Modelo integrado de detección de fraude en la administración pública costarricense: articulación entre control interno, analítica de datos y auditoría forense

Integrated Fraud Detection Model in Costa Rican Public Administration: Linking Internal Control, Data Analytics, and Forensic Auditing

Autor: *MBA. José Gamboa Rodríguez*

Correo electrónico: *jogamro08@gmail.com*

Universidad Internacional San Isidro Labrador

RESUMEN

El fraude en la administración pública constituye uno de los principales factores de deterioro institucional, afectando la eficiencia del gasto público, la confianza ciudadana y la gobernanza. Este estudio tiene como objetivo desarrollar un modelo integrado de detección de fraude en la administración pública costarricense, articulando el control interno basado en el marco COSO, la analítica de datos y la auditoría forense dentro de un enfoque sistémico de gestión de riesgos. Metodológicamente, se adopta un enfoque cualitativo-analítico de carácter propositivo, sustentado en la revisión sistemática de literatura científica indexada en Scopus y Web of Science (Q1–Q2).

Los resultados proponen un modelo trifásico (preventivo, detectivo e investigativo) operacionalizado mediante un árbol de decisiones que permite estructurar la identificación de riesgos, la selección metodológica y la respuesta administrativa frente al fraude. Se evidencia que la integración de herramientas analíticas avanzadas mejora la detección temprana de anomalías, mientras que la auditoría forense fortalece la calidad probatoria para la toma de decisiones legales y administrativas.

Se concluye que la articulación de estos enfoques incrementa significativamente la capacidad institucional para prevenir, detectar y sancionar el fraude, aportando un marco aplicable al sector público costarricense y potencialmente replicable en otros contextos latinoamericanos.

Palabras Claves: fraude, control interno, auditoría forense, analítica de datos, sector público, gestión de riesgos

ABSTRACT

Fraud in public administration represents a critical challenge affecting institutional efficiency, public trust, and governance. This study aims to develop an integrated fraud detection model for Costa Rican public administration by linking internal control frameworks (COSO), data analytics, and forensic auditing within a systemic risk management approach. Methodologically, the study adopts a qualitative-analytical and propositional design based on a systematic review of high-impact scientific literature indexed in Scopus and Web of Science (Q1–Q2).

The findings propose a three-phase model (preventive, detective, and investigative), operationalized through a decision tree that structures risk identification, methodological selection, and administrative response to fraud. Results indicate that advanced analytics significantly enhances early anomaly detection, while forensic auditing strengthens evidentiary robustness for administrative and legal decision-making.

The study concludes that integrating these approaches improves institutional capacity to prevent, detect, and sanction fraud, offering a framework applicable to Costa Rican public administration and adaptable to other Latin American contexts.

Keywords: fraud, internal control, forensic auditing, data analytics, public sector, risk management

1. INTRODUCCIÓN

El fraude en la administración pública es un fenómeno multidimensional que afecta la eficiencia, transparencia y legitimidad estatal. En Costa Rica y otros contextos latinoamericanos, se manifiesta en manipulación financiera, corrupción administrativa y uso indebido de recursos. Según la Association of Certified Fraud Examiners (2022), las organizaciones pierden cerca del 5% de sus ingresos anuales por fraude, lo que evidencia su impacto económico y social.

Desde una perspectiva teórica, el fraude no debe entenderse como un evento aislado, sino como el resultado de fallas sistémicas en los mecanismos de control, supervisión y toma de decisiones (Free, 2015). En este sentido, los modelos tradicionales basados exclusivamente en auditorías ex post han demostrado ser insuficientes para enfrentar esquemas fraudulentos cada vez más sofisticados y digitalizados (Albrecht et al., 2018).

El modelo integra el marco COSO como referencia en gestión de riesgos, cuya efectividad depende de su articulación con herramientas tecnológicas y analíticas (Bierstaker et al., 2014). La analítica de datos permite detectar anomalías mediante minería y aprendizaje automático (Ngai et al., 2011), mientras que la auditoría forense, esencial en la fase investigativa, aporta evidencia válida para procesos legales. Según Singleton y Singleton (2010), esta disciplina supera la auditoría tradicional al incorporar técnicas investigativas, legales y tecnológicas en la confirmación del fraude.

A pesar de estos avances, persiste una fragmentación metodológica en la práctica administrativa. Los sistemas de control interno, la analítica de datos y la auditoría forense suelen operar de manera independiente, limitando su efectividad en la detección integral del fraude (Dorminey et al., 2012). Esta desconexión es particularmente evidente en el sector público costarricense, donde las restricciones institucionales y tecnológicas dificultan la implementación de modelos integrados.

En este contexto, el artículo plantea la necesidad de un enfoque sistémico que articule estos tres componentes dentro de un modelo unificado de gestión antifraude y responda la siguiente pregunta: ¿Cómo integrar de manera sistémica el control interno, la analítica de datos y la auditoría forense para mejorar la detección del fraude en la administración pública costarricense?

El objetivo es desarrollar un modelo integrado de detección de fraude que fortalezca la toma de decisiones mediante evidencia. Estructurado en un árbol de decisiones con fases preventiva, detectiva e investigativa, aporta un marco teórico y práctico que supera la fragmentación de la literatura y ofrece una herramienta

adaptable a instituciones públicas costarricenses, reforzando gobernanza y transparencia.

2. MARCO TEÓRICO

2.1. Control interno basado en el modelo COSO

El control interno es el eje de la prevención del fraude en organizaciones públicas. Según el modelo COSO (2013), se define como un proceso que brinda seguridad razonable en el logro de objetivos de operaciones, información y cumplimiento normativo. Su enfoque sistémico se basa en cinco componentes interrelacionados: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y supervisión.

