Del Procedimiento al Algoritmo: Nuevo Modelo de Auditoría de Sistemas Automatizados en la Administración Pública (MIASA-SP).

Sandra Barrio Carvajal
Auditora de la Cámara de Cuentas de Andalucía

Revista Auditoría Pública nº 86
Diciembre 2025. Páginas: 119-131

Resumen: La Administración Pública ya no se guía únicamente por el juicio humano: los algoritmos comienzan a decidir sobre derechos, ayudas y procedimientos. Las Actuaciones Administrativas Automatizadas (AAA) representan una transformación profunda en la relación entre el Estado y la ciudadanía, abriendo nuevas oportunidades de eficiencia, pero también desafíos éticos, jurídicos y sociales de enorme alcance. ¿Cómo garantizar que las decisiones algorítmicas sean legales, transparentes y justas?
Este artículo propone una innovación metodológica en la auditoría pública, presentando el modelo MIASA-SP, diseñado para auditar sistemas automatizados con rigor técnico, jurídico y ético. A lo largo del texto, se desentraña la diferencia entre AAA y los sistemas que las sustentan, distinguiendo entre tecnologías deterministas y no deterministas, cada una con implicaciones distintas para la trazabilidad y la responsabilidad legal.
Se ofrece una clasificación exhaustiva de riesgos: éticos, jurídicos, de privacidad, de explicabilidad y técnicos, acompañados de matrices que vinculan ejemplos reales, preguntas clave de auditoría y medidas de mitigación concretas. Además, se analizan seis modelos internacionales de auditoría algorítmica, desde enfoques basados en criterios normativos hasta auditorías contínuas asistidas por Inteligencia Artificial, adaptadas al contexto público.
Finalmente, se presenta el modelo MIASA-SP, estructurado en seis fases que abarcan desde el análisis del sistema hasta la evaluación ética y jurídica, con herramientas como minería de procesos, auditoría de logs y entrevistas institucionales.
Este artículo no solo aporta teoría, sino una metodología aplicable que transforma la auditoría pública en tiempos de algoritmos. Ideal para profesionales que buscan auditar con inteligencia, equidad y trazabilidad.

Palabras Clave: Automatización, Inteligencia Artificial, actuaciones administrativas automatizadas, algotitmos y auditoría.

Abstract: Public Administration is no longer guided solely by human judgement: algorithms are beginning to decide on rights, aid, and procedures. Automated Administrative Actions (AAAs) represent a profound transformation in the relationship between the State and its citizens, opening up new opportunities for efficiency but also immense ethical, legal, and social challenges. How can we ensure that algorithmic decisions are legal, transparent, and fair?
This article proposes a methodological innovation in public auditing, presenting the MIASA-SP model, designed to audit automated systems with technical, legal, and ethical rigour. Throughout the text, the difference between AAAs and the systems that support them is unravelled, distinguishing between deterministic and non-deterministic technologies, each with distinct implications for traceability and legal accountability. An exhaustive classification of risks is offered: ethical, legal, privacy, explainability, and technical, accompanied by matrices that link real-world examples, key audit questions, and specific mitigation measures. Furthermore, six international models of algorithmic auditing are analysed, ranging from approaches based on regulatory criteria to continuous audits assisted by Artificial Intelligence, adapted to the public context. Finally, the MIASA-SP model is presented, structured in six phases that cover everything from system analysis to ethical and legal evaluation, with tools such as process mining, log auditing, and institutional interviews. This article provides not only theory but also an applicable methodology that transforms public auditing in the age of algorithms. Ideal for professionals seeking to audit with intelligence, fairness, and traceability.

Keywords: Automation, Artificial Intelligence, automated administrative actions, algorithms and auditing.

1. Introducción.

La transformación digital de las Administraciones Públicas (AAPP) ha pasado de ser un objetivo deseado a constituir una obligación imprescindible. En este contexto, las Actuaciones Administrativas Automatizadas (AAA) representan un salto cualitativo en la forma en que se gestionan los procedimientos, se prestan servicios y se garantiza la trazabilidad de las decisiones públicas. Una AAA se define, según el artículo 41 de la Ley 40/2015, como aquella actuación realizada íntegramente por medios electrónicos, sin intervención directa de un empleado público. Esta definición, aunque aparentemente técnica, encierra profundas implicaciones jurídicas, organizativas y éticas.

Desde la perspectiva de la auditoría pública, el auge de las AAA plantea nuevos desafíos que trascienden a la revisión documental tradicional. La automatización exige una adaptación metodológica que permita evaluar no solo la legalidad formal del procedimiento, sino también la robustez del sistema, la transparencia algorítmica y la equidad en la toma de decisiones. El papel de los auditores del siglo XXI debe evolucionar hacia una figura proactiva, capaz de auditar algoritmos, validar modelos de decisión y garantizar que la tecnología no erosione los derechos fundamentales.

Este trabajo persigue tres objetivos fundamentales: analizar las AAA, contribuir a la comprensión de los nuevos entornos digitales y examinar los riesgos vinculados a su implementación. A partir de estas reflexiones, se presenta el nuevo Modelo Integral para la Auditoría de Sistemas Automatizados en el Sector Público (MIASA-SP), como propuesta innovadora orientada a enfrentar los retos emergentes en la materia. Frente a otros modelos tradicionales, esta propuesta aporta un enfoque multidisciplinar, dinámico y orientado a la trazabilidad, lo que puede contribuir a reforzar la confianza ciudadana en las decisiones automatizadas.

