

**Inteligencia artificial y analítica de datos en la administración tributaria
ecuatoriana: garantías y desafíos jurídicos**

Artificial intelligence and data analytics in Ecuadorian tax administration: legal
safeguards and challenges

Inteligência artificial e análise de dados na administração tributária equatoriana:
garantias e desafios jurídicos

Jonathan Eduardo López Poveda
Universidad Católica Santiago de Guayaquil
Ecuador
info@lopezygomez.com
<https://orcid.org/0009-0009-7058-4279>

Nathalie Fernanda Gómez Suárez
Universidad Católica Santiago de Guayaquil
Ecuador
gerencia@lopezygomez.com
<https://orcid.org/0009-0002-2227-7599>

Forma de citación en APA, séptima edición.

López, J., y Gómez, N. (2026). *Inteligencia artificial y analítica de datos en la administración tributaria
ecuatoriana: garantías y desafíos jurídicos*. Revista Ibero Research, 1(6), 145 – 183.

Fecha de presentación: 03/07/2026

Fecha de aceptación: 12/07/2026

Fecha de publicación: 15/07/2026

Resumen

La transformación digital de la administración tributaria ecuatoriana amplía la capacidad de integrar datos, detectar riesgos y automatizar actuaciones, aunque también incrementa amenazas para la privacidad, la igualdad, la motivación y la defensa, el objetivo consistió en analizar inteligencia artificial, Big Data, decisiones automatizadas, transparencia algorítmica y derechos fundamentales dentro del marco tributario nacional, la metodología aplicó revisión jurídica documental y codificación de veinte fuentes normativas, institucionales y académicas, los resultados identifican cobertura sólida en legalidad y protección de datos, junto con vacíos en auditoría algorítmica, explicación individual, registro público y revisión humana, cuatro tablas y tres gráficos ordenan normas, casos de uso, riesgos y salvaguardias, la conclusión propone una gobernanza basada en riesgo con evaluación de impacto, trazabilidad, control humano significativo, motivación comprensible y recurso efectivo, orientada a compatibilizar eficiencia fiscal, innovación pública y protección del contribuyente.

Palabras clave: Big Data, decisiones automatizadas, explicabilidad, debido proceso, privacidad.

Abstract

The digital transformation of Ecuadorian tax administration expands the capacity to integrate data, detect risks and automate actions, although it also increases threats to privacy, equality, reasoning and defense, the objective was to analyze artificial intelligence, Big Data, automated decisions, algorithmic transparency and fundamental rights within the national tax framework, the methodology applied documentary legal review and coding of twenty regulatory, institutional and academic sources, the results identify strong coverage of legality and data protection, together with gaps in algorithmic auditing, individual explanation, public registration and human review, four tables and three charts organize rules, use cases, risks and safeguards, the conclusion proposes risk based governance with impact assessment, traceability, meaningful human control, understandable reasoning and effective appeal, aimed at reconciling tax efficiency, public innovation and taxpayer protection.

Keywords: Big Data, automated decisions, explainability, due process, privacy.

Resumo

A transformação digital da administração tributária equatoriana amplia a capacidade de integrar dados, detectar riscos e automatizar atuações, embora também aumente ameaças à privacidade, à igualdade, à fundamentação e à defesa, o objetivo consistiu em analisar inteligência artificial, Big Data, decisões automatizadas, transparência algorítmica e direitos fundamentais no marco tributário nacional, a metodologia aplicou revisão jurídica documental e codificação de vinte fontes normativas, institucionais e acadêmicas, os resultados identificam cobertura sólida em legalidade e proteção de dados, junto com lacunas em auditoria algorítmica, explicação individual, registro público e revisão humana, quatro tabelas e três gráficos organizam normas, casos de uso, riscos e salvaguardas, a conclusão propõe uma governança baseada em risco com avaliação de impacto, rastreabilidade, controle humano significativo, fundamentação compreensível e recurso efetivo, orientada a compatibilizar eficiência fiscal, inovação pública e proteção do contribuinte.

Palavras-chave: Big Data, decisões automatizadas, explicabilidade, devido processo, privacidade.

Introducción

La administración tributaria contemporánea depende de información masiva, interoperabilidad institucional y procesamiento automatizado, debido a que la factura electrónica, las declaraciones en línea, los anexos transaccionales y los registros públicos producen volúmenes que superan la revisión exclusivamente manual, este contexto convierte a la analítica de datos en infraestructura de control y transforma la relación entre eficiencia recaudatoria, potestad administrativa y garantías del contribuyente.

La inteligencia artificial añade modelos capaces de clasificar, predecir, recomendar o generar contenidos, mientras el Big Data integra variedad, velocidad y volumen de fuentes heterogéneas, la combinación permite identificar anomalías, segmentar riesgos y priorizar auditorías, aunque la misma capacidad puede convertir correlaciones estadísticas en sospechas administrativas sin explicación suficiente, especialmente cuando el resultado afecta devoluciones, determinaciones, sanciones o acceso a procedimientos simplificados.

El problema jurídico no surge por la sola utilización de tecnología, aparece cuando una inferencia automatizada influye de forma relevante sobre derechos y obligaciones sin base legal clara, información comprensible, control humano efectivo o posibilidad real de contradicción, la opacidad puede trasladar el fundamento del acto desde la norma y los hechos hacia un modelo inaccesible, situación incompatible con motivación, seguridad jurídica y tutela administrativa efectiva.

La Constitución ecuatoriana reconoce la protección de datos personales, la igualdad, la intimidad, el debido proceso, la defensa, la motivación y la seguridad jurídica, además ordena que la administración pública actúe con eficacia, eficiencia, calidad, transparencia y evaluación, el régimen tributario incorpora generalidad, progresividad,

simplicidad, equidad y suficiencia recaudatoria, conjunto que exige innovación útil sin convertir la eficiencia en una excepción tácita a los derechos (Asamblea Nacional del Ecuador, 2008).

El Código Tributario atribuye facultades determinadora, resolutive, sancionadora y recaudadora, pero esas competencias permanecen sometidas a legalidad y procedimiento, un sistema algorítmico puede apoyar la búsqueda de inconsistencias o la organización de expedientes, aunque la decisión jurídica requiere identificar hecho generador, base imponible, sujeto, período, norma y evidencia, elementos que no pueden sustituirse por una puntuación de riesgo presentada como conclusión automática (Congreso Nacional del Ecuador, 2005).

El Código Orgánico Administrativo refuerza juridicidad, proporcionalidad, buena fe, interdicción de arbitrariedad, motivación y responsabilidad, por tanto una actuación digital conserva la naturaleza de ejercicio de potestad pública y debe ser atribuible a una autoridad competente, la automatización no elimina la obligación de explicar premisas, hechos y relación lógica, ni reduce el derecho a conocer el expediente y presentar argumentos antes de una consecuencia desfavorable (Asamblea Nacional del Ecuador, 2017).

La Ley Orgánica de Protección de Datos Personales introduce principios de juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad, calidad, seguridad y responsabilidad proactiva, además reconoce garantías frente a valoraciones automatizadas y elaboración de perfiles, estas reglas resultan directamente relevantes cuando la administración tributaria combina información económica, patrimonial, societaria, laboral, aduanera o financiera para producir clasificaciones que influyen en procedimientos (Asamblea Nacional del Ecuador, 2021).

El reglamento de protección de datos desarrolla gestión de riesgos, seguridad, evaluaciones de impacto, obligaciones del responsable y funciones del delegado, dichas herramientas permiten trasladar principios abstractos a procesos verificables, aunque la aplicación tributaria exige precisar cuándo una analítica interna alcanza suficiente intensidad para afectar significativamente a una persona, cuestión decisiva para activar explicación, intervención humana y revisión del resultado (Presidencia de la República del Ecuador, 2023).

La transparencia algorítmica no equivale a publicar indiscriminadamente código fuente, pesos o reglas de detección, debido a que también deben protegerse datos personales, seguridad informática, secreto tributario y efectividad del control, su contenido adecuado comprende información sobre finalidad, variables relevantes, calidad de datos, lógica general, consecuencias, responsables, mecanismos de supervisión y razones individualizadas que permitan comprender y controvertir una actuación concreta.

