



Arquitectura Empresarial

**Grupo 2**

# **Combi Zajana SAS**

*Juan David Cetina, Ana Lucía Quintero y Mariana Salas*

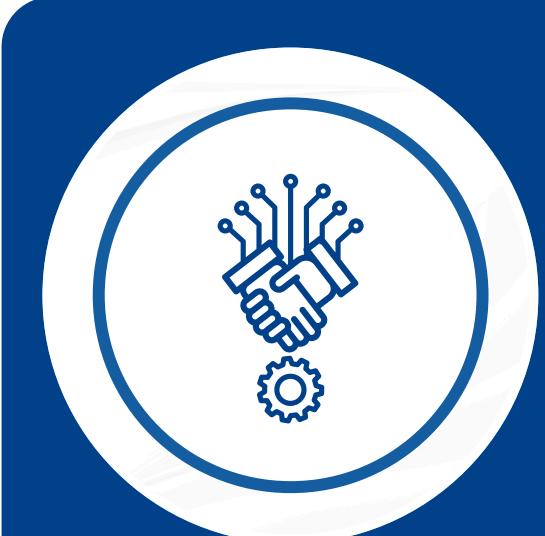


# ¿QUIÉN ES EL CLIENTE?



## Nombre

Zajana SAS



## Sector Económico

Cuaternario



## Empleados

32  
empleados



## Clientes Activos

Alrededor de  
120



## Ubicación

Cl. 98 #64,  
Bogotá

## ¿Qué hacen?

Desarrolla **modelos predictivos** para optimizar la **gestión del ciclo de crédito**, lo que permite a entidades financieras, bancos, FinTech, empresas de cobranza y otros sectores tomar decisiones más informadas.

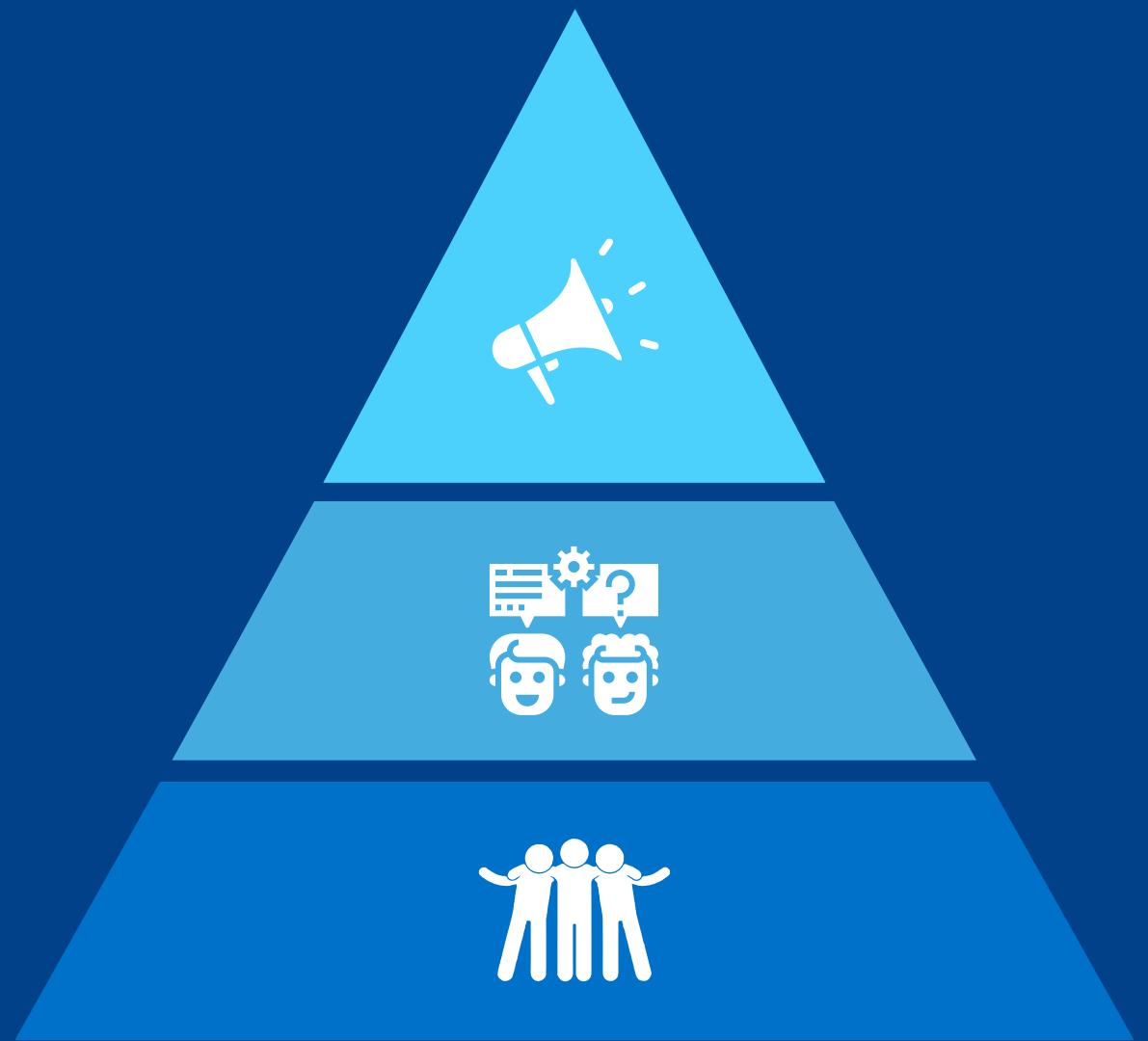
**Producto principal:** Macia

# Objetivos Estratégicos

**O1** Búsqueda de **eficiencias** operativas y administrativas dentro de las áreas.

**O2** Fortalecer su **presencia** en el mercado mexicano con el producto Macia México.

**O3** Mejorar la **toma de decisiones** crediticias mediante el desarrollo y posicionamiento de scores que brinden trazabilidad y observabilidad del ciclo de vida crediticio de las personas.



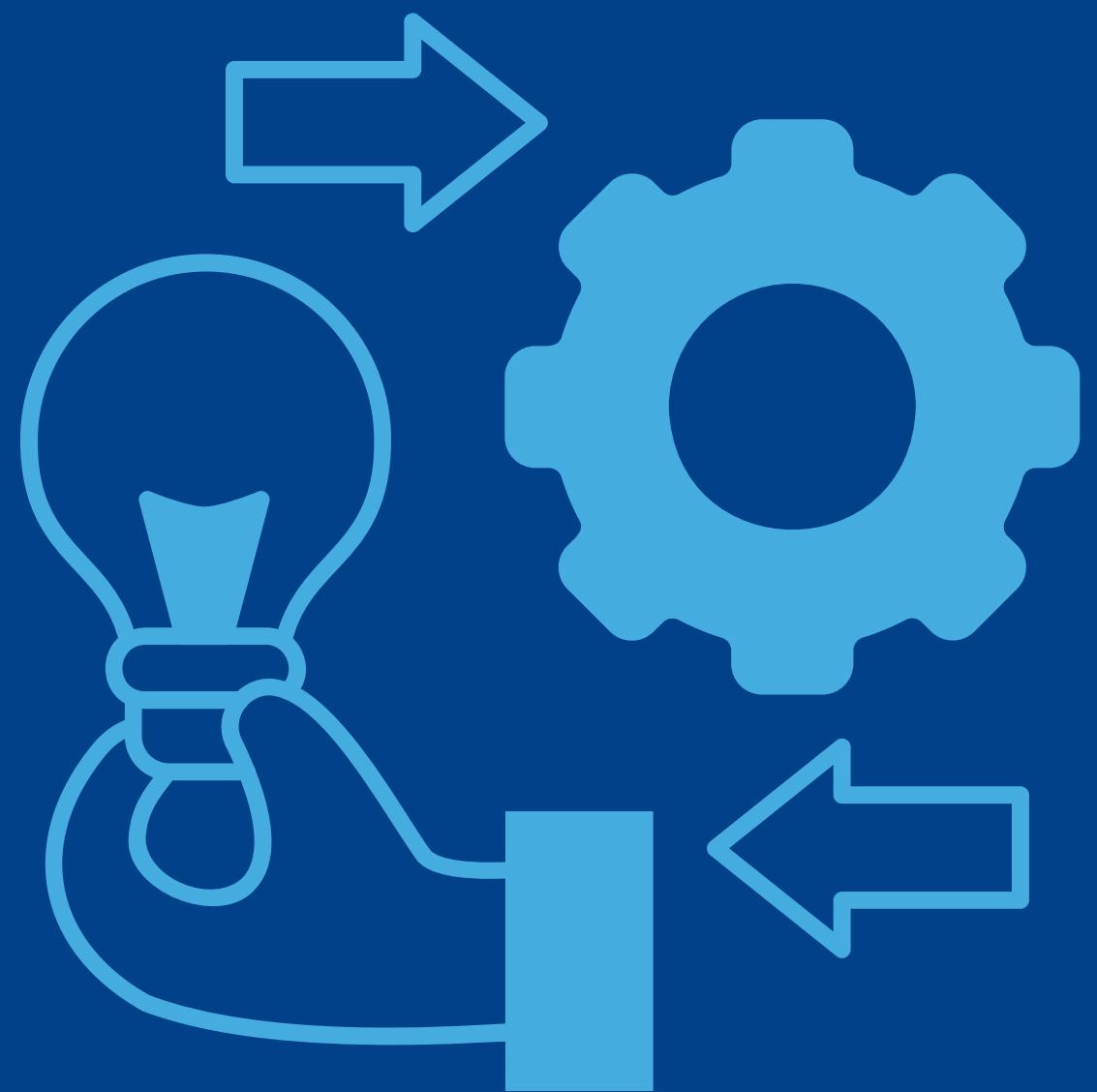


The background features a dark blue gradient with several large, semi-transparent light blue circles of varying sizes scattered across the frame. Overlaid on this is a faint, light blue network of interconnected dots and lines, resembling a complex web or a molecular structure.