Desde una perspectiva crítica, diversos estudios han señalado que la efectividad del modelo COSO depende no solo de su implementación formal, sino de su integración con la cultura organizacional y los sistemas tecnológicos (Power, 2013). En el sector público, esta limitación es particularmente relevante debido a la rigidez normativa y la fragmentación institucional, lo que reduce la capacidad adaptativa del sistema de control interno (Lapsley & Lonsdale, 2016).

La literatura evidencia que los controles internos tradicionales presentan limitaciones frente a esquemas de fraude complejos y dinámicos. Como señalan Bierstaker et al. (2014), los métodos convencionales de auditoría detectan solo una fracción de los fraudes, debido a su enfoque reactivo y basado en muestras. En este sentido, la dependencia exclusiva del control interno puede generar una falsa percepción de seguridad organizacional.

El modelo COSO se convierte en un referente fundamental, cuando se articula con enfoques complementarios. La integración con la gestión de riesgos y la analítica de datos permite transformar el control interno en un sistema dinámico y predictivo, superando su carácter tradicionalmente estático (Beasley et al., 2015).

2.2. Analítica de datos aplicada a la detección del fraude

La analítica de datos (fraud analytics) ha emergido como un componente clave en la evolución de los sistemas antifraude, permitiendo la transición desde enfoques reactivos hacia modelos predictivos. Este enfoque se basa en el uso de técnicas como minería de datos, aprendizaje automático y análisis de anomalías para identificar patrones irregulares en grandes volúmenes de información (Ngai et al., 2011).

Desde una perspectiva empírica, estudios recientes han demostrado que la implementación de herramientas analíticas incrementa significativamente la

capacidad de detección del fraude. Por ejemplo, Jans et al. (2014) evidencian que los modelos de análisis continuo permiten identificar transacciones atípicas en tiempo real, reduciendo el tiempo de detección y el impacto económico del fraude.

Uno de los aportes más relevantes de la analítica de datos es su capacidad para detectar fraudes no evidentes mediante el reconocimiento de patrones ocultos. Técnicas como el clustering, la regresión logística y las redes neuronales han sido ampliamente utilizadas en la identificación de comportamientos fraudulentos (West & Bhattacharya, 2016). Estas herramientas permiten superar las limitaciones de los controles tradicionales, los cuales suelen basarse en reglas predefinidas.

La efectividad de la analítica de datos depende de la calidad, disponibilidad e integridad de la información. Como advierten Appelbaum et al. (2017), la ausencia de sistemas de información robustos puede generar sesgos en los modelos analíticos, afectando la precisión de los resultados. En el sector público, este desafío se ve agravado por la fragmentación de bases de datos y la falta de interoperabilidad entre instituciones.

En el caso de Costa Rica, la incorporación de analítica de datos en la administración pública es aún incipiente, lo que representa una oportunidad significativa para fortalecer los mecanismos de detección del fraude mediante la adopción de tecnologías emergentes.

2.3. Auditoría forense como mecanismo probatorio

La auditoría forense se configura como el componente investigativo del sistema antifraude, orientado a la obtención y análisis de evidencia con validez legal. A diferencia de la auditoría tradicional, cuyo enfoque se centra en la razonabilidad de los estados financieros, la auditoría forense tiene como objetivo principal la detección, documentación y sustentación del fraude en procesos administrativos y judiciales (Singleton & Singleton, 2010).

Uno de los elementos distintivos de la auditoría forense es su énfasis en la cadena de custodia y la validez probatoria de la evidencia. Como señalan Bologna y Lindquist (2018), la calidad de la evidencia es un factor crítico para el éxito de los procesos legales, lo que exige rigurosidad metodológica en la recolección y análisis de información.

Asimismo, la auditoría forense desempeña un papel fundamental en la disuasión del fraude. La existencia de mecanismos investigativos robustos incrementa la percepción de riesgo entre los potenciales infractores, reduciendo la incidencia de conductas fraudulentas (Rezaee & Riley, 2019).

No obstante, su implementación en el sector público enfrenta limitaciones relacionadas con recursos, capacidades técnicas y marcos normativos. En muchos casos, las instituciones carecen de unidades especializadas en auditoría forense, lo que dificulta la investigación efectiva del fraude.

En el contexto costarricense, el fortalecimiento de la auditoría forense representa un desafío estratégico, particularmente en lo relativo a la formación de profesionales especializados y la integración con sistemas de control interno y analítica de datos.

2.4. Gestión de riesgos bajo ISO 31000

La gestión de riesgos constituye el marco conceptual que articula los diferentes componentes del sistema antifraude. La norma ISO 31000 propone un enfoque estructurado para la identificación, análisis y tratamiento de riesgos, enfatizando la integración de la gestión de riesgos en todos los niveles de la organización (ISO, 2018).

Desde una perspectiva teórica, la gestión de riesgos permite anticipar eventos adversos y reducir la incertidumbre en la toma de decisiones. Como señalan Aven y Renn (2010), este enfoque facilita la evaluación sistemática de amenazas, incluyendo el fraude, mediante el análisis de probabilidad e impacto.

La integración de gestión de riesgos, control interno y analítica de datos fortalece los sistemas antifraude al hacerlos más robustos y adaptativos. La identificación temprana de riesgos, clave para la prevención, se alinea con el enfoque proactivo de ISO 31000 (Frigo & Anderson, 2011). Sin embargo, su implementación exige una cultura organizacional orientada a la prevención y el aprendizaje continuo, condición que en el sector público suele verse limitada por enfoques reactivos y baja capacidad de adaptación.

