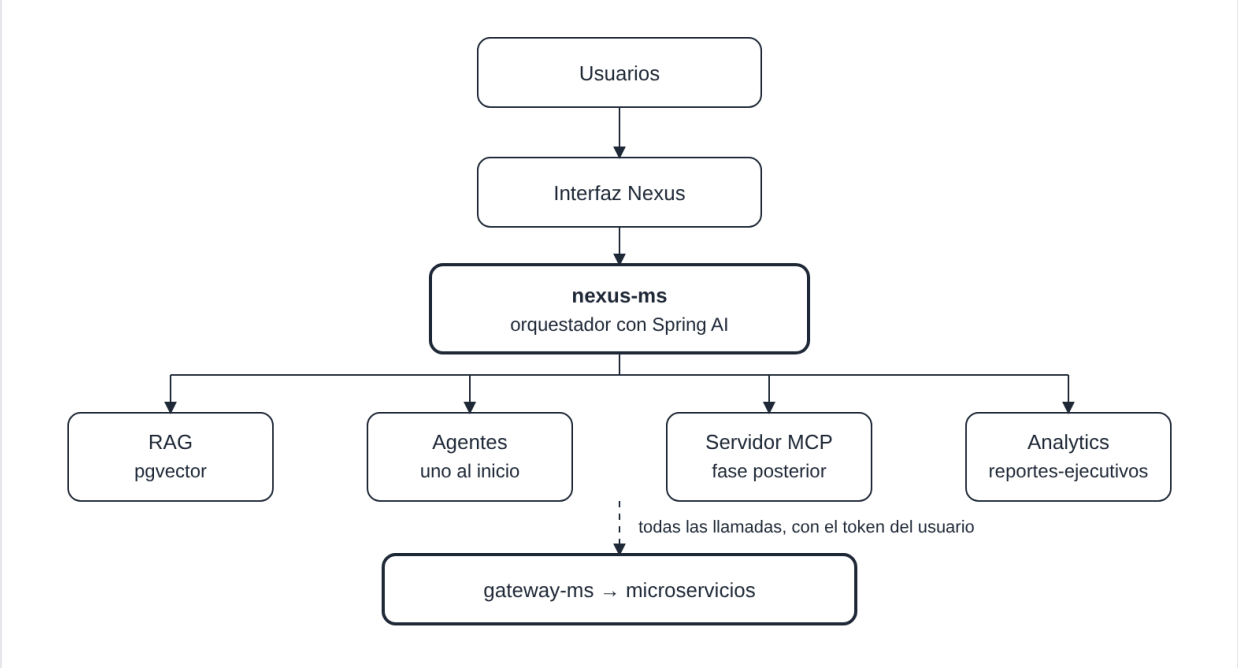
Nexus: diseño del asistente de IA

Nexus es la interfaz única con la que cada persona de EMPRESA_JOSESAID consulta información de todas las áreas, analiza cifras y automatiza tareas. Toda acción que cambie datos requiere confirmación humana. La base actual (gateway, JWT, Eureka y outbox con Kafka) se reutiliza sin cambios de fondo.

Arquitectura



Arquitectura de Nexus · cuatro capacidades detrás del orquestador

Todas las llamadas de Nexus a los microservicios pasan por gateway-ms con el token del usuario, así que los permisos existentes se aplican sin cambios.

Componentes

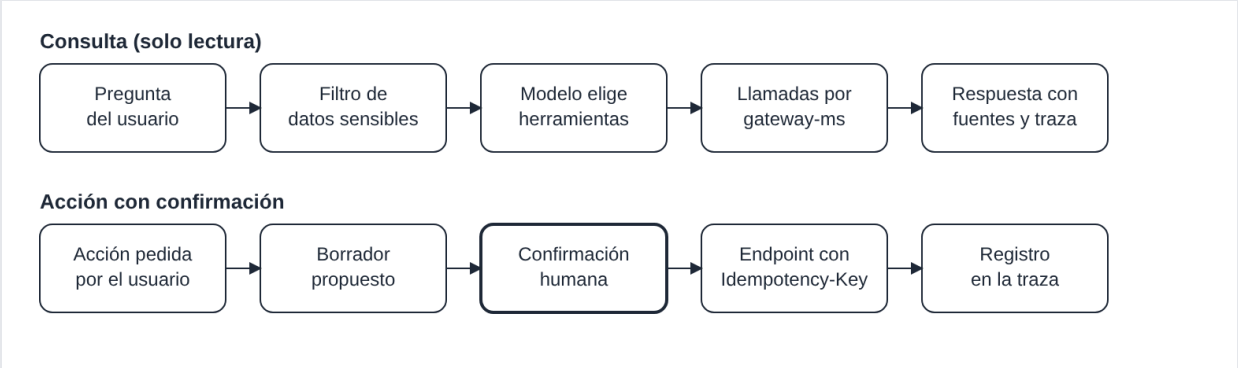
Componente	Implementación	Estado
nexus-ms	Servicio nuevo con Spring Boot 4.1.2 y Spring AI, registrado en Eureka y enrutado como /nexus/	Por crear
nexus-comun	Módulo Maven con filtro de datos sensibles, registro de tokens y prompts versionados	Por crear

Interfaz	Web propia o canal existente	Pendiente de decidir
RAG	pgvector en la base nexus, con espacios por área y filtro por rol	Por crear
Agentes	Uno al inicio; agentes por dominio solo si se justifican	Fase posterior
Servidor MCP	Expone herramientas con el token del usuario	Fase posterior
Analytics	reportes-ejecutivos-ms	Reutilizar
Microservicios	Sin cambios, salvo endpoints de lectura curados	Mínimos

Seguridad

- **Identidad del usuario:** Nexus propaga el JWT de la persona. Nunca usa una cuenta técnica con permisos amplios.
- **Herramientas con lista cerrada:** cada herramienta se define a mano, con alcance de lectura o escritura.
- **Escrituras con confirmación:** Nexus propone un borrador y la persona confirma en un endpoint explícito con Idempotency-Key.
- **RAG con permisos:** el recuperador filtra por rol antes de devolver fragmentos, sobre todo en documentos cifrados.
- **Trazabilidad:** cada respuesta registra usuario, herramientas usadas, fuentes y tokens consumidos.

Flujo de una consulta y de una acción



Consulta de solo lectura y acción con confirmación humana

Una consulta solo lee datos. Una acción siempre llega a un borrador que la persona confirma antes de que cambie algo.

Fases

Fase	Entrega
0	nexus-comun: filtro de datos, observabilidad de tokens y casos de evaluación
1	nexus-ms con herramientas de lectura sobre reportes y clientes
2	RAG de políticas de compras con permisos por rol
3	Sugerencia de cuentas contables para pólizas
4	Servidor MCP
5	Agentes por dominio, si hacen falta
6	Interfaz final de Nexus

Decisiones pendientes

☐ Nombre: Nexus o Nexo, por la colisión con Sonatype Nexus

☐ Interfaz: web propia o canal como Teams o Slack

☐ Modelo y datos: proveedor y si se permite enviar datos aunque estén redactados

☐ Monto límite de aprobación en compras

☐ Presupuesto de tokens por servicio y por usuario

Fuentes

- Repositorio EMPRESA_JOSESAID, revisión del 30 de octubre de 2026: README de cada servicio y especificaciones en area_md_specification_files.