# AS-IS

# Procesos Clave

- 01** Oportunidades de negocio y definición de producto
- 02** Diseño y desarrollo de la solución
- 03** Fuentes de información y autorización

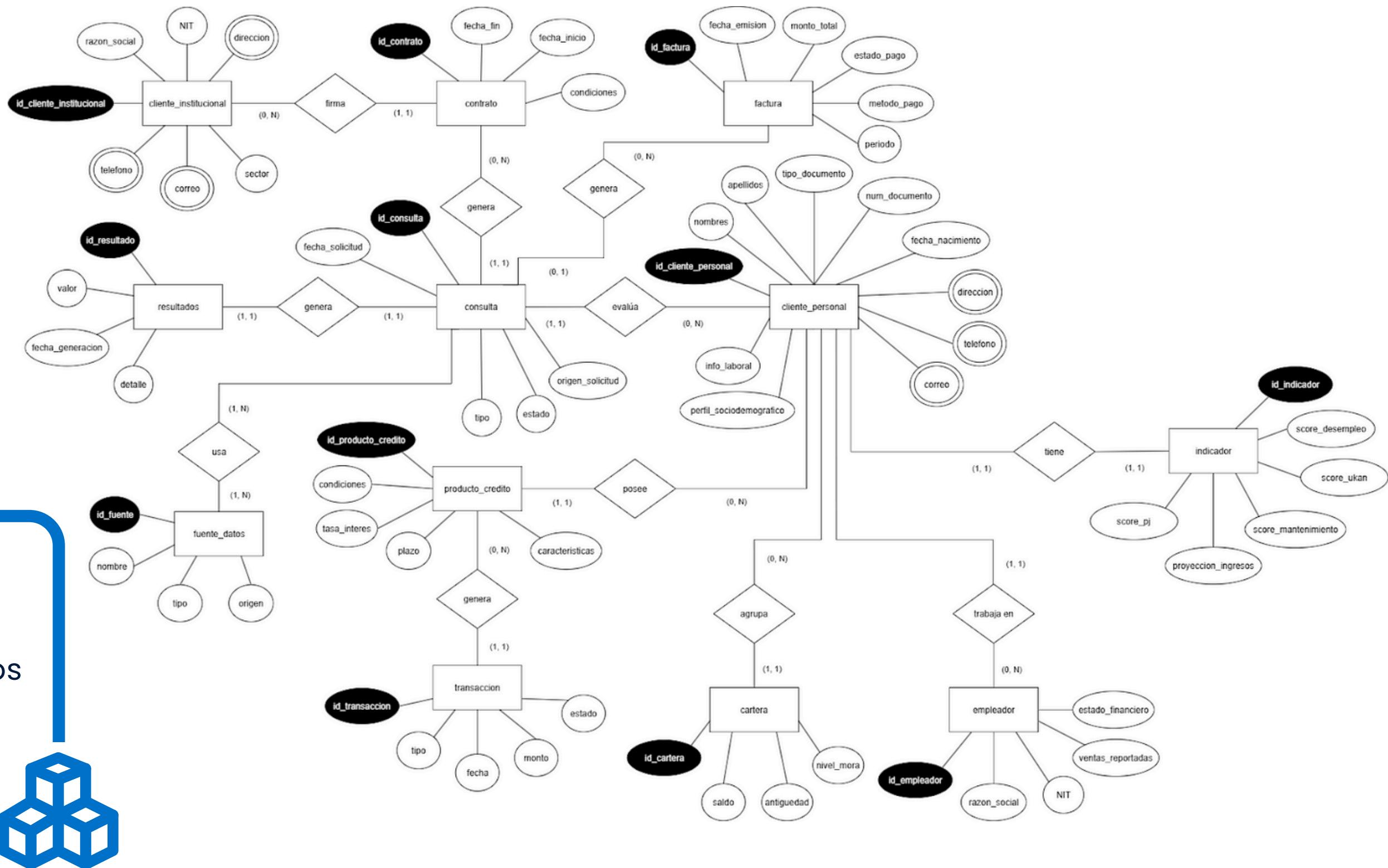


## Principales flujos de información. **Dimensiones:**

- **Administrativa:** clientes, contratos y facturación.
- **Analítica:** consultas, resultados, fuentes e indicadores de riesgo.

## Relaciones

- Cliente institucional **contrata** servicios
- Solicitudes generan **consultas** sobre clientes personales
- **Cálculo** de indicadores con dichas consultas
- Fuentes de datos externas **proveen** para análisis
- Facturación asociada al **consumo** de consultas

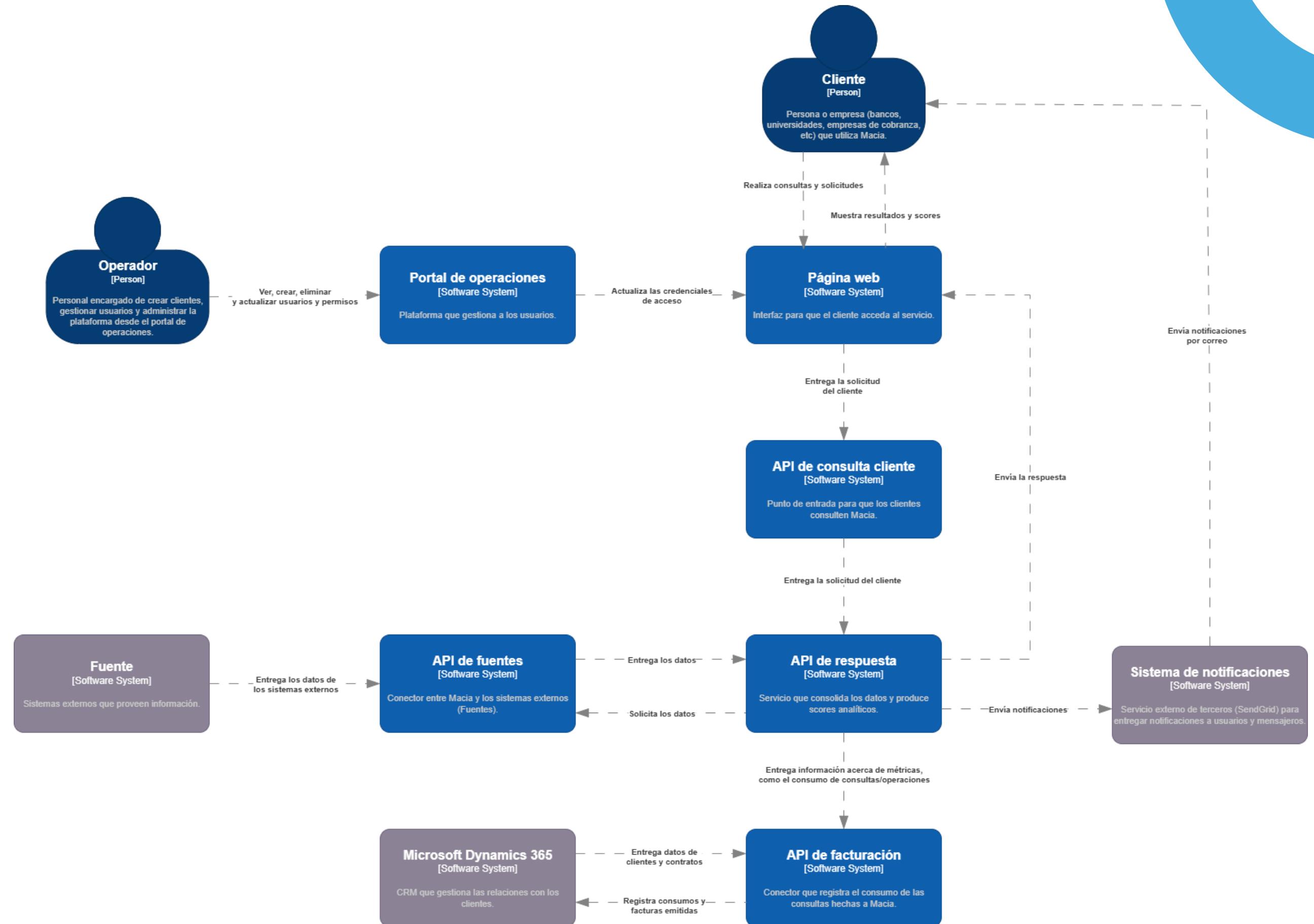
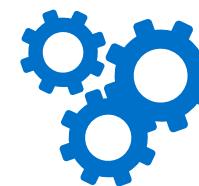


# ERD

# C1: Contexto

## Sistemas

- **Portal de operaciones** para gestionar accesos.
- **Página web** para solicitudes de clientes.
- **API de consulta** como punto de entrada.
- **API de respuesta** que genera scores analíticos.
- **API de facturación** que registra consumos.
- **API de fuentes** extrae la información.

