POLÍTICA DE INTELIGENCIA ARTIFICIAL

Versión No.01 – 28 de noviembre del 2025

TABLA DE CONTENIDO

1. RESUMEN EJECUTIVO 2
2. INTRODUCCIÓN 3
3. OBJETIVO 4
4. ALCANCE DE LA POLÍTICA 4
5. POLÍTICA DE INTELIGENCIA ARTIFICIAL 4
6. GLOSARIO 4
7. MARCO NORMATIVO 5
8. DEFINICIÓN INSTITUCIONAL DE LA INTELIGENCIA ARTIFICIAL 5
9. PRINCIPIOS RECTORES 6
10. GOBERNANZA INSTITUCIONAL DE LA IA 6
10.1 Funciones del Comité 7
10.2 Responsable del Modelo de IA 8
11. GESTIÓN DEL CICLO DE VIDA DE LA IA 8
12. USO SEGURO Y RESPONSABLE DE LA IA 8
12.1 Finalidad institucional y control humano 9
12.2 Protección de datos, transparencia y trazabilidad 9
12.3 Uso ético y controlado de herramientas tecnológicas 9
12.4 Seguridad y resiliencia técnica 9
12.5 Régimen sancionatorio interno por uso indebido de IA 9
13. GESTIÓN DE RIESGO E INCIDENTES 11
13.1 Clasificación institucional de niveles de riesgo en sistemas de Inteligencia Artificial .. 11
14. RELACIÓN CON TERCERO Y PROVEEDORES 13
15. CAPACIDADES Y TALENTO DIGITAL 13
16. INNOVACIÓN APOYADA EN LA INTELIGENCIA ARTIFICIAL PARA LA SAE 14
16.1 Cultura de Innovación para la Transformación Digital 14
16.1.1 Experimentación responsable 14
16.1.2 Aprendizaje continuo 15
16.1.3 Escalamiento progresivo 15
16.2 Cooperación Nacional e Internacional en Innovación Tecnológica 15
17. PROHIBICIONES EN EL USO DE INTELIGENCIA ARTIFICIAL 15
18. SEGUIMIENTO, CONTROL Y ACTUALIZACIÓN 16
19. ANEXOS 17
19.1 Ficha institucional de caso de uso de IA (Formato estándar SAE) 17
19.2 Modelo de evaluación de riesgo ético-técnico (aplicable a cada caso de uso) 17
20. BIBLIOGRAFÍA 18
21. CONTROL DE CAMBIOS 20
22. CONTROL DE ÚLTIMA APROBACIÓN 20

1. RESUMEN EJECUTIVO

La **Sociedad de Activos Especiales - SAE** adopta la **Política de Inteligencia Artificial** como un instrumento estratégico de gobernanza tecnológica, orientado a garantizar que toda solución o servicio basado en IA se desarrolle bajo criterios de **ética, transparencia, seguridad, responsabilidad y beneficio público.** La política consolida un marco integral que regula la adopción, uso y supervisión de la IA en los procesos institucionales, fortaleciendo la confianza ciudadana y la eficiencia en la gestión de los activos.

El documento establece una **definición institucional de IA** adaptada al contexto público, basada en la capacidad de los sistemas para analizar datos, generar conocimiento o apoyar decisiones administrativas mediante métodos automatizados. Esta definición permite un lenguaje común entre áreas técnicas, jurídicas y directivas, facilitando la alineación con los principios del **CONPES 4144 (Política Nacional de IA)** y las recomendaciones de la **OCDE,** la **UNESCO** y el **NIST AI RMF.**

La política establece que todas las responsabilidades relacionadas con la definición de directrices de IA, la aprobación de casos de uso, la supervisión de riesgos éticos, técnicos y jurídicos, así como la coordinación institucional en materia de Inteligencia Artificial, estarán a cargo del **Comité de Arquitectura Empresarial de la SAE**, dicho Comité será el órgano rector único para la toma de decisiones estratégicas en IA y garantizará que su adopción se realice dentro del marco institucional de ética, seguridad, legalidad y transformación digital.

Para el ejercicio de estas funciones, el Comité de Arquitectura Empresarial contará con la participación de representantes de la Oficina de Tecnología y Sistemas de Información, la Dirección de Planeación y Prospectiva, la Oficina Jurídica, la Dirección de Talento Humano y la Oficina de Control Interno, quienes actuarán como responsables técnicos en sus respectivas áreas y presentarán análisis, evaluaciones y recomendaciones a este Comité para la toma de decisiones.

Asimismo, la SAE adopta un enfoque de **riesgo proporcional**, que ajusta los controles y auditorías al impacto potencial de cada sistema de IA sobre los derechos, los datos o los procesos institucionales. Este enfoque se apoya en un **modelo híbrido de gestión de riesgos** que combina el marco **NIST AI RMF (2023),** la norma **ISO 31000:2018** y el **Modelo de Referencia de Arquitectura Empresarial del Estado (MRAEE),** asegurando compatibilidad con los estándares internacionales y los sistemas nacionales de control interno.

La política establece lineamientos claros sobre el **uso responsable de la IA**, incluyendo la obligación de revisión humana significativa, la protección de datos personales conforme a la **Ley 1581 de 2012**, la prohibición del uso no autorizado de plataformas públicas de IA que puedan tomar datos de la organización para entrenar modelos externos y por lo tanto se hace importante la exigencia de validación institucional para todo contenido generado. Además, incorpora un capítulo de **relación con terceros y proveedores**, que obliga a declarar el uso de IA en los productos o servicios contratados, especificando las tecnologías empleadas y los mecanismos utilizados para evitar sesgos o alucinaciones.

En materia de **cumplimiento normativo**, la política se articula con la legislación colombiana en datos, transparencia, contratación y gobierno digital, así como con los marcos internacionales de ética y derechos humanos en IA. Todo proyecto institucional de IA deberá contar con un expediente de cumplimiento, un plan de mitigación de riesgos y evidencias de auditoría.

La SAE fortalecerá el **talento digital institucional** mediante programas de formación en IA responsable, alfabetización ética y capacidades analíticas, lo cual podrá desarrollarse de manera

interna o con apoyo de terceros externos con las competencias para tal fin. Este proceso busca desarrollar competencias técnicas y estratégicas que aseguren la sostenibilidad de la transformación digital pública.

La política incorpora un sistema de **seguimiento, control y actualización anual,** con indicadores de madurez institucional y mecanismos de auditoría semestral. Sus anexos incluyen fichas de caso de uso y un modelo de evaluación de riesgo ético-técnico, garantizando trazabilidad, estandarización y mejora continua.

Con esta política, la SAE reafirma su compromiso con un proceso continuo de crecimiento, fortalecimiento institucional y adopción responsable de tecnologías emergentes. La entidad avanzará en el uso ético y seguro de la Inteligencia Artificial, apalancándose en experiencias, estándares y buenas prácticas tanto nacionales como internacionales, con el fin de contribuir al valor público, promover la transparencia administrativa y apoyar la modernización del Estado colombiano.

