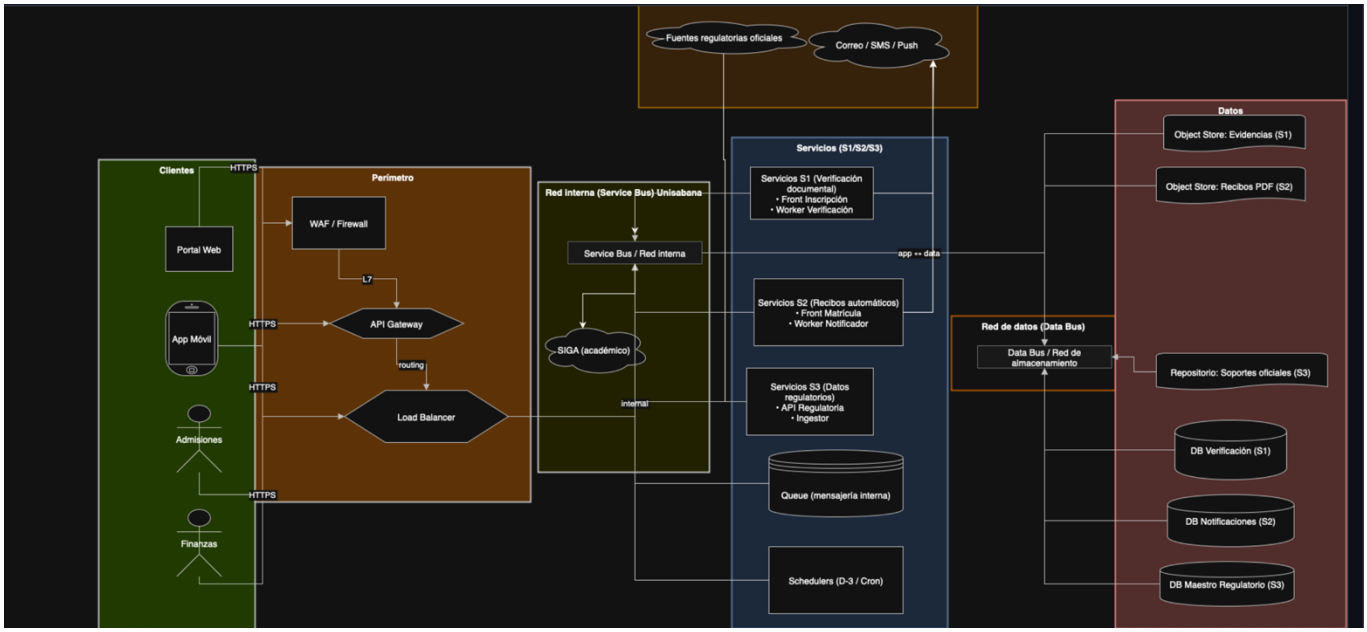
Informe Técnico – Diagnóstico de Infraestructura

Parte 2: Aplicación al Cliente Real (Posgrados – Unisabana)

Sergio Socha, Julian Pinilla, Cristian Soto, Nicolas Rodriguez.



1. Introducción

El presente documento describe la infraestructura tecnológica del sistema de gestión de procesos académicos de posgrados de Unisabana, con base en el mapa de comunicación entre componentes. Se identifican los principales servicios, nodos y bases de datos involucrados, así como los puntos críticos que podrían convertirse en debilidades o cuellos de botella. Adicionalmente, se incluye una revisión de buenas prácticas en arquitecturas híbridas (cloud / on-premise) que servirán como referencia para mejorar la resiliencia y escalabilidad del sistema.

2. Descripción de la Infraestructura Actual

2.1 Clientes y Perímetro

*Clientes: Portal web, aplicación móvil, áreas de Admisiones y Finanzas.

*Perímetro de seguridad: Incluye WAF/Firewall, un API Gateway con enrutamiento y un Load Balancer que distribuye el tráfico entrante.

2.2 Red Interna

*Service Bus (Unisabana): Canal principal de integración con el sistema académico SIGA.