2. Concepto de AAA y sistemas automatizados.

En el marco de la transformación digital de la administración pública, resulta esencial distinguir entre las actuaciones administrativas automatizadas, reguladas en el artículo 41 de la Ley 40/2015 de procedimiento administrativo, y los sistemas automatizados que las sustentan. La AAA constituye una categoría jurídica específica que se refiere a la emisión de actos administrativos con efectos legales mediante medios electrónicos, sin intervención humana en la decisión concreta. Su definición se vincula al resultado jurídico que produce como expresión formal de la voluntad administrativa. En cambio, el sistema automatizado alude al conjunto de herramientas tecnológicas, algoritmos, motores de reglas, interfaces, modelos de inteligencia artificial, que permiten ejecutar tareas de forma automática. No todo sistema automatizado genera una AAA, pero toda AAA se apoya necesariamente en un sistema automatizado. Esta distinción es clave para delimitar el objeto auditable, identificar riesgos normativos y establecer criterios de trazabilidad en entornos automatizados.

Desde una perspectiva técnica, los sistemas automatizados pueden agruparse en dos grandes categorías: deterministas y no deterministas. Los sistemas deterministas operan bajo reglas explícitas y predecibles, lo que significa que ante una misma entrada producen siempre el mismo resultado. Esta lógica secuencial y controlada facilita su trazabilidad, validación y auditoría, siendo especialmente adecuada para entornos normativos exigentes. En la administración pública, el grupo que incluye tecnologías como scripts, macros, automatización de bases de datos y OCR (reconocimiento óptico de caracteres), conforman la automatización básica. La automatización avanzada utiliza tecnologías como RPA (automatización robótica de procesos), BPM (gestión de procesos de negocios) y APIs (interfaz de programación de aplicaciones). Su comportamiento es replicable y verificable, lo que permite aplicar modelos de auditoría tradicionales basados en control de reglas, seguimiento de logs y revisión de parámetros.

Por otro lado, los sistemas no deterministas constituyen un conjunto de tecnologías más complejo y dinámico, caracterizado por comportamientos probabilísticos, aprendizaje autónomo y generación de resultados variables ante entradas similares. Estos sistemas no siguen reglas fijas, sino que operan mediante modelos que evolucionan con el tiempo, adaptándose a patrones, contextos o datos cambiantes. En este grupo se inscriben los niveles de automatización cognitiva y automatización basada en inteligencia artificial, que incluyen tecnologías como machine learning, analítica avanzada, redes neuronales, sistemas expertos, procesamiento de lenguaje natural,

deep learning, agentes autónomos, e IA (inteligencia artificial) generativa. Su capacidad para procesar información estructurada, semiestructurada y no estructurada los convierte en herramientas potentes, pero también plantea desafíos significativos para la auditoría: explicabilidad de decisiones, control de sesgos, validación continua y atribución de responsabilidad jurídica. La naturaleza no determinista exige enfoques de auditoría adaptativos, con criterios de observabilidad, gobernanza algorítmica y evaluación ética.

En síntesis, la correcta identificación de tres elementos diferenciados, la AAA como resultado jurídico, los sistemas automatizados deterministas como soporte técnico trazable y los sistemas no deterministas como entornos dinámicos de decisión, constituye una condición previa para diseñar modelos de auditoría eficaces, proporcionales y jurídicamente fundados en la administración automatizada.

Fuente: Elaboración propia

3. Riesgos de las AAA.

La implementación de Actuaciones Administrativas Automatizadas ha supuesto un avance significativo en la modernización de las Administraciones Públicas. Su uso permite optimizar recursos, agilizar procedimientos y mejorar la trazabilidad de las decisiones. Sin embargo, también plantea riesgos sustanciales que deben ser abordados desde la auditoría pública con un enfoque multidisciplinar.

A continuación, se presenta una clasificación de los distintos tipos de riesgos con los que nos podemos enfrentar, así como una matriz con los riesgos.

Riesgos éticos y sociales.

- Sesgos algorítmicos y discriminación. Los algoritmos entrenados con datos históricos pueden reproducir desigualdades sociales, económicas o de género, afectando a colectivos vulnerables y comprometiendo el principio de igualdad ante la ley (Soriano, 2021).
- Exclusión digital y brecha social. Si ciertos grupos de profesionales, como auditores en mercados emergentes o de firmas más pequeñas, no tienen acceso a las tecnologías más avanzadas o a la capacitación adecuada, podrían quedarse atrás en términos de competencia y efectividad (Chicaiza Ortiz, 2024).
- Sesgo de automatización en empleados públicos. Confianza en exceso en los sistemas automatizados de ayuda a la toma de decisiones que usan cada vez con mayor frecuencia e intensidad (Mir Puigpelat, 2023).
- Desconfianza ciudadana. Impulsada por la percepción de opacidad y la falta de educación tecnológica, representa un obstáculo para la aceptación y efectividad de la IA (Hilario Rivas et al., 2025).
- Deshumanización en la toma de decisiones públicas. La percepción de que las decisiones públicas son tomadas por máquinas opacas puede erosionar la legitimidad institucional y generar desafección política (Boix Palop & Cotino Hueso, 2019).

Matriz de riesgos éticos y sociales.

