

Propuesta de un Modelo de Gobernanza de Datos para el Uso Seguro de Herramientas de Inteligencia Artificial en los Procesos Contables y Tributarios en las Organizaciones.

Angelica María Acevedo Ortiz, Leidy Johana Martínez Sabatà, Luz Mary Medina

Rincón

Informe consolidado del Diplomado en Transformación Digital de la Contaduría:

Analítica de Datos, Power BI e Inteligencia Artificial como opción de grado

Director

Carmen Cecilia Martínez Duran

Especialista en Finanzas y Docencia Universitaria

Universidad Santo Tomás, Bucaramanga

División de Ciencias Económicas, Administrativas y Contables

Especialización en Gerencia Tributaria

2026

Contenido

Introducción	8
1. Propuesta de un modelo de gobernanza de datos para el uso seguro de herramientas de inteligencia artificial en los procesos contables y tributarios en las organizaciones.	9
1.1 Planteamiento del problema	9
1.2 Justificación.....	10
1.3 Objetivos	12
1.3.1. Objetivo general	12
1.3.2 Objetivos específicos	12
2. Casuística	12
2.3 Marco legal.....	17
2.3.1 Normativa constitucional y legal de protección de datos	18
2.3.2 Regulación sectorial contable, tributaria y de tecnologías de la información	19
2.3.3 Estándares y proyectos normativos sobre inteligencia artificial	20
2.3.4 Acuerdos de confidencialidad y tratamiento de información del caso de estudio.....	22
3. Resultados	23
3.1. Riesgos asociados al uso de herramientas de IA en procesos contables y tributarios	23
3.2. Clasificación de datos según nivel de sensibilidad	25
3.3. Medidas de protección y anonimización recomendadas	25
3.4 Componentes del modelo de gobernanza de datos propuesto.....	28
3.5 Guía de buenas prácticas resultante	30
4. Conclusiones	31

Referencias..... 34

Lista de tablas

Tabla 1. <i>Riesgos, controles de gobernanza y buenas prácticas para el uso de IA</i>	14
Tabla 2. <i>Categorización y nivel de criticidad de los riesgos asociados al uso de inteligencia artificial en la gestión contable</i>	23
Tabla 3. <i>Distribución porcentual de riesgos derivados del uso de Inteligencia Artificial en contabilidad</i>	24
Tabla 4. <i>Clasificación según nivel de sensibilidad</i>	25
Tabla 5. <i>Medidas de protección y anonimización para el uso seguro de IA</i>	26
Tabla 6. <i>Componentes del modelo de gobernanza de datos para uso seguro de IA</i>	28
Tabla 7. <i>Guía de buenas prácticas para el uso seguro de IA en contabilidad</i>	30

Lista de figuras

Figura 1. *Flujo de Uso Seguro de Inteligencia Artificial en Procesos Contables y Tributarios.* 27

Figura 2. *Modelo de gobernanza de datos para uso seguro de IA en contabilidad* 29

Resumen

El uso elevado de la inteligencia artificial en procesos contables y tributarios ha incrementado el riesgo de exponer la información y los datos de las organizaciones ya que no existen procesos o políticas que permitan salvaguardar dicha información. Es por ello que se hace necesario diseñar una propuesta de política de gobernanza de Datos que contribuya al uso seguro de la inteligencia artificial por parte de los contadores Públicos en Colombia desarrollando una investigación basada en normas y modelos nacionales e internacionales y que nos permita aplicarlo al contexto contable. Como resultado final se obtendrá una guía de buenas prácticas para la clasificación, anonimización y protección de los datos y así fortalecer la seguridad de la información en nuestra profesión contable .

Palabras clave: gobernanza, política, normas, uso seguro, herramientas

Abstract

The increasing use of artificial intelligence in accounting and tax processes has heightened the risk of exposing organizational information and data, given the absence of processes or policies capable of safeguarding such information. Consequently, designing a data governance policy proposal that promotes the safe use of artificial intelligence by public accountants in Colombia becomes essential. This research, grounded in national and international standards and models, seeks to adapt these frameworks to the accounting context. As a final outcome, a best-practices guide is produced for the classification, anonymization, and protection of data, thereby strengthening information security within the accounting profession.

Keywords: governance, policy, standards, safe use, tools

Introducción

La transformación digital está cambiando la profesión contable y actualmente es necesario poder cambiar la mentalidad y cambiar el chip como profesionales ya que se es urgente mejorar el tiempo de varios procesos que permita obtener resultados óptimos, ágiles y confiables.

La IA llegó para quedarse y para transformar el día a día de esta profesión; miles de organizaciones, contadores y asesores tributarios la utilizan y dan fe de los resultados que se obtienen con el plus actual que es la mejor administración del tiempo. ¿Pero ahora aparece un nuevo riesgo y es que pasa con los datos? ¿Qué pasa con la privacidad? ¿Qué pasa con la información tributaria?

Aunque existen marcos internacionales sobre inteligencia artificial y gobierno de datos, aun son escasas en Colombia las propuestas orientadas a proteger específicamente nuestra profesión contable, especialmente en el uso cotidiano de la Inteligencia Artificial para el tratamiento de datos, contable, financiera y tributarios.

Es por ello que el presente trabajo no solo muestra a manera de investigación que normas existen, sino que también nos dará como resultado final una guía práctica aplicada a el ejercicio de la profesión contable para garantizar que medidas se deben implementar a la hora de usar la IA y como salvaguardamos de esta manera la información frente a garantizar protección de datos, reducir riesgos y fortalecer prácticas de conducta Ética que ayude a firmas contables y contadores.

En este contexto, el presente estudio tiene como objetivo diseñar un modelo de gobernanza de datos que permita orientar el uso seguro y responsable de herramientas de inteligencia artificial en los procesos contables y tributarios desarrollados por los profesionales de la contaduría pública en Colombia.

1. Propuesta de un modelo de gobernanza de datos para el uso seguro de herramientas de inteligencia artificial en los procesos contables y tributarios en las organizaciones.

1.1 Planteamiento del problema

En atención al creciente desarrollo de la industria de la inteligencia artificial y el impacto provocado a partir de su adopción; Vemos que hay una gran tendencia a buscar soluciones que abarcan desde las tareas más complejas cómo lo implica la analítica de datos hasta las actividades más cotidianas como asistencia para el manejo de automóviles.

De igual forma, vemos que, en las organizaciones, no es ajeno su uso consumando la automatización de tareas y la eliminación de errores en la contabilización de los hechos económicos y su proyección de los datos en la elaboración de los informes.

Al mismo tiempo, la responsabilidad por parte de la gerencia, de optimizar los recursos disponibles para mantener la operación competitiva y vanguardista obliga a la implementación de las herramientas basadas en inteligencia artificial que se encuentren disponibles en el mercado.

De esta manera, este panorama motiva la transformación a las medidas y políticas de control interno en aras de administrar el riesgo sobre el saber hacer y el cumplimiento de las regulaciones, entre estas la ley de protección de datos; puesto que diariamente es constante la construcción de bases de datos que contiene información de clientes, proveedores y laborales. En consecuencia, se hace necesario la incorporación en los manuales y políticas internas de cualquier organización la administración del riesgo emergente.

En este sentido, el concepto de gobernanza de datos toma relevancia para la construcción de un modelo de políticas internas visualizando el rápido progreso de la inteligencia artificial

frente a un letargo en su asimilación en los procedimientos de control interno y del aseguramiento de la información, es así, como se hace necesario resolver esa distancia y como primera medida es conocer la asistencia que brinda la implementación de estas políticas y un modelo que le de resolución pero, ¿Cómo debe diseñarse un modelo de control interno que integre principios de gobernanza de datos para garantizar la confiabilidad, trazabilidad y cumplimiento normativo en los procesos contables y tributarios asistidos por inteligencia artificial en las organizaciones?

1.2 Justificación

Actualmente, los profesionales contables utilizan soluciones basadas en IA para apoyar actividades como el análisis de información financiera, la elaboración de informes, la interpretación de normas, la revisión de contratos y la automatización de tareas repetitivas. Sin embargo, el uso creciente de estas tecnologías también ha generado nuevos desafíos asociados con la protección de la información financiera, tributaria y de los datos personales administrados por los contadores públicos.

Uno de los principales riesgos consiste en el suministro de información confidencial a plataformas de inteligencia artificial sin la aplicación de criterios de gobernanza de datos que permitan garantizar su clasificación, protección, anonimización y uso responsable. Esta situación puede comprometer la confidencialidad de la información, incrementar la exposición a riesgos legales y reputacionales, así como afectar el cumplimiento de la normativa vigente sobre protección de datos personales y de los principios éticos que rigen el ejercicio profesional del contador público.

En Colombia, si bien existen disposiciones legales relacionadas con la protección de datos personales, la seguridad de la información y la ética profesional, aún no se cuenta con lineamientos

específicos que orienten el uso seguro de herramientas de inteligencia artificial en la aplicación de los procesos contables y tributarios. Esta ausencia de normas y directrices evidencia la necesidad de desarrollar propuestas que permitan adaptar los principios de gobernanza de datos al contexto de la profesión contable, considerando las características particulares de la información que administra este tipo de organizaciones.

La presente investigación adquiere relevancia tanto desde el punto de vista académico como profesional, al proponer un modelo de gobernanza de datos que contribuya a orientar el uso responsable de la inteligencia artificial en los procesos contables y tributarios. El modelo busca integrar buenas prácticas internacionales de gestión y protección de datos con la normativa colombiana vigente, ofreciendo herramientas que permitan reducir riesgos asociados al tratamiento de información mediante IA.

