



LISTA DE COMPROBACIÓN

Antes de conectar una IA a tu sistema de gestión: 35 comprobaciones

Lista de comprobación para que una IA lea tu ERP, tu CRM o tus informes con seguridad

LCR-IA-GUI-001 · v1.0 · octubre de 2026

Para quién es. Para una empresa que quiere que una IA (Claude, Gemini u otra) lea su ERP, su CRM o su herramienta de informes a través de un conector (el programa que deja a la IA consultar tu sistema, lo que en la jerga técnica se llama un servidor MCP), y no tiene claro qué dejarle hacer. La lista se pasa antes de conectar y se repasa cada vez que cambia algo: un sistema nuevo, un permiso nuevo o una versión nueva del conector.

Cómo se usa. Cada punto es una pregunta que se contesta con un sí y con una prueba. Si la respuesta es «creo que sí», cuenta como «no». Cada punto dice también quién lo contesta. Los de Dirección son decisiones de la empresa y, si el trabajo lo hace un proveedor, las preguntas que hay que hacerle. Los de Sistemas los comprueba quien administra el sistema.

El principio. La IA lee y no escribe. Si algún día tiene que escribir en el sistema, eso es otro proyecto, con su propia lista, y antes hay que revisar los contratos y los seguros que lo cubren.

De dónde sale. De un laboratorio con cuatro sistemas habituales (un ERP, un CRM, una herramienta de informes y una base de datos), cargados con datos inventados, a los que se conectó una IA en solo lectura. La mayoría de los puntos responde a algo que pasó allí, como un conector que quedó autorizado con el administrador sin avisar, un error que la herramienta presentaba como éxito o una contraseña que se podía leer en una tabla de configuración. No es una norma ni sustituye a la revisión de seguridad que cada empresa haga de sus sistemas. Es lo que conviene comprobar para no llevarse esas sorpresas en producción.

1 · Qué se expone

Qué datos puede ver la IA y por dónde podrían salir de la empresa.

□ 1.1 · Dirección · Hay una lista escrita de lo que la IA puede leer: sistemas, módulos y objetos. Lo que no está en la lista queda fuera.

Se comprueba: la lista existe, tiene fecha y la ha aprobado alguien con nombre (ver 3.1).

□ 1.2 · Sistemas · Las primeras pruebas se hacen con datos ficticios o con una copia, nunca en producción.

Se comprueba: hay un entorno de pruebas con datos inventados y unas respuestas conocidas de antemano, para saber si la IA acierta.

□ 1.3 · Sistemas · La IA no puede leer las credenciales guardadas en el sistema. Muchos sistemas guardan contraseñas de correo, de integraciones o de servicios en sus tablas de configuración.

Se comprueba: se buscan esas tablas y se bloquean con un permiso (por ejemplo, DENY SELECT sobre la tabla o la columna). Un filtro por el nombre del campo no basta, porque atrapa campos que no son secretos y deja pasar una contraseña guardada con otro nombre.

□ 1.4 · Sistemas · Las bases de datos y las empresas que no entran en el proyecto están bloqueadas en el acceso, no solo «sin usar».

Se comprueba: el usuario de la IA intenta conectarse a ellas y el sistema se lo niega (en SQL Server, DENY CONNECT).

□ 1.5 · Dirección · Se sabe qué datos personales llegan al modelo y dónde se procesan. Antes de conectar se leen las condiciones del modelo contratado, en qué país procesa los datos y si los usa para entrenar. Si llegan datos personales, hace falta además un contrato de encargo del tratamiento con el proveedor del modelo.

Se comprueba: hay una nota con el modelo, el plan contratado, la región y la cláusula de entrenamiento, y el contrato de encargo está firmado.

□ 1.6 · *Sistemas* · Se ha revisado qué herramientas anuncia el conector, aunque esté en modo lectura. Hay conectores en «solo lectura» que siguen ofreciendo al modelo herramientas para crear, modificar o borrar, y otros que reciben herramientas de escritura en una actualización.

Se comprueba: se listan las herramientas del conector y se anota cuáles son de escritura. Que no las pueda usar depende del punto 2.2.