La doctrina sobre cajas negras advierte que la opacidad puede concentrar poder y dificultar la rendición de cuentas, mientras el debido proceso tecnológico exige procedimientos capaces de revisar errores producidos por sistemas complejos, estas aportaciones resultan pertinentes para el ámbito fiscal porque una selección automatizada puede iniciar cargas probatorias, costos profesionales y riesgos reputacionales aun cuando no constituya formalmente una determinación definitiva (Citron, 2008; Pasquale, 2015).

Las explicaciones contrafácticas ofrecen una vía para informar qué factores relevantes condujeron a un resultado y qué cambios podrían modificarlo, sin revelar necesariamente toda la arquitectura técnica, sin embargo una explicación tributaria debe agregar fundamento normativo y evidencia concreta, debido a que la posibilidad de cambiar una variable futura no sustituye la obligación de demostrar hechos del período

revisado ni permite transformar probabilidades en incumplimientos probados (Wachter, Mittelstadt y Russell, 2018).

Los estudios sobre sistemas sociotécnicos muestran que la equidad no puede resolverse dentro del modelo sin considerar contexto, instituciones, categorías legales y efectos distributivos, por ello una métrica estadística de paridad no garantiza trato igual en tributación, la selección puede reproducir desigualdades por sector, territorio, tamaño, informalidad o acceso digital, aunque no utilice directamente variables protegidas (Selbst, Boyd, Friedler, Venkatasubramanian y Vertesi, 2019).

La Organización para la Cooperación y el Desarrollo Económicos plantea una administración tributaria integrada a los sistemas naturales de empresas y ciudadanía, con datos oportunos y procesos digitales, esa visión promete cumplimiento menos costoso y controles más precisos, pero requiere gobernanza de datos, confianza y arquitectura institucional, porque la integración permanente amplía el alcance de la observación estatal y reduce la visibilidad de las decisiones intermedias (Organización para la Cooperación y el Desarrollo Económicos, 2020).

Los principios internacionales de inteligencia artificial destacan transparencia, explicabilidad, robustez, seguridad, responsabilidad y respeto de derechos humanos, mientras la Recomendación de la UNESCO añade proporcionalidad, supervisión humana, evaluación de impacto y reparación, estos estándares no sustituyen el derecho ecuatoriano, aunque ofrecen criterios interpretativos y modelos de gobernanza útiles para diseñar salvaguardias en sistemas de alto impacto (Organización para la Cooperación y el Desarrollo Económicos, 2024b; UNESCO, 2021).

El Reglamento europeo de inteligencia artificial adopta una clasificación por riesgos y exige gestión, calidad de datos, documentación, registro, transparencia, supervisión humana, exactitud y ciberseguridad para sistemas de alto riesgo, la comparación resulta

relevante como referencia funcional, aunque una trasposición mecánica sería inadecuada, debido a diferencias constitucionales, institucionales y tributarias entre la Unión Europea y Ecuador (Parlamento Europeo y Consejo, 2024).

El objetivo general consiste en analizar los desafíos jurídicos de la inteligencia artificial y la analítica de datos en la administración tributaria ecuatoriana, los objetivos específicos comprenden delimitar casos de uso, identificar garantías aplicables, evaluar riesgos de decisiones automatizadas, determinar exigencias de transparencia y proponer un modelo de gobernanza que proteja derechos fundamentales sin impedir innovación ni control fiscal legítimo.

La hipótesis sostiene que el ordenamiento ecuatoriano contiene bases suficientes para exigir legalidad, finalidad, minimización, motivación, explicación y revisión humana, aunque la dispersión normativa y la ausencia de una política pública específica sobre algoritmos tributarios generan una brecha operativa, dicha brecha puede reducirse mediante evaluación de impacto, registro de sistemas, trazabilidad, auditoría independiente y estándares de control humano proporcional al riesgo.

La relevancia práctica se concentra en evitar dos extremos igualmente problemáticos, una prohibición general de herramientas analíticas que debilite la administración y una adopción opaca que convierta perfiles en decisiones, el equilibrio requiere diferenciar asistencia, recomendación, priorización y decisión, porque cada nivel produce efectos distintos y demanda salvaguardias graduadas, desde información básica hasta intervención humana obligatoria y recurso suspensivo.

Metodología

El enfoque adoptado fue mixto con predominio cualitativo, debido a que el núcleo del estudio correspondió a interpretación constitucional, administrativa, tributaria y de protección de datos, la dimensión cuantitativa se limitó a codificación descriptiva de garantías y riesgos, sin pretensión de medir sistemas internos del Servicio de Rentas Internas ni afirmar la existencia de herramientas no documentadas públicamente.

El tipo de investigación fue exploratorio, descriptivo y propositivo, la fase exploratoria identificó categorías jurídicas emergentes, la fase descriptiva ordenó normas, usos y derechos, la fase propositiva construyó un modelo de gobernanza aplicable a proyectos de inteligencia artificial tributaria, el diseño fue documental, no experimental, transversal y comparado, con revisión cerrada al treinta de junio de dos mil veintiséis.

La población documental comprendió normas ecuatorianas, instrumentos internacionales, documentos institucionales y literatura académica sobre decisiones automatizadas, explicabilidad, administración digital y derechos, la muestra intencional reunió veinte fuentes principales seleccionadas por autoridad, pertinencia y capacidad de cubrir legalidad, protección de datos, transparencia, motivación, revisión humana, auditoría, seguridad y reparación.

Los criterios de inclusión exigieron vigencia o valor doctrinal reconocido, relación directa con tratamiento de datos o potestad pública, disponibilidad verificable y contenido susceptible de codificación, los criterios de exclusión eliminaron materiales comerciales, noticias sin respaldo primario, descripciones técnicas sin conexión jurídica y afirmaciones sobre sistemas tributarios ecuatorianos que no pudieran distinguirse como hechos públicos o escenarios hipotéticos.

La técnica principal fue análisis jurídico de contenido, apoyada por una matriz de ocho dimensiones, cada fuente recibió puntuación cero cuando no contenía la garantía, uno

cuando la referencia era indirecta o parcial y dos cuando existía formulación expresa con elementos operativos, el resultado se normalizó sobre cien para facilitar comparación visual, sin convertir la escala en medición de eficacia institucional real.

El índice de riesgo de casos de uso combinó efecto jurídico, grado de automatización, sensibilidad de datos, escala, opacidad y reversibilidad, cada factor recibió valores entre cero y cuatro, los pesos fueron veinticinco, veinte, quince, quince, quince y diez por ciento respectivamente, la puntuación final se transformó a una escala de cero a cien y se clasificó como baja, media, alta o crítica.

La distinción entre apoyo y decisión constituyó una regla metodológica central, un modelo de apoyo produce indicios sujetos a verificación, una recomendación ordena alternativas para una autoridad, una decisión semiautomatizada incorpora revisión humana con capacidad real de cambio y una decisión automatizada determina efectos sin intervención significativa, esta taxonomía permitió asignar salvaguardias proporcionales y evitar que toda herramienta informática reciba el mismo tratamiento.

El procesamiento se efectuó mediante hojas de cálculo y Python para operaciones descriptivas y elaboración de gráficos, no se aplicaron pruebas inferenciales porque la muestra fue normativa y no probabilística, la confiabilidad se fortaleció mediante doble lectura, registro de justificaciones y revisión de coherencia entre puntuación, evidencia y categoría, las discrepancias se resolvieron priorizando el texto vinculante sobre recomendaciones generales.

Las consideraciones éticas no involucraron datos personales, entrevistas, expedientes tributarios ni experimentación humana, todas las fuentes utilizadas pertenecen al dominio público o a literatura académica citada, la metodología evitó revelar técnicas de detección de fraude o vulnerabilidades operativas, además separó recomendaciones de

gobernanza respecto de afirmaciones sobre capacidades tecnológicas concretas del Servicio de Rentas Internas.

Las limitaciones metodológicas incluyen ausencia de acceso a modelos, datos de entrenamiento, contratos tecnológicos, evaluaciones de impacto y estadísticas internas, por tanto los resultados describen suficiencia normativa y riesgos previsibles, no desempeño real de algoritmos existentes, la codificación contiene juicio jurídico controlado y debe entenderse como herramienta analítica reproducible, no como auditoría oficial ni certificación de cumplimiento.

Resultados

El primer resultado identifica una cadena de valor compuesta por captura, integración, depuración, perfilamiento, priorización, actuación y revisión, cada etapa puede afectar derechos de manera distinta, los errores de origen se amplifican cuando varias bases se cruzan, mientras las inferencias se vuelven difíciles de detectar cuando el contribuyente solo conoce el acto final y no la ruta de datos que produjo la selección.

