GRUPO COLPATRIA

POLÍTICA USO RESPONSABLE Y GOBIERNO DE LA INTELIGENCIA ARTIFICIAL

Grupo Empresarial Colpatria • Versión 01

La IA propone. Las personas validan, deciden y responden.

01 OBJETIVO

Innovar de forma segura, mejorar la eficiencia y el servicio, proteger los derechos y gestionar los riesgos de IA dentro del SIAR.

02 OCHO PRINCIPIOS

1. Centralidad de la persona y supervisión humana.
2. Legalidad y privacidad.
3. Equidad y no discriminación.
4. Transparencia y explicabilidad.
5. Seguridad, robustez y fiabilidad.
6. Prevención del daño.
7. Rendición de cuentas y trazabilidad.
8. Innovación responsable y sostenible.

03 MODELO DE GOBIERNO

- **Junta Directiva:** aprueba la política y sus cambios.
- **Comité Estratégico:** autoriza excepciones permitidas.
- **Comité Ejecutivo:** decide casos de riesgo alto y retiros por riesgo inaceptable.
- **Subcomité de Riesgos y Auditoría:** supervisa y recomienda; no aprueba.
- **VP de Transformación y Datos:** administra catálogo e inventario y aprueba riesgo moderado y bajo.
- **Riesgos, Legal, Protección de Datos y Seguridad:** validan según su competencia; **Auditoría** evalúa de forma independiente.

RESPONSABLES

El dueño de la solución responde por todo su ciclo de vida. Quien utiliza un resultado responde por él y debe verificarlo.

04 HERRAMIENTAS E INFORMACIÓN

- Usa el catálogo autorizado de SharePoint y tu cuenta corporativa personal.
- Las funciones de IA embebidas también requieren autorización.
- **Pública e interna:** admisibles en herramientas autorizadas.
- **Confidencial:** solo en herramientas habilitadas para ese nivel.
- **Datos personales:** caso aprobado, base legal y mínimo necesario.
- **Datos sensibles, biométricos o de menores:** riesgo alto aprobado y controles reforzados.
- Nunca ingreses claves, contraseñas ni tokens.
- No cargues información interna, confidencial o personal en herramientas no autorizadas.

05 REGLAS Y LÍMITES

- Verifica exactitud, vigencia y sesgos.
- Declara el uso de IA en comunicaciones formales y a terceros; etiqueta contenido sintético.
- Respeta la propiedad intelectual y minimiza datos.
- La IA puede apoyar tareas aprobadas; no sustituye el juicio humano ni decide de forma totalmente automatizada con efectos jurídicos o significativos.
- En decisiones críticas una persona valida antes de ejecutar; debe poder corregir o detener el sistema.
- Explica los resultados relevantes en lenguaje comprensible.

06 GESTIÓN DE RIESGOS

Registrar → clasificar → evaluar impacto → aprobar → probar → monitorear → retirar de forma segura.

- **Extremo:** prohibido, nunca se aprueba.
- **Alto:** Comité Ejecutivo, evaluación completa, pruebas de sesgo y robustez, validación humana de cada decisión y monitoreo al menos trimestral.
- **Moderado:** VP de Transformación y Datos, evaluación simplificada, transparencia, supervisión y monitoreo semestral.
- **Bajo:** catálogo autorizado o visto bueno correspondiente, inventario y verificación humana.
- Reevaluar ante cambios; detectar y corregir sesgos durante todo el ciclo.

07 PRIVACIDAD Y CIBERSEGURIDAD

- Finalidad informada, autorización o base legal y privacidad desde el diseño.
- Estudio de impacto de privacidad para alto riesgo con datos personales.
- Acceso con mínimo privilegio, cifrado, trazabilidad y prevención de fugas.
- Proteger modelos frente a inyección de instrucciones y envenenamiento de datos.
- Controlar retención, entrenamiento y transferencias por proveedores.
- Permitir explicación y revisión humana de decisiones.
- **Contacto:** oficialdatospersonales@grupocolpatria.com.

08 USOS PROHIBIDOS

- No usar, desarrollar, adquirir ni implementar IA para manipular perjudicialmente, explotar vulnerabilidades, realizar puntuación social perjudicial o vigilancia biométrica sin base legal y aprobación.
- Prohibidas la categorización biométrica sensible, la extracción indiscriminada de imágenes para reconocimiento facial y las predicciones delictivas basadas solo en perfiles.
- No inferir emociones en el trabajo salvo razones médicas o de seguridad.
- No automatizar decisiones significativas sin intervención humana, producir suplantaciones engañosas ni eludir controles.
- La política toma como referencia el artículo 5 del Reglamento Europeo de IA y añade prohibiciones propias.

09 INCIDENTES

- Reporta de inmediato a soporte@mercantilcolpatria.com o al canal de incidentes de TI; notifica a Riesgos cuando aplique.
- Preserva evidencias → contiene o pasa a operación manual → informa a Seguridad y Transformación y Datos; si hay datos personales, a Protección de Datos → corrige y reevalúa antes de reactivar.
- Los incidentes relevantes llegan al Subcomité.
- El reporte de buena fe está protegido frente a represalias.

10 SOSTENIBILIDAD

- Modelo de menor tamaño y consumo que cumpla los requisitos.
- Revisión anual de herramientas sin uso.
- Preferencia por energía renovable y proveedores de menor impacto, sin comprometer privacidad ni seguridad.

APROBACIÓN

Aprobada por la Junta Directiva de Mercantil Colpatria S.A., previa recomendación del Subcomité de Riesgos y Auditoría.

Grupo Colpatria

Fuente: Política Uso Responsable y Gobierno de la Inteligencia Artificial, versión 01.
Síntesis informativa; no sustituye la política.

ABRIMOS CAMINOS HACIA EL PROGRESO