□ 1.7 · *Sistemas* · Se sabe qué otras herramientas comparte la IA con el conector del sistema, y ninguna puede enviar datos fuera sin que una persona lo confirme. Que la IA solo lea no impide que lo leído salga de la empresa. Puede salir si en la misma sesión puede navegar, enviar correos o guardar ficheros en la nube. También si un texto guardado en el sistema (una nota, el correo de un cliente) lleva instrucciones escondidas y la IA las obedece, lo que se llama inyección de instrucciones.

Se comprueba: hay una lista de las herramientas activas en la sesión, con las que envían datos fuera marcadas, y cada una de ellas pide confirmación antes de enviar.

2 · Permisos

Con qué usuario entra la IA y qué puede hacer con él.

□ 2.1 · *Sistemas* · La IA entra con un usuario propio, de nombre inconfundible (por ejemplo, «Lector IA (solo lectura)»). Nunca entra con el usuario de una persona ni con el de un administrador. El usuario se crea con todos sus datos de perfil rellenos (idioma, zona horaria y compañía), porque algunos sistemas escriben en la ficha del usuario la primera vez que entra por el navegador si encuentran un dato vacío (Odoo, la zona horaria), y esa es una escritura que nadie ha pedido.

Se comprueba: después de autorizar, se pregunta al conector quién es su usuario. Hay que comprobarlo de verdad, porque en un navegador con la sesión de administrador abierta la autorización se concede al administrador sin avisar. Además, la ficha del usuario es la misma antes y después de su primera entrada.

□ 2.2 · *Sistemas* · Hay dos barreras contra la escritura: el conector en modo lectura y un usuario sin permiso de escritura en el sistema. Si una falla, queda la otra.

Se comprueba: se intenta crear, modificar y borrar por el conector y también directamente con el usuario (por la API o por SQL). Las dos vías tienen que fallar, y después se comprueba en el propio sistema que no ha cambiado nada. El mensaje de error no basta, porque hay herramientas que presentan un fallo como si hubiera ido bien, y al revés.

□ 2.3 · *Sistemas* · El usuario tiene un grupo o un rol hecho a medida, con lectura solo de lo que está en la lista del punto 1.1. No se usan roles amplios ya existentes.

Se comprueba: se listan sus grupos o roles y los permisos de cada uno.

□ 2.4 · *Sistemas* · Antes de cada autorización o reautorización se lee la pantalla de consentimiento. El fabricante puede cambiar sin avisar los permisos que pide su conector, y una reautorización puede ampliar lo que lee la IA sin que nadie lo haya decidido.

Se comprueba: se guarda una captura de la pantalla de consentimiento con la fecha. Si pide algo que no está en la lista del punto 1.1, no se autoriza hasta decidirlo.

□ 2.5 · *Sistemas* · La autorización se verifica con datos. Que el navegador diga «Authentication successful» no basta.

Se comprueba: el usuario del conector, los permisos del token y una lectura de prueba con una respuesta conocida.

□ 2.6 · *Sistemas* · Cada clave o token tiene anotada su caducidad y cómo se renueva. Algunos sistemas limitan la duración de las claves de los usuarios que no son administradores (en Odoo 19, la versión probada en octubre de 2026, 90 días).

Se comprueba: hay una tarea con fecha, anterior a la caducidad.

□ 2.7 · *Sistemas* · Las conexiones van cifradas, y cada excepción está acotada y anotada. Si el conector exige HTTPS, no se busca la manera de saltárselo. Si un sistema antiguo obliga a rebajar algo (por ejemplo, a TLS 1.0), la rebaja se limita a ese proceso y queda escrita.

Se comprueba: hay una lista de excepciones, cada una con su motivo y con cómo se deshace.

□ 2.8 · *Sistemas* · En la herramienta de informes, la IA lee con un rol de base de datos en solo lectura (transacciones de solo lectura y solo SELECT), y su usuario no puede guardar consultas, ni en las colecciones compartidas ni en la suya personal.

Se comprueba: un UPDATE y un INSERT lanzados desde la herramienta fallan, y guardar una pregunta también.

□ 2.9 · *Sistemas* · El usuario de la IA se distingue de los usuarios humanos en los informes del propio sistema. En algunos sistemas, entrar solo por la API cuenta como «ha iniciado sesión».