La analítica descriptiva resume comportamiento histórico y puede apoyar gestión sin producir decisiones individuales, la analítica predictiva estima probabilidad de incumplimiento o inconsistencia, la analítica prescriptiva recomienda una actuación y la inteligencia artificial generativa produce textos o respuestas, el riesgo aumenta cuando la salida abandona funciones auxiliares y se incorpora directamente a requerimientos, determinaciones o sanciones.

La asistencia informativa mediante buscadores o chatbots presenta riesgo bajo cuando ofrece orientación general, identifica su naturaleza no vinculante y permite acceso a una persona, el riesgo crece si la respuesta interpreta situaciones particulares, omite excepciones o induce una declaración, debido a que la confianza legítima y el deber de asistencia pueden verse afectados aunque no exista una resolución administrativa formal.

La detección de anomalías utiliza reglas o modelos para localizar diferencias entre declaraciones, facturas, pagos y registros, su utilidad depende de calidad, actualidad y compatibilidad semántica, una discrepancia puede provenir de períodos distintos, notas de crédito, errores de terceros o tratamientos legales legítimos, por tanto una alerta representa un punto de investigación y no una presunción de infracción.

El perfilamiento de riesgo clasifica personas o empresas mediante variables directas y derivadas, esta práctica puede mejorar asignación de recursos, aunque también genera

efectos acumulativos, mayor frecuencia de control produce más hallazgos y esos hallazgos alimentan perfiles futuros, el ciclo puede concentrar fiscalización sobre sectores visibles mientras actividades menos digitalizadas permanecen fuera del radar, fenómeno conocido como retroalimentación selectiva.

La selección de auditorías constituye una decisión procedimental con efectos significativos, incluso cuando no determina deuda, porque impone deberes de información, costos de defensa y exposición a medidas, la justificación no exige revelar umbrales que faciliten evasión, pero sí debe mostrar competencia, finalidad, hechos o inconsistencias relevantes y ausencia de discriminación, además de permitir revisión humana antes de iniciar actuaciones intensivas.

La automatización de devoluciones puede acelerar pagos legítimos, aunque los rechazos o suspensiones requieren cautela porque afectan liquidez y propiedad, un modelo puede priorizar expedientes de bajo riesgo para aprobación automática, mientras los casos adversos deben recibir revisión humana, información sobre factores determinantes y oportunidad de corregir datos antes de una negativa definitiva.

La determinación de obligación y la imposición de sanciones representan usos críticos, debido a que producen efectos jurídicos directos y demandan valoración normativa, prueba y proporcionalidad, la automatización puede calcular montos una vez fijados hechos y reglas, pero no debe sustituir el razonamiento sobre controversias, simulación, culpabilidad, fuerza mayor o interpretación razonable, materias que requieren autoridad identificable y motivación individual.

La Tabla 1 introduce el corpus jurídico e institucional utilizado para delimitar la gobernanza, el cuadro separa instrumentos nacionales vinculantes, orientaciones de política pública y referencias internacionales, la lectura conjunta permite observar que las garantías relevantes no se encuentran en una sola norma, sino en la interacción entre

Constitución, derecho tributario, procedimiento administrativo, protección de datos y transparencia.

Tabla 1. Matriz de fuentes y aportes para la gobernanza algorítmica tributaria

Fuente	Naturaleza	Aporte principal	Vacío o límite identificado
Constitución del Ecuador	Norma suprema	Datos personales, igualdad, debido proceso, motivación, seguridad jurídica y principios tributarios	No desarrolla obligaciones técnicas ni categorías de automatización
Código Tributario	Ley sectorial	Competencia, determinación, prueba, reserva tributaria y derechos procedimentales	No regula perfiles, modelos predictivos ni explicaciones algorítmicas
Código Orgánico Administrativo	Ley general	Juridicidad, motivación, proporcionalidad, expediente, responsabilidad y recursos	La actuación automatizada carece de desarrollo especializado
Ley de Protección de Datos Personales	Ley orgánica	Finalidad, minimización, calidad, seguridad, perfilamiento y decisiones automatizadas	La coordinación con secreto tributario y potestades fiscales requiere precisión
Reglamento de protección de datos	Reglamento	Gestión de riesgos, evaluación de impacto, seguridad y responsabilidad proactiva	No contiene metodología sectorial para administración tributaria
Ley de Transparencia	Ley orgánica	Publicidad, acceso a información, rendición de cuentas y datos abiertos	Las excepciones técnicas y tributarias necesitan prueba de daño y proporcionalidad
Plan estratégico del SRI	Instrumento institucional	Digitalización, gestión de información, eficiencia, control y servicio	La transparencia de modelos y evaluaciones no aparece como régimen específico
Principios de IA de la OCDE	Estándar internacional	Transparencia, explicabilidad, robustez, responsabilidad y derechos	Naturaleza no vinculante y formulación general
Recomendación de la UNESCO	Estándar internacional	Proporcionalidad, evaluación ética, supervisión humana y reparación	Requiere traducción a procedimientos nacionales concretos
Reglamento europeo de IA	Referencia comparada	Gestión de riesgo, datos, documentación, registro, supervisión y auditoría	No resulta directamente aplicable en Ecuador
Reglamento europeo de datos	Referencia comparada	Información, acceso, perfilamiento y decisiones automatizadas	Su arquitectura institucional difiere del sistema ecuatoriano
Convenio del Consejo de Europa	Referencia comparada	Derechos humanos, democracia, Estado de derecho y evaluación de impacto	Necesita implementación y adaptación institucional

Nota, Elaboración propia con base en el corpus normativo y comparado, la identificación de vacíos expresa insuficiencia operativa y no ausencia total de protección.

El análisis de la Tabla 1 confirma una arquitectura normativa distribuida, la Constitución y las leyes ofrecen bases suficientes para controlar legalidad, datos, procedimiento y transparencia, aunque ninguna disposición reúne inventario de

sistemas, clasificación de riesgo, documentación técnica, auditoría y supervisión humana, la principal necesidad no consiste en crear derechos desde cero, sino en articular obligaciones y responsables durante todo el ciclo de vida.

Cobertura de garantías en el marco ecuatoriano

La legalidad alcanza cobertura elevada porque toda potestad tributaria requiere competencia, norma habilitante y finalidad pública, un modelo no puede ampliar hechos generadores, modificar cargas probatorias ni crear presunciones fuera de la ley, la contratación de tecnología tampoco transfiere potestad al proveedor, debido a que diseño, validación y uso permanecen bajo responsabilidad administrativa y control jurisdiccional.

La finalidad exige definir con precisión el objetivo del tratamiento y evitar reutilizaciones incompatibles, datos recabados para facturación, registro societario o seguridad social pueden ser relevantes para control fiscal, aunque el cruce debe responder a base jurídica, necesidad y proporcionalidad, una base disponible no se convierte automáticamente en dato pertinente, especialmente cuando contiene información sensible o de terceros.

La minimización limita variables y períodos a lo necesario para cada propósito, su aplicación resulta compleja en Big Data porque el valor predictivo suele buscarse mediante agregación amplia, sin embargo la eficiencia analítica no justifica acumulación indefinida, deben establecerse reglas de retención, seudonimización, acceso por roles y eliminación, junto con pruebas que demuestren utilidad real de cada atributo incluido.

La calidad de datos adquiere naturaleza de garantía procesal, un registro desactualizado, duplicado o atribuido a persona equivocada puede modificar una puntuación y desencadenar control, la administración debe documentar procedencia, fecha,

transformaciones y nivel de confianza, además de habilitar corrección antes de una decisión adversa, porque la exactitud no puede presumirse por el solo origen público de la fuente.

La transparencia general comprende publicar políticas, finalidades, categorías de datos, tipos de modelos, responsables, niveles de riesgo y mecanismos de reclamo, la transparencia individual exige explicar factores relevantes en el caso, ambas dimensiones pueden coexistir con reserva tributaria y seguridad, mediante descripciones graduadas, acceso controlado y motivaciones que revelen razones sin exponer reglas capaces de ser manipuladas.