2. INTRODUCCIÓN

La Sociedad de Activos Especiales – SAE reconoce la Inteligencia Artificial (IA) como un habilitador estratégico para impulsar la transformación digital, fortalecer la transparencia institucional y optimizar la eficiencia en la gestión pública de activos. La IA constituye un instrumento clave para mejorar la trazabilidad de la información, acelerar la toma de decisiones basada en datos, identificar patrones de riesgo, apoyar la valoración de bienes y fortalecer los procesos misionales relacionados con la administración, disposición y recuperación de activos. Su incorporación progresiva permite modernizar los procesos operativos, reducir cargas administrativas, mejorar la prestación de servicios al ciudadano y promover una gestión más preventiva e inteligente del portafolio estatal. En este sentido, la SAE asume el compromiso de desarrollar y utilizar sistemas de IA de manera ética, segura y responsable, asegurando que su integración contribuya al interés público, al fortalecimiento del gobierno corporativo y a la sostenibilidad institucional en el largo plazo.

En un contexto donde la tecnología redefine la toma de decisiones, la IA ofrece herramientas para mejorar la trazabilidad, la valoración, la administración y la recuperación de activos, contribuyendo al cumplimiento de la misión institucional y a la confianza ciudadana.

Esta política establece el marco institucional que orienta el desarrollo, adopción y uso responsable de sistemas basados en IA en la SAE, garantizando su alineación con los principios éticos, legales y técnicos definidos por el Estado colombiano. Busca asegurar que cada iniciativa de IA maximice el valor público, respete los derechos fundamentales y mantenga la transparencia y la rendición de cuentas.

Su alcance cubre todos los proyectos, procesos y servicios donde se empleen tecnologías de IA, incluidas las de tipo predictivo, generativo, automatizado o analítico, tanto de desarrollo interno como mediante proveedores externos.

Esta política se desarrolla mediante una estructura integral que inicia con un resumen ejecutivo e introducción que contextualizan el propósito institucional del documento, seguido del objetivo y el alcance que delimitan su aplicación; posteriormente, avanza hacia la formulación de la política como marco orientador, apoyada por un glosario y un marco normativo que recoge las disposiciones nacionales relevantes, así como una definición institucional de la IA y los principios rectores que guían su adopción ética y transparente. La política establece un sistema de gobernanza institucional con un Comité de Arquitectura Empresarial y funciones claramente definidas, incorpora la gestión del ciclo de vida de las soluciones tecnológicas y detalla lineamientos para su uso seguro y responsable, incluyendo control humano, protección de datos, transparencia, trazabilidad y autorización de herramientas. A su

vez, contempla la gestión del riesgo y los incidentes, los criterios para la relación con terceros y proveedores, y las acciones para fortalecer las capacidades y el talento digital interno. El documento también desarrolla una estrategia de innovación apoyada en IA que abarca cultura de transformación digital, experimentación responsable, aprendizaje continuo, escalamiento progresivo y cooperación nacional e internacional. Finalmente, incluye mecanismos de seguimiento, control y actualización de la política, anexos con formatos y modelos de evaluación.

3. OBJETIVO

Establecer los lineamientos, principios, roles y directrices estratégicas para el diseño, adopción, uso, supervisión y control de soluciones basadas en inteligencia artificial en la SAE, garantizando su implementación ética, segura y transparente, en armonía con la Política de Gobierno Digital, la Transformación Digital del Estado y la Política Nacional de Inteligencia Artificial (CONPES 4144 de 2021).

4. ALCANCE DE LA POLÍTICA

El alcance de esta política comprende el diseño, implementación, gestión y evaluación de las capacidades de IA en toda la entidad y buscando su articulación con los procesos estratégicos, misionales, de soporte y de seguimiento y evaluación a los que haya lugar y puedan ser permeados o apoyados por la IA, las dependencias y funcionarios de la SAE tanto a nivel central como en las Direcciones Territoriales, así como para los contratistas, proveedores, aliados tecnológicos o terceros que desarrollen, implementen, administren o utilicen soluciones tecnológicas basadas en inteligencia artificial en el marco de las funciones y responsabilidades de la Entidad.

5. POLÍTICA DE INTELIGENCIA ARTIFICIAL

La Sociedad de Activos Especiales - SAE conforme a su misión se compromete con sus grupos de valor e interés a garantizar que el desarrollo, adopción y uso de sistemas de Inteligencia Artificial se realicen dentro de un marco de **legalidad, ética y transparencia,** cumpliendo las disposiciones nacionales que regulan la materia. Esta política se articula con los lineamientos del **Documento CONPES 4144 de 2025 – Política Nacional de Inteligencia Artificial,** que promueve el desarrollo ético, responsable y sostenible de la IA, y con el **Decreto 1263 de 2022**, que establece la estructura del **Gobierno Digital y la Gobernanza de Datos en el Estado colombiano.**

6. GLOSARIO

- **Inteligencia Artificial (IA):** Sistema computacional que realiza tareas que tradicionalmente requieren inteligencia humana, como el razonamiento, el aprendizaje, la predicción o la toma de decisiones. Puede incluir modelos predictivos, algoritmos de aprendizaje automático y sistemas generativos.

- **Gobernanza de IA:** Conjunto de estructuras, políticas y procesos que aseguran que el uso de la IA se realice de manera ética, transparente, trazable y alineada con los objetivos institucionales.

- **Riesgo proporcional:** Principio según el cual las medidas de control, supervisión y auditoría deben ser acordes al nivel de riesgo del sistema de IA, considerando su impacto sobre las personas, los datos o las decisiones.

- **Explicabilidad:** Capacidad de un sistema de inteligencia artificial para proporcionar información clara, comprensible y verificable sobre los factores, datos y procesos que influyen en sus resultados. La explicabilidad permite entender por qué el modelo tomó una decisión o generó una salida, y es esencial para la transparencia, la rendición de cuentas y la supervisión humana efectiva.

- **Sesgo algorítmico:** Tendencia sistemática de un sistema de IA a generar resultados injustos o discriminatorios debido a datos, parámetros o diseños inadecuados.

- **Alucinación (IA generativa):** Resultado falso, engañoso o inventado producido por un modelo de IA generativa, sin fundamento real en los datos de entrenamiento.

- **Caso de uso de IA:** Aplicación específica de IA dentro de un proceso institucional, documentada con su objetivo, alcance, responsable, riesgos y mecanismos de control.

- **Inventario institucional de IA:** Registro oficial que consolida todos los proyectos, sistemas o servicios de IA utilizados o planificados por la SAE.

- **Expediente de cumplimiento:** Conjunto documental que evidencia la conformidad de un caso de uso de IA con las normas legales, los principios éticos y los controles técnicos establecidos por la SAE.

7. MARCO NORMATIVO

En el ámbito nacional, los proyectos de IA deberán observar las siguientes normas:

- **Ley 1581 de 2012** y sus decretos reglamentarios sobre protección de datos personales, garantizando la seguridad, confidencialidad y consentimiento informado en el tratamiento de la información.
- **CONPES 4144 Política Nacional de Inteligencia Artificial** su objetivo general es “Generar las capacidades para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA con el fin de impulsar la transformación social y económica de Colombia a 2030.
- **Ley 1712 de 2014** sobre transparencia y acceso a la información pública, asegurando la trazabilidad de las decisiones automatizadas.
- **Ley 1341 de 2009** y **Decreto 1078 de 2015**, que regulan el uso responsable de tecnologías de información en entidades del Estado.
- **Modelo Integrado de Planeación y Gestión (MIPG)**, como marco para la articulación de la IA con los procesos de mejora institucional y rendición de cuentas.
- **Directrices del MinTIC sobre seguridad digital y ética en IA**, en coherencia con la Política de Gobierno Digital.