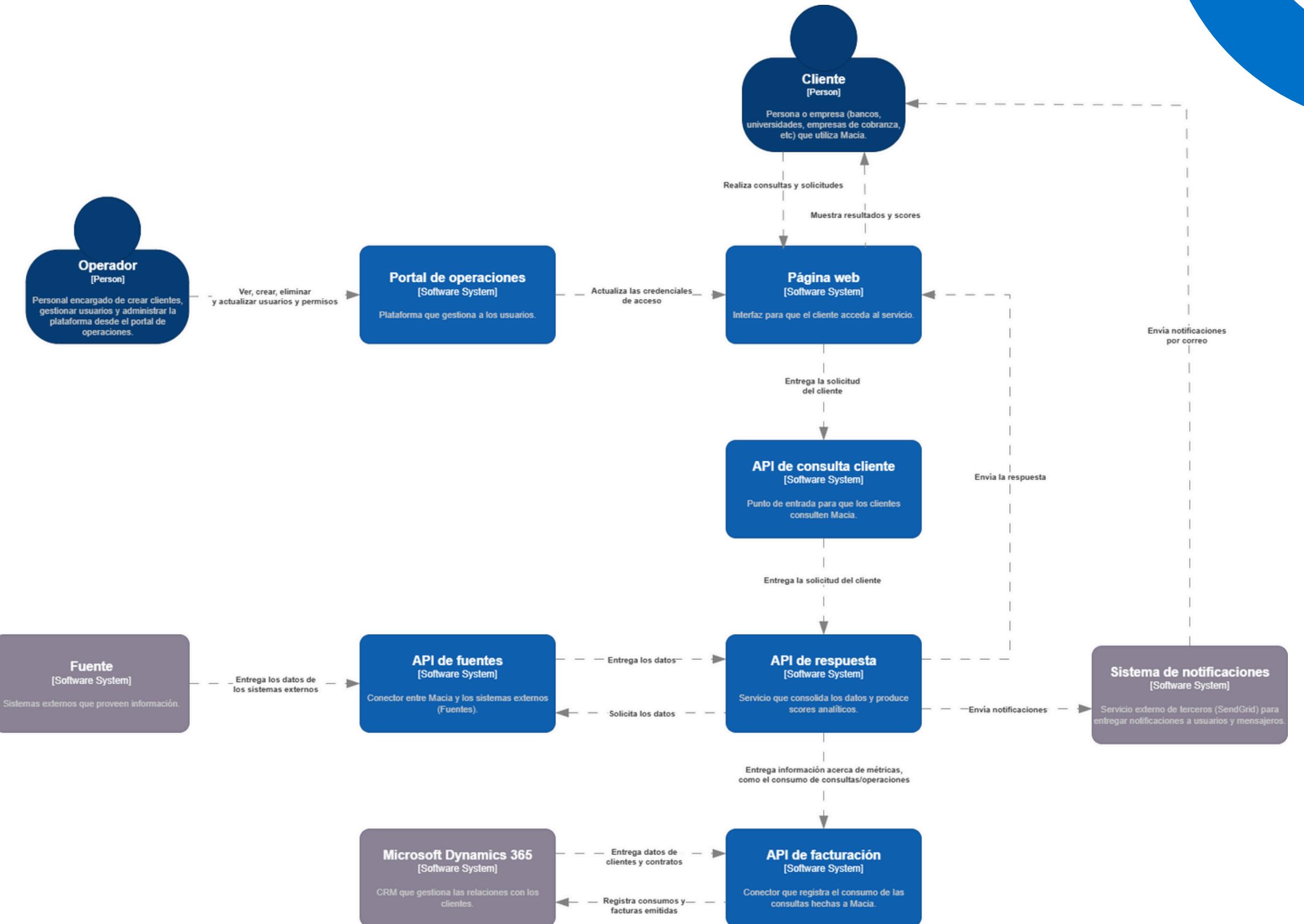


## Sistemas externos

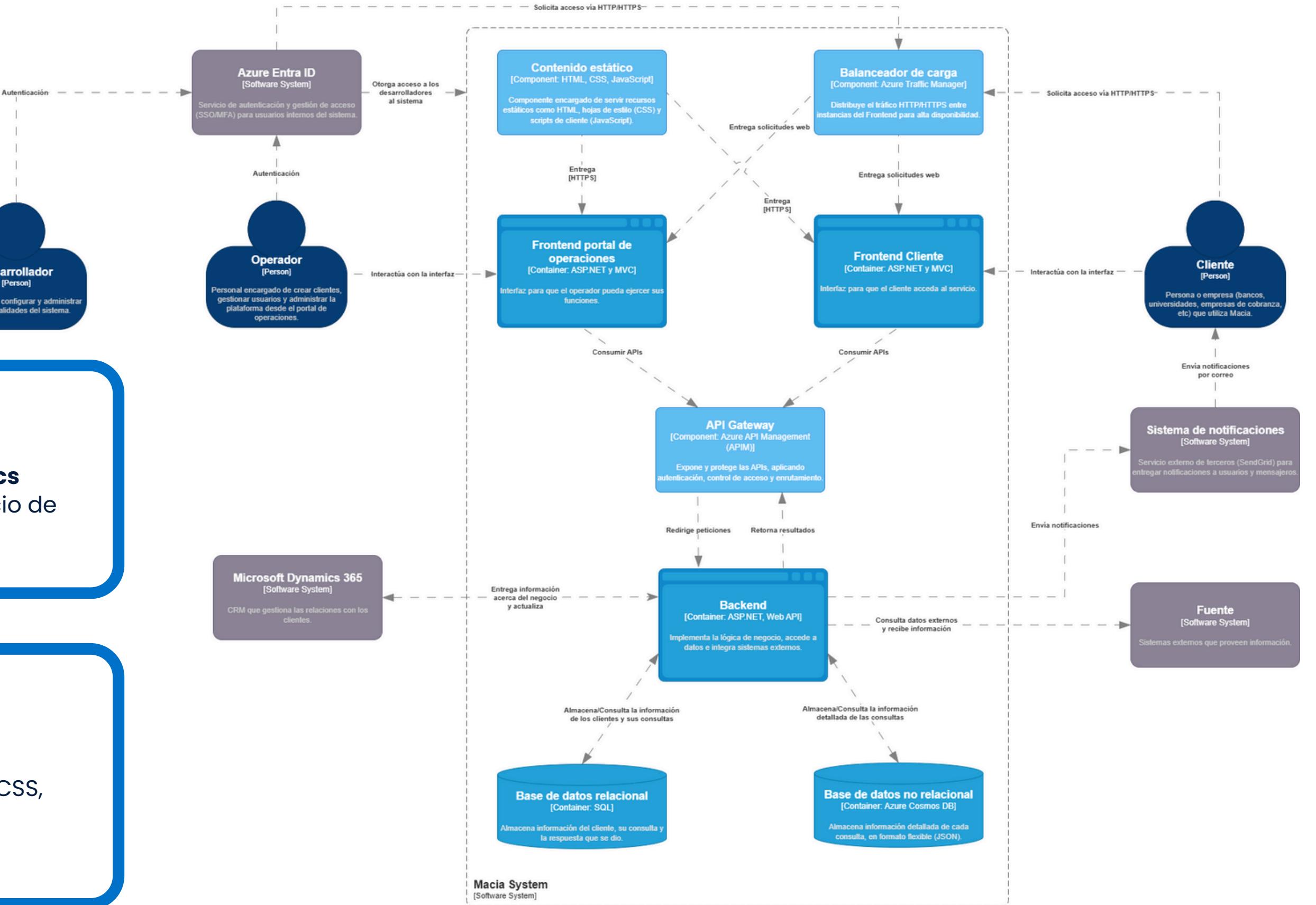
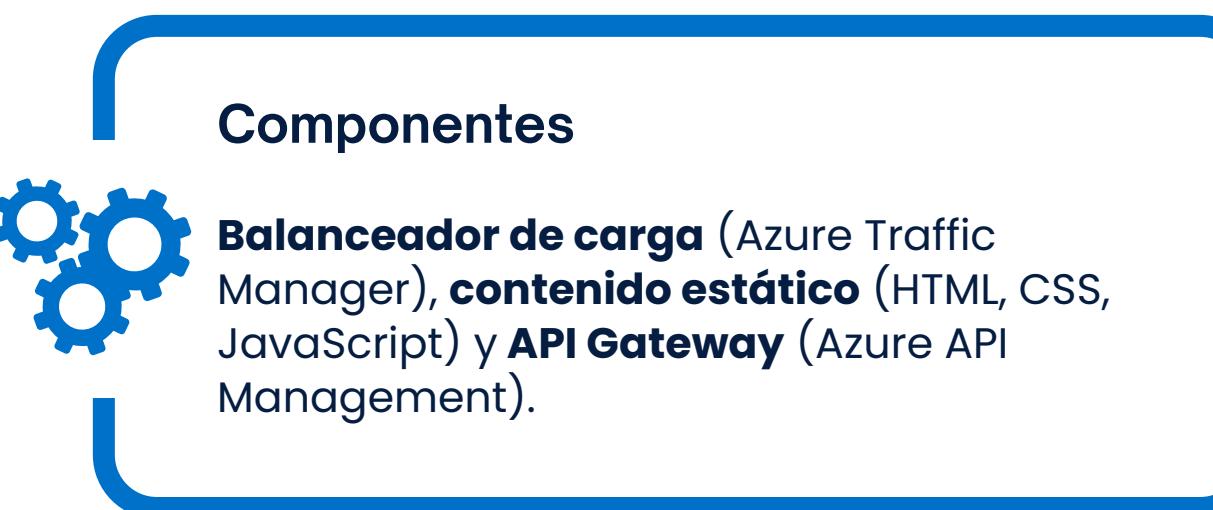
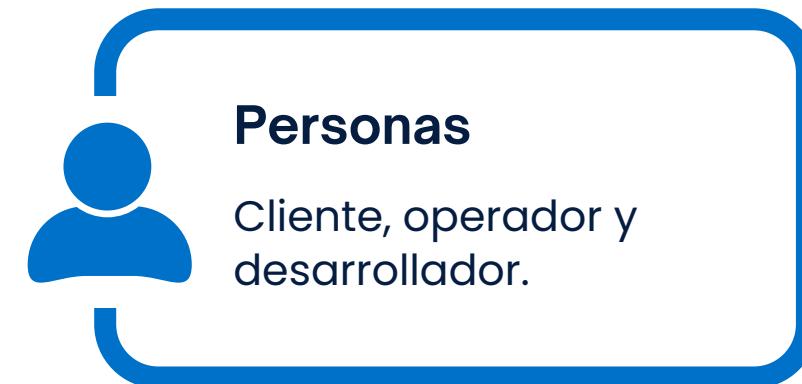
Fuentes de datos que proveen información, **Microsoft Dynamics 365** (CRM) y **SendGrid**, sistema de notificaciones que envía alertas a los usuarios.

## Personas

**Cliente** (usuarios que usan Macia) y **operador** (personal encargado de crear clientes, gestionar usuarios y administrar accesos en el portal de operaciones).