En Costa Rica, la adopción de estándares internacionales como ISO 31000 ha sido impulsada en diversos organismos públicos, aunque su aplicación en la gestión específica del fraude aún presenta oportunidades de mejora, especialmente en términos de integración con herramientas analíticas.

2.5. Toma de decisiones administrativas basada en evidencia

La toma de decisiones administrativas en contextos de fraude requiere un enfoque basado en evidencia que permita reducir la subjetividad y mejorar la efectividad de las acciones institucionales. Este enfoque se fundamenta en la utilización de información confiable y análisis sistemático para la selección de alternativas (Rousseau, 2006).

En el ámbito de la administración pública, la toma de decisiones basada en evidencia se enfrenta a desafíos relacionados con la disponibilidad de información, la capacidad analítica y la presión política. Como señalan Head (2016), la calidad de las decisiones depende en gran medida de la integración entre datos, conocimiento experto y contexto institucional.

La incorporación de analítica de datos y auditoría forense en los procesos de decisión permite mejorar la calidad de la evidencia disponible, fortaleciendo la legitimidad de las acciones administrativas. En este sentido, el árbol de decisiones propuesto en este estudio actúa como un mecanismo estructurador que facilita la selección de estrategias antifraude en función del tipo de riesgo y la disponibilidad de información.

Asimismo, la literatura destaca la importancia de los modelos sistémicos en la toma de decisiones complejas. Según Sterman (2000), los enfoques sistémicos permiten comprender las interrelaciones entre variables organizacionales, evitando soluciones fragmentadas que pueden generar efectos no deseados.

En el contexto del sector público costarricense, la adopción de modelos de decisión basados en evidencia representa una oportunidad para mejorar la transparencia y la eficiencia en la gestión del fraude, contribuyendo al fortalecimiento institucional.

3. METODOLOGÍA

3.1. Enfoque de investigación

El presente estudio adopta un enfoque cualitativo-analítico de carácter propositivo, orientado al diseño de un modelo integrado de detección de fraude aplicable a la administración pública costarricense. Este enfoque se fundamenta en la necesidad de trascender la mera descripción de fenómenos hacia la construcción de soluciones teóricas con aplicabilidad práctica (Gregory & Muntermann, 2014).

Desde una perspectiva epistemológica, la investigación se inscribe en el paradigma interpretativo con orientación aplicada, en el cual el conocimiento se construye a partir del análisis crítico de marcos teóricos existentes y su integración en modelos conceptuales innovadores. En este sentido, el estudio no busca probar hipótesis mediante datos empíricos directos, sino validar teóricamente un modelo a partir de evidencia científica consolidada (Venable et al., 2016).

El carácter propositivo del estudio se justifica en la necesidad de responder a problemas complejos —como el fraude en la administración pública— mediante enfoques sistémicos que integren múltiples disciplinas, incluyendo la administración, la auditoría, la analítica de datos y la gestión de riesgos.

3.2. Diseño metodológico

El diseño metodológico se estructura en tres fases complementarias:

3.2.1. Revisión sistemática de literatura

El diseño metodológico se basó en una revisión sistemática de literatura científica en Scopus y Web of Science, priorizando revistas Q1 y Q2. Se aplicaron criterios de inclusión y exclusión para garantizar calidad y rigor, considerando publicaciones entre 2015 y 2024 sobre fraude, auditoría forense, control interno, analítica de datos y gestión de riesgos. Se excluyó literatura no arbitrada, estudios con bajo rigor y enfoques meramente descriptivos.

La revisión identificó patrones teóricos, metodológicos y empíricos que sustentan el modelo integrado y su aplicación en el sector público costarricense. Se propone complementarla con análisis bibliométrico para mapear tendencias, redes académicas y vacíos temáticos, reforzando la validez del modelo y aportando una visión estratégica del campo. Según Kitchenham et al. (2009), combinar revisión sistemática con análisis cuantitativo fortalece la transparencia y reproducibilidad de los hallazgos.

3.2.2. Análisis crítico e integración teórica

La selección metodológica es una fase estratégica del modelo, basada en un enfoque adaptativo según las condiciones organizacionales. Se privilegia la pertinencia y eficiencia: controles internos robustos como primera defensa, analítica de datos en instituciones con capacidades tecnológicas y auditoría forense ante evidencia preliminar para profundizar la investigación.

Este enfoque adaptativo evita el uso indiscriminado de herramientas y promueve decisiones eficientes y contextualizadas, fortaleciendo la legitimidad institucional. Se propone un marco de evaluación multicriterio que documente la elección metodológica según costo, tiempo, impacto y riesgo, asegurando trazabilidad y transparencia. Según Denyer et al. (2008), la integración metodológica debe desarrollarse mediante procesos que combinen síntesis conceptual y relaciones causales, otorgando solidez teórica y capacidad de adaptación al modelo.

3.2.3. Diseño del modelo propuesto

El modelo integrado se diseñó bajo un enfoque sistémico, en el cual los componentes antifraude se articulan como un proceso dinámico y continuo, orientado a la prevención, detección e investigación de irregularidades. La operacionalización del modelo se materializa en un árbol de decisiones, concebido

como herramienta de apoyo a la gestión administrativa, que facilita la selección de respuestas proporcionales y contextualizadas frente a distintos escenarios de riesgo.