Desde el punto de vista práctico, la investigación pretende proporcionar a contadores públicos, firmas de auditoría, consultores tributarios y organizaciones una guía de referencia para establecer políticas de clasificación de la información, procedimientos de anonimización de datos, controles sobre el uso de herramientas de inteligencia artificial y mecanismos de supervisión que fortalezcan la seguridad de la información y el cumplimiento normativo.

Finalmente, el trabajo aporta al proceso de transformación digital de la profesión contable al promover una cultura de uso ético, seguro y responsable de la inteligencia artificial, fortaleciendo la confianza en estas tecnologías y contribuyendo a que su adopción se realice bajo principios de transparencia, responsabilidad, protección de datos y adecuada gestión del riesgo.

1.3 Objetivos

1.3.1. Objetivo general

Diseñar un modelo de política de Gobernanza de datos frente al uso de la inteligencia Artificial que contribuya a la gestión del riesgo en los procesos contables y tributarios desarrollados por la contaduría pública en Colombia

1.3.2 Objetivos específicos

Identificar los principales riesgos asociados al uso de herramientas de la Inteligencia Artificial en el tratamiento de información contable, tributaria y Financiera.

Analizar estándares Internacionales, Normas y buenas prácticas relacionadas con la gobernanza de datos, la protección de la información y el correcto uso de la IA

Evaluar la aplicación de principio de gobernanza de datos mediante el análisis de un caso práctico relacionado con el uso de la inteligencia artificial en procesos contables y tributarios.

Proponer un modelo de Gobernanza de datos que incluya políticas, procedimientos y controles para el uso seguro de herramientas de inteligencia Artificial en los procesos contables y tributarios.

2. Casuística

Caso de estudio: Uso de la inteligencia Artificial en una firma contable para la elaboración de conceptos, análisis financiero, revisión de documentos y Proyección de respuestas a entidades

Descripción del caso:

La firma contable Asesorías Contables QUANTIFIKA. presta servicios de contabilidad, asesoría tributaria y auditoría a pequeñas y medianas empresas del sector comercial.

Con El propósito de obtener mejores resultados en su productividad, los colaboradores de la firma utilizan herramientas de inteligencia Artificial para apoyarse en actividades como:

- elaboración de conceptos tributarios

- análisis de estados financieros

- redacción de respuestas a requerimientos de la DIAN – ALCALDIAS – ENTES GUBERNAMENTALES

- revisión de contratos

- elaboración de informes de auditoría.

Al revisar el proceso del uso de la IA se puede observar que la empresa no cuenta con una política interna que delimite que información puede compartirse, ni que procedimientos para proteger los datos de los clientes se están utilizando. Como consecuencia, se puede evidenciar que se caga información confidencial tales como:

- Estados Financieros.

- Nómina.

- Contratos laborales.

- Certificados bancarios.

- Información de proveedores.

- Bases de datos de clientes.

- Copias de cédulas.

- Información tributaria

A continuación, se detallan los riesgos identificados:

Tabla 1 *Riesgos, controles de gobernanza y buenas prácticas para el uso de IA*

Riesgo identificado	Control de gobernanza	Buena práctica en el uso de IA
Tratamiento no autorizado de datos personales	Establecer una política que defina qué datos personales pueden ser tratados mediante herramientas de IA y quién está autorizado para hacerlo.	No cargar nombres, cédulas, NIT, direcciones, teléfonos u otros datos identificables sin autorización y controles adecuados.
Exposición de información financiera	Clasificar la información financiera según su nivel de confidencialidad y restringir su ingreso a herramientas de IA.	Utilizar información anonimizada o datos ficticios cuando sea suficiente para realizar el análisis solicitado.
Uso de herramientas de IA sin autorización institucional	Definir herramientas de IA autorizadas, usuarios habilitados y finalidades permitidas.	Utilizar únicamente plataformas aprobadas por la organización y seguir la política interna de uso de IA.
Falta de anonimización de los datos	Implementar un procedimiento previo de anonimización o seudonimización de la información.	Sustituir nombres, NIT, cuentas bancarias y demás identificadores por códigos o información genérica antes de realizar la consulta.
Ausencia de políticas internas para el uso de IA	Crear y comunicar una política institucional que establezca responsabilidades, restricciones y procedimientos para el uso de IA.	Consultar la política antes de cargar información y reportar cualquier incidente o uso inadecuado.
Información incorrecta generada por IA	Establecer un proceso obligatorio de revisión y validación de los resultados generados por IA.	Contrastar las respuestas con fuentes normativas y técnicas confiables antes de utilizarlas en procesos contables o tributarios.
Falta de revisión humana	Asignar un responsable para revisar y aprobar los resultados producidos o apoyados por IA.	El contador debe ejercer juicio profesional y no utilizar directamente una respuesta de IA sin verificar su exactitud y pertinencia.

2.1. Marco conceptual

Inteligencia Artificial (IA): Conjunto de tecnologías y sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el análisis de datos, la interpretación de

normas, la redacción de documentos y la automatización de procesos contables y tributarios. (Union europea, 2024)

Gobernanza de Datos: Sistema de políticas, procedimientos, roles, responsabilidades y estándares que garantiza la disponibilidad, usabilidad, integridad, seguridad y cumplimiento normativo de los datos en una organización. (ISO/IEC 38505-1,2017)

Ciclo de Vida del Dato: Conjunto de fases por las que transita la información (creación, almacenamiento, procesamiento, compartición, archivo y destrucción). En el caso de estudio, la fase crítica radica en la compartición e ingesta de datos sensibles hacia plataformas externas de IA. (ISO/IEC 38505-1, 2017)

Seguridad de la Información: Conjunto de medidas técnicas, administrativas y físicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos frente a accesos no autorizados, pérdidas o alteraciones. (ISO/IEC 27001,2022).

Confidencialidad: Garantía de que la información contable, financiera y tributaria no sea expuesta a personas o sistemas no autorizados (ej. servidores de IA de terceros). (ISO/IEC 27001, 2022; Ley 1581, 2012).

Integridad: Salvaguarda de la exactitud y totalidad de los datos financieros. (ISO/IEC 27001, 2022).

Disponibilidad: Acceso oportuno a la información requerida para el cumplimiento de obligaciones legales. (ISO/IEC 27001, 2022).

Fuga de Datos (Data Leakage): Incidente de seguridad donde información confidencial o protegida (RUT, estados financieros, nómina) es transmitida sin autorización a un entorno no controlado, como los algoritmos de entrenamiento de IA públicas. (Superintendencia de Industria y Comercio [SIC], 2024).

Riesgo de IA: Posibilidad de que el uso de herramientas de inteligencia artificial genere impactos negativos, como la exposición de datos confidenciales, la toma de decisiones erróneas, el incumplimiento normativo o daños reputacionales. (National Institute of Standards and Technology [NIST], 2023).

Riesgo Emergente Tecnológico: Nuevos factores de vulnerabilidad o incertidumbre que surgen del despliegue apresurado de tecnologías destructivas/innovadoras (IAG) sin un marco de control interno preconcebido. (Superintendencia de Sociedades, 2025)

Política de Gobernanza de Datos: Documento formal que establece los lineamientos, principios y controles para el tratamiento adecuado de los datos, incluyendo su clasificación, anonimización, almacenamiento, acceso y uso en herramientas de IA. (ISO/IEC 38505-1, 2017)

Clasificación de Datos: Proceso de categorizar la información según su nivel de sensibilidad (pública, interna, confidencial, crítica) para aplicar medidas de protección diferenciadas. (ISO/IEC 27001, 2022)

Anonimización de Datos: Técnica de protección que elimina o transforma los identificadores personales de un conjunto de datos, de modo que la información no pueda asociarse a un individuo específico, reduciendo riesgos de privacidad. (Centro Interamericano de Administraciones Tributarias [CIAT], 2026).

Procesos Contables y Tributarios: Actividades propias de la profesión contable que incluyen la elaboración de estados financieros, declaraciones de impuestos, análisis financiero, auditoría y atención de requerimientos de entidades como la DIAN. (Ley 43, 1990)

Ética Profesional Contable: Conjunto de principios y valores que orientan el ejercicio responsable, transparente y confiable del contador público, incluyendo el deber de proteger la

información de clientes y cumplir con la normativa vigente. (Ley 43, 1990; Instituto Nacional de Contadores Públicos [INCP], 2026)

Habeas Data: Derecho constitucional que tienen las personas a conocer, actualizar, rectificar y controlar el uso de su información personal almacenada en bases de datos. (Constitución Política de Colombia, 1991, art. 15; Ley 1266, 2008; Ley 1581, 2012)

Control Interno: Sistema integrado de políticas y procedimientos diseñados para garantizar la eficiencia operativa, la confiabilidad de la información financiera y el cumplimiento de leyes y regulaciones. (Decreto 2420, 2015)

Transformación Digital: Proceso de adopción de tecnologías digitales para mejorar la eficiencia, calidad y competitividad de los procesos organizacionales, incluyendo la incorporación de IA en la práctica contable. (CONPES 3975, 2019)

2.2 Marco legal

El marco legal de la presente investigación integra el conjunto de normas nacionales e internacionales, así como los acuerdos de confidencialidad y lineamientos institucionales que dan soporte teórico, analítico y jurídico al diseño del modelo de gobernanza de datos para el uso seguro de la inteligencia artificial en procesos contables y tributarios en Colombia. Este apartado se articula en tres dimensiones: (I) normativa constitucional y legal de protección de datos; (II) regulación sectorial contable, tributaria y de tecnologías de la información; (III) estándares y proyectos normativos sobre inteligencia artificial; y (IV) Normas y estándares internacionales que se analizaron para evaluar el riesgo, producir resultados trazables y verificables sin delegar el juicio profesional

2.2.1 Normativa constitucional y legal de protección de datos

La Constitución Política de Colombia de 1991, en su Artículo 15, reconoce el derecho fundamental a la intimidad personal y familiar, al buen nombre y a la protección de datos personales, estableciendo que las personas tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas. Este mandato constitucional constituye el fundamento jurídico primario que obliga a los contadores públicos y a las organizaciones a garantizar la confidencialidad, integridad y seguridad de la información personal y sensible que administran en el ejercicio de su profesión.