8. DEFINICIÓN INSTITUCIONAL DE LA INTELIGENCIA ARTIFICIAL

La SAE adopta la definición de IA que el CONPES 4144 de 2025 identifica como el conjunto de sistemas tecnológicos capaces de ejecutar tareas que, si fueran realizadas por humanos, requerirían inteligencia, tales como el razonamiento, el aprendizaje, la percepción, la planificación y la interacción lingüística (CONPES 4144, 2025; OCDE, 2019) y abarca los siguientes tipos de IA aplicables al contexto institucional:

- **IA Analítica:** Orientada a la interpretación avanzada de datos para soporte a decisiones sobre

administración y valoración de activos.

- **IA Predictiva:** Usada para estimar comportamientos de mercado, riesgo financiero, o posibles fraudes en procesos de enajenación.
- **IA Automatizada:** Aplicada en la optimización de flujos de trabajo administrativos y jurídicos repetitivos.
- **IA Generativa:** Enfocada en la producción de contenidos o modelos que faciliten la comunicación y la documentación interna.

Toda iniciativa de IA deberá ser documentada y registrada dentro del **Inventario Institucional de Casos de Uso de IA**, administrado por la Dirección de Planeación y Prospectiva de la SAE.

9. PRINCIPIOS RECTORES

El desarrollo y uso de la IA en la SAE se regirá por los siguientes principios:

Nº	Principio ético	Descripción
1	Ética y beneficio público	Cada sistema deberá contribuir al interés general, evitando sesgos, discriminación o impactos adversos sobre la ciudadanía.
2	Transparencia y explicabilidad	Los modelos deben permitir rastrear decisiones y comprender sus fundamentos.
3	Responsabilidad y rendición de cuentas	La SAE y sus funcionarios deben asumir de manera explícita el compromiso de garantizar que los sistemas de Inteligencia Artificial (IA) operen de forma segura, legal, transparente y conforme al interés público. Toda decisión automatizada debe tener siempre un responsable humano claramente identificado, que pueda supervisar, validar y responder por el funcionamiento, los resultados y los impactos del sistema.
4	Privacidad y seguridad	Los datos utilizados deberán cumplir la Ley 1581 de 2012 y las políticas institucionales de seguridad de la información.
5	Equidad e inclusión	La IA debe promover el acceso equitativo a la información y oportunidades, considerando diversidad territorial y social.
6	Sostenibilidad y eficiencia	La adopción tecnológica debe optimizar recursos y generar valor institucional.
7	Seguridad y resiliencia técnica	Los sistemas de Inteligencia Artificial deberán operar con niveles adecuados de robustez, confiabilidad y resistencia frente a fallos, vulnerabilidades y ataques. Cada solución deberá contar con controles técnicos, pruebas de funcionamiento, mecanismos de monitoreo y procedimientos de respuesta que permitan prevenir usos malintencionados, manipulaciones o alteraciones que comprometan su integridad. La SAE garantizará que toda tecnología basada en IA funcione en entornos protegidos, con trazabilidad completa, controles de acceso, revisión continua y medidas de defensa que aseguren su estabilidad operativa durante todo el ciclo de vida del sistema.

10. GOBERNANZA INSTITUCIONAL DE LA IA

La SAE implementará un **Modelo de Gobernanza de IA** articulado con su Política de Gobierno Digital y de Datos.

Se vinculará al Comité de Arquitectura Empresarial, el cual será el responsable de definir lineamientos, aprobar casos de uso y supervisar el cumplimiento ético y normativo.

Dependencia	Rol dentro del Comité de Arquitectura Empresarial	Justificación
Presidencia de la organización	Presidencia del Comité	Garantiza liderazgo estratégico, alineación con la visión institucional y aprobación de políticas y prioridades en materia de IA.
Dirección de Planeación y Prospectiva	Secretaría Técnica del Comité	Coordina la implementación de la política, seguimiento de casos de uso y articulación con el Plan Estratégico de Transformación Digital & IA.
Oficina de Tecnologías y Sistemas de Información	Gestión técnica y arquitectónica	Define estándares tecnológicos, infraestructura, interoperabilidad y seguridad digital de los proyectos de IA.
Oficina de Control Interno	Control, evaluación y auditoría	Supervisa el cumplimiento normativo y ético, y verifica la trazabilidad de decisiones automatizadas.
Oficina Jurídica	Cumplimiento normativo y ético	Evalúa la conformidad legal, derechos de datos personales, propiedad intelectual y uso ético de la IA.
Oficina de Prensa y Comunicaciones	Transparencia y comunicación pública	Asegura la comunicación responsable sobre el uso de IA y la publicación de información al ciudadano.
Dirección de Talento Humano	Gestión de capacidades y formación	Desarrolla los programas de alfabetización digital y ética en IA para los funcionarios.
Vicepresidencia Operativa Vicepresidencia Corporativa Vicepresidencia de Sociedades Vicepresidencia de Muebles e Inmuebles	Casos de uso prioritarios de IA	Representan áreas donde la IA puede aportar más valor (automatización, analítica predictiva, trazabilidad).

10.1 Funciones del Comité

N.º	Función del Comité de Arquitectura Empresaial relacionados con IA
1. Definir lineamientos estratégicos de IA	Establecer los criterios técnicos, éticos y de priorización para el desarrollo, adopción y uso de la IA en la SAE, garantizando coherencia con el CONPES 4144 y la Política de Gobierno Digital.
2. Supervisar el ciclo de vida de los sistemas de IA	Asegurar que los proyectos cumplan las etapas de identificación, diseño, entrenamiento, validación, implementación, monitoreo y retiro, con revisiones éticas, legales y técnicas documentadas.
3. Evaluar impactos y riesgos de IA	Revisar las evaluaciones de impacto ético, social, operativo y reputacional de cada iniciativa de IA, recomendando medidas de mitigación o suspensión según el nivel de riesgo.
4. Garantizar el cumplimiento normativo y ético	Verificar la observancia de la Ley 1581 de 2012, el Decreto 1263 de 2022 y otros marcos aplicables, incluyendo la protección de datos, la transparencia algorítmica y la rendición de cuentas.

N.º	Función del Comité de Arquitectura Empresaial relacionados con IA
5. Aprobar y registrar los casos de uso institucionales	Autorizar formalmente los proyectos de IA, consolidando un inventario único de casos de uso con sus responsables, proveedores y resultados de revisión técnica y ética.
6. Coordinar la formación y sensibilización institucional	Diseñar junto con la Dirección de Talento Humano programas de alfabetización digital, ética y competencias en IA para directivos y servidores, fomentando el uso responsable y seguro.
7. Articular la relación con terceros y proveedores	Definir criterios técnicos y contractuales para la adquisición de soluciones de IA, incluyendo cláusulas de gobernanza, explicabilidad, cesión de derechos y confidencialidad.
8. Monitorear y reportar la madurez institucional en IA	Elaborar informes semestrales sobre avances, cumplimiento, incidentes y lecciones aprendidas, integrándolos al Comité de Arquitectura Empresarial y al Sistema de Control Interno.