El diseño responde a tres principios fundamentales: la integración funcional, que asegura la coherencia entre los mecanismos de control interno, la analítica de datos y la auditoría forense; la adaptabilidad, que permite ajustar el modelo a diferentes contextos institucionales sin perder consistencia metodológica; y la orientación a evidencia, que garantiza que las decisiones se fundamenten en datos verificables y análisis rigurosos.

Se propone complementar el árbol de decisiones con un módulo de retroalimentación inteligente que registre las decisiones y evalúe su efectividad en el tiempo. Este componente refuerza la trazabilidad y transparencia, introduce aprendizaje organizacional y permite ajustar el modelo según resultados. Así, el diseño metodológico se convierte en un sistema vivo, alineado con la mejora continua y la resiliencia institucional, capaz de evolucionar ante los desafíos de la gobernanza pública.

3.3. Construcción del modelo integrado antifraude

El modelo propuesto se estructura en tres niveles metodológicos interdependientes:

3.3.1. Nivel preventivo: control interno

El nivel preventivo, basado en el marco COSO, busca reducir el fraude mediante evaluación del entorno, identificación de riesgos e implementación de controles internos. Como primera etapa del árbol de decisiones, determina indicios de riesgo y medidas iniciales de mitigación. Además, promueve una cultura organizacional sustentada en ética, transparencia y responsabilidad.

Se propone complementar este nivel con indicadores de madurez del control interno, que permitan evaluar periódicamente la efectividad de las medidas y su alineación con estándares internacionales. Este componente facilita la retroalimentación continua y asegura la adaptación de los mecanismos preventivos a cambios normativos, tecnológicos o sociales. Así, el control interno deja de ser estático y se convierte en un sistema dinámico de gestión preventiva, capaz de anticipar riesgos y fortalecer la resiliencia institucional frente al fraude.

3.3.2. Nivel detectivo: analítica de datos

Este nivel incorpora técnicas de analítica avanzada orientadas a la identificación de anomalías que podrían constituir indicios de fraude. Entre las

herramientas utilizadas se incluyen la minería de datos, los modelos predictivos y el análisis de patrones, cuyo propósito es transformar grandes volúmenes de información en evidencia verificable. A diferencia de los controles tradicionales, estas técnicas permiten detectar irregularidades sutiles o encubiertas, ampliando la capacidad institucional para anticipar riesgos y fortalecer la toma de decisiones (Jans et al., 2014).

Como mejora, se propone complementar este nivel con la implementación de sistemas de aprendizaje automático supervisado y no supervisado, capaces de evolucionar en función de nuevos datos y escenarios. Este componente adicional no solo incrementa la precisión en la detección de anomalías, sino que también introduce un mecanismo de adaptación continua frente a patrones emergentes de fraude. De esta manera, la analítica avanzada se convierte en un recurso estratégico que trasciende la mera identificación de irregularidades, consolidándose como un sistema dinámico de vigilancia y resiliencia institucional.

3.3.3. Nivel investigativo: auditoría forense

El nivel investigativo se activa ante indicios de fraude y aplica auditoría forense para confirmar hechos, identificar responsables y generar evidencia legal. Su propósito es aportar insumos sólidos a procesos administrativos y judiciales, garantizando trazabilidad y transparencia. Además, se vincula con la evaluación de evidencias del árbol de decisiones, asegurando conclusiones basadas en pruebas verificables y metodológicamente sustentadas.

Se propone un protocolo interinstitucional de cooperación para facilitar el intercambio de información entre auditorías, órganos de control y autoridades judiciales. Este mecanismo refuerza la cadena de custodia, mejora la respuesta ante casos complejos y evita la fragmentación de esfuerzos. Así, la auditoría forense se consolida como herramienta de investigación y articulación institucional, capaz de transformar hallazgos técnicos en acciones legales y administrativas que fortalezcan la integridad del sector público.

3.4. Operacionalización del árbol de decisiones

El árbol de decisiones constituye el núcleo operativo del modelo, al estructurar el proceso de detección y gestión del fraude en siete etapas secuenciales: evaluación del entorno organizacional, identificación del tipo de riesgo, selección de metodología, evaluación de evidencias, determinación del impacto, respuesta administrativa y retroalimentación con mejora continua. Este diseño metodológico permite reducir la ambigüedad en la toma de decisiones, estandarizar los procesos antifraude e integrar múltiples fuentes de información en un sistema coherente y dinámico.

Actúa como mecanismo de gobernanza adaptativa, guiando a las instituciones públicas en escenarios complejos y reduciendo la discrecionalidad. Se propone añadir un módulo de visualización interactiva para simular riesgos y evaluar consecuencias, lo que fortalece la anticipación, facilita la comunicación con actores estratégicos y aumenta la transparencia y legitimidad del proceso.

Tal como señalan Shmueli et al. (2017), los modelos basados en decisiones estructuradas mejoran la consistencia y la calidad de las decisiones en contextos complejos, lo que refuerza la pertinencia del árbol de decisiones como herramienta central en la gestión antifraude del sector público costarricense.

3.5. Validación teórica del modelo

La validación del modelo se realizó mediante un proceso de triangulación teórica, integrando evidencia proveniente de distintos campos de estudio —auditoría, ciencia de datos, gestión de riesgos y administración pública— con el fin de garantizar su coherencia interna y su alineación con la literatura científica de alto impacto (Flick, 2018). Esta estrategia permitió contrastar enfoques disciplinares, identificar puntos de convergencia y divergencia, y asegurar que la propuesta no se limite a un marco conceptual aislado, sino que se sustente en una base multidimensional.

