RANKMI

Arquitectura e Infraestructura de la Plataforma

Seguridad, Escalabilidad y Cumplimiento ISO 27001/27701/37001

Versión 5.0 | Abril 2026

Historial de Versiones

Versión	Aprobado por	Fecha de Revisión	Descripción del cambio	Autor	Clasificación
1.0	Felipe Mundaca	09/03/2020	Creación del documento	Felipe Mundaca	Privada
2.0	Felipe Mundaca	10/11/2024	Actualización	Franco Quijano	Privada
3.0	Felipe Mundaca	07/06/2024	Actualización	Diego González	Privada
4.0	Felipe Mundaca	27/08/2025	Monitoreo y automatización	Diego González	Privada
4.1	Felipe Mundaca	07/04/2026	Estructura de red, cifrado, vpc, y cambio a público	Diego González	Pública
5.0	Felipe Mundaca Daniel Ramirez	10/04/2026	Estructura del documento	Diego González	Pública

1. Introducción

La Plataforma Rankmi es un Software-as-a-Service (SaaS) especializado en Gestión del Talento Humano, operado por una infraestructura cloud moderna alojada en Amazon Web Services (AWS). Este documento describe la arquitectura, infraestructura, medidas de seguridad y conformidad regulatoria que sustentan la operación de la plataforma, con especial énfasis en los estándares ISO 27001:2022, ISO 27701:2019 e ISO 37001:2016.

1.1 Modelo de Negocio

Rankmi es una plataforma SaaS enfocada en Gestión del Talento Humano (Human Capital Management - HCM), dirigida a medianas y grandes empresas en América Latina. La plataforma integra múltiples módulos: Beneficios, Payroll, Evaluaciones de Desempeño, Clima Laboral, LMS (Learning Management System), ATS (Applicant Tracking System), Genius (módulo de IA), Hub Social, entre otros.

2. Arquitectura General de la Plataforma

La arquitectura cloud de Rankmi se fundamenta en un modelo moderno de microservicios orquestados sobre Amazon EKS (Elastic Kubernetes Service), diseñado bajo principios de alta disponibilidad, seguridad avanzada, escalabilidad automática y resiliencia.

2.1 Pilares de la Arquitectura

- Escalamiento horizontal independiente de cada microservicio mediante HPA
- Despliegues sin tiempo de inactividad (Zero Downtime Deployment)
- Aislamiento de cargas de trabajo en contenedores
- Automatización completa de despliegues mediante GitOps (ArgoCD)
- Monitoreo continuo con observabilidad en tiempo real
- Estrategia **Multitenant** para separación lógica de datos.

