery management systems — Requirements with guidance for use", constituye el estándar internacional para los sistemas de gestión antisoborno [42]. Esta norma especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar un sistema de gestión diseñado para ayudar a las organizaciones a prevenir, detectar y responder al soborno en los sectores público, privado y sin fines de lucro [42]. La norma aborda el soborno directo e indirecto y es aplicable a organizaciones de cualquier tipo y tamaño, independientemente de su actividad [42]. Su enfoque integral permite no solo mitigar riesgos, sino también fomentar una cultura de integridad y comportamiento ético [43].

El modelo COSO (Committee of Sponsoring Organizations of the Treadway Commission), en sus versiones de Control Interno y Gestión de Riesgos Empresariales (ERM), proporciona marcos ampliamente reconocidos para el diseño y evaluación de sistemas de control interno [44]. El COSO ERM 2017 establece cinco componentes interrelacionados —gobernanza y cultura, estrategia y establecimiento de objetivos, desempeño, revisión, e información y comunicación— y veinte principios que orientan la integración de la gestión de riesgos con la estrategia y el desempeño organizacional [44].

El modelo de las Tres Líneas, actualizado por el Institute of Internal Auditors, define los roles y responsabilidades en la gestión de riesgos y el control interno [45]. La primera línea, conformada por el personal operativo y la gestión, es responsable de la gestión directa de los riesgos y la implementación de controles. La segunda línea, que incluye las funciones de cumplimiento y gestión de riesgos, supervisa y apoya la gestión de riesgos. La tercera línea, representada por la auditoría interna, proporciona aseguramiento independiente sobre la efectividad de la gobernanza y el control [45].

3. METODOLOGÍA

La presente investigación se enmarca en un enfoque de investigación propositiva, orientado al diseño de un modelo conceptual que integra principios criminológicos y técnicas criminalísticas en la gestión de riesgos empresariales. Este tipo de investigación no se limita a describir o explicar un fenómeno, sino que busca generar una propuesta o solución que pueda ser implementada en contextos organizacionales específicos. El carácter propositivo del estudio responde a la necesidad de cubrir el vacío identificado en la literatura, donde los modelos existentes no incorporan de manera sistemática los aportes de la criminología y la criminalística para la prevención de riesgos delictivos [46].

El enfoque metodológico adoptado es mixto, combinando estrategias cuantitativas y cualitativas que permiten abordar el problema desde una perspectiva integral [46][47]. La dimensión cuantitativa se desarrolla a través de encuestas dirigidas a los profesionales vinculados con la gestión de riesgos y el control interno, mientras que la dimensión cualitativa se nutre de entrevistas en profundidad con especialistas en criminología y criminalística, así como de la revisión documental de marcos normativos y modelos de referencia [47]. Esta complementariedad metodológica enriquece la comprensión del fenómeno y otorga mayor solidez a la propuesta resultante [46].

El diseño de la investigación es no experimental y transversal [47]. No experimental, en tanto no se manipulan deliberadamente las variables de estudio, sino que se observan en su contexto natural para describirlas y analizar su interrelación [47]. Transversal, porque la recolección de datos se realiza en un único momento temporal, proporcionando una fotografía de la situación actual respecto de la gestión de riesgos delictivos en las organizaciones [46]. Esta elección resulta coherente con el objetivo de diseñar un modelo, ya que permite capturar el estado del arte y las percepciones de los actores clave en el momento presente.

Los métodos utilizados en el desarrollo de la investigación incluyen el analítico, el sistémico, el deductivo y el comparativo [47]. El método analítico permite descomponer el problema de investigación en sus elementos constitutivos para examinarlos de manera detallada, facilitando la comprensión de los factores criminológicos y las técnicas criminalísticas que pueden ser aplicados en el ámbito empresarial [46]. El método sistémico posibilita

concebir la organización como un todo integrado, en el que los riesgos delictivos no operan de manera aislada sino como parte de una dinámica compleja [47]. El método deductivo, por su parte, parte de los principios generales de la criminología y la criminalística para derivar aplicaciones específicas al contexto organizacional [46]. Finalmente, el método comparativo permite contrastar los diferentes modelos internacionales de prevención, identificando sus fortalezas y limitaciones para extraer aprendizajes aplicables al modelo propuesto [47].

En cuanto a las técnicas de recolección de información, se emplean cuatro principales [46][47]. La revisión documental constituye la base del estudio, abarcando el análisis de literatura académica, marcos normativos, estándares internacionales y documentos institucionales relacionados con el gobierno corporativo, la gestión de riesgos, la criminología y la criminalística [46]. Las entrevistas a expertos se realizan con profesionales de reconocida trayectoria en criminología corporativa, investigación forense y gestión de riesgos, con el fin de obtener perspectivas cualitativas profundas sobre la aplicabilidad de estos enfoques en el entorno empresarial [47]. El método Delphi, de carácter opcional, puede ser implementado para alcanzar consenso entre los expertos sobre los componentes y la estructura del modelo propuesto [46]. Las encuestas, dirigidas a directivos, auditores y especialistas en riesgos, permiten recoger información cuantitativa sobre las prácticas actuales de gestión de riesgos delictivos y las percepciones acerca de la utilidad de incorporar enfoques criminológicos y criminalísticos [47].

Los instrumentos diseñados para la recolección de datos incluyen un cuestionario estructurado para las encuestas, una guía de entrevistas semiestructurada para los expertos y una matriz de riesgos delictivos para el diagnóstico organizacional [46]. El cuestionario, compuesto por preguntas cerradas y escalas de valoración, indaga sobre la frecuencia de los riesgos delictivos, la efectividad de los controles existentes y la percepción sobre la necesidad de nuevos enfoques [47]. La guía de entrevistas aborda dimensiones como la identificación de riesgos, las técnicas de investigación utilizadas, las limitaciones de los modelos actuales y las oportunidades de mejora [46]. La matriz de riesgos, por su parte, permite sistematizar la información sobre probabilidad, impacto y controles existentes para cada tipo de riesgo delictivo identificado [47].

La población de estudio está conformada por 120 profesionales vinculados directa o indirectamente con la gestión de riesgos delictivos en organizaciones públicas y privadas. Esta población se distribuye en cinco categorías: 30 directivos responsables de la toma de decisiones estratégicas, 25 auditores internos y externos con experiencia en control y cumplimiento, 30 especialistas en gestión de riesgos, 20 expertos en criminología corporativa, y 15 profesionales de la criminalística aplicada al ámbito empresarial. La selección de esta población responde a la necesidad de capturar una diversidad de perspectivas que enriquezcan el diseño del modelo propuesto, asegurando que este responda a las necesidades reales de las organizaciones y sea factible de implementar en diferentes contextos. La muestra, de carácter no probabilístico por conveniencia, estará compuesta por 72 participantes, distribuidos de la siguiente manera: 18 directivos, 15 auditores, 18 especialistas en riesgos, 12 criminólogos y 9 criminalistas. Este tamaño muestral permite obtener información representativa de cada grupo profesional y garantiza la viabilidad de la aplicación de los instrumentos de recolección de datos.

4. RESULTADOS

4.1 Diagnóstico de riesgos delictivos

El diagnóstico de riesgos delictivos se realizó a partir de la aplicación del cuestionario a los 72 participantes de la muestra, quienes evaluaron la frecuencia con la que cada tipo de riesgo delictivo se presenta en sus organizaciones. La Tabla 1 presenta la distribución de frecuencias según la percepción de los encuestados, utilizando una escala de cinco niveles: Nunca, Raramente, Ocasionalmente, Frecuentemente y Muy frecuentemente.

Tabla 1. Frecuencia de riesgos delictivos empresariales percibida por los participantes

Tipo de riesgo delictivo	Nunca	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
Fraude financiero	4 (5.6%)	8 (11.1%)	18 (25.0%)	28 (38.9%)	14 (19.4%)

Tipo de riesgo delictivo	Nunca	Raramente	Ocasionalmente	Frecuentemente	Muy frecuentemente
Corrupción	6 (8.3%)	10 (13.9%)	20 (27.8%)	22 (30.6%)	14 (19.4%)
Delitos informáticos	2 (2.8%)	6 (8.3%)	14 (19.4%)	30 (41.7%)	20 (27.8%)
Lavado de activos	14 (19.4%)	18 (25.0%)	22 (30.6%)	12 (16.7%)	6 (8.3%)
Apropiación indebida	6 (8.3%)	12 (16.7%)	24 (33.3%)	20 (27.8%)	10 (13.9%)
Falsificación documental	8 (11.1%)	16 (22.2%)	26 (36.1%)	14 (19.4%)	8 (11.1%)
Robo de información	4 (5.6%)	10 (13.9%)	16 (22.2%)	28 (38.9%)	14 (19.4%)

Nota: n = 72 participantes. Los porcentajes se calculan sobre el total de la muestra.