10.2 Responsable del Modelo de IA

Para cada sistema, algoritmo o caso de uso de Inteligencia Artificial implementado en la SAE deberá designarse un Responsable del Modelo. Esta persona será la encargada de supervisar el funcionamiento, vigilar el cumplimiento normativo y ético, garantizar la calidad de los datos utilizados y responder ante auditorías internas y externas por el desempeño del modelo. El Responsable del Modelo velará por que la solución cuente con trazabilidad completa, evidencias de entrenamiento y validación, pruebas de sesgo, mecanismos de supervisión humana y controles de seguridad. Además, deberá asegurar el registro actualizado del caso de uso en el inventario institucional de IA y reportar incidentes, desviaciones o fallas al Comité de Arquitectura Empresarial. Su designación será obligatoria desde la fase de diseño del sistema y se mantendrá durante todo el ciclo de vida del modelo.

11. GESTIÓN DEL CICLO DE VIDA DE LA IA

Todo sistema de IA deberá gestionarse según su ciclo de vida:

1. **Identificación del caso de uso:** justificación técnica y social.
2. **Diseño y desarrollo:** definición de objetivos, fuentes de datos y criterios éticos.
3. **Entrenamiento y validación:** evaluación de sesgos, precisión y explicabilidad.
4. **Implementación controlada:** revisión de seguridad, legalidad y gobernanza.
5. **Monitoreo continuo:** métricas de desempeño, auditorías y retroalimentación.
6. **Retiro o reemplazo:** evaluación de obsolescencia y resguardo de datos.

Cada fase contará con revisiones documentadas en el **Registro Institucional de Proyectos de IA**, y los resultados se reportarán al Comité CIG-IA.

12. USO SEGURO Y RESPONSABLE DE LA IA

El uso responsable de la Inteligencia Artificial en la Sociedad de Activos Especiales - SAE constituye un pilar esencial para garantizar que toda solución tecnológica opere bajo estándares éticos, legales y técnicos que salvaguarden los derechos de las personas y la integridad institucional.

La SAE adopta un enfoque de **riesgo proporcional**[1] en la aplicación de la IA, diferenciando entre usos de bajo impacto y aquellos con implicaciones críticas en la gestión de activos o en la toma de decisiones públicas.

Los sistemas de IA utilizados por la entidad deberán cumplir con los siguientes lineamientos:

12.1 Finalidad institucional y control humano

Todo caso de uso de IA deberá responder a un objetivo legítimo y documentado que aporte eficiencia, trazabilidad o transparencia, garantizando siempre la supervisión humana significativa en decisiones que afecten derechos, valores económicos o información sensible.

12.2 Protección de datos, transparencia y trazabilidad

El tratamiento de la información utilizada por los sistemas de IA deberá cumplir la Ley 1581 de 2012 y ser completamente auditable, de modo que cada acción automatizada sea explicable y revisable por instancias de control interno o externo.

12.3 Uso ético y controlado de herramientas tecnológicas

Se prohíbe el uso no autorizado de plataformas públicas de IA con información institucional. Todo contenido o resultado generado deberá ser validado por un funcionario responsable antes de su publicación o aplicación oficial.

12.4 Seguridad y resiliencia técnica

Los sistemas de Inteligencia Artificial deberán diseñarse, implementarse y operarse garantizando altos niveles de confiabilidad, robustez y resistencia frente a fallos, vulnerabilidades y ataques. Esto implica contar con controles que prevengan usos indebidos, manipulaciones malintencionadas, alteraciones del modelo, inyecciones de datos o cualquier actividad que pueda comprometer la integridad del sistema o afectar la toma de decisiones institucionales. La SAE deberá asegurar que cada solución de IA cuente con mecanismos de protección técnica, verificación continua, pruebas de estrés, supervisión operativa y planes de respuesta ante incidentes, de modo que la tecnología se mantenga estable y segura durante todo su ciclo de vida. Además, cada sistema deberá operar bajo criterios de defensa en profundidad, incluyendo controles de acceso, trazabilidad completa, monitoreo permanente y auditorías técnicas que permitan anticipar y mitigar riesgos, garantizando que la IA funcione dentro de los parámetros de seguridad establecidos por la entidad y por los marcos normativos aplicables.

12.5 Régimen sancionatorio interno por uso indebido de IA

La SAE establecerá un régimen sancionatorio interno aplicable a trabajadores, contratistas y terceros que utilicen tecnologías de Inteligencia Artificial de forma contraria a los lineamientos definidos en esta política. Será considerado uso indebido cualquier acción que implique manipulación no autorizada de modelos, divulgación de información institucional en plataformas externas, uso de IA sin validación oficial, alteración de resultados, omisión deliberada de controles o cualquier conducta que comprometa la seguridad, integridad o legalidad del sistema. Estas conductas podrán dar lugar a la aplicación de medidas disciplinarias conforme al régimen aplicable a os trabajadores de la SAE, así como sanciones contractuales cuando se trate de proveedores o contratistas. La Entidad documentará los incidentes, realizará las investigaciones correspondientes y remitirá los casos a las

[1] El **riesgo proporcional** es un principio de gobernanza que establece que las medidas de control, supervisión y evaluación aplicadas a un sistema de Inteligencia Artificial deben corresponder a la magnitud del impacto potencial que dicho sistema puede generar sobre las personas, los procesos institucionales o los derechos fundamentales. En la práctica, implica que los proyectos de IA con bajo impacto operativo reciben controles ligeros orientados a la eficiencia, mientras que los de alto impacto —por ejemplo, los que inciden en decisiones económicas, jurídicas o sociales— requieren mayores niveles de revisión ética, validación humana y auditoría técnica, garantizando así un equilibrio entre innovación y responsabilidad.

instancias competentes para garantizar la transparencia, la responsabilidad y la protección institucional frente al uso inadecuado de IA.

Las sanciones se clasifican según la gravedad del uso indebido de IA, buscando asegurar proporcionalidad, trazabilidad y mecanismos de responsabilidad institucional.

1. **Amonestación escrita**

   Aplicable cuando se evidencien fallas menores, como incumplimientos leves de los procedimientos definidos para el uso de herramientas de IA, siempre que no generen impacto en datos, procesos o decisiones institucionales. La amonestación incluirá orientación para la corrección de la conducta y registro en el historial del funcionario o contratista.

2. **Suspensión temporal del acceso a herramientas tecnológicas**

   Procede frente a usos inadecuados que, sin causar daño grave, evidencian negligencia, desconocimiento de las políticas o repetición de conductas previamente advertidas. Incluye suspensión de accesos a plataformas, modelos o sistemas de IA hasta completar un proceso obligatorio de capacitación en uso seguro y responsable.

3. **Reporte a la Dirección de Talento Humano, GIT de Asuntos Internos Disciplinarios y apertura de indagación preliminar**

   Se aplica en casos donde el uso indebido pueda comprometer trazabilidad, transparencia o integridad de los datos institucionales. El hecho será trasladado para investigación interna y seguimiento documental, con el fin de determinar responsabilidades y medidas adicionales.

4. **Remoción de responsabilidades en proyectos de IA**

   Procede cuando el funcionario o contratista incumpla las obligaciones del rol asignado, especialmente las del Responsable del Modelo, o cuando se identifique comportamiento que comprometa la seguridad del sistema. Implica reasignación de funciones y pérdida de autorización para manipular modelos o participar en proyectos de IA durante un periodo determinado.

