dezzai™

Política de uso de la Inteligencia Artificial en MMG

ÍNDICE

1 INTRODUCCIÓN

1.1 OBJETIVO

El objetivo de esta política es establecer las directrices y procedimientos para el uso seguro y responsable de la Inteligencia Artificial, dentro de la empresa. El objetivo de esta política es proteger la confidencialidad, integridad y disponibilidad de los datos procesados por Inteligencia Artificial y garantizar el cumplimiento de las leyes y normativas pertinentes.

Este objetivo incluye:

a) Garantizar el uso seguro y responsable de la Inteligencia Artificial en consonancia con los objetivos generales de ciberseguridad en la empresa.

b) Proteger la confidencialidad, integridad y disponibilidad de los datos procesados por Inteligencia Artificial.

c) Cumplir las leyes, reglamentos y normas del sector aplicables en materia de privacidad y seguridad de los datos.

d) Definir funciones y responsabilidades para la gestión y administración de Inteligencia Artificial.

e) Establecer controles de acceso y directrices de uso para Inteligencia Artificial.

f) Permitir una supervisión y un registro eficaces de las actividades de Inteligencia Artificial.

g) Establecer un proceso de respuesta a incidentes para abordar cualquier violación de la seguridad o incidente que afecte a Inteligencia Artificial.

h) Proporcionar programas de formación y concienciación para educar a los empleados sobre el uso seguro de Inteligencia Artificial.

i) Revisar y actualizar periódicamente esta política para reflejar los cambios en la tecnología, las amenazas y los requisitos empresariales

2 OBLIGACIONES

2.1 USO APROPIADO

Las Herramientas IA deben ser utilizadas exclusivamente para fines empresariales legítimos y en línea con las políticas y procedimientos de nuestra organización.

No se deben utilizar Herramientas IA para actividades ilegales, inmorales, discriminatorias o que puedan causar daño a terceros.

Los usuarios de Herramientas IA deben tratar la información generada por el modelo con confidencialidad y no compartirla sin la debida autorización.

La Inteligencia Artificial puede utilizarse para los siguientes fines dentro de la empresa:

a. Asistente general.

b. Ventas y generación de contactos.

c. Servicio de asistencia informática.

d. Investigación y análisis de datos.

e. Generación de documentos.

2.2 USO PROHIBIDO

Las siguientes actividades están estrictamente prohibidas cuando se utiliza herramientas de Inteligencia Artificial:

a. Consultas que involucren datos personales (por ejemplo, recuperación de información personal de clientes).

b. Compartir información confidencial: Los usuarios no deben compartir información confidencial o datos de la empresa.

c. Discutir datos de clientes: Los usuarios no pueden utilizar las herramientas para discutir o divulgar información sobre clientes sin autorización previa.

d. Copiar y pegar información sensible: Los usuarios no pueden copiar y pegar información sensible generada por herramientas de Inteligencia Artificial en aplicaciones o plataformas no seguras.

e. Dejar sesiones de herramientas de Inteligencia Artificial abiertas: Los usuarios deben cerrar las sesiones cuando no las estén utilizando para evitar accesos no autorizados.

f. Tratamiento de información sensible de la empresa[1]. En ese sentido, queda prohibido el uso de herramientas como **GitHub Copilot, Tabnine, Visual Studio IntelliCode, DeepCode, Replit Ghostwriter, Tabby y Kite**; esta lista es enunciativa más no

[1] Se entiende como información sensible cualquier dato relacionado con la imagen personal, dirección, números de teléfono, datos genéticos, correos electrónicos, redes sociales, entre otros datos personales. Así también como cualquier información sensible relacionada a la empresa.

limitativa, por lo que queda prohibido por igual el uso de cualquier otra herramienta cuya utilidad sea similar a las mencionadas anteriormente.

g. Acceso a bases de datos o sistemas internos.

h. Generación de contenidos para su difusión pública sin revisión.

i. Utilizar la Inteligencia Artificial en redes no seguras: No se debe utilizar la Inteligencia Artificial en redes no seguras o públicas que puedan comprometer la seguridad de los datos.

2.3 CAPACITACIÓN Y CONCIENCIACIÓN

Principios a considerar por los empleados en el uso de herramientas de Inteligencia Artificial:

- Transparencia y responsabilidad: Promover una cultura de transparencia al utilizar IA, asegurando que los usuarios comprendan las capacidades y limitaciones del modelo y sean conscientes de su responsabilidad en el uso adecuado de la tecnología.

- Privacidad y confidencialidad: Enfatizar la importancia de proteger la privacidad y confidencialidad de la información generada o compartida a través de IA, evitando revelar información sensible o confidencial sin la autorización adecuada.

- Verificación y comprobación: Fomentar la verificación y comprobación de la información generada por IA antes de tomar decisiones o realizar acciones basadas en ella. Hay que reconocer que la IA es una herramienta de asistencia y no debe considerarse como fuente definitiva o única de información.

- Sesgo y discriminación: Concienciar sobre la posibilidad de sesgos en los resultados de IA y la importancia de evitar el uso discriminatorio o injusto de la tecnología. Alentar a los usuarios a ser conscientes de los sesgos potenciales y a tomar medidas para mitigarlos.

- Uso ético: Destacar la importancia de utilizar IA de manera ética y responsable, evitando actividades ilegales, engañosas o perjudiciales. Fomentar la toma de decisiones éticas al interactuar con la tecnología y considerar el impacto en los usuarios y la sociedad en general.

- Seguridad de la información: Hacer hincapié en la importancia de mantener la seguridad de la información al utilizar IA, incluyendo prácticas como el manejo adecuado de contraseñas, la protección contra el acceso no autorizado y la adhesión a las políticas y controles de seguridad establecidos.

- Actualización y mejora continua: Fomentar la mentalidad de aprendizaje y mejora continua en el uso de IA, animando a los usuarios a mantenerse actualizados sobre las novedades, investigaciones y mejores prácticas en el campo de la IA, y a compartir conocimientos y experiencias para el beneficio de todos.

Las sesiones de formación relacionadas con la seguridad de la Inteligencia Artificial se llevarán a cabo semestralmente para educar a los empleados sobre el uso seguro y responsable de la Inteligencia Artificial. Se ofrecerán programas de concienciación adicionales para mantener informados a los empleados sobre las amenazas emergentes y las mejores prácticas.