



POLÍTICA DE USO INTELIGENCIA ARTIFICIAL (IA) GENERATIVA

PAZ CORP

Uso de herramientas de IA con información corporativa y de clientes.

Política	:	Política de Uso Inteligencia Artificial Generativa Paz Corp
Área responsable	:	Gerencia de Tecnología – AC DATA
Fecha elaboración	:	06 de octubre de 2026
Revisado por	:	Comité de Riesgos y Materias a fines en sesión N° 83 del 05 de octubre 2026
Aprobado por	:	Directorio Paz Corp en sesión N° 278 del 06 de octubre de 2026



CONTENIDO

1. Objetivo
2. Responsabilidad de Aplicación y Alcance
3. Reglas de uso
4. Protocolos Asociados
5. Procedimientos Asociados
6. Riesgos Mitigados
7. Anexos

1. OBJETIVO

Este documento establece los criterios, riesgos y reglas de uso aceptable para el empleo de herramientas de Inteligencia Artificial generativa (IA) — asistentes conversacionales, agentes y copilotos — dentro de PazCorp (Inmobiliaria Paz SpA / Constructora Paz), incluyendo sus operaciones en Chile y Perú.

El objetivo central es reducir el riesgo de exposición o uso indebido de información sensible al interactuar con modelos de IA de terceros, y establecer una ruta de adopción segura y gobernada, en línea con las obligaciones que impone la Ley N° 21.719 sobre Protección de Datos Personales y los marcos internacionales de gestión de riesgos tecnológicos. Asimismo, busca establecer los lineamientos para transitar de manera segura desde el control de procesos hacia el control de decisiones corporativas soportadas por IA.

2. RESPONSABILIDAD DE APLICACIÓN Y ALCANCE

Responsabilidad de la aplicación: Gerencia de Tecnología – AC Data

Alcance: Toda la Organización

3. REGLAS DE USO

3.1 Definiciones

- Inteligencia Artificial (IA): Sistemas informáticos capaces de ejecutar tareas que requieren inteligencia humana.
- Herramientas de IA: Plataformas, aplicaciones o sistemas basados en IA utilizados para apoyo en procesos.
- Información Sensible: Información personal, financiera, estratégica o confidencial.
- Proveedor de IA: Empresa o entidad que suministra soluciones basadas en IA.

3.2 Principios rectores

El uso de IA en Paz Corp se regirá por los siguientes principios:

- Transparencia y Explicabilidad.
- Responsabilidad y Rendición de Cuentas.
- Austeridad y Uso Eficiente de Recursos.
- Eficiencia Operacional.
- Cumplimiento Normativo.
- Protección de Datos Personales.
- Supervisión Humana Permanente.
- Creación de Valor Sostenible.
- Prevención de Sesgos y Discriminación.
- Seguridad Digital y Resiliencia Tecnológica.

3.3 Plataformas y uso de IA Permitidas

- Microsoft 365 Copilot (licencia corporativa del tenant Paz Corp): plataforma oficial, por estar integrada al entorno Microsoft 365 de la compañía.

Esta herramienta puede usarse para:

- Consultas, redacción y análisis sobre la información a la que el usuario tiene acceso legítimo.
- Automatización de tareas administrativas.
- Generación de reportes.
- Asistencia en capacitación y aprendizaje.

- Generación de imágenes y/o videos para comunicaciones internas o externas.
- Desarrollo de presentaciones, resúmenes y documentos.
- Creación de agentes en Microsoft 365 Copilot que apoyen a las distintas áreas en el trabajo con sus documentos e información corporativa (SharePoint, OneDrive, Teams, correo, entre otros), respetando los permisos de acceso de cada usuario, conforme al procedimiento de la sección 5.
- Siempre debe usarse bajo supervisión humana.

En plataformas de IA distintas a la mencionada sólo se pueden consultar: dudas técnicas genéricas, sintaxis, mejores prácticas o documentación pública.

Los datos personales de clientes y colaboradores solo podrán tratarse en Microsoft 365 Copilot, sobre información que ya reside en el entorno Microsoft 365 de Paz Corp y a la que el usuario tiene acceso legítimo, y para la misma finalidad para la que fueron recolectados.

El uso de ChatGPT (Business/Enterprise) y Claude (Team/Enterprise) bajo cuentas corporativas solo podrá autorizarse de manera excepcional, cuando exista una necesidad de negocio debidamente justificada que no pueda ser cubierta mediante Microsoft 365 Copilot.