5. **Suspensión temporal de actividades contractuales**

   En el caso de contratistas o proveedores, podrá aplicarse suspensión parcial o total de sus actividades cuando exista incumplimiento contractual en el uso de IA, incluyendo la manipulación indebida de modelos, el uso no autorizado de datos institucionales o la transferencia de información a plataformas externas.

6. **Sanciones disciplinarias conforme al régimen aplicable**

   Cuando la conducta de un empleado configure una falta disciplinaria, la SAE procederá conforme a su reglamento interno y remitir el caso a la autoridad competente para su respectivo trámite, de acuerdo con lo establecido en el Código Sustantivo del Trabajo y las normativas aplicables del régimen privado. Las sanciones que podrán aplicarse incluyen, según la gravedad del incumplimiento, amonestaciones, multas, suspensión temporal del cargo o incluso la terminación del contrato de trabajo.

7. **Sanciones contractuales y terminación anticipada del contrato**

   Si la conducta corresponde a un proveedor, contratista o tercero y afecta confidencialidad, seguridad o integridad institucional, la SAE podrá aplicar multas contractuales, declarar

incumplimiento, hacer efectiva la cláusula penal o proceder con la terminación anticipada del contrato cuando corresponda.

8. **Reporte a autoridades externas**

   En casos que involucren posibles vulneraciones de datos personales, delitos informáticos o afectaciones a la seguridad digital, la SAE reportará el incidente a las autoridades competentes como la SIC o la Fiscalía General de la Nación, según corresponda.

13. GESTIÓN DE RIESGO E INCIDENTES[2]

La gestión de riesgos e incidentes en la Sociedad de Activos Especiales - SAE busca anticipar, prevenir y mitigar los impactos negativos derivados del uso de la Inteligencia Artificial. Todo proyecto deberá ser evaluado desde su diseño considerando riesgos éticos, legales, técnicos y reputacionales, tales como el tratamiento de datos personales, los sesgos algorítmicos o las vulnerabilidades de ciberseguridad. Para ello, se aplicará el principio de riesgo proporcional, ajustando los niveles de control y supervisión según el impacto potencial de cada caso de uso.

Cada iniciativa de IA deberá clasificarse como de bajo, medio o alto riesgo, según su alcance y efecto en los procesos institucionales. Los proyectos de alto riesgo requerirán aprobación formal del Comité de Arquitectura Empresarial antes de su implementación. Además, cada responsable deberá definir medidas preventivas y correctivas, incluyendo revisiones humanas, auditorías técnicas y validaciones normativas que garanticen cumplimiento con la Ley 1581 de 2012, el Decreto 1263 de 2022 y las directrices del CONPES 4144 de 2025.

Cuando ocurra un incidente, desviación o falla, el hecho deberá reportarse de inmediato a la Oficina de Tecnologías de Información y al Comité de Arquitectura Empresarial, quienes activarán los protocolos de respuesta establecidos. Estas acciones podrán incluir análisis de causa raíz, suspensión temporal del sistema, corrección de sesgos y comunicación a los órganos de control interno. Los aprendizajes obtenidos de cada evento serán documentados para fortalecer la mejora continua, consolidando una cultura institucional de **uso seguro, transparente y responsable de la IA.**

13.1 Clasificación institucional de niveles de riesgo en sistemas de Inteligencia Artificial

La clasificación institucional de riesgos asociados al uso de sistemas de Inteligencia Artificial permite establecer un marco uniforme para determinar el nivel de supervisión, control y responsabilidad requerido en cada caso de uso. Con base en el marco normativo colombiano y en estándares internacionales como la OCDE, UNESCO, NIST y el AI Act,, la SAE adopta cuatro categorías diferenciadas de riesgo que orientan la toma de decisiones y la implementación de medidas técnicas, éticas y jurídicas proporcionales al impacto potencial de cada sistema. La siguiente tabla presenta las definiciones, ejemplos y obligaciones aplicables para cada nivel de riesgo.

[2] El modelo híbrido de gestión de riesgos en Inteligencia Artificial propuesto para la SAE combina los principios del NIST AI Risk Management Framework (2023) y el Modelo de Referencia de Arquitectura Empresarial del Estado (MRAEE). Este enfoque integrador permite identificar, evaluar y mitigar riesgos éticos, legales, técnicos y operativos en cada fase del ciclo de vida de la IA. El NIST aporta la estructura específica para gobernar, mapear, medir y gestionar riesgos algorítmicos; la ISO 31000 brinda el marco organizacional para tratarlos dentro del sistema institucional de control interno; y el MRAEE garantiza su alineación con la política pública digital, asegurando interoperabilidad, trazabilidad y ética en el uso responsable de la IA.

N.º	Categoría de riesgo	Descripción	Ejemplos típicos	Acciones y controles requeridos
1	Riesgo prohibido	Corresponde a sistemas o prácticas de IA que representan una amenaza grave para los derechos fundamentales, la dignidad humana, la seguridad pública o la integridad institucional. Estas aplicaciones están prohibidas por marcos como la OCDE, UNESCO, NIST y el AI Act europeo, y no pueden ser desarrolladas, contratadas ni utilizadas en la SAE.	Manipulación subliminal o coercitiva. Vigilancia biométrica masiva en tiempo real sin habilitación legal. Sistemas de análisis emocional para decisiones públicas. Clasificación de personas basada en características sensibles. Uso de IA que afecte irreversiblemente derechos individuales o colectivos.	Prohibición absoluta. Documentar la identificación del riesgo. Reportar al Comité de Arquitectura Empresarial Registrar en el inventario institucional. Activar medidas internas para evitar su desarrollo, contratación o despliegue.
2	Riesgo alto	Comprende sistemas que pueden generar impactos significativos sobre derechos, decisiones administrativas, recursos públicos o datos sensibles. Requieren controles estrictos, evaluación técnica y jurídica y supervisión humana significativa. Están regulados conforme al CONPES 4144, el AI Act y el NIST AI RMF.	Modelos utilizados para valoración de activos. Analítica de riesgo con impacto en decisiones administrativas. Sistemas de clasificación de casos jurídicos o financieros. Modelos que operan con datos sensibles permitidos por ley. Automatización parcial de procesos misionales.	Evaluación de impacto ético y técnico. Aprobación previa del Comité. Pruebas de sesgos y robustez. Trazabilidad completa. Verificaciones de explicabilidad. Auditorías periódicas. Supervisión humana obligatoria y validación de resultados antes de decisiones.
3	Riesgo limitado	Incluye sistemas que interactúan con usuarios o funcionarios pero que no influyen en decisiones críticas. Requieren obligaciones de transparencia, trazabilidad funcional y controles moderados.	Chatbots institucionales sin capacidad de decisión. Sistemas generativos para apoyo documental. Herramientas de recomendación sin efecto directo en actos administrativos. Analítica descriptiva sin automatización de decisiones.	Informar al usuario que interactúa con IA. Mantener trazabilidad operativa. Validar contenido generado antes de uso oficial. Supervisión moderada y controles básicos de calidad. Registro cuando aplique.
4	Riesgo mínimo	Aplicaciones de IA de bajo impacto que cumplen funciones administrativas, educativas u operativas rutinarias. No afectan derechos, decisiones ni datos sensibles. Su uso está permitido con controles	Búsquedas inteligentes. Organización preliminar de documentos. Optimización de recursos internos. Análisis descriptivo con datos no sensibles.	Aplicar lineamientos generales de seguridad digital. Realizar pruebas internas básicas. Supervisión proporcional al riesgo.

