Supersubsidio

MANUAL TÉCNICO

PLATAFORMA DE INTEROPERABILIDAD DE LA SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR

SuperSubsidio
Dirección: Carrera 69 No. 25B - 44. Pisos 3, 4 y 7
Edificio World Business Port
Conmutador: (+57) (601) 348 78 00
Línea Gratuita: (+57) 018000 910 110
Correo institucional: ssf@ssf.gov.co

Contenido

1 INFORMACIÓN GENERAL 3

2 INFORMACIÓN DEL SISTEMA O APLICACIÓN 3

2.1 NOMBRE DEL SISTEMA 3
2.2 VERSIÓN DEL SISTEMA 3
2.3 IMAGEN DEL SISTEMA 4
2.4 FECHA DE ELABORACIÓN 5
2.5 ALCANCE DEL DESARROLLO 5

3 GLOSARIO DE TÉRMINOS 6

4 REQUERIMIENTOS 8

4.1 REQUERIMIENTOS DE HARDWARE 8
4.2 REQUERIMIENTOS DE SOFTWARE 9
4.3 ESTÁNDARES TÉCNICOS Y PROTOCOLOS. ..... **¡ERROR! MARCADOR NO DEFINIDO.**
4.4 REQUERIMIENTOS DE RED Y COMUNICACIONES 11

5 USUARIOS DEL SERVICIO 12

5.1 MATRIZ DE ROLES Y PERFILES 14
5.2 ROLES TÉCNICOS DE API MANAGEMENT APIM 15

6 PROCESO DE INSTALACIÓN Y/O DESPLIEGUE. 18

6.1 RECOMENDACIONES 20

7 CONTINGENCIAS Y SOPORTE TÉCNICO. 22

7.1 POLÍTICA DE BACKUP 22
7.2 ERRORES CONOCIDOS. 25

8 INSTALADORES 29

9 ACUERDOS DE NIVELES DE SERVICIO – SLA 33

9.1 DISPONIBILIDAD DEL SERVICIO 33
9.2 IMPACTO DEL SERVICIO 33
9.3 TIEMPOS DE ATENCIÓN Y SOLUCIÓN – SLA 34

10 USO Y APROPIACIÓN 34

11 ANEXOS 38

13CONTROL DE CAMBIOS DEL DOCUMENTO 41

1 INFORMACIÓN GENERAL

Desarrollo	*NA*
Proyecto o Requerimiento	*PLATAFORMA DE INTEROPERABILIDAD MICROSOFT*
Célula	*INFRAESTRUCTURA*
Servicio, Sistema y/o Aplicación Relacionada	Elija un elemento. *APIM (API Management Azure)* *AKS (Azure Kubernetes Service)* *Azure Monitor, el que incluye tambien la caracteristica Application Insights* *Pipelines de Azure DevOps*
Desarrollador(es)	*Unified - Microsoft*

2 INFORMACIÓN DEL SISTEMA O APLICACIÓN

2.1 Nombre del Sistema

PLATAFORMA DE INTEROPERABILIDAD MICROSOFT

2.2 Versión del Sistema

TABLA 1
Versión / SKU de Recursos Azure del Sistema.

Grupo de Recursos	Recurso	Nombre	Versión / SKU
RG-SOA-EU2-DEV	Container Registry	ACRAKSEU2DES	Standard
RG-SOA-EU2-DEV	Servicio de Kubernetes	AKS-SOA-EU2-DES	1.32.9
RG-SOA-EU2-DEV	Servicio de API Management	API-SOA-EU2-DES	Developer
RG-SOA-EU2-DEV	Azure Managed Grafana	GRAFANA-20251126104322	11.6.3

2.3 Imagen del sistema

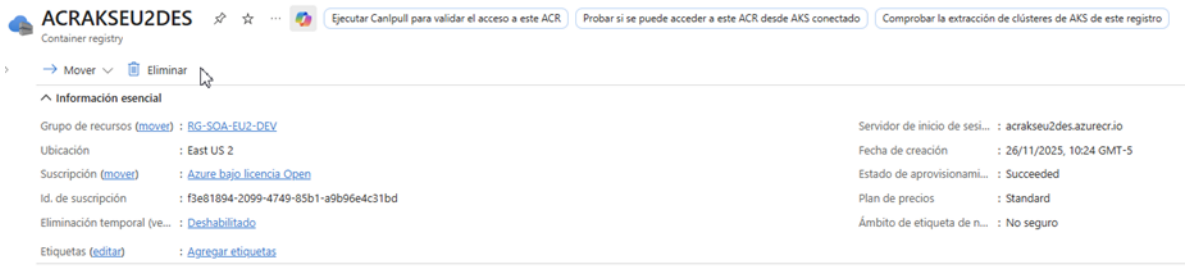


Figura 1
Versión del Recurso Container Registry en Azure

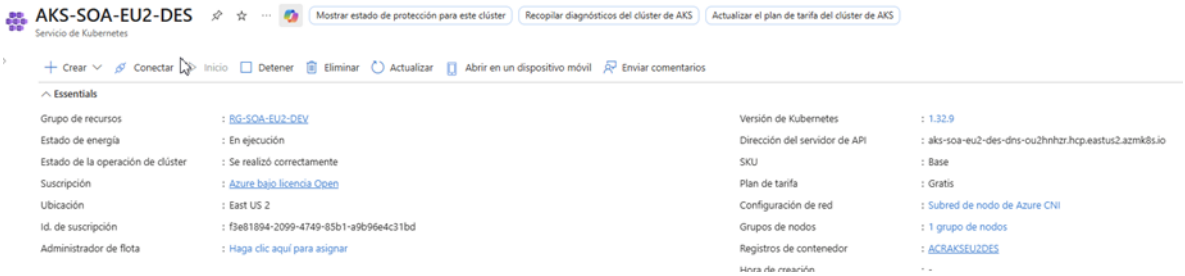


Figura 2
Versión del Servicio de Kubernetes (AKS) en Azure

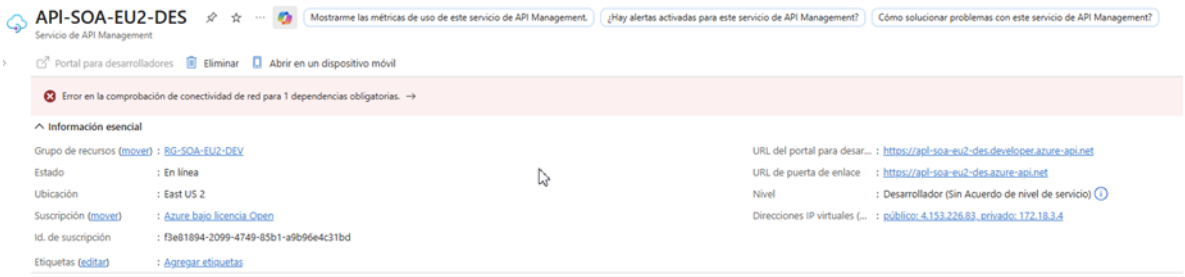


Figura 3
Nivel de Servicio (SKU) de API Management en Azure



Figura 4
Versión Azure Managed Grafana en Azure

2.4 Fecha de Elaboración

Diciembre 19, 2025

2.5 Alcance del desarrollo

Indique los nombres y descripciones de los componentes que se entregaran.

Componente	Descripción
APIM (API Management Azure)	Permite publicar, proteger, versionar, documentar y monitorear APIs. Actúa como un **gateway** entre los consumidores (apps, partners, terceros) y los servicios backend, aplicando políticas como autenticación, rate-limit, transformación de mensajes y caching.
AKS (Azure Kubernetes Service)	Facilita el despliegue, escalamiento y operación de aplicaciones contenarizadas (Docker), gestionando clústeres Kubernetes sin necesidad de administrar la infraestructura subyacente.

Azure Monitor	Plataforma unificada de observabilidad, permite detectar fallos, analizar desempeño y soportar operaciones y SRE.
Application Insights	monitoreo de aplicaciones (APM), trazas distribuidas, dependencias, errores y rendimiento.
Pipelines de Azure DevOps	Servicio de CI/CD (Integración y Despliegue Continuo). Automatiza build, pruebas y despliegues de aplicaciones e infraestructura (IaC), integrándose con repositorios Git, AKS, App Services, APIM, entre otros.