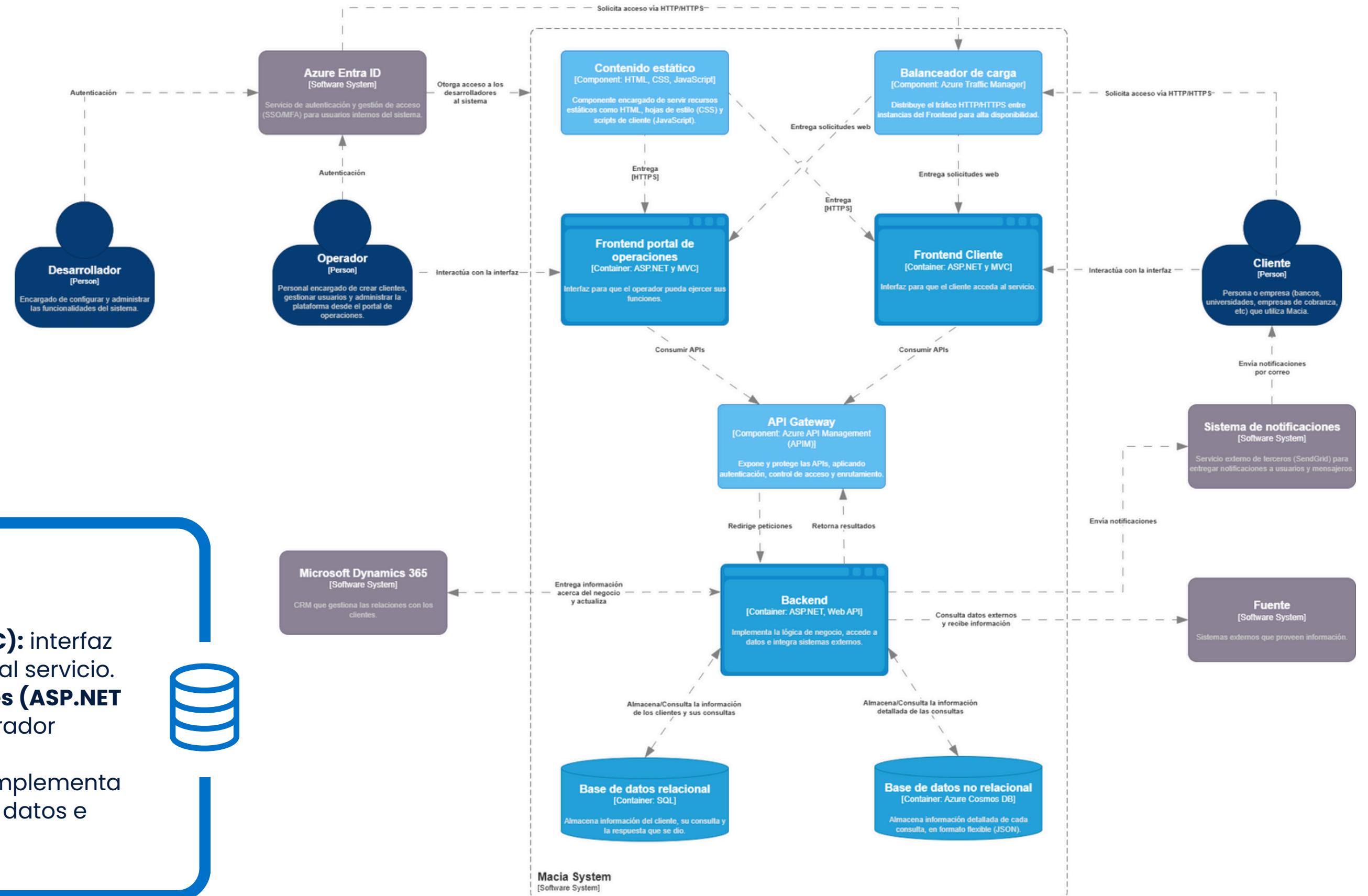


# C2

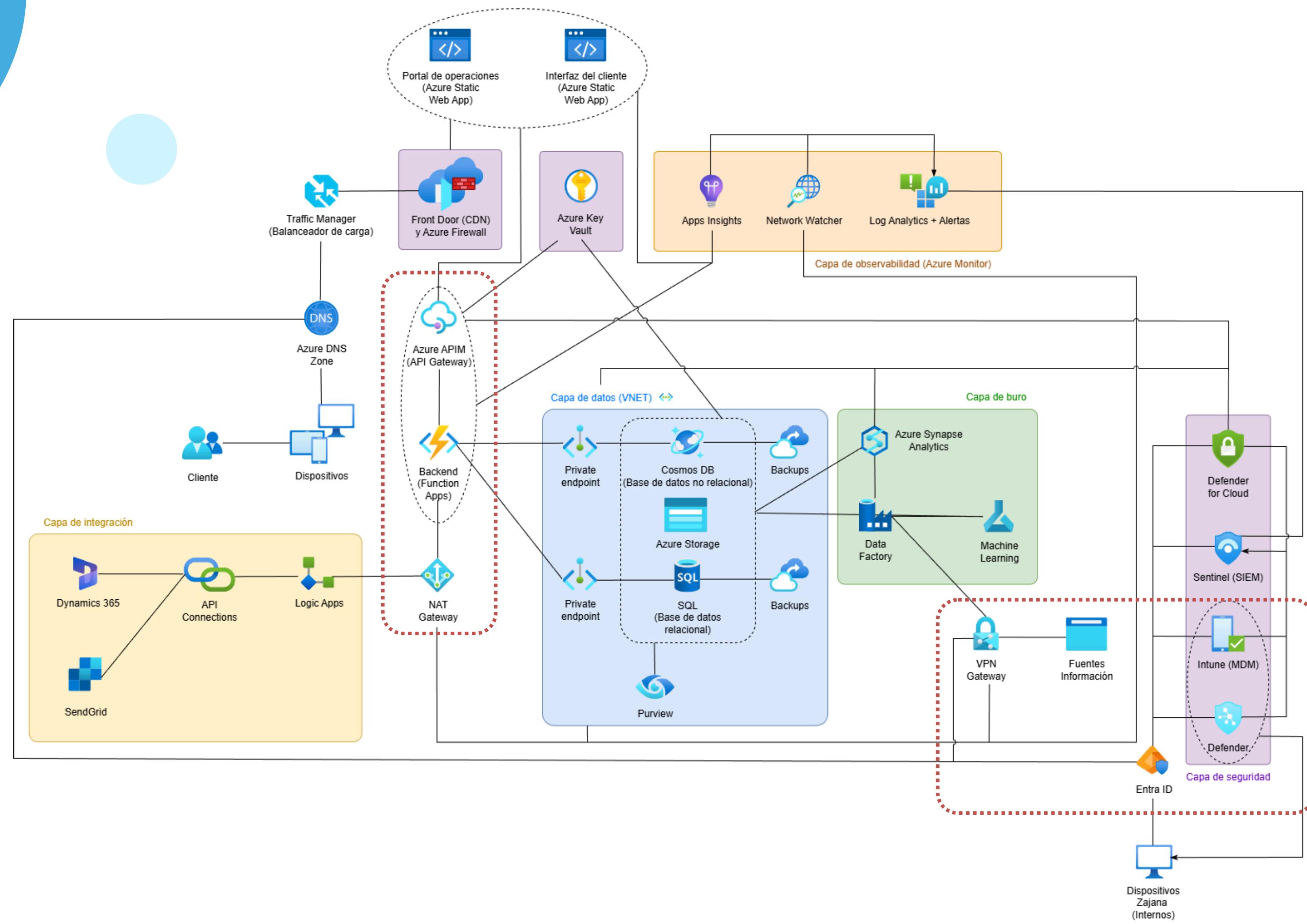


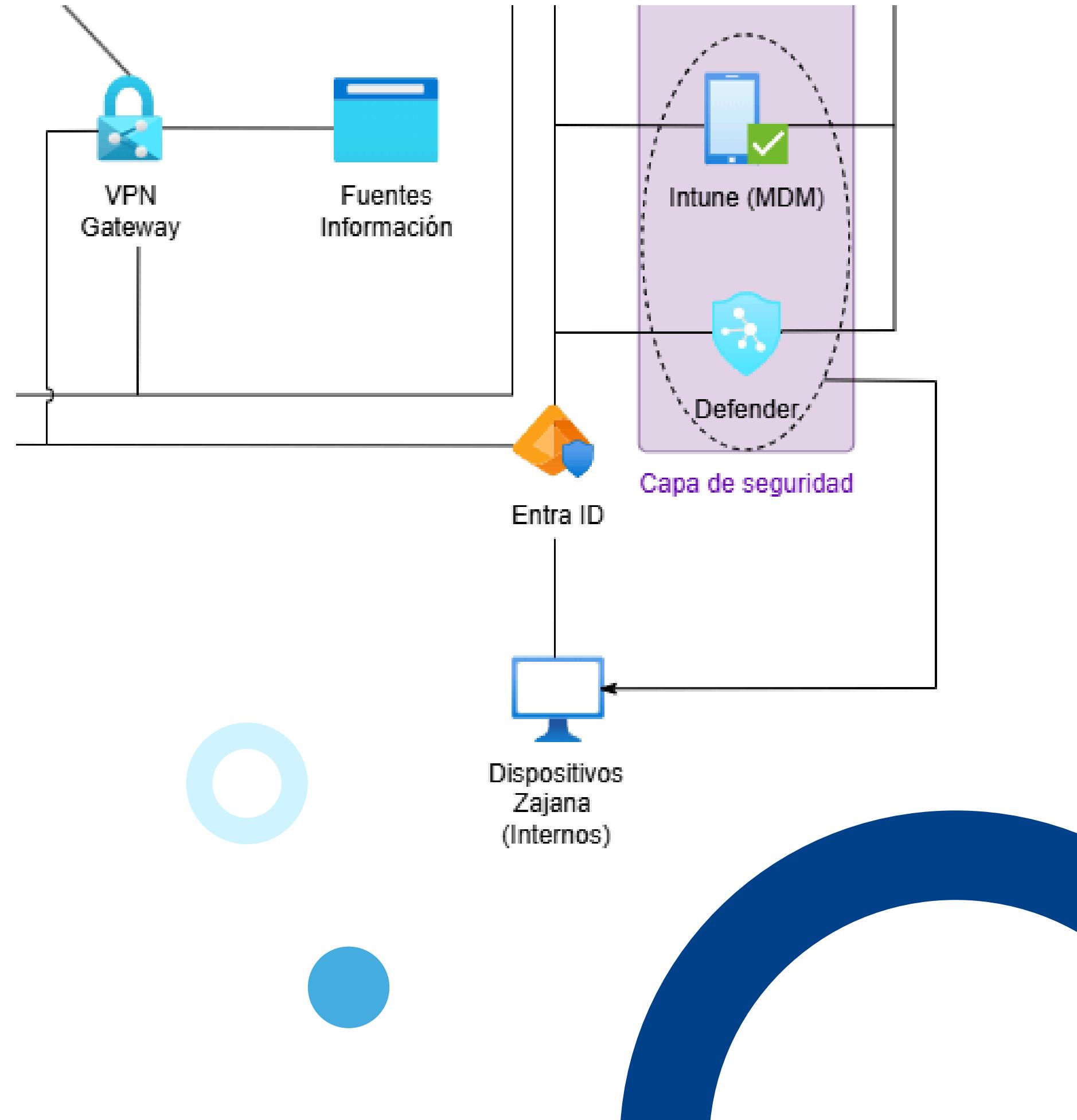
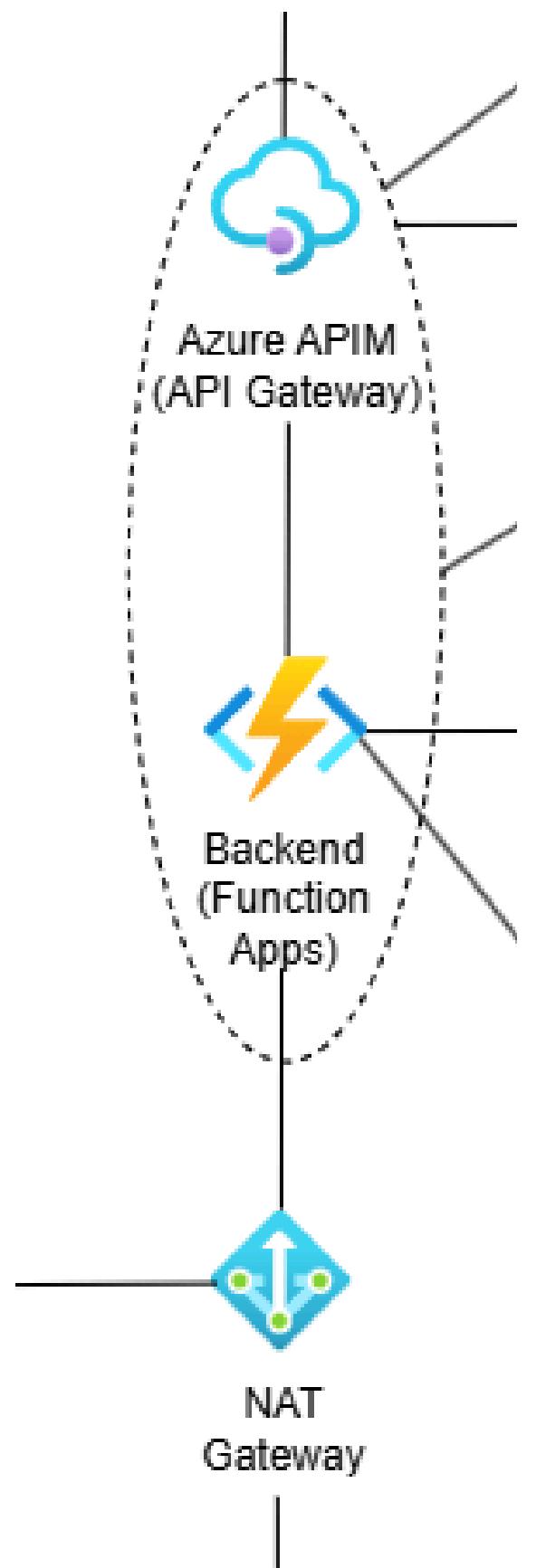
## Bases de datos

- **Base de datos relacional (SQL):** almacena información de clientes y respuestas de consultas.
- **Base de datos no relacional (Azure Cosmos DB):** guarda información detallada de cada consulta en formato JSON.



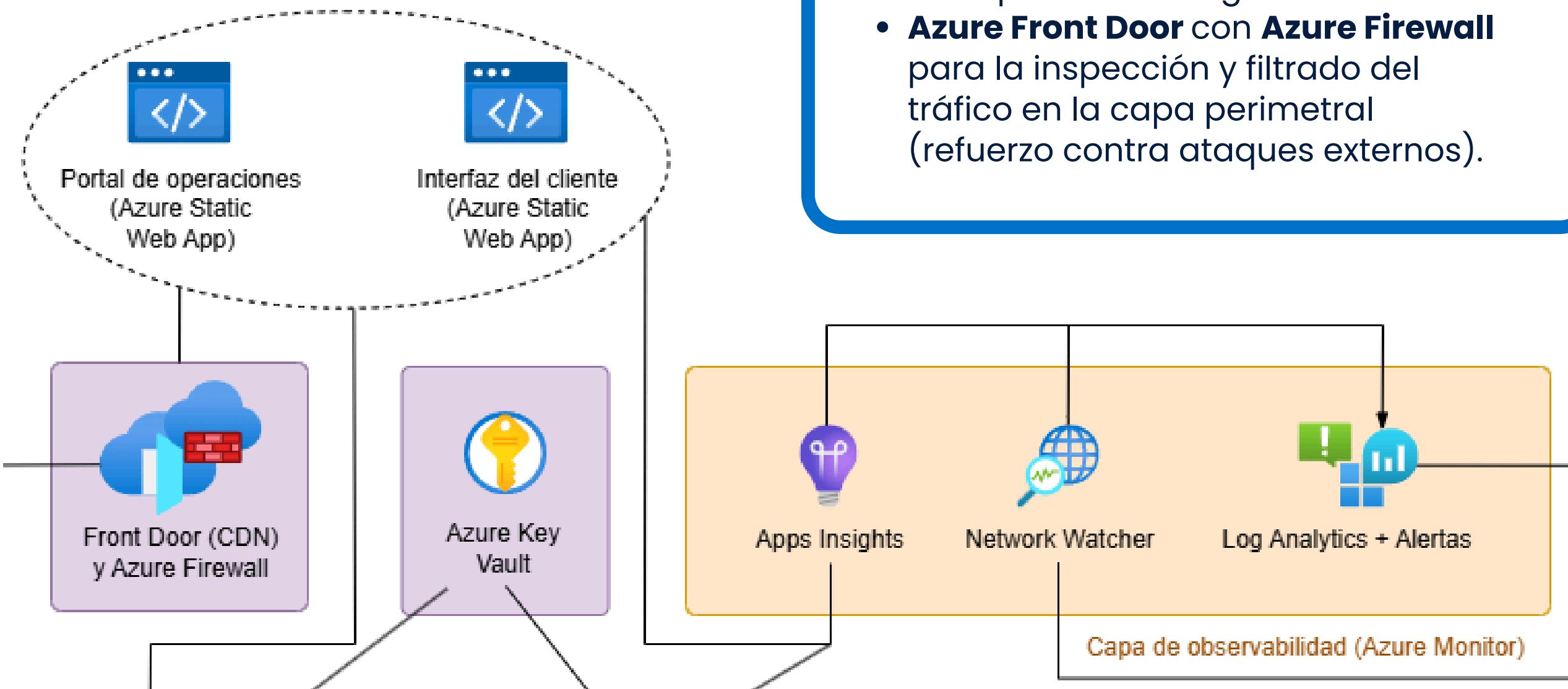
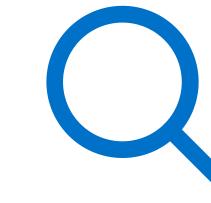
# Infraestructura Lógica