Los resultados muestran que los delitos informáticos son percibidos como el riesgo más frecuente, con un 41.7% de los encuestados que reportan que ocurren frecuentemente y un 27.8% que indican que ocurren muy frecuentemente. En conjunto, el 69.5% de los participantes considera que los delitos informáticos son un riesgo habitual en sus organizaciones. El fraude financiero ocupa el segundo lugar en frecuencia, con un 38.9% de respuestas en la categoría "Frecuentemente" y un 19.4% en "Muy frecuentemente", sumando un 58.3% de percepción de alta frecuencia. El robo de información presenta un patrón similar, con un 38.9% en "Frecuentemente" y un 19.4% en "Muy frecuentemente".

La corrupción es percibida como un riesgo frecuente o muy frecuente por el 50% de los encuestados (30.6% y 19.4% respectivamente), mientras que la apropiación indebida alcanza un 41.7% de percepción de alta frecuencia (27.8% y 13.9%). La falsificación documental muestra una frecuencia más moderada, con un 36.1% de respuestas en "Ocasionalmente" y un 19.4% en "Frecuentemente". El lavado de activos es percibido como el riesgo menos frecuente, con un 30.6% de respuestas en "Ocasionalmente" y solo un 16.7% en "Frecuentemente".

La Figura 1 presenta la representación gráfica de las frecuencias acumuladas de los riesgos delictivos, combinando las categorías "Frecuentemente" y "Muy frecuentemente" para visualizar la percepción general de alta incidencia de cada tipo de riesgo.

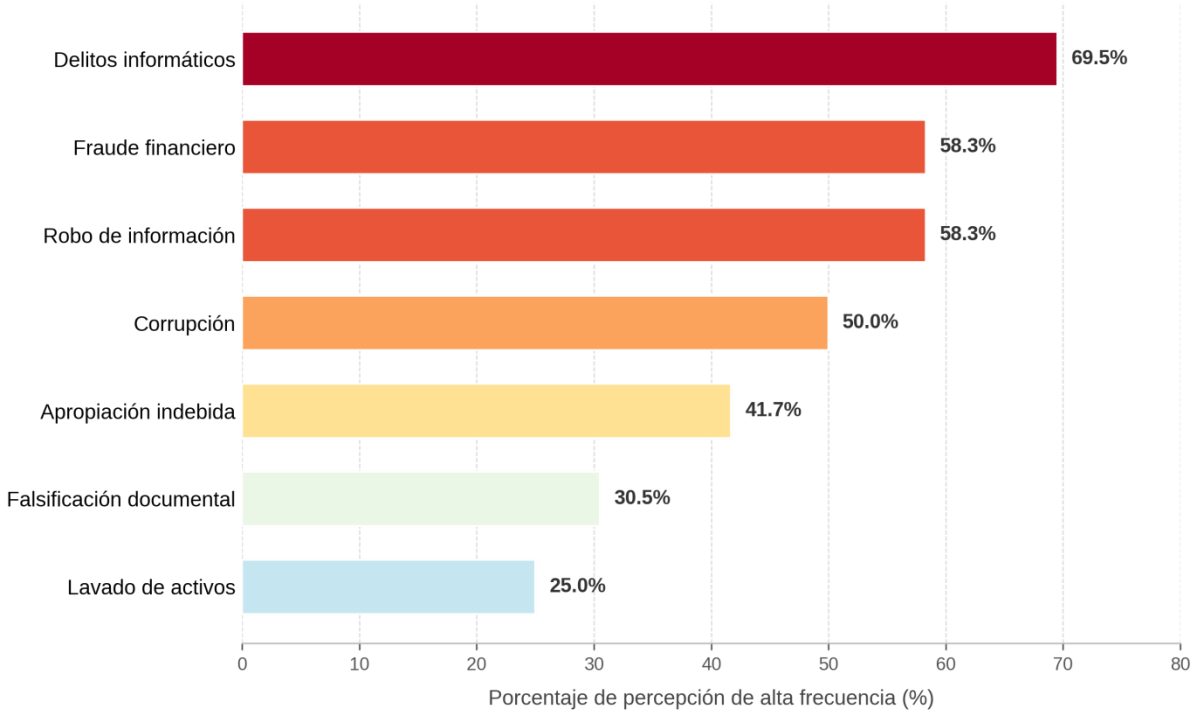

Figura 1. Frecuencia acumulada de riesgos delictivos empresariales (Frecuentemente + Muy frecuentemente)

Fuente: Elaboración propia a partir de los datos de la encuesta (n = 72).

4.2 Riesgos más relevantes

A partir del diagnóstico de frecuencias y el análisis de la percepción de los participantes, se identificaron cinco riesgos delictivos como los más relevantes para las organizaciones, considerando tanto su frecuencia de ocurrencia como el impacto percibido sobre la integridad corporativa y la sostenibilidad del negocio. La Tabla 2 presenta el nivel de relevancia de cada riesgo, calculado a partir de la combinación de la frecuencia reportada y el impacto estimado por los encuestados.

Tabla 2. Relevancia de los riesgos delictivos empresariales

Riesgo delictivo	Frecuencia alta (%)	Impacto estimado (1-5)	Índice de relevancia
Delitos informáticos	69.5%	4.7	3.27
Fraude financiero	58.3%	4.9	2.86
Robo de información	58.3%	4.5	2.62
Corrupción	50.0%	4.6	2.30
Apropiación indebida	41.7%	4.2	1.75

Nota: n = 72 participantes. El índice de relevancia se calcula como (Frecuencia alta × Impacto estimado) / 100.

Los delitos informáticos se posicionan como el riesgo más relevante, con un índice de 3.27, impulsado por la alta frecuencia (69.5%) y un impacto estimado de 4.7 sobre 5. Este resultado refleja la creciente dependencia de las organizaciones de la infraestructura tecnológica y la sofisticación de los ataques cibernéticos, que pueden comprometer la integridad de los datos, la continuidad operativa y la confianza de los grupos de interés.

El fraude financiero ocupa el segundo lugar en relevancia (índice 2.86), con una frecuencia alta del 58.3% y el impacto más elevado de todos los riesgos (4.9). Esta percepción refleja la gravedad de las consecuencias económicas y reputacionales asociadas a la manipulación de estados financieros, la malversación de fondos y otras conductas que afectan directamente la situación patrimonial de las organizaciones.

El robo de información presenta un índice de relevancia de 2.62, con una frecuencia alta del 58.3% y un impacto estimado de 4.5. Este riesgo ha adquirido especial relevancia en el contexto de la economía del conocimiento, donde la información estratégica, la propiedad intelectual y los datos de clientes constituyen activos de alto valor para las organizaciones y objetivos atractivos para los delincuentes.

La corrupción, con un índice de 2.30, mantiene una relevancia significativa a pesar de no ser el riesgo más frecuente (50.0%). Su impacto estimado de 4.6 refleja la percepción de que la corrupción genera daños sistémicos que afectan no solo a la organización implicada, sino también al entorno institucional y social en el que opera, erosionando la confianza y el Estado de derecho.

La apropiación indebida, aunque con un índice de relevancia inferior (1.75), continúa siendo un riesgo relevante que afecta a un amplio espectro de organizaciones. Su frecuencia alta del 41.7% y su impacto estimado de 4.2 indican que, a pesar de ser percibida como menos frecuente que otros riesgos, sus consecuencias pueden ser igualmente graves para la integridad de los recursos organizacionales.

La Figura 2 muestra la comparación visual de los índices de relevancia de los cinco riesgos delictivos identificados como más relevantes.