3 GLOSARIO DE TÉRMINOS

- **Diccionario de datos:** Listado organizado de todos los datos pertinentes al sistema con definiciones precisas y rigurosas para que tanto el usuario como el analista tengan un entendimiento en común de todas las entradas, salidas, componentes y cálculos.
- **API (Application Programming Interface):** Conjunto de definiciones y protocolos que permiten la comunicación entre sistemas de información, facilitando la interoperabilidad mediante servicios expuestos.
- **API Management (APIM):** Servicio administrado de Microsoft Azure que permite la publicación, gestión, seguridad, control y monitoreo de APIs.
- **AKS (Azure Kubernetes Service):** Servicio administrado de Kubernetes en Microsoft Azure que permite la orquestación y ejecución de aplicaciones basadas en contenedores.
- **ACR (Azure Container Registry**): Servicio administrado de Azure para el almacenamiento, versionamiento y distribución de imágenes de contenedores.
- **Application Insights:** Servicio de monitoreo de aplicaciones que permite la recolección de métricas, trazas y telemetría para el análisis del desempeño.
- **Azure Monitor**: Plataforma de monitoreo integral de Microsoft Azure para la supervisión de recursos, aplicaciones y servicios.

- **Azure Log Analytics:** Servicio que permite la recolección, almacenamiento y análisis de logs mediante consultas estructuradas.
- **Azure Event Grid:** Servicio de mensajería basada en eventos que facilita la integración asíncrona entre sistemas y componentes.
- **Azure Functions:** Servicio serverless de Microsoft Azure que permite ejecutar código sin administrar infraestructura.
- **Azure Key Vault:** Servicio administrado de seguridad para la gestión y protección de secretos, claves criptográficas y certificados.
- **Azure Policy:** Servicio para crear, asignar y administrar políticas que aplican reglas y efectos sobre recursos de Azure.
- **APIM Policies:** Conjunto de declaraciones XML que definen el comportamiento de una API en Azure API Management (ej: transformación, limitación, validación).
- **Blob Storage:** Servicio de almacenamiento de objetos de Azure utilizado para almacenar archivos y datos no estructurados.
- **CI/CD (Continuous Integration / Continuous Deployment):** Conjunto de prácticas que automatizan la integración, pruebas y despliegue de aplicaciones.
- **Developer Portal:** Portal autohospedado de Azure API Management que proporciona documentación interactiva de APIs para consumidores externos.
- **Grafana:** Herramienta de visualización que permite la creación de dashboards para el análisis de métricas y monitoreo.
- **GitHub:** Plataforma de control de versiones y gestión de código fuente utilizada para el desarrollo colaborativo.
- **Interoperabilidad:** Capacidad de los sistemas de información para intercambiar datos y utilizar la información intercambiada de manera efectiva.
- **JSON Schema:** Estándar para definir la estructura, tipos de datos y reglas de validación de documentos JSON, utilizado en políticas de validación de APIM.
- **JWT (JSON Web Token):** Token compacto y autocontenido utilizado para transmitir información de seguridad entre clientes y servidores de APIs.
- **Kubernetes:** Plataforma de código abierto para la automatización del despliegue, escalado y gestión de aplicaciones en contenedores.
- **Microsoft Entra ID:** Servicio de identidad y acceso de Microsoft que proporciona autenticación, autorización y control de acceso.
- **OAuth 2.0:** Protocolo estándar de autorización utilizado para asegurar el acceso a las APIs mediante Microsoft Entra ID.

- **OpenAPI:** Especificación estándar para documentar APIs RESTful, utilizado por Azure API Management para generar documentación automática en el portal de desarrolladores.
- **Prometheus:** Sistema de monitoreo y recolección de métricas orientado a entornos de contenedores y microservicios.
- **REST (Representational State Transfer):** Estilo arquitectónico para el diseño de servicios web basado en protocolos HTTP.
- **VNet (Virtual Network):** Red virtual de Microsoft Azure que permite la comunicación segura entre recursos desplegados en la nube.
- **Observabilidad:** Capacidad de supervisar, analizar y comprender el comportamiento interno de un sistema a partir de métricas, logs y trazas.

4 REQUERIMIENTOS

4.1 Requerimientos de Hardware.

La solución de Interoperabilidad se encuentra implementada sobre una Infraestructura en la Nube Microsoft Azure, haciendo uso de servicios administrados (PaaS y CaaS), por lo cual no se requiere la provisión ni instalación de hardware físico dedicado por parte de la entidad.

Los componentes de la plataforma, incluyendo Azure API Management, Azure Kubernetes Service (AKS), Azure Container Registry (ACR), Azure Functions, Event Grid, Azure Monitor, Azure Log Analytics, Application Insights, Microsoft Entra ID y Azure Key Vault, se ejecutan sobre Infraestructura gestionada por el proveedor de Nube, quien es responsable del suministro, mantenimiento y disponibilidad del hardware subyacente.

No obstante, para efectos de operación y dimensionamiento, se establecen los requerimientos mínimos referenciales de infraestructura lógica, necesarios para garantizar el correcto funcionamiento de los servicios desplegados.

Requerimientos mínimos de infraestructura (referenciales):

Componente	Requerimiento mínimo
Plataforma de ejecución	Infraestructura en la nube Microsoft Azure
Servicio de exposición de APIs	Azure API Management (servicio administrado)

Plataforma de contenedores	Azure Kubernetes Service (AKS)
CPU	Mínimo 2 vCPU por nodo de trabajo del clúster AKS
Memoria RAM	Mínimo 8 GB RAM por nodo del clúster AKS
Almacenamiento	Almacenamiento administrado en Azure (Blob Storage y discos administrados)
Registro de contenedores	Azure Container Registry (ACR)
Red	Red virtual Azure (VNet) con subred dedicada para AKS
Alta disponibilidad	Configuración de múltiples nodos y servicios administrados
Escalabilidad	Autoescalamiento horizontal habilitado

Observaciones relevantes:

- El hardware físico (servidores, almacenamiento y red) es totalmente administrado por Microsoft Azure, garantizando niveles adecuados de disponibilidad, desempeño y resiliencia.
- La plataforma permite escalamiento dinámico de recursos de procesamiento, memoria y almacenamiento, de acuerdo con la demanda de consumo de los servicios de interoperabilidad.
- No se requiere adquisición, instalación ni mantenimiento de servidores físicos locales.
- Los componentes de seguridad, identidad y gestión de secretos (Microsoft Entra ID y Azure Key Vault) operan como servicios administrados y no demandan recursos de hardware dedicados.
- En caso de integración con sistemas externos u on-premise, dichos sistemas deberán contar con recursos de hardware suficientes para soportar la carga de interoperabilidad, responsabilidad que recae en la entidad propietaria de dichos sistemas.

4.2 Requerimientos de Software.

La solución de interoperabilidad se apoya en una plataforma tecnológica basada en servicios administrados de Microsoft Azure, por lo cual no se requiere la instalación de software base (sistemas operativos, middleware o plataformas de ejecución) por parte de la entidad, ya que estos son provistos y gestionados directamente por el proveedor de nube.

Los componentes de software que conforman la plataforma garantizan la correcta exposición, seguridad, orquestación, monitoreo e integración de los servicios de interoperabilidad.

Requerimientos de software de la plataforma:

Componente	Tipo	Descripción
Azure API Management	PaaS	Plataforma de exposición, gestión y seguridad de APIs
Azure Kubernetes Service (AKS)	CaaS	Orquestación y ejecución de contenedores
Kubernetes	Plataforma	Orquestador de contenedores gestionado por AKS
Azure Container Registry (ACR)	PaaS	Registro y almacenamiento de imágenes de contenedor
Azure Functions	PaaS	Ejecución de funciones serverless para lógica de integración
Azure Event Grid	PaaS	Enrutamiento y gestión de eventos
Microsoft Entra ID	SaaS	Gestión de identidad, autenticación y autorización
Azure Key Vault	PaaS	Gestión segura de secretos, claves y certificados
Azure Monitor	PaaS	Monitoreo integral de la plataforma
Azure Log Analytics	PaaS	Recolección y análisis de logs
Azure Application Insights	PaaS	Telemetría y monitoreo de aplicaciones
Prometheus	Plataforma	Recolección de métricas del clúster Kubernetes
Grafana Dashboard	Aplicación	Visualización de métricas y dashboards
GitHub	SaaS	Gestión de código fuente
Azure Pipelines	SaaS	Automatización de procesos CI/CD
Microsoft Defender for Cloud	PaaS	Seguridad y protección de la plataforma

Observaciones relevantes:

- No se requiere instalación de sistemas operativos, bases de datos ni middleware por parte de la entidad.
- La plataforma permite la integración con sistemas externos mediante APIs REST, eventos y servicios de mensajería.
- El uso de pipelines CI/CD garantiza la correcta gestión del ciclo de vida del software, desde la construcción hasta el despliegue en ambientes controlados.

