POLÍTICA DE USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

PARKER RANDALL COLOMBIA SAS

27 de Agosto del 2026

TABLA DE CONTENIDO

INTRODUCCIÓN

Los sistemas de Inteligencia Artificial (IA) están cada vez más presentes en los servicios, soluciones y procesos internos de **PARKER RANDALL COLOMBIA SAS**, integrándose en los flujos de trabajo diarios y en la forma en que se presta los servicios a los clientes. Esto genera la expectativa, por parte de clientes, colaboradores, reguladores y demás grupos de interés, de que la organización utilice la IA de manera fiable, segura, ética y respetuosa de la privacidad y la integridad de los datos, así como de las normas aplicables.

En este contexto, **PARKER RANDALL COLOMBIA SAS** asume el compromiso de gestionar de forma proactiva los riesgos y oportunidades asociados al uso de la IA, alineándose con la Responsible AI Policy de la red **PARKER RANDALL COLOMBIA SAS** y con el marco normativo vigente en las jurisdicciones donde opera. Esta Política de Uso Responsable de la Inteligencia Artificial describe el enfoque adoptado por **PARKER RANDALL COLOMBIA SAS** para diseñar, adquirir, desarrollar, desplegar y utilizar sistemas de IA éticos, seguros, fiables y transparentes, siendo de obligatorio cumplimiento para todas las personas y unidades que intervienen en actividades relacionadas con la IA dentro de la organización.

OBJETIVO

El objetivo de esta Política es establecer el marco común para el uso responsable de la inteligencia artificial en **PARKER RANDALL COLOMBIA SAS**, fijando los principios, criterios y requisitos mínimos que deben cumplirse al diseñar, adquirir, implementar y utilizar sistemas de IA, de manera segura, ética, transparente y alineada con la normativa aplicable y los lineamientos de la oficina Global.

ALCANCE

La presente Política de Uso Responsable de la Inteligencia Artificial aplica a todas las operaciones de **PARKER RANDALL COLOMBIA SAS**. Su cumplimiento es obligatorio para todas las personas que actúan en nombre de la Firma, por clientes y demás partes interesadas externas, incluyendo empleados, contratistas, consultores, filiales y demás terceros que utilicen, desarrollen, adquieran, implementen o supervisen sistemas o herramientas de IA en el marco de sus funciones.

MARCO NORMATIVO

PARKER RANDALL COLOMBIA SAS reconoce y tiene en cuenta las principales normativas e instrumentos internacionales que orientan sobre el uso responsable y ético de la Inteligencia Artificial en los países donde opera, entre ellos:

- Decreto No. 234 de 2025 – Asamblea Legislativa de la República de El Salvador.
- b. Circular No. 002 de 2024 – Superintendencia de Industria y Comercio – Colombia.
- c. CONPES 4144 de 2025 – Política Nacional de Inteligencia Artificial – Colombia.
- d. Recomendación sobre la Ética de la Inteligencia Artificial – UNESCO (2021).

- e. Recomendación sobre la Inteligencia Artificial de la OCDE.
- f. Declaración de Santiago "Para promover una inteligencia artificial ética en América Latina y el Caribe" (2023).
- g. Carta Iberoamericana de Principios y Derechos en Entornos Digitales (2023).
- h. Lineamientos interamericanos de gobernanza de datos e inteligencia artificial – DGPE/OEA (2024).

Este listado es referencial y no limitativo.

DEFINICIONES

- Inteligencia Artificial (IA): Conjunto de tecnologías integradas en sistemas o herramientas que permiten analizar información, generar contenidos, apoyar la toma de decisiones o automatizar tareas, simulando capacidades humanas como el aprendizaje, el razonamiento o la interacción.
- Sistema de Inteligencia Artificial: Herramienta, aplicación o componente tecnológico que utiliza inteligencia artificial, ya sea desarrollado internamente o provisto por terceros, e integrado en los procesos, servicios o plataformas de **PARKER RANDALL COLOMBIA SAS**.
- Uso Responsable de la IA: Aplicación de la inteligencia artificial de manera ética, transparente, segura y alineada con la legislación vigente, los valores corporativos y los principios definidos por **PARKER RANDALL COLOMBIA SAS**, garantizando la supervisión humana y la gestión adecuada de los riesgos.
- Usos Inaceptables de la IA: Prácticas de uso de inteligencia artificial que están prohibidas por **PARKER RANDALL COLOMBIA SAS** por ser contrarias a la ética, la ley, los valores corporativos o el Código de Ética y Conducta, incluyendo usos discriminatorios, engañosos o indebidos.
- Sistema de IA de Alto Riesgo: Sistema de inteligencia artificial cuyo uso puede generar impactos significativos sobre personas, clientes, procesos críticos, información o la reputación de la Firma, y cuyo nivel de riesgo es determinado conforme a la metodología corporativa de gestión de riesgos de **PARKER RANDALL COLOMBIA SAS**.
- Supervisión Humana: Capacidad de las personas designadas por **PARKER RANDALL COLOMBIA SAS** para revisar, validar, interpretar y, cuando sea necesario, corregir o detener los resultados generados por un sistema de inteligencia artificial.
- Decisión Automatizada: Resultado generado por un sistema de inteligencia artificial sin intervención humana directa en el momento de la ejecución, que puede influir o determinar una acción, recomendación o resultado dentro de un proceso.
- Transparencia de la IA: Principio que garantiza que las personas puedan identificar cuándo están interactuando con un sistema de inteligencia artificial y comprender, a un nivel adecuado, su propósito, funcionamiento general y limitaciones.

