ANEXO TÉCNICO: ARQUITECTURA DE SEGURIDAD, SOBERANÍA TECNOLÓGICA Y PROTOCOLOS DE INTEGRACIÓN

Referencia: Contrato No. CO26000117-GAC
Contratista: Cloud City Colombia SAS
Entidad: Caja de Sueldos de Retiro de la Policía Nacional – CASUR

1. OBJETO DEL ANEXO TÉCNICO

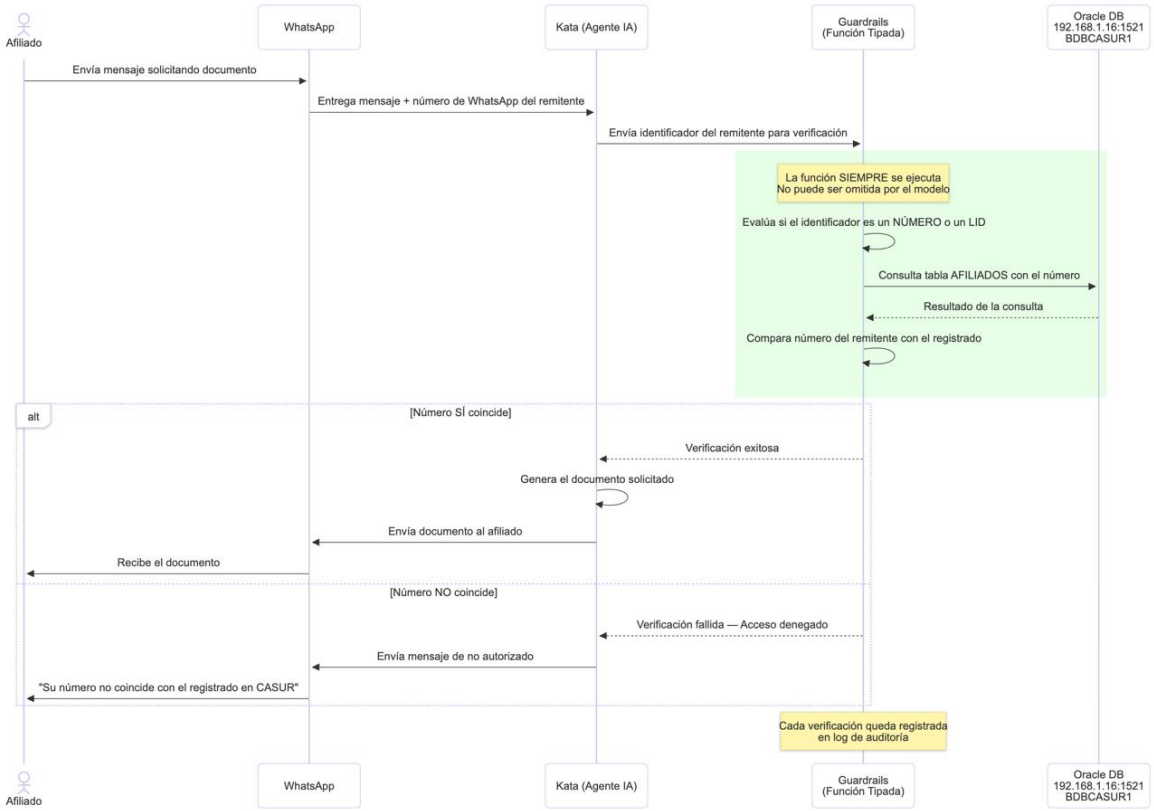
El presente anexo técnico tiene como finalidad documentar la arquitectura tecnológica, los protocolos de seguridad, los mecanismos de autenticación, las políticas de tratamiento de datos y los componentes de integración implementados sobre la plataforma SAYFORM IA ADVANCED, correspondiente al asistente virtual institucional “Kata en Línea”. La solución tecnológica fue diseñada bajo principios de seguridad transaccional, autenticación determinística, segmentación lógica de servicios, soberanía tecnológica y protección integral de la información institucional, garantizando que los procesos de validación, autenticación y entrega documental operen mediante controles programáticos obligatorios y mecanismos criptográficos de seguridad.

2. ARQUITECTURA DE INFRAESTRUCTURA Y CONECTIVIDAD

Los componentes encargados de la orquestación transaccional, validación de identidad, procesamiento conversacional, autenticación, generación documental y lógica de negocio se encuentran desplegados exclusivamente sobre infraestructura física dedicada de alta disponibilidad dentro del Data Center privado de Cloud City Colombia SAS. La arquitectura opera bajo un modelo de nube privada segmentada mediante microservicios contenedorizados y políticas de aislamiento de red, eliminando dependencias operativas sobre infraestructuras públicas de terceros y reduciendo significativamente las superficies de exposición externas.

La solución implementa una separación lógica y operativa entre los servicios de autenticación, validación transaccional, procesamiento conversacional, generación documental, persistencia temporal, auditoría técnica y entrega segura de recursos. Cada uno de estos componentes opera bajo políticas independientes de autorización y control de acceso, permitiendo aislar funcionalmente los procesos críticos y fortalecer la contención de seguridad entre servicios.

La interconexión entre la infraestructura de Cloud City Colombia SAS y la infraestructura tecnológica de CASUR se realiza exclusivamente mediante túneles privados VPN punto a punto suministrados por la Entidad. El tráfico se encuentra protegido mediante cifrado extremo a extremo y segmentación de red entre la infraestructura Fortinet institucional y los nodos MikroTik del Data Center de Cloud City. Las consultas hacia los motores Oracle institucionales únicamente son autorizadas cuando las solicitudes provienen de segmentos previamente autenticados dentro del túnel institucional VPN y validados mediante listas de control de acceso y políticas de seguridad perimetral.