La evaluación del modelo se realizó con criterios de calidad reconocidos en investigación aplicada. Se verificó la coherencia entre teoría y operación, su relevancia para el sector público costarricense, la capacidad explicativa del fraude desde una visión sistémica y la transferibilidad a otros contextos institucionales con mínimos ajustes, ampliando su impacto regional.

Se propone complementar la validación teórica con estudios de caso comparados que verifiquen la aplicabilidad del modelo en distintas instituciones públicas y generen evidencia práctica de su efectividad. Este componente fortalece la robustez del modelo al vincular la triangulación teórica con resultados observables en la gestión antifraude, consolidando su pertinencia y sostenibilidad en escenarios reales de gobernanza pública.

3.6. Consideraciones éticas

El estudio se fundamenta en literatura científica, sin involucrar sujetos humanos ni datos sensibles. Se asegura el uso responsable de fuentes académicas, respeto a la propiedad intelectual y rigor en la citación según APA 7.

4. RESULTADOS

4.1. Modelo integrado antifraude en la administración pública

El principal resultado de esta investigación es el diseño de un modelo integrado de detección de fraude, estructurado bajo un enfoque sistémico que articula tres niveles funcionales: preventivo, detectivo e investigativo. Este modelo responde a las limitaciones identificadas en enfoques tradicionales y propone una arquitectura operativa basada en la integración de control interno, analítica de datos y auditoría forense.

Desde una perspectiva conceptual, el modelo se fundamenta en la premisa de que el fraude es un fenómeno dinámico que requiere mecanismos adaptativos y multidimensionales. En este sentido, la integración de componentes permite generar sinergias que incrementan la capacidad institucional de respuesta (Beasley et al., 2015; Dorminey et al., 2012).

4.1.1. Fase preventiva: fortalecimiento del control interno

La fase preventiva se sustenta en el marco del Committee of Sponsoring Organizations of the Treadway Commission (COSO), orientado a la mitigación de riesgos antes de su materialización. En esta etapa, se identifican vulnerabilidades organizacionales mediante la evaluación del entorno institucional, la identificación de riesgos de fraude y el diseño e implementación de controles internos. Este nivel corresponde a la primera línea de defensa del modelo, en la cual se busca anticipar posibles irregularidades y reducir la probabilidad de ocurrencia de eventos fraudulentos.

El modelo plantea una evolución del control interno hacia un enfoque dinámico, donde los controles se ajustan continuamente según la información analítica. La prevención deja de ser estática y se convierte en un sistema adaptable a cambios normativos, tecnológicos y sociales. Como señalan Beasley et al. (2015), integrar control interno y gestión de riesgos fortalece la capacidad preventiva al vincular detección temprana con decisiones estratégicas.

En el sector público costarricense, los controles internos suelen ser estáticos y reactivos, limitando su eficacia ante fraudes sofisticados. El modelo propone incorporar indicadores de riesgo dinámicos que anticipen eventos mediante monitoreo continuo, fortaleciendo la resiliencia institucional y consolidando una cultura de prevención y transparencia, esencial para la gobernanza contemporánea.

4.1.2. Fase detectiva: analítica de datos como herramienta estratégica

La fase detectiva emplea analítica de datos para identificar anomalías en tiempo real, superando los controles periódicos y fortaleciendo la detección temprana de irregularidades (Jans et al., 2014). El modelo combina tres técnicas:

minería de datos para descubrir patrones ocultos, análisis de anomalías para detectar desviaciones y modelos predictivos para anticipar fraudes.

Estos resultados coinciden con lo planteado por Appelbaum et al. (2017), quienes destacan que la analítica avanzada transforma la auditoría en un proceso continuo, disminuyendo la dependencia de revisiones periódicas y fortaleciendo la capacidad de vigilancia institucional. Sin embargo, el análisis revela que la implementación de estas herramientas en el sector público costarricense sigue siendo limitada, principalmente por la falta de infraestructura tecnológica y de capacidades analíticas especializadas.

Se propone incorporar un plan de madurez digital institucional con fases progresivas de adopción tecnológica, desde la integración básica de sistemas hasta algoritmos avanzados de aprendizaje automático. Este enfoque gradual garantiza que la analítica de datos sea sostenible y escalable dentro del sistema antifraude. Así, la fase detectiva no solo identifica irregularidades, sino que impulsa la transformación digital del sector público, consolidando un control más proactivo, resiliente y alineado con estándares internacionales de gobernanza.

4.1.3. Fase investigativa: auditoría forense y validación del fraude

La fase investigativa se activa cuando los mecanismos detectivos generan evidencia preliminar de fraude. En esta etapa, la auditoría forense desempeña un papel central en la confirmación del fraude y la generación de evidencia con validez legal.

El modelo plantea un enfoque estructurado de auditoría forense que abarca recolección de evidencia, análisis técnico, documentación probatoria e identificación de responsables. Según Rezaee y Riley (2019), esta práctica no solo confirma el fraude, sino que también fortalece la capacidad institucional para sancionar y prevenir futuras irregularidades.

En el contexto costarricense, los resultados evidencian una necesidad crítica de fortalecer las capacidades en auditoría forense, particularmente en lo relativo a formación especializada y recursos técnicos.

4.2. Operacionalización del árbol de decisiones

El árbol de decisiones desarrollado en este estudio constituye la principal herramienta operativa del modelo integrado. Su estructura permite guiar la toma de decisiones administrativas en función de la información disponible y el tipo de riesgo identificado.