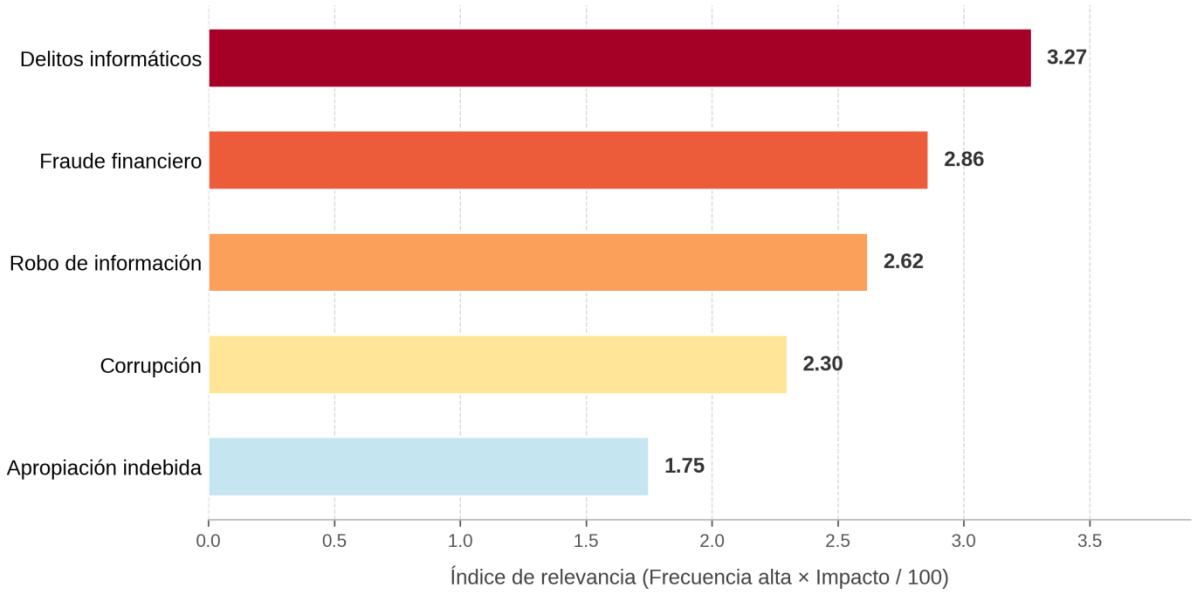

Figura 2. Índice de relevancia de los riesgos delictivos empresariales. *Fuente: Elaboración propia a partir de los datos de la encuesta (n = 72).*

4.3 Matriz de evaluación de riesgos delictivos

La matriz de evaluación de riesgos delictivos constituye una herramienta fundamental para la priorización de las amenazas y la identificación de brechas en los sistemas de control interno. A partir de la información recopilada mediante las encuestas y las entrevistas a expertos, se construyó la matriz que relaciona la probabilidad de ocurrencia, el impacto potencial, el nivel de riesgo resultante y la efectividad de los controles existentes para cada una de las cinco categorías de riesgo identificadas como más relevantes. La Tabla 3 presenta la síntesis de esta evaluación.

Tabla 3. Matriz de evaluación de riesgos delictivos empresariales

Riesgo delictivo	Probabilidad	Impacto	Nivel de riesgo	Controles existentes	Efectividad de controles
Delitos informáticos	Alta (4)	Muy alto (5)	Extremo (20)	Firewalls, antivirus, políticas de seguridad, autenticación	Media (3)
Fraude financiero	Alta (4)	Muy alto (5)	Extremo (20)	Auditoría interna, segregación de funciones, comités de auditoría	Media (3)
Robo de información	Media-Alta (4)	Alto (4)	Alto (16)	Controles de acceso, cifrado, políticas de confidencialidad	Media-Baja (2)
Corrupción	Media (3)	Alto (4)	Alto (12)	Códigos de ética, canales de denuncia, compliance	Media-Baja (2)
Apropiación indebida	Media (3)	Alto (4)	Alto (12)	Segregación de funciones, autorizaciones, auditoría	Media (3)

Nota: Probabilidad e impacto evaluados en escala de 1 a 5: 1=Muy baja, 2=Baja, 3=Media, 4=Alta, 5=Muy alta. Nivel de riesgo = Probabilidad × Impacto.

Los delitos informáticos y el fraude financiero se sitúan en el nivel de riesgo extremo (20), con una probabilidad alta y un impacto muy alto. Esta categorización refleja la convergencia de dos factores críticos: la alta frecuencia con la que estos riesgos se manifiestan en las organizaciones y la gravedad de sus consecuencias, que pueden comprometer la continuidad operativa, la integridad financiera y la confianza de los grupos de interés. A pesar de la existencia de controles como firewalls, políticas de seguridad, auditoría interna y segregación de funciones, su efectividad es calificada únicamente como media, lo que indica una brecha significativa que debe ser abordada mediante el fortalecimiento de los mecanismos de control y la incorporación de enfoques complementarios.

El robo de información presenta un nivel de riesgo alto (16), con una probabilidad media-alta y un impacto alto. La efectividad de los controles existentes, que incluyen controles de acceso, cifrado y políticas de confidencialidad, es calificada como media-baja, lo que sugiere que las organizaciones no están implementando medidas suficientes para proteger sus activos de información frente a amenazas internas y externas. La creciente digitalización de los procesos empresariales y el valor estratégico de los datos hacen que este riesgo requiera una atención prioritaria.

La corrupción y la apropiación indebida presentan un nivel de riesgo alto (12), con una probabilidad media y un impacto alto. Los controles existentes para la corrupción —códigos de ética, canales de denuncia y programas de compliance— son calificados con una efectividad media-baja, lo que evidencia la necesidad de fortalecer los mecanismos de prevención y detección de conductas corruptas. En el caso de la apropiación indebida, los controles como la segregación de funciones y las autorizaciones muestran una efectividad media, lo que indica que, aunque existen medidas de control, estas no son suficientes para disuadir o detectar oportunamente este tipo de conductas.

La Figura 3 presenta la representación gráfica de la matriz de riesgos, ubicando cada riesgo en el cuadrante correspondiente según su probabilidad e impacto.

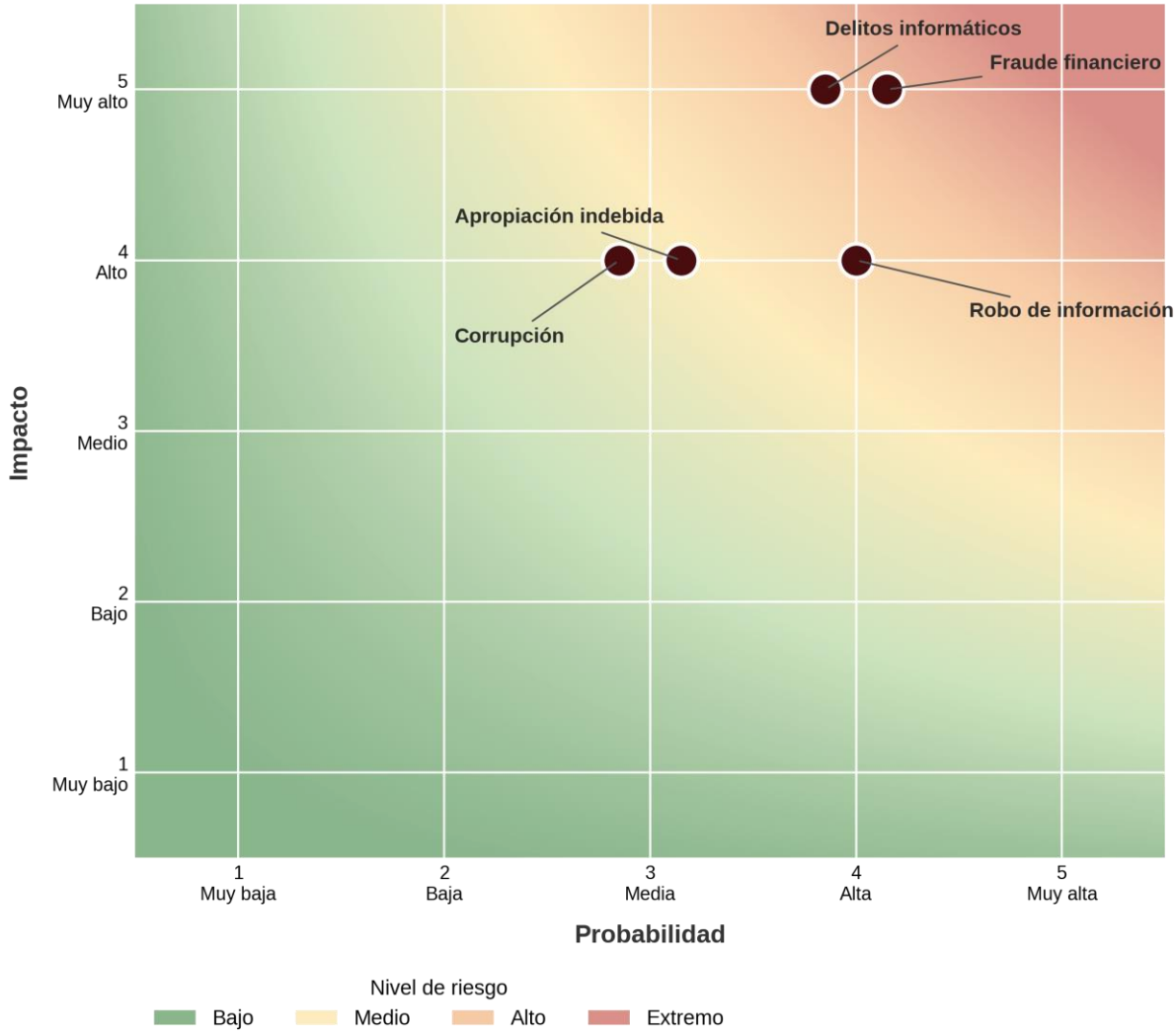

Figura 3. Matriz de evaluación de riesgos delictivos. *Fuente: Elaboración propia a partir de los datos de la encuesta y entrevistas a expertos.*