3. SOBERANÍA TECNOLÓGICA Y TRATAMIENTO DE DATOS

La plataforma SAYFORM IA ADVANCED ejecuta los procesos de inferencia conversacional y procesamiento semántico mediante infraestructura privada administrada por Cloud City Colombia SAS. El procesamiento de lenguaje natural y la ejecución de modelos conversacionales se realizan sobre hardware especializado con aceleración GPU dedicada, evitando la utilización de servicios públicos o comerciales de inteligencia artificial para el tratamiento de información institucional sensible. La arquitectura implementada garantiza que no existan transferencias de datos hacia nubes públicas, mecanismos de entrenamiento cruzado con información institucional ni persistencia de información sensible fuera del entorno tecnológico autorizado.

Adicionalmente, la solución implementa un modelo de persistencia efímera orientado a minimizar la exposición documental y la permanencia residual de información sensible. Los documentos son generados únicamente bajo demanda, almacenados temporalmente bajo políticas de expiración automática y eliminados programáticamente posterior a la entrega autorizada. La arquitectura contempla mecanismos de destrucción segura de recursos temporales, evitando persistencia permanente o almacenamiento residual innecesario dentro de la infraestructura del contratista.

4. COMPONENTE TRANSACCIONAL Y GENERACIÓN DOCUMENTAL

La plataforma integra una capa de microservicios especializados orientados a la generación automatizada y escalable de documentos institucionales relacionados con:

- desprendibles de nómina,

- certificados de prima,
- certificados de retroactivo,
- certificados de ingresos y retenciones,
- resoluciones administrativas,
- hojas de servicio,
- certificados de sanidad,
- certificaciones laborales,
- y certificaciones de beneficiarios y titulares.

Toda generación documental se encuentra condicionada a la validación satisfactoria de autenticación y autorización transaccional, garantizando que los recursos únicamente puedan ser liberados posterior a la verificación integral de identidad del afiliado.

5. MODELO DE SEGURIDAD Y VALIDACIÓN DE IDENTIDAD

La plataforma implementa un modelo de validación basado en funciones tipadas determinísticas ejecutadas de manera programática como middleware obligatorio de autorización transaccional. Esta arquitectura elimina la dependencia exclusiva sobre mecanismos probabilísticos de inferencia conversacional para procesos críticos de seguridad, reemplazándolos por validaciones algorítmicas estrictas, reglas tipadas de autenticación y controles programáticos obligatorios de ejecución. El sistema impide técnicamente la generación documental cuando las validaciones de identidad y autorización no retornan un estado válido previamente autenticado.

La solución incorpora adicionalmente un esquema de autenticación multifactor adaptativa para procesos documentales sensibles. Cuando el canal de WhatsApp opera bajo identificadores de privacidad tipo LID (Linked Identity), el sistema ejecuta automáticamente un flujo complementario de verificación MFA mediante OTP criptográfico temporal. El proceso contempla:

- consulta de información institucional en Oracle,
- recuperación de canales oficiales registrados del afiliado,
- generación de códigos OTP de un solo uso con expiración temporal,
- validación transaccional del código,
- y liberación controlada del recurso documental solicitado.

Los códigos implementados operan bajo mecanismos de unicidad, expiración automática e invalidación contextual de sesión.

La arquitectura implementa igualmente mecanismos de enrolamiento progresivo de identificadores autorizados asociados al afiliado institucional. Una vez completada satisfactoriamente la validación MFA, el identificador contextual puede ser asociado al registro institucional para permitir reconocimiento controlado de futuras interacciones bajo políticas de seguridad, trazabilidad y revalidación dinámica ante cambios de dispositivo o renovación de identificadores.

La entrega documental opera mediante recursos criptográficos efímeros, incluyendo tokens temporales, URLs firmadas, expiración automática y validación contextual de sesión. Cada transacción documental posee restricciones de autenticidad, vigencia temporal limitada y mecanismos de revocación automática posteriores al consumo autorizado del recurso.

Complementariamente, la plataforma integra mecanismos avanzados de auditoría técnica y trazabilidad operacional mediante:

- registros transaccionales,
- logs de autenticación,
- monitoreo de eventos de validación,
- control de expiración documental,
- y seguimiento de eventos de seguridad.

Dichos registros operan bajo políticas de minimización de persistencia y segregación de información sensible, garantizando cumplimiento normativo y trazabilidad operacional de las transacciones ejecutadas.

La WebApp segura de descarga documental opera bajo protocolos HTTPS cifrados, validación contextual, endpoints restringidos, control de sesión y mecanismos anti reutilización de recursos. Los endpoints críticos implementan políticas de limitación de consumo, validación obligatoria de autenticación, segmentación de privilegios operativos y control transaccional de acceso a documentos sensibles.

6. CUMPLIMIENTO NORMATIVO Y GOBIERNO DIGITAL

La solución tecnológica implementada por Cloud City Colombia SAS cumple con los lineamientos establecidos en la Ley 1581 de 2012, los principios de Gobierno Digital y las políticas institucionales de protección de datos personales. La arquitectura garantiza soberanía tecnológica institucional, control exclusivo sobre los datos procesados, conectividad privada segura, procesamiento aislado y protección integral de la información sensible administrada dentro del ecosistema tecnológico de CASUR.

Atentamente:



JONATHAN DAVID LUNA
Cédula de Ciudadanía No. 1.073.706.360
En Calidad de REPRESENTANTE LEGAL
Empresa: CLOUD CITY COLOMBIA SAS
Nit: 901.249.716-3
Email: administrativo@cloudcity.com.co
Website: www.cloudcitycolombia.com
Ciudad: Bogotá