- Explicabilidad: Capacidad de un sistema de inteligencia artificial para que sus resultados, decisiones o recomendaciones puedan ser comprendidos y explicados por personas, de forma proporcional a su nivel de riesgo y uso.
- Sesgo: Distorsión o desviación en los resultados de un sistema de inteligencia artificial que puede generar decisiones injustas, discriminatorias o no representativas, generalmente asociada a los datos utilizados, al diseño del sistema o a su forma de uso.
- Datos de Entrada y Salida de IA: Información utilizada por un sistema de inteligencia artificial para generar resultados (datos de entrada) y la información producida por dicho sistema como resultado de su procesamiento (datos de salida).
- Proveedor con IA: Tercero que suministra, desarrolla, implementa o utiliza sistemas de inteligencia artificial en la prestación de servicios o productos a **PARKER RANDALL COLOMBIA SAS**.
- Debida Diligencia en IA: Proceso de evaluación inicial y periódica de proveedores que utilizan inteligencia artificial, orientado a identificar riesgos, controles y cumplimiento de los principios definidos en la Política de Uso Responsable de IA y en los procedimientos corporativos aplicables.
- Incidente de Seguridad de la Información: Evento asociado al uso de sistemas de inteligencia artificial que puede afectar la confidencialidad, integridad o disponibilidad de la información de **PARKER RANDALL COLOMBIA SAS** y que debe ser gestionado conforme a los procedimientos corporativos definidos.
- Ciclo de Vida del Sistema de IA: Conjunto de etapas por las que pasa un sistema de inteligencia artificial, desde su diseño o adquisición, implementación, uso, mantenimiento, modificación y eventual retiro.
- Inventario de Sistemas de IA: Registro corporativo que identifica los sistemas de inteligencia artificial utilizados por **PARKER RANDALL COLOMBIA SAS**, incluyendo su propósito, responsables y nivel de riesgo.
- Contenido Generado por IA: Texto, imagen, audio, video u otro tipo de información creada total o parcialmente por un sistema de inteligencia artificial.
- Sostenibilidad en IA: Consideración de los impactos ambientales, sociales y económicos asociados al uso de sistemas de inteligencia artificial, promoviendo un uso eficiente, responsable y alineado con los objetivos corporativos de la Firma.

DOCUMENTOS

- **PARKER RANDALL COLOMBIA SAS** Responsible AI Policy
- **PARKER RANDALL COLOMBIA SAS** Network, 1 de Octubre de 2024.
- POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center
- PRO-SCM-01 Procedimiento Compra de Bienes y Servicios

- MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información **PARKER RANDALL COLOMBIA SAS**
- FOR-GSI-17 Matriz de Requisitos legales SGSI.
- PRO-GSI-01 Procedimiento Gestión de Incidentes Seguridad de la información.
- DOG-GEA-31 Metodología para la Gestión de Riesgos de **PARKER RANDALL COLOMBIA SAS**.
- POL-GEA(ITR)-03 Política de tratamiento de datos personales del grupo empresarial **PARKER RANDALL COLOMBIA SAS**.

6.1 DESARROLLO Y DESPLIEGUE CON GESTIÓN DE SESGOS

6.1.1 Usos inaceptables de la IA

La firma no hará uso de la inteligencia artificial en contextos que comprometan la integridad profesional y generen riesgos de tipo ético, legal o reputacional. Para garantizarlo ha establecido una serie de lineamientos en los cuales los profesionales, contratistas y terceros que actúan en su nombre no deben verse involucrados en estas prácticas inaceptables en ninguna circunstancia.

A continuación, se relacionan algunas prácticas inaceptables:

– Utilizar sistemas de IA que no sean los autorizados por la firma.

– Introducir información sensible de los clientes en plataformas de IA públicas o no autorizadas por la firma.

– Confiar solamente en la información generada por la IA para la ejecución de los trabajos, prescindiendo del criterio profesional.

– Emplear la IA para crear documentos fraudulentos.

– Contratar proveedores de servicios que proporcionen soluciones de IA, sin validar su metodología, seguridad o cumplimiento normativo.

– Utilizar la IA sin comprender las limitaciones y riesgos.

La Firma comunica y refuerza estos lineamientos mediante procesos periódicos de formación y sensibilización, con el objetivo de prevenir prácticas contrarias a la ética profesional, a la legislación vigente o a los valores corporativos.

Adicionalmente la firma no deberá verse involucrada en los usos inaceptables de la IA contenidos en la política global “Responsible AI Policy” en el Apéndice 1.