Se comprueba: el usuario de la IA se reconoce en la lista de usuarios por su nombre o por una marca, y se excluye al contar los usuarios humanos.

□ 2.10 · *Sistemas* · Si la IA maneja el navegador (para hacer clics, rellenar pantallas o capturarlas para un manual), lo hace con otro usuario, distinto del lector, y se trata como un usuario que puede escribir. Muchos sistemas esconden los botones a quien no tiene permiso de escritura, así que ese usuario necesita esos permisos. Que no escriba es una conducta, no una barrera, y las dos barreras del punto 2.2 no lo protegen.

Se comprueba: el usuario es propio y tiene un nombre inconfundible. Su contraseña está en el gestor de contraseñas y en ningún fichero. Después de cada uso se revisa qué registros creó o modificó (con una foto de antes como referencia), y al terminar se desactiva.

□ 2.11 · *Dirección* · Se sabe quién puede usar la IA conectada, y lo que lee la IA no supera lo que puede ver el que menos permisos tiene, o hay un usuario de IA por perfil. Las barreras anteriores protegen el sistema, no a la persona que pregunta. Si el usuario de la IA lee las nóminas y la usa todo el equipo, cualquier comercial puede preguntarle por los sueldos.

Se comprueba: hay una lista de quién usa la IA, y lo que lee su usuario cabe dentro de los permisos de cada una de esas personas (o cada perfil tiene su propio usuario de IA).

□ 2.12 · *Sistemas* · Las consultas de la IA tienen un límite de filas o de tiempo, o se hacen sobre una copia. Una consulta generada por la IA sin límite puede cargar el servidor de producción o sacar de una vez la base de clientes entera.

Se comprueba: una consulta de prueba que pediría todas las filas se corta en el límite, o se lanza contra la copia y no contra producción.

3 · Aprobaciones

Quién decide lo que lee la IA y con qué conector.

□ 3.1 · *Dirección* · Una persona de la empresa, con nombre, aprueba por escrito la lista del punto 1.1 y cada ampliación posterior: un sistema nuevo, un objeto nuevo o un permiso nuevo.
Se comprueba: hay un registro de aprobaciones con fecha y nombre.

□ 3.2 · *Sistemas* · La IA no amplía sus propios permisos ni recomienda hacerlo como paso siguiente. Si detecta que le falta acceso, lo dice como hallazgo («esto no se ha podido leer») y quien decide es una persona.
Se comprueba: las instrucciones de la IA lo dicen, y en sus informes no aparece «vuelva a autorizar el conector» como recomendación.

□ 3.3 · *Sistemas* · Se sabe quién ha hecho el conector, dónde funciona y qué versión se usa. Puede ser del fabricante del sistema o de la comunidad. Puede funcionar en los equipos de la empresa o en el servidor de un tercero, que entonces ve todos los datos que pasan por él.
Se comprueba: hay una nota con el autor del conector, dónde se ejecuta y la versión fijada, y nadie la cambia sin pasar por el punto 3.4.

□ 3.4 · *Sistemas* · Las nuevas versiones del conector o del servidor se revisan antes de instalarlas.
Se comprueba: hay un procedimiento de revisión, y después de actualizar se repiten las pruebas del punto 2.2.

4 · Registro

Qué queda escrito de lo que ha leído la IA.

□ 4.1 · *Sistemas* · Cada sesión de la IA deja su transcripción guardada: qué consultó, con qué herramienta y qué le devolvió. Las transcripciones llevan datos sensibles, así que se guardan en un sitio conocido y solo las leen las personas autorizadas.
Se comprueba: después de cada sesión, el fichero existe, y se sabe dónde está y quién puede abrirlo. Una sesión lanzada desde otra puede no guardar su transcripción si hereda su configuración, y a esas hay que limpiarles el entorno antes.

□ 4.2 · *Sistemas* · También queda registro en el lado del sistema (el log del ERP, de la herramienta de informes o de la base de datos), no solo en el de la IA.
Se comprueba: en el log del sistema se encuentra una consulta concreta de la IA.

□ 4.3 · *Sistemas* · Las transcripciones se revisan de vez en cuando para buscar lecturas de lo prohibido (credenciales, bases fuera del alcance).
Se comprueba: hay una fecha de la última revisión y su resultado.