- Todos los componentes software cumplen con un modelo de interoperabilidad basado en estándares abiertos.

4.3 Requerimientos de Red y Comunicaciones.

La plataforma de interoperabilidad se encuentra desplegada sobre una Infraestructura de Red en la Nube Microsoft Azure, diseñada para garantizar conectividad segura, segmentación de red, alta disponibilidad y control de acceso entre los distintos componentes de la solución.

La comunicación entre los servicios se realiza mediante protocolos estándar, utilizando redes virtuales y mecanismos de seguridad gestionados por el proveedor de nube.

Requerimientos de Red:

Elemento	Descripción
Red virtual (VNet)	Red virtual dedicada para la plataforma de interoperabilidad
Espacio de direccionamiento	Rango IP privado definido para la VNet
Subredes	Subred dedicada para AKS y servicios asociados
Conectividad interna	Comunicación privada entre servicios dentro de la VNet
Conectividad externa	Acceso controlado desde clientes externos hacia Azure API Management
Resolución de nombres	DNS administrado por Azure
Seguridad perimetral	Exposición de servicios únicamente a través de Azure API Management

Modelo de comunicaciones:

- Azure API Management actúa como punto único de entrada para los consumidores de servicios (Client Apps).
- La comunicación entre API Management y los servicios backend (AKS, Functions, Event Grid) se realiza mediante canales seguros dentro de la red virtual.

- Azure Kubernetes Service (AKS) opera dentro de una subred dedicada, garantizando aislamiento y control del tráfico.
- Azure Container Registry (ACR) es accedido de forma segura desde AKS para la descarga de imágenes de contenedores.
- Los servicios de monitoreo y observabilidad (Azure Monitor, Log Analytics, Application Insights, Prometheus y Grafana) se comunican de manera interna y segura con la plataforma.

Protocolos y estándares de comunicación:

Protocolo / Estándar	Uso
HTTPS (TLS 1.2 o superior)	Exposición y consumo de APIs
REST	Intercambio de información entre sistemas
JSON	Formato de intercambio de datos
OAuth 2.0 / OpenID Connect	Autenticación y autorización
Webhooks / Eventos	Integración basada en eventos (Event Grid)
Tokens (JWT – Token Web Jason)	Acceso por token

Observaciones relevantes:

- Todo el tráfico expuesto hacia internet se realiza de forma segura a través de Azure API Management, evitando accesos directos a los servicios backend.
- La plataforma soporta escalabilidad y alta disponibilidad, gracias a la Infraestructura de Red administrada por Azure.
- Se garantiza la segregación de ambientes (Desarrollo, Pruebas, Producción) mediante redes virtuales y grupos de recursos independientes.
- En caso de integración con Sistemas On-premise, la conectividad podrá realizarse mediante VPN Site-to-Site o ExpressRoute, según las necesidades de la entidad.

5 USUARIOS DEL SERVICIO

Definir las áreas organizacionales, usuarios funcionales y clientes que harán uso de la

plataforma de interoperabilidad basada en tecnologías Microsoft, con el fin de garantizar un uso controlado, seguro y alineado con los objetivos del negocio y los lineamientos de seguridad de la información.

Áreas Internas Usuarias del Servicio

Las siguientes áreas de la organización podrán hacer uso del servicio de interoperabilidad, de acuerdo con sus funciones y necesidades operativas:

- **Grupo de infraestructura**
  Responsable de la administración, soporte y operación técnica de la plataforma de interoperabilidad.
- **Grupo de Desarrollo de Software / Sistemas**
  Encargada del desarrollo, mantenimiento y consumo de servicios web para la integración entre sistemas internos y externos.
- **Grupo de Seguridad de la Información / Riesgos**
  Supervisión del cumplimiento de los controles de seguridad, monitoreo y gestión de riesgos asociados a la interoperabilidad.
- **Áreas misionales**
  Áreas usuarias de la interoperabilidad para la ejecución de procesos misionales que dependen del intercambio de información entre sistemas.

Usuarios Funcionales

Los usuarios funcionales que interactúan con la plataforma de interoperabilidad se clasifican de la siguiente manera:

- **Usuarios Técnicos**
  - Administradores de la plataforma
  - Arquitectos de integración
  - Desarrolladores autorizados
    Acceden para configuración, desarrollo, pruebas y monitoreo.

- **Usuarios Operativos**
  - Funcionarios que utilizan aplicaciones integradas
  - No acceden directamente a los servicios web, sino a través de sistemas consumidores.
- **Usuarios de Soporte**
  - Personal encargado de atender incidentes y requerimientos relacionados con la interoperabilidad.

NOTA: *El acceso de los usuarios estará limitado de acuerdo con el* ***principio de mínimo privilegio****.*

5.1 Matriz de Roles y Perfiles

La matriz de Roles y perfiles definida para la Plataforma de Interoperabilidad se encuentra en la siguiente ruta:

(clic aquí para ver el archivo)

GRUPO	PERFIL	Descripcion de Perfil
Roles de Seguridad	Administrador Global/Personalizado	Gestionan la configuración y acceso en 365/Power Platform.
	Usuarios sin acceso de administrador	Roles operativos estánda
Sistema y Aplicaciones	Cuenta de Servicio de Plataforma	Utilizada para administración de alto nivel en entornos empresariales.

GRUPO	PERFIL	Descripcion de Perfil
	Administradores de Aplicaciones	Cuentas específicas para gestionar implementaciones, con roles de seguridad asignados, como el usuario de administración de aplicaciones.
	Servicios de Aplicación	Cuentas automatizadas, por ejemplo, para el despliegue de paquetes (CAPPackageDeployerServiceDVClient) o motores de búsqueda (RelevanceSearch).
Usuarios Finales	Usuarios Activos	Miembros de la organización con licencias activas que acceden a aplicaciones y datos
	Usuarios Invitados/Externos	Usuarios fuera de la organización que interactúan mediante interoperabilidad, comunes en Teams, con autenticación personalizada.

5.2 Roles técnicos de API management APIM

La siguiente tabla define los roles técnicos específicos para la operación y administración de Azure API Management (APIM), componente central de la plataforma de interoperabilidad. Cada rol se homologa con los perfiles establecidos en la matriz general (sección 5.1), detallando sus responsabilidades técnicas clave y los permisos de Azure RBAC (Role-Based Access Control) recomendados para garantizar una gestión segura y alineada con el principio de mínimo privilegio. Esta especificación permite una asignación clara de responsabilidades dentro de la plataforma Microsoft Azure.

Rol Técnico APIM	Homólogo en Matriz 5.1	Responsabilidades Clave en APIM	Permisos Azure RBAC Recomendados
Administrador APIM	Administrador Plataforma	- Gestionar instancia APIM	API Management Service Contributor
		- Configurar productos y APIs	Contributor (Resource Group)
		- Gestionar suscripciones	
		- Monitorear métricas y logs	
Desarrollador de APIs	Desarrollador	- Diseñar y documentar APIs (OpenAPI)	API Management Service Developer
		- Configurar operaciones y políticas	API Management Service Operator
		- Probar APIs en Developer Portal	
		- Gestionar versiones	
Arquitecto de Integración	Arquitecto de Integración	- Diseñar esquemas de contratos API	API Management Service Reader
		- Definir estándares y patrones	Reader (Resource Group)
		- Revisar políticas de seguridad	
		- Optimizar performance APIs	
Ingeniero DevOps CI/CD	Administrador Plataforma (parcial)	- Configurar pipelines de despliegue	Contributor (APIM + ACR + AKS)
		- Automatizar publicación APIs	Azure DevOps Project Admin
		- Gestionar entornos (dev/test/prod)	
		- Implementar GitOps para APIM	
Consumidor Externo (Técnico)	Cliente Externo	- Obtener claves de suscripción	API Management Service Reader (limitado)
		- Usar Developer Portal	Acceso solo a Developer Portal

Rol Técnico APIM	Homólogo en Matriz 5.1	Responsabilidades Clave en APIM	Permisos Azure RBAC Recomendados
		- Integrar APIs en sistemas externos	
		- Reportar incidencias técnicas	
Analista de Seguridad APIs	Seguridad Información	- Revisar políticas JWT/OAuth	Security Reader
		- Auditar logs de acceso	Log Analytics Reader
		- Validar cumplimiento de estándares	
		- Gestionar certificados y secrets	
Operador de Monitoreo	Soporte Técnico	- Monitorear dashboards APIM	Monitoring Reader
		- Responder alertas de disponibilidad	Application Insights Component Contributor
		- Reportar métricas SLA	
		- Escalar incidencias	
Gestor de Productos API	Responsable OTIC	- Definir productos API (bundles)	API Management Service Contributor
		- Establecer cuotas y límites	Cost Management Reader
		- Gestionar ciclos de vida	
		- Reportar uso y adopción	

6 PROCESO DE INSTALACIÓN Y/O DESPLIEGUE.

El proceso de instalación y despliegue de la solución de interoperabilidad se realiza sobre la plataforma Microsoft Azure, mediante un modelo automatizado de despliegue continuo (CI/CD), garantizando consistencia, trazabilidad y reducción de errores manuales.