6.1.2 Desarrollo ético y libre de sesgos discriminatorios

La firma garantizará que, en el desarrollo de sistemas de Inteligencia Artificial, estos se diseñen de manera ética y objetiva, evitando la generación de decisiones o resultados discriminatorios o sesgados. Para ello, se implementarán las medidas definidas en las etapas validación, pruebas y verificaciones de los sistemas de IA, las cuales deberán ejecutarse

conforme a los lineamientos establecidos en la POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.1.3 Criterios de sostenibilidad en el desarrollo y despliegue

La firma promueve la incorporación de criterios ambientales, sociales y económicos en el desarrollo y despliegue de sistemas de inteligencia artificial. Entre estos aspectos se destaca la evaluación del impacto ambiental de las soluciones de IA, con especial atención a su contribución hacia los objetivos de reducción de emisiones. Estas acciones se materializan a través de las mediciones de huella de carbono de la Firma, cuyos resultados se presentan en el informe de sostenibilidad anual.

6.2 TRANSPARENTE Y EXPLICABLE

6.2.1 Documentación y accesibilidad de la información de sistemas de IA desarrollados por la firma

PARKER RANDALL COLOMBIA SAS asegura que los sistemas de inteligencia artificial que desarrolle o implemente cuenten con documentación clara, completa y accesible, que permita comprender su propósito, alcance, capacidades, limitaciones y criterios generales de uso. Esta documentación facilita la supervisión, el control y la correcta operación de las herramientas de IA por parte de las áreas responsables.

La información asociada a cada sistema de IA se documenta y mantiene actualizada en las fichas técnicas o registros definidos por la Firma. Estos se encuentran disponibles para las partes interesadas pertinentes tales como: socios, personal, clientes y reguladores, en el momento que sean requeridos, con el propósito de asegurar su entrega oportuna.

6.2.2 Transparencia en sistemas de IA de terceros de alto riesgo.

Antes de utilizar sistemas de inteligencia artificial potencialmente de alto riesgo desarrollados por terceros, la firma revisará y analizará la información que describa su funcionamiento.

Previo a esto, el área de compras solicitará al proveedor de servicio que suministre la información relacionada con el sistema de IA, la cual deberá incluir: la descripción del modelo y su propósito, los datos utilizados para el entrenamiento y los métodos de validación y pruebas aplicados. Esta revisión formará parte de los procesos de evaluación y selección de proveedores.

6.2.3 Divulgación del uso de IA ante usuarios finales.

La firma informará de manera transparente a los usuarios finales cuando interactúen con sistema de inteligencia artificial implementado por la firma, como por ejemplo un Chatbot. En estos casos, los mensajes de las aplicaciones deberán indicar “contenido generado por IA y/o es posible que el contenido generado por IA sea incorrecto”.

6.3 RESPONSABILIDAD Y SUPERVISIÓN HUMANA

6.3.1 Rendición de cuentas y uso de IA de terceros.

Para los sistemas de IA desarrollados por la firma, el área de I&T Center será la responsable del diseño e implementación de estas herramientas, así como de supervisar su uso, con el fin de asegurar la transparencia y control.

Para sistemas de IA potencialmente de alto riesgo que sean desarrollados por terceros para su implementación en la firma, el área de compras en conjunto con el área de seguridad de la información y de IT serán los responsables de asegurar que cuenten con todas las medidas de seguridad y privacidad para su funcionamiento, dentro del proceso de selección del proveedor de servicio.

El uso de sistemas de inteligencia artificial (IA) desarrollados por terceros en la firma, estará estrictamente limitado a aquellos que hayan sido evaluados y aprobados conforme al proceso de selección y evaluación de proveedores establecido por la firma.

En caso de fallos o vulnerabilidades de seguridad en los sistemas de IA, estos deberán ser reportadas de manera inmediatas a las áreas de Seguridad de la información y de IT para su gestión y mitigación.

Ante la identificación de fallos o vulnerabilidades de seguridad, se deberá notificar de manera inmediata a las áreas responsables de Seguridad de la Información y Tecnología de la Información (IT) para su gestión y mitigación.

La identificación y evaluación de los riesgos asociados al uso de IA se realiza conforme a los lineamientos establecidos en el documento DOG-GEA-31 Metodología para la Gestión de Riesgos de **PARKER RANDALL COLOMBIA SAS**.

6.3.2 Supervisión y control humano de sistemas de IA de alto riesgo

Todo sistema de inteligencia artificial considerados de alto riesgo no podrán funcionar de manera totalmente autónoma, sino que estará sujeto a supervisión y control humano.

Ante errores o riesgos presentados por los sistemas de IA clasificados de alto riesgo, la firma ha designado responsables para intervenir el sistema, lo que incluye detener su uso, revertir o invalidar los resultados generados por el sistema de IA y realizar las correcciones necesarias. Lo anterior para asegurar la transparencia, responsabilidad y protección frente a estos posibles fallos o riesgos.

La clasificación del nivel de riesgo de los sistemas de IA se determina aplicando los criterios establecidos en el documento DOG-GEA-31 Metodología para la Gestión de Riesgos, y se complementa con los criterios técnicos definidos en la POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.3.3 Medidas para decisiones automatizadas de alto impacto

Antes de la puesta en marcha de sistemas de inteligencia artificial con capacidad de tomar decisiones automatizadas que puedan tener un impacto significativo sobre personas, clientes o procesos críticos, se deberán aplicar controles mínimos orientados a la evaluación de riesgos,

protección de la privacidad y validar los resultados generados, que estén bajo la supervisión de las áreas responsables de la firma.

Estas medidas incluyen, cuando aplique, la evaluación preliminar de impacto en privacidad y la realización de pruebas de validación con fuentes de información aprobadas por la Firma, conforme a los criterios definidos para cada caso de uso.