4.2.1. Evaluación del entorno organizacional

El proceso inicia con la identificación de indicios de riesgo de fraude, lo cual se alinea con los principios de gestión de riesgos establecidos por la International Organization for Standardization (ISO 31000, 2018). Esta etapa permite determinar la necesidad de activar mecanismos de control o monitoreo preventivo.

4.2.2. Identificación del tipo de fraude

La identificación del tipo de fraude es una fase crítica del modelo, que clasifica las irregularidades en fraude financiero, operativo y digital. Esta tipología orienta la selección de metodologías específicas, optimizando la detección y ajustando las respuestas institucionales al riesgo (West & Bhattacharya, 2016). El fraude financiero implica manipulación de recursos, el operativo alteración de procesos administrativos y el digital uso indebido de tecnologías de información.

El modelo no se limita a una clasificación estática, sino que propone una matriz de riesgo-fraude, en la cual cada categoría se evalúa en función de su probabilidad de ocurrencia y su impacto potencial. Esta mejora permite priorizar los esfuerzos de detección y asignar recursos de manera proporcional, fortaleciendo la capacidad institucional para enfrentar esquemas complejos y dinámicos. Además, la incorporación de esta matriz contribuye a la construcción de un enfoque más integral, en el que la tipología del fraude se vincula directamente con la gobernanza pública y la gestión estratégica de riesgos.

4.2.3. Selección de metodología

La metodología del modelo adopta un enfoque adaptativo según las condiciones de cada organización. Se privilegia la pertinencia y eficiencia: controles internos robustos como primera defensa, analítica de datos en instituciones con capacidades tecnológicas, y auditoría forense cuando existe evidencia preliminar de fraude.

Este enfoque adaptativo no solo optimiza el uso de recursos institucionales, sino que también fortalece la legitimidad de las acciones emprendidas, al garantizar que cada herramienta se aplique en el contexto adecuado. Como mejora, se propone la incorporación de un marco de criterios de selección documentados, que permita justificar la elección metodológica y asegurar la trazabilidad de las decisiones. De esta manera, el modelo se alinea con las recomendaciones de Aven y Renn (2010), quienes destacan la importancia de vincular la gestión de riesgos con procesos de gobernanza que privilegien la transparencia y la rendición de cuentas.

4.2.4. Evaluación de evidencias

La evaluación de evidencias constituye un eje central en la determinación de la existencia de fraude, al integrar de manera articulada los resultados provenientes del análisis de datos y de la auditoría forense. Este proceso no solo incrementa la calidad y confiabilidad de la información disponible para la toma de decisiones, sino que también fortalece la legitimidad institucional al basar las conclusiones en pruebas verificables y metodológicamente sustentadas. En este sentido, la evaluación rigurosa de evidencias se convierte en un puente entre la detección técnica y la acción administrativa, garantizando que las medidas adoptadas respondan a criterios objetivos y transparentes.

Como mejora, se propone la incorporación de protocolos estandarizados de validación y trazabilidad de evidencias, que permitan asegurar la consistencia en su análisis y la posibilidad de auditorías externas. Este componente metodológico añade un nivel de garantía adicional, al facilitar la revisión independiente y la rendición de cuentas. Tal como señalan Singleton y Singleton (2010), la calidad de la evidencia es determinante para la credibilidad de los hallazgos, lo que refuerza la necesidad de que los procesos de evaluación se desarrollen bajo estándares internacionales y con una perspectiva de mejora continua.

4.2.5. Determinación del impacto

El modelo clasifica el impacto del fraude en tres niveles —bajo, medio y alto— para diseñar respuestas proporcionales según principios de gestión de riesgos y gobernanza pública. Esta tipología optimiza la asignación de recursos y prioriza acciones correctivas: ajustes operativos en impactos bajos, reestructuración de procesos en impactos medios y sanciones ejemplarizantes junto con reformas estructurales en impactos altos, fortaleciendo la resiliencia institucional.

Como mejora, se propone complementar esta clasificación con la incorporación de criterios cualitativos, tales como el efecto reputacional, la confianza ciudadana y la legitimidad institucional. De este modo, el modelo no se limita a medir el impacto en términos cuantitativos, sino que reconoce la dimensión social y política del fraude. Tal como señalan Aven y Renn (2010), la gestión de riesgos en el sector público debe integrar tanto la probabilidad y severidad de los eventos como sus implicaciones para la gobernanza democrática, lo que refuerza la pertinencia de una clasificación multidimensional en el contexto costarricense.

4.2.6. Respuesta administrativa

La respuesta administrativa al fraude se concibe como un proceso integral que incluye corrección, prevención y sanción. El modelo contempla controles

correctivos para cerrar brechas, reestructuración de procesos para optimizar la eficiencia y sanciones que aseguren responsabilidad administrativa y fortalezcan la credibilidad del sistema antifraude.

Este enfoque garantiza que la detección de irregularidades se traduzca en medidas concretas que refuercen el control interno. Se propone incorporar un mecanismo de trazabilidad para documentar y evaluar el impacto de cada acción, orientando la respuesta institucional no solo a la corrección inmediata, sino también a la generación de aprendizajes que fortalezcan la cultura de integridad.

Tal como señala la literatura especializada, “la efectividad de los sistemas antifraude depende de su capacidad para transformar la detección en acción” (OECD, 2020), lo cual reafirma la necesidad de que las medidas administrativas se integren en un ciclo de mejora continua y de rendición de cuentas.