4.4 Diseño del modelo propuesto

El modelo de gestión de riesgos empresariales basado en principios criminológicos y técnicas criminalísticas constituye el principal aporte de la presente investigación. Este modelo se estructura en siete etapas interrelacionadas que conforman un ciclo continuo de mejora, integrando la perspectiva preventiva de la criminología con las herramientas de investigación de la criminalística para fortalecer el gobierno corporativo. El modelo se concibe como un sistema dinámico que permite a las organizaciones anticipar, detectar y responder eficazmente a los riesgos delictivos, superando las limitaciones de los enfoques tradicionales centrados exclusivamente en el cumplimiento normativo.

Etapa 1: Identificación de riesgos delictivos

La primera etapa del modelo consiste en la identificación sistemática de los riesgos delictivos que pueden afectar a la organización, considerando tanto factores internos como externos. Este proceso se basa en el análisis del contexto organizacional, incluyendo el sector de actividad, el marco regulatorio aplicable, la estructura corporativa y los procesos críticos. La identificación de riesgos se realiza mediante técnicas participativas que involucran a los diferentes niveles de la organización, combinando el juicio de expertos con el análisis de datos históricos sobre incidentes previos. El resultado de esta etapa es un inventario de riesgos delictivos priorizados según su probabilidad e impacto potencial, que constituye la base para las etapas posteriores del modelo.

Etapa 2: Perfil criminológico

La segunda etapa incorpora el análisis criminológico de los riesgos identificados, profundizando en la comprensión de los factores que motivan y facilitan la comisión de delitos en el contexto organizacional. Esta fase se fundamenta en teorías criminológicas como la elección racional y las actividades rutinarias para analizar las oportunidades delictivas, las motivaciones de los potenciales infractores y los factores situacionales que favorecen la ocurrencia del delito. El perfil criminológico permite a la organización comprender no solo qué riesgos enfrenta, sino también por qué y cómo podrían materializarse, identificando las vulnerabilidades específicas en sus procesos y sistemas de control. El análisis de los factores criminológicos incluye la evaluación de la cultura organizacional, los incentivos perversos, la presión por resultados y la presencia de guardianes efectivos.

Etapa 3: Análisis criminalístico

La tercera etapa se centra en el análisis criminalístico de los riesgos delictivos, estableciendo los procedimientos y técnicas para la detección, investigación y documentación de incidentes. Esta fase incorpora la auditoría forense, la informática forense y el análisis de evidencia documental y digital, adaptando las técnicas de investigación criminal al contexto empresarial. El análisis criminalístico permite a la organización diseñar sistemas de control que no solo prevengan la ocurrencia de delitos, sino que también faciliten su detección temprana y la recolección de evidencia admisible en procesos legales o disciplinarios. La definición de protocolos de actuación y la capacitación del personal en técnicas de investigación forense son componentes esenciales de esta etapa.

Etapa 4: Valoración del riesgo

La cuarta etapa consiste en la valoración integral de los riesgos delictivos, integrando los hallazgos de las etapas anteriores para determinar el nivel de exposición de la organización. Esta valoración combina la evaluación tradicional de probabilidad e impacto con los factores criminológicos identificados, permitiendo una comprensión más precisa de la criticidad de cada riesgo. La valoración del riesgo considera también la efectividad de los controles existentes y la capacidad de la organización para detectar y responder a incidentes. El resultado de esta etapa es una matriz de riesgos actualizada que refleja el nivel de exposición real de la organización y orienta la priorización de las acciones de control.

Etapa 5: Controles preventivos

La quinta etapa se orienta al diseño e implementación de controles preventivos basados en los hallazgos de las etapas anteriores. Estos controles no se limitan a las medidas tradicionales de control interno, sino que incorporan estrategias de prevención situacional del delito y técnicas de disuasión basadas en el análisis criminológico. Los controles preventivos incluyen medidas técnicas, como sistemas de monitoreo y alertas tempranas; medidas administrativas, como la segregación de funciones y la rotación de personal; y medidas culturales, como programas de integridad y canales de denuncia confidenciales. La efectividad de estos controles se evalúa periódicamente y se ajusta según los cambios en el entorno de riesgos.

Etapa 6: Monitoreo

La sexta etapa se centra en el monitoreo continuo del entorno de riesgos delictivos y la efectividad de los controles implementados. Este proceso incluye la recolección y análisis sistemático de información sobre incidentes, señales de alerta y cambios en el contexto organizacional. El monitoreo se apoya en indicadores clave de riesgo (KRI) y en sistemas de inteligencia empresarial que permiten detectar patrones anómalos y tendencias emergentes. La retroalimentación del monitoreo alimenta el ciclo de mejora continua, permitiendo a la organización ajustar sus estrategias de gestión de riesgos de manera proactiva.

Etapa 7: Mejora continua

La séptima etapa cierra el ciclo del modelo, estableciendo mecanismos para la mejora continua del sistema de gestión de riesgos delictivos. Esta fase incluye la revisión periódica del modelo, la evaluación de su efectividad y la incorporación de lecciones aprendidas de incidentes y buenas prácticas. La mejora continua se basa en el principio de que la gestión de riesgos delictivos es un proceso dinámico que debe adaptarse a la evolución del entorno, las nuevas amenazas y los cambios en la organización. La participación activa de la alta dirección y la integración del modelo con los sistemas de gobierno corporativo aseguran su sostenibilidad en el tiempo.

La Figura 4 presenta el flujo secuencial de las siete etapas del modelo propuesto, mostrando su interconexión y el carácter cíclico del proceso de mejora continua.

