ANEXO DE SEGURIDAD

Versión: 2.4

Actualizada a: 23 / Abril / 2026

Contenido

1. Introducción

El presente documento describe las medidas de seguridad implementadas en el SERVICIO AVI (Asistente Virtual Inteligente), con el objetivo de resguardar la confidencialidad,

integridad y disponibilidad de la información que procesa. El SERVICIO AVI está diseñado para operar en la nube de Microsoft Azure, adoptando un modelo multi-tenant que permite a múltiples clientes usar la plataforma bajo una misma infraestructura lógica, con estricta separación y control de acceso a los datos.

2. Arquitectura General

2.1. Infraestructura en la Nube

Proveedor: Microsoft Azure.

Modelo de Despliegue: Multi-tenant, donde EL CLIENTE tiene su espacio lógico, pero comparte la infraestructura subyacente con otros clientes.

2.2. Componentes Principales

App Service: Aloja la aplicación web del SERVICIO AVI.

Azure Storage Account: Almacena los documentos de la Base de Conocimiento.

Azure Cognitive Search: Realiza la indexación y búsqueda (RAG).

Azure OpenAI: Proporciona la capacidad de lenguaje natural (LLM).

Azure Key Vault: Guarda secretos, contraseñas y tokens.

2.3. Comunicación Interna

Todos los componentes se comunican a través de TLS (HTTPS), encriptando datos en tránsito.

3. Manejo de Datos

3.1. Datos en Reposo

En Azure Storage, se aplica encriptación AES-256 (Habilitada por defecto en Azure).

La Base de Conocimiento (documentos PDF, Word, etc.) se organiza por contenedores y rutas específicas para EL CLIENTE, garantizando separación lógica.

3.2. Datos en Tránsito

Todo acceso a la aplicación web es vía HTTPS (TLS 1.2+).

La comunicación con Azure OpenAI y otros servicios de Azure también usa canales cifrados.

3.3. Base de Conocimiento y LLM

E SERVICIO AVI funciona bajo la técnica de Retrieval-Augmented Generation (RAG).

Los documentos no se suben permanentemente al modelo de OpenAI, sino que se indexan en Azure Cognitive Search y pasan como contexto al momento de generar respuestas (sin re-entrenar el modelo).

3.4 Integraciones documentales

Cuando el SERVICIO AVI se sincronice con carpetas de Microsoft OneDrive/SharePoint, los documentos se procesarán e indexarán conforme a estos lineamientos de seguridad y a los permisos definidos por EL CLIENTE en su plataforma de origen.

4. Control de Acceso y Autenticación

4.1 Métodos de Autenticación

Correo y Contraseña Temporal: El administrador crea la cuenta ingresando el correo del usuario, se envía una contraseña inicial que el usuario debe cambiar al primer acceso.

SSO Opcional: El SERVICIO AVI se puede integrar con proveedores de identidad (Microsoft, Google), habilitando inicio de sesión único.

4.2 Permisos a Documentos

El acceso a la Base de Conocimiento se gestiona mediante Grupos de Usuarios y políticas del Agente, de forma que cada usuario sólo puede consultar la información autorizada por EL CLIENTE.

4.3 Políticas de Contraseñas

Sin política de expiración por defecto.

El usuario puede cambiar su contraseña en cualquier momento.

Sugerencia de complejidad mínima (longitud, caracteres), pero no forzada.

5. Registro de Interacciones y Privacidad

5.1. Log de Interacciones

Se conserva un historial de consultas y respuestas para fines de auditoría y mejora del servicio.

El nivel de detalle (usuario, fecha y hora de interacción, pregunta del usuario, respuesta del servicio, chunks utilizados como contexto en la respuesta, etc.) puede configurarse según el nivel de privacidad que EL CLIENTE desee.

5.2. Retención de Logs

La retención de interacciones y registros operativos del SERVICIO AVI se realizará conforme a lo previsto en los TÉRMINOS Y CONDICIONES y a la configuración de trazabilidad establecida por EL CLIENTE, sin perjuicio del derecho de EL CLIENTE a solicitar su eliminación anticipada conforme a la legislación aplicable.

5.3. Confidencialidad

Todos los consultores de INFOSAPIENS y el personal que dan soporte firman NDA y se rigen por contratos de confidencialidad.

No se utilizan los datos de EL CLIENTE para entrenar modelos externos.

6. Resguardo de Secretos

6.1. Azure Key Vault

Las credenciales de servicio (ej. contraseñas del motor DB, tokens, client secrets) se guardan cifradas en Key Vault.

Los accesos a Key Vault se otorgan mediante identidades administradas de Azure o roles específicos.

6.2. Rotación

Ante un incidente de seguridad o petición de EL CLIENTE, se pueden regenerar secretos sin interrumpir el servicio.

7. Red y Disponibilidad

7.1. Arquitectura de Red

El App Service se ejecuta bajo una configuración de red controlada por Azure, con su propio Reverse Proxy y DDoS Protection.

No se exponen puertos innecesarios. Todo el tráfico pasa por HTTPS (puerto 443).

7.2. Anti-DDoS

Azure brinda DDoS Protection a nivel de infraestructura, complementado por la seguridad del App Service.

7.3. Disponibilidad

La aplicación es una región de Azure. Se basa en la alta disponibilidad propia de la región de Azure en que corre.

Si EL CLEINTE requiere mayor resiliencia geográfica, se evaluaría un despliegue en otra región (no estándar, genera costos adicionales).

8. Copias de Seguridad y Plan de Incidentes

8.1. Backups

Los datos de la Base de Conocimiento (en Storage) y la BD de la aplicación se respaldan según la política de Azure.

El equipo de INFOSAPIENS puede restaurar en caso de eliminación accidental (RPO/RTO sujetos a la suscripción y configuración actual) conforme a los TÉRMINOS Y CONDICIONES y sus políticas vigentes.

8.2. Respuesta a Incidentes

Ante un incidente de seguridad (acceso indebido, filtración) se activa un plan de respuesta interno:

Se aíslan credenciales comprometidas.

INFOSAPIENS notificará a EL CLIENTE conforme a lo previsto en los TÉRMINOS Y CONDICIONES y a los canales de soporte vigentes, documentando el evento y las medidas correctivas.

Se documenta el incidente y las medidas tomadas para que no se repita.

9. Cumplimiento y Contratos

9.1. Cumplimiento Azure

Microsoft Azure cumple con ISO 27001, ISO 27018, FedRAMP, entre otros estándares reconocidos.

El SERVICIO AVI se beneficia de dichas certificaciones al hospedarse en Azure.

9.2. Contratos y NDA

INFOSAPIENS firma NDAs y contratos de confidencialidad con sus colaboradores y con EL CLIENTE.

EL CLIENTE es responsable de manejar sus datos de acuerdo con la legislación aplicable (p. ej., LFPDPPP, GDPR, etc., si corresponde).

9.3. Datos Personales

El SERVICIO AVI maneja datos de usuarios finales (nombres, correos), pero no los usa para ningún fin de entrenamiento masivo.

EL CLIENTE puede solicitar la supresión de datos al terminar la relación contractual.

10. Conclusión

Este documento refleja la configuración y medidas actuales de seguridad del SERVICIO AVI, enfatizando la protección de datos, la confidencialidad en el acceso a la Base de Conocimiento y la robustez de la nube de Azure como infraestructura subyacente. A medida que las necesidades de seguridad de EL CLIENTE crezcan, el SERVICIO AVI está preparado para evolucionar, incorporando capas adicionales como multi-región, MFA y políticas más estrictas de contraseñas, siempre con miras a mantener un equilibrio entre usabilidad y protección.