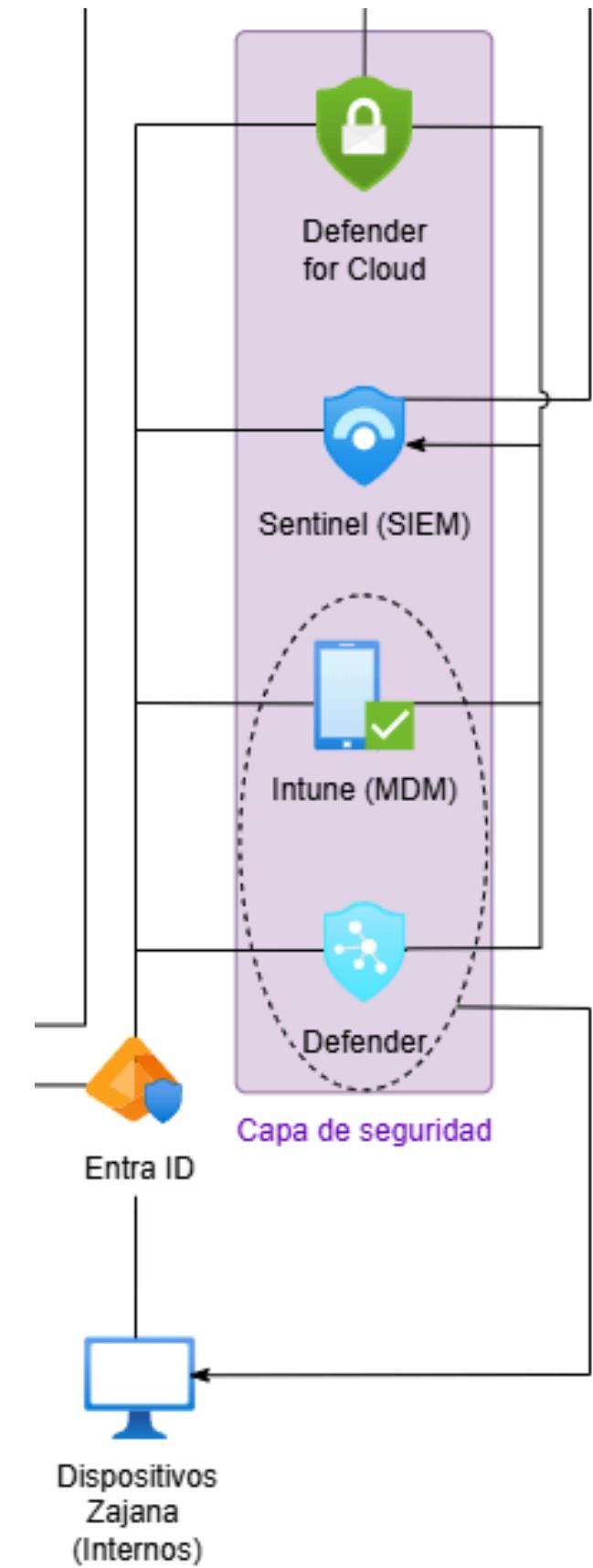
## Capa de Observabilidad

- **Azure Monitor:** monitorea aplicaciones, red y desempeño en tiempo real.



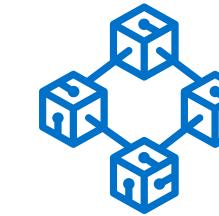
## Capa de Seguridad

- **Microsoft Intune (MDM)** y **Microsoft Defender**
- **Microsoft Sentinel (SIEM)** recoleta logs, alertas y eventos.
- **Defender for Cloud** para monitoreo de la postura de seguridad.
- **Azure Front Door** con **Azure Firewall** para la inspección y filtrado del tráfico en la capa perimetral (refuerzo contra ataques externos).



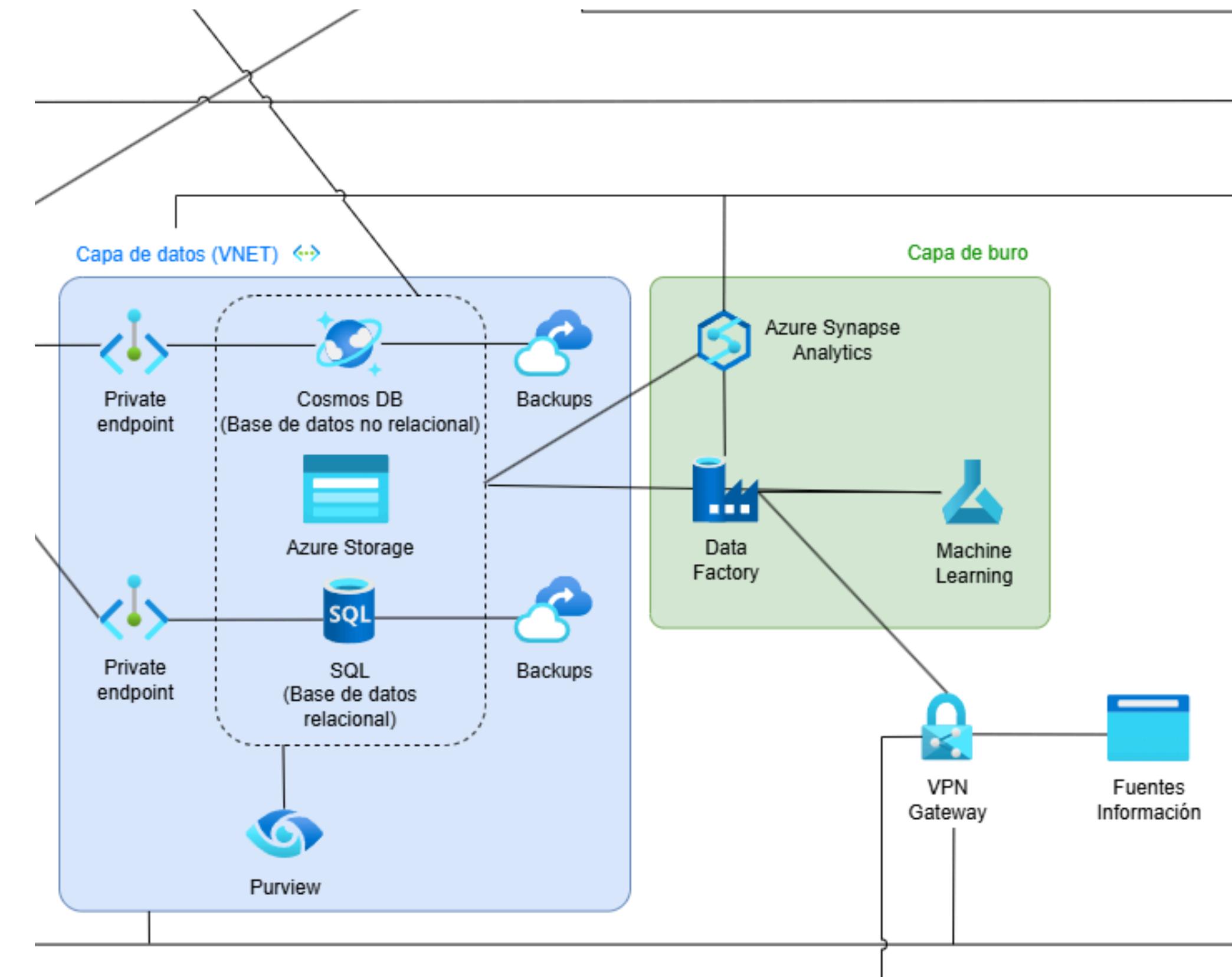
## Capa de Buro

Integración segura de datos,  
procesamiento protegido y modelado.  
**Data Factory, Azure Synapse  
Analytics y Azure ML**



