

Política de uso de LLM corporativo - Empresa: CibersegurIA

Versión 1.0 – Julio 2025

Ruta del documento original: \NormativaInterna\PolíticasIA\ManualLLM.pdf

1. Objetivo

Esta política establece los principios y normas de uso del sistema de lenguaje natural basado en modelos LLM desplegado por CibersegurIA para la consulta automatizada de contratos, acuerdos marco y pliegos técnicos.

2. Alcance

Aplica a todos los empleados de CibersegurIA con acceso autorizado al sistema LLM interno para análisis de documentos contractuales. Incluye a miembros de los departamentos de proyectos, legal, compras, cumplimiento, y atención a cliente.

3. Descripción del sistema

El sistema LLM permite realizar consultas mediante lenguaje natural sobre una base documental indexada que contiene:

- Contratos activos firmados.
- Pliegos de licitaciones públicas ganadas.
- Anexos, SLA y condiciones particulares.

Ejemplo de pregunta al sistema: '¿Qué penalizaciones hay si se incumple el SLA del contrato ORC-22-GP? ¿Cuál es el tiempo de respuesta máximo para un ticket prioridad baja-media-alta?'

4. Principios de uso

4.1. Supervisión humana

- Ninguna respuesta del sistema puede considerarse vinculante.
- Toda información obtenida deberá ser revisada y validada por el responsable del contrato correspondiente.

4.2. Transparencia

- El sistema mostrará siempre la fuente documental asociada a la respuesta.
- Se incluirá un aviso legal permanente: 'Este sistema ofrece apoyo informativo, no asesoramiento legal'.

4.3. Confirmación de uso responsable

- En cada interacción, el usuario debe aceptar explícitamente esta cláusula: 'Confirmando que revisaré esta información con el responsable del contrato antes de tomar ninguna acción'.

4.4. Límites del sistema

- No se permite usar el sistema para:
 - Consultas relacionadas con personas físicas.
 - Análisis de contenido confidencial no preautorizado.
 - Cualquier fin ajeno al contexto contractual o profesional.

5. Registro y trazabilidad

- Todas las interacciones serán registradas, incluyendo:
 - Fecha y hora
 - Usuario interno
 - Pregunta realizada
 - Documento fuente referenciado

Los registros se almacenan durante 18 meses en la ruta:

`\LogsLLM\interacciones\YYYY\MM\`

Ejemplo: [2025-07-10 16:42:01] userID=MARodriguez | prompt='¿Quién firma el contrato de soporte del CSIRT?'

6. Responsabilidades

- El IA Officer de CibersegurIA es el responsable técnico y ético del sistema.
- El DPO supervisa el cumplimiento de privacidad y uso de datos.
- Cada jefe de departamento es responsable de la supervisión del uso correcto por parte de su equipo.

7. Formación obligatoria

- Todo usuario debe haber completado el curso 'Uso seguro y ético del sistema LLM' disponible en:
`\FormacionInterna\LLM2025\`
- Debe renovar dicha formación cada 12 meses.

8. Medidas disciplinarias

- El mal uso del sistema puede conllevar sanciones según el reglamento interno de CibersegurIA.

- Casos como:

- Uso sin revisión del responsable.
- Difusión externa de respuestas del sistema.
- Búsquedas repetidas sobre contenido restringido.

Podrán dar lugar a suspensión de acceso o expediente disciplinario.

9. Revisión de la política

- Esta política será revisada trimestralmente por el Comité de Gobernanza de IA.

- Las versiones actualizadas se almacenarán en:

\NormativaInterna\PolíticasIA\Historial\ManualLLM_v*.pdf