N.º	Categoría de riesgo	Descripción	Ejemplos típicos	Acciones y controles requeridos
		básicos y monitoreo proporcional.		Registro institucional si corresponde. Validación interna mínima.

14. RELACIÓN CON TERCERO Y PROVEEDORES

La Sociedad de Activos Especiales - SAE reconoce que gran parte del desarrollo y uso de tecnologías de Inteligencia Artificial involucra la participación de terceros, proveedores, contratistas, aliados tecnológicos o consultores, por lo cual establece una política de **responsabilidad compartida y control ético-tecnológico** frente a los sistemas de IA adquiridos o implementados mediante contratación pública o alianzas estratégicas.

Todo proveedor de servicios, plataformas o modelos de IA deberá demostrar **cumplimiento normativo, técnico y ético**, garantizando la protección de datos personales, la explicabilidad de los algoritmos, la trazabilidad de las decisiones y la seguridad de la información institucional. En los procesos contractuales, la SAE incorporará cláusulas específicas que incluyan:

- **Transparencia algorítmica y acceso a documentación técnica**, asegurando que los sistemas contratados permitan auditorías internas o externas.
- **Cumplimiento con los principios de ética y gobernanza de IA**, definidos por el CONPES 4144 y el Comité Institucional de Gobernanza de IA.
- **Garantías de confidencialidad y propiedad de los datos**, prohibiendo el uso de información institucional para fines distintos al contrato.
- **Derecho a auditoría y revisión de desempeño**, habilitando la verificación periódica del comportamiento de los modelos y su alineación con los objetivos públicos.

Toda relación con terceros deberá documentarse en el **Registro Institucional de Proveedores de IA,** donde se consignarán los contratos, las evaluaciones de cumplimiento, los informes de desempeño y las auditorías efectuadas. Con ello, la SAE garantiza un ecosistema de inteligencia artificial **transparente, confiable y alineado con el interés público**, fortaleciendo la rendición de cuentas y la confianza ciudadana.

Adicionalmente, todo proveedor o contratista deberá **declarar expresamente si utiliza herramientas de Inteligencia Artificial en la ejecución, diseño o entrega de productos o servicios contratados.** En caso afirmativo, deberá informar qué modelos, plataformas o sistemas fueron empleados, su finalidad y los mecanismos implementados para **prevenir sesgos, alucinaciones o resultados engañosos**. Esta declaración formará parte del expediente contractual y será evaluada por el Comité Institucional de Gobernanza de IA, con el fin de garantizar que la tecnología aplicada sea ética, verificable y coherente con los estándares de calidad y transparencia exigidos por la entidad.

15. CAPACIDADES Y TALENTO DIGITAL

El fortalecimiento del talento humano es un componente esencial para garantizar la adopción ética, segura y sostenible de la Inteligencia Artificial (IA) en la Sociedad de Activos Especiales (SAE). La entidad promoverá una **cultura institucional de innovación digital responsable**, en la cual los servidores públicos comprendan el alcance, los riesgos y las oportunidades que la IA ofrece en la gestión de activos, la analítica de datos y la optimización de procesos administrativos.

La SAE impulsará un **Programa de Formación y Alfabetización en IA responsable**, articulado con el **Comité de Arquitectura Empresarial** y la **Dirección de Talento Humano,** enfocado en tres niveles de desarrollo:

1. **Sensibilización general:** dirigida a todos los funcionarios, con el objetivo de fomentar la comprensión básica sobre el funcionamiento de la IA, sus implicaciones éticas y su relación con la transparencia institucional.
2. **Capacitación técnica especializada:** orientada a toda la entidad, abordando temas como el diseño de modelos, la gestión de datos, la mitigación de sesgos, la ciberseguridad y la trazabilidad algorítmica.
3. **Formación estratégica y ética directiva:** destinada a mandos medios y altos directivos, enfocada en la toma de decisiones basadas en IA, la gobernanza tecnológica y el uso de herramientas de análisis predictivo para la planeación institucional.

16. INNOVACIÓN APOYADA EN LA INTELIGENCIA ARTIFICIAL PARA LA SAE

La Sociedad de Activos Especiales, SAE concibe la innovación como un pilar fundamental para fortalecer su capacidad institucional, modernizar sus procesos misionales y consolidar un modelo de gestión de activos basado en analítica avanzada, automatización y toma de decisiones informadas. En este contexto, la Inteligencia Artificial (IA) se reconoce como un catalizador estratégico que permite transformar la manera en que la entidad administra, protege, valora y dispone los activos a su cargo.

La incorporación progresiva de tecnologías de IA abre oportunidades para diseñar soluciones más eficientes, transparentes y centradas en el valor público, favoreciendo una gestión estatal más ágil, preventiva y orientada al servicio.

La innovación apoyada en IA implica adoptar nuevas metodologías, herramientas y modelos organizacionales que faciliten la experimentación controlada, la validación técnica y la escalabilidad de iniciativas institucionales. Este enfoque incluye capacidades como automatización inteligente de procesos, analítica predictiva, sistemas de alerta temprana, modelos de clasificación para apoyo a decisiones, motores generativos de documentación y soluciones de auditoría avanzada. Estas tecnologías no solo fortalecen la eficiencia operativa de la SAE, sino que permiten anticipar riesgos, detectar oportunidades de mejora y elevar la trazabilidad en todo el ciclo de vida de los activos especiales del Estado.

16.1 Cultura de Innovación para la Transformación Digital

Para garantizar un proceso de innovación institucional coherente y sostenible, la SAE promoverá un modelo de cultura innovadora basado en tres ejes: **(i)** experimentación responsable, donde los pilotos de IA se desarrollen bajo criterios de seguridad, ética y legalidad; **(ii)** aprendizaje continuo, mediante el análisis de resultados, retroalimentación interdependencias y ajustes iterativos; y **(iii)** escalamiento progresivo, priorizando las iniciativas de mayor impacto misional y menor nivel de riesgo.

16.1.1 Experimentación responsable

La SAE impulsará procesos de experimentación responsable que permitan desarrollar y probar pilotos de Inteligencia Artificial en entornos controlados, garantizando siempre el cumplimiento de criterios de seguridad, ética y legalidad. Cada piloto deberá contar con un objetivo claramente definido, una evaluación preliminar de riesgos y un protocolo de validación que asegure que la tecnología no genere afectaciones al servicio público, a los derechos ciudadanos ni a la integridad de los datos institucionales.

La experimentación incluirá mecanismos de revisión humana, pruebas de sesgos, análisis de impacto y controles de acceso, de modo que las soluciones emergentes avancen únicamente cuando demuestren niveles adecuados de confiabilidad y pertinencia misional.