La motivación requiere relación entre norma, hechos y conclusión, una alerta algorítmica solo aporta evidencia auxiliar y debe transformarse en razones verificables, expresiones como riesgo alto o patrón atípico carecen de suficiencia si no indican datos, comparación, período y efecto, la explicación técnica puede acompañar, pero no reemplazar la argumentación jurídica exigida para afectar derechos.

La revisión humana debe ser significativa, no basta una firma automática o aprobación rutinaria, la persona revisora necesita competencia, tiempo, información, capacidad para apartarse del resultado y responsabilidad sobre la decisión, además debe conocer limitaciones y tasas de error, el control humano meramente ceremonial reproduce la automatización y genera una apariencia de garantía sin posibilidad real de corrección.

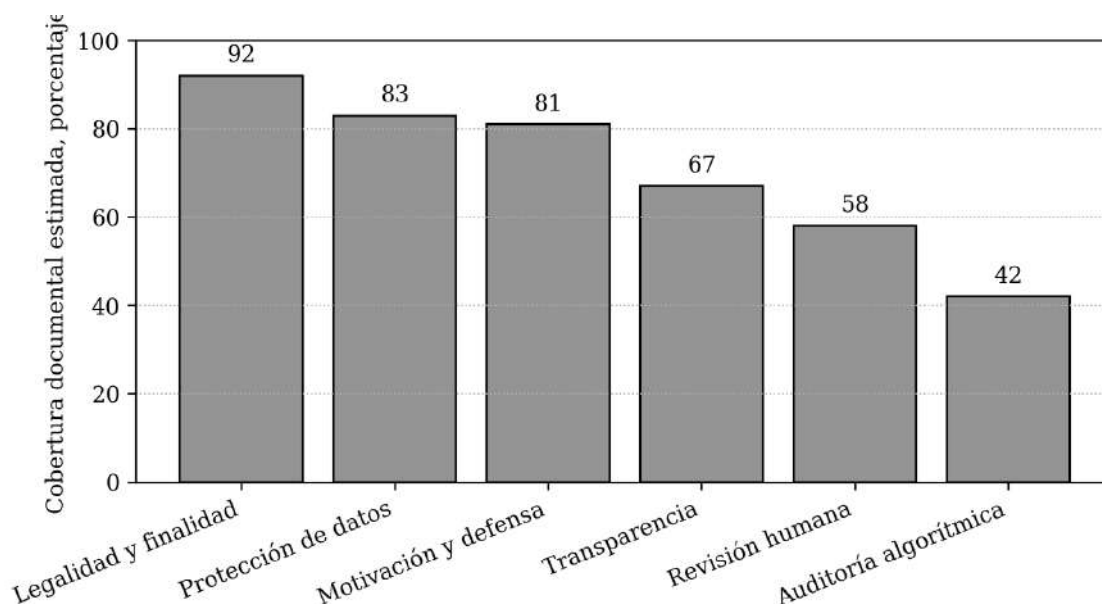
La auditabilidad comprende registros de versiones, datos, parámetros, accesos, salidas y cambios, junto con pruebas de rendimiento, sesgo y seguridad, esta dimensión recibe menor cobertura explícita en normas generales, aunque puede derivarse de responsabilidad, motivación, expediente y seguridad, la ausencia de trazabilidad impide reconstruir por qué una persona recibió una clasificación y debilita defensa, supervisión y aprendizaje institucional.

La ciberseguridad protege confidencialidad, integridad y disponibilidad, pero también exactitud decisional, un ataque, error de integración o acceso indebido puede alterar perfiles y actuaciones, por ello los controles deben incluir autenticación, cifrado, segregación, pruebas, respuesta a incidentes y continuidad, la seguridad no debe utilizarse como argumento absoluto para negar transparencia, debido a que ambas obligaciones requieren ponderación y diseño coordinado.

La reparación efectiva exige canales para corregir datos, impugnar resultados, suspender efectos y obtener revisión, un sistema responsable debe conservar información suficiente para explicar el caso y ofrecer una respuesta dentro de plazos, la carga de descubrir el error no puede recaer íntegramente en el contribuyente, especialmente cuando la administración posee fuentes, transformaciones y reglas inaccesibles desde el exterior.

El Gráfico 1 presenta la cobertura estimada de seis salvaguardias dentro de los instrumentos nacionales codificados, la introducción visual permite comparar garantías jurídicas consolidadas con obligaciones técnicas menos desarrolladas, los porcentajes expresan presencia y nivel operativo en el corpus, no cumplimiento institucional, desempeño de sistemas ni valoración sobre casos concretos.

Gráfico 1. Cobertura documental de salvaguardias en el marco ecuatoriano



Nota, Elaboración propia mediante codificación de Constitución, Código Tributario, Código Orgánico Administrativo, Ley de Protección de Datos, reglamento, Ley de Transparencia y plan estratégico institucional.

El análisis del Gráfico 1 muestra fortaleza en legalidad, finalidad y protección de datos, mientras revisión humana y auditoría algorítmica permanecen menos desarrolladas, esta asimetría explica por qué una administración puede disponer de autorización general para tratar información y aun carecer de protocolos suficientes para justificar modelos complejos, la prioridad regulatoria debe concentrarse en convertir principios existentes en evidencia técnica y procedimental verificable.

Riesgos jurídicos según el caso de uso

El segundo bloque de resultados demuestra que el riesgo depende menos del nombre inteligencia artificial que de la función cumplida, un modelo sencillo que deniega automáticamente una devolución puede ser más riesgoso que una red neuronal utilizada para ordenar expedientes sin efecto directo, la clasificación debe considerar consecuencias, posibilidad de error, datos utilizados, escala y capacidad de revisión, no complejidad tecnológica aislada.

La asistencia informativa obtiene riesgo bajo porque la salida puede presentarse como orientación, siempre que exista aviso claro, actualización normativa y acceso alternativo, sin embargo la generación automática de respuestas particulares puede producir errores convincentes, por tanto deben excluirse decisiones vinculantes, conservar fuentes y permitir que la ciudadanía verifique la norma, especialmente cuando una recomendación influye en plazos o declaraciones.

La detección de anomalías recibe riesgo medio porque identifica eventos para revisión posterior, sus controles mínimos incluyen validación de datos, umbrales documentados, pruebas de falsos positivos y prohibición de considerar la alerta como incumplimiento, la administración debe medir si el modelo mejora selección frente a métodos previos y si concentra errores en sectores con menor capacidad de registro o digitalización.

El perfilamiento de riesgo obtiene nivel alto por combinar múltiples fuentes y producir efectos acumulativos, aunque la puntuación no se comunique, puede determinar frecuencia, intensidad y duración del control, esta influencia exige información general sobre categorías de variables, revisión periódica, exclusión de atributos discriminatorios, mecanismos de corrección y límites temporales, además de evaluación sobre variables proxy que reproduzcan condiciones protegidas.

La selección de auditorías alcanza riesgo alto porque inicia una actuación formal y distribuye carga estatal de manera desigual, una selección puede apoyarse en modelo, pero la orden debe contener razones suficientes y revisión por autoridad, los criterios no necesitan revelar detalles explotables, aunque sí demostrar conexión entre datos relevantes y finalidad fiscal, evitando listas negras permanentes o selección basada únicamente en pertenencia sectorial.

Los requerimientos automatizados presentan riesgo alto cuando se generan sin verificar pertinencia, un sistema puede solicitar información repetida, imposible o ajena al

período, aumentando costos y vulnerando minimización, el control adecuado incluye plantillas adaptativas, validación humana, historial de solicitudes y explicación de relevancia, además de impedir que la falta de respuesta a un requerimiento defectuoso produzca sanción automática.

Las devoluciones reciben riesgo crítico cuando una puntuación suspende o rechaza el pago, debido a que el efecto patrimonial puede ser inmediato y la persona desconoce la causa, el modelo puede automatizar aprobaciones favorables de bajo riesgo, pero los resultados adversos necesitan revisión humana, motivación, acceso a datos relevantes y plazo breve para subsanar, principio conocido como automatización asimétrica favorable a derechos.

La determinación tributaria obtiene riesgo crítico porque transforma información y reglas en deuda exigible, los cálculos mecánicos pueden automatizarse cuando hechos no están controvertidos, mientras la subsunción jurídica, valoración probatoria y selección de norma requieren responsabilidad humana, cualquier sistema utilizado debe conservar versión normativa, parámetros, datos de entrada y justificación, permitiendo reconstrucción completa durante reclamo y control judicial.