4.2.7. Retroalimentación y mejora continua

El modelo incorpora un ciclo de retroalimentación que permite ajustar de manera sistemática los sistemas de control interno, alineándose con el enfoque de mejora continua, promovido por la norma ISO 31000. Este proceso no se concibe como una etapa final, sino como un mecanismo permanente de aprendizaje organizacional, en el cual los resultados obtenidos retroalimentan las decisiones estratégicas y operativas. La lógica de mejora continua asegura que las instituciones públicas no solo corrijan desviaciones, sino que también identifiquen oportunidades de innovación y adaptación frente a cambios normativos, tecnológicos y sociales.

Como mejora, se propone complementar este ciclo con la incorporación de indicadores de desempeño y métricas de impacto, que permitan evaluar no solo la eficiencia de los controles internos, sino también su contribución a la transparencia, la confianza ciudadana y la legitimidad institucional. De esta manera, la retroalimentación deja de ser un ejercicio meramente técnico y se convierte en un instrumento de gobernanza, capaz de fortalecer la resiliencia organizacional y consolidar una cultura de integridad en el sector público costarricense.

4.3. Aplicación al sector público costarricense

La aplicación del modelo al contexto costarricense revela un panorama complejo, marcado por avances significativos en materia de transparencia y digitalización, pero también por limitaciones estructurales que condicionan su efectividad. El análisis evidencia tanto fortalezas como debilidades que deben ser consideradas en la implementación.

Entre las fortalezas, destaca la existencia de marcos normativos sólidos en materia de control interno, los cuales proporcionan una base jurídica y

procedimental para la adopción del modelo. Asimismo, se observa un creciente interés institucional en promover la transparencia y la rendición de cuentas, lo que favorece la aceptación de herramientas innovadoras. A esto se suma el progreso en procesos de digitalización, que ha permitido modernizar ciertos sistemas administrativos y abrir la puerta a la integración tecnológica.

Persisten debilidades que limitan la respuesta del sector público: la integración de sistemas sigue fragmentada, dificultando información confiable; la adopción de analítica de datos es incipiente, reduciendo la capacidad de anticipar riesgos; y la falta de especialistas en auditoría forense restringe la aplicación de metodologías avanzadas para investigar fraudes y corrupción.

Estos hallazgos coinciden con estudios sobre gobernanza pública en América Latina, que subrayan la necesidad de modernizar los sistemas de control mediante la incorporación de tecnologías avanzadas y el fortalecimiento de las competencias institucionales (OECD, 2020). En el caso costarricense, la aplicación del modelo no solo permitiría superar las limitaciones identificadas, sino también consolidar una cultura organizacional orientada a la prevención y detección temprana de riesgos.

Se propone incorporar un componente de articulación interinstitucional que fomente la cooperación entre entidades públicas en el intercambio de datos, metodologías y buenas prácticas. Este eje colaborativo reduce la fragmentación, potencia la analítica avanzada y fortalece capacidades técnicas. Así, el modelo trasciende el fortalecimiento aislado de cada institución y contribuye a un ecosistema público más robusto, transparente y resiliente frente a los desafíos de la gobernanza contemporánea.

4.4. Propuesta operativa para la implementación

El modelo plantea una hoja de ruta progresiva y articulada para su incorporación en instituciones públicas costarricenses, concebida como un proceso dinámico que combina diagnóstico, fortalecimiento de capacidades, formación del recurso humano y evaluación constante.

En primer lugar, se propone un diagnóstico institucional que permita identificar las capacidades existentes en materia de control interno, tecnología y auditoría. Este ejercicio inicial no solo delimita el punto de partida, sino que también visibiliza las brechas que deben ser atendidas para garantizar la viabilidad del modelo.

Posteriormente, se plantea el fortalecimiento de los sistemas de información, mediante la integración de bases de datos y la mejora en la calidad de los registros. La consolidación de información confiable y accesible constituye un requisito

indispensable para la toma de decisiones fundamentadas y para la aplicación rigurosa de técnicas de auditoría forense.

El tercer componente corresponde a la capacitación del personal, orientada a la formación en analítica de datos y auditoría forense. La transferencia de conocimientos y habilidades asegura que los equipos institucionales cuenten con las competencias necesarias para interpretar la información y aplicar el modelo con criterios técnicos y éticos.

Una vez fortalecidas las capacidades, se plantea la implementación del árbol de decisiones como herramienta de gestión. Este instrumento se convierte en un mecanismo operativo que guía la respuesta institucional frente a situaciones críticas, estandarizando procedimientos y reduciendo la discrecionalidad en la toma de decisiones.

Finalmente, el modelo incorpora un eje de evaluación continua, que permite monitorear su desempeño y realizar ajustes en función de los resultados obtenidos. Este componente asegura la sostenibilidad del modelo, al promover la retroalimentación constante y la adaptación a los cambios en el entorno institucional.

En conjunto, la propuesta operativa se concibe como un proceso integral que articula diagnóstico, fortalecimiento, capacitación, implementación y evaluación, garantizando que el modelo no se limite a un diseño teórico, sino que se traduzca en prácticas efectivas y sostenibles dentro de la administración pública costarricense.

6. CONCLUSIONES

El estudio tuvo como objetivo desarrollar un modelo integrado de detección de fraude en la administración pública costarricense, articulando control interno (COSO), analítica de datos y auditoría forense dentro de un enfoque sistémico de gestión de riesgos. Los resultados evidencian que la fragmentación de estos enfoques es una debilidad clave en los sistemas antifraude, limitando su capacidad de respuesta ante esquemas cada vez más complejos y digitalizados.