6.3.4 Colaboración eficaz entre personas y sistemas de IA

Los sistemas de IA pueden ser utilizada por los profesionales de la firma como apoyo en las tareas y para la mejora de los procesos, pero la responsabilidad de la toma de decisiones será de los profesionales de la firma y no únicamente del sistema de IA.

Cuando se implemente un sistema de IA en los procesos de la firma, se deberá realizar de manera que el personal se adapte y lo integre a su trabajo sin generar barreras ni pérdida de control.

Los sistemas de IA utilizados no deberán vulnerar los derechos de los profesionales ni deberán reducir el valor de su trabajo.

6.3.5 Revisión, validación y verificación de resultados de IA

Los resultados generados por los sistemas de IA utilizados en la firma no podrán ser aceptados de manera automática sin la supervisión adecuada.

Para esto la firma ha designado responsables y criterios formales para la revisión, validación y verificación estos resultados, considerando la coherencia de los resultados, la trazabilidad de la información utilizada y el riesgo asociado a su uso.

Los lineamientos técnicos y operativos relacionados con estas actividades se desarrollan conforme al documento POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.4 SE RESPETAN LOS DERECHOS Y LA INTEGRIDAD DE LOS DATOS

6.4.1 Evaluación de la calidad, cantidad y adecuación de los datos

La firma revisará la calidad de los datos que se utilizan en los sistemas de IA, verificando que estos sean precisos, completos y estén libres de errores, adicionalmente, se asegurará que la información sea suficiente para para el correcto funcionamiento y se comprobará que los datos correspondan al propósito para el cual se va a utilizar.

Se deberá garantizar que los datos utilizados en el desarrollo de sistemas de IA provengan de fuentes confiables y actualizadas para evitar la toma de decisiones basadas en información obsoleta.

Los criterios y responsabilidades asociados a esta evaluación se desarrollan conforme a la POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.4.2 Privacidad, seguridad y confidencialidad de los datos.

La firma adopta medidas adecuadas para proteger la privacidad, seguridad y confidencialidad de los datos de entrada y salida utilizados por los sistemas de inteligencia artificial, en cumplimiento de la legislación aplicable, incluida la normativa vigente sobre protección de datos personales, y de las obligaciones contractuales vigentes.

El tratamiento, almacenamiento y protección de los datos se realizan conforme a los lineamientos establecidos en la POL-GEA(ITR)-03 Política de tratamiento de datos personales, el MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información **PARKER RANDALL COLOMBIA SAS**, y a los controles definidos en la POL-INV(ITR)- 01 Política de Desarrollo Seguro para I&T Center, cuando aplique.

6.4.3 Derechos de propiedad intelectual sobre datos y desarrollos

Todo desarrollo tecnológico realizado en el marco de la relación contractual entre la Firma y los profesionales, contratistas o terceros, incluyendo, pero sin limitarse a software, aplicaciones, algoritmos, diseños, códigos, documentación técnica y cualquier otro resultado derivado de la actividad profesional será considerado propiedad intelectual exclusiva de la firma, especialmente en lo que respecta a los derechos patrimoniales sobre dichas obras. Lo anterior se entiende sin perjuicio de los derechos morales que, conforme a la legislación aplicable a cada uno de los países que hacen parte de **PARKER RANDALL COLOMBIA SAS**, corresponden a las personas naturales integrantes del equipo desarrollador, quienes conservarán dichos derechos en los términos previstos por la ley.

En el marco de las relaciones de la firma, todos los desarrollos tecnológicos producidos para **PARKER RANDALL COLOMBIA SAS** serán de titularidad patrimonial de **PARKER RANDALL COLOMBIA SAS** conforme se materialice según el vínculo: para trabajadores, la transferencia patrimonial opera automáticamente por presunción legal en el contrato de trabajo; para contratistas, la cesión se perfecciona mediante las cláusulas del contrato de prestación de servicios o de las cláusulas de seguridad de la información; y para clientes, el reconocimiento de dicha titularidad se incorpora en el contrato o carta arreglo correspondiente. En todos los casos, los derechos morales sobre las obras pertenecen exclusivamente a las personas naturales que las crean, mientras que los derechos patrimoniales se regulan y definen conforme a lo pactado en los respectivos contratos.

6.4.4 Cifrado y control de acceso a la información

La firma implementa medidas de cifrado, autenticación y control de acceso para evitar que los sistemas de inteligencia artificial accedan, procesen o divulguen información a personas o sistemas no autorizados.

Estos controles se aplican conforme a los principios de clasificación de la información, gestión de accesos, registro y trazabilidad definidos en el MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información **PARKER RANDALL COLOMBIA SAS** y a los controles técnicos establecidos en la POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.5 DOCUMENTADAS Y SUPERVISADAS CONTINUAMENTE

6.5.1 Inventario de sistemas de IA

La firma mantiene un inventario actualizado de los sistemas de inteligencia artificial desarrollados internamente o provistos por terceros identificando su propósito, uso, responsables y nivel de riesgo; Este inventario constituye un insumo clave para la supervisión, la gestión de riesgos y la rendición de cuentas. Este inventario es revisado de manera periódica y aprobado por los líderes de las áreas de I&T Center y de IT de la firma.