Dado que la solución se apoya en servicios administrados, no se realiza una instalación tradicional de software en servidores físicos, sino un proceso de aprovisionamiento y despliegue de componentes en la nube.

6.1. Prerrequisitos

Antes de iniciar el proceso de despliegue, se deben cumplir los siguientes prerrequisitos:

- Suscripción activa de Microsoft Azure.
- Creación del Resource Group destinado a la plataforma de interoperabilidad.
- Accesos y permisos configurados en Microsoft Entra ID para los roles de administración y despliegue.
- Repositorios de código fuente disponibles en GitHub.
- Configuración inicial de Azure DevOps / Azure Pipelines.
- Imágenes de contenedores disponibles o listas para ser construidas.

6.2. Creación y Configuración de la Infraestructura base

Paso 1: Creación del Resource Group
Se crea el grupo de recursos que contendrá los componentes de la plataforma.

Paso 2: Aprovisionamiento de Azure Container Registry (ACR)
Se crea el servicio Azure Container Registry, el cual almacenará las imágenes de los microservicios.

Paso 3: Aprovisionamiento de Azure Kubernetes Service (AKS)
Se crea el clúster AKS, configurando:

- Número inicial de nodos
- Red virtual y subred
- Integración con ACR

6.3 Configuración de seguridad e identidad

Paso 4: Configuración de Microsoft Entra ID
Se configura una aplicación en Microsoft Entra ID para habilitar los mecanismos de autenticación y autorización de los consumidores de servicios de interoperabilidad.

- Aplicaciones registradas
- Permisos OAuth 2.0
- Roles y accesos para consumidores de APIs

Paso 5: Configuración de Azure Key Vault
Se configura Azure Key Vault como repositorio central de secretos, claves y certificados.

- Secretos
- Claves
- Certificados

6.4 Despliegue de la plataforma de integración

Paso 6: Configuración de Azure API Management

Se aprovisiona Azure API Management y se configura como punto único de entrada, definiendo:

- APIs publicadas
- Políticas de seguridad
- Integración con Entra ID

Paso 7: Despliegue de servicios backend

- Los microservicios son desplegados en AKS mediante contenedores obtenidos desde ACR.

Paso 8: Configuración de integración basada en eventos

- Se configura Azure Event Grid para la comunicación asíncrona entre componentes.

6.5 Automatización del despliegue (CI/CD)

Paso 9: Configuración de Azure Pipelines
Se configuran los pipelines para:

- Construcción de imágenes
- Publicación en ACR
- Despliegue automático en AKS

6.6 Verificación y validación

Paso 10: Validación de servicios
Se verifica:

- Disponibilidad de las APIs
- Autenticación y autorización
- Correcto enrutamiento de solicitudes
- Registro de logs y métricas

6.7 Consideraciones finales del despliegue

- El proceso de despliegue es repetible, automatizado y auditable.
- No se requiere instalación manual de software.
- Los cambios y actualizaciones se realizan mediante pipelines CI/CD.
- El uso de servicios administrados reduce riesgos operativos.
- La solución cumple con los lineamientos de interoperabilidad y seguridad.

6.1 RECOMENDACIONES

Con el fin de garantizar una correcta instalación, configuración y operación de los componentes del sistema de interoperabilidad, se presentan las siguientes recomendaciones técnicas que deben ser tenidas en cuenta por los usuarios y administradores de la plataforma.

El cumplimiento de estas recomendaciones permitirá asegurar una instalación adecuada, una operación estable y una evolución controlada de la plataforma de interoperabilidad, alineada con buenas prácticas de arquitectura, seguridad y gobierno de servicios.

R-1. Planeación y preparación del entorno

- Definir previamente los ambientes (desarrollo, pruebas, producción) y mantenerlos separados mediante Resource Groups y VNets independientes.
- Validar los permisos y roles necesarios en Microsoft Entra ID antes de iniciar el despliegue.
- Establecer una nomenclatura estándar para recursos, APIs, repositorios y pipelines.

R-2. Seguridad e identidad

- Utilizar Microsoft Entra ID como mecanismo centralizado de autenticación y autorización.
- Evitar el uso de credenciales embebidas en código; todos los secretos deben almacenarse en Azure Key Vault.
- Implementar políticas de validación JWT y control de acceso en Azure API Management.
- Revisar periódicamente las recomendaciones de Microsoft Defender for Cloud.

R-3. Despliegue y automatización

- Realizar los despliegues exclusivamente mediante pipelines CI/CD, evitando despliegues manuales en ambientes controlados.
- Versionar todas las APIs y microservicios para facilitar la gestión de cambios.
- Validar los despliegues en ambientes de prueba antes de promoverlos a producción.

R-4. Operación y monitoreo

- Habilitar y revisar de forma permanente los servicios de Azure Monitor, Log Analytics y Application Insights.
- Configurar dashboards en Grafana para monitorear métricas críticas del clúster AKS.
- Definir alertas proactivas para identificar incidentes o degradaciones del servicio.

R-5. Escalabilidad y disponibilidad

- Configurar el autoescalamiento en Azure Kubernetes Service (AKS) para atender variaciones de carga.
- Evaluar periódicamente el consumo de recursos y ajustar los límites según la demanda.
- Utilizar servicios administrados para reducir riesgos operativos y puntos únicos de falla.

R-6. Integración e interoperabilidad

- Utilizar formatos estándar (JSON) y protocolos abiertos (REST, HTTPS).
- Implementar integración basada en eventos mediante Azure Event Grid cuando se requiera desacoplamiento.
- Documentar claramente los contratos de las APIs y mantenerlos actualizados.

R-7. Mantenimiento y mejora continua

- Mantener actualizadas las versiones de los componentes gestionados.
- Revisar periódicamente los pipelines, políticas de seguridad y configuraciones.
- Documentar cualquier cambio relevante en la arquitectura o configuración de la plataforma.

7 CONTINGENCIAS Y SOPORTE TÉCNICO.

La siguiente matriz indica los contactos asociados al soporte técnico de la aplicación, señalándo nombre, cargo, e-mail y teléfonos de contacto (Matriz RACI)

MATRIZ RACI

ACTIVIDAD / RECURSO	Dueño de la Solución	Líder TI	Líder Area	Líder de célula	Consultor Mesa especializada	Usuario final
Diagnóstico del incidente	C / I	I	C / I / A	C / I	R	I
Diseño de la solución	C / I	C / I	C / I / A	C / I	R	I
Solucionar Incidentes del Servicio	C / I / A	I	C / I	C/I	R	I

R= Responsable, A= Aprobador, C=Consultado, I=Informado

7.1 Política de Backup

Las copias de seguridad de los sistemas de computación deben estar almacenadas en una zona diferente de donde reside la información original. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente con el fin de asegurar la integridad y disponibilidad de la información.

7.2 Lineamiento para la recuperación del servicio

7.2.1 Detección y Registro del Incidente

- Monitorear la plataforma mediante **Azure Monitor**, **Log Analytics** y alertas configuradas.

- Detectar indisponibilidad de servicios como **API Management, Logic Apps, Service Bus o Azure Fabric**.
- Registrar el incidente en la mesa de servicios.
- Escalar al Líder DRP.