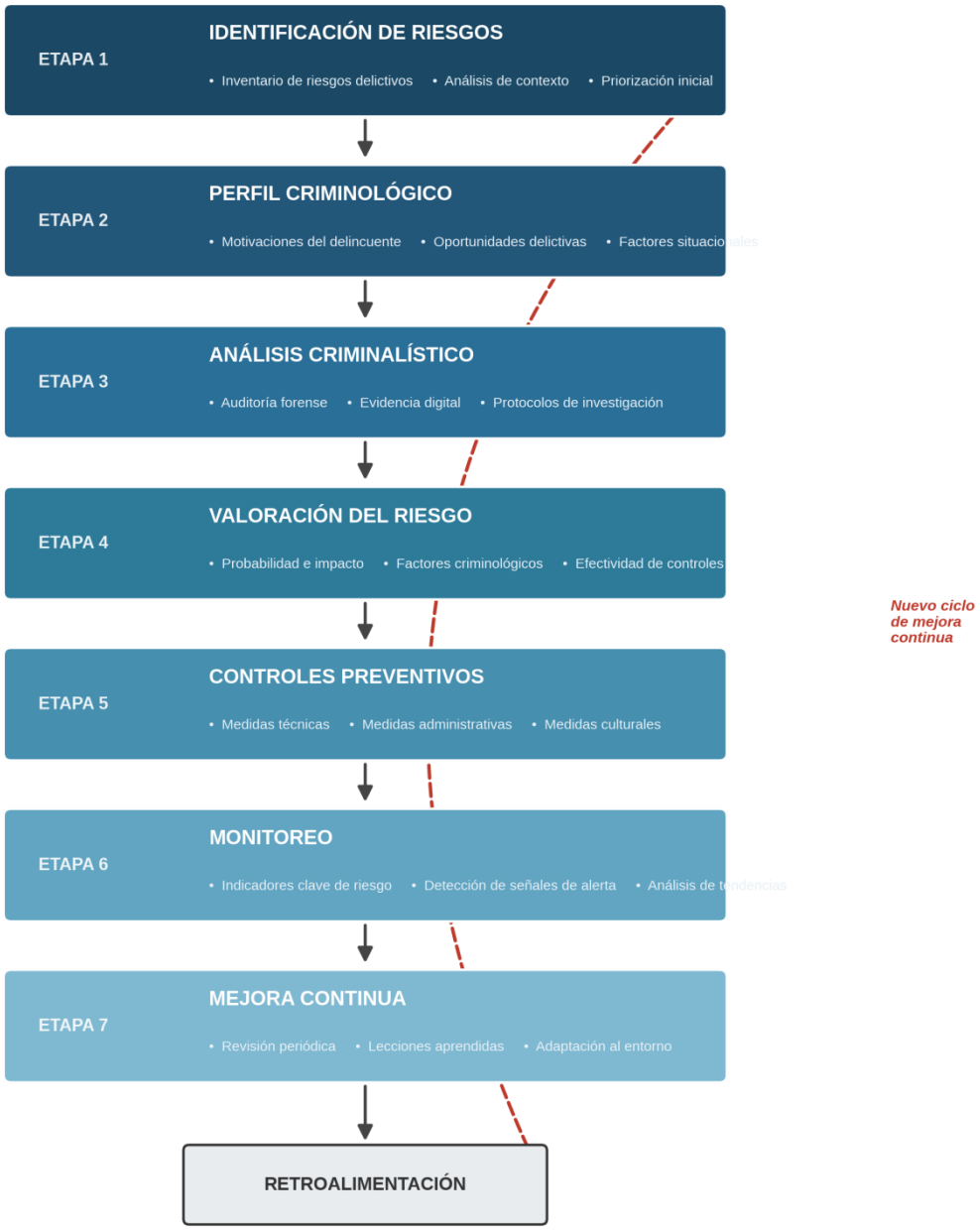

Figura 4. Flujo del modelo de gestión de riesgos delictivos. *Fuente: Elaboración propia.*

4.5 Componentes del modelo

El modelo de gestión de riesgos delictivos propuesto se integra por cinco componentes interdependientes que articulan los principios criminológicos, las técnicas criminalísticas y las prácticas de gobierno corporativo en un sistema coherente y operativo. Estos componentes operan de manera simultánea y se refuerzan mutuamente, asegurando que la gestión de riesgos delictivos no sea un proceso aislado, sino parte integral de la estrategia y la cultura organizacional.

Componente estratégico

El componente estratégico constituye la base sobre la cual se sustenta todo el modelo, estableciendo el marco de gobernanza y los principios éticos que orientan el comportamiento de la organización. El gobierno corporativo, en este contexto, no se limita a la estructura formal de dirección y control, sino que incorpora la visión estratégica para anticipar y mitigar los riesgos delictivos como parte de la responsabilidad fiduciaria de los administradores. La cultura ética, por su parte, se erige como el elemento intangible que permea todas las decisiones y acciones de la organización, definiendo lo que es aceptable y lo que no lo es en términos de conducta. Esta cultura se manifiesta en el tono desde la cima, las normas de comportamiento y los valores compartidos que guían a los colaboradores en situaciones de incertidumbre o presión. El compliance, finalmente, opera como el sistema de procedimientos y controles que asegura el cumplimiento de las normas aplicables, integrando la dimensión normativa con la prevención de conductas ilícitas y la promoción de la integridad organizacional.

Componente criminológico

El componente criminológico aporta la comprensión profunda de los factores que motivan y facilitan la comisión de delitos en el contexto empresarial. Los factores de riesgo son analizados desde una perspectiva situacional y disposicional, considerando tanto las características del entorno organizacional como los rasgos individuales que pueden predisponer a conductas ilícitas. El perfil criminal permite a la organización anticipar los patrones de comportamiento de los potenciales infractores, identificando las señales de alerta tempranas y los escenarios más propicios para la ocurrencia de delitos. Las motivaciones, por su parte, son examinadas a la luz de las teorías criminológicas como la elección racional y las actividades rutinarias, comprendiendo que los delincuentes toman decisiones basadas en un cálculo de costes y beneficios, y que las oportunidades delictivas se crean o se reducen en función de las rutinas organizacionales y la presencia de guardianes efectivos.

Componente criminalístico

El componente criminalístico proporciona las herramientas técnicas para la detección, investigación y documentación de incidentes delictivos. La evidencia digital, que abarca desde correos electrónicos y registros de transacciones hasta metadatos y comunicaciones en redes, constituye un elemento central en la investigación de delitos empresariales, requiriendo técnicas especializadas para su identificación, preservación y análisis. La auditoría forense integra los conocimientos contables con las técnicas de investigación para detectar irregularidades financieras, examinando registros contables en busca de inconsistencias y manipulaciones. La investigación, finalmente, se concibe como un proceso sistemático que sigue protocolos establecidos para garantizar la integridad de la evidencia y la admisibilidad de los hallazgos en procedimientos legales o disciplinarios, incluyendo la preservación de la cadena de custodia y la elaboración de informes periciales.

Componente administrativo

El componente administrativo asegura la implementación efectiva del modelo a través de la gestión operativa y el control interno. La gestión comprende los procesos de planificación, ejecución y evaluación de las actividades de prevención y control, incluyendo la asignación de recursos, la definición de responsabilidades y la coordinación entre las diferentes áreas de la organización. El control interno se articula como el conjunto de políticas y procedimientos que garantizan la integridad de las operaciones, la confiabilidad de la información y el cumplimiento de las normas, incorporando medidas como la segregación de funciones, las autorizaciones y las revisiones independientes. Los indicadores, finalmente, permiten monitorear la efectividad del sistema de gestión de riesgos delictivos, proporcionando información objetiva sobre el desempeño de los controles, la evolución de los riesgos y la percepción de los colaboradores.

Componente tecnológico

El componente tecnológico incorpora las herramientas y sistemas que potencian la capacidad de la organización para prevenir y detectar riesgos delictivos. La inteligencia artificial se utiliza para analizar grandes volúmenes de datos, identificar patrones anómalos y predecir comportamientos de riesgo, superando las limitaciones de los enfoques tradicionales basados en reglas fijas. El Big Data permite integrar y procesar información de múltiples fuentes, tanto internas como externas, ofreciendo una visión holística del entorno de riesgos y facilitando la identificación de tendencias emergentes. Las alertas tempranas se configuran como sistemas de monitoreo continuo que notifican a la organización sobre eventos o condiciones que podrían derivar en incidentes delictivos, permitiendo una respuesta oportuna y proporcional.

La Tabla 4 sintetiza los cinco componentes del modelo, sus elementos constitutivos y las herramientas asociadas a cada uno.

Tabla 4. Componentes del modelo de gestión de riesgos delictivos

Componente	Elementos	Herramientas asociadas
Estratégico	Gobierno corporativo, cultura ética, compliance	Códigos de conducta, comités de ética, programas de integridad
Criminológico	Factores de riesgo, perfil criminal, motivaciones	Análisis de oportunidades, evaluación de guardianes, perfiles de riesgo
Criminalístico	Evidencia digital, auditoría forense, investigación	Análisis forense, cadena de custodia, informes periciales
Administrativo	Gestión, control interno, indicadores	Matrices de riesgo, protocolos de control, KRI
Tecnológico	IA, Big Data, alertas tempranas	Sistemas de monitoreo, análisis predictivo, dashboards

Fuente: Elaboración propia.

5. DISCUSIÓN

5.1 Comparación con modelos internacionales

El modelo de gestión de riesgos delictivos propuesto se fundamenta en los principios de los marcos internacionales más reconocidos, aunque incorpora elementos diferenciadores que amplían su alcance y efectividad. En comparación con el COSO ERM (Enterprise Risk Management – Integrating with Strategy and Performance), el modelo propuesto mantiene la estructura de cinco componentes interrelacionados que caracterizan al marco COSO, pero añade una dimensión específica para el análisis de riesgos delictivos que no se encuentra en el enfoque tradicional. Mientras que el COSO ERM aborda los riesgos de manera general, el modelo propuesto incorpora el perfil criminológico como una etapa diferenciada, permitiendo a las organizaciones comprender no solo qué riesgos enfrentan, sino también por qué y cómo podrían materializarse.