Riesgo	Ejemplo en la administración pública	Pregunta de auditoría	Medidas de mitigación
Sesgos algorítmicos y discriminación	Sistema de asignación de ayudas sociales discrimina indirectamente a colectivos vulnerables.	¿Se han realizado pruebas de impacto algorítmico que verifiquen que el sistema no discrimina directa ni indirectamente a colectivos vulnerables?	Auditorías de sesgos, pruebas de impacto algorítmico, datasets inclusivos.
Exclusión digital y brecha social	Contralorías locales sin acceso a software de IA, mientras que ministerios centrales sí lo tienen.	¿Todos los organismos y funcionarios implicados cuentan con acceso equitativo a la tecnología y capacitación necesaria para utilizar el sistema automatizado?	Programas de capacitación pública, licencias gubernamentales compartidas.
Sesgo de automatización	Órgano fiscalizador aprueba cuentas públicas basándose solo en reportes de IA sin análisis humano.	¿Existen mecanismos que obliguen a la revisión humana crítica de los resultados generados por el sistema antes de adoptar decisiones relevantes?	Normas que obliguen revisión humana en procesos críticos.
Desconfianza ciudadana	Ciudadanos sospechan manipulación en algoritmos de control tributario.	¿La Administración publica de forma accesible la lógica, criterios o reglas del sistema automatizado para garantizar transparencia ante la ciudadanía?	Publicación de algoritmos auditados, comunicación transparente.
Deshumanización en decisiones	Denegación automática de subsidios sin revisión de un funcionario.	¿El sistema contempla instancias de apelación o revisión por parte de un funcionario cuando la decisión afecta directamente a derechos ciudadanos?	Establecer instancias de apelación humanas.

Riesgos jurídicos y normativos.

- Desactualización normativa. Incertidumbre sobre el impacto potencial de la nueva tecnología y un marco legal existente no adaptado para el nuevo escenario sociotécnico ha generado una serie de dificultades en relación con el uso de la IA. (Sobrino-García, 2021).

- Responsabilidad difusa. La atribución de responsabilidad en caso de errores algorítmicos es incierta: ¿responde el programador, el proveedor o la Administración? Esto compromete la seguridad jurídica (Cerrillo i Martínez, 2021).

- Falta de garantías jurídicas en controles automatizados. Sistemas como los utilizados por la Agencia Tributaria pueden presentar errores sistemáticos si no se auditan adecuadamente, afectando la robustez y legalidad de los procedimientos (Capdeferro Villagrasa, 2025).

Matriz de riesgos jurídicos y normativos.

Riesgo	Ejemplo en la administración pública	Pregunta de auditoría	Medidas de mitigación
Desactualización normativa	Ley de procedimiento administrativo no regula decisiones automatizadas.	¿El marco legal y reglamentario vigente regula explícitamente las actuaciones automatizadas que realiza el sistema auditado?	Reforma normativa, incorporación de capítulos de IA en leyes administrativas.
Responsabilidad difusa	Error en asignación de becas estatales: ¿culpa del proveedor, del ministerio o del programador?	¿Están claramente definidas y documentadas las responsabilidades de cada actor (programador, proveedor, administración) en caso de fallo del sistema?	Contratos con cláusulas claras de responsabilidad compartida.
Falta de garantías jurídicas	Uso automatizado de historiales médicos en auditorías de hospitales públicos.	¿Se han establecido medidas efectivas (anonimización, limitaciones de acceso, consentimiento informado) para proteger los datos personales tratados por el sistema?	Anonimización de datos, límites legales estrictos.

Riesgos en protección de datos y privacidad.

- Tratamiento masivo de datos personales. La automatización implica un uso intensivo de datos, lo que puede vulnerar la privacidad. El artículo 22 del Reglamento General de Protección de Datos limita las decisiones basadas exclusivamente en procesos automatizados con efectos jurídicos.
- Estado vigilante. El uso indiscriminado de datos puede generar una sensación de vigilancia constante, afectando la dignidad y autonomía de las personas (Mir Puigpelat, 2023).

Matriz de riesgos en protección de datos y privacidad.

Riesgo	Ejemplo en la administración pública	Pregunta de auditoría	Medidas de mitigación
Tratamiento masivo de datos	Agencia Tributaria aplica cruces masivos de datos que generan sanciones erróneas.	¿Existen controles jurídicos y técnicos que aseguren que los cruces masivos de datos no generan decisiones erróneas sin posibilidad de reclamación ciudadana?	Supervisión jurídica previa, mecanismos de reclamación ciudadana.
Estado vigilante	Sistemas de control fiscal que rastrean transacciones personales constantemente.	¿Se informa de manera clara a los ciudadanos sobre qué datos se recopilan, con qué finalidad y bajo qué salvaguardas, evitando la percepción de vigilancia excesiva?	Transparencia en políticas de datos, auditorías de privacidad.

Fuente: Elaboración propia

Riesgos de transparencia y explicabilidad.

- Opacidad algorítmica. Los efectos de "caja negra" (black box) del funcionamiento de este tipo de sistemas que, a partir de un determinado punto, impiden incluso a sus programadores una predeterminación fiable de los resultados concretos (Boix Palop, A. 2020). Esto impide la trazabilidad y el control efectivo.

- Falta de motivación suficiente. Las decisiones automatizadas debido a su complejidad dificultan y complican la motivación de los actos limitando la capacidad de los ciudadanos para recurrir las decisiones de la Administración (Jiménez-Castellanos, 2023).

- Dificultad para auditar sistemas opacos. En auditoría, los algoritmos complejos como las redes neuronales dificultan la revisión técnica y jurídica de los procesos automatizados (Michifuji, 2024).

Matriz de riesgos de trazabilidad y explicabilidad.

Riesgo	Ejemplo en la administración pública	Pregunta de auditoría	Medidas de mitigación
Opacidad algorítmica	Ministerio de Hacienda no puede justificar cómo un algoritmo detecta fraude fiscal.	¿El sistema utiliza modelos interpretables y mantiene registros de trazabilidad que permitan justificar cómo se generan los resultados?	Uso de modelos interpretables, registro de trazabilidad obligatorio.
Falta de motivación suficiente	Contribuyente sancionado automáticamente sin explicaciones claras.	¿Las resoluciones emitidas por el sistema incluyen explicaciones claras y comprensibles que permitan al ciudadano conocer los fundamentos de la decisión?	Generar notificaciones con justificación detallada y comprensible.
Dificultad de auditoría	Tribunal de Cuentas no puede auditar un sistema automatizado usado en control de contrataciones públicas.	¿El sistema facilita el acceso regulado a su código fuente, reglas de decisión o documentación técnica suficiente para permitir una auditoría efectiva?	Estándares de "IA auditable", acceso regulado a código fuente.