La imposición de sanciones representa el máximo riesgo por incorporar culpabilidad, proporcionalidad y circunstancias eximentes, una decisión exclusivamente automatizada sería incompatible con evaluación individual y defensa, el sistema puede detectar incumplimientos formales o calcular rangos, pero la autoridad debe verificar tipicidad, imputación, prueba, reincidencia y razones de graduación, además de separar el modelo de riesgo respecto del juicio sancionador.

La interoperabilidad aumenta todos los niveles porque vincula errores y amplía finalidades, un dato correcto en su fuente puede adquirir significado equivocado al combinarse con otro registro, la evaluación debe revisar identificadores, equivalencias,

fechas y reglas de actualización, también debe limitar inferencias sobre familiares, socios o grupos económicos cuando no exista base jurídica y conexión suficiente con la obligación investigada.

La Tabla 2 introduce la matriz de casos de uso y condiciones mínimas, su finalidad consiste en diferenciar niveles de impacto y evitar una política uniforme, la categoría crítica no implica prohibición absoluta, pero exige habilitación clara, evaluación de impacto, validación independiente, revisión humana obligatoria y recurso efectivo antes de consolidar una consecuencia desfavorable.

Tabla 2. Casos de uso, riesgos y salvaguardias mínimas

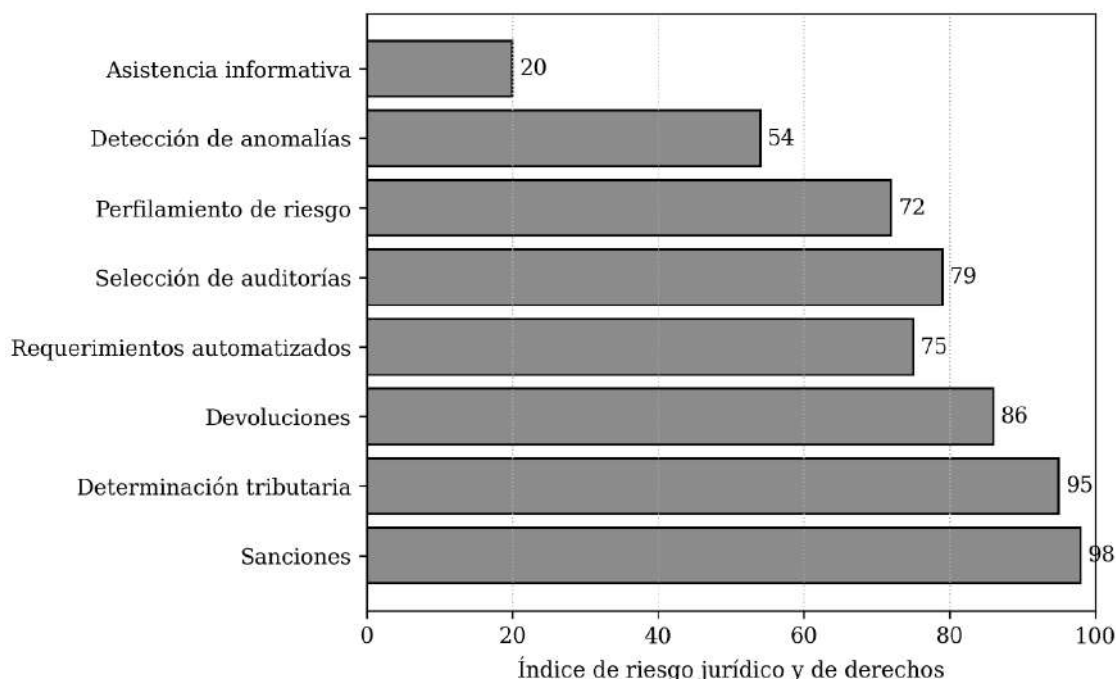
Caso de uso	Efecto principal	Nivel	Derechos comprometidos	Condiciones mínimas
Asistencia informativa	Orientación general o respuesta frecuente	Bajo	Información, confianza legítima y accesibilidad	Aviso no vinculante, fuentes actualizadas, canal humano y monitoreo de errores
Detección de anomalías	Generación de alertas para análisis	Medio	Calidad de datos, igualdad y privacidad	Validación, medición de falsos positivos y prohibición de inferir incumplimiento
Perfilamiento de riesgo	Clasificación y priorización permanente	Alto	Igualdad, protección de datos y no discriminación	Evaluación de impacto, límites de variables, revisión y corrección de perfil
Selección de auditorías	Inicio o intensidad del control	Alto	Motivación, defensa y proporcionalidad	Revisión humana, razones verificables y prohibición de selección por proxy discriminatorio
Requerimientos automatizados	Solicitud de documentos o información	Alto	Minimización, defensa y costos de cumplimiento	Pertinencia individual, control de duplicidad y validación previa
Devoluciones	Aprobación, suspensión o rechazo	Crítico	Propiedad, motivación y recurso	Automatización favorable, revisión humana adversa y subsanación rápida
Determinación tributaria	Fijación de obligación y monto	Crítico	Legalidad, prueba, motivación y tutela	Autoridad responsable, trazabilidad integral y acceso al expediente
Sanciones	Imposición y graduación de pena administrativa	Crítico	Tipicidad, culpabilidad, proporcionalidad y defensa	Prohibición de decisión exclusivamente automatizada y revisión individual

Nota, Elaboración propia, el nivel deriva de efecto jurídico, automatización, sensibilidad, escala, opacidad y reversibilidad.

El análisis de la Tabla 2 demuestra que las salvaguardias deben intensificarse a medida que la salida se acerca al acto administrativo, la separación entre alertar y decidir reduce riesgos si existe una barrera institucional real, la administración necesita documentar quién verifica, qué evidencia adicional se exige y cómo se registra el apartamiento, de otro modo la recomendación algorítmica puede dominar la decisión aunque formalmente exista intervención humana.

El Gráfico 2 representa el índice de riesgo calculado para ocho casos de uso, la introducción permite observar una progresión desde asistencia hasta sanción, los valores no describen sistemas actuales ni probabilidades de daño, expresan una estimación jurídica comparativa construida con seis factores ponderados y sirven para asignar controles proporcionales durante diseño, adquisición y operación.

Gráfico 2. Índice de riesgo jurídico por caso de uso tributario



Nota, Elaboración propia con escala de cero a cien, los usos superiores a ochenta requieren tratamiento crítico y revisión humana obligatoria.

El análisis del Gráfico 2 confirma que devoluciones, determinaciones y sanciones deben permanecer bajo supervisión reforzada, mientras asistencia y detección pueden

experimentar con controles menos intensos, el enfoque basado en riesgo evita exigir el mismo expediente técnico a toda herramienta, aunque mantiene requisitos comunes de inventario, finalidad, seguridad, calidad y responsable identificado, necesarios incluso para sistemas aparentemente simples.

Decisiones automatizadas, explicación y derechos del contribuyente

La decisión automatizada debe definirse por su efecto material y no por la presencia de una firma humana, cuando la autoridad acepta de manera rutinaria una recomendación sin comprenderla ni poder modificarla, la intervención carece de significado, el análisis debe considerar autonomía real, tiempo de revisión, formación, acceso a evidencia y porcentaje de apartamiento, indicadores que permiten detectar supervisión meramente formal.

La protección de datos ecuatoriana reconoce garantías frente a valoraciones automatizadas, incluso cuando la decisión se apoya parcialmente en procesos automáticos, esta formulación resulta especialmente protectora para sistemas híbridos, porque evita que una aprobación superficial excluya derechos, el responsable debe informar la existencia del tratamiento, explicar lógica relevante, permitir observaciones y facilitar intervención humana cuando exista impacto significativo (Asamblea Nacional del Ecuador, 2021).

El derecho europeo aporta una referencia comparada sobre información significativa de la lógica y sobre decisiones exclusivamente automatizadas, aunque la doctrina discute el alcance de un derecho general a la explicación, la lección aplicable consiste en combinar transparencia previa, explicación posterior y posibilidad de impugnación, evitando prometer una descripción técnica total que no permita comprender ni actuar (Parlamento Europeo y Consejo, 2016).

La explicación adecuada posee cuatro capas, la capa institucional identifica sistema, finalidad, responsable y categoría de riesgo, la capa de datos informa fuentes y variables relevantes, la capa decisional muestra factores que influyeron en el caso y la capa jurídica conecta esos factores con la norma y el efecto, esta estructura permite adaptar detalle sin confundir transparencia con divulgación indiscriminada de secretos o vulnerabilidades.

