GrupoMéxico
TRANSPORTES

Política Corporativa de Uso y Desarrollo de Inteligencia Artificial

1. Objetivo

Establecer los principios, lineamientos, responsabilidades, controles y restricciones para el uso, adquisición, desarrollo, entrenamiento, implementación y operación de sistemas de Inteligencia Artificial (IA) dentro de la organización, garantizando:

- La protección de la información y la ciberseguridad.
- El cumplimiento regulatorio y contractual.
- El respeto a los derechos de las personas y la privacidad de los datos.
- La mitigación de riesgos operativos, éticos y reputacionales.
- La transparencia, trazabilidad y supervisión humana de los sistemas de IA.
- El uso responsable y sostenible de tecnologías de IA.

2. Alcance

La presente política aplica a:

- Todas las unidades de negocio y subsidiarias de Grupo México Transportes (GMXT).
- Todos los colaboradores, directivos, contratistas, proveedores y terceros autorizados.
- Cualquier herramienta, modelo, plataforma o servicio de IA utilizado o desarrollado por GMXT, incluyendo:
  - IA generativa.
  - Machine Learning.
  - Modelos predictivos.
  - Automatización inteligente.
  - Modelos entrenados internamente.
  - Servicios SaaS con capacidades de IA.
  - APIs y plataformas de terceros, tales como las que procesan:
    - Base de datos con información interna, no pública.
    - Fuentes de datos: cámaras, telefonía, videoconferencias, telemetría, GPS.
    - Información estructurada o no estructurada.
    - Información de terceros no publicada o autorizada.
- En el caso de infraestructura tecnológica, se incluyen los siguientes ambientes:
  - Productivo
  - Desarrollo.
  - Pruebas.
  - Sandbox.
  - Cloud y on-premise.

3. Principios Rectores

Grupo México Transportes, como organización adopta los siguientes principios para el uso responsable de IA:

3.1. Supervisión Humana

Toda decisión derivada del resultado del uso y/o aplicación de la IA que pueda afectar a personas, clientes, colaboradores, proveedores, cumplimiento regulatorio, seguridad, finanzas, la infraestructura de GMXT, áreas civiles, ecosistemas naturales o comprometer el entorno futuro sin elementos sustentables, deberá contar con supervisión y validación humana.

La IA

- No sustituye la responsabilidad humana.
- No puede tomar decisiones autónomas irreversibles.
- Debe permitir intervención, corrección y reversión.
- Debe contar con trazabilidad de sus decisiones, uso y gestor de cada aplicación.
- Nunca debe de atentar contra la seguridad o vida de las personas.
- Será propiedad de GMXT cualquier desarrollo, iniciativa, producto, servicio o proyecto desarrollado, diseñado o ejecutado por empleados, ejecutivos, directivos, proveedores o terceros que presten servicios a GMXT.

3.2. Transparencia y Entendimiento

Todos los desarrollos, sistemas, esfuerzos y actividades que utilicen Inteligencia Artificial (IA) deberán:

- Documentar la lógica, propósito y alcance.
- Permitir explicar razonablemente los resultados esperados y la toma de decisiones.

- Mantener trazabilidad de la entrada de información, los modelos y resultados.
- Poder ser plenamente identificados como sistemas de IA.
- Todo modelo de IA deberá ser probado y validado por la Dirección de Transformación Digital antes de su implementación.
- El equipo técnico-funcional responsable y la Dirección del área con mayor impacto en el uso del modelo deberán verificar la razonabilidad, consistencia y veracidad de los resultados generados.
- Los modelos de alto impacto requerirán la aprobación de la Dirección General y del Comité Técnico.
- Los colaboradores podrán desarrollar y probar soluciones de IA con autorización de su Dirección y validación de la Dirección de Transformación Digital.
- La contratación, renta, adquisición o uso de herramientas de IA requerirá evaluación y certificación previa de la Dirección de Transformación Digital.