Riesgos técnicos en auditoría automatizada.

- Dependencia excesiva de sistemas automatizados. La confianza desmedida en herramientas automatizadas puede debilitar el juicio profesional del auditor. Esto representa un riesgo, ya que, puede limitar la capacidad de los auditores para ejercer juicio crítico y detectar errores que requieren un análisis humano más profundo (Hurtado-Guevara, 2024).

- Sobrecarga de información y ruido de datos. La automatización permite auditar el 100% de las transacciones, pero también genera grandes volúmenes de datos que pueden dificultar la identificación de hallazgos relevantes. A medida que se automatizan más procesos, la cantidad de información que los auditores deben analizar puede resultar abrumadora, dificultando la identificación de los aspectos críticos que requieren atención (Hurtado-Guevara, 2024).

- Falta de trazabilidad en los procesos algorítmicos. En ocasiones, los sistemas automatizados no ofrecen trazabilidad clara sobre cómo se generan los resultados, e incluso se puede dar el caso de que se haya retirado dicho sistema y no hayan sido guardados correctamente el respal-

do de los logs.

- Necesidad de nuevas competencias. Los auditores que se enfrentan con auditorías de este tipo de sistemas deberán formarse y adquirir los conocimientos necesarios, así como, en la medida de lo posible, contar con la ayuda de expertos.
- Audit-washing[1]. Existe el riesgo de que una auditoría esté mal diseñada o ejecutada. Las auditorías inadecuadas o aquellas sin estándares claros proporcionan una falsa garantía de cumplimiento con normativas y leyes, "Audit-washing" de prácticas problemáticas o ilegales (Goodman et al., 2022).

Matriz de riesgos técnicos en auditoría automatizada.

Riesgo	Ejemplo en la administración pública	Pregunta de auditoría	Medidas de mitigación
Dependencia excesiva	Un equipo de fiscalización confía solo en el sistema de alertas sin revisión documental.	¿Se verifica que los auditores ejercen un juicio profesional independiente y no se limitan a aceptar los resultados de los sistemas automatizados sin análisis adicional?	Capacitación en juicio profesional y ética pública.
Sobrecarga de información	Un OCEX recibe bases de datos sin depurar y mucha información no relevante.	¿Existen mecanismos (herramientas de minería de datos, paneles de control) que permitan filtrar, priorizar y depurar la información generada por el sistema?	Herramientas de minería de datos y dashboards de priorización.
Falta de trazabilidad	El sistema no registra logs de acceso ni de modificaciones a la información financiera	¿El sistema registra de forma inviolable los accesos, modificaciones y operaciones realizadas, garantizando la trazabilidad de todo el proceso?	Implementar logs automáticos e inviolables de accesos y cambios en el sistema.
Nuevas competencias	Auditores que carecen de conocimientos para revisar algoritmos de contratación automatizada.	¿El personal auditor cuenta con formación y capacitación específica para revisar algoritmos, datos y procesos automatizados de manera competente?	Plan de formación en auditoría digital.
Audit-washing	Informe de auditoría externa avala un sistema de contratación, pese a evidencias de favoritismo.	¿Se aplican estándares oficiales y metodologías rigurosas de auditoría algorítmica que eviten evaluaciones superficiales o legitimadoras de malas prácticas?	Estándares oficiales de auditoría algorítmica en sector público.

Fuente: Elaboración propia

1 Fenómeno por el cual auditorías mal diseñadas ofrecen una falsa sensación de cumplimiento.

En síntesis, los riesgos y desafíos éticos de la automatización en la Administración Pública obligan a replantear los modelos de gobernanza. No basta con incorporar tecnología avanzada, es imprescindible integrar principios éticos como la equidad, la transparencia, la responsabilidad y la inclusión. Solo de este modo la automatización podrá convertirse en un instrumento al servicio de la ciudadanía y no en un mecanismo de erosión de derechos fundamentales.

4. Modelos de auditoría aplicables.

La auditoría de Actuaciones Administrativas Automatizadas exige modelos adaptados a la complejidad técnica, jurídica y organizativa de los sistemas implicados. En los últimos años, se han desarrollado enfoques innovadores que permiten auditar algoritmos, sistemas de decisión automatizada y herramientas basadas en inteligencia artificial (IA), especialmente en el contexto de la administración pública. A continuación, se presentan una serie de modelos doctrinales.

1. Auditoría basada en criterios (Criterion Audit).

Lam et al. (2024) proponen el modelo de criterion audit, diseñado para auditar sistemas algorítmicos desde una perspectiva de cumplimiento normativo y garantía externa. La definen como una evaluación externa independiente basada en criterios de un sistema algorítmico realizada por un auditor para determinar si el sistema dado cumple con los requisitos establecidos por un marco normativo. Este enfoque se inspira en la auditoría financiera tradicional, pero adaptado a sistemas de IA. El modelo se basa en criterios verificables, independencia del auditor, formación especializada y publicación parcial de resultados. Se ha aplicado con éxito en auditorías de sesgo algorítmico en procesos de selección automatizados. Es decir, una auditoría basada en criterios evalúa si el sistema cumple con normas, políticas y buenas prácticas predefinidas. Se centra en identificar brechas entre los criterios establecidos y el funcionamiento real, detectando riesgos como fallas de seguridad, trazabilidad o confiabilidad de los datos.
Este modelo puede adaptarse a AAA en el sector público, incorporando criterios como trazabilidad, explicabilidad, control humano y respeto a derechos fundamentales.