En primer lugar, el control interno, aunque esencial, resulta insuficiente si actúa de forma aislada. Su efectividad depende de integrarse con herramientas analíticas capaces de detectar anomalías en tiempo real y anticipar fraudes. En este marco, la analítica de datos se convierte en un componente estratégico que transforma la auditoría en un sistema continuo y predictivo, superando el enfoque tradicional de revisiones periódicas.

En segundo lugar, la auditoría forense se consolida como un elemento indispensable para la validación del fraude, aportando rigor probatorio y

fortaleciendo la capacidad institucional para la sanción de conductas ilícitas. Su integración dentro del modelo propuesto permite cerrar el ciclo antifraude, garantizando que la detección se traduzca en acciones concretas y legalmente sustentadas.

En tercer lugar, la incorporación de los principios de gestión de riesgos promovidos por la International Organization for Standardization (ISO 31000) permite estructurar el proceso antifraude dentro de un enfoque preventivo y sistemático. Esta integración facilita la identificación temprana de riesgos y mejora la calidad de la toma de decisiones administrativas.

Uno de los principales aportes del estudio es la operacionalización del modelo mediante un árbol de decisiones, el cual actúa como herramienta estructuradora del proceso antifraude. Este instrumento permite reducir la ambigüedad en la toma de decisiones, estandarizar procedimientos y optimizar la selección de metodologías en función del tipo de riesgo y la disponibilidad de información.

Desde una perspectiva aplicada, el modelo ofrece una hoja de ruta clara para su implementación en el sector público costarricense. Su efectividad dependerá de factores como la madurez tecnológica, la calidad de los sistemas de información y el desarrollo de capacidades institucionales en analítica de datos y auditoría forense.

En términos de contribución académica, el estudio aporta un enfoque integrador que supera la fragmentación existente en la literatura sobre fraude, proponiendo una arquitectura sistémica que articula prevención, detección e investigación. Este aporte resulta particularmente relevante para contextos latinoamericanos, donde los desafíos en materia de gobernanza y transparencia requieren soluciones innovadoras y basadas en evidencia.

Finalmente, se concluye que la implementación de modelos integrados antifraude no solo contribuye a la reducción de pérdidas económicas, sino que fortalece la confianza ciudadana y la legitimidad institucional. En este sentido, el modelo propuesto constituye una herramienta estratégica para la modernización de la administración pública y el fortalecimiento de los sistemas de control.

REFERENCIAS

- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2018). *Fraud examination* (5th ed.). Cengage Learning.
- Appelbaum, D., Kogan, A., Vasarhelyi, M., & Yan, Z. (2017). Impact of business analytics and enterprise systems on managerial accounting.

International Journal of Accounting Information Systems, 25, 29–44. https://doi.org/10.1016/j.accinf.2017.03.003

- Aven, T., & Renn, O. (2010). Risk management and governance: Concepts, guidelines and applications. *Risk Analysis, 30*(4), 659–674. https://doi.org/10.1111/j.1539-6924.2010.01368.x
- Beasley, M. S., Clune, R., & Hermanson, D. R. (2015). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 34*(3), 219–243. https://doi.org/10.1016/j.jaccpubpol.2015.01.001
- Bierstaker, J. L., Brody, R. G., & Pacini, C. (2014). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal, 29*(5), 520–536.
- Bologna, J., & Lindquist, R. (2018). *Fraud auditing and forensic accounting*. Wiley.
- Denyer, D., Tranfield, D., & Van Aken, J. (2008). Developing design propositions through research synthesis. *Organization Studies, 29*(3), 393–413.
- Dorminey, J., Fleming, A., Kranacher, M., & Riley, R. (2012). The evolution of fraud theory. *Issues in Accounting Education, 27*(2), 555–579.
- Flick, U. (2018). *An introduction to qualitative research* (6th ed.). Sage.
- Free, C. (2015). Looking through the fraud triangle. *Accounting, Organizations and Society, 45*, 1–17.
- Gregory, R. W., & Muntermann, J. (2014). Hevner's IS research framework revisited. *Information Systems Journal, 24*(6), 495–504.
- Head, B. W. (2016). Toward more "evidence-informed" policy making? *Public Administration Review, 76*(3), 472–484.
- Jans, M., Alles, M., & Vasarhelyi, M. (2014). A field study on continuous auditing. *Journal of Information Systems, 28*(2), 63–77.
- Kitchenham, B., et al. (2009). Systematic literature reviews in software engineering. *Information and Software Technology, 51*(1), 7–15.
- Lapsley, I., & Lonsdale, J. (2016). New public management and risk management. *Financial Accountability & Management, 32*(1), 3–21.
- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data
  mining techniques in financial fraud detection. *Decision Support Systems, 50*(3), 559–569.
- Organization for Economic Co-operation and Development. (2020). *Public integrity handbook*. OECD Publishing.
- Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society, 38*(6–7), 525–543.
- Rezaee, Z., & Riley, R. (2019). *Financial statement fraud: Prevention and detection*.
  Wiley.
- Rousseau, D. M. (2006). Is there such a thing as "evidence-based management"?

Academy of Management Review, 31(2), 256–269.

- Shmueli, G., Bruce, P., & Patel, N. (2017). *Data mining for business analytics*. Wiley.
- Singleton, T., & Singleton, A. (2010). *Fraud auditing and forensic accounting* (4th ed.). Wiley.
- Sterman, J. (2000). *Business dynamics: Systems thinking and modeling*. McGraw-Hill.
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection. *Decision Support Systems, 50*(3), 559–569.