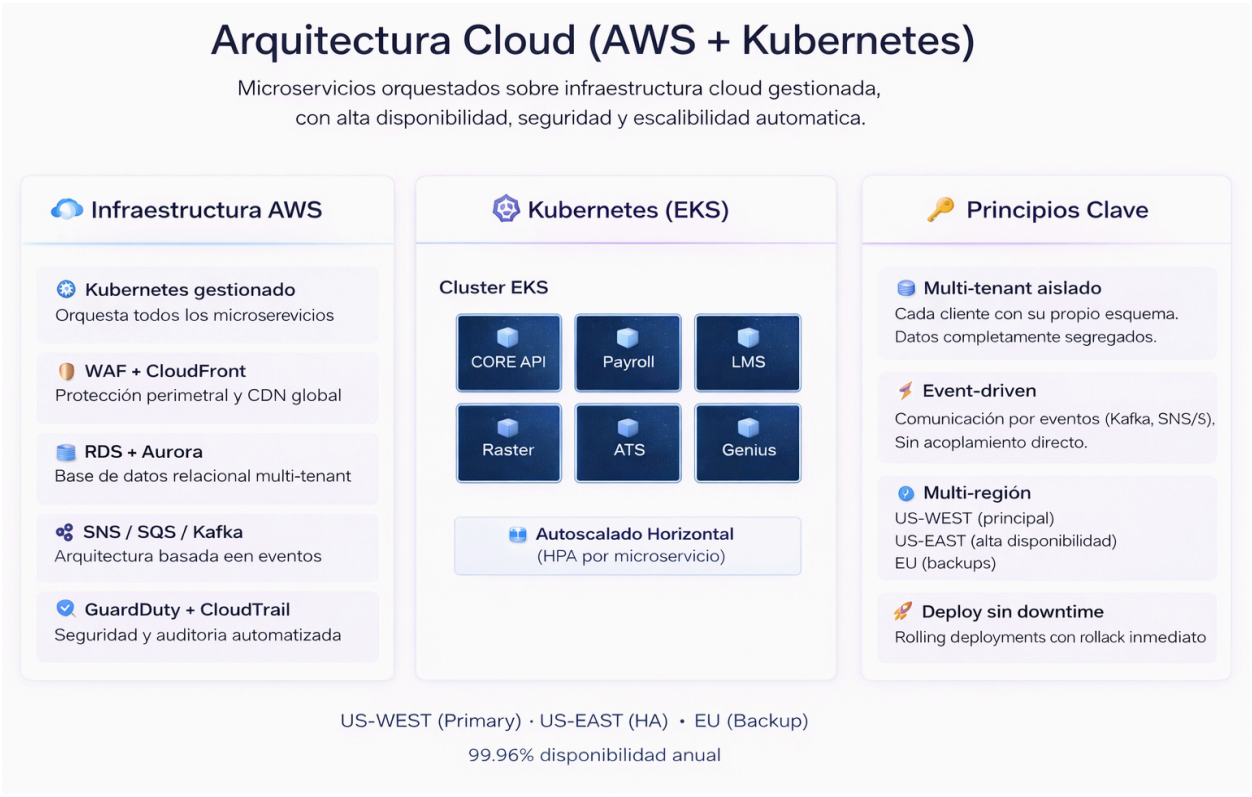

***Imagen 1**. Arquitectura General de Rankmi*

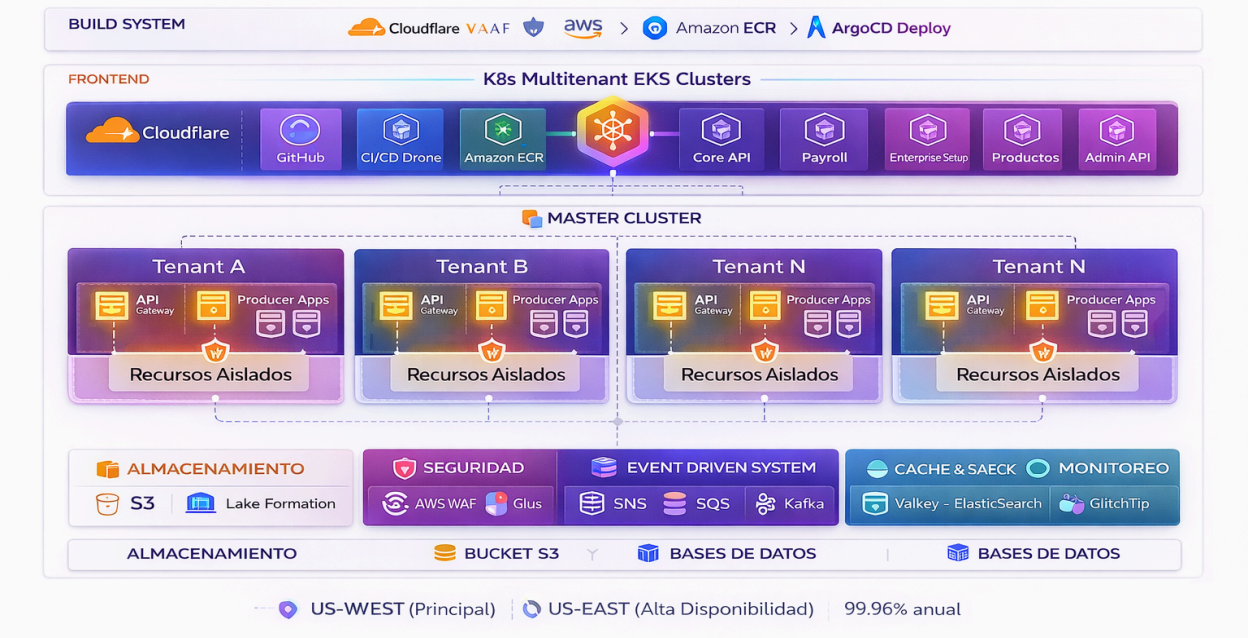

***Imagen 2.** Arquitectura detallada Multitenant de Rankmi*

2.2 Ecosistema de Servicios AWS

Seguridad Perimetral

AWS WAF (Web Application Firewall) + CloudFront (CDN global): Protección contra amenazas web comunes (OWASP Top 10) como inyección SQL, XSS, DDoS y aceleración de contenido a nivel mundial.

