Política de uso de inteligencia artificial en [NOMBRE DEL DESPACHO]

1. Objeto y alcance

La presente «Política de uso de inteligencia artificial» (en adelante, la «Política») tiene por objeto establecer el marco normativo interno que regula el acceso, selección, uso y supervisión de las herramientas de inteligencia artificial (IA) por parte del personal de [NOMBRE DEL DESPACHO] (en adelante, el «Despacho»).

Esta Política es de aplicación obligatoria para todos los empleados, colaboradores, becarios, pasantes y cualquier persona que actúe en nombre del Despacho, independientemente de su categoría profesional o relación contractual. El objetivo fundamental es garantizar que la adopción de tecnologías de IA se realice de manera ética, segura y conforme a la normativa vigente, protegiendo el secreto profesional, la confidencialidad de los datos de los clientes y la integridad de los servicios jurídicos y consultivos prestados.

2. Definiciones breves

Para los efectos de esta Política, se establecen las siguientes definiciones operativas:

- **IA generativa:** Sistemas de inteligencia artificial que generan contenido nuevo (texto, código, imágenes, audio o vídeo) basándose en patrones aprendidos de grandes conjuntos de datos. Incluye modelos de lenguaje grande (LLM), asistentes conversacionales y herramientas de creación asistida.
- **Herramienta autorizada:** Aplicación o plataforma de IA que ha sido evaluada, aprobada formalmente por la Dirección del Despacho y registrada en el inventario interno, cumpliendo con los requisitos de seguridad, privacidad y contractualidad exigidos por esta Política.
- **Dato confidencial:** Cualquier información relativa a clientes, asuntos, estrategias legales, datos personales (especialmente categorías especiales) o secretos comerciales del Despacho que, si se revelara, pudiera causar perjuicio a la parte interesada o vulnerar el secreto profesional y el deber de confidencialidad.

3. Herramientas autorizadas y prohibidas

El uso de herramientas de IA está estrictamente regulado. Queda terminantemente prohibido el uso de aplicaciones no listadas en el siguiente inventario, salvo autorización expresa y temporal por escrito de la Dirección.

HERRAMIENTA	USO PERMITIDO	CONDICIONES	RESPONSABLE
[NOMBRE HERRAMIENTA 1] (ej. Copilot Enterprise)	Redacción de borradores, resumen de jurisprudencia, análisis de documentos internos.	Solo con cuenta corporativa gestionada por TI. Prohibido el uso en modo gratuito o personal.	[Nombre del Responsable TI]
[NOMBRE HERRAMIENTA 2] (ej. ChatGPT Business)	Lluvia de ideas creativa, estructuración de argumentos generales, traducción de textos genéricos.	Exclusivamente para datos anonimizados. Prohibido pegar textos completos de expedientes.	[Nombre del Responsable Legal/Compliance]
Herramientas locales/offline	Procesamiento de datos sensibles en entornos aislados.	Requiere validación técnica previa para asegurar que no hay transmisión externa de datos.	[Nombre del Responsable TI]
Cualquier otra herramienta (ChatGPT gratuito, Gemini, Claude, etc.)	**PROHIBIDO** para cualquier dato relacionado con clientes o asuntos del Despacho.	No se permite el uso bajo ninguna circunstancia sin autorización expresa y contrato de encargado firmado.	Dirección General

4. Reglas de oro

Todo el personal debe adherirse estrictamente a las siguientes diez reglas fundamentales:

1. Nunca introducir datos identificativos de clientes, nombres reales, direcciones, números de expediente o información sensible en herramientas no autorizadas o públicas.
2. Verificar siempre la identidad y la naturaleza jurídica del proveedor de IA antes de cualquier interacción; asegurarse de que actúa como encargado del tratamiento si se procesan datos personales.
3. Anonimizar o pseudonimizar rigurosamente toda información antes de introducirla en una herramienta autorizada, sustituyendo nombres por códigos genéricos (ej. «Cliente A», «Empresa X»).
4. Considerar todo resultado generado por IA como un borrador preliminar; la responsabilidad profesional del contenido final recae exclusivamente en el abogado

o asesor que lo utilice.

5. No utilizar herramientas de IA para tomar decisiones automatizadas que afecten directamente a los derechos de los clientes sin intervención humana significativa y evaluación previa.
6. Mantener un registro básico de las interacciones significativas con IA cuando se trate de asuntos complejos, como evidencia del proceso de trabajo realizado.
7. Reportar inmediatamente cualquier fallo técnico, filtración de datos o comportamiento inesperado de la herramienta al departamento de Tecnología o Compliance.
8. No compartir credenciales de acceso a herramientas corporativas de IA con terceros ni utilizarlas en dispositivos personales no gestionados por el Despacho.
9. Respetar los derechos de propiedad intelectual y autoría; citar adecuadamente las fuentes cuando la herramienta proporcione referencias bibliográficas o jurisprudenciales.
10. Participar activamente en las sesiones de formación obligatoria sobre alfabetización en IA, comprendiendo tanto las capacidades como las limitaciones inherentes a estas tecnologías.