Queda prohibido el uso de modelos con un alto grado de opacidad en procesos críticos sin excepcion y haber considerado los puntos de transparencia y entendiemiento antes establecidos.

3.3. Privacidad y Protección de Datos

Toda implementación de Inteligencia Artificial deberá dar cumplimiento al marco normativo y regulatorio aplicable actualmente a Grupo México Transportes:

- Regulación del Sector Ferroviario
  - Ley Reglamentaria del Servicio Ferroviario y su Reglamento.
  - Normas Oficiales Mexicanas (NOMs) de la SCT
  - Regulaciones de la Agencia Reguladora del Transporte Ferroviario (ARTF).
  - Normativas de la Federal Railroad Administration (FRA) para los tramos operados en Estados Unidos.

- Normas de Seguridad, Medio Ambiente y Laborales
  - Ley Federal del Trabajo.
  - Ley General del Equilibrio Ecológico y la Protección al Ambiente (LGEEPA)
  - Normas de la STPS

- Marco Fiscal y Aduanero.
  - Código Fiscal de la Federación (CFF).
  - Ley Aduanera.
  - Ley del Impuesto Sobre la Renta (ISR).

- Gobierno Corporativo y Ética.
  - Disposiciones de la CNBV.
  - Ley del Mercado de Valores.
  - Manual de Gobierno Corporativo de GMXT.
  - Código de Ética de GMXT.

- La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Contratos de confidencialidad con socios, clientes y proveedores.

Se prohíbe:

- Introducir datos sensibles, confidenciales o regulados en herramientas públicas no autorizadas.
- Utilizar información personal sin base legal o consentimiento correspondiente.
- Reutilizar datos personales para entrenamiento sin autorización formal.

3.4. Seguridad y Ciberseguridad

Todo sistema de IA deberá incorporar controles de seguridad alineados con las políticas corporativas de ciberseguridad.

Los controles mínimos incluyen:

- Gestión de identidades y accesos.
- MFA para administradores.
- Cifrado en tránsito y reposo.
- Monitoreo y registro de actividad.
- Gestión de vulnerabilidades.
- Validación de integridad de modelos.
- Protección contra prompt injection, data poisoning y model theft.
- Segregación de ambientes.

3.5. Prevención de Sesgos y Uso Ético

Los modelos de IA deberán diseñarse y operarse minimizando:

- Discriminación.
- Sesgos injustificados.
- Exclusión indebida.
- Impactos desproporcionados.

Para mantener un correcto uso ético y optimizar de manera continua la operación minimizando sesgos, se deberán realizar de forma recurrente:
Evaluaciones periódicas de sesgo.

- Validaciones estadísticas.
- Revisiones multidisciplinarias.
- Monitoreo continuo de resultados.

3.6. Responsabilidad y Rendición de Cuentas

La responsabilidad sobre resultados generados por IA siempre recaerá en personas o áreas designadas por la organización.

La IA:

- No podrá ser considerada responsable legal.
- No sustituye aprobaciones formales.
- No reemplaza controles regulatorios.

Cada sistema, aplicación y/o herramienta de IA deberá tener:

- Dueño de negocio.
- Responsable técnico.
- Responsable de seguridad.
- Responsable de cumplimiento

La Dirección de Transformación Digital, a través del IA Squad Team, será responsable de la evaluación, certificación y seguimiento del uso, calidad, confiabilidad y propósito de las herramientas, servicios y soluciones de Inteligencia Artificial (IA) utilizadas en GMXT. Asimismo, supervisará la vigencia de las certificaciones otorgadas y establecerá, en coordinación con las áreas correspondientes, los costos, esquemas de almacenamiento, operación y responsabilidades asociadas a los ambientes digitales internos y externos propiedad de GMXT.