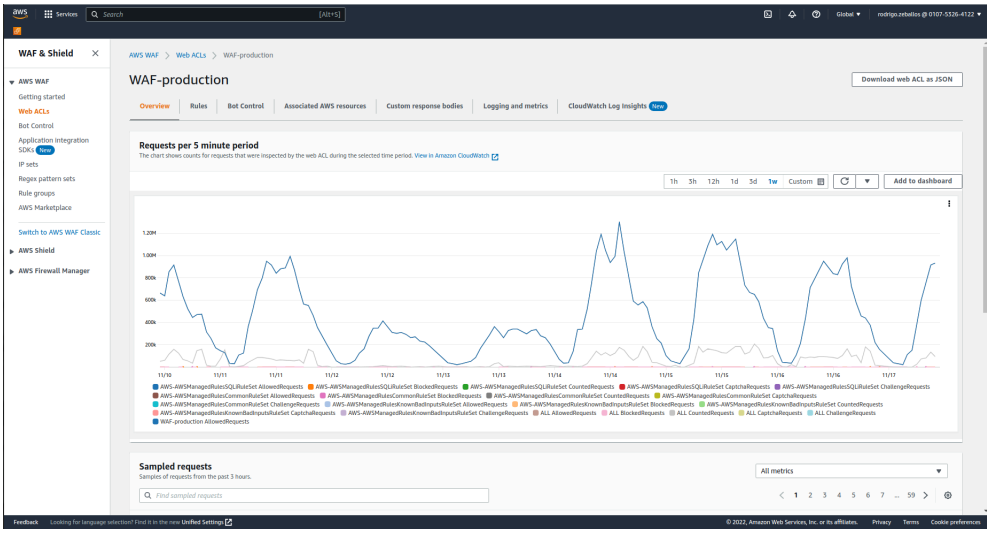

***Imagen 3**. Evidencia de activación WAF*

Persistencia de Datos

RDS Aurora PostgreSQL en modo Multi-AZ: Base de datos relacionales de alto rendimiento con replicación automática entre Zonas de Disponibilidad dentro de la región.

Mensajería y Eventos

SNS, SQS y Apache Kafka: Arquitectura event-driven que desacopla microservicios y garantiza procesamiento asíncrono de transacciones críticas como nómina.

Seguridad y Auditoría

AWS GuardDuty, CloudTrail, VPC Flow Logs y Rankmi Audit: Monitoreo continuo, detección de anomalías y registro inmutable de accesos para cumplimiento ISO 27001.