La Ley Estatutaria 1581 de 2012 desarrolla el derecho constitucional a la protección de datos personales y establece el régimen general aplicable a todo tratamiento de datos en territorio colombiano, independientemente de la naturaleza pública o privada del responsable o encargado. Esta norma consagra los principios rectores del tratamiento de datos (libertad, veracidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad) y reconoce los derechos de los titulares (conocer, actualizar, rectificar, suprimir, revocar la autorización, presentar quejas ante la Superintendencia de Industria y Comercio). Para el caso de la firma QUANTIFIKA, la Ley 1581 implica la obligación de contar con políticas de tratamiento de datos, manuales internos, canales de atención a titulares y medidas de seguridad técnicas y administrativas antes de cargar información de clientes en herramientas de IA.

El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 de 2012 y establece requisitos específicos para el consentimiento informado, las políticas de tratamiento de datos, los avisos de privacidad y las medidas de seguridad en entornos digitales, incluyendo la obligación de implementar protocolos de seguridad para el almacenamiento y transmisión de datos personales. Este decreto es particularmente relevante para el uso de IA, ya que exige que los responsables y

encargados del tratamiento adopten medidas técnicas (cifrado, control de acceso, trazabilidad) y organizacionales (capacitación, auditoría, gestión de incidentes) para proteger la información contra accesos no autorizados, pérdidas o alteraciones.

La Ley 1266 de 2008 regula el manejo de información financiera, crediticia, comercial y de servicios, estableciendo límites al tratamiento automatizado de datos y garantizando el derecho al habeas data en el ámbito económico. Esta norma es aplicable a los procesos contables y tributarios asistidos por IA, ya que los estados financieros, declaraciones de renta, información de proveedores y bases de datos de clientes constituyen información financiera y comercial protegida por esta ley.

La Ley 1341 de 2009 (Ley General de Telecomunicaciones y TIC) define los principios y orientaciones sobre el uso de las tecnologías de la información y las comunicaciones, incluyendo la protección de datos, la seguridad de la información y la promoción de la competencia en el mercado digital. Aunque no regula específicamente la IA generativa, esta ley proporciona un marco legal que guía el uso adecuado de tecnologías emergentes en la contabilidad y finanzas, estableciendo obligaciones de seguridad, privacidad y ética en el tratamiento de datos a través de medios electrónicos.

2.2.2 Regulación sectorial contable, tributaria y de tecnologías de la información

El Código de Ética del Contador Público, establecido en la Ley 43 de 1990 y desarrollado en el Decreto 2420 de 2015, consagra los principios fundamentales de integridad, objetividad, independencia, confidencialidad y comportamiento profesional que deben orientar el ejercicio de la contaduría pública en Colombia. En el contexto de la IA, estos principios implican que el contador debe mantener el control humano sobre decisiones críticas, evitar el uso de herramientas

que comprometan la confidencialidad de la información de clientes y garantizar la trazabilidad y explica los procesos automatizados.

La Superintendencia de Sociedades, mediante sus planes estratégicos de tecnologías de la información (PETI/PTRI 2025-2026), ha emitido lineamientos sobre la gestión de riesgos tecnológicos, la protección de datos y la adopción responsable de tecnologías emergentes en el sector empresarial, incluyendo la obligación de las sociedades vigiladas de implementar controles de seguridad de la información y políticas de gobernanza de datos. Estos lineamientos son aplicables a las firmas contables que prestan servicios a empresas vigiladas por la Superintendencia.

2.2.3. Estándares y proyectos normativos sobre inteligencia artificial

El Documento CONPES 3975 de 2019 constituye el punto de partida de la política nacional de inteligencia artificial en Colombia, definiendo directrices para promover el desarrollo de capacidades técnicas, la adopción ética y la coordinación interinstitucional en materia de IA. Este documento estratégico establece los lineamientos para la formación de talento humano, la investigación y desarrollo, y la adopción responsable de IA en el sector público y privado.

El Documento CONPES 4144 de 2025 actualiza la política nacional de IA, estableciendo principios de transparencia, seguridad, protección de derechos fundamentales y coordinación institucional para el desarrollo y uso de sistemas de inteligencia artificial en Colombia.

El Proyecto de Ley 042 de 2025 (también referido como Proyecto de Ley 43 de 2025 en algunas fuentes), radicado en el Congreso de la República, busca establecer un marco normativo integral para regular el desarrollo, uso, implementación y supervisión de sistemas de IA en Colombia, con un enfoque basado en la ética, los derechos humanos, la salud mental, el bienestar

emocional, la equidad y la sostenibilidad. Este proyecto de ley propone principios como transparencia, neutralidad tecnológica, seguridad, protección de datos personales, supervisión humana y responsabilidad por decisiones automatizadas, y establece obligaciones específicas para los desarrolladores, proveedores y usuarios de sistemas de IA.

La Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio orienta sobre la aplicación de la normativa de protección de datos en el contexto de tecnologías emergentes, incluyendo la IA generativa, y establece lineamientos para el tratamiento de datos personales mediante herramientas de IA.

Ley 2502 de 2025 (Julio 28) Por medio de la cual se modifica y establece un agravante al artículo 296 de la Ley 599 del 2000, Código Penal Colombiano y se dictan otras disposiciones

En el ámbito internacional, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (Reglamento UE 2016/679) establece principios y obligaciones para el tratamiento de datos personales que son aplicables como referente de buenas prácticas en gobernanza de datos y privacidad, incluso para organizaciones colombianas que procesen datos de residentes europeos o que busquen alinearse con estándares internacionales.

La ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su propósito es proporcionar un marco para gestionar los riesgos relacionados con la seguridad de la información que una organización posee o administra.

Aplicación al trabajo: protección de estados financieros, declaraciones tributarias, bases de datos de clientes, información bancaria y papeles de trabajo.

La ISO/IEC 27701:2025 establece requisitos y orientaciones para implementar y mejorar un Sistema de Gestión de Información de Privacidad (PIMS). La norma está dirigida a

organizaciones que realizan tratamiento de información de identificación personal y busca fortalecer la responsabilidad y gestión de los riesgos relacionados con la privacidad.

Aplicación al trabajo: establecer qué datos personales pueden ser utilizados en procesos de IA y bajo qué controles.

La ISO/IEC 42001:2023 establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Inteligencia Artificial (AIMS) dentro de una organización. La norma está orientada a organizaciones que desarrollan o utilizan sistemas basados en IA y proporciona un marco para gestionar los riesgos y oportunidades asociados con su utilización.

Aplicación al trabajo: política de uso de IA, responsabilidades del contador, evaluación de riesgos, supervisión y revisión de los resultados generados por IA.

La ISO/IEC 23894 proporciona orientación para que las organizaciones gestionen los riesgos relacionados con sistemas de inteligencia artificial. ISO la identifica expresamente como una norma destinada a brindar orientación sobre la gestión de riesgos relacionados con IA.

2.3.4 Acuerdos de confidencialidad y tratamiento de información del caso de estudio

En relación con el caso de estudio de la firma Asesorías Contables QUANTIFIKA, se debe tener en cuenta que la información utilizada para el análisis corresponde a datos de dominio público en lo relacionado con la descripción general del caso, pero la información específica de clientes (estados financieros, declaraciones de renta, nómina, contratos, bases de datos, etc.) está protegida por acuerdos de confidencialidad implícitos en la relación profesional entre el contador público y sus clientes, así como por las obligaciones legales de confidencialidad establecidas en el Código de Ética del Contador Público y la Ley 1581 de 2012.

3. Resultados

A continuación, se presentan los resultados obtenidos a partir del análisis de la información recolectada mediante la revisión documental de normativa nacional e internacional, estándares de gobernanza de datos y estudios sobre el uso de inteligencia artificial en procesos contables y tributarios. Los resultados se organizan en cuatro categorías: (I) riesgos identificados en el uso de IA en contabilidad; (II) clasificación de datos según nivel de sensibilidad; (III) medidas de protección y anonimización recomendadas; y (IV) componentes del modelo de gobernanza de datos propuesto.

3.1. Riesgos asociados al uso de herramientas de IA en procesos contables y tributarios

El análisis de la literatura y normativa permitió identificar los principales riesgos que enfrentan las firmas contables y contadores públicos al utilizar herramientas de inteligencia artificial sin políticas de gobernanza de datos. La Tabla 1 presenta la clasificación de riesgos según su naturaleza y frecuencia de aparición en los estudios revisados.