2. Auditoría asistida por IA y análisis de datos.

KPMG (2024) destaca el uso de IA y analítica avanzada en auditoría interna, especialmente para detectar fraudes, evaluar riesgos y automatizar tareas rutinarias. Este enfoque permite cubrir el 100% de las transacciones, identificar patrones complejos y mejorar la calidad de las auditorías. En el contexto de AAA, estas herramientas pueden ser utilizadas para validar trazabilidad, revisar logs, y detectar desviaciones y tendencias en procesos automatizados.

3. Modelos de auditoría adaptados al contexto cultural y regulatorio.

Pugliese (2025), desde el Instituto de Auditores Internos (IIA), analiza cómo la adopción de IA en auditoría varía según el contexto geopolítico y cultural. En Europa, por ejemplo, se prioriza la ética y la privacidad, mientras que en EE.UU. se favorece la innovación. Se subraya la necesidad de que los auditores comprendan las dinámicas locales para aplicar modelos de auditoría adecuados, especialmente en entornos públicos donde la gobernanza algorítmica es crítica.

4. Auditoría asistida por tecnología (CAATs).

Almagrashi et al. (2023) presentan un modelo basado en la teoría UTAUT para analizar la intención de uso de técnicas de auditoría asistidas por ordenador (CAATs) en el sector público. El estudio identifica factores como la confianza, la satisfacción y la influencia organizativa como claves para la adopción de estas herramientas.
En el contexto de AAA, las CAATs permiten realizar auditorías más eficientes, especialmente en entornos con gran volumen de datos.

5. Auditoría algorítmica con estándares.

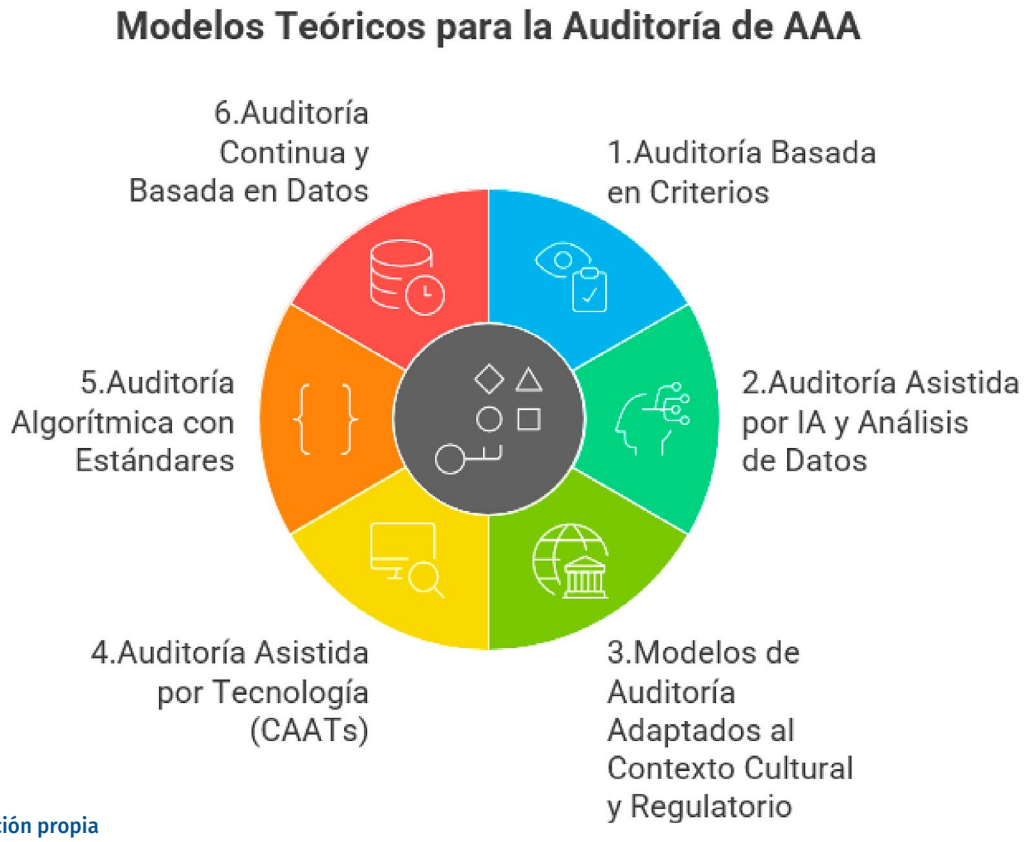
La Harvard Journal of Law & Technology propone una aproximación inspirada en la auditoría financiera para regular los sistemas de inteligencia artificial. Se destaca la necesidad de establecer estándares de auditoría algorítmica que incluyan pruebas de sesgo, validación de modelos y evaluación del impacto social.
Este enfoque sugiere que los auditores deben ser técnicamente competentes e independientes, y sus auditorías deben llevarse a cabo de acuerdo con los estándares establecidos y estar sujetas a la supervisión del gobierno. Además, es importante que los informes de auditoría deben ser accesibles tanto para expertos como para la ciudadanía.

6. Auditoría continua y basada en datos.

Bowling y Jenkins (2024) destacan el potencial de la auditoría continua mediante el uso de inteligencia artificial y análisis de datos. Este enfoque permite realizar revisiones en tiempo real, identificar riesgos emergentes y adaptar los procedimientos de auditoría a los cambios tecnológicos y organizativos.

La auditoría continua puede aplicarse a AAA mediante la integración de sistemas de monitorización, revisión automatizada de logs, y alertas sobre desviaciones normativas o técnicas.