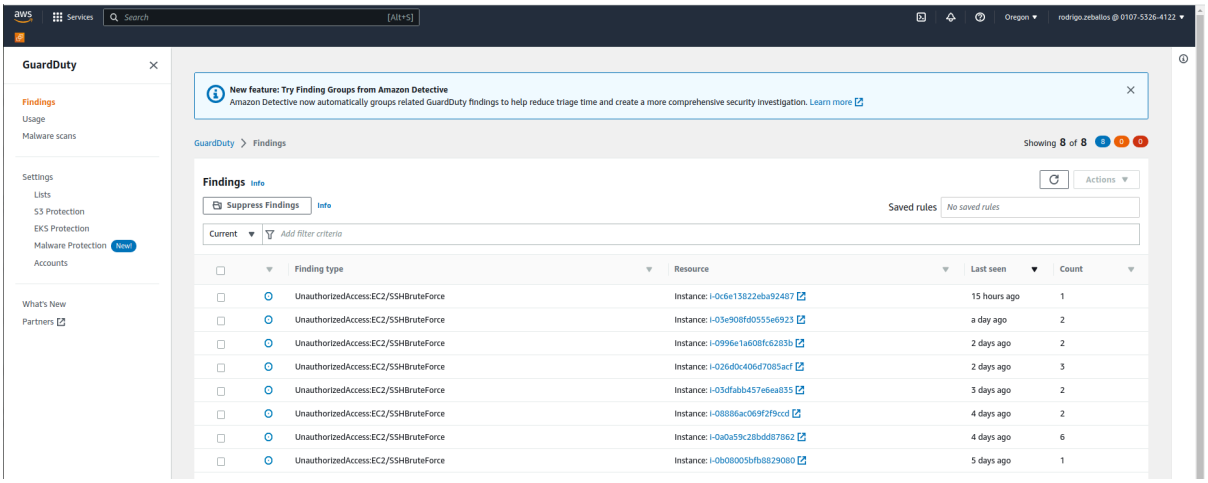

***Imagen 4**. Evidencia de activación GuarDuty*

Política de almacenamiento de Logs. Los Logs son almacenados en línea hasta 6 meses.

3. Infraestructura de Red y Ubicación

3.1 Estructura de la VPC

La infraestructura de red de Rankmi se despliega sobre una Virtual Private Cloud (VPC) de AWS con:

- Rango CIDR dedicado para EKS: /16
- Subredes públicas y privadas distribuidas en múltiples Zonas de Disponibilidad
- VPC Endpoints para acceso privado a servicios AWS
- Security Groups y Network ACLs para restricción granular de tráfico

