Política de Uso Responsable de Herramientas de Inteligencia Artificial

---

1. Objetivo

El propósito principal de esta política es establecer los lineamientos, restricciones y responsabilidades asociados al uso de herramientas de Inteligencia Artificial (IA) dentro del entorno laboral de [Nombre de la Empresa]. Dada la creciente adopción de plataformas basadas en IA generativa, como ChatGPT, Copilot, Bard, entre otras, es fundamental proteger la integridad, confidencialidad y seguridad de la información corporativa.

Esta política busca promover un entorno de innovación responsable, en el que los colaboradores puedan beneficiarse del uso de tecnologías emergentes bajo un marco ético y seguro. Al mismo tiempo, establece límites claros respecto al uso de herramientas de IA externas no autorizadas, especialmente aquellas que operan fuera del entorno tecnológico controlado por la empresa. La finalidad es evitar la fuga de información sensible, prevenir riesgos reputacionales y garantizar el cumplimiento de regulaciones de privacidad y protección de datos personales.

Asimismo, esta política se alinea con los principios corporativos de seguridad de la información, gobernanza digital, transformación tecnológica y cumplimiento normativo, promoviendo una cultura de uso consciente y estratégico de las nuevas tecnologías.

---

2. Alcance

Esta política es de cumplimiento obligatorio para todo el personal vinculado a [Nombre de la Empresa], incluyendo, pero no limitado a: empleados de nómina, colaboradores bajo contrato temporal, pasantes, consultores externos, proveedores de servicios tercerizados y cualquier otra persona o entidad que tenga acceso a los sistemas, datos o procesos de la organización mediante recursos tecnológicos facilitados por la empresa.

La política aplica a cualquier tipo de actividad relacionada con el uso de plataformas de IA, independientemente del dispositivo o red que se utilice. Esto incluye el uso desde equipos corporativos, personales o móviles, ya sea dentro o fuera de las instalaciones físicas de la empresa, durante el horario laboral o fuera de este, siempre que la actividad esté relacionada con funciones, tareas o datos vinculados a la organización.

También se incluye dentro del alcance de esta política cualquier desarrollo, automatización, generación de contenido o análisis realizado a través de herramientas de IA, así como la capacitación o entrenamiento de modelos que utilicen datos provenientes de la empresa. Todo uso debe ser previamente evaluado y, de ser el caso, aprobado por el área de Tecnología, Seguridad de la Información o el Comité de Transformación Digital.

3. Lineamientos Generales

3.1. Uso Exclusivo de Herramientas de IA Corporativas

Queda estrictamente prohibido el uso de herramientas de Inteligencia Artificial que no hayan sido expresamente aprobadas por [Nombre de la Empresa]. Esto incluye plataformas accesibles vía web o por aplicaciones que operen fuera del entorno corporativo, como OpenAI ChatGPT, Google Bard, Anthropic Claude, Jasper, Midjourney, entre otras.

La organización proveerá acceso a soluciones de IA evaluadas en cuanto a seguridad, privacidad y alineación estratégica, que serán habilitadas únicamente bajo esquemas controlados. Todo desarrollo basado en IA deberá canalizarse por medio de estas plataformas oficiales, en coordinación con los equipos responsables de tecnología e innovación.

3.2. Prohibición de Ingreso de Información Corporativa a Herramientas Externas

Está terminantemente prohibido ingresar, copiar, transcribir o compartir información de carácter confidencial o estratégico en herramientas de IA externas. Esta restricción aplica a datos financieros, nombres de clientes o empleados, códigos fuente, información sobre proyectos internos, estrategias de negocio, contratos, planes de mercadeo, documentos legales, reportes internos, métricas de desempeño, y cualquier tipo de contenido sensible que pertenezca o esté relacionado con la empresa.

Dado que muchas plataformas de IA utilizan los datos ingresados para entrenar sus modelos, aún de manera anónima, existe el riesgo de exposición y uso no autorizado. Este tipo de prácticas representa una grave amenaza a la seguridad corporativa y será tratada como una falta crítica.

3.3. Promoción de una Cultura de Seguridad Digital

Todos los colaboradores deben fomentar activamente una cultura de uso ético, consciente y seguro de las tecnologías emergentes. El uso de IA debe siempre orientarse a mejorar la eficiencia operativa, la calidad del trabajo y la innovación, sin comprometer la protección de los activos de información ni los valores institucionales.

El área de Tecnología y/o Seguridad realizará capacitaciones periódicas para asegurar que los colaboradores comprendan los riesgos asociados al uso indebido de IA, y conozcan las herramientas habilitadas, así como las consecuencias del incumplimiento.

