Política Interna de Uso Seguro de Inteligencia Artificial

Directiva operativa y cláusulas de confidencialidad para el equipo de trabajo

Empresa: _____	**Fecha de entrada en vigor:** ____/____/2026
Ámbito: Todos los empleados, directores y contratistas	**Responsable de cumplimiento:** Dirección / RRHH

1. Objeto y alcance

Esta política establece las condiciones obligatorias para el uso de herramientas de Inteligencia Artificial generativa (modelos de lenguaje, asistentes y visión artificial) en el desempeño de tareas laborales. El objetivo es **aprovechar la productividad de la IA sin exponer secretos comerciales, datos de clientes ni incurrir en faltas legales o éticas**.

2. Cuentas autorizadas vs. Cuentas prohibidas

- **Cuentas corporativas obligatorias:** Solo se permite el uso de herramientas de IA contratadas o habilitadas oficialmente por la empresa (por ejemplo, planes Team/Enterprise o API keys corporativas).
- **Prohibición estricta de cuentas personales:** Queda prohibido utilizar cuentas personales gratuitas de ChatGPT, Claude, Gemini u otras plataformas para redactar documentos, analizar archivos o procesar información del negocio, dado que dichas plataformas pueden usar los datos ingresados para entrenar sus modelos públicos.

3. Clasificación de información: qué NUNCA ingresar

Bajo ninguna circunstancia se ingresará en un prompt o archivo adjunto a una IA:

Categoría de información	Ejemplos específicos	Consecuencia / Criterio
Credenciales y accesos	Contraseñas, tokens de API, accesos a servidores o homebanking	Falta grave. Riesgo crítico de intrusión.
Datos bancarios / tarjetas	Números de cuenta, CBU/CVU, tarjetas de crédito, claves fiscales	Prohibido por normativa financiera.
Datos identificables de clientes	Nombre y apellido junto con DNI, teléfono, dirección o correos	Violación de privacidad. Anonimizar.
Secretos del negocio	Estrategias de licitación, costos internos, código fuente exclusivo	Pérdida de ventaja competitiva.

Plantilla de gestión operativa y gobernanza KALKORA Labs. Adaptar a la normativa local aplicable.

4. Regla obligatoria de anonimización

Cuando se utilice IA para redactar propuestas, analizar situaciones comerciales o generar correos, el colaborador debe **anonimizar previamente todo dato sensible**. Reemplazar nombres reales por identificadores genéricos (ej: «Cliente A», «Inmueble X», «Importe $100») y recién al pegar el resultado final en el sistema interno completar los datos reales.

5. Validación humana obligatoria y principio de responsabilidad

PRINCIPIO DE RESPONSABILIDAD INELUDIBLE:
La IA es una herramienta de asistencia que genera **borradores**. La IA suele afirmar con total seguridad datos inexistentes o cálculos erróneos (alucinaciones).
El colaborador que envía, publica o firma un documento o mensaje es el único responsable de su veracidad, exactitud y tono. No se aceptará como justificación de un error operativo que «la IA lo redactó así».

6. Propiedad intelectual de lo producido

Todo contenido, código, análisis o procedimiento generado mediante el uso de herramientas de IA durante la jornada de trabajo o utilizando recursos de la empresa es de exclusiva propiedad de la empresa, sin derecho a reclamo o compensación adicional.

7. Protocolo ante incidentes o sospecha de fuga

Si por error se ingresó información confidencial o credenciales en una IA no autorizada, el colaborador debe **notificar de inmediato (plazo máximo: 2 horas)** a su superior para revocar credenciales y mitigar el incidente. La notificación transparente inmediata atenúa cualquier sanción administrativa.

8. Compromiso y firma del colaborador

Declaro que he leído, comprendido y recibido copia de la presente Política de Uso Seguro de Inteligencia Artificial, y me comprometo a cumplir estrictamente sus pautas en el ejercicio de mis funciones.

Nombre y Apellido: _____	**DNI / ID:** _____
Puesto / Área: _____	**Fecha:** _____ / _____ / 2026
Firma del Colaborador: _____	**Aclaración:** _____

Plantilla de gestión operativa y gobernanza KALKORA Labs. Adaptar a la normativa local aplicable.