De forma gráfica se representan los 6 modelos teóricos para auditar AAA.



Fuente: Elaboración propia

5. Propuesta metodológica.

La auditoría de Actuaciones Administrativas Automatizadas no puede concebirse como una tarea aislada ni meramente técnica. Requiere una arquitectura institucional sólida que garantice la supervisión efectiva de los sistemas automatizados, la trazabilidad de las decisiones y la protección de los derechos fundamentales. En este contexto, el papel del auditor adquiere una relevancia estratégica.

Genaro–Moya et al. (2025) analizan el impacto de la inteligencia artificial en las instituciones fiscalizadoras superiores (SAIs), destacando la necesidad de adaptar sus recursos humanos y tecnológicos para auditar sistemas automatizados. Proponen estrategias de formación, rediseño metodológico para auditar los sistemas de IA de manera efectiva y eficiente.

Por tanto, la creciente utilización de Actuaciones Administrativas Automatizadas en las Administraciones Públicas exige un modelo metodológico multidisciplinar y adaptado a la complejidad técnica y jurídica de los sistemas implicados. Dicho modelo debe permitir a los órganos de control evaluar tanto la eficiencia tecnológica como la legalidad y la ética de los sistemas.

Con base en la experiencia acumulada en auditorías de sistemas automatizados y en las propuestas recientes sobre control de AAA, se presenta un Modelo Integral de Auditoría de Sistemas Automatizados en el Sector Público (MIASA-SP), estructurado en seis fases secuenciales.

Fase 1. Análisis del sistema.

- Objetivo: identificar con precisión el tipo de actuación automatizada y su marco de referencia.
- Acciones principales: Análisis del entorno y del sistema que va a ser objeto de auditoría

a) Determinación del nivel de automatización (parcial/total; sistemas deterministas vs. sistemas no deterministas).
b) Identificación de las tecnologías implicadas (RPA, IA, machine learning, bases de datos interoperables…).
c) Análisis del marco normativo aplicable: Esquema Nacional de Seguridad (RD 311/2022), RGPD, normativa sectorial y planes de digitalización.

- Herramientas: matrices de clasificación, análisis documental, entrevistas preliminares con responsables técnicos.

Fase 2. Revisión organizativa.

- Objetivo: evaluar la gobernanza algorítmica y la estructura institucional que soporta el sistema.
- Acciones principales:

a) Análisis de responsabilidades asignadas (designación de responsables del sistema, control humano en fases críticas).
b) Revisión de la estrategia institucional de automatización y de la existencia de protocolos ante incidencias.
c) Evaluación de la cultura organizativa: grado de formación digital de los equipos, existencia de manuales y guías de uso.
d) Comprobación de la integración del sistema en la arquitectura organizativa (unidades responsables, supervisión).

- Herramientas: entrevistas semiestructuradas, revisión de organigramas, análisis de políticas internas, benchmark con buenas prácticas (ej. Unidad de Automatización Inteligente de la Junta de Andalucía).

Fase 3. Evaluación de riesgos y análisis técnico.

- Objetivo: identificar vulnerabilidades técnicas y validar la fiabilidad del sistema automatizado.
- Acciones principales:

a) Revisión de algoritmos, validaciones y fórmulas.
b) Evaluación de los datos utilizados: integridad, fiabilidad, calidad, posibles duplicidades o inconsistencias.
c) Identificación de riesgos críticos: ciberseguridad, obsolescencia, sesgo algorítmico, falta de interoperabilidad, entre otros.
d) Priorización de riesgos en función de impacto y probabilidad.
e) Análisis de las APIs de las que se obtiene información.

- Herramientas: GPF-OCEX 1315 (riesgos de incorrección material), minería de procesos (process mining), auditoría de código y parametrizaciones, pruebas de integridad de datos, análisis comparativo con estándares internacionales.

Fase 4. Revisión de controles.

- Objetivo: comprobar la existencia y eficacia de los controles establecidos.
- Acciones principales:

a) Validación de accesos: gestión de identidades, roles y permisos, bajas oportunas.
b) Revisión de backups y planes de continuidad de negocio.
c) Análisis de logs y trazabilidad de operaciones realizadas por el sistema.
d) Revisión de pruebas de funcionalidad y control interno realizadas por la entidad antes de la puesta en producción.

- Herramientas: técnicas CAATs, auditoría de logs históricos, cuestionarios de cumplimiento ENS, pruebas de recorrido (walkthrough), simulaciones de incidencias.

Fase 5. Análisis ético y jurídico.

- Objetivo: garantizar el respeto a derechos fundamentales, conductas éticas y principios de buena administración.
- Acciones principales:

a) Verificación del cumplimiento normativo (ENS, RGPD, normativa sectorial…).
b) Evaluación de transparencia, motivación de resoluciones y posibilidad de revisión administrativa.
c) Análisis del grado de explicabilidad del sistema y accesibilidad de la información para el ciudadano.
d) Comprobación de la existencia de control humano en fases críticas del proceso automatizado.
e) Identificación de sesgos o impactos discriminatorios en los resultados.

- Herramientas: metodologías de Evaluación de Impacto Algorítmico (AIA), auditoría de sesgos, listas de verificación de cumplimiento normativo, análisis de jurisprudencia y doctrina.

Fase. 6. Emisión del informe y seguimiento.