En estos casos, el colaborador deberá solicitar la autorización a través de la Mesa de Ayuda, conforme al procedimiento de licencias establecido en el punto 5 de la presente política. La solicitud deberá contar con la aprobación de la Gerencia de Tecnología y del Gerente General antes de la contratación, asignación o uso de la herramienta.

No está permitido ingresar datos personales en ChatGPT, Claude u otras plataformas de inteligencia artificial, aun cuando se utilicen cuentas corporativas.

3.4 Usos Restringidos y Prohibidos

- Ingresar datos personales de clientes o colaboradores (RUT, nombres completos con datos de contacto, información financiera, contratos, historial médico o de salud, etc.) en ChatGPT, Claude o cualquier plataforma de IA distinta de Microsoft 365 Copilot, sea bajo cuenta corporativa, personal o gratuita (ver 3.3).
- El uso, copia, reproducción, extracción o recopilación de cualquier contenido, datos, textos, imágenes, código fuente o información disponible para el desarrollo, entrenamiento, prueba, validación o perfeccionamiento de modelos de inteligencia artificial, sin autorización de la Gerencia de Tecnología (no se considera entrenamiento el uso de información corporativa como fuente de consulta de agentes autorizados).
- Usar el botón de feedback (pulgar arriba/abajo) en cualquier plataforma de IA cuando la conversación contenga datos sensibles, ya que este mecanismo puede habilitar el uso de esos datos para entrenamiento incluso con la opción general desactivada.
- Compartir credenciales, tokens de API o claves de ningún sistema de Paz Corp con ninguna herramienta de IA.
- Ingresar información confidencial o estratégica en plataformas no autorizadas.
- Tomar decisiones finales de negocios u operacionales exclusivamente mediante IA.
- Utilizar IA para manipulación de información.
- Uso con fines personales no autorizados.
- Generar contenidos discriminatorios, engañosos o contrarios al Código de Ética de la Compañía
- Utilizar DeepSeek (web, app o API) en cualquier escenario corporativo (ver Anexo).

3.5 Configuración mínima obligatoria para quienes usen ChatGPT o Claude

- Desactivar el entrenamiento de modelos con datos de la cuenta (Settings → Privacy / Data Controls).
- Activar autenticación de doble factor (MFA) en la cuenta.

* Siempre consultar con el área de TI de la Compañía para asegurar que lo anterior sea efectivo.

3.6 Incidentes y Reportabilidad

El ingreso accidental de información confidencial en modelos no autorizados, o la detección de fallos críticos derivados de decisiones asistidas por IA, será tipificado como un incidente de ciberseguridad. Todo colaborador tiene la obligación de reportar estos eventos de manera inmediata a la Mesa de Ayuda y al mail encargadodecumplimiento@pazcorp.cl, activando los protocolos definidos en la Política de Gestión de Incidentes de Seguridad.

Adicionalmente, todo incidente de ciberseguridad relacionado con el uso de herramientas de Inteligencia Artificial deberá ser informado al Directorio, incluyendo una descripción del incidente.

3.7 Capacitaciones

La Gerencia de Recursos Humanos, en coordinación con la Gerencia de Tecnología, implementará programas de concientización. Estos módulos abordarán técnicas de “Prompt Engineering” seguro, conocimientos generales de IA, cómo prevenir e identificar alucinaciones algorítmicas, uso adecuado de las herramientas de IA y la responsabilidad sobre el uso de los datos corporativos frente a inteligencias artificiales.

3.8 Integración con otras políticas, protocolos, manuales, procedimientos y prácticas corporativas

Esta política se integra con otras políticas, protocolos, manuales, procedimientos y prácticas corporativas relacionadas con el buen gobierno corporativo, la gestión de riesgos, el cumplimiento normativo, la responsabilidad social empresarial y la sostenibilidad. Se establecen vínculos y sinergias entre estos documentos, y se promueve una visión integrada de la gestión empresarial basada en la ética, la transparencia y la responsabilidad. Además, se impulsa la colaboración transversal con todas las áreas de la empresa, para garantizar una implementación efectiva y coordinada de los documentos y prácticas relacionadas con la prevención de delitos.

3.9 Incumplimiento de la Política

El incumplimiento de esta política podrá ser considerado como un incumplimiento grave de las obligaciones del trabajador, pudiendo ser amonestado de conformidad al Reglamento Interno de Orden, Higiene y Seguridad.

Es deber de todo aquel que tenga conocimiento de cualquier violación a esta política, ponerse en contacto con la compañía a través del canal de denuncias:

- Correo electrónico a denunciasleyesanticorrupcion@pazcorp.cl
- Página web de la compañía ingresando a <https://www.paz.cl/relacion-inversionistas/ley-20393#canaldenuncia>, sección Canales de Denuncia, opción enviar denuncia por mail o enviar denuncia por formulario.