Tabla 2. *Categorización y nivel de criticidad de los riesgos asociados al uso de inteligencia artificial en la gestión contable*

Categoría de riesgo	Riesgo específico	Descripción	Frecuencia en literatura	Nivel de criticidad
Protección de datos	Exposición de información confidencial	Carga de datos sensibles (estados financieros, declaraciones, nómina) en plataformas de IA sin controles.	Muy alta	Crítico
Protección de datos	Vulneración de privacidad	Tratamiento de datos personales sin consentimiento o medidas de seguridad adecuadas.	Alta	Crítico
Protección de datos	Brechas de seguridad	Acceso no autorizado a bases de datos de clientes por vulnerabilidades en herramientas de IA.	Media	Alto

Categoría de riesgo	Riesgo específico	Descripción	Frecuencia en literatura	Nivel de criticidad
Ético-profesional	Falta de transparencia	Decisiones de IA tipo "caja negra" sin explicabilidad ni trazabilidad.	Alta	Alto
Ético-profesional	Ausencia de supervisión humana	Automatización total sin revisión crítica del contador.	Media	Alto
Legal-normativo	Incumplimiento Ley 1581 de 2012	Tratamiento de datos sin políticas ni medidas de seguridad exigidas.	Muy alta	Crítico
Legal-normativo	Responsabilidad por decisiones automatizadas	Dificultad para determinar responsable en caso de errores o fraudes.	Media	Alto
Técnico-operativo	Sesgo algorítmico	Algoritmos que replican sesgos históricos o estructurales en datos.	Media	Medio
Técnico-operativo	Dependencia tecnológica	Excesiva confianza en resultados de IA sin análisis crítico.	Alta	Medio
Técnico-operativo	Errores en interpretación normativa	IA que interpreta incorrectamente normas tributarias complejas.	Media	Alto
Reputacional	Daño a la imagen profesional	Pérdida de confianza de clientes por incidentes de seguridad.	Media	Alto

Nota: Elaboración con base en la revisión de normativa y literatura especializada.

La Tabla 3 ilustra la distribución porcentual de los riesgos identificados según su categoría, evidenciando que los riesgos relacionados con protección de datos y cumplimiento legal representan el 45% del total, seguidos por riesgos ético-profesionales (25%) y técnico-operativos (20%).

Tabla 3. *Distribución porcentual de riesgos derivados del uso de Inteligencia Artificial en contabilidad*

Categoría de riesgo	Porcentaje	Gráfico de barras
Protección de datos y legal	45%	 45%
Ético-profesional	25%	 25%
Técnico-operativo	20%	 20%
Reputacional	10%	 10%

Nota: Evaluación de riesgos por categoría en el uso de herramientas de Inteligencia Artificial (IA) en contabilidad, basados en un análisis cualitativo preliminar

3.2. Clasificación de datos según nivel de sensibilidad

A partir del caso de estudio de la firma QUANTIFIKA y los lineamientos de la Ley 1581 de 2012, se estableció una clasificación de los tipos de información que habitualmente manejan los contadores públicos, categorizándolos según su nivel de sensibilidad y las medidas de protección requeridas.

Tabla 4. *Clasificación según nivel de sensibilidad*

Nivel de sensibilidad	Tipo de dato	Ejemplos en el caso QUANTIFIKA	Medidas de protección mínimas	¿Se puede cargar en IA pública?
Crítico	Datos personales sensibles	Copias de cédulas, RUT, NIT, información biométrica	Cifrado de extremo a extremo, anonimización total, acceso restringido	NO
Crítico	Información financiera confidencial	Estados financieros auditados, declaraciones de renta, declaraciones de IVA	Alta Anonimización, eliminación de identificadores, uso de IA privada o local	NO
Alto	Información tributaria	Respuestas a requerimientos DIAN, actas de fiscalización	Anonimización parcial, eliminación de NIT y nombres	NO (solo con anonimización)
Alto	Información laboral	Nómina, contratos laborales, certificados bancarios	Eliminación de nombres, salarios y números de identificación	NO (solo con anonimización)
Medio	Información comercial	Bases de datos de clientes, información de proveedores	Eliminación de datos de contacto directos, uso de códigos	CONDICIONAL (solo si está anonimizada)
Bajo	Información pública	Normas tributarias, conceptos generales, plantillas de documentos	Ninguna restricción especial	SÍ
Alto	Información tributaria	Respuestas a requerimientos DIAN, actas de fiscalización	Anonimización parcial, eliminación de NIT y nombres	NO (solo con anonimización)

Nota: Elaboración con base en la Ley 1581 de 2012 y el Decreto 1377 de 2013.

3.3. Medidas de protección y anonimización recomendadas

El análisis de estándares internacionales (GDPR, AI Act, NIST AI RMF, ISO 27001) y guías de buenas prácticas permitió identificar un conjunto de medidas técnicas y organizacionales

para proteger la información antes, durante y después del uso de herramientas de IA. La Tabla 3 resume estas medidas según la fase del proceso.

Tabla 5. *Medidas de protección y anonimización para el uso seguro de IA*

Fase del proceso	Medida	Descripción	Herramienta/técnica	Responsable
Antes de cargar datos	Clasificación de datos	Categorizar información según nivel de sensibilidad	Matriz de clasificación	Contador/Líder de proyecto
Antes de cargar datos	Anonimización	Eliminar o transformar identificadores personales	Enmascaramiento, generalización, seudonimización	Analista de datos
Antes de cargar datos	Evaluación de riesgos	Identificar riesgos específicos del uso de IA para cada caso	Checklist de riesgos	Comité de gobernanza
Antes de cargar datos	Selección de herramienta	Elegir IA según nivel de riesgo y tipo de datos	Matriz de decisión	Gerencia/TI
Durante el uso	Supervisión humana	Revisión crítica de todos los resultados generados por IA	Revisión por pares	Contador senior
Antes de cargar datos	Anonimización	Eliminar o transformar identificadores personales	Enmascaramiento, generalización, seudonimización	Analista de datos
Antes de cargar datos	Evaluación de riesgos	Identificar riesgos específicos del uso de IA para cada caso	Checklist de riesgos	Comité de gobernanza
Durante el uso	Trazabilidad	Registrar qué datos se cargaron, en qué herramienta y con qué propósito	Bitácora de uso de IA	Todos los usuarios
Durante el uso	Limitación de acceso	Restringir uso de IA a personal capacitado y autorizado	Control de accesos	TI/Seguridad
Después del uso	Eliminación de datos	Borrar datos cargados en plataformas de IA según políticas del proveedor	Confirmación de borrado	Usuario/TI
Después del uso	Auditoría	Verificar cumplimiento de políticas y detectar incidentes	Auditoría trimestral	Auditor interno
Continuo	Capacitación	Formar al personal en uso seguro de IA y protección de datos	Programa de capacitación	Gerencia/RRHH

Nota: Elaboración con base en NIST AI RMF, ISO 27001 y GDPR.

La Figura 1 presenta el flujo recomendado para el uso seguro de IA en procesos contables, integrando las medidas de protección identificadas.

Figura 1. *Flujo de Uso Seguro de Inteligencia Artificial en Procesos Contables y Tributarios*

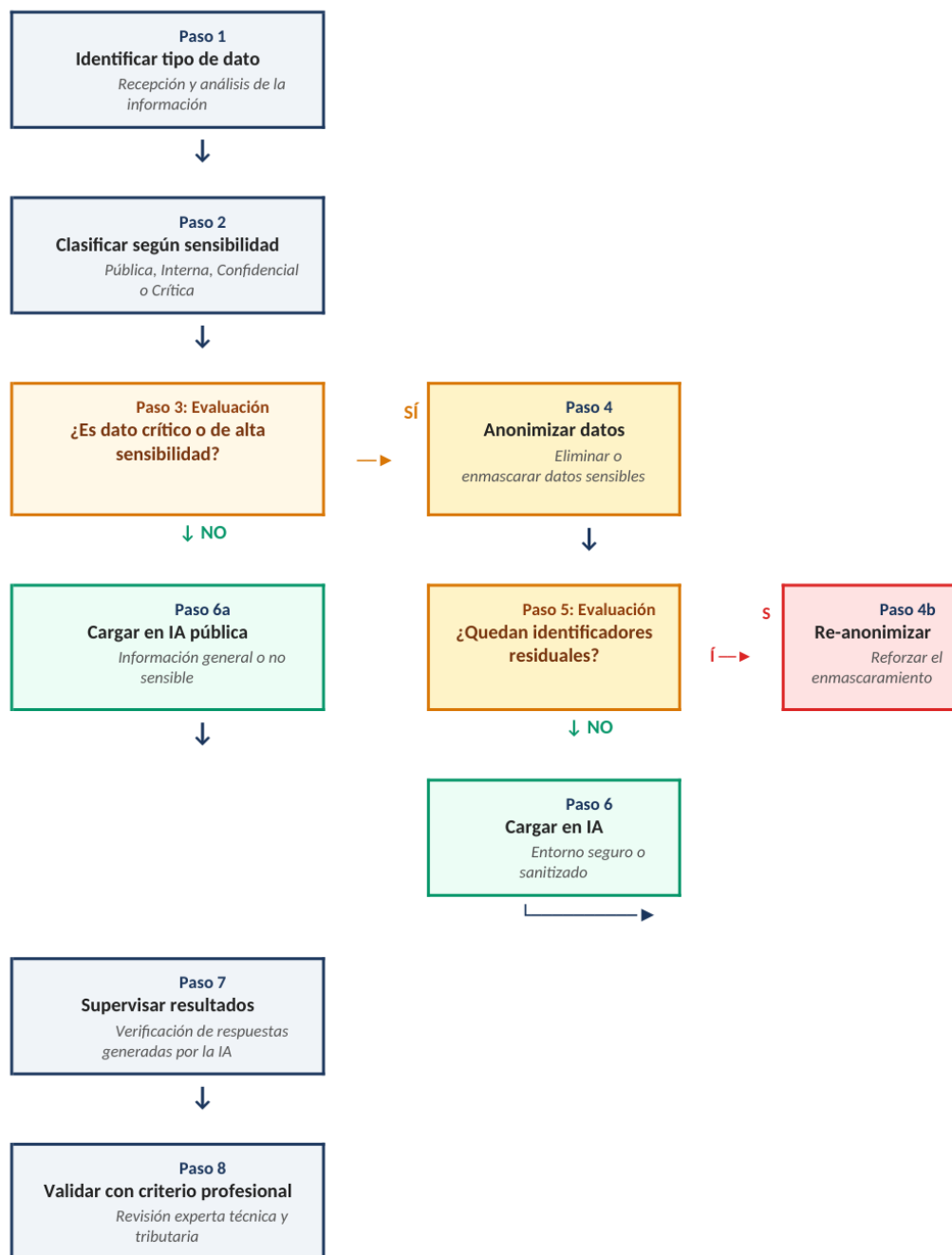
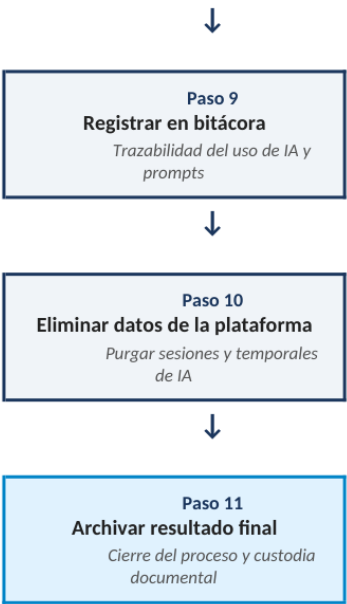


Figura 2. *Flujo de Uso Seguro de Inteligencia Artificial en Procesos Contables y Tributarios*



Nota: Diagrama de flujo metódico para la incorporación segura y responsable de modelos de inteligencia artificial en procesos contables y tributarios. Muestra el protocolo de clasificación, anonimización, validación profesional, trazabilidad en bitácora y purga de información. Adaptado para entregables de transformación digital contable.