La explicación global describe cómo funciona el sistema en términos generales, mientras la explicación local muestra por qué ocurrió un resultado particular, ambas son necesarias en tributación, debido a que la primera permite escrutinio público y la segunda sostiene defensa, un registro de algoritmos sin razones individuales sería insuficiente, del mismo modo una motivación aislada sin información sobre calidad, validación y responsables impediría control sistémico.

La transparencia debe incorporar incertidumbre, un modelo predictivo no descubre hechos con certeza, estima probabilidad según datos históricos y supuestos, por ello la comunicación debe indicar que la puntuación constituye señal, mostrar límites y evitar lenguaje categórico, una autoridad que presenta el resultado como verdad oculta la naturaleza estadística y desplaza indebidamente la carga de demostrar que el perfil es incorrecto.

La igualdad exige pruebas de desempeño entre grupos relevantes, aunque el sistema no recoja categorías sensibles, variables como ubicación, actividad, facturación, conectividad o forma societaria pueden funcionar como proxies, el análisis debe valorar tasas de selección, falsos positivos, resultados de auditoría y carga de cumplimiento, no para imponer paridad matemática automática, sino para identificar diferencias injustificadas y corregir diseño o uso.

La defensa requiere acceso oportuno a datos y documentos utilizados, posibilidad de rectificación, conocimiento de razones y plazo para aportar contexto, un expediente digital debe incluir versiones y transformaciones que permitan reconstrucción, la administración puede reservar información de terceros o técnicas sensibles, pero debe entregar una explicación equivalente y justificar cualquier restricción mediante legalidad, necesidad y proporcionalidad.

La motivación algorítmica no debe reducirse a listar variables, debido a que la persona necesita entender relación causal o inferencial relevante, una explicación útil señala qué inconsistencia se observó, con qué fuente, durante qué período, qué regla se aplicó y cómo influyó en la actuación, también debe indicar límites, revisión humana y vías de corrección, transformando una salida técnica en razón administrativa controlable.

La impugnación efectiva requiere que el órgano revisor pueda acceder a documentación técnica y ordenar pruebas, una revisión limitada al texto final repetiría la opacidad, deben existir perfiles especializados capaces de examinar datos, código, validación y seguridad bajo reserva cuando corresponda, además de peritaje independiente en litigios de alto impacto, porque el control judicial necesita traducir complejidad sin abdicar frente a proveedores o expertos.

La Tabla 3 introduce la correspondencia entre derechos, riesgos y evidencia de cumplimiento, su estructura transforma principios generales en requisitos auditables, el propósito consiste en orientar diseño y revisión de expedientes, no crear una lista cerrada, debido a que la intensidad debe variar según datos, efecto, escala y vulnerabilidad de las personas afectadas.

Tabla 3. Derechos fundamentales y evidencia operativa de cumplimiento

Derecho o principio	Riesgo algorítmico	Salvaguardia operativa	Evidencia exigible
Legalidad y competencia	Modelo utilizado fuera de habilitación o por proveedor sin autoridad	Mapa de base jurídica, finalidad y responsable público	Dictamen jurídico, acto de aprobación y matriz de competencias

Derecho o principio	Riesgo algorítmico	Salvaguardia operativa	Evidencia exigible
Protección de datos	Exceso, reutilización, perfilamiento o conservación indefinida	Minimización, retención, acceso por roles y evaluación de impacto	Inventario de datos, flujos, plazos y evaluación firmada
Igualdad	Proxies, sesgo histórico y concentración de controles	Pruebas por grupos, revisión de variables y monitoreo de resultados	Informes de desempeño, falsos positivos y medidas correctivas
Motivación	Puntuación o alerta presentada como razón suficiente	Explicación local y vínculo entre hecho, norma y consecuencia	Registro de factores, fuentes, revisión y texto de motivación
Defensa	Imposibilidad de conocer o corregir datos y supuestos	Acceso, rectificación, audiencia y plazo de respuesta	Expediente reproducible, constancia de notificación y observaciones
Revisión humana	Aprobación ceremonial o dependencia automática	Competencia, tiempo, formación y facultad de apartamiento	Identidad de revisor, registro de cambios y tasa de discrepancia
Transparencia	Ausencia de información pública sobre sistemas de impacto	Registro graduado de algoritmos y documentación accesible	Ficha pública, versión, proveedor, finalidad y nivel de riesgo
Tutela efectiva	Recurso incapaz de revisar técnica o suspender efectos	Revisión especializada, peritaje y medidas provisionales	Protocolo de impugnación, acceso experto y trazabilidad completa

Nota, Elaboración propia, la evidencia propuesta puede integrarse al expediente administrativo y a la evaluación de impacto algorítmico.

El análisis de la Tabla 3 revela que la protección depende de documentación contemporánea y no de declaraciones generales de ética, una política institucional sin inventario, registros y pruebas no permite demostrar cumplimiento, la evidencia debe generarse desde diseño y mantenerse durante operación, debido a que reconstrucciones posteriores pueden ocultar cambios de versión, datos defectuosos o ausencia de revisión en el momento de la decisión.

Modelo de gobernanza para la administración tributaria ecuatoriana

El tercer resultado propone un modelo de gobernanza con ocho fases, identificación, clasificación, evaluación, autorización, desarrollo o adquisición, validación, operación y retiro, cada fase produce documentos, responsables y controles, el modelo evita concentrar cumplimiento al final del proyecto, cuando modificar datos, arquitectura o contrato resulta costoso, además permite suspender herramientas que cambien de finalidad o presenten degradación.

La identificación exige un inventario que incluya reglas expertas, modelos estadísticos, aprendizaje automático, sistemas generativos y servicios de proveedores, la etiqueta inteligencia artificial no debe decidir inclusión, cualquier herramienta que clasifique, recomiende o afecte actuaciones requiere registro, la ficha mínima contiene nombre, finalidad, unidad responsable, datos, proveedor, versión, usuarios, efecto, población y fecha de revisión.

La clasificación combina nivel de riesgo y tipo de intervención, los sistemas prohibidos abarcarían decisiones sancionadoras sin revisión, perfilamiento basado en categorías sensibles sin habilitación y reutilización incompatible, los sistemas críticos incluirían determinación, devolución adversa y selección intensiva, los sistemas altos comprenderían perfiles y requerimientos, mientras los medios y bajos mantendrían controles simplificados pero documentados.

La evaluación de impacto debe integrar derechos, datos, seguridad y operación, no limitarse a privacidad, su contenido comprende necesidad, proporcionalidad, alternativas menos intrusivas, calidad, grupos afectados, errores, explicabilidad, control humano, proveedor, ciberseguridad y reparación, el documento debe aprobarse antes del piloto y actualizarse ante cambios de datos, modelo, finalidad o efecto.

La autorización debe corresponder a un comité multidisciplinario con representación jurídica, tributaria, tecnológica, seguridad, protección de datos, auditoría y atención al contribuyente, la decisión necesita condiciones, indicadores, período y responsable, los proyectos críticos requieren revisión de una instancia independiente, evitando que la misma unidad que busca eficiencia evalúe sin contrapeso riesgos para derechos.

La adquisición tecnológica exige contratos que garanticen acceso a documentación, portabilidad, auditoría, notificación de cambios, seguridad, conservación probatoria y terminación, una cláusula de secreto comercial no puede impedir motivación ni control

público, el proveedor debe informar datos de entrenamiento, limitaciones, subcontratistas y métricas, mientras la administración conserva capacidad técnica para verificar y no depender totalmente de afirmaciones externas.

La validación previa necesita conjuntos representativos, pruebas funcionales, seguridad, robustez, sesgo, explicabilidad y revisión humana, el rendimiento promedio resulta insuficiente cuando el costo de falsos positivos recae en contribuyentes, deben medirse tasas por segmentos relevantes y escenarios extremos, además de comparar el modelo con procesos existentes, porque una innovación solo se justifica si mejora precisión, tiempo o costos sin deteriorar derechos.

La operación requiere monitoreo continuo, registros inalterables, alertas de degradación, control de accesos y revisión periódica, los cambios automáticos o aprendizaje continuo deben estar limitados, una versión nueva no puede afectar decisiones sin validación y aprobación, los indicadores deben incluir resultados favorables y adversos, apartamientos humanos, reclamos, correcciones, incidentes, sesgos y tiempo de explicación.