Siempre que exista alguna duda sobre el cumplimiento o posible incumplimiento de esta Política, debe consultarse al EPD (encargadodecumplimiento@pazcorp.cl), pidiendo su opinión en el tema sin necesidad que ésta sea emitida o enviada de manera formal.

3.10 Actualización de la Política

La presente Política será revisada semestralmente para asegurar su vigencia, efectividad y alineamiento con la normativa aplicable y las necesidades de la Compañía. Asimismo, podrá actualizarse en cualquier momento cuando existan cambios regulatorios, tecnológicos o de negocio que así lo requieran.

4. PROTOCOLOS ASOCIADOS

- Política de Privacidad y Tratamiento de Datos Personales.
- Política de Gestión de Incidentes de Seguridad

5. PROCEDIMIENTO DE LICENCIAS

- **Solicitud de licencias de IA:** El colaborador deberá solicitar la licencia de Microsoft 365 Copilot, ChatGPT o Claude a través de la Mesa de Ayuda, contando previamente con la aprobación de su jefatura directa. La Gerencia de Tecnología evaluará la solicitud en función de la necesidad del negocio, los riesgos asociados y las políticas vigentes de la compañía. Las solicitudes de licencias para ChatGPT o Claude requerirán adicionalmente la aprobación expresa del Gerente General. En caso de aprobación, procederá a la asignación de la licencia y de la cuenta corporativa correspondiente. Asimismo, la Gerencia de Tecnología será responsable de revocar el acceso y dar de baja la licencia cuando este deje de ser requerida para el desempeño de las funciones del colaborador o cuando este finalice su relación laboral con la compañía.
- **Autorización de conexión de aplicaciones:** cuando una herramienta de IA solicite acceso a la cuenta corporativa o a información de Microsoft 365 (consentimiento de administrador), el colaborador debe pedirlo a través de la Mesa de Ayuda. La Gerencia de Tecnología revisa los permisos solicitados, el proveedor y la necesidad del negocio, y aprueba o rechaza la conexión. Los colaboradores no pueden otorgar este acceso por su cuenta.
- **Creación y publicación de agentes:** el área interesada presenta la solicitud a la Gerencia de Tecnología indicando el objetivo del agente, las fuentes de información que utilizará y los usuarios que tendrán acceso. La Gerencia de Tecnología revisa los permisos de esas fuentes, desarrolla o habilita el agente, lo prueba y lo publica solo para los usuarios definidos. Cada agente tendrá un responsable del área y quedará registrado en un inventario que se revisará periódicamente.
- **Reporte de incidentes de IA:** todo colaborador que detecte que una herramienta o agente de IA le muestra información a la que no debería tener acceso, que ingresó por error información confidencial o datos personales en una plataforma no autorizada, o que un resultado de IA generó un error con impacto relevante, debe reportarlo de inmediato a la Mesa de Ayuda y al mail encargadodecumplimiento@pazcorp.cl, conforme al punto 3.6. La Gerencia de Tecnología suspenderá el agente o acceso involucrado, corregirá los permisos y evaluará, junto al EPD, si corresponde alguna notificación. Adicionalmente, todo incidente de ciberseguridad relacionado con el uso de herramientas de Inteligencia Artificial deberá ser informado al Directorio, incluyendo una descripción del incidente.

6. RIESGOS MITIGADOS

- **Riesgo de Confidencialidad y Exfiltración:** Compromiso y exposición no autorizada de activos de información críticos (datos personales y estratégicos de la compañía) mediante su procesamiento en modelos fundacionales externos.
- **Riesgo de Integridad en la Toma de Decisiones:** Adopción de resoluciones corporativas viciadas o perjudiciales derivadas de la dependencia y confianza ciega en resultados algorítmicos inexactos, falaces o no verificados empíricamente (alucinaciones).

- Riesgo de Ciberseguridad y Sesgo Algorítmico: Inyección de vulnerabilidades tecnológicas y sesgos sistemáticos en la infraestructura corporativa a través del despliegue de código fuente o contenido generado sin revisión bajo el principio de Security-by-Design.
- Riesgo Legal y Regulatorio: Exposición a contingencias jurídicas, daño reputacional y sanciones pecuniarias por inobservancia de los deberes fiduciarios exigidos por la Ley N° 21.719 sobre Protección de Datos Personales.

7. ANEXOS

- Comparativas de plataformas de IA evaluadas