6.5.2 Documentación del ciclo de vida de los sistemas de IA

PARKER RANDALL COLOMBIA SAS documenta el ciclo de vida de los sistemas de inteligencia artificial que utiliza, incluyendo responsables, decisiones relevantes, cambios significativos y usos previstos.

La documentación se conserva en los repositorios oficiales definidos por la Firma, aplicando los lineamientos de custodia, clasificación y control de acceso establecidos en el MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información **PARKER RANDALL COLOMBIA SAS**, en coordinación con el área de I&T Center.

6.5.3 Evaluación de impactos de sistemas de IA de alto riesgo

La firma evalúa de manera previa a la puesta en funcionamiento los posibles impactos de los sistemas de inteligencia artificial clasificados como de alto riesgo, analizando su desarrollo, implementación y uso frente a los principios de esta Política.

Dicha evaluación de impactos y riesgos se realiza conforme a los lineamientos del DOG-GEA-31 Metodología para la Gestión de Riesgos, permitiendo identificar el nivel de riesgo, definir controles y establecer planes de tratamiento cuando sea necesario. Esta evaluación se documenta y se mantiene actualizada.

Cuando estos sistemas de IA de alto riesgo son provistos o gestionados por terceros, la firma incorpora criterios específicos de evaluación de impactos y riesgos de IA dentro de la evaluación anual de proveedores, asegurando que estos criterios formen parte del seguimiento continuo del proveedor.

6.5.4 Monitoreo contínuo

La firma monitorea de forma continua los riesgos asociados al uso de sistemas de inteligencia artificial, especialmente aquellos clasificados como de alto riesgo, verificando la eficacia de los controles implementados y la evolución del riesgo residual.

El monitoreo y actualización de los riesgos se realiza conforme a las etapas definidas en el DOG-GEA-31 Metodología para la Gestión de Riesgos.

6.6 GOBERNANZA DE LA IA

6.6.1 Principios de la gobernanza de IA

PARKER RANDALL COLOMBIA SAS establece una gobernanza robusta de la inteligencia artificial (IA) para asegurar su uso ético, seguro, transparente y responsable, alineado con los objetivos estratégicos de la Firma, con la Responsible AI Policy de la red **PARKER RANDALL COLOMBIA SAS** y con el marco normativo aplicable en las jurisdicciones donde opera.

La gobernanza de la IA se fundamenta en los siguientes principios rectores:

- Transparencia y socialización: garantizar que los usuarios y partes interesadas comprendan el propósito, funcionamiento general y limitaciones de los sistemas de IA.
- Responsabilidad y rendición de cuentas: definir claramente los responsables de decisiones, supervisión y controles asociados al ciclo de vida de la IA.
- Supervisión humana efectiva: asegurar que los sistemas de alto riesgo estén sujetos a intervención y control humano oportuno.
- Cumplimiento normativo y ético: observar la legislación aplicable y los estándares internos de la Firma, priorizando el mayor nivel de protección cuando existan diferencias regulatorias.
- Gestión integral de riesgos: identificar, evaluar, monitorear y tratar los riesgos de IA.
- Mejora continua: revisar y actualizar procedimientos, controles y capacidades de la organización en respuesta a cambios tecnológicos, regulatorios y de operación.

6.6.2 Estructura y gobernanza y roles.

La gobernanza de la IA en **PARKER RANDALL COLOMBIA SAS** se articula mediante roles y responsabilidades claramente definidos y un órgano colegiado para la supervisión estratégica:

- *Comité de IA: *Grupo responsable de la supervisión estratégica y la toma de decisiones en materia de IA. Está conformado, al menos, por representantes de: I&T Center, Infraestructura y Tecnología (IT), Seguridad de la Información, LR&C (Legal, Risk & Compliance), Ética e Independencia/IQ&R/SoQM (según aplique) y si es el caso se incluyen líderes de procesos/unidades de negocio vinculados a casos de uso relevantes.

Funciones principales:

- Aprobación de casos de uso críticos y de sistemas de IA de alto riesgo, incluyendo decisiones automatizadas de alto impacto.
- Supervisión del cumplimiento de esta Política y del alineamiento con la Responsible AI Policy de la red **PARKER RANDALL COLOMBIA SAS**.
- Revisión de incidentes significativos y no conformidades relacionadas con IA, y definición de acciones correctivas y preventivas.
- Recomendación de ajustes a políticas, procedimientos y controles, en coordinación con LR&C e I&T Center.

- Articulación con la Oficina Global y, cuando corresponda, con reguladores.

Operación mínima:

- Periodicidad: sesión ordinaria trimestral y sesiones extraordinarias cuando se identifiquen eventos relevantes.
- Quórum: mayoría simple de sus miembros habilitados; las decisiones se documentan en actas y repositorios oficiales.

I&T Center: responsable del diseño, implementación y documentación de sistemas de IA desarrollados por la Firma; lidera las pruebas, validaciones y verificaciones conforme a la POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center y coordina con IT y Seguridad de la Información los controles técnicos de seguridad. *Infraestructura y Tecnología (IT)*: responsable de la operación tecnológica, la interoperabilidad con la red **PARKER RANDALL COLOMBIA SAS** y la seguridad de la información durante el ciclo de vida de la IA, aplicando lineamientos del MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información **PARKER RANDALL COLOMBIA SAS**.