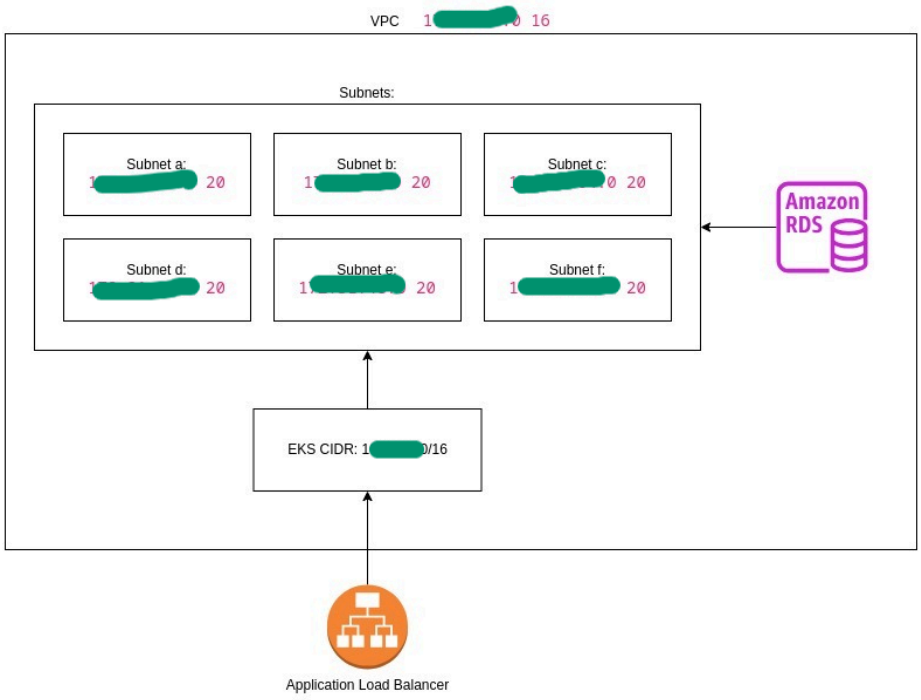

***Imagen 5**. Estructura de Red*

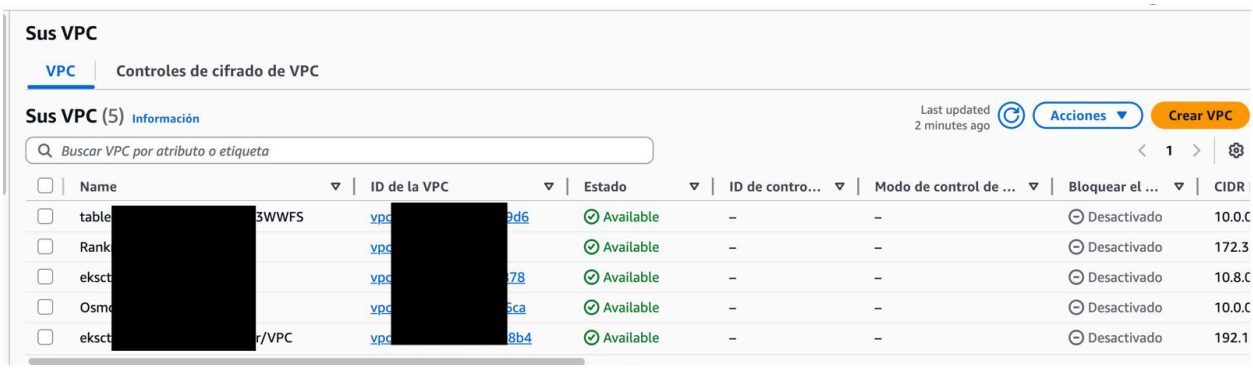

***Imagen 6**. Evidencia de VPCs configuradas*

3.2 Ubicación Geográfica

Producción (Principal):

- AWS US-EAST-1 (N. Virginia): Región primaria
- AWS US-WEST-2 (Oregon): Región secundaria para redundancia

Respaldos y Recuperación:

- AWS EU-WEST-1 (Irlanda): Respaldos replicados de bases de datos y archivos

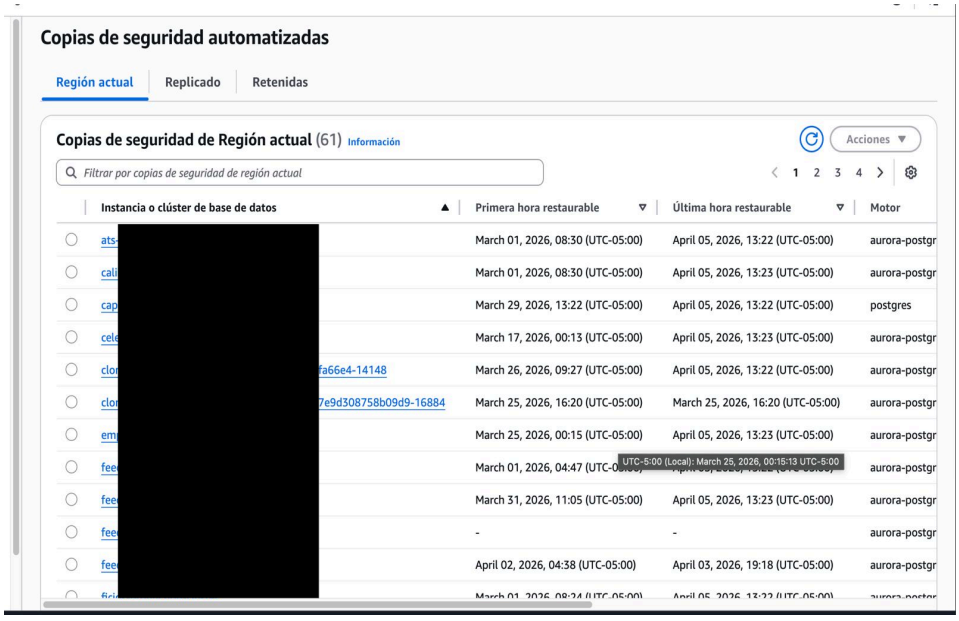

***Imagen 7**. Evidencia de respaldos automáticos*

4. Componentes Clave de Infraestructura

4.1 EKS (Elastic Kubernetes Service)

Estado: Producción (Go-Live Marzo 2026)

El clúster EKS constituye el corazón de la plataforma, proporcionando orquestación de contenedores con:

- Network policies para restricción de tráfico inter-pod
- Pod Security Standards para prevención de ejecución privilegiada
- RBAC (Role-Based Access Control) con control granular
- Audit logging de todas las acciones
- Secrets encryption con AWS KMS

4.2 ArgoCD (GitOps y Despliegue Continuo)

Estado: Operativo en no-producción; Migrando a producción (BHP-Production)

ArgoCD automatiza despliegues mediante el modelo GitOps, garantizando:

- Acceso controlado vía SSO (Keycloak + Google OAuth)
- Infraestructura accesible solo vía Teleport
- Auditoría completa de cambios mediante repositorio Git
- Rollback inmediato ante fallos

4.3 Infisical (Gestión de Secretos)

Estado: Beta en pruebas; Sustituyendo a Doppler

Proporciona gestión centralizada y cifrada de secretos (API keys, tokens, credenciales) con:

- Sincronización automática con roles IAM de AWS
- Rotación automática de credenciales
- Acceso restringido vía Teleport
- Auditoría granular de accesos

4.4 Teleport (Acceso Administrativo Zero Trust)

Teleport es el punto centralizado de acceso para toda administración de infraestructura:

- Autenticación multifactor (MFA) requerida para todos los accesos
- Grabación y auditoría de todas las sesiones
- RBAC con permisos granulares por rol

- Cumplimiento ISO 27001: Control A.9.2 (Acceso de usuario)

4.5 Drone (CI/CD Pipeline)

Estado: Estable en producción; Migrando Payroll-API, Payroll-App y App

Ejecuta construcción, pruebas e integración continua de código:

- Pruebas automáticas bloqueantes
- Escaneo de vulnerabilidades en imágenes Docker
- Multipool de máquinas para aislar cargas de trabajo
- Gestión de secretos mediante Infisical

5. Monitoreo, Logging y Observabilidad

5.1 GlitchTip (Monitoreo de Errores y Performance)

Estado: Operativo pero aún no productivo, esperando aprobación de Daniel

- Seguimiento de errores en tiempo real
- Monitoreo de Performance (APM)
- Acceso vía SSO (Google OAuth) + Teleport
- Actualizado a última versión de seguridad

5.2 SigNoz (Observabilidad Distribuida)

Estado: Operativo pero aún no productivo

- Tracing distribuido a través de microservicios
- OpenTelemetry para recopilación estándar
- Sharding en ClickHouse para escalabilidad
- Acceso vía SSO + Teleport

5.3 Rankmi Audit (Auditoría Nativa)

Sistema propio para auditoría y trazabilidad de la plataforma:

- pgAudit: Auditoría a nivel PostgreSQL
- Justificación obligatoria para accesos a base de datos
- Integración n8n para orquestación de solicitudes
- Cumplimiento ISO 27001 A.12.4.1

5.4 Ntfy (Notificaciones de Alertas)

Estado: Pruebas finales en curso esta semana

- Notificaciones push en tiempo real
- Integración con webhooks de Prometheus, GlitchTip, SigNoz

6. Esquemas de Integración

En Rankmi contamos con 3 modalidades de integración segura, las mismas que son descritas a continuación:

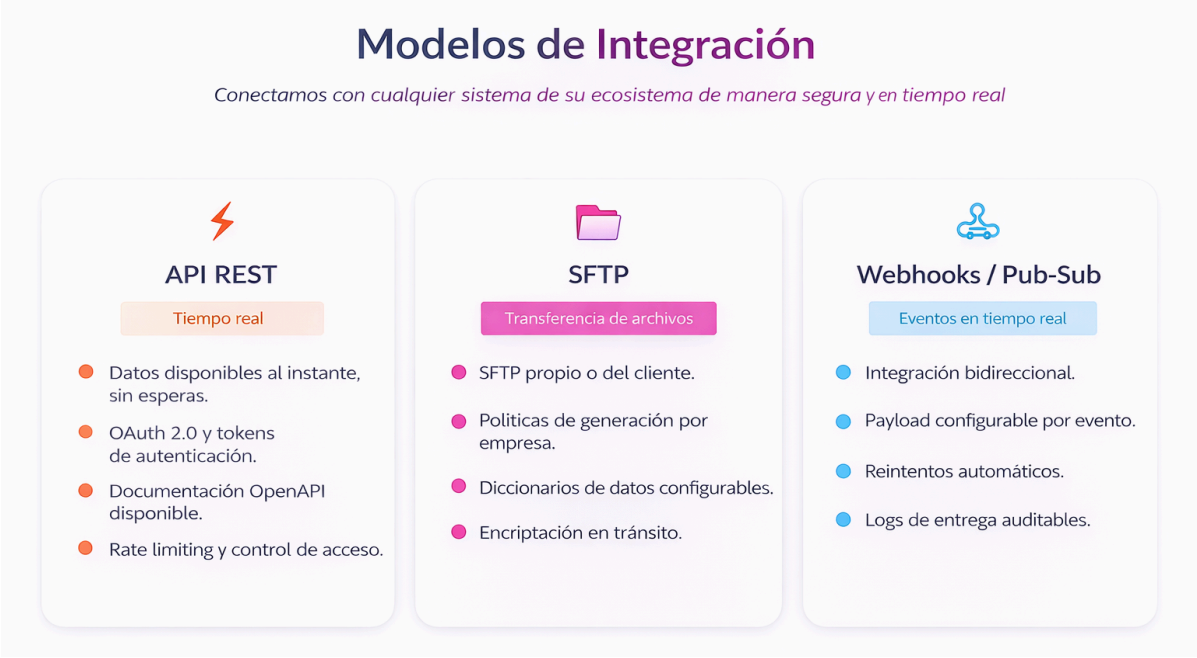

***Imagen 8**. Evidencia de VPCs configuradas*

7. Capacidad Transaccional

La capacidad transaccional de Rankmi está concebida para ser un sistema de alto rendimiento, elástico y desacoplado, diseñado para manejar virtualmente infinitas segmentaciones de datos y cálculos intensivos en tiempo real. Esta capacidad se sustenta en tres pilares:

1. Una infraestructura de cómputo sobre Amazon EKS que utiliza Horizontal Pod Autoscaling (HPA), permitiendo que microservicios críticos como CORE API, Payroll y LMS escalan de forma independiente ante picos de demanda.
2. Una capa de datos robusta que combina la estabilidad de Amazon Aurora con una estrategia de caché intensiva mediante Memcached sobre Elasticache, optimizando la velocidad de respuesta para los datos más consultados
3. Finalmente, una arquitectura Event-driven (asíncrona) soportada por SNS, SQS y Kafka, que garantiza que las transacciones y comunicaciones entre servicios no se bloqueen entre sí, permitiendo una integración bidireccional y una disponibilidad de datos al instante.

Todo este ecosistema es acelerado globalmente por CloudFront, asegurando que la capacidad transaccional se mantenga fluida y con baja latencia para nuestros clientes.

8. Cumplimiento Normativo ISO 27001/27701/37001

Rankmi está certificada en ISO 27001:2022, ISO 27701:2019 e ISO 37001:2016. La arquitectura de infraestructura ha sido diseñada explícitamente para soportar estos estándares internacionales.

8.1 Mapeo de Dominios ISO 27001

Control de Acceso (A.9)

- A.9.1: Principio de menor privilegio en todos los niveles
- A.9.2: Teleport + Keycloak para gestión centralizada
- A.9.3: MFA obligatorio + políticas de contraseñas fuertes
- A.9.4: Security Groups y Network ACLs

Criptografía (A.10)

- A.10.1: Política de criptografía documentada
- A.10.2: TLS 1.3 en tránsito; AES-256 en reposo
- A.10.3: Gestión de claves mediante AWS KMS

Seguridad Operacional (A.12)

- A.12.2: GitOps mediante ArgoCD
- A.12.4: Logging (CloudTrail, pgAudit, Rankmi Audit)
- A.12.5: Escaneo de vulnerabilidades en contenedores
- A.12.6: Backups Multi-AZ con replicación a otras regiones

9. Conclusión

La infraestructura de Rankmi representa un esfuerzo coordinado de modernización, seguridad y cumplimiento normativo. Rankmi mantiene certificaciones ISO 27001:2022, ISO 27701:2019 e ISO 37001:2016, garantizando que cada componente ha sido diseñado conforme a estándares internacionales. Este documento sirve como referencia técnica para clientes, auditores y reguladores que deseen validar la postura de seguridad.

Aprobación

Los miembros del Comité Directivo que aprueban la versión vigente de la presente política es:

Nombre	Cargo	Fecha de la Revisión
Diego González	Head of Security	10-04-2026
Daniel Ramirez	VP of Engineering	10-04-2026
Franco Quijano	Head of Infrastructure	10-04-2026
Felipe Mundaca	CTO	10-04-2026