16.1.2 Aprendizaje continuo

El aprendizaje continuo será un componente central del proceso de innovación institucional, permitiendo a la SAE analizar sistemáticamente los resultados de cada piloto o implementación de IA, obtener retroalimentación de las áreas involucradas y aplicar ajustes iterativos basados en evidencia. Este enfoque promoverá ciclos de mejora permanente en los modelos, los datos y los procedimientos institucionales, fortaleciendo la capacidad de la entidad para adaptarse a los cambios tecnológicos y a las necesidades operativas. A través de este eje, la SAE consolidará un repositorio de lecciones aprendidas, buenas prácticas y análisis comparativos, que servirán de insumo estratégico para futuras implementaciones y para la toma de decisiones informadas en materia de innovación tecnológica.

16.1.3 Escalamiento progresivo

La SAE adoptará un modelo de escalamiento progresivo que asegure que las soluciones de IA con resultados positivos en fase piloto puedan ampliarse gradualmente según su impacto esperado, nivel de riesgo y capacidad institucional para operarlas. Este proceso priorizará aquellas iniciativas que contribuyan directamente a los objetivos misionales de la entidad, generen mejoras verificables en eficiencia y transparencia, y presenten un perfil de riesgo bajo o mitigable. El escalamiento incluirá la formalización de responsabilidades, la integración con los sistemas institucionales, la capacitación de los equipos y la implementación de auditorías técnicas y éticas que garanticen la sostenibilidad de la solución. De este modo, la SAE podrá consolidar tecnologías maduras y confiables que aporten valor público de manera sostenible.

Toda acción de innovación deberá contar con una justificación institucional clara, registro documental y mecanismos de validación técnica que aseguren confiabilidad y transparencia.

16.2 Cooperación Nacional e Internacional en Innovación Tecnológica

La innovación apoyada en IA también se apalancará en el fortalecimiento de alianzas nacionales e internacionales con entidades públicas, universidades, centros de investigación y organismos multilaterales. Estas alianzas facilitarán el acceso a estándares globales, buenas prácticas, modelos de evaluación de riesgo, marcos de referencia éticos y soluciones tecnológicas emergentes. De igual manera, permitirán que la SAE participe en redes de cooperación para el desarrollo de proyectos piloto, investigación aplicada, interoperabilidad de datos y formación especializada en IA responsable.

17. PROHIBICIONES EN EL USO DE INTELIGENCIA ARTIFICIAL

La SAE establece un conjunto de restricciones obligatorias para garantizar que el uso de la Inteligencia Artificial no genere riesgos legales, éticos o de seguridad para la entidad. Estas prohibiciones aplican a todo funcionario, contratista, proveedor, aliado tecnológico o tercero que participe en actividades relacionadas con sistemas de IA.

Queda prohibido utilizar plataformas públicas de IA para cargar, introducir o procesar cualquier tipo de información institucional que sea reservada, sensible o confidencial, incluyendo datos personales, datos de procesos misionales, información contractual, jurídica, financiera, técnica o estratégica. Ningún dato institucional podrá ser transferido a servicios externos que utilicen dicha información para entrenar o mejorar modelos sin aprobación explícita del Comité de Arquitectura Empresarial.

No se permite el uso de herramientas de IA para generar documentos, conceptos, análisis o comunicaciones oficiales sin validación previa de un responsable institucional. Toda salida generada por IA deberá ser revisada, ajustada y aprobada antes de su difusión interna o externa.

Se prohíbe el desarrollo o utilización de sistemas de IA que tomen decisiones automáticas sin supervisión humana en procesos que puedan afectar derechos, valores económicos, vida jurídica de expedientes o información crítica. Toda decisión asistida por IA deberá contar con un responsable humano plenamente identificado.

Queda prohibido modificar modelos, algoritmos o parámetros sin autorización técnica de la Oficina de Tecnologías y Sistemas de Información y sin la debida trazabilidad. Cualquier ajuste no autorizado será considerado una alteración indebida del sistema.

No se permite instalar, ejecutar o integrar soluciones de IA no autorizadas en los equipos, redes o plataformas de la SAE. Solo podrán utilizarse herramientas evaluadas y aprobadas conforme a los lineamientos de la política.

Se prohíbe compartir accesos, claves, credenciales o roles que permitan entrenar, modificar o administrar sistemas de IA institucionales. Toda gestión deberá realizarse siguiendo las políticas de seguridad de la información vigentes.

Queda estrictamente prohibido que terceros utilicen información institucional para entrenar modelos propios, desarrollar productos comerciales o alimentar sistemas externos, sin cláusulas contractuales explícitas y sin autorización del Comité.

18. SEGUIMIENTO, CONTROL Y ACTUALIZACIÓN

La implementación de la Política de Inteligencia Artificial de la Sociedad de Activos Especiales - SAE será objeto de **seguimiento continuo, control técnico y actualización periódica**, con el fin de garantizar su vigencia, eficacia y alineación con los avances tecnológicos, normativos y organizacionales. El monitoreo permanente permitirá evaluar el grado de madurez institucional en el uso de IA, identificar oportunidades de mejora y asegurar la rendición de cuentas frente a los órganos de control y la ciudadanía.

El **Comité de Arquitectura Empresarial** será el responsable de liderar este proceso, elaborando **informes semestrales** sobre el estado de implementación de la política, los proyectos en ejecución, los incidentes reportados y los resultados de las auditorías técnicas y éticas. Dichos informes serán integrados al sistema de gestión de calidad institucional y remitidos al **Comité de Arquitectura Empresarial,** a la **Oficina de Control Interno** y a la **Alta Dirección**, asegurando la trazabilidad de las acciones y el cumplimiento del marco normativo.

La política será **revisada y/o actualizada** si existen cambios significativos en la regulación nacional, la arquitectura tecnológica o los riesgos asociados al uso de la IA. El proceso de actualización incluirá la revisión de los principios éticos, los procedimientos de evaluación, las metodologías de gestión de riesgos y las responsabilidades institucionales. Toda modificación deberá ser aprobada por el Comité de Arquitectura Empresarial y la Junta Directiva.

Para el control de desempeño y madurez, se establecerán **indicadores institucionales** tales como:

- Número de proyectos de IA registrados y validados por el Comité.
- Cumplimiento de revisiones éticas y de riesgo documentadas.
- Número de incidentes gestionados y mitigados satisfactoriamente.
- Nivel de formación del talento humano en IA responsable.
- Grado de interoperabilidad y cumplimiento de estándares de seguridad.

19. ANEXOS

19.1 Ficha institucional de caso de uso de IA (Formato estándar SAE)

Campo	Descripción / Instrucción
Nombre del caso de uso	Título breve y descriptivo del sistema o proyecto de IA.
Dependencia responsable	Área o dirección líder del desarrollo o adopción del sistema.
Objetivo institucional	Propósito del caso de uso, vinculado al cumplimiento de una meta misional o estratégica.
Tipo de IA aplicada	Seleccionar: predictiva, clasificatoria, generativa, analítica, automatización inteligente, etc.
Datos utilizados	Fuente, tipo (estructurados/no estructurados), nivel de sensibilidad y mecanismos de anonimización.
Nivel de riesgo	Clasificar: bajo / medio / alto (según impacto sobre derechos, datos o decisiones).
Evaluación de sesgos	Indicar métodos aplicados para detectar y mitigar sesgos algorítmicos o de datos.
Revisión humana	Describir el mecanismo de validación o supervisión humana en la toma de decisiones.
Proveedor o desarrollador	Nombre, naturaleza (interno/externo), certificaciones y declaración de uso de IA.
Medidas de seguridad	Controles técnicos, lógicos y administrativos aplicados.
Fecha de aprobación	Fecha de validación por el Comité Institucional de Gobernanza de IA.
Resultados esperados	Indicadores de desempeño, eficiencia o trazabilidad derivados del caso de uso.
Informe de desempeño anual	Resumen de auditoría o monitoreo del sistema (llenado por el Comité).