- *Seguridad de la Información:* define y supervisa controles de confidencialidad, integridad y disponibilidad, gestiona incidentes conforme al PRO-GSI-01 Procedimiento de Gestión de Incidentes de Seguridad de la Información e integra la gestión de riesgos de IA en la matriz corporativa. *LR&C (Legal, Risk & Compliance)*: monitorea el marco regulatorio de IA, actualiza el FOR-GSI-17 Matriz de Requisitos Legales SI, y asesora sobre obligaciones y ajustes necesarios para el cumplimiento. *Compras/SCM*: integra criterios de IA en la debida diligencia de proveedores conforme al PRO-SCM-03, exige transparencia técnica a terceros y coordina evaluaciones reforzadas para alto riesgo. *Ética e Independencia / IQ&R / SoQM (según aplique)*: vela por la alineación ética y de calidad, revisa casos de uso críticos y apoya la rendición de cuentas y mejora continua. Responsables de procesos / unidades de negocio: aseguran el uso conforme de la IA en sus procesos, la supervisión humana y la validación de resultados, reportando riesgos y no conformidades. *Responsables de procesos / unidades de negocio*: Aseguran el uso conforme de la IA en sus procesos, la supervisión humana y la validación de resultados; reportan riesgos y no conformidades. *Mecanismos de escalamiento*: Ante eventos relevantes (incidentes, desviaciones, riesgos emergentes), se debe escalar inmediatamente a Seguridad de la Información e IT; cuando el impacto incluya cumplimiento regulatorio o contractual, se notifica a LR&C; y si la legislación local impide cumplir la política, se comunica a la Oficina Global conforme al apartado de "Comunicación a la oficina global".

6.6.3 Políticas, Procedimiento y Marcos de Control

La gobernanza de IA se implementa mediante la articulación de políticas y procedimientos institucionales:

- Desarrollo seguro y ciclo de vida: POL-INV(ITR)-01 define controles técnicos, validaciones y documentación del desarrollo, despliegue, mantenimiento y retiro de sistemas de IA.

- Seguridad y privacidad: MAN-GSI(ITR)-01 establece clasificación de la información, controles de acceso, cifrado y custodia de datos; PRO-GSI-01 regula la gestión de incidentes.
- Gestión de riesgos: DOG-GEA-31 determina criterios para identificar, evaluar y tratar riesgos de IA, con énfasis en alto riesgo y decisiones automatizadas de alto impacto.
- Proveedores y terceros: PRO-SCM-01 incorpora criterios específicos de IA en la debida diligencia inicial y periódica (transparencia del modelo, datos de entrenamiento y métodos de validación).
- Cumplimiento normativo: LR&C mantiene actualizada la matriz de requisitos y coordina ajustes de controles ante cambios regulatorios.

Estos instrumentos conforman el marco de control que asegura coherencia entre diseño técnico, seguridad, cumplimiento, ética y operación.

6.6.4 Atribuciones de Supervisión del Comité de IA

El Comité de IA ejerce supervisión estratégica y de alineamiento sobre los mecanismos ya definidos en la Firma, sin sustituir los procedimientos operativos existentes. En particular:

- Inventario y ciclo de vida (ver 6.5): revisa consolidado trimestral del inventario y cambios relevantes del ciclo de vida; solicita medidas cuando identifique riesgos transversales o dependencias críticas.
- Evaluaciones de impacto y riesgos (ver 6.5 y DOG-GEA-31): valida criterios aplicados en sistemas de alto riesgo, especialmente cuando involucren decisiones automatizadas de alto impacto; puede requerir evaluaciones adicionales o medidas de tratamiento.
- Auditorías y verificaciones (ver 6.5): conoce hallazgos y planes de acción de auditorías internas/externas relacionadas con IA; verifica su cierre oportuno y la consistencia con esta Política.
- Actualización normativa y de políticas (ver Cumplimiento y LR&C): coordina con LR&C para aterrizar cambios regulatorios en políticas/procedimientos de IA; prioriza acciones y comunica impactos a las áreas responsables.

6.6.5 Articulación y Comunicación Institucional del Comité de IA

El Comité de IA asegura que la comunicación sobre IA sea coherente y oportuna, articulando con los propietarios de proceso:

- Interna (ver 6.10 y Cumplimiento): divulgar decisiones estratégicas, cambios relevantes y lecciones aprendidas a socios y personal mediante los canales oficiales; integrar contenidos en los planes de capacitación por roles.
- Clientes y proveedores (ver 6.2.3 y 6.11): validar mensajes clave sobre uso de IA y asegurar que Compras/SCM exija notificación formal de cambios relevantes de IA; cuando haya impacto transversal o alto riesgo, el Comité avala el plan de comunicación.
- Oficina Global y reguladores (ver Comunicación a la oficina global): coordinar reportes y notificaciones cuando existan restricciones legales o casos de alto riesgo con impacto

regional; canalizar solicitudes de información que requieran visión integral de la gobernanza.

6.6.6 Supervisión de Incidentes y No Conformidades

La gestión operativa de incidentes de información y no conformidades de IA se realiza conforme al PRO-GSI-01 y a Cumplimiento de esta política.