7.2.2 Evaluación y Declaración

- Evaluar impacto en servicios críticos de interoperabilidad.
- Verificar afectación por región de Azure, red o seguridad.
- Determinar activación del DRP según RTO/RPO definidos.
- Autorizar formalmente la activación del DRP.

7.2.3 Comunicación del Incidente

- Notificar a la alta dirección, TI y seguridad de la información.
- Comunicar a usuarios y sistemas integrados el estado del servicio.
- Publicar avisos internos si aplica.

7.2.4 Activación del Entorno Alterno en Azure

- Activar la **región secundaria de Azure** previamente definida.
- Validar disponibilidad de:
  - Suscripciones
  - Resource Groups
  - Redes virtuales (VNet)
- Verificar reglas de Network Security group - **NSG**, firewalls y conectividad VPN/ExpressRoute.

7.2.5 Recuperación de Servicios de Interoperabilidad Azure

- Restaurar y validar:
  - **Azure API Management** (configuración, APIs, policies)
  - **Azure Logic Apps** (workflows y conectores)
  - **Azure Service Bus** (colas, topics, subscriptions)
  - **Azure Fabric / Data Services** si aplica
- Reconfigurar endpoints y dependencias entre servicios.

7.2.6 Gestión de Identidades y Seguridad

- Validar autenticación mediante **Azure Entra ID**.

- Verificar certificados, secretos y claves desde **Azure Key Vault**.
- Confirmar funcionamiento de tokens (JWT / OAuth 2.0).

7.2.7 Recuperación de Información

- Restaurar respaldos de configuraciones y datos críticos.
- Validar integridad y consistencia de la información.
- Confirmar cumplimiento del RPO definido.

7.2.8 Validación Técnica y Funcional

- Ejecutar pruebas de conectividad entre servicios Azure.
- Validar consumo de APIs desde sistemas internos y externos.
- Confirmar operación de mensajería y flujos de integración.

7.2.9 Retorno a la Operación Normal

- Confirmar estabilidad de la plataforma en la región activa.
- Habilitar accesos completos a usuarios y sistemas.
- Monitorear la operación post-recuperación.

7.2.10 Actividades Posteriores al Incidente

- Documentar el incidente y tiempos de recuperación.
- Realizar análisis de causa raíz.
- Definir e implementar acciones correctivas.
- Actualizar el DRP si es necesario.

7.2.11 Evidencias del Procedimiento

- Registro del incidente.
- Autorización de activación del DRP.
- Logs de recuperación.
- Resultados de pruebas post-recuperación.

7.2.12 Pruebas del DRP

- Realizar pruebas del DRP al menos una vez al año.
- Documentar resultados y oportunidades de mejora.

7.2.13 Control de Cambios

Todo cambio en la plataforma que impacte la continuidad debe evaluarse y reflejarse en este procedimiento.

7.2.14 Revisión y Actualización

Este procedimiento debe revisarse periódicamente o ante cambios significativos en la plataforma, infraestructura o normativa aplicable

7.3 Errores conocidos.

Componente	Error / Síntoma	Causa Probable	Detección (Azure Monitor)	Acción / Mitigación
API Management	HTTP 401 / 403 al consumir API	Token inválido o expirado, suscripción inexistente, política validate-jwt mal configurada	Métricas APIM por código HTTP, logs del gateway	Validar configuración de identidad, issuer/audience, expiración del token y suscripción
API Management	HTTP 429 Too Many Requests	Políticas de rate-limit o quota restrictivas, picos de tráfico	Métricas de throttling y conteo de 429	Ajustar límites, aplicar control por consumidor y backoff
API Management	HTTP 502 Bad Gateway	Backend AKS no disponible, error de red, Ingress o DNS	Logs APIM + errores de conexión backend	Verificar estado del backend, conectividad y configuración de Ingress
API Management	HTTP 504 Gateway Timeout	Backend lento, timeouts no alineados, saturación de pods	Métricas de latencia p95/p99, timeouts	Optimizar backend, escalar pods y alinear timeouts

Componente	Error / Síntoma	Causa Probable	Detección (Azure Monitor)	Acción / Mitigación
API Management	Error de certificado TLS / mTLS	Certificado expirado, CA no confiable, CN/SAN incorrecto	Logs de errores TLS	Renovar certificados y validar cadena completa
API Management	Error CORS en consumo web	Política CORS inexistente o restrictiva	Errores en navegador y ausencia de headers	Configurar política CORS adecuada
API Management	404 / 400 por versión o ruta incorrecta	Versionamiento inconsistente o API no publicada	Métricas de 404/400	Aplicar estrategia de versionado y deprecación
AKS	Pods en CrashLoopBackOff	Error de configuración, fallo de inicio, excepción	Eventos del pod, logs del contenedor	Revisar logs, variables de entorno y healthchecks
AKS	ImagePullBackOff / ErrImagePull	Permisos ACR, imagen inexistente, error de red	Eventos del pod	Validar ACR, identidad administrada y tags
AKS	Pods en Pending	Falta de CPU o memoria	Métricas de nodos y eventos de scheduling	Ajustar requests/limits y escalar clúster
AKS	Fallas en readiness / liveness	Probes mal configuradas	Eventos de probes	Ajustar endpoints, tiempos y umbrales
AKS	Errores Ingress (404 / 502)	Reglas incorrectas, service o puerto errado	Logs del Ingress Controller	Corregir reglas, servicios y annotations

Componente	Error / Síntoma	Causa Probable	Detección (Azure Monitor)	Acción / Mitigación
AKS	Fallas de DNS interno	CoreDNS degradado, políticas de red	Logs CoreDNS, pruebas DNS	Revisar CoreDNS y políticas de red
AKS	Bloqueo por NetworkPolicy	Políticas demasiado restrictivas	Timeouts entre servicios	Ajustar reglas de ingress/egress
AKS	Alta latencia del servicio	Saturación de nodos o throttling	Métricas CPU/memoria, latencia	Escalar nodos/pods y optimizar workloads
AKS	Falla por secretos expirados	Certificados o claves vencidas	Errores recurrentes de conexión	Implementar rotación y monitoreo de secretos
Azure Monitor	Dashboards sin datos	Diagnóstico no habilitado, workspace incorrecto	Ausencia de métricas/logs	Validar diagnostic settings y conexión
Azure Monitor	Falta de trazabilidad end-to-end	No propagación de correlation-id	Logs inconexos	Estandarizar correlación y logging
Azure Monitor	Alertas no disparan	Umbrales mal definidos, acción inválida	Revisión post-incidente	Ajustar métricas, umbrales y Action Groups
Azure Monitor	Exceso de alertas	Umbrales agresivos, métricas ruidosas	Volumen elevado de alertas	Ajustar severidades y ventanas

Componente	Error / Síntoma	Causa Probable	Detección (Azure Monitor)	Acción / Mitigación
Azure Monitor	Costos altos de logs	Logging excesivo, retención alta	Métricas de ingesta	Optimizar niveles y políticas de retención
Integración	Timeouts desalineados entre capas	Configuración distinta APIM–Ingress–App	Análisis de latencias	Definir estándar de timeouts
Integración	Errores durante despliegue	Rolling update mal configurado	Picos de 5xx en despliegue	Ajustar estrategia de despliegue
Integración	APIM no actualizado tras cambios AKS	Backend/rutas modificadas	Errores posteriores a release	Gobernar cambios vía CI/CD

A continuación se incluye documentación de apoyo del fabricante:

- Diagnósticos de Azure API Management
- Solucion de problemas al actualizar nombres del host
- Solución de problemas de tiempo de espera y errores de respuesta del cliente con API Management
- Diagnósticos en Azure App Service
- Diagnosticar y solucionar problemas de Azure Kubernetes Service

8 INSTALADORES

Este capítulo describe los **componentes tecnológicos base, prerrequisitos y consideraciones de instalación** que soportan la Plataforma de Interoperabilidad de la Superintendencia del Subsidio Familiar (SSF), implementada sobre servicios de Microsoft Azure.

El objetivo es proporcionar a los equipos técnicos una **visión clara y homogénea de los elementos que deben estar disponibles y correctamente configurados** para habilitar la plataforma, sin entrar en procedimientos operativos detallados, los cuales se documentan en guías y runbooks complementarios.

