CENCADE

Manual

Uso de Agente de Inteligencia Artificial

Clave:	**SGIA-SI-MAN-023**
Versión:	**0**
Entrada en vigor:	**29-04-2026**
Clasificación:	**Público**

Elaboró	Revisó	Aprobó
Rafael Ramírez **Oficial de Seguridad de la Información** **29-04-2026**	**Alfredo Esponda** **Director General** **30-04-2026**	**Alfredo Esponda** **Director General** **30-04-2026**

1 Control de cambios

Versión	Entrada en vigor	Descripción de los cambios
0	29-04-2026	Creación de Manual

2 Propósito

Este documento tiene como objetivo proporcionar a los usuarios (colaboradores y clientes de Cencade) una guía clara sobre el uso, las capacidades y las limitaciones de los Sistemas y/o Agentes de IA para asegurar una interacción segura, eficiente y transparente, cumpliendo con los requisitos de la norma ISO/IEC 42001.

3. Identificación y Transparencia

Toda interacción con este sistema se realiza mediante un modelo de lenguaje automático. El agente siempre se identificará al inicio de la conversación como una Inteligencia Artificial. No es un ser humano y no posee criterio subjetivo; sus respuestas se basan exclusivamente en la base de conocimientos proporcionada por Cencade, y puede presentar sesgos inherentes a los modelos de lenguaje.

4. Alcance y Capacidades

El Agente de IA está diseñado específicamente para:

- Consultar información técnica dentro de los manuales institucionales autorizados.
- Responder dudas sobre procesos operativos alojados en SharePoint - Cencade Connect.
- Facilitar la localización de datos específicos en documentos extensos.

5. Limitaciones y Restricciones

Para garantizar la seguridad de la información, el usuario debe considerar las siguientes limitaciones:

Categoría	Descripción de la Limitación
Exactitud	La IA puede generar respuestas inexactas o "alucinaciones". Siempre valide la información crítica con el manual original.
Fecha de Corte	El agente solo conoce la información con la que ha sido entrenado hasta su última actualización.
Datos Personales	Queda estrictamente prohibido introducir datos personales sensibles (nombres, teléfonos, cuentas bancarias) en el chat.
Decisiones Críticas	El agente es una herramienta de consulta, no de asesoría legal, financiera o técnica vinculante.

6. Responsabilidades del Usuario

- Utilizar un lenguaje claro y profesional para obtener mejores resultados.
- Reportar cualquier respuesta coherente o sesgada al **Oficial de Seguridad de la Información**.
- No intentar manipular el comportamiento del bot mediante "Prompt Injection" o comandos de ingeniería social.

7. Soporte y Retroalimentación

Si detecta alguna anomalía, debe levantar un ticket en **Helpdesk CEN** seleccionando la opción **'Incidente de IA'**.

8. Sanciones

El mal uso del agente, como el intento de extracción de datos confidenciales o 'Prompt Injection', será sancionado conforme al reglamento interior de trabajo.

9 Vigencia

Este documento será vigente de forma indefinida, solo cuando surja un cambio que se requiera modificar el documento se deberá cambiar la fecha de la vigencia. Esto no implica que no se realicen las revisiones una vez por año.