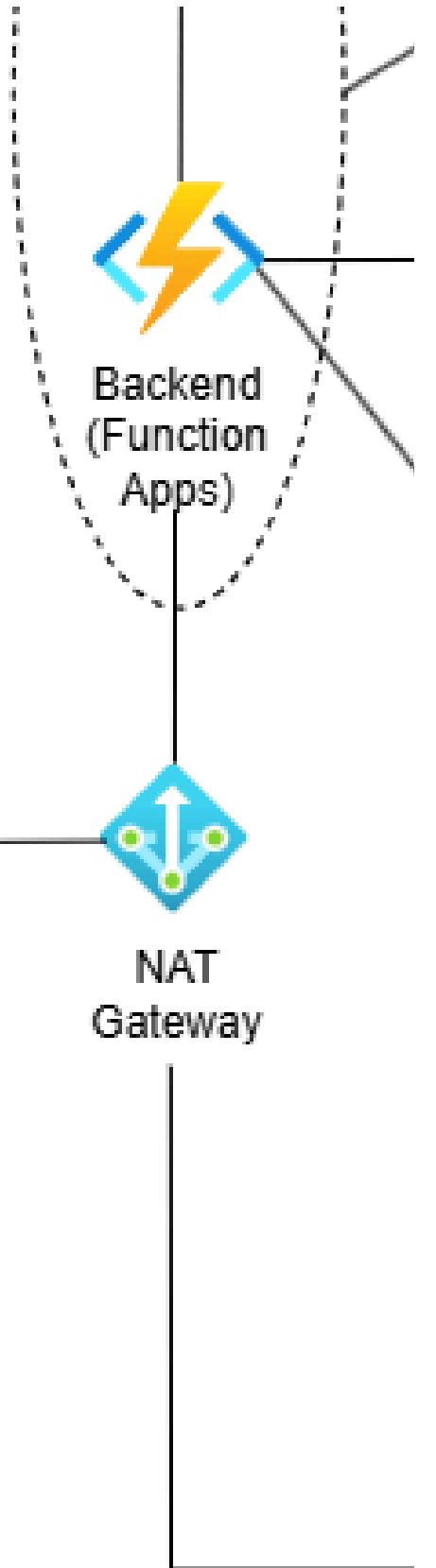
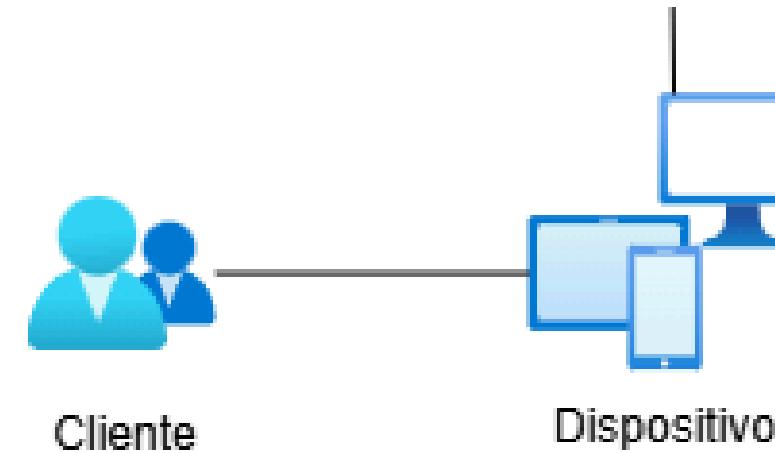
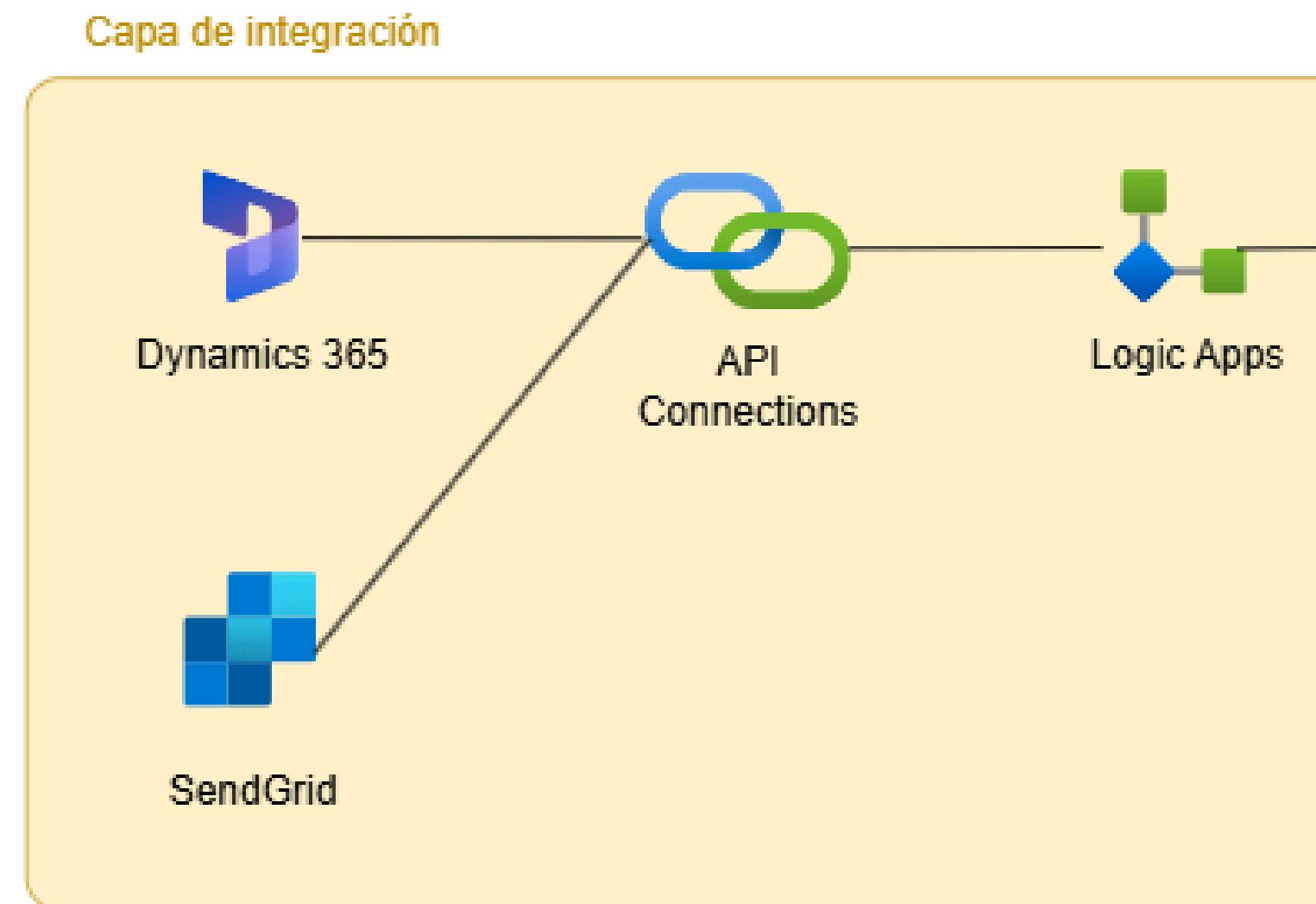
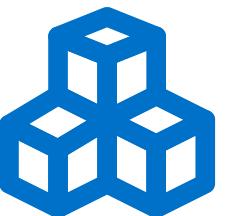
## Capa de Datos

- **VNET y private endpoints** para aislamiento lógico.
- **Azure Key Vault** para gestionar credenciales, copias de seguridad cifradas.
- **Purview** para gobernanza de datos.



## Capa de Integración

- **Dynamics 365 (CRM)** para administrar relación comercial con clientes y centralizar trazabilidad de operaciones.
- **Logic Apps y API Connections** para automatizar flujos entre aplicaciones y servicios, asegurando consistencia en intercambios de datos.
- **SendGrid** para gestionar envío de notificaciones y correos automáticos a clientes.



# Propuesta TO-BE

# Necesidades identificadas

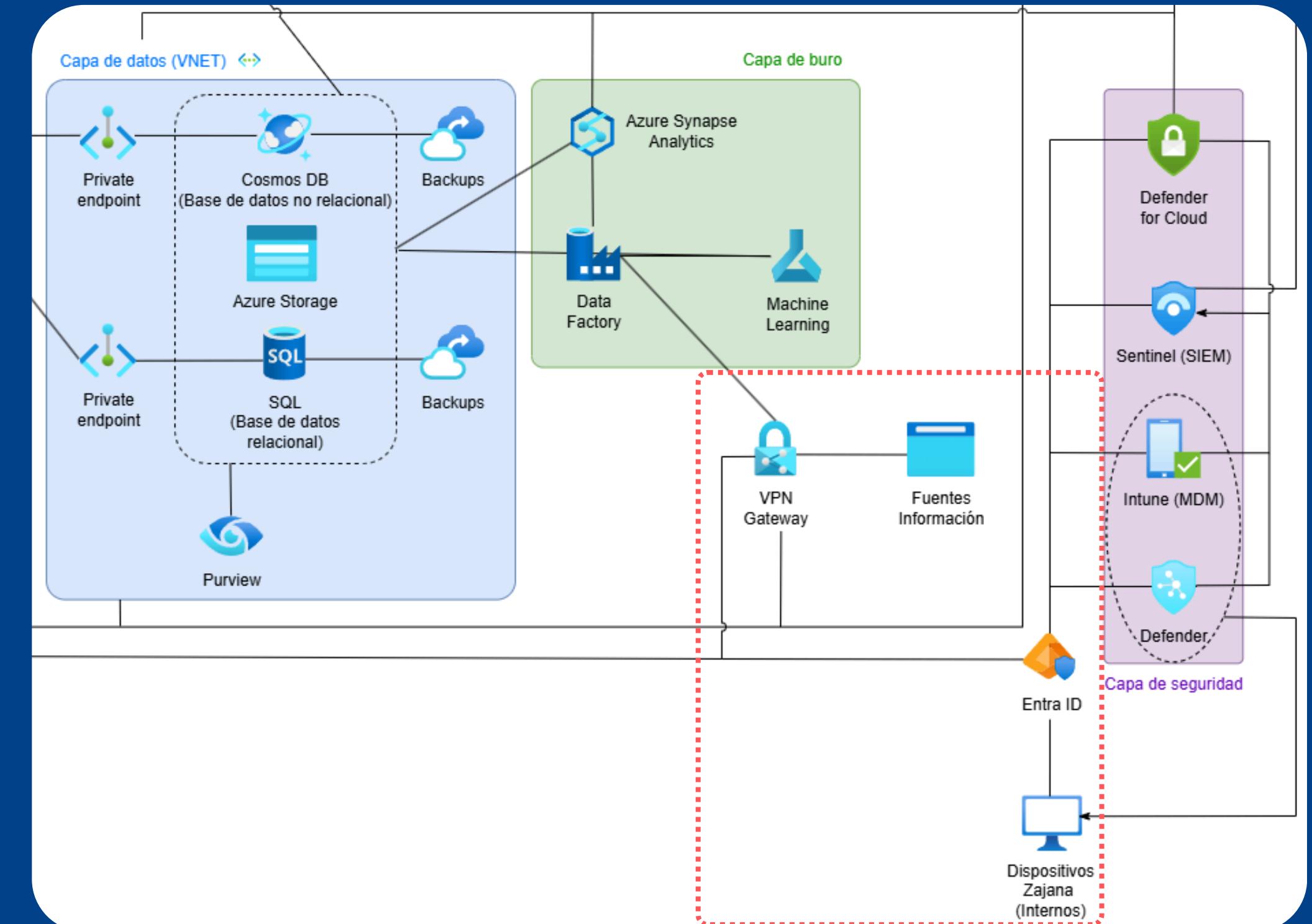
## A nivel de Infraestructura

### Dependencia exclusiva de VPN Gateway

El acceso a las fuentes de información y Data Factory está protegido solo por una VPN.

### Exposición indirecta de las fuentes

Si bien el VPN es un filtro, no hay evidencia de **firewalls de aplicación** que refuercen la seguridad, lo que deja a las fuentes expuestas a **accesos no autorizados** en caso de que la **VPN sea comprometida**.