El retiro procede cuando expira la finalidad, cambia la norma, disminuye rendimiento, surge riesgo no mitigable o termina el contrato, la administración debe conservar evidencia necesaria para procesos abiertos y eliminar datos conforme a retención, también debe comunicar reemplazo y garantizar continuidad de recursos, un sistema retirado no puede permanecer operando por inercia ni alimentar nuevos modelos sin evaluación de compatibilidad.

La supervisión externa puede articular competencias del órgano de protección de datos, control administrativo, transparencia, auditoría y jurisdicción, sin crear una autoridad única de manera inmediata, aunque resulta recomendable establecer un protocolo interinstitucional, publicar reportes agregados y permitir auditorías bajo reserva, la

coordinación evita zonas grises donde cada entidad considere que la revisión corresponde a otra.

La Tabla 4 introduce el modelo de gobernanza propuesto y sus productos verificables, la secuencia permite asignar responsabilidades desde la idea hasta el retiro, además convierte transparencia, protección de datos y debido proceso en controles concretos, la tabla puede utilizarse como base de política institucional, manual de proyectos o cláusulas de contratación tecnológica.

Tabla 4. Ciclo de gobernanza algorítmica tributaria propuesto

Fase	Responsable principal	Producto obligatorio	Control de derechos	Indicador mínimo
Identificación	Unidad propietaria y tecnología	Ficha de inventario y mapa de datos	Finalidad, base jurídica y población afectada	Cobertura total de sistemas registrados
Clasificación	Comité multidisciplinario	Nivel de riesgo y tipo de intervención	Prohibiciones, revisión humana y vía de recurso	Porcentaje con clasificación vigente
Evaluación	Protección de datos, jurídico y seguridad	Evaluación de impacto integral	Necesidad, proporcionalidad, sesgo, explicación y seguridad	Riesgos críticos mitigados antes del piloto
Autorización	Autoridad competente o comité independiente	Resolución con condiciones y plazo	Responsable identificable y límites de uso	Autorizaciones con fecha de revisión
Desarrollo o compra	Tecnología y contratación	Documentación técnica y cláusulas de auditoría	Acceso, portabilidad, secreto limitado y trazabilidad	Proveedores con obligaciones completas
Validación	Equipo independiente de prueba	Informe de rendimiento, sesgo y robustez	Calidad, grupos afectados y capacidad de revisión	Umbrales aprobados y falsos positivos aceptables
Operación	Unidad usuaria y auditoría interna	Registros, monitoreo y reportes periódicos	Explicación, corrección, reclamo y control humano	Incidentes, apartamientos y reclamos resueltos
Retiro	Autoridad propietaria y archivo	Plan de desactivación y conservación probatoria	Eliminación, continuidad y protección de procesos abiertos	Sistemas retirados sin uso residual

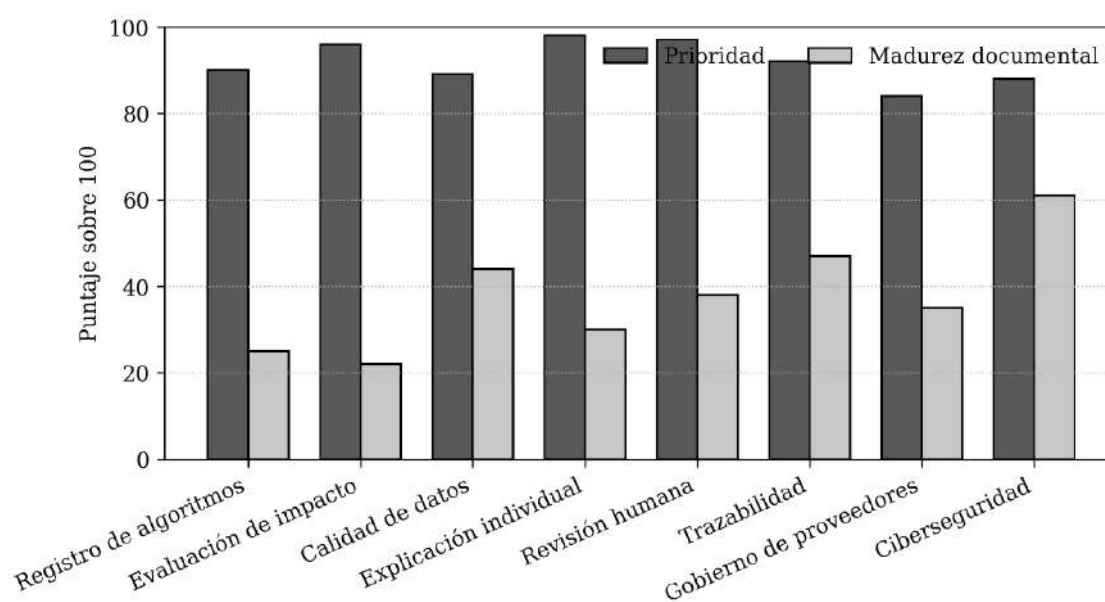
Nota, Elaboración propia a partir del enfoque basado en riesgo, responsabilidad proactiva y debido proceso tecnológico.

El análisis de la Tabla 4 evidencia que la gobernanza requiere productos obligatorios y no recomendaciones voluntarias, el inventario permite conocer qué existe, la evaluación anticipa daños, la autorización asigna responsabilidad y el monitoreo detecta degradación, esta arquitectura puede implementarse mediante regulación interna sin

esperar una ley especial, aunque los usos críticos deberían recibir desarrollo normativo expreso para fortalecer seguridad jurídica.

El Gráfico 3 compara prioridad de implementación y madurez documental estimada para ocho controles, la introducción visual destaca las brechas que demandan atención inmediata, los puntajes de madurez derivan del corpus público y no evalúan prácticas internas no publicadas, mientras la prioridad considera efecto sobre derechos, capacidad preventiva y dependencia respecto de otros controles.

Gráfico 3. Brecha de prioridad y madurez de controles algorítmicos



Nota, Elaboración propia, una brecha amplia indica necesidad de política, procedimiento y evidencia pública, no incumplimiento institucional demostrado.

El análisis del Gráfico 3 ubica explicación individual, revisión humana y evaluación de impacto como prioridades principales, el registro público y la calidad de datos también muestran brechas relevantes, la ciberseguridad presenta mayor madurez relativa por su tradición institucional, aunque debe integrarse con derechos y no operar de forma aislada, el orden recomendado comienza por inventario y clasificación, continúa con impacto y termina con auditoría permanente.

Discusión

Los resultados coinciden con la idea de administración tributaria digital integrada, aunque introducen una condición jurídica esencial, la disponibilidad temprana de datos no autoriza decisiones invisibles, el cumplimiento por diseño debe acompañarse de garantías por diseño, de modo que cada automatización reduzca cargas y mejore precisión sin impedir conocimiento, corrección y recurso (Organización para la Cooperación y el Desarrollo Económicos, 2020; Organización para la Cooperación y el Desarrollo Económicos, 2024a).

La comparación con el Reglamento europeo de inteligencia artificial muestra convergencia en gestión de riesgos, calidad, documentación, supervisión y seguridad, pero el derecho tributario ecuatoriano exige incorporar motivación, reserva legal y prueba, la clasificación europea puede inspirar controles, aunque la categoría de alto riesgo debe adaptarse al efecto fiscal, incluyendo devolución, selección, determinación y sanción como ámbitos prioritarios.

El Convenio del Consejo de Europa refuerza la relación entre inteligencia artificial, derechos humanos, democracia y Estado de derecho, su enfoque de evaluación de riesgos e impactos confirma que la gobernanza no puede limitarse a precisión, la administración tributaria ejerce poder público y sus sistemas deben permitir responsabilidad, información y remedios, incluso cuando el modelo provenga de un proveedor privado (Consejo de Europa, 2024).

La rendición de cuentas algorítmica puede lograrse sin exigir transparencia absoluta, mediante documentación, pruebas, registros y acceso diferenciado, la propuesta coincide con modelos de algoritmos responsables que combinan verificabilidad técnica y control institucional, un auditor puede revisar código o datos bajo reserva mientras el

contribuyente recibe razones comprensibles y el público conoce finalidad, riesgos y desempeño agregado (Kroll y colaboradores, 2017).