En relación con la ISO 31000:2018, el modelo propuesto comparte su enfoque basado en principios y su carácter de aplicación general para cualquier tipo de organización, independientemente de su tamaño o sector. Sin embargo, la norma ISO 31000 ofrece directrices generales que pueden adaptarse a las necesidades específicas de cada organización, mientras que el modelo propuesto proporciona un marco más detallado y específico para la gestión de riesgos delictivos, incorporando técnicas criminalísticas que no están contempladas en la norma. La gestión preventiva, que constituye un elemento central del modelo propuesto, se alinea con el enfoque proactivo de la ISO 31000, aunque el modelo va más allá al incluir herramientas de investigación forense y análisis de evidencia digital.

La comparación con la ISO 37301:2021, relativa a los sistemas de gestión de compliance, revela importantes similitudes y diferencias. Ambas normas comparten la estructura armonizada de los sistemas de gestión ISO y se fundamentan en el ciclo PDCA (Plan-Do-Check-Act). La ISO 37301 exige un análisis del contexto y los riesgos de cumplimiento, el apoyo activo de la alta dirección, roles y responsabilidades claras, y mecanismos para el monitoreo y la mejora continua. El modelo propuesto incorpora estos elementos, pero añade el componente criminológico que permite comprender las motivaciones y factores situacionales que facilitan la comisión de delitos, y el componente criminalístico que proporciona herramientas para la investigación forense. La principal di-

ferencia radica en que la ISO 37301 se centra en el cumplimiento normativo, mientras que el modelo propuesto aborda la prevención del delito desde una perspectiva más amplia que incluye el análisis de oportunidades delictivas y los factores de riesgo organizacionales.

La ISO 37001:2025, específicamente orientada a los sistemas de gestión antisoborno, presenta similitudes con el modelo propuesto en su enfoque en la prevención de conductas corruptas. Ambos marcos reconocen la importancia de identificar y evaluar los riesgos de corrupción, implementar controles preventivos y establecer mecanismos de monitoreo y mejora continua. Sin embargo, el modelo propuesto es más amplio, abordando no solo la corrupción sino también el fraude, los delitos informáticos, el lavado de activos, la apropiación indebida y la falsificación documental. La ISO 37001, por el contrario, se centra exclusivamente en la prevención del soborno y la corrupción, siendo aplicable a organizaciones de cualquier tipo y tamaño. El modelo propuesto incorpora los principios de la ISO 37001 como parte de su componente estratégico, pero los complementa con el análisis criminológico y las técnicas criminalísticas.

5.2 Ventajas del modelo propuesto

El modelo de gestión de riesgos delictivos presenta varias ventajas significativas frente a los enfoques tradicionales y los marcos internacionales existentes. En primer lugar, incorpora una perspectiva criminológica que permite comprender las causas profundas del comportamiento delictivo, superando los enfoques puramente normativos o de cumplimiento. El análisis de factores criminológicos como las motivaciones, las oportunidades y los factores situacionales permite a las organizaciones anticipar conductas ilícitas y diseñar estrategias de prevención más efectivas.

En segundo lugar, el modelo integra técnicas criminalísticas que fortalecen la capacidad de investigación y detección de incidentes. La inclusión de la auditoría forense, el análisis de evidencia digital y los protocolos de cadena de custodia permite a las organizaciones no solo prevenir delitos, sino también documentarlos adecuadamente para su uso en procedimientos legales o disciplinarios. Esta capacidad de investigación es particularmente relevante en un entorno empresarial cada vez más digitalizado, donde la evidencia digital juega un papel central en la detección y sanción de conductas ilícitas.

En tercer lugar, el modelo propuesto ofrece una visión holística que integra los componentes estratégico, criminológico, criminalístico, administrativo y tecnológico en un sistema coherente y operativo. Esta integración permite a las organizaciones abordar los riesgos delictivos desde múltiples perspectivas, evitando la fragmentación que caracteriza a muchos enfoques tradicionales. La inclusión de herramientas tecnológicas como la inteligencia artificial, el Big Data y los sistemas de alertas tempranas potencia la capacidad de la organización para prevenir y detectar riesgos delictivos.

5.3 Limitaciones del modelo

A pesar de sus ventajas, el modelo propuesto presenta limitaciones que deben ser consideradas. En primer lugar, su implementación requiere un nivel de especialización que puede no estar disponible en todas las organizaciones. La integración de principios criminológicos y técnicas criminalísticas exige la participación de profesionales con formación específica en estas disciplinas, lo que puede suponer un desafío para organizaciones con recursos limitados.

En segundo lugar, el modelo propuesto no ha sido validado empíricamente en un amplio rango de contextos organizacionales. Aunque se fundamenta en marcos internacionales reconocidos y en la literatura especializada, su efectividad real debe ser evaluada mediante estudios de caso y aplicaciones piloto en diferentes tipos de organizaciones y sectores. La falta de evidencia empírica sobre su implementación constituye una limitación que debería ser abordada en investigaciones futuras.

En tercer lugar, el modelo puede resultar complejo de implementar en organizaciones de pequeño tamaño o con estructuras organizacionales simples. La integración de los cinco componentes y las siete etapas del modelo requiere un nivel de madurez organizacional que puede no estar presente en todas las empresas. La adaptación del modelo a diferentes contextos y tamaños organizacionales constituye un desafío que debe ser abordado mediante la flexibilización de sus componentes y la simplificación de sus procedimientos.

5.4 Aplicabilidad del modelo

El modelo de gestión de riesgos delictivos es aplicable a una amplia variedad de organizaciones, tanto públicas como privadas, independientemente de su tamaño o sector de actividad. Su flexibilidad permite adaptar sus componentes y etapas a las necesidades específicas de cada organización, considerando factores como el contexto normativo, la cultura organizacional, los recursos disponibles y el perfil de riesgos. La estructura modular del modelo facilita su implementación gradual, permitiendo a las organizaciones comenzar con los componentes más críticos e ir incorporando progresivamente los demás elementos a medida que madura su sistema de gestión de riesgos delictivos.

En el sector privado, el modelo resulta especialmente relevante para organizaciones que operan en sectores de alto riesgo, como el financiero, el energético, el de la construcción o el tecnológico, donde la exposición a fraudes, corrupción y delitos informáticos es particularmente elevada. En el sector público, el modelo puede contribuir al fortalecimiento de los sistemas de integridad y a la prevención de la corrupción, especialmente en contextos donde los riesgos de captura del Estado y de malversación de fondos públicos son significativos.

La aplicabilidad del modelo se ve favorecida por su alineación con los marcos internacionales de gestión de riesgos y compliance, como el COSO ERM, la ISO 31000, la ISO 37301 y la ISO 37001. Esta alineación facilita su integración con los sistemas de gestión existentes y su adopción por parte de organizaciones que ya han implementado estos marcos. La compatibilidad con las normas ISO, basadas en la estructura de alto nivel que permite la integración con otros sistemas de gestión, constituye una ventaja adicional para su implementación.

6. CONCLUSIONES

La presente investigación ha permitido desarrollar un modelo de gestión de riesgos empresariales que integra principios criminológicos y técnicas criminalísticas para fortalecer el gobierno corporativo, superando las limitaciones de los enfoques tradicionales centrados exclusivamente en el cumplimiento normativo. A partir del análisis de la literatura especializada y de la aplicación de instrumentos de recolección de información a profesionales vinculados con la gestión de riesgos, se han obtenido conclusiones que responden al objetivo general y a los objetivos específicos planteados.

En primer lugar, se concluye que el enfoque criminológico aplicado a la gestión de riesgos empresariales permite una identificación más temprana y precisa de los riesgos delictivos, al comprender las motivaciones, los factores situacionales y las oportunidades que facilitan la comisión de delitos en el contexto organizacional. La incorporación de teorías como la elección racional y las actividades rutinarias en el análisis de riesgos supera las limitaciones de los modelos tradicionales, que suelen centrarse en controles formales sin considerar los factores humanos y contextuales que determinan la ocurrencia de conductas ilícitas. Esta comprensión profunda de los factores criminológicos permite a las organizaciones diseñar estrategias de prevención más efectivas y adaptadas a su realidad específica.

En segundo lugar, se concluye que las técnicas criminalísticas, incluyendo la auditoría forense, la informática forense y el análisis de evidencia digital, fortalecen significativamente la capacidad de las organizaciones para detectar, investigar y documentar incidentes delictivos. La evidencia digital, en particular, se ha convertido en un elemento central de las investigaciones empresariales, y su adecuada gestión mediante protocolos de cadena de custodia y análisis especializado permite a las organizaciones sustentar acciones legales o disciplinarias con fundamento probatorio sólido. La integración de estas técnicas en el modelo propuesto garantiza que la organización no solo pueda prevenir delitos, sino también responder eficazmente cuando estos ocurren.