8.1 Enfoque de instalación adoptado

La Plataforma de Interoperabilidad de la SSF **no utiliza instaladores tradicionales ejecutables**, sino que se basa en un **modelo de provisión de servicios cloud administrados**, bajo los principios de:

- Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS).
- Automatización mediante plantillas y pipelines.
- Separación por ambientes (desarrollo, pruebas, producción).
- Gobierno y control centralizado de los servicios expuestos.

Por tanto, el término *instaladores* se entiende como:

El conjunto de servicios, configuraciones base y dependencias técnicas que deben ser aprovisionadas y habilitadas en Azure para la correcta operación de la plataforma.

8.2 Componentes de la plataforma y prerrequisitos

8.2.1 Azure API Management (APIM)

Rol en la plataforma Azure API Management actúa como el **punto central de exposición, gobierno y seguridad de los servicios de interoperabilidad**, permitiendo el control del acceso a APIs internas y externas.

Prerrequisitos de instalación

- Suscripción activa de Azure.
- Grupo de recursos definido para interoperabilidad.
- Red virtual (VNET) definida según el modelo de conectividad de la SSF.
- Definición previa de ambientes (Dev / Test / Prod).

- Identidades y permisos adecuados para administración (RBAC).

Componentes habilitados

- Instancia de API Management (SKU acorde a la criticidad del servicio).
- Productos y suscripciones.
- Políticas base (seguridad, control de tráfico, transformación).
- Conectividad con backends desplegados en AKS.

Consideraciones técnicas

- Versionamiento de APIs.
- Separación de APIs internas y externas.
- Gestión de certificados y autenticación de servicios.
- Integración con Azure Monitor para métricas y logs.

8.2.2 Azure Kubernetes Service (AKS)

Rol en la plataforma AKS es la **plataforma de ejecución de los servicios backend** que implementan la lógica de negocio de interoperabilidad, bajo un enfoque de microservicios.

Prerrequisitos de instalación

- Suscripción Azure con permisos para crear clústeres administrados.
- Red virtual y subredes asignadas.
- Registro de contenedores (ACR) accesible.
- Definición de namespaces por dominio o servicio.
- Políticas de seguridad y acceso definidas.

Componentes habilitados

- Clúster AKS administrado.
- Node pools según necesidades de carga.
- Ingress Controller para exposición controlada.
- ConfigMaps y Secrets.
- Integración con Azure Monitor para contenedores.

Consideraciones técnicas

- Dimensionamiento inicial y escalabilidad.
- Estrategias de despliegue (rolling update).
- Configuración de health checks.
- Gestión de secretos y certificados.

8.2.3 Azure Monitor

Rol en la plataforma Azure Monitor provee las **capacidades de observabilidad, monitoreo, alertamiento y trazabilidad** de la Plataforma de Interoperabilidad.

Prerrequisitos de instalación

- Log Analytics Workspace habilitado.
- Permisos para configurar Diagnostic Settings.
- Definición de métricas críticas y umbrales.

Componentes habilitados

- Recolección de métricas de APIM.
- Monitoreo de clúster AKS y contenedores.
- Logs centralizados.
- Alertas y Action Groups.
- Dashboards operativos.

Consideraciones técnicas

- Retención de logs acorde a lineamientos institucionales.
- Control de costos por ingesta.
- Correlación de eventos entre APIM y AKS.
- Uso de identificadores de trazabilidad.

8.3 Relación entre componentes

La instalación de los componentes debe entenderse como un **ecosistema integrado**, donde:

- **APIM** actúa como capa de exposición y gobierno.
- **AKS** ejecuta la lógica de integración y servicios.
- **Azure Monitor** garantiza la observabilidad transversal.

Ningún componente opera de manera aislada; su instalación y habilitación deben realizarse considerando las dependencias técnicas y de seguridad entre ellos.

8.4 Gestión de ambientes

La Plataforma de Interoperabilidad debe contar, como mínimo, con los siguientes ambientes:

- **Desarrollo:** validación técnica inicial.
- **Pruebas:** validación funcional e integración.
- **Producción:** operación institucional.

Cada ambiente debe:

- Contar con instancias independientes de APIM, AKS y Azure Monitor.
- Mantener configuraciones coherentes, ajustadas a su criticidad.
- Respetar los lineamientos de seguridad y control definidos por la SSF.

A continuación se relacionan las grabaciones del ejercicio inicial de instalación de los componentes, este material se relaciona específicamente con propósito referencial de orientación para la instalación, ante la necesidad de realizar una nueva instalación de los componentes de la plataforma de interoperabilidad, es requerido tener presente que los parámetros de configuración deben corresponder a los establecidos y documentados, los cuales pueden diferir de los parámetros originales presentados en los videos de instalación:

- Sesión 11 de Diciembre
- Sesión 09 de Diciembre
- Sesión 05 de Diciembre
- Sesión 27 de Noviembre
- Sesión 26 de Noviembre
- Sesión 24 de Noviembre
- Sesión 14 de Noviembre

9 ACUERDOS DE NIVELES DE SERVICIO – SLA

9.1 Disponibilidad del servicio

Considerando que la plataforma de interoperabilidad se soporta sobre infraestructura Azure Microsoft, los acuerdos de niveles de servicio establecidos en la entidad, se enriquecen con los niveles de servicio definidos por el proveedor, para lo cual se remite en este apartado la información comercial del fabricante Niveles v2 de Azure API Management

9.2 Impacto del Servicio

<< Indicar el Impacto con el que se clasifica el Servicio o Aplicación entregado. Recuerde que los servicios en la actualidad ya tienen una prioridad asociada en el documento de Catálogo de Servicios de TI. Si se requiere cambiar deberá quedar definido a través del proceso de Gestión de Cambios.

Si el servicio es completamente nuevo, y no está referenciado en el catálogo de servicios de TI, deberá indicar el impacto que tiene ese servicio en el negocio teniendo en cuenta la siguiente tabla >>.

Impacto	Descripción
Crítico	Servicio cuya Indisponibilidad afectara significativamente a uno o más departamentos, gerencias o unidades del negocio.
Alto	Servicio cuya indisponibilidad alterara a determinadas funciones o a un grupo de usuarios.
Medio	Servicio cuya intermitencia no controlada afectara la disponibilidad de otros servicios no críticos, o a un grupo reducido de usuarios (máximo 10)
Bajo	Servicio cuya afectación está planificada a través de alguna Actividad o Requerimiento de servicios negociados con de usuario. Ejemplo: preguntas del tipo “Cómo hacer…”.

9.3 Tiempos de Atención y Solución – SLA

<<Teniendo en cuenta que, en la definición de un ANS, se debe acordar con el usuario, cliente, unidad de negocio y/o proveedores de servicio el tiempo de solución en horas para cada solicitud, es necesario indicar de acuerdo con la prioridad listada a continuación el tiempo de respuesta acordado: >>

IMPACTO	TIEMPO MAXIMO ATENCION	TIEMPO MAXIMO SOLUCION
Crítico		
Alto		
Medio		
Bajo		

10 USO Y APROPIACIÓN

El propósito de del uso y apropiación es establecer los lineamientos de la Plataforma de Interoperabilidad Microsoft, con el fin de asegurar que los componentes técnicos implementados sean utilizados de manera correcta, consistente y segura por los diferentes roles definidos en el servicio.

El uso adecuado de la plataforma permitirá garantizar la continuidad operativa, la confiabilidad del intercambio de información entre sistemas y el cumplimiento de los objetivos funcionales asociados a los procesos misionales y de soporte que dependen de la interoperabilidad.

Usuarios y roles involucrados en el uso

El uso y apropiación de la plataforma se soporta en los roles definidos en el capítulo Usuarios del Servicio y su respectiva Matriz de Roles y Perfiles, los cuales interactúan con la solución en distintos niveles de responsabilidad y acceso.

Clasificación de usuarios según uso de la plataforma

Usuarios Técnicos

- Administrador de Plataforma
- Arquitecto de Integración
- Desarrolladores autorizados

- Ingenieros DevOps / CI-CD
- Analistas de Seguridad

Estos usuarios acceden directamente a los componentes de Azure API Management, AKS, el flujo de trabajo, monitoreo y seguridad, y son responsables de la configuración, operación y evolución técnica de la plataforma.

Usuarios Operativos

- Funcionarios que utilizan aplicaciones integradas
- Usuarios de áreas misionales

Interactúan de forma indirecta con la plataforma a través de los sistemas consumidores de los servicios de interoperabilidad.

Usuarios de Soporte

- Personal de soporte técnico y monitoreo: Atienden incidentes, alertas y requerimientos relacionados con la disponibilidad y el desempeño del servicio.