La transparencia predictiva enfrenta una tensión entre revelar criterios y preservar efectividad del control, esa tensión no debe resolverse mediante secreto total, pueden publicarse categorías, gobernanza y métricas, mientras los detalles manipulables permanecen restringidos, la restricción necesita fundamento, prueba de daño y revisión periódica, porque la opacidad institucional también produce costos, errores y pérdida de legitimidad (Zarsky, 2013).

La novedad científica consiste en integrar cinco campos que suelen analizarse por separado, potestad tributaria, procedimiento administrativo, protección de datos, transparencia y gobernanza de inteligencia artificial, la matriz propuesta no considera el algoritmo como objeto técnico aislado, sino como parte de un sistema sociotécnico que incluye datos, personas, contratos, normas, incentivos y recursos, perspectiva necesaria para evaluar impactos reales.

La primera aplicación práctica corresponde a diseño institucional, el modelo puede convertirse en política del Servicio de Rentas Internas con inventario, clasificación, evaluación y reportes, la segunda aplicación corresponde a contratación, mediante cláusulas que aseguren auditoría y portabilidad, la tercera se orienta a expedientes, incorporando explicación local, registro de revisión y acceso a datos, la cuarta apoya control externo y litigio.

La automatización favorable ofrece una estrategia de innovación compatible con derechos, aprobaciones, devoluciones o correcciones beneficiosas pueden procesarse automáticamente cuando existe alta confianza, mientras resultados adversos se derivan a revisión humana, este diseño reduce carga y tiempo sin trasladar el costo del error a la

persona, además crea incentivos para mejorar calidad y evita que eficiencia se concentre exclusivamente en control y sanción.

La participación de contribuyentes, profesionales, academia y sociedad civil puede mejorar comprensión y legitimidad, las consultas no deben revelar métodos de evasión, pero sí discutir finalidades, categorías de datos, mecanismos de explicación y reclamo, la participación temprana identifica efectos no previstos sobre pequeños negocios, personas con baja conectividad o sectores informales, además facilita lenguaje claro y accesibilidad de comunicaciones.

La alfabetización algorítmica del personal resulta tan importante como la formación técnica, quienes utilizan modelos necesitan comprender límites, correlación, incertidumbre, sesgo y obligación de apartamiento, mientras los equipos tecnológicos requieren conocimiento de legalidad, prueba y procedimiento, la colaboración interdisciplinaria evita que la decisión se fragmente hasta el punto de que ninguna persona pueda explicar finalidad, datos, modelo y consecuencia.

Las limitaciones del estudio impiden afirmar qué sistemas se encuentran operativos o cómo funcionan, la ausencia de información pública puede reflejar inexistencia, reserva legítima o falta de transparencia, por tanto las puntuaciones describen documentos y no desempeño institucional, también existe riesgo de cambio normativo, debido a que la regulación de inteligencia artificial evoluciona rápidamente y las propuestas deben revisarse de forma periódica.

Las investigaciones futuras deberían examinar expedientes anonimizados, tasas de falsos positivos, perfiles de selección, contratos y evaluaciones de impacto, también conviene estudiar percepción de contribuyentes y funcionarios, eficacia de explicaciones, accesibilidad y costos de recurso, una línea comparada regional

permitiría identificar modelos de supervisión tributaria y adaptar estándares sin reproducir estructuras extranjeras incompatibles con capacidades nacionales.

Conclusiones

La inteligencia artificial y la analítica de datos pueden fortalecer control, asistencia y eficiencia tributaria, siempre que su función permanezca delimitada por legalidad, finalidad y proporcionalidad, el valor tecnológico no elimina la naturaleza pública de la actuación, cualquier resultado que influya sobre una obligación requiere autoridad responsable, evidencia verificable y posibilidad de revisión, incluso cuando el sistema solo aparezca como herramienta de apoyo.

El marco ecuatoriano contiene protección constitucional y legal suficiente para exigir datos pertinentes, calidad, transparencia, motivación, defensa y revisión humana, aunque las obligaciones aparecen dispersas y carecen de desarrollo técnico sectorial, la brecha principal se ubica en inventario, clasificación, evaluación de impacto, trazabilidad, auditoría, explicación individual y coordinación entre protección de datos, transparencia y administración tributaria.

La distinción entre asistencia, alerta, recomendación, decisión semiautomatizada y decisión automatizada resulta indispensable, porque el riesgo depende del efecto y del control real, no del nombre del software, los usos relacionados con devoluciones adversas, determinación y sanción requieren tratamiento crítico, mientras herramientas informativas o descriptivas pueden operar bajo controles simplificados, siempre con finalidad, seguridad, actualización y responsable identificado.

La transparencia algorítmica compatible con secreto tributario y ciberseguridad debe organizarse por capas, información pública sobre finalidad, datos, responsables y desempeño, explicación individual sobre factores y fuentes, acceso especializado a documentación técnica y control reservado cuando exista riesgo, este modelo evita tanto divulgación indiscriminada como opacidad absoluta y permite que la persona comprenda, corrija e impugne.

La revisión humana solo protege derechos cuando existe capacidad efectiva de apartarse, conocimiento de limitaciones, tiempo suficiente y responsabilidad, una firma formal no transforma una decisión automática en decisión humana, por ello deben registrarse identidad, evidencia revisada, cambios y motivos, además de medir tasas de discrepancia, reclamos y correcciones, indicadores que muestran si el control opera o funciona como simple validación ceremonial.

La propuesta de gobernanza basada en ocho fases permite implementar controles desde identificación hasta retiro, su aplicación no depende por completo de una nueva ley, debido a que puede apoyarse en responsabilidad proactiva, procedimiento administrativo y competencias institucionales, sin embargo los usos críticos necesitan regulación expresa que determine límites, intervención humana, contenido de la explicación, conservación probatoria y efectos de una falla algorítmica.

La protección de derechos no constituye obstáculo externo a la innovación, representa condición de calidad y sostenibilidad, datos corregibles, modelos auditables y decisiones motivadas reducen litigios, errores y pérdida de confianza, la automatización favorable demuestra que eficiencia y garantías pueden reforzarse, siempre que el costo del error no se traslade al contribuyente y que los resultados adversos reciban revisión reforzada.

Referencias Bibliográficas

Asamblea Nacional del Ecuador. (2008). Constitución de la República del Ecuador.

Registro Oficial 449.

Asamblea Nacional del Ecuador. (2017). Código Orgánico Administrativo. Registro

Oficial Segundo Suplemento 31.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos

Personales. Registro Oficial Quinto Suplemento 459.

Asamblea Nacional del Ecuador. (2023). Ley Orgánica de Transparencia y Acceso a la

Información Pública. Registro Oficial Segundo Suplemento 245.

Citron, D. K. (2008). Technological due process. *Washington University Law Review*,

85(6), 1249–1313.

Congreso Nacional del Ecuador. (2005). Código Tributario, Codificación 9. Registro

Oficial Suplemento 38.

Consejo de Europa. (2024). Convenio marco sobre inteligencia artificial, derechos

humanos, democracia y Estado de derecho, CETS 225.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., y

Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*,

165(3), 633–705.

Organización para la Cooperación y el Desarrollo Económicos. (2020). Tax

administration 3.0: The digital transformation of tax administration. OECD

Publishing.

Organización para la Cooperación y el Desarrollo Económicos. (2024a). Tax

administration 2024: Comparative information on OECD and other advanced

and emerging economies. OECD Publishing.

Organización para la Cooperación y el Desarrollo Económicos. (2024b).

Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

Parlamento Europeo y Consejo. (2016). Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Diario Oficial de la Unión Europea.

Parlamento Europeo y Consejo. (2024). Reglamento UE 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea.

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Presidencia de la República del Ecuador. (2023). Reglamento General a la Ley Orgánica de Protección de Datos Personales, Decreto Ejecutivo 904. Registro Oficial Tercer Suplemento 435.

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., y Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. Proceedings of the Conference on Fairness, Accountability, and Transparency, 59–68.

Servicio de Rentas Internas. (2021). Plan Estratégico Institucional 2021–2025. Servicio de Rentas Internas.

UNESCO. (2021). Recomendación sobre la ética de la inteligencia artificial.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Wachter, S., Mittelstadt, B., y Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law and Technology, 31(2), 841–887.

Zarsky, T. Z. (2013). Transparent predictions. University of Illinois Law Review, 2013(4), 1503–1570.