5 · Marcha atrás

Cómo se corta el acceso y cómo se vuelve a como estaba.

□ 5.1 · *Dirección* · El acceso de la IA se puede cortar en minutos, y está escrito cómo: revocar la clave o el token, desactivar el usuario y quitar el conector.
Se comprueba: se ha hecho una vez en el entorno de pruebas y se ha medido cuánto tarda.

□ 5.2 · *Dirección* · Antes de cualquier carga o cambio hay una copia, y la restauración se ha probado. Una copia que nunca se ha restaurado no cuenta.
Se comprueba: la fecha de la última restauración de prueba.

□ 5.3 · *Sistemas* · Cada cambio de configuración hecho para conectar la IA está anotado con cómo deshacerlo: cortafuegos, redirecciones de puertos, certificados, excepciones de TLS.

Se comprueba: hay una tabla con «antes, ahora y cómo se deshace». Las órdenes para deshacer se guardan separadas de las de instalar, para que nadie las ejecute por error.

□ 5.4 · *Sistemas* · Lo que crean las cargas de datos de prueba se identifica y se puede retirar.

Se comprueba: se puede listar lo creado (por usuario, por origen o por fecha), y se sabe cuánto tiempo guarda la papelera del sistema.

6 · Fiabilidad de lo que devuelve

No es seguridad en sentido estricto, pero una cifra equivocada en un informe hace tanto daño como un dato que se escapa.

□ 6.1 · *Sistemas* · Las cifras que se entregan están comprobadas. Cada cifra lleva su identificador y su origen, y un verificador independiente (otra vía de lectura que no pasa por la IA) da el mismo número, o se comprueba una muestra a mano.

Se comprueba: el informe dice cómo se verificó y qué no se pudo verificar.

□ 6.2 · *Sistemas* · El conector devuelve los textos en el idioma de la empresa. Hay conectores que no usan el idioma del usuario con el que entran y devuelven los nombres en inglés aunque el sistema esté en español. Esos nombres acaban en los informes. En algunos hay que fijar el idioma en su lanzador (en `mcp-server-odoo`, un conector de la comunidad y no de Odoo, con la variable `ODOO_LOCALE`; versión 0.8.0, probada en octubre de 2026).

Se comprueba: una lectura de prueba de un campo traducido (un estado, un impuesto) sale en el idioma de la empresa.

□ 6.3 · *Sistemas* · Lo que se diga sobre las pantallas sale de las pantallas, no del conector. Un conector suele leer los datos pero no las vistas, así que no sabe qué campos ve el usuario ni cuáles son obligatorios en el formulario. Un manual o una guía hecha solo con el conector describe campos que el usuario no ve.

Se comprueba: cada campo que se nombra en un manual aparece en una captura de pantalla o en la definición de la vista, leída aparte (en Odoo, `get_views`).

□ 6.4 · *Sistemas* · Cada informe lleva una fecha de referencia fija, y se avisa cuando una vista o una consulta del sistema usa «hoy». Si no, la misma pregunta da cifras distintas según el día en que se hace.

Se comprueba: la fecha sale en la cabecera del informe.

□ 6.5 · *Sistemas* · No se lee justo después de una carga o de un borrado masivo. Algunos sistemas tardan minutos en rellenar campos (por ejemplo, el origen del registro) o en mover registros a la papelera.

Se comprueba: hay un tiempo de espera anotado entre la carga y la lectura.

Licencia. Esta lista se publica con la licencia [Creative Commons Atribución 4.0 Internacional \(CC BY 4.0\)](#). Puedes copiarla, adaptarla y usarla en tu trabajo, también con fines comerciales, siempre que la cites así:

Luis Calvo Ruiz, *Antes de conectar una IA a tu sistema de gestión*, versión 1.0, luiscalvoruiz.es/ia-aplicada/conectar-ia-con-seguridad/, licencia CC BY 4.0.

Sin garantía. La lista se ofrece tal cual, sin ninguna garantía. Cumplirla no certifica que un sistema sea seguro.

Autor. Luis Calvo Ruiz, consultor de sistemas de gestión e IA aplicada, Valencia.

Cambios.

1.0 · 26 de octubre de 2026 · Primera versión pública.