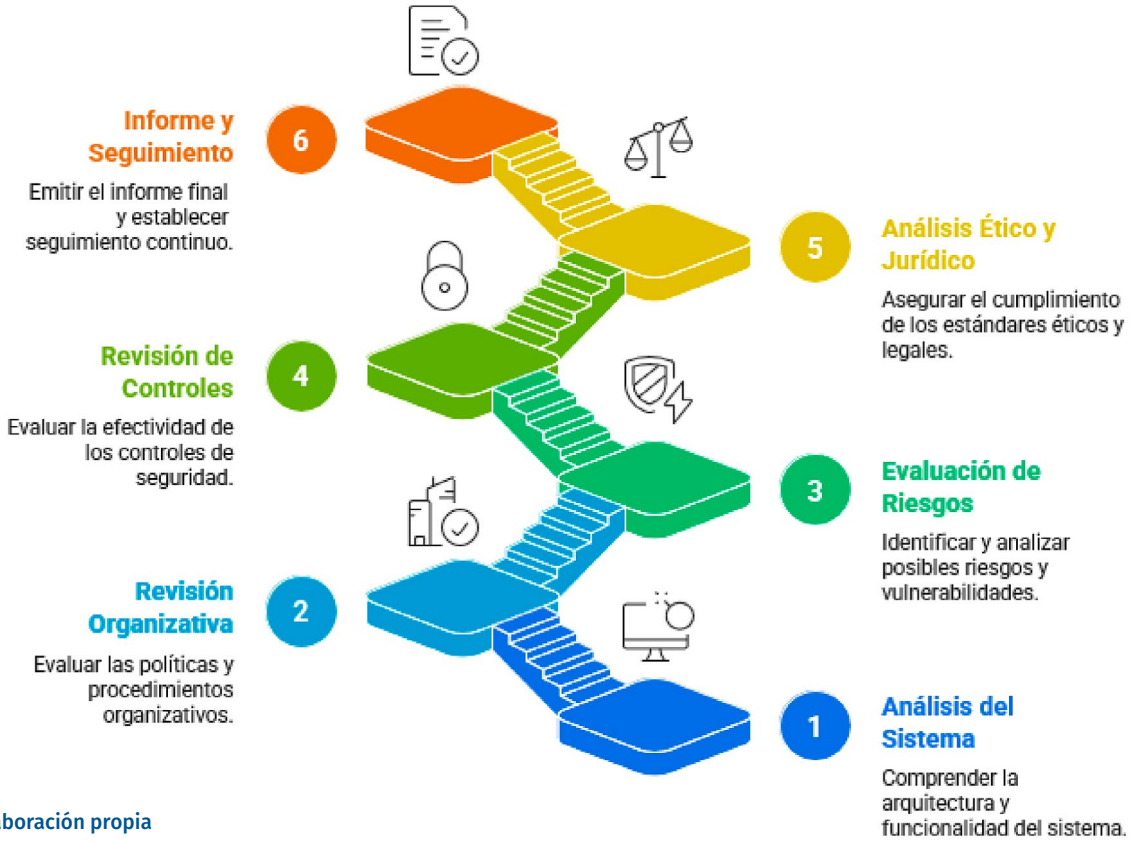
- Objetivo: consolidar los hallazgos de la auditoría en un documento claro y útil.
- Acciones principales:

a) Redacción de un informe estructurado, con hallazgos clasificados por riesgo (alto, medio, bajo).

b) Inclusión de evidencias y trazabilidad de los resultados obtenidos.
c) Formulación de recomendaciones priorizadas y propuestas de mejora.
d) Propuesta de mecanismos de auditoría continua mediante monitorización y alertas automáticas.

- Herramientas: cuadros de mando (dashboards), indicadores de desempeño (KPI), sistemas de auditoría continua, plantillas normalizadas de informes.

Fases auditoría según el modelo MIASA-SP



Fuente: Elaboración propia

El modelo propuesto MIASA-SP aporta cuatro innovaciones clave:

- Integración multidimensional, al combinar evaluación técnica, jurídica, organizativa y ética.
- Énfasis en la gobernanza algorítmica, revisando las responsabilidades institucionales, cultura organizativa y estructuras de control, entendiendo la automatización como un fenómeno no solo técnico, sino también de gestión pública.
- Orientación a la trazabilidad y transparencia, asegurando que los resultados sean comprensibles para auditores, gestores y ciudadanía.
- Carácter dinámico y preventivo, gracias a la inclusión de auditoría continua y uso de analítica avanzada para detectar riesgos emergentes.

10. Conclusiones.

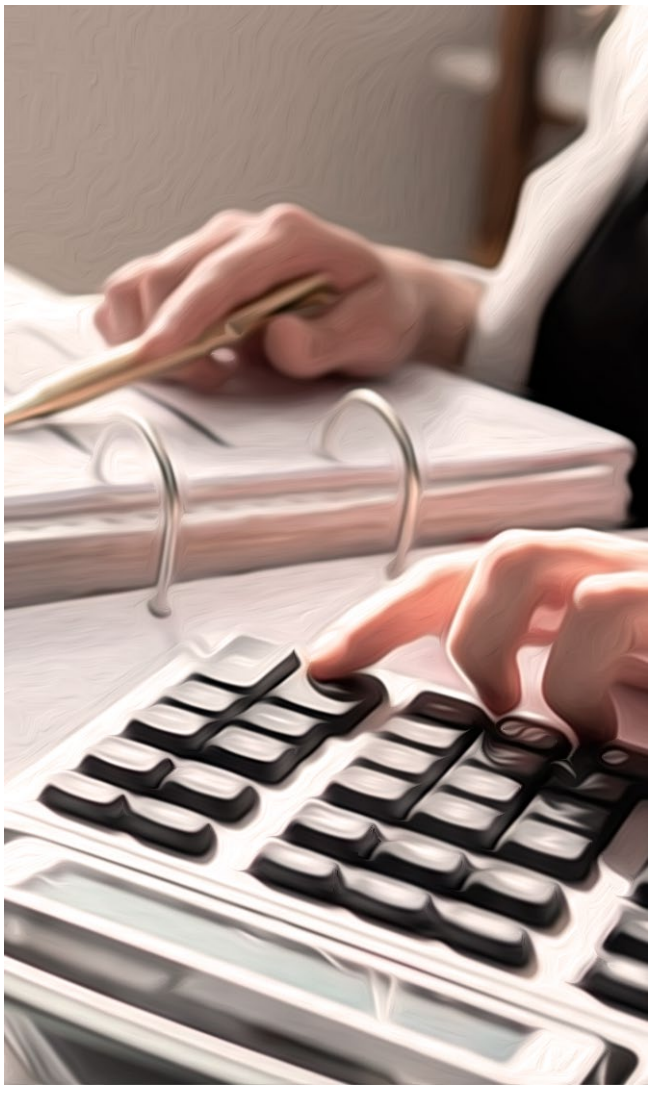
La irrupción de las Actuaciones Administrativas Automatizadas no supone únicamente un cambio tecnológico en la gestión pública, sino una transformación estructural que redefine la forma de ejercer el control y garantizar la legalidad en la Administración. Este artículo ha mostrado que la automatización obliga al auditor a incorporar competencias técnicas, jurídicas y éticas en su trabajo.