3.4 Componentes del modelo de gobernanza de datos propuesto

Como resultado principal de la investigación, se diseñó un modelo de gobernanza de datos para el uso seguro de IA en procesos contables y tributarios, estructurado en cinco componentes interrelacionados. La Tabla 5 detalla cada componente, sus elementos y los entregables esperados.

Tabla 6 *Componentes del modelo de gobernanza de datos para uso seguro de IA*

Componente	Elementos clave	Descripción	Entregable
1. Marco de gobernanza	Políticas, principios, roles y responsabilidades	Establece la estructura organizacional y los principios rectores para el uso de IA	Política de gobernanza de datos; Matriz de roles (RACI)

2. Gestión de datos	Clasificación, inventario, calidad, metadatos	Define cómo se identifican, categorizan y documentan los datos en la organización	Inventario de datos; Matriz de clasificación
3. Seguridad y protección	Controles de acceso, cifrado, anonimización, gestión de incidentes	Implementa medidas técnicas y administrativas para proteger la información	Manual de seguridad; Protocolo de anonimización
4. Cumplimiento normativo	Evaluación de riesgos, auditoría, trazabilidad, documentación	Garantiza el cumplimiento de la Ley 1581 de 2012, Código de Ética y estándares internacionales	Registro de cumplimiento; Bitácora de uso de IA
5. Cultura y capacitación	Formación, comunicación, monitoreo, mejora continua	Fomenta una cultura de uso ético, seguro y responsable de la IA	Programa de capacitación; Guía de buenas prácticas

Nota: Elaboración con base en ISO 38505, NIST AI RMF y marco de gobernanza de datos del IGAC.

La Figura 2 representa gráficamente la estructura del modelo de gobernanza de datos propuesto, mostrando la interrelación entre sus cinco componentes.

Figura 3 Modelo de gobernanza de datos para uso seguro de IA en contabilidad



Nota: Modelo jerárquico de gobernanza de datos diseñado para integrar sistemas de inteligencia artificial en entornos contables. Muestra la secuencia estratégica desde la definición del marco normativo y operativo, pasando por la gestión, seguridad y auditoría, hasta la consolidación de la cultura organizacional y la guía de aplicación práctica.

3.5 Guía de buenas prácticas resultante

Como producto final de la investigación, se consolidó una guía de buenas prácticas que integra los hallazgos de los componentes anteriores. La guía está estructurada en 10 prácticas esenciales que los contadores públicos y firmas contables deben implementar para garantizar el uso seguro de la inteligencia artificial.

Tabla 7 *Guía de buenas prácticas para el uso seguro de IA en contabilidad*

NO.	Práctica	Descripción breve	Prioridad
1	Clasificar datos antes de usar IA	Identificar si la información es crítica, alta, media o baja sensibilidad	Crítica
2	Anonimizar datos sensibles	Eliminar nombres, NIT, números de identificación y datos únicos antes de cargar	Crítica
3	No cargar datos críticos en IA pública	Usar solo IA privada o local para estados financieros, declaraciones y nómina	Crítica
4	Mantener supervisión humana	Revisar críticamente todos los resultados generados por IA	Alta
5	Registrar uso de IA en bitácora	Documentar qué datos se cargaron, en qué herramienta y con qué propósito	Alta
6	Capacitar al personal	Formar continuamente en protección de datos y uso seguro de IA	Alta
7	Evaluar proveedores de IA	Verificar políticas de seguridad, privacidad y tratamiento de datos del proveedor	Media
8	Implementar controles de acceso	Restringir uso de IA a personal autorizado y capacitado	Media
NO.	Práctica	Descripción breve	Prioridad
9	Realizar auditorías periódicas	Verificar cumplimiento de políticas y detectar incidentes	Media
10	Actualizar políticas continuamente	Revisar y ajustar políticas según cambios normativos y tecnológicos	Media

Nota: Elaboración con base en el análisis de riesgos, normativa y estándares internacionales.

Los resultados presentados en esta sección evidencian que el uso de inteligencia artificial en procesos contables y tributarios sin políticas de gobernanza de datos expone a las organizaciones a riesgos críticos de protección de datos, cumplimiento legal y ética profesional. La implementación del modelo propuesto, estructurado en cinco componentes y operacionalizado mediante la guía de 10 buenas prácticas, permite a las firmas contables y contadores públicos en Colombia aprovechar los beneficios de la IA (eficiencia, agilidad, análisis avanzado) mientras minimizan los riesgos y garantizan el cumplimiento de la Ley 1581 de 2012, el Código de Ética del Contador Público y los estándares internacionales aplicables.

4. Conclusiones

La contaduría pública en Colombia está viviendo una transformación trascendental: la inteligencia artificial ya no es el futuro, es el presente en el quehacer de la profesión. Sin embargo, como descubrimos en este trabajo, la velocidad de adopción de estas herramientas ha superado en gran medida la capacidad de las organizaciones para proteger la información que manejamos. Este estudio nació precisamente de esa coyuntura entre la eficiencia que promete la IA y el deber irrenunciable de reserva profesional que nos exige la Ley 43 de 1990 y el Estatuto Tributario y termina con un modelo concreto, aplicable y verificable.

En primer lugar, cumplimos con lo que nos propusimos. Identificamos los riesgos reales a los que nos exponemos a partir del ejercicio profesional, los mismos se materializan cuando se carga o sube documentación completa y privilegiada a un chatbot gratuito; cuando se usan estados financieros sin anonimizar datos sensibles contenidos en ellos para pedirle a la IA un análisis de liquidez, o desconociendo que al cargar los datos del cliente están sirviendo para entrenar un modelo de inteligencia insipiente. Analizamos estándares internacionales ISO 27001, 27701,

42001, las normas del IESBA y los cruzamos con nuestra normativa local: la Ley 1581 de 2012, la Circular SIC 002 de 2024, el CONPES 4144 de 2025 y la reserva tributaria absoluta del artículo 583 del Estatuto Tributario. Además, incorporamos el nuevo marco penal colombiano: la Ley 2502 de 2025, vigente desde julio de ese año, que tipifica con penas de 48 a 96 meses de prisión la violación de datos personales y el fraude de identidad mediante inteligencia artificial, elevando la exposición del contador público desde el ámbito disciplinario al penal. Evaluamos el caso de la firma QUANTIFIKA y exponemos en detalle lo que ocurre cuando la productividad se prioriza sobre la gobernanza: información confidencial expuesta, ausencia de bitácoras, cuentas personales mezcladas con datos corporativos y como resultado, diseñamos un Manual de Gobernanza de Datos estructurado en cinco componentes estratégicos: Estrategia, Arquitectura, Organización, Talento y Modelo Relacional que transforma la teoría académica en procedimientos de trabajo cotidianos.

Respondimos así la pregunta que nos hicimos al inicio: ¿cómo diseñar un modelo de control interno que integre gobernanza de datos en procesos contables y tributarios asistidos por IA? La respuesta es que no basta con una política de papel, se requiere un ambiente de cinco componentes congruentes entre sí; inicialmente una estrategia que defina qué se automatiza y qué no, una arquitectura que decida dónde viven los datos (nube pública, privada o local), una organización que separe quien centraliza las reglas de quien ejecuta, un talento humano que entienda que el contador del siglo XXI propone a partir de análisis de los datos y finalmente, un nuevo modelo relacional que nos vincule con clientes, proveedores y organismos de control desde la confianza demostrable.

El hallazgo más valioso de esta investigación es que el riesgo principal no está en la tecnología, sino en la ausencia de cultura de gobernanza. Advertimos que la mayor filtración no

ocurre por un hackeo sofisticado, sino por la carga inadvertida de un documento a una herramienta de consumo masivo. Descubrimos que la "alucinación" de la IA está latente a suministrar un concepto tributario errado, una tarifa de retención obsoleta y esta situación puede conllevar a consecuencias disciplinarias y fiscales tan graves como una violación de datos. De igual manera pudimos validar que la transparencia con el cliente sobre el uso de la IA no es una debilidad, sino una ventaja competitiva: las firmas que demuestren ser Aliados de datos confiables ganarán posicionamiento con sus clientes y las entidades financieras que ya exigen estos estándares expandiendo internamente las oportunidades en el mercado existente. En este escenario, la Ley 2502 de 2025 no es una amenaza lejana: es un recordatorio de que la gobernanza de datos no constituye una práctica opcional, sino un pilar frente a la gestión de riesgos a prácticas que configuren una responsabilidad penal.