4. Sanciones

El incumplimiento de esta política constituye una infracción a las normas internas de [Nombre de la Empresa] y puede acarrear consecuencias disciplinarias proporcionales a la

gravedad de la falta cometida. Las sanciones se aplicarán conforme al Reglamento Interno de Trabajo, las políticas de seguridad de la información, y la legislación vigente en materia laboral y de protección de datos.

Entre las posibles sanciones se incluyen, pero no se limitan a:

- Amonestación verbal o escrita.
- Suspensión temporal de funciones o acceso a sistemas.
- Reasignación de responsabilidades o limitación de acceso a herramientas digitales.
- Terminación de la relación laboral o contractual por causa justificada, en caso de reincidencia o daño grave.
- Responsabilidad civil o penal si se comprueba que el uso indebido causó perjuicios financieros, legales o reputacionales a la organización.

La empresa se reserva el derecho de investigar cualquier actividad sospechosa o no autorizada relacionada con el uso de IA. Esto incluye auditorías de uso, revisiones de sistemas, trazabilidad de accesos y entrevistas al personal involucrado. En caso de detectar una transgresión a esta política, se activarán los protocolos internos de respuesta a incidentes, involucrando a las áreas de Recursos Humanos, Tecnología y Asesoría Legal.

Adicionalmente, cualquier persona que, de forma intencional o negligente, comprometa la seguridad de la información de la empresa mediante el uso inadecuado de plataformas de IA podrá ser reportada ante las autoridades competentes, si así lo exige el marco legal vigente.

---

5. Revisión y Actualización

Debido al constante avance de las tecnologías de Inteligencia Artificial y a la aparición de nuevas herramientas, esta política será revisada de forma periódica para asegurar su relevancia, aplicabilidad y coherencia con las mejores prácticas de seguridad, innovación y cumplimiento normativo.

La responsabilidad de la revisión y actualización de este documento recae en el Comité de Tecnología e Innovación, en conjunto con el área de Seguridad de la Información y Recursos Humanos. Estas instancias deberán evaluar al menos una vez al año (o antes si se presentan cambios significativos en el entorno tecnológico) la necesidad de modificar, añadir o eliminar disposiciones de la política.

Cualquier modificación será comunicada oportunamente a todos los colaboradores mediante los canales oficiales internos (correo institucional, intranet o reuniones de equipo), y se establecerá un período de actualización o capacitación obligatoria cuando las modificaciones afecten de forma sustancial los lineamientos o restricciones.

Los colaboradores deberán firmar o aceptar digitalmente las versiones actualizadas de esta política como condición para el uso continuo de las herramientas tecnológicas de la empresa. Su desconocimiento no exime de responsabilidad, por lo que es obligación de cada miembro de la organización mantenerse informado y actuar conforme a los lineamientos vigentes.

6. Aceptación y Compromiso

Todos los colaboradores, sin excepción, deberán leer, comprender y aceptar esta Política de Uso Responsable de Herramientas de Inteligencia Artificial como parte de su compromiso con la seguridad de la información, el cumplimiento normativo y la cultura de innovación de [Nombre de la Empresa]. La aceptación de esta política será considerada una condición indispensable para el uso de plataformas tecnológicas provistas por la organización.

La aceptación podrá realizarse mediante firma física, declaración escrita, consentimiento digital a través del correo institucional o mediante los mecanismos que la empresa disponga para formalizar el conocimiento de políticas internas. Una vez aceptada, se asumirá que el colaborador conoce los riesgos derivados del uso inapropiado de tecnologías de IA y se compromete a cumplir íntegramente con los lineamientos establecidos.

Este compromiso incluye:

- Utilizar únicamente herramientas de IA habilitadas o autorizadas por la empresa.
- Abstenerse de compartir o cargar información corporativa en plataformas externas.
- Actuar de forma ética, profesional y consciente ante el uso de tecnologías emergentes.
- Reportar inmediatamente cualquier uso indebido, sospechoso o violación de esta política.

El colaborador entiende que su responsabilidad es continua, no limitada al momento de la firma, y que el desconocimiento o falta de lectura de esta política no lo exime de sus obligaciones ni de las consecuencias por incumplimiento.

De igual forma, las jefaturas y líderes de equipo tienen la responsabilidad de asegurar que sus equipos estén debidamente informados sobre el contenido de esta política, promoviendo una cultura organizacional orientada a la seguridad digital y el uso estratégico de tecnologías innovadoras.