# Ideas de mejora

## Firewall corporativo para dispositivos internos

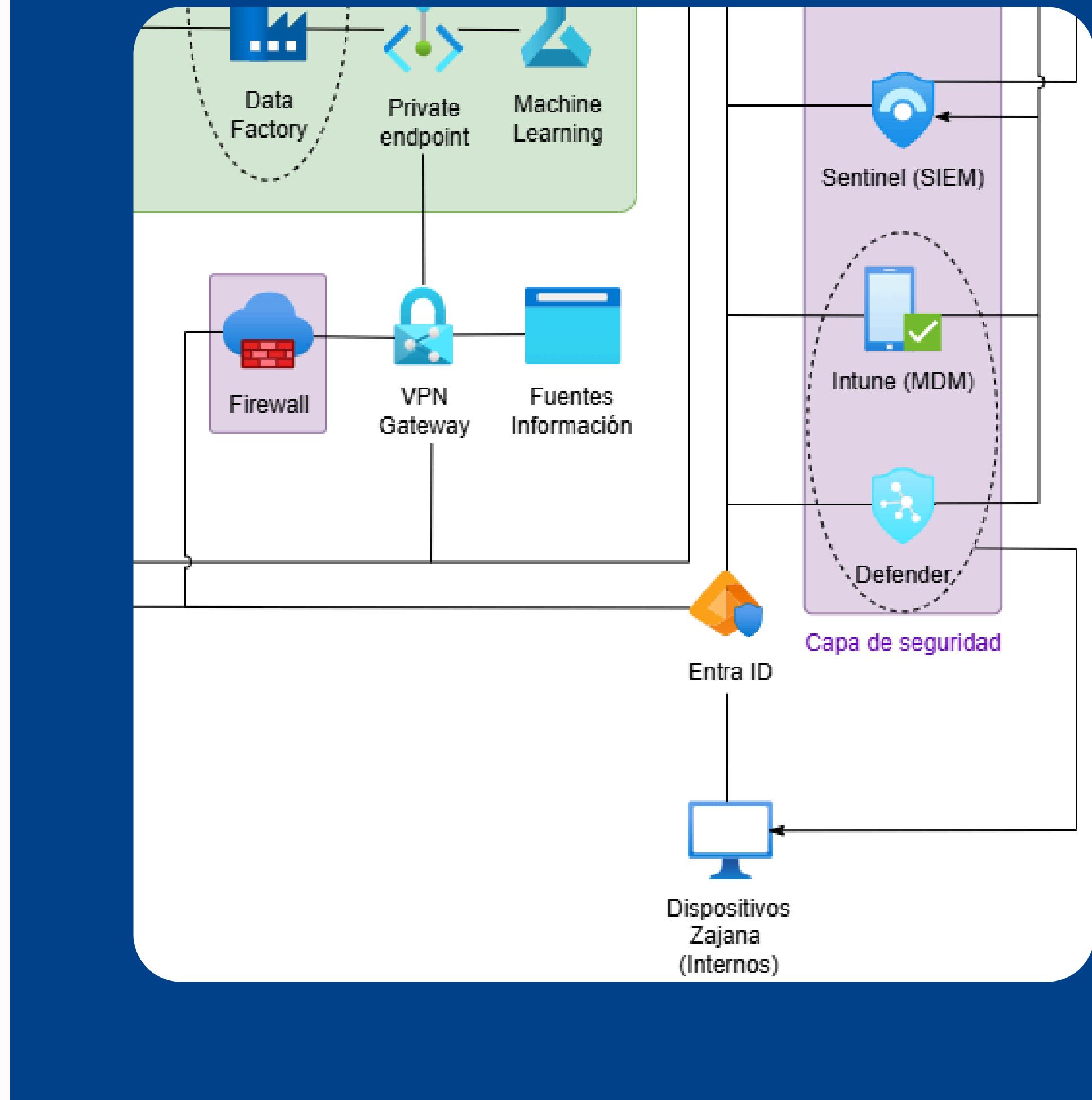
Firewall corporativo **refuerza la seguridad** al **filtrar** y **segmentar** el **tráfico** que proviene de los equipos internos hacia el buro.

- Evita que dispositivos comprometidos accedan a servicios sensibles
- Reduce riesgos de exposición no autorizada.

## VNET dedicada para la capa de buro

VNET exclusiva permite **aislar los servicios analíticos**

- Garantiza que comunicación se realice solo por endpoints privados y autorizados.
- Mejora control del tráfico y disminuye superficie de ataque.



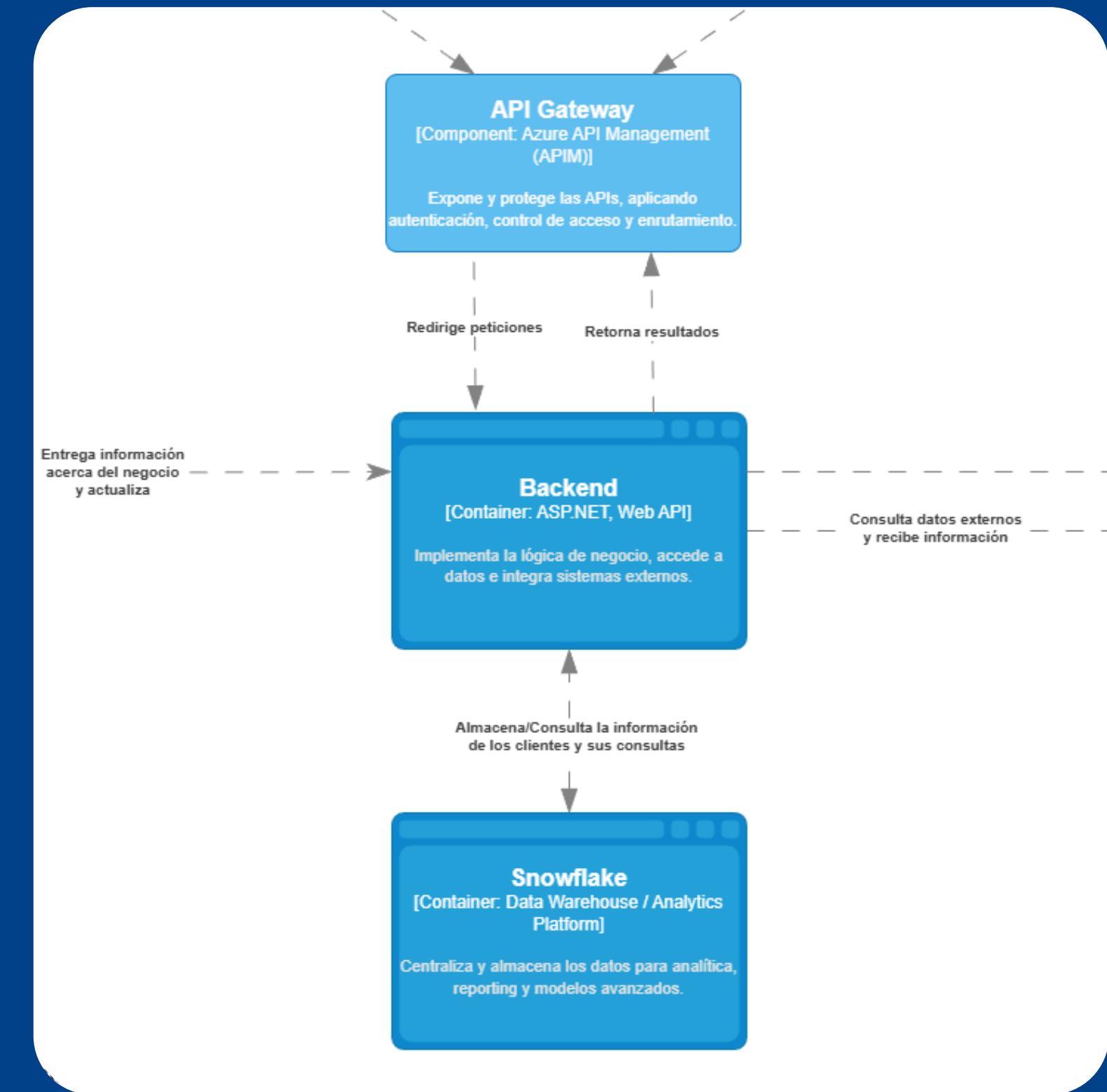
# Objetivo de la empresa

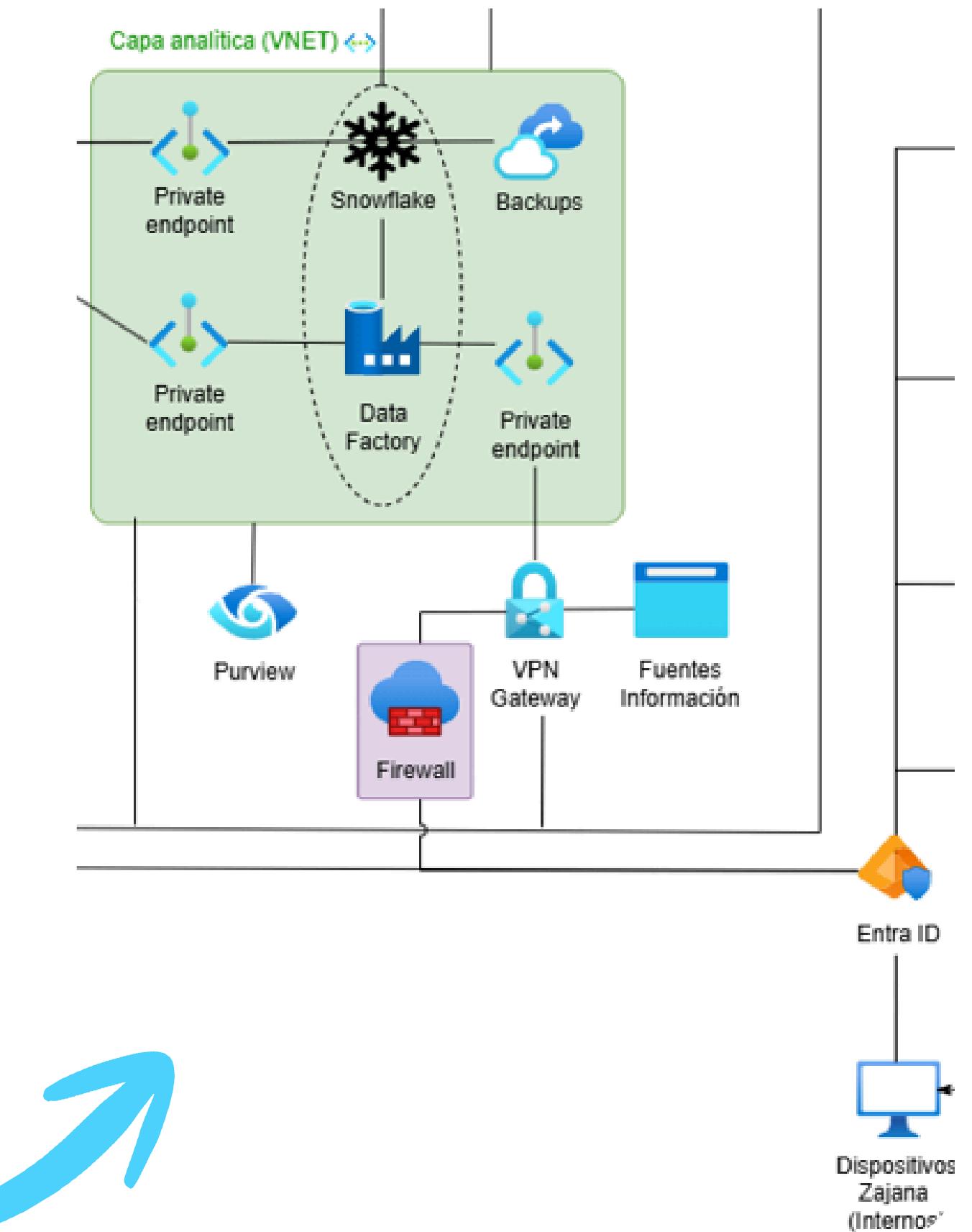
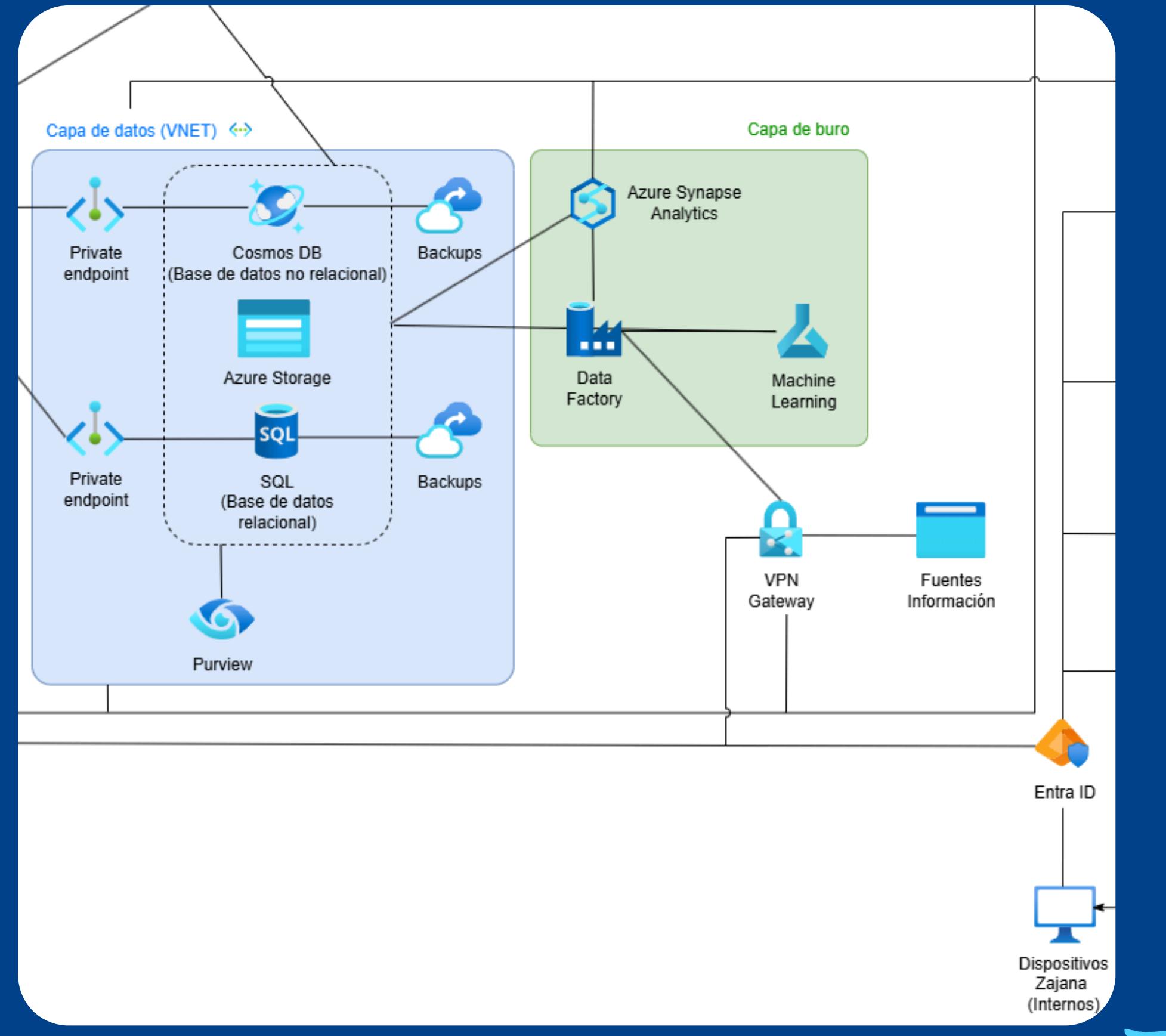
## Migración a Snowflake