Usuarios Externos

- Entidades o proveedores autorizados como consumidores de APIs: Acceden únicamente a los servicios habilitados, bajo controles de autenticación y autorización definidos.

Escenarios de uso de la plataforma

La plataforma de interoperabilidad es utilizada en los siguientes escenarios operativos:

Escenario 1: Consumo de servicios de interoperabilidad
Los sistemas consumidores realizan solicitudes a las APIs publicadas a través de Azure API Management, utilizando mecanismos de autenticación basados en OAuth 2.0 y tokens JWT.

Escenario 2: Gestión y publicación de APIs
Los desarrolladores y arquitectos de integración diseñan, documentan, versionan y publican APIs, definiendo contratos, políticas y productos asociados.

Escenario 3: Operación y monitoreo

Los administradores y operadores de monitoreo supervisan la disponibilidad, desempeño y errores de la plataforma mediante Azure Monitor, Log Analytics, Application Insights, Prometheus y Grafana.

Escenario 4: Atención de incidentes
El personal de soporte atiende incidentes técnicos relacionados con fallos de integración, indisponibilidad del servicio o degradación del desempeño, siguiendo los lineamientos de contingencias y SLA definidos.

Escenario 5: Gestión de proyectos y arquitectura empresarial
En este escenario, la plataforma facilita la preservación, optimización y mejora continua del intercambio de información entre aplicaciones internas y entre la entidad y organizaciones externas, garantizando la alineación de las soluciones de integración con los lineamientos técnicos, los estándares de interoperabilidad y la evolución controlada de la arquitectura.

Este uso permite evaluar impactos, gestionar cambios, estandarizar integraciones y asegurar la trazabilidad entre las necesidades identificadas, las soluciones técnicas implementadas y los servicios de interoperabilidad expuestos.

Lineamientos de uso correcto

Para garantizar una apropiación adecuada de la plataforma, se establecen los siguientes lineamientos:

- El acceso a los componentes debe realizarse conforme al principio de mínimo privilegio, según los roles definidos.
- Todas las APIs deben contar con documentación OpenAPI actualizada y versionada.
- Los despliegues deben ejecutarse exclusivamente mediante flujos automatizados que permiten construir, probar y desplegar de forma controlada y repetible (Los Flujos CI/CD definidos).
- Los secretos, claves y certificados deben gestionarse únicamente a través de Azure Key Vault.
- Las integraciones deben cumplir con los estándares técnicos definidos (JSON, REST, HTTPS, OAuth 2.0).
- Se deben revisar periódicamente las métricas y alertas de operación para detectar fallos de forma temprana.

Capacitación asociada al uso de la plataforma

La capacitación asociada al uso y apropiación de la plataforma se orienta exclusivamente al correcto uso técnico y operativo de los componentes implementados, de acuerdo con el rol de cada usuario.

Tipos de capacitación requeridos

- **Inducción técnica**: Dirigida a nuevos usuarios técnicos, enfocada en arquitectura general, roles, accesos y flujos de interoperabilidad.

- **Capacitación operativa**: Orientada a administradores y personal de soporte, enfocada en monitoreo, atención de incidentes y uso de herramientas de supervisión.

- **Capacitación de profundización**: Dirigida a desarrolladores y arquitectos de integración, enfocada en diseño de APIs, políticas de APIM, seguridad y buenas prácticas.

Los materiales de capacitación pueden incluir guías técnicas, documentación operativa, ejemplos de uso y sesiones prácticas controladas en ambientes de desarrollo o pruebas.

Seguimiento y control del uso

El seguimiento al uso y apropiación de la plataforma se realiza mediante mecanismos técnicos de monitoreo y control, sin intervención directa del usuario final.

Indicadores de uso

- Cantidad de APIs publicadas y activas
- Número de solicitudes procesadas por API
- Errores por tipo y frecuencia
- Disponibilidad del servicio
- Cumplimiento de los SLA definidos

Mecanismos de control

- Dashboards de monitoreo en Azure Monitor y Grafana
- Alertas automáticas por degradación del servicio
- Revisión periódica de logs y métricas
- Reportes de uso y desempeño del servicio

Responsabilidades frente al uso y apropiación

- Los **usuarios técnicos** son responsables del uso correcto, seguro y documentado de la plataforma.

- Los **administradores de la plataforma** deben garantizar la disponibilidad, seguridad y evolución controlada del servicio.
- El **personal de soporte** debe atender incidentes y escalar conforme a los procedimientos definidos.
- Los **consumidores externos** deben cumplir las condiciones de uso, seguridad y consumo autorizadas.

11 ANEXOS

El presente capítulo contiene los anexos técnicos de soporte que complementan la información descrita en el Manual Técnico de Interoperabilidad, proporcionando una referencia visual y descriptiva de la arquitectura, componentes y flujos de interoperabilidad implementados.

11.1 Diagramas de Arquitectura

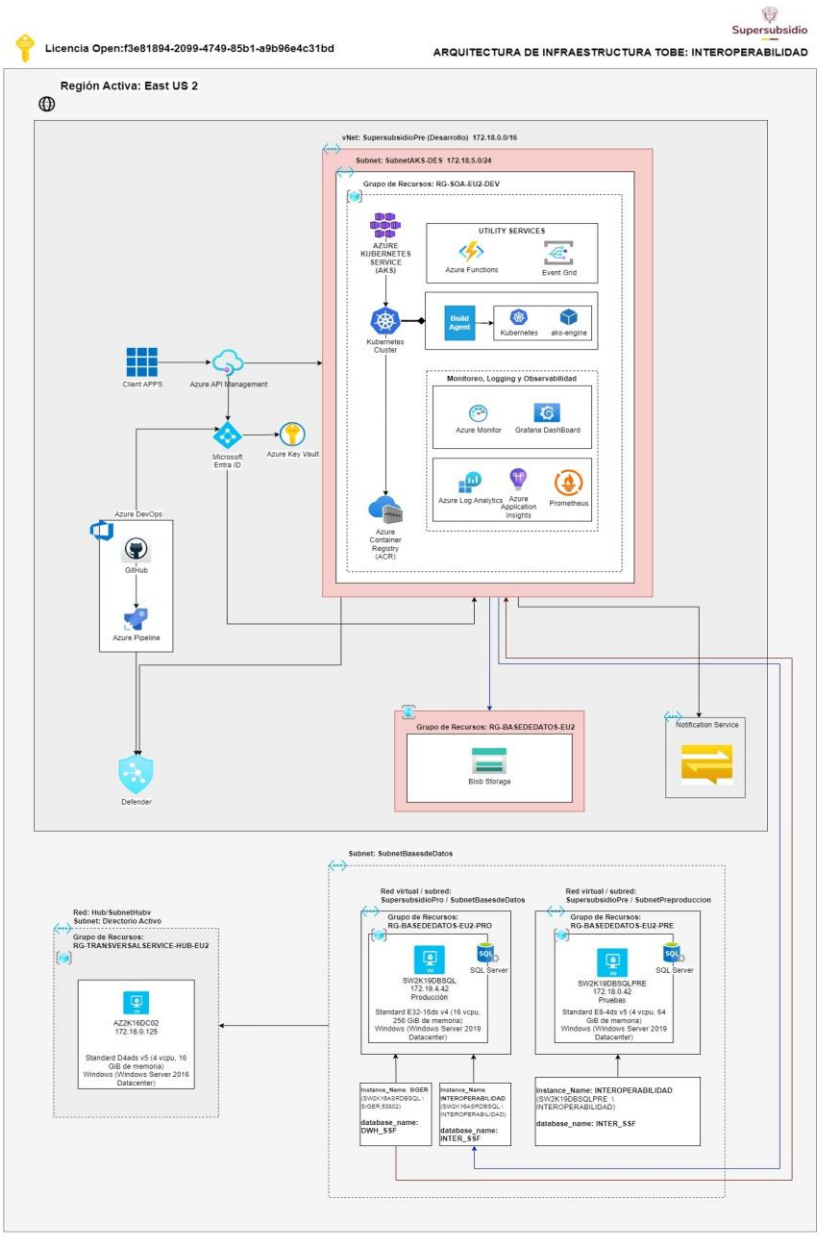
Se incluyen los diagramas que describen la arquitectura general de la plataforma de interoperabilidad, destacando los componentes principales y su interacción.