3.7. Sostenibilidad

La organización deberá promover:

- Uso eficiente de recursos computacionales.
- Selección de modelos energéticamente eficientes.
- Optimización de inferencia y entrenamiento.
- Evaluación del impacto ambiental de cargas intensivas de IA.

4. Clasificación de Sistemas de IA

Los sistemas de IA serán clasificados según su nivel de riesgo:

NIVEL	DESCRIPCIÓN	EJEMPLOS
Bajo	Sin impacto relevante en personas o decisiones críticas	Asistentes internos, generación de borradores
Medio	Soporte administrativo o analítico	Predicción de demanda, automatización documental
Alto	Impacto financiero, operativo, legal, regulatorio o humano	Riesgo crediticio, optimización de las operaciones, RRHH, fraude, salud
Prohibido	Uso no permitido	Vigilancia biométrica masiva, social scoring

5. Usos Permitidos para la IA

La organización considera apto el uso de herramientas de IA para:

- Automatización de tareas administrativas.
- Asistencia de lectura y análisis documental.
- Análisis de datos.
- Optimización de los procesos clave de la operación.
- Optimización de procesos financieros, administrativos y de soporte.
- Generación y optimización de código bajo revisión humana.
- Revisión, optimización e identificación de vulnerabilidades para mejora de controles de ciberseguridad.
- Soporte operativo.
- Atención a clientes supervisada.
- Detección de anomalías.
- Analítica avanzada.

Todo uso, herramienta, servicio o modelo de IA no contemplado en esta política requerirá, sin excepción, la autorización y certificación previa de la Dirección de Transformación Digital.

Lo anterior siempre y cuando:

- Existan controles aprobados.
- Se respeten límites regulatorios.
- La información utilizada esté autorizada.
- Se tenga supervisión humana en el desarrollo y validación.

6. Usos Restringidos

El desarrollo de sistemas de IA requiere autorización formal del Comité de IA y Riesgos cuando se presente una o más de las siguientes situaciones:

- Uso de datos sensibles.
- Modelos entrenados con información confidencial.
- IA con impacto en decisiones laborales.
- IA generativa conectada a información regulada.
- Modelos de auto aprendizaje en producción.
- Cualquier sistema, herramienta, servicio o modelo de IA que, a juicio de la Dirección de Transformación Digital (IA Squad Team), presente riesgos potenciales directos o indirectos que requieran evaluación y autorización del Comité de IA y Riesgos.

7. Usos Restringidos

Queda estrictamente prohibido el uso de la IA en los siguientes casos:

7.1. Prácticas Prohibidas

- Manipulación psicológica o conductual.
- Explotación de vulnerabilidades de personas.
- Social scoring.
- Vigilancia biométrica masiva no autorizada.
- Reconocimiento emocional sin base legal.
- Perfilamiento ilegal o discriminatorio.

7.2. Seguridad y Datos

- Uso de IA para evadir controles de seguridad.
- Generación de malware o ataques.
- Entrenamiento con datos robados o no autorizados.
- Compartir información confidencial con IA pública.

7.3. Operación Autónoma Crítica

- Toma autónoma de decisiones legales o financieras sin supervisión humana.
- Despliegue de modelos sin validación.
- Modificación automática de modelos en producción sin gobierno formal.

8. Gobierno Corporativo de IA

8.1. Comité de IA

La organización establecerá un Comité de Inteligencia Artificial integrado por representantes de las siguientes áreas de especialidad y direcciones:

- Tecnología – Dirección de Transformación Digital.
- Ciberseguridad – Dirección de Infraestructura Digital.
- Riesgos – Dirección de Finanzas.
- Cumplimiento – Dirección de Jurídico.
- Legal – Dirección de Jurídico.
- Auditoría – Dirección de Auditoría.
- Negocio – Dirección General de Administración, Dirección General de Operaciones, Dirección General Comercial.
- Protección de datos – Dirección de Jurídico.