Teniendo una visión panorámica más amplia la primera puerta se abrirá cuando Colombia consolide su ley general de inteligencia artificial, que hoy está en trámite. La ley obligará a actualizar este manual y probablemente a crear registros obligatorios de algoritmos en contaduría. La segunda puerta es la auditoría de la propia IA. No solo proteger los datos que entran, sino también verificar los sesgos y errores de lo que sale. La tercera puerta es medir cuantitativamente el impacto. ¿Cuánto reduce una firma sus incidentes de seguridad tras implementar estos cinco componentes? Esa pregunta solo la responderá el tiempo y nuevas investigaciones. Asimismo, será necesario observar cómo la jurisprudencia colombiana interpreta la aplicación de la Ley 2502 de 2025 al ejercicio profesional contable. La jurisprudencia colombiana es particularmente importante en lo relativo al fraude de identidad mediante IA y la suplantación en procesos tributarios.

En definitiva, esta investigación demuestra que la inteligencia artificial y la ética profesional no son opuestas. La IA puede ser una aliada poderosa para el contador público, pero solo si la adoptamos con reglas claras, si sensibilizamos al equipo para que previamente clasifique la información al usar las herramientas disponibles y si recordamos que, al final del día, el juicio profesional humano y la responsabilidad que conlleva no se puede delegar a un algoritmo. La gobernanza de datos no es un lujo administrativo si tenemos en contexto que la Ley 2502 de 2025 y la normativa de protección de datos define que es un imperativo legal, ético y de supervivencia profesional.

Referencias

- Agencia Española de Supervisión de Inteligencia Artificial. (s. f.). *Guía de datos y gobernanza de datos*. Ministerio de Transformación Digital y de la Función Pública.
<https://aesia.digital.gob.es/storage/media/07-guia-de-datos-y-gobernanza-de-datos.pdf>
- Asociación Interamericana de Contabilidad. (2026). *Inteligencia artificial responsable: Gobernanza de datos, transparencia y confianza pública para la profesión contable*.
<http://contadores-aic.org/wp-content/uploads/2026/06/Inteligencia-artificial-responsable-gobernanza-de-datos-transparencia-y-confianza-publica-para-la-profesion-contable.pdf>
- Centro Interamericano de Administraciones Tributarias. (2026). *Guía para la protección y uso ético de la información en poder de las administraciones tributarias*.
<https://www.ciat.org/nueva-publicacion-guia-para-la-proteccion-y-uso-etico-de-la-informacion-en-poder-de-las-administraciones-tributarias/>

Congreso de la República de Colombia. (1990, 13 de diciembre). *Ley 43 de 1990: Por la cual se reglamenta la profesión de Contador Público y se dictan otras disposiciones*. Diario Oficial No. 39.602.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Congreso de la República de Colombia. (2008, 31 de diciembre). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales*. Diario Oficial No. 47.219.
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=94408&dt=S>

Congreso de la República de Colombia. (2009, 30 de julio). *Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC)*. Diario Oficial No. 47.426.

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.583. <https://sedeelectronica.sic.gov.co/transparencia/normativa/ley-estatutaria-1581-de-2012>

Congreso de la República de Colombia. (2025). *Proyecto de Ley 042 de 2025: Por medio de la cual se establece el marco regulatorio e integral de la Inteligencia Artificial en Colombia*. Cámara de Representantes. <https://www.camara.gov.co/marco-regulatorio-inteligencia-artificial-263/>

Consejo Nacional de Política Económica y Social. (2019, 8 de noviembre). *Documento CONPES 3975: Política Nacional para la Transformación Digital y la Inteligencia Artificial*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social. (2025). *Documento CONPES 4144: Política Nacional de Inteligencia Artificial*. Departamento Nacional de Planeación.

Constitución Política de Colombia. (1991). *Gaceta Constitucional No. 114*. 7 de julio de 1991.

Dirección de Impuestos y Aduanas Nacionales. (2020). *Circular Externa 0026 de 2020: Lineamientos sobre la protección de datos personales y seguridad de la información*. https://normograma.mintic.gov.co/mintic/compilacion/docs/circular_dian_0026_2020.htm

Instituto Geográfico Agustín Codazzi. (s. f.). *Manual para la gobernanza de los datos y la información* (MN-GET-01). [https://www.igac.gov.co/sites/default/files/listadomaestro/MN-GET-01 Manual para la Gobernanza de los Datos y la Información.pdf](https://www.igac.gov.co/sites/default/files/listadomaestro/MN-GET-01_Manual_para_la_Gobernanza_de_los_Datos_y_la_Informacion.pdf)

Instituto Nacional de Contadores Públicos. (2026). *Uso responsable de IA: Ética, regulación y seguridad en la profesión contable*. <https://incp.org.co/wp-content/uploads/2026/03/Uso-responsable-IA-etica-regulacion-y-seguridad-1.pdf>

International Organization for Standardization & International Electrotechnical Commission. (2017). *Information technology — Governance of IT — Governance of data — Part 1: Governance management framework* (ISO/IEC 38505-1:2017). <https://webstore.ansi.org/standards/incits/incitsisoiec385052017r2023>

International Organization for Standardization & International Electrotechnical Commission.

(2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022).
<https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071622>

Ministerio de Comercio, Industria y Turismo. (2013, 27 de junio). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial No. 48.834.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.
<https://doi.org/10.6028/NIST.AI.100-1>

Superintendencia de Industria y Comercio. (2024). *Circular Externa 002 de 2024: Orientaciones sobre el tratamiento de datos personales en el contexto de tecnologías emergentes y la IA generativa*.

Unión Europea. (2016, 27 de abril). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos - GDPR)*. Diario Oficial de la Unión Europea, L 119/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679>

Unión Europea. (2024, 13 de junio). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial - AI Act)*. Diario Oficial de la Unión Europea.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es>

ANEXO A

MANUAL DE GOBERNANZA DE DATOS

MANUAL DE GOBERNANZA DE DATOS

PARA EL USO CORRECTO DE LA INTELIGENCIA

ARTIFICIAL

En el ejercicio de la Contaduría Pública y la Asesoría Tributaria

Marco de referencia: normas internacionales (ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 42001, IFAC–IESBA, NIA/ISA) y normas nacionales de Colombia (Ley 1581 de 2012, Ley 1266 de 2008, Ley 43 de 1990, Estatuto Tributario, Circular Externa 002 de 2024 – SIC, CONPES 4144 de 2025)

Versión 1.0

Bucaramanga, Colombia — agosto de 2026

Control de versiones

Versión	Fecha	Elaboró / Revisó	Descripción del cambio
1.0	Agosto 2026	Área de Diplomado en transformación digital y uso de la Inteligencia Artificial	Emisión inicial del manual

Aviso importante sobre el marco normativo

⚠ A la fecha de emisión de este manual, Colombia no cuenta con una ley general de Inteligencia Artificial vigente. El Proyecto de Ley 043 de 2025 (Senado) – 324 de 2025 (Cámara) se encuentra en trámite legislativo. Este manual se construye sobre la normativa sí vigente hoy (protección de datos, reserva tributaria, ética profesional) y sobre lineamientos, guías y proyectos regulatorios que anticipan el estándar exigible. El Comité de Gobernanza de Datos debe actualizar este documento cuando se sancione la ley de IA o se expidan nuevas circulares de la SIC, la DIAN o la Junta Central de Contadores.

1. Introducción

La incorporación de herramientas de Inteligencia Artificial (IA) generativa y analítica en la práctica contable y tributaria ofrece ganancias reales de eficiencia: análisis de grandes volúmenes de información financiera, redacción de conceptos, conciliaciones, revisión de declaraciones y automatización de procesos de auditoría interna. Sin embargo, el contador público y el asesor tributario manejan de forma cotidiana información altamente sensible —estados financieros, nóminas, cuentas bancarias, declaraciones tributarias, datos de identificación, información societaria confidencial— cuya divulgación indebida genera responsabilidad disciplinaria, civil, fiscal y penal.

Este manual establece los lineamientos de gobernanza de datos que deben seguirse antes, durante y después de utilizar sistemas de IA en el ejercicio profesional, de manera que la adopción tecnológica sea compatible con el secreto profesional, la reserva de la información tributaria, la protección de datos personales y los principios éticos que rigen la profesión contable.

2. Objetivo y alcance

2.1 Objetivo general

Definir las políticas, roles, controles y procedimientos que garanticen un uso responsable, seguro y conforme a la normativa vigente de las herramientas de Inteligencia Artificial por parte de contadores públicos, revisores fiscales, asesores tributarios y su personal de apoyo, particularmente en lo relacionado con la carga, el tratamiento y la conservación de documentos e información de clientes.

2.2 Alcance

Aplica a toda persona natural o jurídica que preste servicios de contaduría pública, revisoría fiscal, auditoría, asesoría tributaria o servicios contables afines, y que utilice cualquier herramienta de IA (asistentes conversacionales, copilotos ofimáticos, motores de OCR/clasificación documental, herramientas de analítica de datos, automatización robótica de procesos - RPA con componentes de IA, entre otras) para el procesamiento de información propia o de terceros.

2.3 Destinatarios

- Socios, contadores públicos y revisores fiscales.
- Asesores y consultores tributarios.
- Personal auxiliar, practicantes y contratistas con acceso a información de clientes.
- Áreas de tecnología, seguridad de la información y cumplimiento.

3. Marco normativo de referencia

El presente manual se fundamenta en un marco normativo de doble nivel: estándares internacionales de gestión de datos, seguridad de la información e IA, y normas nacionales colombianas de protección de datos, reserva tributaria y ética profesional.