El modelo metodológico MIASA-SP constituye un marco integral capaz de abordar esa complejidad desde seis dimensiones interconectadas: análisis técnico, revisión

organizativa, evaluación de riesgos, controles, implicaciones ético–jurídicas y seguimiento continuo. Frente a modelos tradicionales, esta propuesta aporta un enfoque multidisciplinar, dinámico y orientado a la trazabilidad, lo que refuerza la confianza ciudadana en las decisiones automatizadas.

Como auditora, considero que debemos asumir un rol activo en la supervisión de sistemas automatizados, garantizando que la tecnología se utilice al servicio de la legalidad, la equidad y la transparencia. Para ello, es imprescindible contar con modelos de auditoría adaptados, formación específica y una gobernanza algorítmica sólida.

La digitalización no debe ser una amenaza, sino una oportunidad para reforzar el control público, mejorar la eficiencia administrativa y proteger los derechos de la ciudadanía.



Bibliografía.

- Almagrashi, A., Mujalli, A., Khan, T., & Attia, O. (2023). Factors determining internal auditors' behavioral intention to use computer-assisted auditing techniques: An extension of the UTAUT model and an empirical study. Future Business Journal, 9(74). https://doi.org/10.1186/s43093-023-00231-2.
- Goodman, E. P., & Tréhu, J. (2022, November 15). AI audit-washing and accountability. German Marshall Fund of the United States. https://www.gmfus.org/news/ai-audit-washing-and-accountability.
- Boix Palop, A. (2020). Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales. Vol. 1 | 2020 pp. 223-270.
- Boix Palop, A., Cotino Hueso, L. (2019). El derecho a la transparencia algorítmica en Big Data e inteligencia artificial. Revista General de Derecho Administrativo, nº50.
- Bowling, S., & Jenkins, J. G. (2024). Using technology to boost audit quality. Journal of Accountancy.
- Chicaiza Ortiz, W. (2024). La inteligencia artificial en auditoría: riesgos éticos y requisitos normativos. ECiencia, 1(3). https://doi.org/10.71022/jtl1iy06.
- Genaro-Moya, D., López-Hernández, A. M., & Godz, M. (2025). Artificial Intelligence and Public Sector Auditing: Challenges and Opportunities for Supreme Audit Institutions. World, 6(2), 78.
- Harvard Journal of Law & Technology. (2023). AI Auditing: First Steps Towards the Effective Regulation of Artificial Intelligence Systems. Harvard JOLT Digest.
- Hurtado-Guevara, R. F. (2024). Impacto de la automatización en la auditoría: ventajas y desafíos. Revista Científica Zambos, 3(3).
- KPMG. (2024). Revolutionizing internal audit: The power of AI and data analytics in audit execution. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/revolutionizing-internal-audit-power-of-ai.pdf
- Lam, K., Lange, B., Blili-Hamelin, B., Davidovic, J., Brown, S., & Hasan, A. (2024). A framework for as-

surance audits of algorithmic systems. Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24). https://doi.org/10.1145/3630106.3658957

- Michifuji, K. (2024). Audit Automation Unpacked: Types, Benefits, and Challenges. Datasnipper. https://www.datasnipper.com/resources/audit-automation-types-benefits-and-challenges

- Mir Puigpelat, O. (2023) La automatización y el uso de algoritmos e inteligencia artificial en derecho administrativo comparado. Revista General de Derecho Administrativo, ISSN-e 1696-9650, Nº 63, 2023

- Pugliese, A. (2025). Voice of the CEO: AI and internal audit—5 global trends. Internal Auditor Magazine. https://internalauditor.theiia.org/en/articles/2025/june/voice-of-the-ceo-ai-and-internal-audit-5-global-trends/

- Soriano, A. (2021). Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos. Revista de Derecho Público: Teoría y Método, 3, 85–127. Marcial Pons Ediciones Jurídicas y Sociales. Vol. 3 | 2021 pp. 85-127

- Sobrino-García, I. (2021). Artificial Intelligence Risks and Challenges in the Spanish Public Administration: An Exploratory Analysis through Expert Judgements. Administrative Sciences, 11(3), 102. https://doi.org/10.3390/admsci11030102

- Wolswinkel, J. (2022). Artificial intelligence and administrative law: Comparative study on administrative law and the use of artificial intelligence and other algorithmic systems in administrative decision-making in the member States of the Council of Europe. Committee on Legal Co-operation Council of Europe.