Las funciones del Comité son:

- Aprobar iniciativas de IA.
- Evaluar riesgos.
- Autorizar excepciones.
- Supervisar cumplimiento.
- Revisar incidentes y sesgos.

9. Roles y Responsabilidades

La organización deberá comunicar el rol y responsabilidades a los colaboradores de la organización en cuanto a el desarrollo y uso de la IA:

ROL	RESPONSABILIDAD
Usuarios	Uso responsable y cumplimiento de política
Dueños de proceso	Validar resultados y riesgos
Transformación Digital	Desarrollo y validación técnica de aplicaciones de IA apegadas a la presente política
Infraestructura Digital	Infraestructura y operación
Ciberseguridad	Protección y monitoreo
Jurídico	Cumplimiento regulatorio
Auditoría	Verificación independiente
Comité IA	Gobierno y aprobación
IA Squad Team	Equipo especializado en IA con autoridad técnica y de certificación.

10. Requisitos para nuevos desarrollos de IA

Desde el punto de vista de Tecnologías de Información, todo desarrollo deberá incluir:

10.1. Documentación

- Objetivo del desarrollo, modelo y/o sistema.
- Descripción del conjunto de datos utilizados.
- Descripción de las variables consideradas.
- Definición de las Métricas.
- Riesgos identificados.
- Alcances y limitaciones conocidas.

10.2. Validación

- Validación técnica.
- Pruebas funcionales.
- Evaluación de sesgos.
- Validación de precisión.
- Evaluación de ciberseguridad.
- Pruebas UAT
- Aprobación de negocio.

10.3. Monitoreo

- Drift de modelos.
- Precisión.
- Incidentes.
- Uso indebido.
- Comportamientos anómalos.

11. Gestión de Terceros

Todo proveedor de Grupo México Transportes que desarrolle y/o haga uso de herramientas de IA deberá:

- Cumplir con los requisitos de seguridad corporativa.
- Permitir la evaluación de riesgos.
- Establecer los acuerdos de confidencialidad requeridos.
- Definir y comunicar el tratamiento de los datos utilizados.
- Informar la ubicación del resguardo y procesamiento de información.
- Garantizar la no reutilización indebida de información.

12. Gestión de Incidentes

Cualquier incidente relacionado con IA deberá reportarse inmediatamente a:

- Ciberseguridad.
- Riesgos.
- Cumplimiento.
- IA Squad Team

Estos incidentes incluyen de manera enunciativa, más no limitativa, eventos de:

- Fuga de información.
- Sesgos detectados.
- Resultados erróneos críticos.
- Uso indebido.
- Compromiso de modelos.
- Acceso no autorizado.

13. Auditoría y Cumplimiento

La organización podrá en cualquier momento:

- Auditar cualquier sistema de IA.
- Solicitar evidencia técnica y documental.
- Suspender modelos de alto riesgo.
- Revocar accesos.
- Aplicar sanciones disciplinarias.

14. Capacitación

Todo colaborador que utilice las herramientas, modelos o capacidades de IA deberá recibir capacitación sobre:

- Riesgos.
- Privacidad.
- Seguridad.
- Sesgos.
- Uso responsable.
- Límites permitidos.

15. Sanciones

El incumplimiento de esta política podrá derivar en:

- Suspensión de accesos.
- Medidas disciplinarias.
- Terminación contractual.
- Acciones legales.
- Reportes regulatorios.

16. Relación con Otras Políticas

Esta política complementa las políticas vigentes de Grupo México Transportes:

- Política de Seguridad de la Información.
- Política de Protección de Datos Personales.
- Política de Riesgos Tecnológicos.
- Código de Ética.
- Política de Desarrollo Seguro.
- Política de Gestión de Proveedores.

17. Vigencia y Revisión

La presente política deberá:

- Revisarse al menos una vez por año.
- Actualizarse ante cambios regulatorios o tecnológicos relevantes.
- Ser aprobada por la Alta Dirección y el Comité correspondiente.