3.1 Normas y estándares internacionales

Norma / Estándar	Relevancia para la gobernanza de datos e IA
ISO/IEC 27001	Sistema de gestión de seguridad de la información (SGSI). Base para controles de acceso, cifrado y gestión de incidentes aplicables a los repositorios de información contable que interactúan con IA.
ISO/IEC 27701	Extensión de la ISO 27001 para gestión de la privacidad (PIMS). Orienta el tratamiento de datos personales de clientes, empleados y terceros en procesos automatizados.
ISO/IEC 42001	Primer estándar internacional de sistema de gestión de IA (AIMS). Marco de referencia para gobernanza, evaluación de riesgos y ciclo de vida de sistemas de IA usados por la firma.
ISO/IEC 23894	Guía de gestión de riesgo específicamente aplicada a sistemas de Inteligencia Artificial.
Código de Ética del IESBA / IFAC	Principios de integridad, objetividad, confidencialidad y competencia profesional del contador; orienta el uso responsable de IA sin delegar el juicio profesional.
Normas Internacionales de Auditoría (NIA/ISA), en especial NIA 230, 315 y 500	Documentación, evaluación de riesgos y evidencia de auditoría; establecen el estándar cuando la IA participa en la generación o análisis de evidencia.
NIIF / IFRS	Marco contable de referencia; la IA usada para clasificación o análisis financiero debe producir resultados trazables y verificables frente a estos estándares.

Norma / Estándar	Relevancia para la gobernanza de datos e IA
Reglamento General de Protección de Datos – RGPD (UE)	Referente comparado de buenas prácticas (minimización, privacidad desde el diseño, evaluaciones de impacto) útil como benchmarking, aunque no vincula directamente en Colombia.
Principios de IA de la OCDE	Principios de transparencia, robustez, rendición de cuentas y centralidad en el ser humano, adoptados como referencia por la política pública colombiana.

3.2 Normas nacionales (Colombia)

Norma	Contenido relevante
Constitución Política, art. 15	Derecho fundamental al habeas data y a la intimidad; base constitucional de toda restricción al tratamiento de datos con IA.
Ley 1581 de 2012 y Decreto 1377 de 2013	Régimen general de protección de datos personales: principios de finalidad, libertad, necesidad, seguridad y confidencialidad; autorización previa del titular.
Ley 1266 de 2008 (Habeas Data financiero)	Tratamiento de datos financieros, crediticios y comerciales; aplicable a información de clientes cargada en herramientas de IA para análisis financiero.
Circular Externa N.º 002 de 2024 – SIC	Lineamientos específicos de la Superintendencia de Industria y Comercio para el tratamiento de datos personales en sistemas de IA: exige que el tratamiento sea idóneo, necesario, razonable y proporcional (juicio de proporcionalidad en sentido estricto).
CONPES 4144 de 2025	Política Nacional de Inteligencia Artificial; fija la hoja de ruta y los principios éticos (transparencia, responsabilidad demostrada, privacidad desde el diseño) que anticipan la futura regulación.

Norma	Contenido relevante
Proyecto de Ley 043/2025 – 324/2025 (en trámite)	Marco regulatorio integral de IA basado en riesgo; aún no vigente, pero orienta las obligaciones de clasificación de riesgo, transparencia y supervisión que este manual anticipa.
Estatuto Tributario, art. 583 y ss.	Reserva de la información tributaria; restringe el uso, la divulgación y el almacenamiento externo de información de declaraciones y procesos ante la DIAN.
Ley 2502 2025	Por medio de la cual se modifica y establece un agravante al artículo 296 de la Ley 599 del 2000, Código Penal Colombiano y se dictan otras disposiciones
Ley 43 de 1990 y Código de Ética del Contador Público (JCC)	Deber de reserva y confidencialidad profesional del contador público; sujeción a la Junta Central de Contadores.
Ley 527 de 1999	Validez de mensajes de datos y firmas electrónicas; relevante para trazabilidad de documentos procesados con IA.
Código Penal, arts. 246, 269A-269J (modificado por Ley 2502 de 2025)	Delitos de violación de datos personales, acceso abusivo a sistemas informáticos y agravante específico por fraude de identidad mediante IA (suplantación).

⚠ Este cuadro normativo debe revisarse mínimo cada seis (6) meses, dado el ritmo de expedición de circulares de la SIC y el avance del trámite legislativo de IA en Colombia.

4. Glosario de términos

Término	Definición
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Término	Definición
Dato sensible	Datos que afectan la intimidad del titular o cuyo uso indebido genera discriminación (salud, datos biométricos, entre otros).
Información tributaria reservada	Datos contenidos en declaraciones, procesos de fiscalización o expedientes ante la DIAN, protegidos por reserva legal.
Anonimización	Proceso irreversible que elimina la posibilidad de identificar al titular de la información.
Seudonimización	Sustitución de datos identificativos por un identificador reversible bajo controles de seguridad.
Prompt	Instrucción o consulta que un usuario ingresa a un sistema de IA generativa, la cual puede contener información cargada por el usuario.
Encargado del tratamiento	Quien realiza el tratamiento de datos personales por cuenta del responsable (por ejemplo, el proveedor de la herramienta de IA).
Responsable del tratamiento	La firma o profesional contable que decide sobre la finalidad y los medios del tratamiento de los datos de sus clientes.
Evaluación de Impacto en la Protección de Datos (EIPD)	Análisis previo de los riesgos que un tratamiento de datos (incluido el uso de IA) representa para los titulares.

5. Principios de gobernanza de datos aplicados a la IA

Todo uso de IA en la firma debe regirse por los siguientes principios, derivados de la Ley 1581 de 2012, la Circular 002 de 2024 de la SIC y los estándares ISO citados:

- **Finalidad:** la información solo se procesa con IA para fines específicos, legítimos e informados al cliente; no se usa para entrenar modelos de terceros sin autorización expresa.
- **Necesidad y minimización de datos:** se carga a la herramienta de IA únicamente la información estrictamente necesaria para la tarea (nunca el expediente completo si basta un extracto).

- **Proporcionalidad:** se pondera el beneficio del uso de IA frente al riesgo de exposición de datos sensibles, conforme al juicio de idoneidad, necesidad, razonabilidad y proporcionalidad exigido por la SIC.
- **Responsabilidad demostrada:** la firma debe poder evidenciar, en cualquier momento, qué herramienta se usó, qué información se cargó, quién lo hizo y bajo qué autorización.
- **Privacidad y seguridad desde el diseño:** la configuración de cada herramienta de IA se revisa antes de habilitarla (retención de datos, uso para entrenamiento, ubicación de servidores, cifrado).
- **Transparencia frente al cliente:** se informa cuándo un producto o análisis fue generado o asistido por IA y se mantiene la revisión y el juicio profesional humano sobre el resultado.
- **Confidencialidad y secreto profesional:** prevalece sobre cualquier ganancia de productividad; ante la duda razonable sobre el destino de la información, no se carga el documento.

6. Clasificación de la información contable y tributaria

Toda la información que maneja la firma debe clasificarse antes de decidir si puede o no ser cargada a una herramienta de IA. Se establecen cuatro niveles:

Nivel	Ejemplos	Tratamiento con IA permitido	Condición
1 — Pública	Normativa, formatos en blanco, contenido educativo, plantillas sin datos de cliente	Libre	Ninguna restricción adicional
2 — Interna	Procedimientos internos, políticas de la firma, papeles de trabajo genéricos sin datos identificables	Permitido con herramientas aprobadas	Uso de cuentas corporativas, no personales
3 — Confidencial	Estados financieros, nómina, contratos, cifras de clientes identificables, declaraciones tributarias	Solo anonimizado/seudonimizado o en herramientas con Acuerdo de Tratamiento de Datos (ATD) vigente	Autorización del cliente + registro en bitácora

Nivel	Ejemplos	Tratamiento con IA permitido	Condición
4 — Restringida / Reserva legal	Expedientes DIAN, información de procesos de fiscalización, datos sensibles, información penal-tributaria, secretos industriales	Prohibido cargar a IA de uso general	Solo en entornos privados certificados, con autorización expresa y escrita del cliente y del Comité de Gobernanza

⚠ Ante la duda sobre el nivel de un documento, se clasifica siempre en el nivel más restrictivo hasta que el Oficial de Protección de Datos confirme lo contrario.

7. Ciclo de vida del dato en el uso de IA

7.1 Recolección y verificación de la base de licitud

Antes de cargar cualquier documento del cliente a una herramienta de IA, se verifica: (i) existencia de autorización del titular para el tratamiento (Ley 1581/2012); (ii) que la finalidad declarada al cliente cubra el uso de IA; (iii) que exista, si aplica, un Acuerdo de Tratamiento de Datos o cláusula de confidencialidad con el proveedor de la herramienta.

7.2 Tratamiento (carga, procesamiento, generación de resultados)

Se privilegia el uso de entornos empresariales de IA con controles de nivel corporativo (gestión de acceso, cifrado en tránsito y en reposo, opción de exclusión del entrenamiento de modelos) frente a versiones gratuitas o de consumo masivo, cuyas condiciones de uso suelen permitir el reentrenamiento con los datos ingresados.

7.3 Almacenamiento y retención

Los resultados generados por IA que contengan información de nivel 3 o 4 se almacenan únicamente en los repositorios autorizados de la firma, con los mismos controles de acceso que el expediente original, y se eliminan del historial de conversación o proyecto de la herramienta de IA cuando la tarea concluya, en la medida en que la configuración de la herramienta lo permita.

7.4 Eliminación y disposición final

Se aplican los tiempos de conservación documental exigidos por el Código de Comercio (10 años) y el Estatuto Tributario para soportes contables y tributarios; vencido el plazo, o cuando la finalidad se cumpla, la información se elimina de forma segura, incluidas las copias generadas o cacheadas por herramientas de IA cuando sea técnicamente posible.