La migración consiste en **retirar** SQL Database, Cosmos DB, Synapse, Delta Lake y Machine Learning Studio, para consolidar toda la gestión de datos en Snowflake.

Snowflake es una plataforma de almacenamiento y analítica, que desde un solo entorno escalable y gobernado:

- **Centraliza** la información.
- **Elimina la duplicidad** de herramientas.
- Permite realizar **consultas, reportes y modelos avanzados de machine learning**.





# PLAN DE MIGRACIÓN

## Fase 0 **Preparación**



Reducir superficie de ataque  
Conectividad segura

## Fase 1 **Diseño de la solución**



Modelo de datos en Snowflake  
Inventario de fuentes y procesos

## Fase 2 **Piloto controlado en Snowflake**



Selección del caso piloto  
Implementación pipeline

## Fase 5 **Optimización**



Ajustes de rendimiento  
Evaluación

## Fase 4 **Integración**

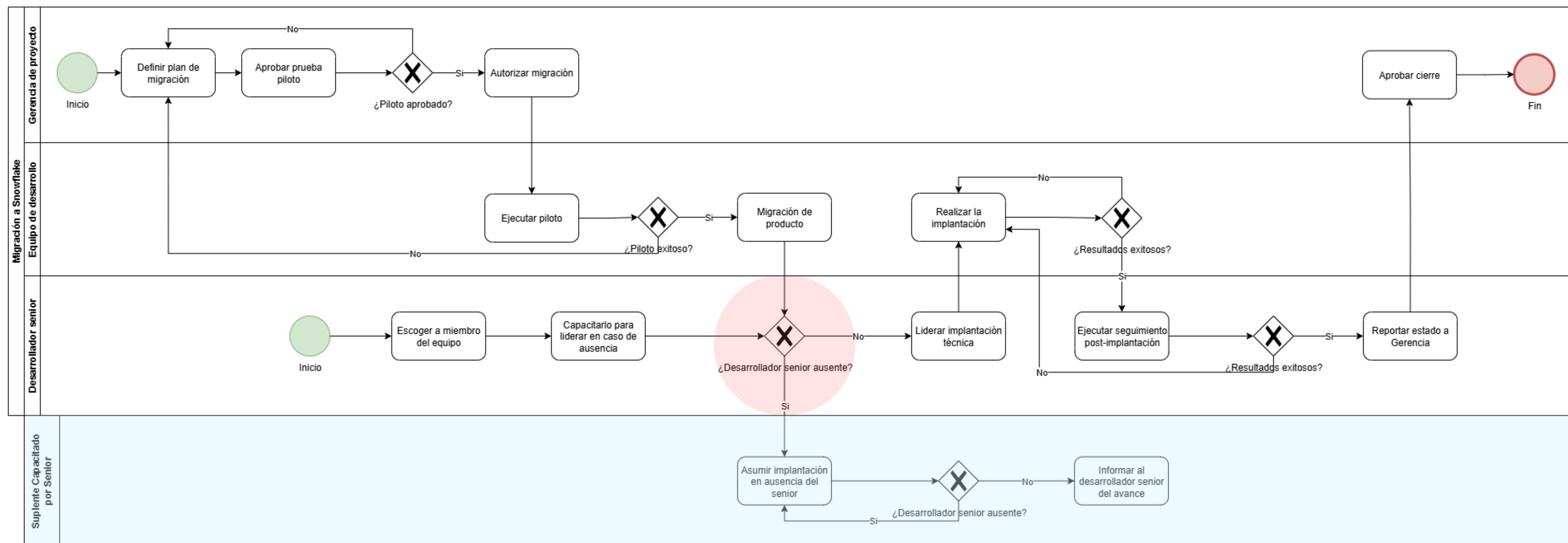


Consolidar monitoreo y seguridad  
Reducir costos y complejidad

## Fase 3 **Migración por dominios de datos**



Migrar progresivamente  
Capacitaciones internas



# STRIDE

Permite identificar **amenazas clave** y validar los **controles** necesarios para mitigarlas.

	Amenaza principal	Controles	Riesgo / Impacto
S – Spoofing	Suplantación de usuarios o servicios	Entra ID (MFA, RBAC), Key Vault	Riesgo Medio, Impacto Alto
T – Tampering	Manipulación o alteración de datos	VNET, cifrado, Private Endpoints, Backups	Riesgo Medio, Impacto Alto
R – Repudiation	Negación de acciones ejecutadas	Sentinel, Azure Monitor, auditorías	Riesgo Bajo, Impacto Medio
I – Information Disclosure	Fuga o exposición de información	Key Vault, Purview, cifrado, redes privadas	Riesgo Alto, Impacto Alto
D – Denial of Service	Interrupción por saturación o ataques	Azure Front Door, Web App Firewall (WAF)	Riesgo Medio, Impacto Alto
E – Elevation of Privilege	Escalamiento de permisos no autorizados	RBAC, MFA, Defender, Intune, Sentinel	Riesgo Medio, Impacto Alto

# Normatividad

## Checklist normativo

Categoría	Criterio de Cumplimiento	Nivel de Cumplimiento	Recomendaciones
Finalidad del Tratamiento	Los datos se usan para trámites legítimos	Alto	Garantizar que durante la migración a Snowflake se mantengan las <b>mismas condiciones</b> declaradas en las políticas de tratamiento y privacidad
Protección de Datos Sensibles	El sistema reconoce y maneja datos sensibles	Alto	Asegurar que los <b>mecanismos de cifrado y anonimización</b> actuales se mantengan durante la migración de datos a Snowflake
Seguridad y Control Normativo	Se declara que se está sujeto a normativas como la Ley 1581 de 2012 e ISO 27001	Alto	Incluir la infraestructura y los procesos de Snowflake dentro del alcance de la certificación ISO 27001 y con los lineamientos de la Superintendencia Financiera de Colombia

Categoría	Criterio de Cumplimiento	Nivel de Cumplimiento	Recomendaciones
Trazabilidad Operativa	Se tiene registro de interacciones	Alto	Integrar la <b>trazabilidad</b> de Snowflake con Sentinel y Purview para mantener una <b>cadena de custodia continua</b> entre entornos Azure y Snowflake
Clasificación de Datos	Diferenciación entre datos personales y sensibles	Alto	Asegurar que los mecanismos de cifrado y anonimización actuales se mantengan durante la migración de datos a Snowflake
Seguridad y Control Normativo	Política de retención según finalidad y supresión o anonimización de datos	Alto	Configurar en Snowflake <b>políticas de retención automática</b> mediante funcionalidades como Time Travel y Fail-safe, alineadas con las políticas de Purview
Auditoría	Auditorías para verificar el cumplimiento de políticas y controles	Alto	Continuar realizando <b>auditorías periódicas</b> y manteniendo la certificación ISO

# Beneficios y Riesgos

Beneficio	Riesgo
Mayor <b>eficiencia operativa</b> por integración y consolidación de datos	Complejidad en la migración desde SQL, Cosmos DB y Synapse hacia Snowflake
Mejora en la <b>satisfacción del cliente</b> gracias a mayor disponibilidad y seguridad	Dependencia tecnológica de Snowflake como proveedor principal
<b>Escalabilidad</b> flexible para manejar grandes volúmenes de datos	Curva de aprendizaje del personal técnico con nuevas herramientas
<b>Firewall</b> corporativo que protege de accesos y amenazas internas	Posibles <b>costos adicionales</b> por su administración y mantenimiento
<b>VNET</b> dedicada que aísla servicios sensibles y evita exposición pública	Dependencia de la conectividad y disponibilidad de la nube
Reducción de dependencia de personal específico	<b>Retrasos iniciales</b> por la capacitación del suplente

# Conclusiones

- Arquitectura actual cuenta con bases sólidas en Azure y un camino ya iniciado hacia Snowflake.
- Snowflake puede fortalecer la trazabilidad, disponibilidad y gobierno del dato, manteniendo la coherencia normativa.
- Aspectos operativos pueden reforzarse para asegurar sostenibilidad en el tiempo.

# Recomendaciones

- Migración por fases, iniciando con un piloto controlado.
- Extender los controles ya implementados en Azure hacia Snowflake para mantener consistencia.
- Fortalecer la seguridad con Firewall corporativo, VNET dedicada y Private Endpoints, reduciendo dependencia en la VPN actual.
- Plan de continuidad operativa mediante documentación y transferencia de conocimiento del equipo técnico.
- Gobernanza de costos y monitoreo para optimizar el uso de Snowflake.



¡Gracias por  
su atención!