5. Datos de clientes y secreto profesional

El Despacho se rige por los principios de minimización de datos y limitación de la finalidad (art. 5 RGPD). Al utilizar herramientas de IA:

- **Anonimización:** Antes de cualquier entrada en un sistema de IA, el personal debe eliminar o modificar toda referencia directa e indirecta a personas físicas identificables, salvo que sea estrictamente necesario para el análisis jurídico y la herramienta autorizada cuente con garantías técnicas robustas.
- **Contrato de encargado (art. 28 RGPD):** El Despacho solo utilizará proveedores de IA en la nube que hayan firmado un contrato de encargo de tratamiento que garantice que los datos se procesarán exclusivamente según las instrucciones del Responsable y que se implementarán medidas de seguridad técnicas y organizativas adecuadas (art. 32 RGPD).
- **Secreto profesional:** En cumplimiento con el Estatuto General de la Abogacía y el deber de confidencialidad, cualquier filtración de información confidencial a través de una herramienta de IA puede vulnerar el deber de secreto profesional y dar lugar a responsabilidad disciplinaria y civil, además de constituir un incumplimiento grave de esta Política; puede acarrear responsabilidad civil y penal. El personal debe ser consciente de que los datos introducidos en herramientas públicas pueden ser utilizados para entrenar modelos futuros, comprometiendo irreversiblemente la confidencialidad.

6. Revisión humana obligatoria

Se establece el principio de «supervisión humana significativa». Todo resultado producido por una herramienta de IA (ya sea texto, análisis o recomendación) debe ser revisado, verificado y validado por un profesional cualificado del Despacho antes de ser utilizado en la comunicación con el cliente, en documentos oficiales o en estrategias legales.

La revisión debe incluir:

- Verificación factual de los datos presentados.
- Comprobación de la vigencia y aplicabilidad de la normativa citada.
- Detección de posibles sesgos o alucinaciones (información inventada).
- Ajuste del tono y estilo para garantizar la adecuación profesional.

Usar con un cliente un resultado no revisado se considera un incumplimiento grave de esta Política.

7. Transparencia con el cliente

El Despacho mantendrá una relación de transparencia con sus clientes respecto al uso de herramientas de IA. Cuando el uso de estas tecnologías sea relevante para la prestación del servicio (por ejemplo, en grandes volúmenes de revisión documental), se informará al cliente de manera clara y comprensible. Esta información podrá incluirse en las condiciones generales del encargo o en comunicaciones específicas, explicando cómo se protege la confidencialidad y cómo se garantiza la calidad del trabajo final mediante la supervisión humana.

8. Incidentes

En caso de que un empleado introduzca datos por error en una herramienta no autorizada o detecte una posible brecha de seguridad:

1. **Contención inmediata:** El empleado debe cerrar la sesión, eliminar los datos locales si es posible y notificar al departamento de Tecnología/Compliance de inmediato y, en todo caso, el mismo día.
2. **Evaluación de riesgo:** El Responsable de Protección de Datos evaluará si el incidente supone un riesgo para los derechos y libertades de las personas físicas.
3. **Notificación regulatoria:** Si procede, se notificará a la autoridad de control competente (AEPD) en un plazo máximo de 72 horas desde que se haya tenido constancia de la violación de seguridad (art. 33 RGPD).
4. **Comunicación al afectado:** Si el riesgo es alto para los clientes, se comunicará el incidente a los afectados sin dilación indebida (art. 34 RGPD).
5. **Documentación:** Se registrará el incidente en el registro de violaciones de seguridad, detallando las circunstancias, efectos y medidas correctoras adoptadas.

9. Formación

Conforme al artículo 4 del Reglamento (UE) 2024/1689 (AI Act), que exige un nivel suficiente de alfabetización en IA para el personal y demás personas que utilicen sistemas de IA en nombre del Despacho, este implementa un plan de formación continuo.

Esta Política se complementa con el «Plan de Formación por Puesto», disponible en la intranet del Despacho [ENLACE]. Dicho plan detalla las competencias específicas requeridas para cada rol (abogados, paralegales, administrativos) y establece las sesiones periódicas sobre:

- Funcionamiento básico de los modelos utilizados.
- Técnicas de *prompt engineering* seguras.
- Identificación de riesgos éticos y legales.
- Actualizaciones normativas.

La asistencia a estas formaciones es obligatoria y se considerará como evidencia del cumplimiento de la obligación de medios establecida por la normativa europea.

10. Responsabilidades y revisión anual

- **Dirección General:** Es responsable última de la aprobación de esta Política, la asignación de recursos para su implementación y la supervisión de su eficacia.
- **Responsable de Protección de Datos (RPD):** Supervisa el cumplimiento del RGPD y la normativa de IA, asesora sobre evaluaciones de impacto y gestiona incidentes.
- **Jefes de Departamento:** Velan por el cumplimiento de esta Política en sus equipos, fomentando una cultura de uso responsable y reportando necesidades de formación.
- **Personal:** Es responsable de cumplir las normas establecidas, participar en la formación y reportar incidencias.

Esta Política se revisará anualmente o cuando ocurran cambios significativos en la normativa (como el AI Act), en las herramientas tecnológicas utilizadas o en la estructura del Despacho. La versión vigente estará siempre disponible en [ENLACE A INTRANET].

11. Acuse de recibo

Yo, abajo firmante, declaro haber leído, comprendido y aceptado íntegramente el contenido de la «Política de uso de inteligencia artificial» de [NOMBRE DEL DESPACHO]. Entiendo que su incumplimiento puede acarrear sanciones disciplinarias conforme al régimen interno del Despacho y responsabilidades legales derivadas de la normativa vigente.

Nombre y Apellidos	Cargo / Departamento	Fecha de lectura	Firma electrónica o manuscrita
[Nombre Empleado 1]	[Cargo]	[DD/MM/AAAA]	_____
[Nombre Empleado 2]	[Cargo]	[DD/MM/AAAA]	_____
[Nombre Empleado 3]	[Cargo]	[DD/MM/AAAA]	_____
[Espacio para más firmas]			

[NOMBRE DEL DESPACHO] [Ciudad, Fecha]