8. Roles y responsabilidades

Rol	Responsabilidades principales
Socio director / Contador responsable	Aprobar el manual, asignar recursos, responder ante clientes y organismos de control por el cumplimiento general.
Oficial de Protección de Datos / Cumplimiento	Mantener el inventario de herramientas de IA aprobadas, evaluar nuevas herramientas, gestionar incidentes y atender solicitudes de titulares (habeas data).
Líder de Tecnología / Seguridad de la Información	Configurar controles técnicos, gestionar accesos, cifrado, copias de seguridad y monitoreo del uso de IA.
Contador público / Asesor tributario a cargo del cliente	Clasificar la información antes de cargarla, verificar autorización del titular, revisar y validar profesionalmente todo resultado generado por IA.
Personal auxiliar / practicantes	Usar únicamente las herramientas y cuentas autorizadas; reportar cualquier uso indebido o incidente detectado.
Comité de Gobernanza de Datos e IA	Revisar periódicamente este manual, aprobar excepciones, evaluar nuevas normas y decidir sobre la incorporación de nuevas herramientas.

9. Evaluación de riesgos e impacto en la protección de datos

Antes de habilitar una nueva herramienta de IA para el manejo de información de nivel 3 o 4, se realiza una Evaluación de Impacto en la Protección de Datos (EIPD) que responda, como mínimo, a las siguientes preguntas:

- ¿Dónde se alojan los servidores del proveedor y bajo qué jurisdicción operan los datos (transferencia internacional de datos)?
- ¿La herramienta utiliza los datos ingresados para entrenar o mejorar sus modelos? ¿Existe opción de exclusión (opt-out)?
- ¿Qué certificaciones de seguridad posee el proveedor (ISO/IEC 27001, SOC 2, entre otras)?
- ¿Existen antecedentes de incidentes de seguridad o fuga de información del proveedor?
- ¿Qué controles de retención y eliminación de datos ofrece la herramienta?
- ¿El resultado generado por la IA puede contener errores ("alucinaciones") que requieran validación humana obligatoria antes de su uso?

El resultado de la EIPD determina si la herramienta se incorpora al listado de herramientas aprobadas, se aprueba con restricciones (solo información nivel 1-2), o se rechaza.

10. Medidas de seguridad técnicas y organizativas

10.1 Medidas técnicas

- Uso exclusivo de cuentas corporativas o empresariales con autenticación multifactor para acceder a herramientas de IA.
- Configuración de la opción de no uso de los datos para entrenamiento de modelos, cuando la herramienta lo permita.
- Cifrado de la información en tránsito y en reposo antes de su carga.
- Segmentación de accesos: cada usuario accede solo a la información de los clientes que le fueron asignados.
- Registro (log) de las cargas de información de nivel 3 y 4 a herramientas de IA: fecha, usuario, cliente, herramienta, finalidad.

10.2 Medidas organizativas

- Inventario actualizado de herramientas de IA aprobadas por el Comité de Gobernanza.
- Acuerdos de confidencialidad y de tratamiento de datos con cada proveedor de IA utilizado.
- Capacitación obligatoria y periódica a todo el personal antes de otorgar acceso a herramientas de IA.

- Cláusulas contractuales con clientes que informen el uso de IA como parte de la prestación del servicio.
- Procedimiento formal de gestión de incidentes de seguridad de la información.

11. Procedimiento operativo estándar: carga de documentos a herramientas de IA

Antes de cargar cualquier documento o dato a una herramienta de IA, el profesional debe seguir los siguientes pasos, en orden:

1. Identificar la herramienta: ¿está en el listado de herramientas de IA aprobadas por la firma?
2. Clasificar la información según la matriz de la sección 6 (pública, interna, confidencial, restringida).
3. Verificar la existencia de autorización del titular y, si aplica, de un Acuerdo de Tratamiento de Datos con el proveedor de la IA.
4. Minimizar: eliminar o anonimizar todo dato personal, financiero o tributario que no sea estrictamente necesario para la tarea (nombres, números de identificación, cuentas bancarias, direcciones).
5. Cargar la información únicamente desde la cuenta corporativa autorizada, nunca desde cuentas personales o gratuitas.
6. Registrar la operación en la bitácora de uso de IA cuando se trate de información de nivel 3 o 4.
7. Validar profesionalmente el resultado generado: ningún producto de IA se entrega al cliente ni se usa como soporte de un concepto tributario o contable sin revisión humana experta.
8. Eliminar del proyecto o historial de la herramienta la información sensible una vez cumplida la finalidad, cuando sea técnicamente posible.

12. Consentimiento informado y relación con el cliente

La firma debe informar a sus clientes, mediante cláusula contractual o comunicación escrita, que en la prestación del servicio se podrán utilizar herramientas de IA como apoyo (nunca como reemplazo) del juicio profesional, especificando: qué tipo de tareas se apoyan en IA, qué categorías de datos podrían tratarse, y el derecho del cliente a solicitar que su información no sea procesada por estas herramientas. El Anexo C de este manual contiene el modelo de cláusula sugerido.

13. Capacitación y cultura de gobernanza

-
- Inducción obligatoria sobre este manual para todo nuevo colaborador antes de otorgarle acceso a herramientas de IA.
 - Capacitación anual de actualización normativa (protección de datos, reserva tributaria, novedades de la SIC y del proyecto de ley de IA).

- Simulacros o casos prácticos sobre qué información sí y qué información no se puede cargar a un asistente de IA.
- Canal interno para consultas rápidas al Oficial de Protección de Datos ante casos dudosos.

14. Supervisión, auditoría y gestión de incidentes

14.1 Auditoría interna

El Comité de Gobernanza realiza al menos una revisión semestral de la bitácora de uso de IA, del inventario de herramientas aprobadas y del cumplimiento de este manual, dejando constancia escrita de los hallazgos y planes de acción.

14.2 Gestión de incidentes

Ante la sospecha o confirmación de que información confidencial fue expuesta indebidamente a través de una herramienta de IA (por ejemplo, carga accidental en una cuenta no corporativa, o filtración por parte del proveedor), se debe: (i) notificar de inmediato al Oficial de Protección de Datos; (ii) contener el incidente (revocar accesos, eliminar la información cuando sea posible); (iii) evaluar si corresponde notificar a la Superintendencia de Industria y Comercio y a los titulares afectados conforme a la Ley 1581 de 2012; (iv) documentar el incidente en el registro del Anexo D.

15. Régimen de incumplimiento

El incumplimiento de este manual por parte de cualquier colaborador podrá dar lugar a medidas disciplinarias internas, sin perjuicio de la responsabilidad disciplinaria ante la Junta Central de Contadores, la responsabilidad civil frente al cliente afectado, y la responsabilidad administrativa (sanciones de la SIC) o penal a que haya lugar conforme al Código Penal colombiano.

16. Revisión y actualización del manual

Este manual se revisará como mínimo una vez al año, y de forma extraordinaria cuando: (i) se sancione la ley general de IA en Colombia; (ii) la Superintendencia de Industria y Comercio, la DIAN o la Junta Central de Contadores expidan nueva regulación aplicable; (iii) se identifiquen incidentes que evidencien vacíos en los controles vigentes; (iv) la firma incorpore nuevas herramientas o modelos de IA a su operación.

17. Anexos

Anexo A — Matriz rápida de clasificación de información

Tipo de documento	Nivel	¿Se puede cargar a IA de uso general?
Plantilla o formato en blanco	1 — Pública	Sí
Procedimiento interno sin datos de cliente	2 — Interna	Sí, con cuenta corporativa
Estado financiero con nombre del cliente	3 — Confidencial	Solo anonimizado o con ATD vigente
Declaración de renta / IVA de un cliente	3 — Confidencial	Solo anonimizado o con ATD vigente
Nómina con datos de empleados	3 — Confidencial	Solo anonimizado o con ATD vigente
Expediente de fiscalización DIAN	4 — Restringida	No, salvo entorno certificado y autorización expresa
Datos biométricos o de salud	4 — Restringida	No

Anexo B — Checklist previo a cargar información a una herramienta de IA

- ☐ La herramienta está en el listado de herramientas de IA aprobadas por la firma.
- ☐ Identifiqué el nivel de clasificación de la información (1 a 4).
- ☐ Verifiqué que existe autorización del titular para este tratamiento.

- ☐ Eliminé o anonimicé los datos personales, financieros o tributarios innecesarios.
- ☐ Estoy usando mi cuenta corporativa, no una cuenta personal o gratuita.
- ☐ Registré la operación en la bitácora, si el nivel es 3 o 4.
- ☐ Revisaré y validaré profesionalmente el resultado antes de usarlo o entregarlo.
- ☐ Eliminaré la información sensible del historial de la herramienta cuando finalice la tarea.

Anexo C — Modelo de cláusula de autorización al cliente (sugerido)

"El cliente autoriza a [NOMBRE DE LA FIRMA] a apoyar la prestación del servicio contable y/o tributario contratado en herramientas de Inteligencia Artificial, bajo los controles de seguridad y confidencialidad descritos en su Manual de Gobernanza de Datos, entendiendo que dichas herramientas constituyen un apoyo y no un sustituto del juicio profesional del contador o asesor a cargo, y que el cliente podrá en cualquier momento solicitar que su información no sea procesada mediante estas herramientas, sin que ello afecte la prestación del servicio."

Anexo D — Registro de incidentes (modelo)

Fecha	Descripción del incidente	Información afectada	Acciones tomadas	Responsable

Anexo E — Listado de herramientas de IA aprobadas (modelo a diligenciar)

Herramienta	Proveedor	Nivel de información autorizado	Fecha de última evaluación (EIPD)

Fin del documento.