Bajo lo anterior, el Comité de IA:

- Monitorea los incidentes significativos y los riesgos materializados de IA (consolidado trimestral), y verifica la eficacia de acciones correctivas/preventivas.
- Prioriza acciones transversales de mejora cuando detecte tendencias (p. ej., debilidades de control repetitivas, fuentes de datos problemáticas, sesgos recurrentes).
- Escala a la Oficina Global o LR&C cuando el incidente implique limitaciones regulatorias o reputacionales de amplio impacto.

6.7 SEGURIDAD Y FIABILIDAD

6.7.1 Diseño seguro y funcionamiento confiable

Los sistemas de inteligencia artificial desarrollados por la firma operan de manera estable, segura y precisa, en condiciones normales y también en situaciones que puedan preverse.

Los sistemas de IA deben proteger la información, evitando vulnerabilidades y minimizando los riesgos para los usuarios. Adicionalmente dicho sistema debe mantener un rendimiento estable y sin fallos frecuentes. Los resultados generados deberán ser consistentes y verificables.

6.7.2 Identificación de fallos previsibles y planes de contingencia

La firma identifica fallos previsibles en los sistemas de inteligencia artificial y define medidas de mitigación y planes de contingencia que permitan responder de manera adecuada a estos escenarios, minimizando impactos sobre la operación y la información.

Cuando un evento asociado al uso de IA genere un impacto sobre la confidencialidad, integridad o disponibilidad de la información, dicho evento será tratado como un riesgo materializado conforme al DOG-GEA-31 Metodología para la Gestión de Riesgos, y cuando corresponda a un incidente de seguridad de la información, será gestionado conforme al PRO-GSI-01 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

6.7.3 Resiliencia frente a manipulaciones o usos indebidos

Cuando los sistemas de IA sean desarrollados por la firma, deberán ser creados para resistir intentos de manipulación o uso incorrectos, ya sea que ocurran de manera deliberada o accidental. Los sistemas deberán contar con mecanismos de seguridad que impidan que alguna persona lo altere con fines maliciosos.

La firma hace uso de componentes de Inteligencia Artificial (IA) integrados en herramientas corporativas; sin embargo, no desarrolla ni implementa modelos de lenguaje (LLM) ni otros

desarrollos propios de IA. Además, trabaja en coordinación con el área de Infraestructura y Tecnología (IT) para la revisión de la seguridad de la información.

La firma aplica controles para prevenir manipulaciones, usos indebidos o alteraciones no autorizadas de los sistemas de inteligencia artificial, en coordinación con el área de IT y conforme a los lineamientos técnicos definidos por la firma.

6.7.4 Pruebas y validaciones continúas

La firma realiza pruebas y validaciones continuas sobre los sistemas de inteligencia artificial que utiliza, con el fin de asegurar que mantienen el comportamiento esperado y se ajustan a los usos definidos.

Los resultados de estas pruebas se documentan y conservan conforme a los lineamientos internos aplicables.

6.8 SEGURIDAD Y SOLIDEZ

6.8.1 Seguridad y robustez frente a amenazas y ataques

La firma adopta medidas de seguridad integrales para que los sistemas de inteligencia artificial sean robustos frente a amenazas o ataques que puedan comprometer su integridad, funcionalidad o disponibilidad, aplicando controles de seguridad durante todo su ciclo de vida.

Los controles definidos para asegurar estas medidas de seguridad se ejecutan teniendo en cuenta lo establecido en el documento POL-INV(ITR)-01 Política de Desarrollo Seguro para I&T Center.

6.8.2 Compatibilidad e interoperabilidad con la red PARKER RANDALL COLOMBIA SAS

La firma asegura que los sistemas de inteligencia artificial utilizados sean compatibles e interoperables con los sistemas, procesos y arquitecturas tecnológicas de la red **PARKER RANDALL COLOMBIA SAS**, evitando impactos negativos sobre la calidad o disponibilidad de los servicios corporativos.

6.9 CUMPLIMIENTO DE LA LEGISLACIÓN LOCAL APLICABLE

La firma cumple con la legislación, regulación o norma local vigente y aplicable relacionada con el desarrollo, adopción, implementación y uso de sistemas de inteligencia artificial, en las oficinas de Interaméricas. Cuando no exista una regulación suficiente o dicha regulación no cumpla con los estándares definidos en la política global sobre uso responsable de la IA, la firma se rige por lo dispuesto en la presente Política. Si la regulación local establece un nivel de protección más alto, aplica ese estándar superior.

El área de LR&C monitorea al menos cada seis meses, o cuando se requiera, el marco regulatorio en materia de IA mantiene actualizada la Matriz de Requisitos Legales en el FOR-GSI-17 y comunica oportunamente a las áreas involucradas los cambios normativos necesarios para asegurar el cumplimiento integral y actualizado dentro de la Firma.

Nota: **PARKER RANDALL COLOMBIA SAS** revisa de manera periódica los lineamientos emitidos por la Superintendencia de Industria y Comercio (SIC) y por las autoridades competentes en los países donde opera, con el fin de identificar los criterios y obligaciones generales aplicables al desarrollo, adopción, implementación y uso de sistemas de inteligencia artificial; estos lineamientos sirven como base para la estructuración y actualización de esta Política, asegurando que se mantiene alineada con las mejores prácticas y exigencias regulatorias vigentes.