*Comunicación interna entre aplicaciones y servicios de backend.

2.3 Servicios

*Servicios S1: Verificación documental (Front Inscripción, Worker Verificación).

*Servicios S2: Recibos automáticos (Front Matrícula, Worker Notificador).

*Servicios S3: Datos regulatorios (API Regulatoria, Ingestor).

*Mensajería y schedulers internos: Soportan la comunicación asíncrona y procesos batch.

2.4 Datos

*Object Store: Evidencias (S1), Recibos PDF (S2).

*Repositorio: Soportes oficiales (S3).

*Bases de datos: Verificación (S1), Notificaciones (S2), Maestro Regulatorio (S3).

*Data Bus / Red de almacenamiento: Intermediario entre aplicaciones y repositorios.

2.5 Integraciones externas

*Fuentes regulatorias oficiales.

*Servicios de mensajería (correo, SMS, push).

3. Diagnóstico Técnico

3.1 Fortalezas

*Arquitectura modular con separación clara de responsabilidades (S1, S2, S3).

*Uso de balanceador de carga y API Gateway que permiten escalar horizontalmente.

*Integración de mensajería asíncrona (queues) para desacoplar procesos.

3.2 Debilidades y Cuellos de Botella

1. **Punto único de fallo en el API Gateway y Load Balancer:**

   *Aunque permiten distribuir tráfico, no se evidencia redundancia geográfica o en caliente.

   *Riesgo: caída total del servicio ante incidentes de red o hardware.

2. **Bases de datos monolíticas por servicio:**

   *Actualmente aisladas (S1, S2, S3), lo cual facilita segmentación, pero pueden generar latencia en consultas conjuntas.

   *Riesgo: fragmentación de datos regulatorios, duplicidad o inconsistencias.

3. **Data Bus centralizado:**

   *Potencial cuello de botella en alto volumen de transacciones (temporadas de matrícula o auditorías regulatorias).

   *Riesgo: congestión que afecte procesamiento de colas y almacenamiento.

4. **Integraciones externas sin redundancia clara:**

    *Dependencia de fuentes regulatorias y mensajería externa sin mecanismos de fallback.

    *Riesgo: retrasos en notificaciones y validaciones regulatorias.

5. **Seguridad y cumplimiento:**

    *El diagrama contempla firewall, pero no evidencia mecanismos de encriptación en reposo ni controles de acceso basados en roles para las bases de datos.

4. Buenas Prácticas de Arquitectura

4.1 Escalabilidad y Disponibilidad

*Implementar **redundancia activa-activa** en el API Gateway y el Load Balancer.

*Desplegar clusters replicados de bases de datos (multi-AZ o geo-replicación en la nube).

*Adoptar autoscaling groups en servicios críticos (S1–S3).

4.2 Seguridad

*Uso de **cifrado en tránsito (TLS 1.3)** y en reposo (AES-256).

* Implementación de **IAM granular** y segregación de funciones en bases de datos y servicios.

*Auditorías de cumplimiento con **ISO 27001** y **NIST CSF**.

4.3 Integraciones externas

*Establecer proovedores para correo/SMS/push (ej. integración multi-proveedor).

*Uso de circuit breakers y patrones de retry para servicios regulatorios externos.

4.4Cloud / On-Premise / Híbrida

*Migrar almacenamiento de objetos (evidencias, recibos, soportes) a un bucket cloud con redundancia,

*Mantener servicios regulatorios y académicos en un modelo híbrido:

*On-premise: datos académicos sensibles (SIGA, BD Verificación).

*Cloud: microservicios escalables y colas de mensajería.

5. Conclusiones

La infraestructura actual es sólida en su modularidad, pero presenta riesgos de disponibilidad y escalabilidad ante escenarios de alta demanda. Para fortalecerla, se recomienda evolucionar hacia una arquitectura híbrida con redundancia distribuida, mayor resiliencia en integraciones externas y prácticas de seguridad avanzadas. Estas medidas permitirán asegurar continuidad, cumplimiento regulatorio y confianza de los usuarios finales.