Los diagramas presentados describen:

- Arquitectura lógica de la plataforma en Microsoft Azure
- Capa de exposición de servicios mediante Azure API Management
- Plataforma de orquestación basada en Azure Kubernetes Service (AKS)
- Servicios de seguridad, identidad y gestión de secretos
- Servicios de integración y mensajería basada en eventos
- Componentes de monitoreo y observabilidad

Estos diagramas permiten una comprensión integral del modelo de interoperabilidad adoptado.

- **Vista de Tecnología: Infraestructura y Servicios Tecnológicos**



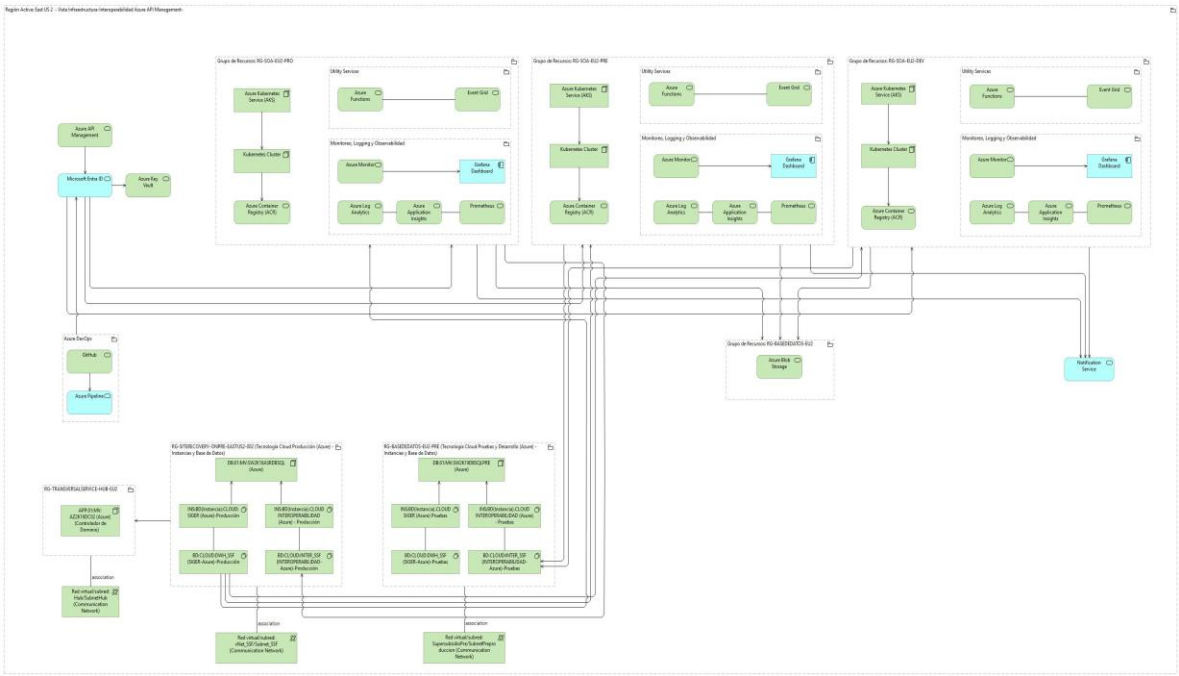
Esta vista puede observarse en tamaño completo en el repositorio del SharePoint:
(dar clic aquí)

11.2 Diagramas ArchiMate

Los diagramas ArchiMate permiten mantener la trazabilidad entre los componentes técnicos y la Arquitectura Empresarial.

Se incluyen diagramas elaborados bajo el estándar ArchiMate, los cuales representan:

- **Vista de Tecnología: Infraestructura y Servicios tecnológicos**



Esta vista puede observarse en tamaño completo en el repositorio del SharePoint:

https://ssfgov.sharepoint.com/sites/ARQUITECTURAEMPRESARIALSSF/Documentos%20compartidos/Forms/AllItems.aspx?viewid=0d7415c5%2Dfe6c%2D43af%2D8d70%2D89130fb20b2f&id=%2Fsites%2FARQUITECTURAEMPRESARIALSSF%2FDocumentos%20compartidos%2FGeneral%2F3%2E%20Repositorio%20de%20Arquitectura%2D%20Artefactos%20AS%2DIS%20Artefactos%20TO%2DBE%2FEjercicios%20de%20AE%2F2025%20%2D%20PRY%20ESTRATEGIA%20INTEROPERABILIDAD%2F%5BMTR%5D%204%2E2%2E6%20%2D%20Vista%20Infraestructura%2DInteroperabilidad%20Azure%20API%20Management%2Epdf&parent=%2Fsites%2FARQUITECTURAEMPRESARIALSSF%2FDocumentos%20compartidos%2FGeneral%2F3%2E%20Repositorio%20de%20Arquitectura%2D%20Artefactos%20AS%2DIS%20Artefactos%20TO%2DBE%2FEjercicios%20de%20AE%2F2025%20%2D%20PRY%20ESTRATEGIA%20INTEROPERABILIDAD

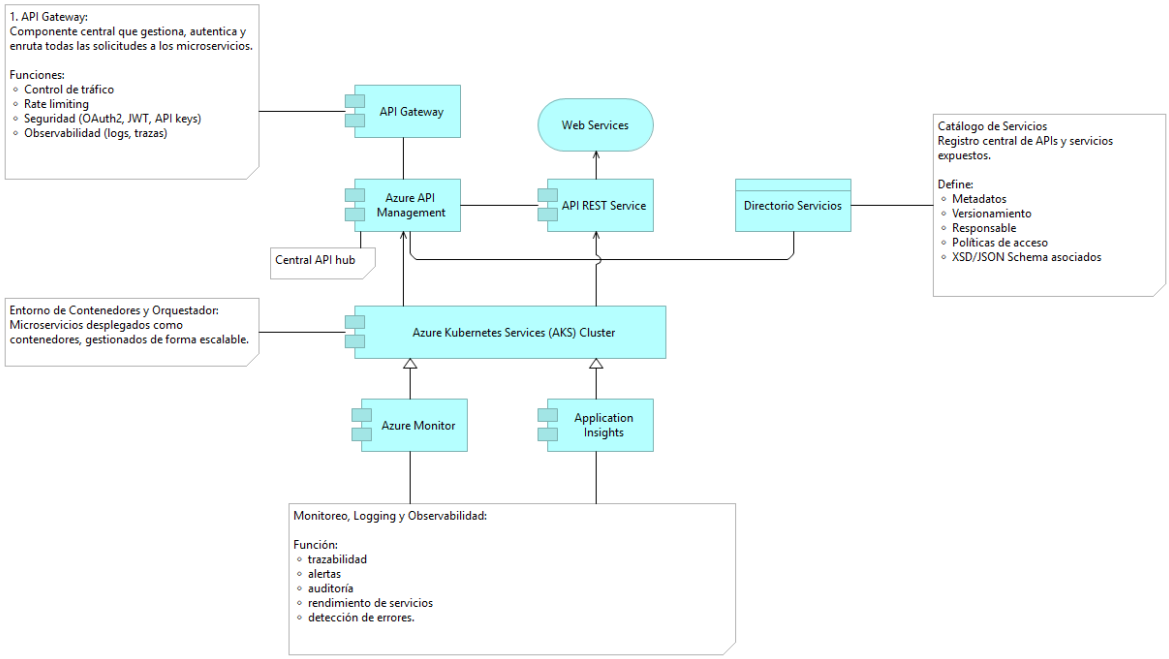
- **Vista de Aplicación: Servicios de interoperabilidad y Componentes de integración**

Trabajo

Vista de Colaboración de Componentes
Estrategia de Interoperabilidad

Arquitectura de Referencia - Transición 1

Supersubsidio



[Esta vista puede observarse en tamaño completo en el repositorio del SharePoint]

12 CONTROL DE CAMBIOS DEL DOCUMENTO

FECHA	AUTOR	VERSION	DESCRIPCION CAMBIO
15/12/25	Jennyfer Forero	1.0	Creación del documento
17/12/25	Jorge Amaya	1.0	Actualización del Documento
19/12/25	Jorge Amaya	1.0	Actualización del Documento
22/12/25	Nidia Prodigo	1.0	Actualización del documento
22/12/25	Julián Salinas	1.0	Incorporación Uso y Apropiación
29/12/25	Jose Leonardo Carrillo	1.0	Actualización del Documento