19.2 Modelo de evaluación de riesgo ético-técnico (aplicable a cada caso de uso)

A. Identificación de riesgos principales

Dimensión	Riesgo potencial	Probabilidad	Impacto	Nivel de riesgo (PxI)	Medidas de mitigación
Ética y derechos	Sesgos algorítmicos o discriminación involuntaria.	Media	Alta	9	Pruebas de equidad, revisión humana obligatoria.
Privacidad y datos	Uso indebido o filtración de información sensible.	Baja	Alta	6	Anonimización, cumplimiento Ley 1581, cifrado y trazabilidad.
Seguridad técnica	Manipulación o vulneración del modelo.	Media	Media	6	Evaluaciones de penetración,

					controles NIST/ISO 27001.
Legal y regulatorio	Incumplimiento de normativa o ausencia de consentimiento.	Media	Alta	9	Validación jurídica previa, revisión por Comité IA.
Transparencia y explicabilidad	Resultados no auditables o difíciles de interpretar.	Alta	Media	9	Documentación del modelo, herramientas de interpretabilidad.
Gobernanza y supervisión	Falta de control o reporte de incidentes.	Media	Alta	9	Reporte obligatorio al Comité y monitoreo semestral.

B. Escala de valoración institucional SAE

Nivel	Rango (P x I)	Significado	Acción requerida
Bajo	1–4	Riesgos controlables.	Seguimiento rutinario.
Medio	5–8	Riesgos relevantes.	Mitigación y revisión semestral.
Alto	9–12	Riesgos críticos.	Aprobación previa y auditoría continua.

C. Reporte de mitigación y validación

Cada caso de uso deberá incluir un **informe de validación ética-técnica**, firmado por el responsable del proyecto, el delegado de seguridad de la información y un miembro del Comité de Gobernanza de IA. Este informe documentará los riesgos identificados, las medidas aplicadas y los resultados de las pruebas de desempeño y equidad.

D. Registro y trazabilidad

Toda la información generada será archivada en el **Repositorio Institucional de Gobernanza de IA**, administrado por la Dirección de Planeación y Prospectiva, asegurando integridad, transparencia y rendición de cuentas ante los órganos de control.

20. BIBLIOGRAFÍA

20.1 Fuentes normativas nacionales

- Congreso de la República de Colombia. (2009). *Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC.* Diario Oficial No. 47.426.
- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial No. 48.587.
- Congreso de la República de Colombia. (2014). *Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.* Diario Oficial No. 49.084.
- Departamento Nacional de Planeación (DNP). (2025). *Documento CONPES 4144: Política Nacional de Inteligencia Artificial.* Bogotá D.C.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). *Política de Gobierno Digital.* Bogotá D.C.

- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022). *Decreto 1263 de 2022: Por el cual se establece el Modelo de Gobernanza Digital del Estado colombiano.* Diario Oficial No. 52.153.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). *Modelo de Referencia de Arquitectura Empresarial del Estado (MRAEE).* Bogotá D.C.
- Presidencia de la República de Colombia. (2015). *Decreto 1078 de 2015: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.* Bogotá D.C.
- Departamento Administrativo de la Función Pública. (2019). *Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG).* Bogotá D.C.

20.2 Fuentes internacionales y marcos de gobernanza de IA

- European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 July 2024 laying down harmonised rules on artificial intelligence (AI Act).* Official Journal of the European Union.
- National Institute of Standards and Technology (NIST). (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0).* U.S. Department of Commerce.
- Organisation for Economic Co-operation and Development (OECD). (2019). *Recommendation of the Council on Artificial Intelligence.* OECD Legal Instruments No. 0449.
- United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). *Recommendation on the Ethics of Artificial Intelligence.* Paris: UNESCO.
- PwC. (2024). *Responsible AI and Risk Management: From Principles to Practice.* PricewaterhouseCoopers Global.
- Gartner. (2024). *AI Governance: Establishing Risk-Based Policies for Responsible Artificial Intelligence.* Gartner Research.
- Desai, A. (2024). *Building Ethical and Resilient AI Governance Frameworks.* Schellman & Company LLC.

20.3 Fuentes técnicas y conceptuales

- Bhattacharya, A., Mann, S., & Ray, S. (2022). *Ethical AI in Public Administration: Frameworks for Trustworthy Implementation. Government Information Quarterly*, 39(4), 101742.
- Dong, J. Q., & Hussain, T. (2011). *Understanding the Role of Digital Transformation in Organizational Change. Information Systems Frontiers*, 13(2), 235–244.
- Verhoef, P. C., Broekhuizen, T., & Bart, Y. (2019). *Digital Transformation: A Multidisciplinary Reflection and Research Agenda. Journal of Business Research*, 122, 889–901.
- Ghani, R. (2024). *AI Policy Design and Continuous Improvement Framework.* Carnegie Mellon University.
- Kornutick, L. (2024). *AI Governance Maturity Models in the Public Sector. Gartner Insights Report*, 15(2), 34–42.
- Kay, K., & Ladner, T. (2024). *Corporate AI Policy Development in Financial Institutions.* Principal Financial Group & Aflac Global Security.
- Levitt, L. (2024). *Cross-Functional Governance for Responsible AI.* Intuit Legal Affairs Whitepaper.
- Sen, R. (2024). *AI Risk Management and Third-Party Dependencies.* PwC Global Advisory Series.
- Vohra, S. (2024). *AI Compliance and Operational Readiness in Enterprises.* Genpact Technology Review.

20.4 Fuentes complementarias

- Sánchez Torres, J. (2017). *Guía metodológica para la vigilancia tecnológica e inteligencia competitiva.* Universidad Nacional de Colombia.
- Kitchenham, B. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report*, Keele University.
- Desai, A., Priest, D., & Kornutick, L. (2024). *Managing AI Failures: Building Technical and Ethical Response Plans. PwC – Responsible AI Review*.
- OCDE. (2023). *Trustworthy AI in the Public Sector: Policy Framework and Implementation Toolkit.* OECD Digital Economy Papers No. 355.

21. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de cambios	Justificación del cambio
1	18/11/2025	Primera versión	Creación de la política

22. CONTROL DE ÚLTIMA APROBACIÓN

	Nombre	Área	Cargo
Elaboración Técnica	Lucas Adolfo Giraldo Ríos	Dirección de Planeación y Prospectiva	Contratista
Acompañamiento metodológico	Lucas Adolfo Giraldo Ríos	Dirección de Planeación y Prospectiva	Contratista
Revisión Técnica	Daniel Sebastian Contreras Ortiz	Dirección de Planeación y Prospectiva	Director de Planeación y Prospectiva
Revisión Metodológica	Carol Alexandra Campos Vieda	Dirección de Planeación y Prospectiva	Profesional Especializada III
Aprobación	Daniel Sebastian Contreras Ortiz	Dirección de Planeación y Prospectiva	Director de Planeación y Prospectiva