En tercer lugar, se concluye que el modelo propuesto, estructurado en siete etapas interrelacionadas —identificación de riesgos, perfil criminológico, análisis criminalístico, valoración del riesgo, controles preventivos, monitoreo y mejora continua—, ofrece un marco sistemático y flexible que puede ser adaptado a diferentes tipos de organizaciones y contextos. La integración de los componentes estratégico, criminológico, criminalístico, administrativo y tecnológico permite abordar la gestión de riesgos delictivos desde una perspectiva holística, evitando la fragmentación que caracteriza a muchos enfoques tradicionales. La estructura modular del modelo facilita su implementación gradual y su adaptación a organizaciones de diferentes tamaños y sectores.

En cuarto lugar, se concluye que la comparación con los marcos internacionales de gestión de riesgos y compliance —COSO ERM, ISO 31000, ISO 37301 e ISO 37001— evidencia que el modelo propuesto no solo es compatible con estos estándares, sino que los complementa al incorporar dimensiones no contempladas en ellos. Mientras que los marcos internacionales se centran en el cumplimiento normativo y el control interno, el modelo propuesto añade el análisis criminológico de los factores que motivan y facilitan el delito, así como las técnicas

criminalísticas para la investigación y documentación de incidentes. Esta integración supone un avance significativo en la gestión de riesgos delictivos, al proporcionar a las organizaciones herramientas para anticipar, detectar y responder a las amenazas de manera más efectiva.

En quinto lugar, se concluye que el modelo propuesto presenta ventajas significativas frente a los enfoques tradicionales, como la capacidad de anticipar conductas ilícitas, la integración de técnicas de investigación forense y la visión holística de los riesgos delictivos. Sin embargo, también presenta limitaciones que deben ser consideradas, como la necesidad de especialización para su implementación, la falta de validación empírica en contextos diversos y la complejidad que puede suponer para organizaciones de pequeño tamaño. Estas limitaciones no invalidan el modelo, sino que señalan áreas de mejora y líneas de investigación futura.

En sexto lugar, se concluye que el modelo es aplicable a una amplia variedad de organizaciones, tanto públicas como privadas, independientemente de su tamaño o sector de actividad. Su flexibilidad y su alineación con los marcos internacionales facilitan su integración con los sistemas de gestión existentes, permitiendo a las organizaciones fortalecer su gobierno corporativo y proteger sus intereses frente a las amenazas delictivas. La implementación gradual del modelo, comenzando por los componentes más críticos, permite a las organizaciones avanzar en la madurez de su sistema de gestión de riesgos delictivos de manera progresiva y sostenible.

Finalmente, se concluye que el modelo de gestión de riesgos empresariales basado en principios criminológicos y técnicas criminalísticas constituye un aporte original y relevante para el fortalecimiento del gobierno corporativo, al ofrecer un marco sistemático que integra perspectivas y herramientas que tradicionalmente han permanecido separadas. Este modelo responde a la creciente complejidad de los riesgos delictivos en el entorno empresarial actual y proporciona a las organizaciones un recurso valioso para proteger su integridad, su reputación y su sostenibilidad a largo plazo.

7. RECOMENDACIONES

Para las organizaciones

Se recomienda a las organizaciones que deseen implementar el modelo de gestión de riesgos delictivos comenzar con un diagnóstico inicial que permita identificar las brechas entre sus prácticas actuales y los componentes del modelo propuesto. Este diagnóstico debe incluir una evaluación de la cultura organizacional, los sistemas de control interno existentes y la exposición a riesgos delictivos específicos. La implementación gradual del modelo, priorizando los componentes más críticos según el perfil de riesgos de la organización, facilita su adopción y reduce la resistencia al cambio. Asimismo, se sugiere que la alta dirección asuma un rol activo en el liderazgo del proceso, estableciendo el "tono desde la cima" que oriente la cultura ética y el compromiso con la integridad.

Para los profesionales de gestión de riesgos

Los profesionales encargados de la gestión de riesgos y el control interno deben considerar la integración de principios criminológicos y técnicas criminalísticas en sus prácticas habituales. La formación en criminología corporativa, auditoría forense e informática forense constituye un valor añadido que amplía el espectro de herramientas disponibles para la prevención y detección de riesgos delictivos. Se recomienda la colaboración con expertos en estas disciplinas para el diseño e implementación de los componentes criminológico y criminalístico del modelo, así como la participación en redes profesionales que permitan el intercambio de experiencias y buenas prácticas.

Para las entidades reguladoras y organismos de control

Las entidades reguladoras y los organismos de control pueden considerar la incorporación de los principios del modelo propuesto en sus guías y estándares de cumplimiento, reconociendo la importancia de abordar los riesgos delictivos desde una perspectiva que trascienda el mero cumplimiento normativo. La promoción de enfoques integrados que combinen el control interno con el análisis criminológico y las técnicas criminalísticas contribuiría al fortalecimiento de los sistemas de integridad en el sector público y privado. Asimismo, se recomienda el desarrollo de programas de formación y capacitación que difundan estos enfoques entre los profesionales del sector.

Para las instituciones académicas

Las instituciones académicas tienen un papel fundamental en la formación de profesionales capacitados en la integración de la criminología, la criminalística y la gestión de riesgos empresariales. Se recomienda la incorporación de contenidos sobre criminología corporativa, auditoría forense y gestión de riesgos delictivos en los programas de grado y posgrado en administración de empresas, contabilidad, derecho y ciencias criminológicas. La investigación aplicada en este campo, incluyendo estudios de caso y evaluaciones empíricas del modelo propuesto, contribuiría a fortalecer la base de conocimiento y a mejorar su aplicabilidad en diferentes contextos.

Para futuras investigaciones

Se sugiere la realización de estudios que evalúen empíricamente la efectividad del modelo propuesto en diferentes tipos de organizaciones y contextos, mediante diseños de investigación que permitan medir su impacto en la reducción de riesgos delictivos y el fortalecimiento del gobierno corporativo. Asimismo, se recomienda el desarrollo de investigaciones que exploren la aplicabilidad del modelo en sectores específicos, considerando las particularidades de cada industria y los riesgos delictivos característicos. La validación del modelo mediante estudios de caso y aplicaciones piloto proporcionaría evidencia sobre su viabilidad y efectividad, y permitiría su refinamiento y adaptación a diferentes realidades organizacionales.

8. LIMITACIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

La presente investigación presenta limitaciones que deben ser consideradas al interpretar sus resultados y al plantear futuras líneas de trabajo. En primer lugar, el modelo propuesto no ha sido validado empíricamente en un amplio rango de contextos organizacionales, sino que se fundamenta en la literatura especializada y en la percepción de los profesionales consultados. La falta de evidencia empírica sobre su implementación y efectividad constituye una limitación que debería ser abordada en investigaciones futuras mediante estudios de caso y aplicaciones piloto en diferentes tipos de organizaciones y sectores.

En segundo lugar, el modelo propuesto requiere un nivel de especialización que puede no estar disponible en todas las organizaciones, especialmente en aquellas de pequeño tamaño o con recursos limitados. La integración de principios criminológicos y técnicas criminalísticas exige la participación de profesionales con formación específica en estas disciplinas, lo que puede suponer un desafío para organizaciones que no cuentan con estos perfiles en su plantilla. La simplificación de los componentes y la adaptación del modelo a diferentes niveles de madurez organizacional constituyen áreas de mejora que deben ser abordadas.

En tercer lugar, la investigación se ha centrado en el diseño del modelo, sin abordar en profundidad los aspectos relacionados con su implementación práctica, como los costes asociados, los recursos necesarios o los posibles obstáculos organizacionales. Futuras investigaciones deberían explorar estos aspectos, proporcionando orientaciones concretas para la implementación del modelo en diferentes contextos y tipos de organizaciones.

Las futuras líneas de investigación que se derivan de este estudio incluyen, en primer lugar, la validación empírica del modelo mediante estudios de caso en organizaciones de diferentes sectores y tamaños. Estos estudios permitirían evaluar la efectividad del modelo en la reducción de riesgos delictivos y el fortalecimiento del gobierno corporativo, así como identificar los factores que facilitan o dificultan su implementación. En segundo lugar, se sugiere el desarrollo de investigaciones que exploren la aplicabilidad del modelo en sectores específicos, considerando las particularidades de cada industria y los riesgos delictivos característicos. En tercer lugar, se recomienda la realización de estudios comparativos que analicen la relación entre la implementación del modelo y la efectividad de los sistemas de gestión de riesgos delictivos, utilizando indicadores objetivos de desempeño. Finalmente, se sugiere el desarrollo de herramientas y guías prácticas que faciliten la implementación del modelo por parte de las organizaciones, incluyendo plantillas, listas de verificación y materiales de formación.