6.10 CUMPLIMIENTO DE ESTA POLÍTICA

La firma es responsable de asegurar el cumplimiento de esta Política en todas las oficinas de Interaméricas, disponiendo de los recursos, controles y mecanismos de seguimiento necesarios para su correcta implementación y mejora contínua.

Cualquier uso indebido de sistemas de IA o evento que implique exposición, alteración o uso no autorizado de información deberá ser reportado a través de los canales oficiales, registrado conforme a los lineamientos de registro y trazabilidad del MAN-GSI(ITR)-01 Manual de Políticas Específicas de Seguridad de la Información

, y gestionado de acuerdo con el PRO-GSI-01 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

6.11 ALFABETIZACIÓN Y FORMACIÓN EN IA

6.11.1 Capacitación general en uso responsable de IA

La firma incluye en el plan anual de capacitación, formación sobre el uso responsable de la inteligencia artificial dirigidas a todos los profesionales de las oficinas de Interaméricas, asegurando una comprensión básica de los riesgos, responsabilidades y buenas prácticas asociadas al uso seguro y ético de la IA.

Esta capacitación es impartida por personal especializado en temas de inteligencia artificial de la firma, en conjunto con el área de ética e independencia y coordinado por el área de P&C, la cual llevará todos los controles del proceso de formación.

6.11.2 Capacitación específica según roles y contextos

La formación en inteligencia artificial, enfocada en su uso responsable, se dirige al personal de acuerdo con el contexto de su rol. Su propósito es asegurar que todos los profesionales adquieran un nivel básico de conocimientos, comprendan el impacto en terceros y reconozcan las implicaciones éticas y prácticas de la IA.

Así mismo, esta capacitación considera el nivel técnico, la experiencia, la educación y la formación de cada profesional de la firma, de modo que se adapte a sus necesidades específicas y promueva una comprensión adecuada del uso seguro y responsable de la inteligencia artificial.

6.12 DEBIDA DILIGENCIA DE LOS PROVEEDORES

6.12.1 Proceso de debida diligencia para proveedores con IA

La firma tiene establecidos mecanismos de control para asegurar que los proveedores de servicio que, suministren, implementen o utilicen sistemas de inteligencia artificial en la prestación de servicios o productos a la firma, con el fin de que lo hagan de manera segura, responsable y conforme a las políticas internas de la firma. Los lineamientos para llevar a cabo este proceso se encuentran definidos en el documento PRO-SCM-03 Procedimiento de Debida Diligencia de Proveedores de Bienes y Servicios y se realiza en el marco de la para la evaluación inicial previo a la contratación del proveedor y periódica (anual) de los proveedores de servicio.

En este procedimiento se incorporan criterios específicos relacionados con el uso de IA, de manera que la debida diligencia cubra tanto los aspectos generales del proveedor como los riesgos y controles asociados a la inteligencia artificial.

6.12.2 Evaluación de proveedores de alto riesgo.

Cuando un proveedor utilice sistemas de inteligencia artificial clasificados como de alto riesgo, la firma realizará una evaluación reforzada conforme al PRO-SCM-03. Esta evaluación incluirá criterios adicionales relacionados con la gobernanza y uso de la IA, la transparencia del sistema, los usos aceptables e inaceptables, los incidentes y riesgos conocidos, y estará alineada con los principios de esta Política.

La profundidad de la evaluación se ajusta al nivel de riesgo asociado al uso de IA en los servicios o productos contratados.

6.12.3 Mecanismos de notificación de cambios relevantes

La firma exige a sus proveedores la existencia de mecanismos formales para notificar cualquier cambio significativo en sus sistemas o prácticas de inteligencia artificial que pueda afectar los principios y requisitos de seguridad, ética y cumplimiento establecidos en la política.

Estos cambios incluyen, entre otros, modificaciones relevantes en los modelos de IA, en el tratamiento de datos o en los controles de seguridad y privacidad, y se comunican a través de los canales definidos en el PRO-SCM-03, pudiendo dar lugar a nuevas evaluaciones de debida diligencia o a la adopción de medidas contractuales adicionales.

6.12.4 Registros de la debida diligencia en IA

La firma conserva registros completos y trazables de todas las actividades de debida diligencia y de las evaluaciones realizadas a proveedores relacionadas con el uso de sistemas de inteligencia artificial, especialmente aquellos clasificados como de alto riesgo. Estos registros, incluidos formularios, evidencias, decisiones de aceptación, condicionamiento o rechazo, así como comunicaciones relevantes, serán almacenados en los repositorios definidos, conforme a lo establecido en el PRO-SCM-03 y bajo la custodia de los responsables designados.

6.13 COMUNICACIÓN A LA OFICINA GLOBAL

La firma notificará de forma inmediata a la oficina global cuando determine que la legislación local aplicable, o las normas y obligaciones profesionales, le impiden cumplir o afectan de manera sustancial su capacidad para cumplir con las obligaciones establecidas en esta Política.

PROPIEDADES DEL DOCUMENTO

Elaborado por: Ana Milena García – Manager IQ&R Interaméricas Revisado por: Olga Montejo – Directora IQ&R Interaméricas Aprobado por: Fredy Castro – Líder SoQM Interaméricas