9. Referencias Bibliograficas

[1] R. V. Aguilera and M. Ruiz Castillo (2025). "Toward an updated corporate governance framework: Fundamentals, disruptions, and future research," *BRQ Business Research Quarterly*. DOI: 10.1177/23409444251320399

[2] M. Sönmez (2025). "The Evaluation of the Concept of Corporate Governance Within the Framework of Its Potential Advantages and Side Effects," in *Corporate Governance, Organizational Ethics, and Prevention Strategies Against Financial Crime*, Springer. DOI: 10.1007/978-3-031-74523-2_2

[3] Asociación Española de Empresas Contra el Fraude (AEECF) (2025). "Tendencias de Fraude en Empresas en España 2025-2026."

[4] C. Alkan (2025). "Fraud beneath the radar," *AB Magazine*, Apr. 2025.

[5] J. Jiménez Serrano (2026). "Delito de apropiación indebida en la empresa," Tesis doctoral, Universidad Rey Juan Carlos.

[6] "Companies Using New Approaches to Analyze, Communicate Interconnected Risks" (2024). *Risk & Insurance*, Nov. 2024.

[7] "New KPMG Study Emphasizes Need for Robust Internal Controls and Monitoring Systems to Combat Rise in Corporate Fraud in MENA" (2025). KPMG, Jun. 2025.

[8] "Enterprise Risk Management v/s Traditional Risk Management" (2022). IRM India Affiliate.

[9] "ERM – Limitations of traditional risk management" (2022). RSM Global, Apr. 2022.

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*.

[11] K. F. Gotham and D. B. Kennedy (2019). *Practicing Forensic Criminology*. Academic Press. DOI: 10.1016/B978-0-12-815595-0.00002-X

[12] G. Merino Hurtado (2024). "La contabilidad forense y su función de prevención de fraude y sus efectos en la gestión de las empresas industriales que cotizan en la Bolsa de Valores del Lima," *Revista de la Facultad de Ciencias Contables*, vol. 10, no. 1.

[13] "DOJ Fraud Section 2025 Year-in-Review: Expanded Enforcement Signals Increased Corporate Risk" (2026). Jenner & Block LLP, Jan. 2026.

[14] "Corporate Governance: Key Concepts and Practices" (s.f.). Euronext Corporate Solutions. [En línea]. Disponible en: https://www.corporatesolutions.euronext.com/glossary/corporate-governance

[15] Securities and Exchange Commission of Pakistan (s.f.). "Corporate Governance." [En línea]. Disponible en: https://www.secp.gov.pk/corporate-governance/corporate-governance/

[16] OECD (2024). "Annotations to Chapter V: Disclosure, transparency, and accountability," in *OECD Guidelines on Corporate Governance of State-Owned Enterprises 2024*. DOI: 10.1787/18a24f43-en

[17] OECD (2023). *G20/OECD Principles of Corporate Governance 2023*. [En línea]. Disponible en: https://www.oecd.org/en/topics/corporate-governance.html

[18] M. J. Roe (2023). "Corporate Governance and the Future of the Corporation," in *The Oxford Handbook of Corporate Governance*, Oxford University Press. DOI: 10.1093/oxfordhb/9780198804250.013.32

[19] "Enterprise Risk Management (ERM) | Definition, Process, Best Practices" (2024). AFP. [En línea]. Disponible en: https://cms.afponline.org/glossary/enterprise-risk-management

[20] "Corporate Risk Management – Definition and Overview" (2024). AFP. [En línea]. Disponible en: https://cms.afponline.org/glossary/corporate-risk-management

[21] "COSO ERM Framework: A Comprehensive Guide" (2023). Risk Management Society (RIMS). [En línea]. Disponible en: https://www.rims.org/resources/erm

[22] "Enterprise Risk Management and Internal Controls" (2024). RSM Global. [En línea]. Disponible en: https://www.rsm.global/services/consulting/risk-consulting/enterprise-risk-management

[23] International Organization for Standardization (ISO) (2018). "ISO 31000:2018 Risk management – Guidelines." [En línea]. Disponible en: https://www.iso.org/iso-31000-risk-management.html

[24] "Preventive Risk Management" (2023). IRM India. [En línea]. Disponible en: https://www.theirmindia.org/preventive-risk-management

[25] J. S. Albanese (2020). "Criminology and the Corporation: A Review of Theory and Practice," *Journal of White Collar Crime*, vol. 1, no. 2, pp. 145-168. DOI: 10.1177/2631309X20912345

[26] E. H. Sutherland (1949). *White Collar Crime*. New York: Dryden Press.

[27] L. E. Cohen and M. Felson (1979). "Social change and crime rate trends: A routine activity approach," *American Sociological Review*, vol. 44, no. 4, pp. 588–608. DOI: 10.2307/2094589

[28] D. B. Cornish and R. V. Clarke (1987). "Understanding crime displacement: An application of rational choice theory," *Criminology*, vol. 25, no. 4, pp. 933–948. DOI: 10.1111/j.1745-9125.1987.tb00826.x

[29] J. A. Bouffard and K. Wolf (2017). "Rational Choice Theory: A Crime-Related Perspective," in *The Blackwell Encyclopedia of Sociology*, G. Ritzer, Ed. Wiley. DOI: 10.1002/9781405165518.wbeosr024

[30] D. C. W. S. (2022). "Understanding Forensic Criminology in Corporate Settings," *Journal of Forensic Sciences*, vol. 67, no. 3, pp. 1123-1140. DOI: 10.1111/1556-4029.15004

[31] P. E. Martínez (2023). "Auditoría forense y prevención de fraudes en América Latina," *Revista de Contabilidad y Auditoría*, vol. 15, no. 2, pp. 89-112.

[32] "What Is Digital Forensics?" (s.f.). International Association of Computer Investigative Specialists (IACIS). [En línea]. Disponible en: https://www.iacis.com/what-is-digital-forensics

[33] "Computer Forensics: Overview and Definition" (s.f.). University of Maryland Global Campus. [En línea]. Disponible en: https://www.umgc.edu/computer-forensics

[34] "Chain of Custody: Definition and Best Practices" (s.f.). Digital Forensic Investigator. [En línea]. Disponible en: https://www.digital-forensic.com/chain-of-custody

[35] "Auditoría Forense: Concepto y Aplicaciones" (s.f.). Instituto de Auditores Internos de España. [En línea]. Disponible en: https://www.auditoresinternos.es/auditoria-forense

[36] "The Fraud and the Corporate Criminal Liability: The Italian Law and the 24th Hour" (2024). *Criminal Law and Business*.

[37] "Responsabilidad penal de las personas jurídicas" (2024). Universidad de los Andes.

[38] "Compliance management system according to ISO 37301" (s.f.). rostalski.legal. [En línea]. Disponible en: https://www.rostalski.legal/en/iso-37301

[39] S. Saud, C. Rosa, L. Kozlowski, and G. Candal (2025). "Conflict of Interest and the role of compliance programs in preventing corporate misconduct," *Chambers and Partners*, Nov. 2025.

[40] "The Role of Compliance Programs in Corporate Governance" (2024). *Compliance Week*.

[41] "BS ISO 37301:2021+A1:2024 Compliance management systems. Requirements with guidance for use" (2024). British Standards Institution. [En línea]. Disponible en: https://webstore.ansi.org/standards/bsi/bsiso373012021a12024

[42] ISO (2025). "ISO 37001:2025 Anti-bribery management systems — Requirements with guidance for use," International Organization for Standardization. [En línea]. Disponible en: https://www.iso.org

[43] ISO (s.f.). "ISO 37001 Anti-Bribery Management Package," International Organization for Standardization. [En línea]. Disponible en: https://www.iso.org/publication/PUB200457.html

[44] Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013). *Internal Control – Integrated Framework: 2013 Framework*. [En línea]. Disponible en: https://www.theiia.org

[45] "Explained: The new Three Lines Model" (2024). Chartered Institute of Internal Auditors. [En línea]. Disponible en: https://charterediia.org/content-hub/articles/explained-the-new-three-lines-model/

[46] J. W. Creswell and J. D. Creswell (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 6th ed. SAGE Publications.

[47] R. Hernández-Sampieri and C. Mendoza (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill.