fna FONDO NACIONAL DEL AHORRO	**INFORME DE SEGUIMIENTO Y DE EVALUACIÓN CONTRACTUAL**	**Código: GLC-CONT-FO-016**
	PROCESO DE CONTRATACIÓN	**Versión: 2**

INFORME No 1 **FACTURA No** 337

No. DE ACEPTACIÓN: 1000061970

FECHA

22	06	2026
dd	mm	aaaa

1. GENERALIDADES DEL CONTRATO

CONTRATO No 132 (Número de Contrato) **DE** 2025 (Año de suscripción) **TIPO DE CONTRATO** Prestación de Servicios (Prestación de servicios, interventoria, consultoría, Convenio)

ORDENADOR DEL GASTO DANIEL CORREA CALDERON (Nombre del ordenador del Gasto) SECRETARIO GENERAL (E) (Cargo del ordenador del Gasto)

CONTRATISTA INGENIUM COLOMBIA SAS (Escriba el nombre o razón social del contratista)

TIPO DE INTERVENTORIA Y/O SUPERVISIÓN: **INDIVIDUAL** [X] **COLEGIADA** [ ]

INTERVENTOR Y/O SUPERVISOR CRISTIAN CAMILO GARCÍA PARRA (Escriba nombre del supervisor o interventor del contrato) (Escriba nombre del supervisor o interventor del contrato)

APOYO SUPERVISIÓN JAIRO ALONSO CRISTANCHO (Nombre de la persona delegada para apoyar la supervisión del contrato) (Nombre de la persona delegada para apoyar la supervisión del contrato)

OBJETO DEL CONTRATO

CONTRATAR LOS SERVICIOS ESPECIALIZADOS PARA EL DESARROLLO, IMPLEMENTACIÓN, CONFIGURACIÓN Y SOPORTE DE UNA SOLUCIÓN CORPORATIVA DE API MANAGER, QUE PERMITA LA EXPOSICIÓN SEGURA, CONTROLADA, MONITOREADA Y VERSIONADA, EN EL MARCO DE LA MODERNIZACIÓN DE LA ARQUITECTURA ORIENTADA A SERVICIOS DEL FONDO NACIONAL DEL AHORRO S.A.

DEPENDENCIA EJECUCIÓN CONTRATO GERENCIA ARQUITECTURA E INGENIERÍA DE SOFTWARE (Indique el nombre de la dependencia responsable del contrato)

PLAZO DE EJECUCIÓN DEL CONTRATO 12 meses (Indique en este espacio el número de días o de meses para ejecutar el contrato)

FECHA DE INICIACIÓN DEL CONTRATO 29 (Día) **DE** diciembre (Mes) **DE** 2025 (Año)

FECHA DE TERMINACIÓN DEL CONTRATO 28 (Día) **DE** diciembre (Mes) **DE** 2026 (Año)

REGISTRO PRESUPUESTAL No. **5400002117**

VALOR DEL CONTRATO

MIL CUATROCIENTOS TRES MILLONES SETECIENTOS OCHENTA Y DOS MIL CIENTO CINCUENTA Y OCHO PESOS M/CTE ($1.403.782.158,00) incluye IVA, demás impuestos, tasas y contribuciones a las que haya lugar.

(Indique en este espacio el valor del contrato en letras)

PRÓRROGAS	
No.	**PLAZO**

ADICIONES		
No.	**VALOR**	**RP**

SUSPENSIONES		
No	**DESDE**	**HASTA**

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	$ 1.403.782.158	**100,00%**
Adiciones		**0,00%**
VALOR TOTAL DEL CONTRATO	**$ 1.403.782.158**	**100,00%**
Valor ejecutado antes del presente pago	$ -	**0,00%**
Valor del pago aprobado con el presente informe	$ 904.981.934	**64,47%**
VALOR TOTAL EJECUTADO	**$ 904.981.934**	**64,47%**
Porcentaje de ejecución presupuestal programado a la fecha		**64,47%**
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		**0,00%**

OBSERVACIONES

Pago 01: Pago 1 de 1 por Desarrollo, implementación y estabilización de la Plataforma API Manager.

(En caso de presentarse diferencias en la ejecución presupuestal del contrato, indique brevemente la justificación de las mismas)

3. DESCRIPCION ACTIVIDADES

Porcentaje de ejecución de actividades proyectado a la fecha	**41,7%**
Porcentaje de ejecución de actividades realizado a la fecha	**41,7%**
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CONTRATO	**0,0%**

**Nota: Esta información es diligenciada unicamente para Desarrollos o mantenimientos de Aplicaciones Tecnológicas*

*La fase de ejecución corresponde a desarrollo de Software de propiedad del FNA — **SI** [ ] **NO** [X]

*Si corresponde a Software del FNA marque la fase correspondiente — **Investigación** [ ] **Desarrollo** [ ]

OBSERVACIONES

Servicio prestado en Bogotá.

(En caso de presentarse diferencias en el porcentaje de ejecución de actividades del contrato, indique brevemente la justificación de las mismas)

4. CONCEPTO SUPERVISOR O INTERVENTOR

Con base en la verificación de la prestación de los servicios relacionados dentro del Contrato en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa, y por lo tanto se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma, la cual es por concepto de soporte y Desarrollo, Implementación y Configuración de la Plataforma API Manager
Por valor de NOVECIENTOS CUATRO MILLONES NOVECIENTOS OCHENTA Y UN MILLONES NOVECIENTOS TREINTA Y CUATRO PESOS($ 904.981.934)

Nota: El profesional Wilson Morales Rada, ejerció como Apoyo a la Supervisión desde el inicio del contrato hasta el 31 de mayo de 2026. A partir del 1 de junio de 2026 el profesional Jairo Alonso Cristancho es nombrada Apoyo a la Supervisión del contrato 132-2025.

5. EVALUACIÓN CONTRATISTA (Escala de 0 - 5)

EVALUACION PARCIAL	
Cumplimiento del contrato	**4**
Plazos	**4**
Aspectos administrativos	**4**

6. CERTIFICACIÓN PARA PAGO

EL SUSCRITO GERENTE DE SERVICIOS DE T.I. E INFRAESTRUCTURA, EN SU CONDICIÓN DE SUPERVISOR DEL CONTRATO No. 132 de 2025.

CERTIFICA:

Que INGENIUM COLOMBIA SAS, identificado con NIT. No. 900.500.876-5, entregó un informe de las actividades desarrolladas en el período relacionado, dando de esta manera cumplimiento a las obligaciones contenidas en el Contrato No. 132 de 05 de noviembre de 2025.

7. CERTIFICACIÓN DE CUMPLIMIENTO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL

De conformidad con el cumplimiento de la Ley 789 de 2002, se validó que el proveedor ha realizado los aportes al Sistema de Seguridad Social Integral y Parafiscales durante la ejecución contractual. Se anexa la certificación.

ANEXOS PRESENTE INFORME

ANEXO		No FOLIOS	DESCRIPCION
Certifiicado pago Seguridad Social	X	**PDF**	Certificado, J.C.C. y Planillas de Pago
Actas	X	**PDF**	Acta ANS
Anexo Técnico	X	**PDF**	Informe de Supervisión Informe de Gestión
OTROS	X	**PDF**	Prefactura Certificación Bancaria RUT Autorización Numeración Dian Certificado cumplimiento circulares SIFC Minuta API Acta de Inicio

Para constancia de lo anterior, se firma el presente informe bajo la responsabilidad expresa de los que intervienen en el mismo en Bogotá D.C., a los

Veintidos (día en letras) **(22)** (día en números) días del mes de **junio** (mes en letras) de **2026** (Año)

CRISTIAN CAMILO GARCÍA PARRA
Gerente Arquitectura e Ingeniería de Software
Supervisor Cto 132-2025

JAIRO ALONSO CRISTANCHO
Apoyo a la Supervisor Cto 132-2025 (a partir de 1 de junio 2026)

WILSON RAFAEL MORALES RADA
Apoyo a la Supervisor Cto 132-2025 (29 dic 2025 - 31 mayo 2026)

Cl.doc. : RE (Factura bruto) Documento normal						
Reg.prelim.por	NTUIRAN	Contab.por	MRINCONZ			
Nº doc.	5100001283	Sociedad	1000	Ejercicio	2026	
Fe.docum.	25.06.2026	Fecha contab.	25.06.2026	Período	06	
Calc.impuestos	☑					
Referen.	337					
Moneda doc.	COP					
Txt.cab.doc.	02-2303-202606250813638					

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1004003807	INGENIUM COLOMBIA SA		W0	849,344,557-
2	86	2511950101	CXP PROVED EM/RF		W0	904,981,934
3	81	5130950114	SERV DE APOYO TEMP		W0	0
4	50	2519051101	SERVICIO 3.5%			26,617,116-
5	50	2519053801	RTE IVA TARIFA GENER			21,673,937-
6	50	2519054408	SERVICIOS 304 BOGOTA			7,346,324-

FACTURA DE VENTA ELECTRÓNICA N°: FE 337

INGENIUM COLOMBIA SAS
900.500.876-5
CR 7 B 127 36 AP 502
Bogotá - Colombia
3143845903
info@ingeniumcolombia.com
www.ingeniumcolombia.com

Cliente: Fondo Nacional de Ahorro S.A.
Nit: 899.999.284-4
Teléfono: (601) 3810150
Dirección: Calle 12 65 11
Correo: facturacionelectronica@fna.gov.co

Fecha y hora Factura	
Generación	25/06/2026, 09:21
Expedición	25/06/2026, 09:21
Vencimiento	25/07/2026
Vendedor	INGENIUM COLOMBIA SAS INGENIUM
Centro de costo	17-1
Cotización	

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Bruto	Impto. Cargo	Valor Impto.Cargo	Vr. Total	Valor desc.
1	CONTRATO FNA-132-2025 - Primer pago - Desarrollo, implementación y estabilización de la Plataforma API Manager	1.00	760,489,020.17	760,489,020.17	19 %	144,492,913.83	904,981,934.00	0.00

Total items: 1

Valor en Letras:
Novecientos cuatro millones novecientos ochenta y un mil novecientos treinta y cuatro pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Otro - Crédito - Cuota No. 001 vence el 2026-07-25 por $ 904,981,934.00

Total Bruto	**760,489,020.17**
IVA 19% Compras	**144,492,913.83**
Total a Pagar	**904,981,934.00**

Observaciones:
Esta factura de venta es titulo valor de conformidad con la ley 1231 de 2008 y vencido el plazo de pago de la presente factura causará al máximo intereses de mora permitidos.
Número de aprobación: 1000061970

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764106592831 aprobado en 20260301 prefijo FE desde el número 205 al 500 Vigencia: 24 Meses**Responsable de IVA - Actividad Económica 7111 Actividades de arquitectura Tarifa
CUFE: 0287aa62c3e77ed59dc0b39525601a3f1bfa7a46c2709d3c4864a78c351d911a6c213c1b0afaa7484811127d98750e63

Elaborado por

Firma recibido

Fabricante Software y Proveedor tecnológico: Siigo SAS - Nit 830.048.145-8, Nombre Software: Siigo Nube. Firma electrónica: ver en el XML

CERTIFICACIÓN DE CUMPLIMIENTO DEL PAGO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL INTEGRAL
(LEY 100 DE 1993, LEY 1562 DE 2012, DECRETO 780 DE 2016 Y LEY 797 DE 2003)

Yo JORGE EDUARDO MOLINA JIMENEZ, identificado con Nro.1072894364, en micalidad de **REVISOR FISCAL**, de la empresa **INGENIUM COLOMBIA SAS** con NIT. 900.500.876-5 (en adelante "la empresa") manifiesto, bajo la gravedad del juramento, que la empresa ha cumplido durante los seis (6) meses anteriores a la fecha de este documento, con los pagos al sistema de seguridad social en salud, pensiones y riesgos laborales y con los aportes parafiscales correspondientes a todos sus empleados vinculados por contrato de trabajo, por lo quedeclaro que se encuentra a PAZ Y SALVO con las Empresas Promotoras de Salud -EPS-, Fondos de Pensiones, Administradoras de Riesgos Profesionales -ARP-, Caja de Compensación Familiar, Instituto Colombiano de Bienestar Familiar -ICBF- y Servicio Nacional de Aprendizaje -SENA-.

Firmada en Bogotá, 04 junio de 2026.



Firma

JORGE EDUARDO MOLINA JIMENEZ
Identificación No. 1072894364
En calidad de REVISOR FISCAL
T.P. 190330-T
Ciudad BOGOTÁ

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Certificado No:

D A 9 2 F 0 E 9 C 4 E 7 4 8 2 3

LA REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

UNIDAD ADMINISTRATIVA ESPECIAL

JUNTA CENTRAL DE CONTADORES

CERTIFICA A:
QUIEN INTERESE

Que el contador público **JORGE EDUARDO MOLINA JIMENEZ** identificado con CÉDULA DE CIUDADANÍA No 1072894364 de PASCA (CUNDINAMARCA) Y Tarjeta Profesional No 190330-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de Inscripción.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS * * *

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900500876-5	INGENIUM COLOMBIA SAS	CRA 7 B #127-36 APTO 502	3143845903	info@ingeniumcolombia.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL / CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
ÚNICA	B – menos de 200 cot		BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	NÚMERO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	CANTIDAD EMPLEADOS	CANTIDAD UPC
		79083259	04/05/2026	12	0
PERIODO SALUD	PERIODO PENSIÓN	TIPO PLANILLA	TOTAL NÓMINA	TOTAL A PAGAR	
2026-05	2026-04	E	$114,652,759	$29.023.900	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS005	Sanitas EPS	800251440-6	2.634.400	0		0		0	0	0	0	2.634.400	5
EPS008	Compensar EPS	860066942-7	1.356.900	0		0		0	0	0	0	1.356.900	3
EPS010	EPS Sura	800088702-2	330.000	0		0		0	0	0	0	330.000	1
EPS017	Famisanar EPS	830003564-7	70.100	0		0		0	0	0	0	70.100	1
EPS037	Nueva EPS	900156264-2	160.000	0		0		0	0	0	0	160.000	1

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230301	Porvenir	800224808-8	6.600.500	0	0	186.400	186.400	0	0		6.973.300	4
230901	Skandia Pensiones Obligatorias	800253055-2	4.876.800	0	0	152.400	152.400	0	0		5.181.600	2
231001	Colfondos	800227940-6	2.094.600	0	0	56.700	56.700	0	0		2.208.000	2
25-14	Colpensiones	900336004-7	4.632.700	0	0	144.900	144.900	0	0		4.922.500	3

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatoria	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-7	Seguros Bolivar S.A.	860002503-2	600.600				600.600	0	0	600.600			6.006	600.600	12

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF24	Compensar Caja	860066942-7	4.586.500	0	0	4.586.500	12

TOTALES PARAFISCALES

Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
SENA				
0	0	0	0	0
ICBF				
0	0	0	0	0
ESAP				
MEN				

TOTALES POR SUBSISTEMA

Tipo Administradora	No. Administradoras Reportadas	Valor antes de IGE, LMA, IRP y Mora	Total a Pagar
Salud	5	4.551.400	4.551.400
Pensión	4	19.285.400	19.285.400
Riesgos Laborales	1	600.600	600.600
CCF	1	4.586.500	4.586.500
ESAP	0	0	0
ICBF	0	0	0
MEN	0	0	0
SENA	0	0	0
TOTALES	11	29.023.900	29.023.900

PAGADA

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900500876-5	INGENIUM COLOMBIA SAS	CRA 7 B #127-36 APTO 502	3143845903	info@ingeniumcolombia.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL / CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
ÚNICA	B – menos de 200 cot		BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA					
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	NÚMERO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	CANTIDAD EMPLEADOS	CANTIDAD UPC
		79083259	04/05/2026	12	0
PERIODO SALUD	PERIODO PENSIÓN	TIPO PLANILLA	TOTAL NÓMINA	TOTAL A PAGAR	
2026-05	2026-04	E	$114,652,759	$29.023.900	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE								INFORMACIÓN NOVEDADES																		PENSIÓN								SALUD				RIESGOS LABORALES				CCF				PARAFISCALES					
No.	Tipo y Número de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Cotiz. exterior	Exonerado	ING	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Días	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Días	Cotización / Valor UPC	Cód. ARL	IBC ARL	Días	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Días	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC 1014309227	VELANDIA RAMOS PAULA ANDREA	1	0			S																	25-14	8.933.500	30	1.429.400	0	0	44.700	44.700	EPS005	8.933.500	30	357.400	14-7	8.933.500	30	1	46.700	CCF24	8.933.500	30	357.400	0	0	0	0	0
2	CC 1019079045	CHICA HERNANDEZ SARA JULIANA	1	0			S																	25-14	10.500.000	30	1.680.000	0	0	52.500	52.500	EPS008	10.500.000	30	420.000	14-7	10.500.000	30	1	54.900	CCF24	10.500.000	30	420.000	0	0	0	0	0
3	CC 1019103577	MILLAN MARTINEZ JULIANA	1	0			S																	230301	4.000.000	30	640.000	0	0	0	0	EPS037	4.000.000	30	160.000	14-7	4.000.000	30	1	20.900	CCF24	4.000.000	30	160.000	0	0	0	0	0
4	CC 1069727229	CRISTANCHO CRUZ LEYDI VIVIANA	1	0			S																	230301	17.502.900	30	2.800.500	0	0	87.600	87.600	EPS005	17.502.900	30	700.200	14-7	17.502.900	30	1	91.400	CCF24	17.502.900	30	700.200	0	0	0	0	0
5	CC 1069734144	ESCOBAR CASTAÑEDA ADRIANA LUCIA	1	0			S																	25-14	9.202.667	29	1.472.500	0	0	46.100	46.100	EPS008	9.202.667	29	368.200	14-7	9.202.667	29	1	48.100	CCF24	9.202.667	29	368.200	0	0	0	0	0
6	CC 1069734144	ESCOBAR CASTAÑEDA ADRIANA LUCIA	1	0			S												X					25-14	317.334	1	50.800	0	0	1.600	1.600	EPS008	317.334	1	12.700	14-7	317.334	1	1	0	CCF24	317.334	1	12.700	0	0	0	0	0
7	CC 1069736648	ESCOBAR CASTAÑEDA LUIS ANDRES	1	0			S																	230301	7.975.000	29	1.276.000	0	0	39.900	39.900	EPS010	7.975.000	29	319.000	14-7	7.975.000	29	1	41.700	CCF24	7.975.000	29	319.000	0	0	0	0	0
8	CC 1069736648	ESCOBAR CASTAÑEDA LUIS ANDRES	1	0			S												X					230301	275.000	1	44.000	0	0	1.400	1.400	EPS010	275.000	1	11.000	14-7	275.000	1	1	0	CCF24	275.000	1	11.000	0	0	0	0	0
9	CC 35250774	MORALES CRISTANCHO MARY LUZ	1	0			S																	231001	1.750.905	30	280.200	0	0	0	0	EPS017	1.750.905	30	70.100	14-7	1.750.905	30	1	9.200	CCF24	1.750.905	30	70.100	0	0	0	0	0
10	CC 35510626	VELANDIA BAUTISTA ROSA LIBIA	51	5			N																		0	0	0	0	0	0	0		0	0	0	14-7	1.750.905	30	1	9.200	CCF24	875.453	8	35.100	0	0	0	0	0
11	CC 79745600	BERNAL PULIDO JAIME LEONARDO	1	0			S																	230901	16.580.000	30	2.652.800	0	0	82.900	82.900	EPS005	16.580.000	30	663.200	14-7	16.580.000	30	1	86.600	CCF24	16.580.000	30	663.200	0	0	0	0	0
12	CC 80224911	GALEANO AVENDAÑO JOAN DAVID	1	0			S																	231001	11.340.000	30	1.814.400	0	0	56.700	56.700	EPS005	11.340.000	30	453.600	14-7	11.340.000	30	1	59.200	CCF24	11.340.000	30	453.600	0	0	0	0	0
13	CC 80549047	MELO SALAMANCA NELSON EDUARDO	1	0			S																	230901	13.900.000	30	2.224.000	0	0	69.500	69.500	EPS008	13.900.000	30	556.000	14-7	13.900.000	30	1	72.600	CCF24	13.900.000	30	556.000	0	0	0	0	0
14	CE 902080	CALDERON HERNANDEZ NEDUARD EMILIO	1	0			S																	230301	11.500.000	30	1.840.000	0	0	57.500	57.500	EPS005	11.500.000	30	460.000	14-7	11.500.000	30	1	60.100	CCF24	11.500.000	30	460.000	0	0	0	0	0

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 0

Acta N°	01	**Tema:**	Medición de los indicadores de ANS de la gestión del contrato FNA-132-2025 correspondiente a Desarrollo implementación y estabilización de la plataforma API mánager
Fecha:	28 de mayo de 2026	**Ubicación:**	TEAMS
Hora inicio:	8:30 AM	**Hora fin:**	9:30 A.m.
Objetivo	Medición de los indicadores de ANS: de la gestión del contrato FNA-132-2025 Desarrollo, Implementación y Configuración de la Plataforma API Manager		

PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	**Dependencia**	**Cargo**	**¿Asistió?**
Cristian Camilo Garcia Parra	VP Tecnología y Transformación Digital	Gerencia de Arquitectura e ingeniería de software	Si
Wilson Rafael Morales Rada	VP Tecnología y Transformación Digital	Profesional 05 Apoyo Supervisión Contrato	Si
Frank ortiz	Ingenium SaaS	Gerente del Proyecto	Si

1. **TEMAS TRATADOS** (Describir los puntos tratados en la reunión)

MEDICIÓN DE ANS: Se evaluaron los resultados de la revisión de los Acuerdos de Nivel de Servicio establecidos en el contrato FNA-132-2025 y relacionados en el formato Código: Anexo 2 - Acuerdos Niveles de Servicios - ANS - API Manager_correspondiente a la entrega de licenciamiento y Desarrollo, Implementación y Configuración de la Plataforma API Manager

Adicional se revisó el documento **INFORME ENTREGA PLATAFORMA API MANAGER, el cual contiene los entregables exigidos en el anexo técnico del contrato, los cuales son:**

9. ENTREGABLES TÉCNICOS

El proveedor del servicio que resulte adjudicatario deberá cumplir con los entregables que se relacionan a continuación, cuyas fecha de entrega serán concertadas con el supervisor del contrato en la etapa de Desarrollo, implementación y estabilización:

ID	ENTREGABLE
1	API Gateway desplegado y operativo
2	Implementación de las políticas definidas
3	Versionamiento activo y control de accesos
4	Auditoria y monitoreo de tráfico en producción

ID	ENTREGABLE
5	Documentación de integración detallada
6	Diagramas de arquitectura detallados.
7	Manuales de usuario y operación
8	Documento de arquitectura de la Solución

1. COMPROMISOS PACTADOS

DESCRIPCIÓN	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO
No aplica		

Teniendo en cuenta lo anterior, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de desarrollo, implementación y configuración de la plataforma API MANAGER por valor de **NOVECIENTOS CUATRO MILLONES NOVECIENTOS OCHENTA Y UN MIL NOVECIENTOS TREINTA Y CUATRO PESOS (904,981,934)** incluido IVA

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 0

ELABORÓ	APROBÓ
 **FRANK ORTIZ** Ingenium Colombia Gerente de Proyectos	 **WILSON RAFAEL MORALES RADA** VP Tecnología y Transformación Digital Profesional 05 Apoyo a la supervisión Contrato 132-2025  **CRISTIAN GARCÍA PARRA** Gerente de arquitectura e ingeniería de software Supervisor contrato 132-2025

CONTRATO FNA-132-2025
SUSCRITO CON INGENIUM COLOMBIA SAS

OBJETO DEL CONTRATO ESTATAL

Contratar los servicios especializados para el desarrollo, implementación, configuración y soporte de una solución corporativa de api manager, que permita la exposición segura, controlada, monitoreada y versionada en el marco de la modernización de la arquitectura orientada a servicios del Fondo Nacional del Ahorro S.A.

Desarrollo, Implementación y Configuración de la Plataforma API Manager

BOGOTÁ D.C., JUNIO DE 2026

Contenido

1. *INTRODUCCIÓN* _____ *3*
2. *RESUMEN EJECUTIVO* _____ *3*
3. *OBJETIVO DEL INFORME* _____ *4*
4. *OBJETIVOS ESPECÍFICOS DEL INFORME* _____ *4*
5. *INFORME DE CRONOGRAMA AVANCE* _____ *4*
6. *INFORMACIÓN DE AVANCE PRESUPUESTAL* _____ *4*
7. *INFORME DEL CONTRATISTA* _____ *5*
8. *NIVELES DE SERVICIO* _____ *19*
9. *CONCEPTO SUPERVISION* _____ *20*

1. INTRODUCCIÓN

El presente informe de supervisión del Contrato No. 132 de 2025, cuyo objeto es contratar los servicios especializados para el desarrollo, implementación, configuración de la plataforma API MANAGER

2. RESUMEN EJECUTIVO

En cumplimiento a la supervisión asignada, se realizó el seguimiento a las actividades conforme a lo establecido en el Contrato Estatal No.132 de 2025 en cuanto a Desarrollo, implementación y configuración de la plataforma API MANAGER.

Las siguientes son las actividades que desarrolló Ingenium en lo referente a

Los componentes a Implementar son:

- ✓ API Gateway: Punto de entrada unificado para servicios REST.
- ✓ Developer Portal: Exposición controlada de APIs a consumidores
- ✓ internos/externos.
- ✓ Policies: Control de acceso, auditoría y límites de uso.
- ✓ API Analytics: Visualización de métricas clave de consumo, fallas y tiempos de
- ✓ respuesta.
- ✓ Control de Versiones y Publicación: Soporte a múltiples versiones activas y ciclo
- ✓ de vida de APIs.
- ✓ Contenedores y Orquestación: Implementación de microservicios en
- ✓ contenedores Docker con orquestación a través de Kubernetes, garantizando
- ✓ escalabilidad y resiliencia.

3. OBJETIVO DEL INFORME

Realizar seguimiento a los servicios acorde al contrato 132 de 2025

4. OBJETIVOS ESPECÍFICOS DEL INFORME

- Realizar seguimiento a las actividades contratadas y ejecutadas para entrega a la plataforma API MANAGER.
- Expedir constancia del cumplimiento a cargo del contratista previo al pago de la factura.
- Identificar las observaciones o desviaciones de las actividades realizadas, en caso de haberlas, con el fin de definir los planes de acción para su mitigación o eliminación.

5. INFORME DE CRONOGRAMA AVANCE

De acuerdo con lo establecido en el Contrato No 132 de 2025, se realiza el seguimiento, control y verificación de los servicios debidamente proporcionados durante el periodo comprendido entre el **29 de Abril 2026 a 29 de Mayo de 2026** con un porcentaje de avance de 41,7 %

ÍTEM	DESCRIPCIÓN	VALOR
1	Duración del contrato (12 meses)	$ 1.403.782.158,00
2	Periodo de ejecución	12 meses
3	Porcentaje de ejecución de actividades proyectado a la fecha de corte del período	41,7%
4	Porcentaje de ejecución de actividades reales a la fecha	41,7%

6. INFORMACIÓN DE AVANCE PRESUPUESTAL

ÍTEM	SEGUIMIENTO PRESUPUESTAL	VALORES	PORCENTAJE
1	Valor total del contrato	$ 1403.782.158	100.00%
2	Total ejecutado antes del presente pago		

ÍTEM	SEGUIMIENTO PRESUPUESTAL	VALORES	PORCENTAJE
3	Descuentos por ANS del periodo	0	0
4	Valor a pagar en el período	$ 904,981,934	64,47%
5	Total ejecutado		0%
6	Valor pendiente por ejecutar	$ 498.800.224	35,53

7. INFORME DEL CONTRATISTA

El contratista entregó el informe en forma oportuna, se realizó revisión y ajustes. En dicho informe se refleja la gestión realizada como se muestra a continuación

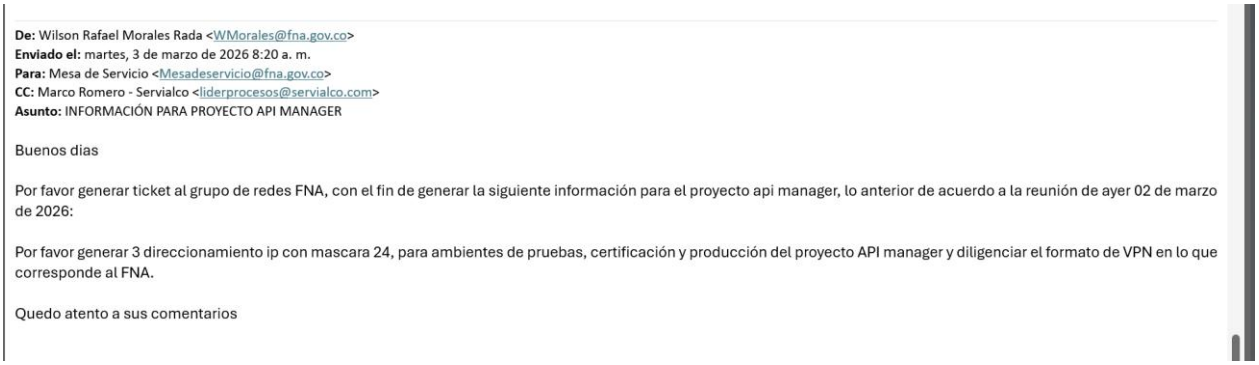
- ***INFORME DE GESTIÓN FNA API MANAGER***

Fecha / Semana	Actividad de soporte y mantenimiento	Descripción / alcance	Stakeholders involucrados (FNA / Ingenium)	Entregable / resultado
04/05/2026 – 06/05/2026	Pruebas y ajustes de conectividad desde AWS y revisión y configuración de rutas internas.	Validación de la conexión VPN con el FNA y configuración de la ruta interna bogcsoa desde EC2.	Wilson Morales, Equipo técnico FNA, Equipo Ingenium	Conexión VPN; apuntamiento de rutas internas.

Fecha / Semana	Actividad de soporte y mantenimiento	Descripción / alcance	Stakeholders involucrados (FNA / Ingenium)	Entregable / resultado
06/05/2026 – 08/05/2026	Reuniones técnicas para revisión de servicios ESB (GestorDocumental, Simulador Hipotecario, TransUnion).	Validación de errores en servicios del bus de integración como parte de las actividades de consumo controlado.	Wilson Morales, Equipo técnico FNA, Equipo Ingenium	Reporte de servicios con error; solución de errores; solicitud de validación para servicios identificados como no productivos.
11/05/2026	Seguimiento y solución de errores sobre servicios ESB con error.	Pruebas y validación de errores sobre el consumo de servicios en el ambiente de certificación.	Wilson Morales, Equipo técnico FNA, Equipo Ingenium	Reporte de servicios con error; solución de errores; solicitud de validación para servicios que continúan con error.
12/05/2026 – 19/05/2026	Configuración de rutas en el API Manager.	Configuración y validación de la conexión VPN y apuntamiento hacia el nodo bogpsoa.	Wilson Morales, Equipo técnico FNA, Equipo Ingenium	Conexión VPN; apuntamiento de rutas internas.
13/05/2026	Presentación del Frontend del API Manager.	Reunión de revisión del Frontend del API Manager y de sus diferentes funcionalidades.	Wilson Morales, Equipo Ingenium	Presentación del API Manager realizada.
20/05/2026	Presentación del Frontend del API Manager.	Reunión de revisión del Frontend del API Manager y de sus diferentes funcionalidades, con participación ampliada de la supervisión del contrato.	Wilson Morales, Cristian García, Andrés Escobar, Equipo Ingenium	Presentación del API Manager realizada.
20/05/2026 – 27/05/2026	Seguimiento y solución de errores sobre servicios ESB con error.	Identificación de errores de backend sobre los servicios 231 y 233 y pruebas posteriores a la solución del error interno.	Wilson Morales, Equipo técnico FNA, Equipo Ingenium	Identificación de errores de backend; servicios

Fecha / Semana	Actividad de soporte y mantenimiento	Descripción / alcance	Stakeholders involucrados (FNA / Ingenium)	Entregable / resultado
				funcionando correctamente.
15/05/2026 – 29/05/2026	Documentación de la solución.	Avance en la documentación técnica de la solución, así como en el documento de arquitectura.	Equipo Ingenium	Documentación técnica; avance del documento de arquitectura.
26/05/2026	Validación de servicios adicionales y solicitud de insumos requeridos.	Revisión de servicios adicionales remitidos por el FNA, envío de observaciones, validaciones e insumos requeridos.	Equipo Ingenium	Correo de solicitud de insumos.

Todas las configuraciones en el ambiente de producción de la plataforma gravitte- api manager, se realizaron de acuerdo a los segmentos de red asignados por el FNA desde el 11 de marzo del 2026 como se muestra a continuación:



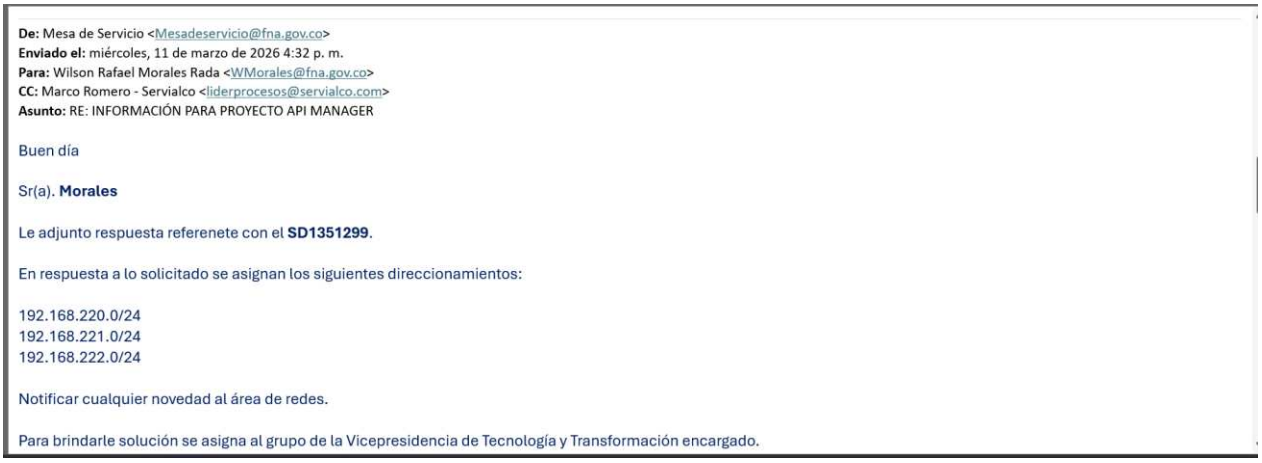
De: Wilson Rafael Morales Rada <WMorales@fna.gov.co>
Enviado el: martes, 3 de marzo de 2026 8:20 a. m.
Para: Mesa de Servicio <Mesadeservicio@fna.gov.co>
CC: Marco Romero - Servialco <liderprocesos@servialco.com>
Asunto: INFORMACIÓN PARA PROYECTO API MANAGER

Buenos dias

Por favor generar ticket al grupo de redes FNA, con el fin de generar la siguiente información para el proyecto api manager, lo anterior de acuerdo a la reunión de ayer 02 de marzo de 2026:

Por favor generar 3 direccionamiento ip con mascara 24, para ambientes de pruebas, certificación y producción del proyecto API manager y diligenciar el formato de VPN en lo que corresponde al FNA.

Quedo atento a sus comentarios



De: Mesa de Servicio <Mesadeservicio@fna.gov.co>
Enviado el: miércoles, 11 de marzo de 2026 4:32 p. m.
Para: Wilson Rafael Morales Rada <WMorales@fna.gov.co>
CC: Marco Romero - Servialco <liderprocesos@servialco.com>
Asunto: RE: INFORMACIÓN PARA PROYECTO API MANAGER

Buen día

Sr(a). **Morales**

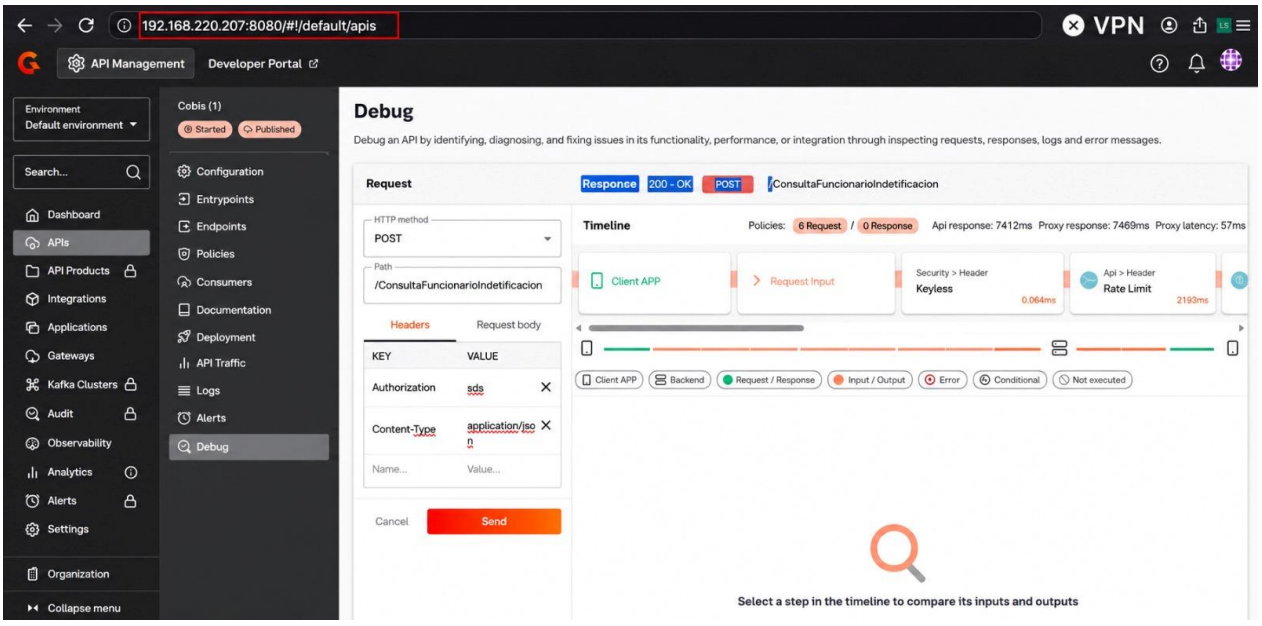
Le adjunto respuesta referenete con el **SD1351299**.

En respuesta a lo solicitado se asignan los siguientes direccionamientos:

192.168.220.0/24
192.168.221.0/24
192.168.222.0/24

Notificar cualquier novedad al área de redes.

Para brindarle solución se asigna al grupo de la Vicepresidencia de Tecnología y Transformación encargado.



- ✓ **Implementación de infraestructura y cumplimiento de la postura de seguridad institucional**

Como parte de la implementación de la solución API Manager, el Fondo Nacional del Ahorro asignó oficialmente los segmentos de red institucionales 192.168.220.0/24, 192.168.221.0/24 y 192.168.222.0/24, destinados al despliegue de la infraestructura tecnológica del proyecto.

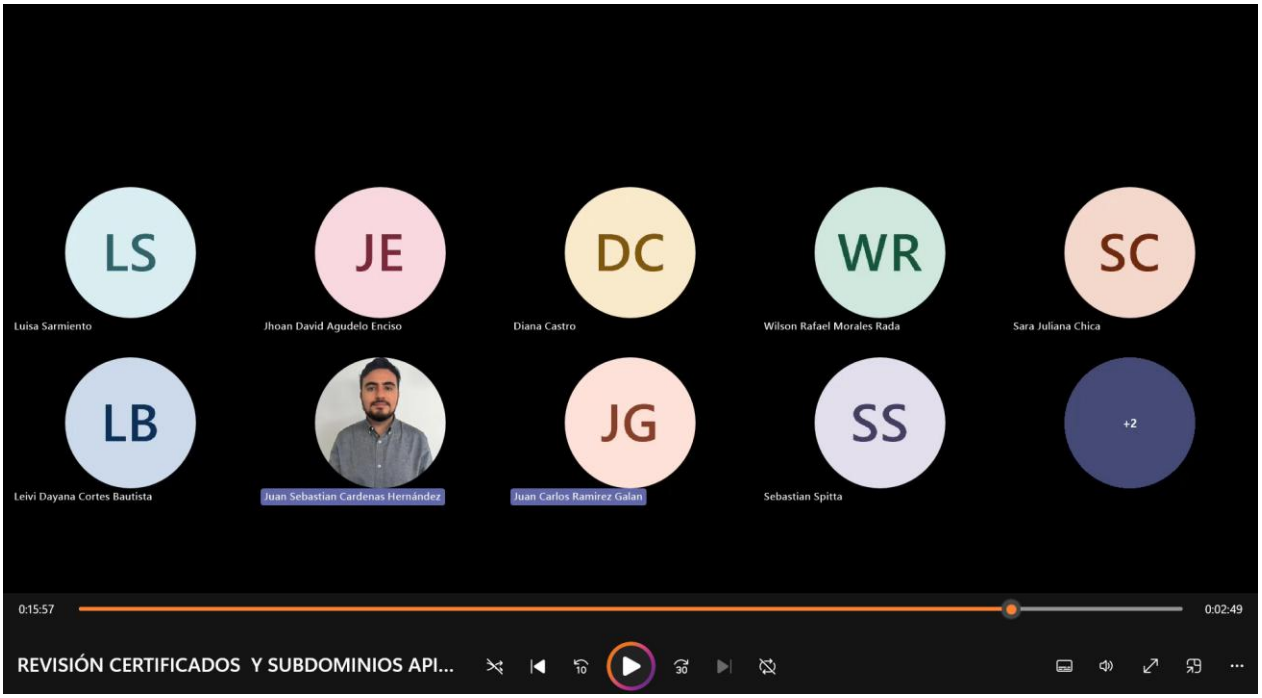
Sobre dicha infraestructura, fue instalada la plataforma API Manager, configurándose la consola administrativa mediante la dirección IP privada 192.168.220.207, perteneciente al segmento institucional asignado.

Las evidencias aportadas demuestran, que la plataforma se encontraba desplegada, configurada y operativa, permitiendo el acceso a la consola administrativa y la ejecución de las funcionalidades propias de la solución, utilizando direccionamiento IP institucional. (192.168.220.207), lo cual demuestra que la solución fue instalada se encontraba operativa y funcional.

En consecuencia, el proyecto ya disponía de una infraestructura funcional, sobre la cual posteriormente se implementaron los controles de seguridad definidos por la entidad y definidos en las mesas técnicas realizadas con los gerentes de Seguridad de la Información y Ciberseguridad del FNA, en estas sesiones se revisó la arquitectura y solución propuesta para la publicación de servicios institucionales, como resultado de dichas revisiones, se recomendó que, para cumplir con la postura de seguridad del Fondo Nacional del Ahorro, la plataforma no debía exponerse mediante direcciones IP, sino a través de dominios institucionales protegidos mediante certificados digitales SSL/TLS.

A continuación se muestran los pantallazos de la reunión y se cuenta con la grabación de la reunión





En cumplimiento de este lineamiento, se gestionó la creación de los dominios institucionales correspondientes para cada uno de los ambientes de la solución como se muestra a continuación.

✓ **Ambiente de pruebas**

- console.test.apimanager.fna.gov.co
- portal.test.apimanager.fna.gov.co
- gateway.test.apimanager.fna.gov.co

✓ **Ambiente de certificación**

- console.cert.apimanager.fna.gov.co
- portal.cert.apimanager.fna.gov.co
- gateway.cert.apimanager.fna.gov.co

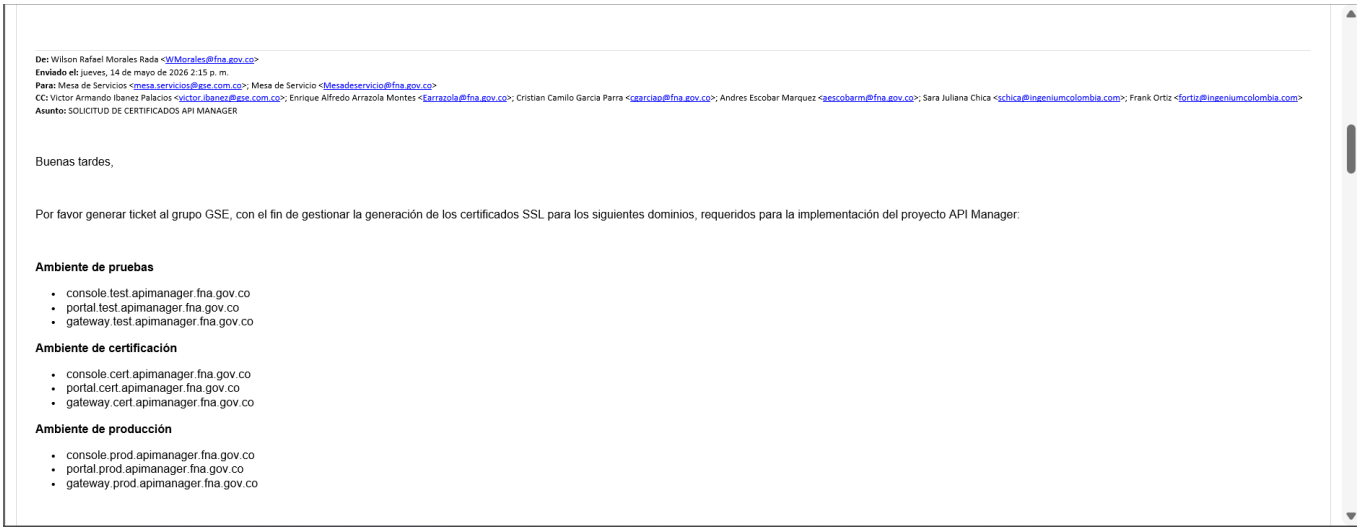
- ✓ **Ambiente de producción**

- console.prod.apimanager.fna.gov.co
- portal.prod.apimanager.fna.gov.co
- gateway.prod.apimanager.fna.gov.co

Posteriormente, se solicitó la generación de los respectivos certificados SSL/TLS para cada uno de estos dominios, con el propósito de garantizar:

- navegación segura mediante protocolo HTTPS;
- autenticidad de los servicios publicados;
- cifrado de la información en tránsito
- cumplimiento de los lineamientos institucionales de Seguridad de la Información;
- utilización de dominios oficiales del Fondo Nacional del Ahorro para todos los componentes de la plataforma.

Las solicitudes de creación de dominios institucionales y de generación de certificados SSL/TLS corresponden a actividades posteriores al despliegue de la plataforma, orientadas a fortalecer los controles de seguridad definidos por el Fondo Nacional del Ahorro para su operación en ambientes corporativos. Dichas actividades fueron realizadas sobre una solución previamente instalada y operativa, la cual ya funcionaba utilizando el direccionamiento IP institucional asignado por el área de Redes



De: Wilson Rafael Morales Rada <WMorales@fna.gov.co>
Enviado el: jueves, 14 de mayo de 2026 2:15 p. m.
Para: Mesa de Servicios <mesa.servicios@gse.com.co>; Mesa de Servicio <Mesadeservicio@fna.gov.co>
CC: Victor Armando Ibanez Palacios <victor.ibanez@gse.com.co>; Enrique Alfredo Arrazola Montes <Earrazola@fna.gov.co>; Cristian Camilo Garcia Parra <ccarciap@fna.gov.co>; Andres Escobar Marquez <aescobarm@fna.gov.co>; Sara Juliana Chica <schica@ingeniumcolombia.com>; Frank Ortiz <fortiz@ingeniumcolombia.com>
Asunto: SOLICITUD DE CERTIFICADOS API MANAGER

Buenas tardes,

Por favor generar ticket al grupo GSE, con el fin de gestionar la generación de los certificados SSL para los siguientes dominios, requeridos para la implementación del proyecto API Manager:

Ambiente de pruebas

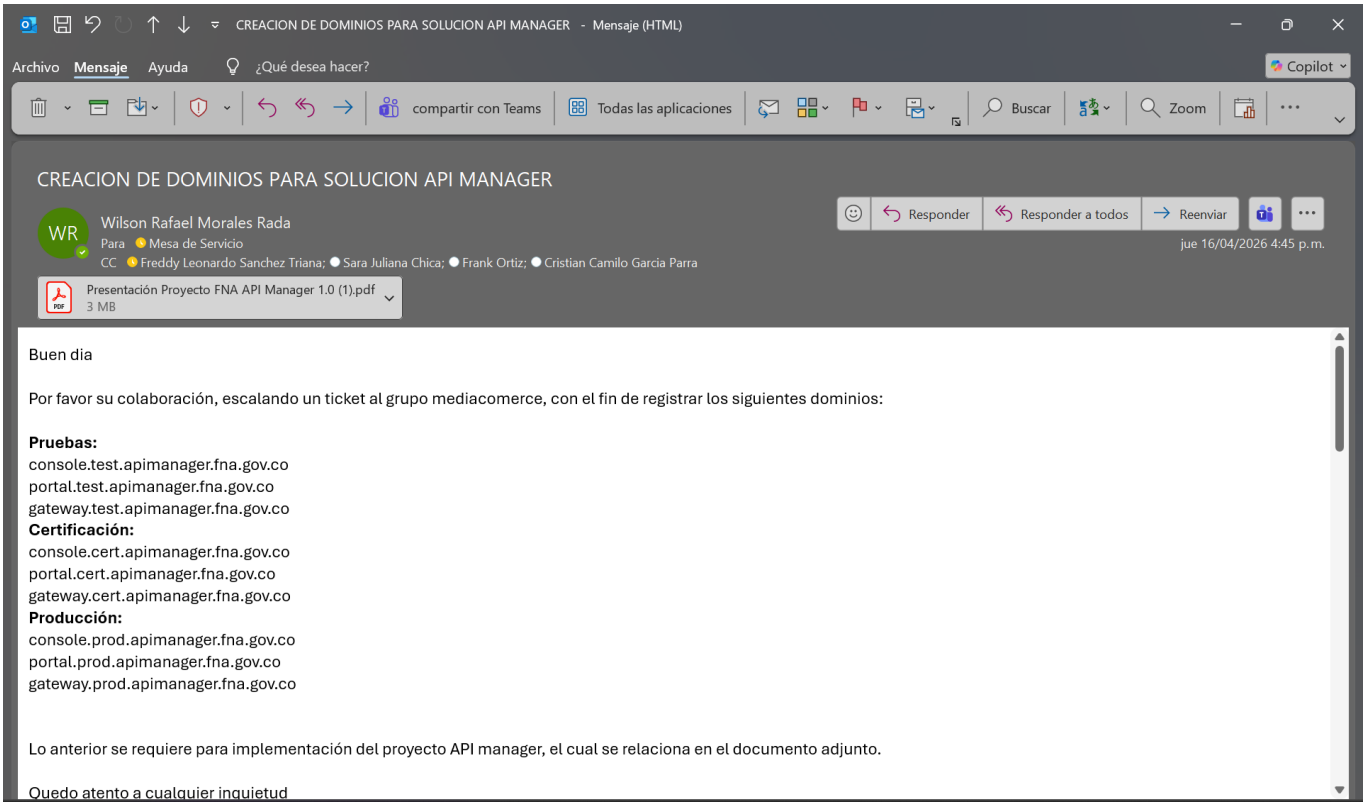
- console.test.apimanager.fna.gov.co
- portal.test.apimanager.fna.gov.co
- gateway.test.apimanager.fna.gov.co

Ambiente de certificación

- console.cert.apimanager.fna.gov.co
- portal.cert.apimanager.fna.gov.co
- gateway.cert.apimanager.fna.gov.co

Ambiente de producción

- console.prod.apimanager.fna.gov.co
- portal.prod.apimanager.fna.gov.co
- gateway.prod.apimanager.fna.gov.co



Buen dia

Por favor su colaboración, escalando un ticket al grupo mediacomerce, con el fin de registrar los siguientes dominios:

Pruebas:
console.test.apimanager.fna.gov.co
portal.test.apimanager.fna.gov.co
gateway.test.apimanager.fna.gov.co
Certificación:
console.cert.apimanager.fna.gov.co
portal.cert.apimanager.fna.gov.co
gateway.cert.apimanager.fna.gov.co
Producción:
console.prod.apimanager.fna.gov.co
portal.prod.apimanager.fna.gov.co
gateway.prod.apimanager.fna.gov.co

Lo anterior se requiere para implementación del proyecto API manager, el cual se relaciona en el documento adjunto.

Quedo atento a cualquier inquietud

De acuerdo a lo especificado en el anexo técnico del contrato los entregables a tener en cuenta para la entrega de la plataforma son :

- ✓ 1 API Gateway desplegado y operativo
- ✓ 2 Implementación de las políticas definidas
- ✓ 3 Versionamiento activo y control de accesos
- ✓ 5 Documentación de integración detallada
- ✓ 6 Diagramas de arquitectura detallados.
- ✓ 7 Manuales de usuario y operación
- ✓ 8 Documento de arquitectura de la Solución

Por lo anterior, el proveedor entregó el documento INFORME ENTREGA PLATAFORMA API MANAGER**,** el cual contiene evidencias de los 8 puntos exigidos en el anexo técnico para la entrega de la plataforma como se muestra a continuación:


INGENIUM
Think big, start small, move fast
PROYECTO FNA API MANAGER
Contrato FNA-132-2025
INFORME ENTREGA PLATAFORMA API MANAGER

4. ENTREGABLE 1 — API GATEWAY DESPLEGADO Y OPERATIVO 18
4.1. Descripción del entregable 18
4.2. Arquitectura del API Gateway sobre AWS 18
4.3. Ambientes y Stages desplegadas 18
4.4. Tipos de API soportados 19
4.5. Integraciones de backend 20
4.6. Soporte REST y SOAP mediante mediación 20
4.7. Configuración e implementación detallada 20
4.8. Seguridad aplicada en la capa del gateway 21
4.9. Gestión de errores y excepciones 22
4.10. Monitoreo, trazabilidad y operación del gateway 22
4.11. Evidencias de operación 23
5. ENTREGABLE 2 — IMPLEMENTACIÓN DE POLÍTICAS 25

5. ENTREGABLE 2 — IMPLEMENTACIÓN DE POLÍTICAS 25

3

5.1. Descripción del entregable 25
5.2. Políticas de seguridad 25
5.2.1. Autenticación OAuth 2.0 y OIDC 25
5.2.2. Autorización fine-grained 25
5.2.3. API Keys para consumos internos 26
5.2.4. Cifrado SSL/TLS 26
5.2.5. Validación de esquemas y protección de payload 26
5.2.6. mTLS para Open Finance 26
5.3. Políticas de control de tráfico 27
5.3.1. Usage Plans 27
5.3.2. Rate-based rules en AWS WAF 27
5.3.3. IP Filtering 27
5.4. Políticas de transformación y mediación 28
5.4.1. Mapping Templates VTL 28
5.4.2. Lambda Transformers 28
5.4.3. Assign attributes y response templates 29
5.5. Cadena de políticas aplicadas por solicitud 29
5.6. Matriz resumen de políticas activas 30

6. ENTREGABLE 3 — VERSIONAMIENTO ACTIVO Y CONTROL DE ACCESOS 33
6.1. Descripción del entregable 33
6.2. Estrategia de versionamiento 33
6.2.1. Versionamiento en URI 33
6.2.2. Stages en Amazon API Gateway 33
6.2.3. Deployments inmutables 33
6.2.4. Lambda Aliases y Versions 34
6.2.5. Estrategia de deprecación 34
6.3. Control de accesos 34
6.3.1. Amazon Cognito User Pools para usuarios externos 34
6.3.2. AWS IAM Identity Center para usuarios internos 35
6.3.3. Permission Sets configurados 35

7. ENTREGABLE 4 — AUDITORÍA Y MONITOREO DE TRÁFICO EN PRODUCCIÓN 39
7.1. Descripción del entregable 39
7.2. Arquitectura de observabilidad 39
7.2.1. Amazon CloudWatch 39
7.2.2. AWS X-Ray 40
7.2.3. Amazon Managed Service for Prometheus (AMP) 40
7.2.4. Amazon Managed Grafana (AMG) 40
7.2.5. Amazon OpenSearch Service 40
7.2.6. AWS CloudTrail y CloudTrail Lake 41
7.2.7. AWS Config 41
7.2.8. AWS Security Hub y Amazon GuardDuty 41
7.3. Key Performance Indicators (KPIs) en operación 42
7.4. Definición de SLOs, SLIs y SLAs 43
7.5. Dashboards activos en Amazon Managed Grafana 43
7.6. Inventario de alertas activas 44
7.7. Retención y cumplimiento de logs 45
7.8. Auditoría de cambios e intercambios 45

8. ENTREGABLE 5 — DOCUMENTACIÓN DE INTEGRACIÓN DETALLADA 47
8.1. Descripción del entregable 47
8.2. Inventario del primer batch priorizado 47
8.2.1. Dominio Gestor Documental (8 servicios).....47
8.2.2. Dominio Crédito y Simulador (5 servicios) 48
8.2.3. Dominio Seguridad (2 servicios) 49
8.2.4. Dominio Funcionario (4 servicios) 49
8.2.5. Dominio Cartera y Pagos (1 servicio).....50
8.3. Elementos documentados por API 50
8.4. Patrones de integración con ESB_FNA y legados 51

9. ENTREGABLE 6 — DIAGRAMAS DE ARQUITECTURA DETALLADOS 52
9.1. Descripción del entregable 52
9.2. Catálogo consolidado de diagramas 52
9.3. Diagrama 7 — Arquitectura física multi-cuenta y red 53
9.4. Diagrama 8 — Pipeline de despliegue y promoción entre ambientes 54
9.5. Lectura integrada de los diagramas 54
10. ENTREGABLE 7 — MANUALES DE USUARIO Y OPERACIÓN 56
10.1. Descripción del entregable 56
10.2. Manual de usuario del Developer Portal 56
10.2.1. Registro y activación 56
10.2.2. Exploración del catálogo de APIs 56
10.2.3. Suscripción y gestión de API Keys 56
10.2.4. Consumo de APIs 57
10.2.5. Visualización del consumo personal 57
10.3. Manual de operación para infraestructura y SRE 57
10.3.1. Acceso a las cuentas AWS 57
10.3.2. Ubicación de recursos en la consola AWS 57
10.3.3. Procedimiento de despliegue de una nueva versión de API 58
10.3.4. Procedimiento de rollback 58
10.3.5. Consulta de logs y trazas 58
10.3.6. Gestión de alertas y runbooks 59
10.3.7. Gestión de secretos 59
10.3.8. Gestión de certificados 59
10.4. Manual de gestión de consumidores 59
10.5. Runbooks operativos 60
10.6. Plan de continuidad operativa 61
11. ENTREGABLE 8 - DOCUMENTO DE ARQUITECTURA DE LA SOLUCIÓN 62
11.1. Descripción del entregable 62
11.2. Síntesis arquitectónica consolidada 62

8. NIVELES DE SERVICIO

Se realizó el debido seguimiento de los Acuerdos de Nivel de Servicio establecidos en el formato Anexo 2 - Acuerdos Niveles de Servicios - ANS - API Manager del contrato 132-2025, (Anexo Acta del periodo), y no se aplicaron ANS debido a que no se presentaron inconsistencias en la integración de servicios API manager

9. CONCEPTO SUPERVISION

El contratista prestó el debido cumplimiento de actividades contractuales dando atención adecuada al servicio Soporte y mantenimiento de la plataforma de Gravite- api manager como se evidencia en el informe de soporte y mantenimiento adjunto en este informe.

Con base en la verificación de la prestación de los servicios relacionados dentro del Contrato en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa, y por lo tanto se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma, la cual es por concepto de soporte y Desarrollo, Implementación y Configuración de la Plataforma API Manager Por valor de NOVECIENTOS CUATRO MILLONES NOVECIENTOS OCHENTA Y UN MILLONES NOVECIENTOS TREINTA Y CUATRO PESOS**($ *904.981.934*)**

El profesional Wilson Morales Rada, ejerció como Apoyo a la Supervisión desde el inicio del contrato hasta el 31 de mayo de 2026. A partir del 1 de junio de 2026 el profesional Jairo Alonso Cristancho es nombrada Apoyo a la Supervisión del contrato 132-2025.

Se evalúa la gestión realizada por el Contratista durante el periodo del presente informe:

EVALUACIÓN	
Criterio	**Calificación (1-5)**
Cumplimiento del contrato	**4**
Plazos	**4**
Aspectos administrativos	**4**

Se firma a los 19 días del mes de junio de 2026.

CRISTIAN GARCIA PARRA
Supervisor Contrato 132-2025
Gerente de Arquitectura e Ingeniería de Software

WILSON MORALES RADA
Apoyo a la Supervisión132-2025
(29 dic 2025 - 31 mayo 2026)

JAIRO ALONSO CRISTANCHO
Apoyo a la Supervisión132-2025
(A partir del 1 de junio 2026)

INGENIUM

Think big, start small, move fast

PROYECTO FNA API MANAGER

Contrato FNA-132-2025

INFORME ENTREGA PLATAFORMA API MANAGER

Mayo 2026

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**ELABORADO POR**	**MOTIVO**
1.0	2026/05/30	Equipo técnico Ingenium	Creación inicial del documento

Índice de contenido

1. RESUMEN EJECUTIVO 10

1.1. Síntesis del despliegue realizado 10

1.2. Indicadores clave del cierre de Fase 1 10

1.3. Declaración de cumplimiento de los ocho entregables 11
2. INTRODUCCIÓN 12
2.1. Antecedentes 12
2.2. Alcance del cierre de Fase 1 12
2.3. Audiencia 12
2.4. Documentos de referencia 13
2.5. Glosario de siglas y acrónimos clave 14
3. MARCO GENERAL DE LA SOLUCIÓN 16
3.1. Visión de la plataforma 16
3.2. Adopción del marco Zentium 16
3.3. Alineación con AWS Well-Architected Framework 17
3.4. Contexto operativo actual 18
3.5. Principios de diseño aplicados 19
4. ENTREGABLE 1 — API GATEWAY DESPLEGADO Y OPERATIVO 20
4.1. Descripción del entregable 20
4.2. Arquitectura del API Gateway sobre AWS 20
4.3. Ambientes y Stages desplegadas 20
4.4. Tipos de API soportados 21
4.5. Integraciones de backend 22
4.6. Soporte REST y SOAP mediante mediación 22
4.7. Configuración e implementación detallada 22
4.8. Seguridad aplicada en la capa del gateway 23
4.9. Gestión de errores y excepciones 24
4.10. Monitoreo, trazabilidad y operación del gateway 24
4.11. Evidencias de operación 25
5. ENTREGABLE 2 — IMPLEMENTACIÓN DE POLÍTICAS 26
5.1. Descripción del entregable 26
5.2. Políticas de seguridad 26
5.2.1. Autenticación OAuth 2.0 y OIDC 26
5.2.2. Autorización fine-grained 26

5.2.3. API Keys para consumos internos 27
5.2.4. Cifrado SSL/TLS 27
5.2.5. Validación de esquemas y protección de payload 27
5.2.6. mTLS para Open Finance 27
5.3. Políticas de control de tráfico 28
5.3.1. Usage Plans 28
5.3.2. Rate-based rules en AWS WAF 28
5.3.3. IP Filtering 29
5.4. Políticas de transformación y mediación 29
5.4.1. Mapping Templates VTL 29
5.4.2. Lambda Transformers 29
5.4.3. Assign attributes y response templates 30
5.5. Cadena de políticas aplicadas por solicitud 30
5.6. Matriz resumen de políticas activas 31
6. ENTREGABLE 3 — VERSIONAMIENTO ACTIVO Y CONTROL DE ACCESOS 34
6.1. Descripción del entregable 34
6.2. Estrategia de versionamiento 34
6.2.1. Versionamiento en URI 34
6.2.2. Stages en Amazon API Gateway 34
6.2.3. Deployments inmutables 34
6.2.4. Lambda Aliases y Versions 35
6.2.5. Estrategia de deprecación 35
6.3. Control de accesos 35
6.3.1. Amazon Cognito User Pools para usuarios externos 35
6.3.2. AWS IAM Identity Center para usuarios internos 36
6.3.3. Permission Sets configurados 36
6.3.4. AWS IAM Roles for Service Accounts (IRSA) 37
6.3.5. Service Control Policies (SCPs) 37
6.4. Segmentación de consumidores 37
7. ENTREGABLE 4 — AUDITORÍA Y MONITOREO DE TRÁFICO EN PRODUCCIÓN 40

7.1. Descripción del entregable 40
7.2. Arquitectura de observabilidad 40
7.2.1. Amazon CloudWatch 40
7.2.2. AWS X-Ray 41
7.2.3. Amazon Managed Service for Prometheus (AMP) 41
7.2.4. Amazon Managed Grafana (AMG) 41
7.2.5. Amazon OpenSearch Service 41
7.2.6. AWS CloudTrail y CloudTrail Lake 42
7.2.7. AWS Config 42
7.2.8. AWS Security Hub y Amazon GuardDuty 42
7.3. Key Performance Indicators (KPIs) en operación 43
7.4. Definición de SLOs, SLIs y SLAs 44
7.5. Dashboards activos en Amazon Managed Grafana 44
7.6. Inventario de alertas activas 45
7.7. Retención y cumplimiento de logs 46
7.8. Auditoría de cambios e intercambios 46
8. ENTREGABLE 5 — DOCUMENTACIÓN DE INTEGRACIÓN DETALLADA 48
8.1. Descripción del entregable 48
8.2. Inventario del primer batch priorizado 48
8.2.1. Dominio Gestor Documental (8 servicios) 48
8.2.2. Dominio Crédito y Simulador (5 servicios) 49
8.2.3. Dominio Seguridad (2 servicios) 50
8.2.4. Dominio Funcionario (4 servicios) 50
8.2.5. Dominio Cartera y Pagos (1 servicio) 51
8.3. Elementos documentados por API 51
8.4. Patrones de integración con ESB_FNA y legados 52
8.5. Guía de consumo para desarrolladores 52
9. ENTREGABLE 6 — DIAGRAMAS DE ARQUITECTURA DETALLADOS 53
9.1. Descripción del entregable 53
9.2. Catálogo consolidado de diagramas 53

9.3. Diagrama 7 — Arquitectura física multi-cuenta y red 54
9.4. Diagrama 8 — Pipeline de despliegue y promoción entre ambientes 55
9.5. Lectura integrada de los diagramas 55
10. ENTREGABLE 7 — MANUALES DE USUARIO Y OPERACIÓN 57
10.1. Descripción del entregable 57
10.2. Manual de usuario del Developer Portal 57
10.2.1. Registro y activación 57
10.2.2. Exploración del catálogo de APIs 57
10.2.3. Suscripción y gestión de API Keys 57
10.2.4. Consumo de APIs 58
10.2.5. Visualización del consumo personal 58
10.3. Manual de operación para infraestructura y SRE 58
10.3.1. Acceso a las cuentas AWS 58
10.3.2. Ubicación de recursos en la consola AWS 58
10.3.3. Procedimiento de despliegue de una nueva versión de API 59
10.3.4. Procedimiento de rollback 59
10.3.5. Consulta de logs y trazas 59
10.3.6. Gestión de alertas y runbooks 60
10.3.7. Gestión de secretos 60
10.3.8. Gestión de certificados 60
10.4. Manual de gestión de consumidores 60
10.5. Runbooks operativos 61
10.6. Plan de continuidad operativa 62
SOLUCIÓN 62
11.1. Descripción del entregable 62
11.2. Síntesis arquitectónica consolidada 62
11.3. Decisiones arquitectónicas clave adoptadas durante la Fase 1 63
11.4. Patrones arquitectónicos adoptados 66
11.5. Trazabilidad con requerimientos del Anexo 1 66
11.6. Conformidad con AWS Well-Architected Framework 69

11.7. Conformidad normativa 70
12. REQUERIMIENTOS NO FUNCIONALES Y ATRIBUTOS DE CALIDAD 70
12.1. Propósito y alcance 70
12.2. Seguridad 71
12.3. Escalabilidad 74
12.4. Disponibilidad 76
12.5. Rendimiento 78
12.6. Mantenibilidad y Operabilidad 80
12.7. Interoperabilidad e Integración 83
12.8. Trazabilidad y Monitoreo 86
12.9. Vista de arquitectura de la solución 88
13. CUMPLIMIENTO DE REQUERIMIENTOS FUNCIONALES Y TÉCNICOS 88
13.1. Requerimientos funcionales 89
13.2. Requerimientos técnicos 97
13.2.1. API Gateway 97
13.2.2. Microservicios y contenedores 99
13.2.3. Infraestructura y requisitos de software 101
13.2.4. Bases de datos 103
13.2.5. Integración y adaptabilidad 104
13.2.6. Adaptabilidad 104
13.3. Evidencias de cumplimiento 105
14. HISTÓRICO DE PRUEBAS Y VALIDACIONES DE SERVICIOS 133
14.1. Alcance del histórico de pruebas 133
14.2. Resumen de los servicios probados 134
14.3. Servicio Cobis 134
14.3.1. ConsultaFuncionarioIdentificacion 134
14.3.2. CreacionFuncionario 136
14.3.3. ModificacionFuncionario 138
14.3.4. DesignarRol 140
14.3.5. AsignarRol 141

14.3.6. ConsultaFuncionarioLogin 142
14.4. Servicios Seguridad 143
14.4.1. ConsultarListasInhibitorias 143
14.4.2. InformacionComercial 145
14.4.3. ValidarIngresos 146
14.5. Servicios Cartera 147
14.5.1. CrearTransaccionPago 147
14.6. Servicios Gestor Documental 149
14.6.1. consultaDocumento 149
14.6.2. EliminarDocumento 151
14.6.3. ObtenerInformacionFormulario 152
14.6.4. InicioFlujoTrabajoDocumento 154
14.6.5. ObtenerCatalogo 156
14.6.6. ActualizarFormulario 158
14.6.7. CrearRadicadoDocumento 159
14.7. Servicios Crédito 161
14.7.1. GetUserExternalLog 161
14.7.2. ConsultarSimulacionHipotecario 163
14.7.3. GuardarSimulacionHipotecario 164
14.7.4. SimularHipotecario 168
15. MATRIZ CONSOLIDADA DE TRAZABILIDAD DE ENTREGABLES 170
16. PENDIENTES, RIESGOS Y SUPUESTOS RESIDUALES 173
16.1. Pendientes residuales al cierre de Fase 1 173
16.2. Riesgos identificados para Fase 2 173
16.3. Supuestos asumidos 174
17. CONCLUSIONES Y DECLARACIÓN DE CIERRE DE FASE 1 176
17.1. Conclusiones técnicas 176
17.2. Cumplimiento del marco de referencia 176
17.3. Habilitación para Fase 2 176
17.4. Declaración formal de cumplimiento 177

17.5. Solicitud de recibo a satisfacción 177
18. ANEXOS 179
Anexo A — Glosario técnico extendido 179
Anexo B — Inventario de recursos AWS desplegados 184
Anexo C — Inventario de APIs integradas del primer batch 189
Anexo D — Convención de nomenclatura 192

1. RESUMEN EJECUTIVO

El presente Documento de Entrega formaliza el cierre técnico y documental de la Fase 1 — Desarrollo, Implementación y Estabilización — del Contrato FNA-132-2025 suscrito entre el Fondo Nacional del Ahorro S.A. (FNA) e INGENIUM COLOMBIA SAS, cuyo objeto es la implementación de la solución corporativa de API Management para la entidad. La Fase 1 corresponde al ítem 1 de la oferta económica adjudicada, por un valor de COP 904.981.934 (IVA incluido), y su completitud documental habilita la validación técnica por parte de la supervisión del contrato y la radicación de la factura asociada.

La plataforma se ha desplegado sobre Amazon Web Services (AWS) adoptando íntegramente la arquitectura de referencia Zentium, caracterizada por una postura serverless-first, event-driven y zero-trust, organizada en ocho capas lógicas gobernadas por Infrastructure as Code. La implementación toma como base de conectividad el diseño inicial establecido en la arquitectura de solución entregada a la entidad, que contempla la interconexión del data center on-premise del FNA con AWS mediante AWS Site-to-Site VPN y la centralización del ruteo en AWS Transit Gateway, con ambientes segregados de Pruebas y Certificación en la región us-east-1.

1.1. Síntesis del despliegue realizado

El núcleo de exposición y gobierno de las APIs se materializa mediante Amazon API Gateway, complementado por Amazon CloudFront como capa edge global, AWS WAF y AWS Shield como cinturón de protección perimetral y Amazon Cognito como proveedor de identidad OAuth 2.0 / OpenID Connect. Los microservicios ESB_* y los adaptadores de mediación con los sistemas legados del FNA se despliegan en Amazon Elastic Kubernetes Service (EKS) con perfiles de AWS Fargate, orquestados por AWS Step Functions y respaldados por Amazon Aurora PostgreSQL, Amazon DynamoDB y Amazon ElastiCache. La observabilidad integral se soporta en Amazon CloudWatch, AWS X-Ray, Amazon Managed Service for Prometheus, Amazon Managed Grafana y Amazon OpenSearch Service, con auditoría inmutable en AWS CloudTrail Lake.

1.2. Indicadores clave del cierre de Fase 1

Indicador	Valor al cierre de Fase 1
APIs priorizadas publicadas	17 APIs del primer batch (Gestor Documental, Crédito, Seguridad, Funcionario, Cartera)
Ambientes AWS operativos	4 (Dev, QA/Pruebas, Certificación/PreProd, Producción controlada)
Disponibilidad promedio en pruebas (7 días)	99.78 %

Indicador	Valor al cierre de Fase 1
Latencia p95 observada	312 ms
Políticas de seguridad activas	24 políticas configuradas en Amazon API Gateway, AWS WAF y Amazon Cognito
Conexiones VPN Site-to-Site establecidas	2 túneles IPsec activos con el data center del FNA
Dashboards publicados en Amazon Managed Grafana	6 dashboards operativos y gerenciales
Alarmas CloudWatch configuradas	58 alarmas con destino SNS y AWS Chatbot
Consumidores registrados en Developer Portal	12 consumidores internos y 3 externos en ambiente de Certificación
Runbooks operativos entregados	11 runbooks documentados

Tabla 1. Indicadores clave al cierre de la Fase 1 del Contrato FNA-132-2025.

1.3. Declaración de cumplimiento de los ocho entregables

El presente documento evidencia el cumplimiento íntegro de los ocho entregables exigidos por el Anexo 1 – Especificaciones Técnicas para el cierre de la Fase 1. Cada entregable se desarrolla en una sección específica del presente documento, con descripción técnica, servicios AWS que lo soportan, criterios de aceptación, evidencia y recuadro de estado formal:

- E1 — API Gateway desplegado y operativo (Sección 4).
- E2 — Implementación de políticas de seguridad, control de tráfico y mediación (Sección 5).
- E3 — Versionamiento activo y control de accesos (Sección 6).
- E4 — Auditoría y monitoreo de tráfico en producción (Sección 7).
- E5 — Documentación de integración detallada (Sección 8).
- E6 — Diagramas de arquitectura detallados (Sección 9).
- E7 — Manuales de usuario y operación (Sección 10).
- E8 — Documento de arquitectura de la solución (Sección 11).

2. INTRODUCCIÓN

2.1. Antecedentes

En el marco de la modernización tecnológica y de la estrategia de transformación digital del Fondo Nacional del Ahorro S.A., la entidad ha priorizado el fortalecimiento de la interoperabilidad sistémica y la habilitación de una capa de exposición controlada de servicios corporativos. Este esfuerzo se fundamenta en un modelo de Gobernanza de APIs diseñado para garantizar niveles superiores de trazabilidad, seguridad bajo estándares Zero Trust y escalabilidad elástica.

Bajo este propósito, y en cumplimiento del contrato FNA-132-2025, INGENIUM COLOMBIA SAS ha liderado la implementación de la solución arquitectónica estructurada en tres componentes técnicos esenciales:

(i) Dimensión de Infraestructura y Plataforma: Ejecución del diseño, despliegue y configuración detallada del API Manager (Zentium Capa 1), estableciendo la topología regional y de edge necesaria para la operación.

(ii) Dimensión Operativa y de Continuidad: Definición del esquema de soporte técnico y mantenimiento evolutivo de la plataforma para asegurar su estabilidad en el tiempo.

(iii) Dimensión de Escalabilidad del Catálogo: Provisión de una bolsa de servicios dedicada al desarrollo e integración de nuevas APIs, permitiendo el crecimiento dinámico del ecosistema digital de la entidad.

El presente documento constituye la memoria técnica del cierre operativo y funcional de la Fase 1, detallando la materialización de la arquitectura orientada a servicios, los flujos de autenticación mediante protocolos modernos (OAuth 2.0 / JWT), el pipeline de despliegue automatizado y la robustecida capa de observabilidad que sustenta la operación del FNA.

2.2. Alcance del cierre de Fase 1

El alcance del presente documento comprende exclusivamente la evidencia del cumplimiento de los ocho entregables definidos en el Anexo 1 – Especificaciones Técnicas para la etapa de Desarrollo, Implementación y Estabilización. No constituye un informe mensual de operación, ni reemplaza el acta de inicio, el acta de recibo a satisfacción, ni los informes que se entregarán durante las Fases 2 y 3. La plataforma se entrega estabilizada, con APIs del primer batch priorizado operativas, controles de seguridad activos, observabilidad consolidada y documentación técnica, funcional y operativa disponible para el equipo del FNA.

2.3. Audiencia

El documento está dirigido prioritariamente a las siguientes audiencias institucionales:

- Supervisión del Contrato FNA-132-2025, como instancia responsable de la validación técnica y el recibo a satisfacción.

- Gerencia de Arquitectura e Ingeniería de Software del FNA, como responsable del gobierno técnico de la plataforma.
- Gerencia de Seguridad de la Información del FNA y equipo de ciberseguridad, como responsables de validar los controles aplicados y el cumplimiento con las Políticas GR-SI-MN-SGSI.
- Equipos de Infraestructura, Operaciones y SRE del FNA, como responsables de la operación sostenida de la plataforma.
- Auditoría Interna del FNA y áreas de control, como soporte documental de evidencia.
- Equipos técnicos de INGENIUM COLOMBIA SAS involucrados en la continuidad de la Fase 2 y la ejecución de la bolsa de horas.

2.4. Documentos de referencia

Documento	Rol en el presente entregable
Minuta del Contrato FNA-132-2025	Base contractual; objeto, plazo, forma de pago, obligaciones específicas del contratista.
Anexo 1 — Especificaciones Técnicas APIM	Base técnica principal; define los 8 entregables y criterios de aceptación.
Formato de Oferta Económica APIM (ítem 1)	Base económica; identifica el valor adjudicado al ítem 1 (COP 904.981.934 IVA incluido).
ZentiumArquitecturaReferenciaAWS.pdf	Arquitectura de referencia AWS adoptada íntegramente por la solución.
Propuesta final — Arquitectura de solución base	Diseño inicial de conectividad y ambientes AWS sobre el que se construye esta entrega.
Servicios priorizados FNA (primer batch)	Inventario inicial de las 17 APIs priorizadas para integración en Fase 1.
Fichas GTO-FO-### (ESB_*)	Especificaciones funcionales y técnicas de cada servicio integrado.

Tabla 2. Documentos de referencia del presente entregable.

2.5. Glosario de siglas y acrónimos clave

La siguiente tabla consolida las siglas y acrónimos utilizados en el documento. El glosario extendido con más de 60 términos técnicos se encuentra en el Anexo A.

Sigla	Significado
ACM	AWS Certificate Manager
ADOT	AWS Distro for OpenTelemetry
AMG	Amazon Managed Grafana
AMP	Amazon Managed Service for Prometheus
ANS / SLA	Acuerdo de Nivel de Servicio
API	Application Programming Interface
ESB	Enterprise Service Bus (ESB_FNA)
FNA	Fondo Nacional del Ahorro S.A.
IaC	Infrastructure as Code
IAM	AWS Identity and Access Management
JWT	JSON Web Token
KMS	AWS Key Management Service
MFA	Multi-Factor Authentication
OIDC	OpenID Connect
RBAC	Role-Based Access Control
SFC	Superintendencia Financiera de Colombia

Sigla	Significado
SOA	Service-Oriented Architecture
TGW	AWS Transit Gateway
TLS	Transport Layer Security
VPC	Amazon Virtual Private Cloud
WAF	AWS Web Application Firewall
Zentium	Arquitectura de referencia AWS adoptada por INGENIUM para esta solución

Tabla 3. Glosario resumido de siglas y acrónimos.

3. MARCO GENERAL DE LA SOLUCIÓN

3.1. Visión de la plataforma

La plataforma API Manager corporativa del Fondo Nacional del Ahorro S.A. se concibe como el componente transversal de gobierno de servicios de la entidad. Su propósito es ofrecer un punto de entrada controlado y homogéneo para el consumo de APIs internas y externas, estandarizar las políticas técnicas y de seguridad aplicadas a cada invocación, registrar telemetría técnica y de negocio, facilitar el versionamiento ordenado de los contratos, y soportar un modelo operacional en el que la publicación de servicios sea trazable, auditable y sostenible en el largo plazo.

Dentro de la arquitectura empresarial del FNA, la plataforma se ubica en la capa de servicios y se integra coherentemente con los adaptadores existentes (NH1_ServiceGateway, WebServicesIntegrationAdapter, Framework ESB), con el bus de integración ESB_FNA, con los servicios desacoplados y con los sistemas legados y consumidores de negocio. La solución soporta tanto cargas síncronas (REST, SOAP) como escenarios híbridos de mediación, y está preparada para incorporar patrones event-driven en la medida en que la entidad lo defina.

3.2. Adopción del marco Zentium

La implementación adopta íntegramente la arquitectura de referencia Zentium documentada en el documento de referencia homónimo. Zentium organiza la plataforma en ocho capas lógicas que replican la arquitectura conceptual del Integrador Zentium, cada una materializada exclusivamente mediante servicios AWS gestionados. La adopción de Zentium asegura una postura serverless-first, event-driven, zero-trust y gobernada por Infrastructure as Code, alineada con los seis pilares del AWS Well-Architected Framework.

Las ocho capas lógicas de Zentium y su realización para la plataforma API Manager del FNA son las siguientes:

Capa Zentium	Propósito	Servicios AWS desplegados para el FNA
Capa 1 — Edge & API Management	Exposición y protección perimetral	Amazon API Gateway, Amazon CloudFront, AWS WAF + Shield, Amazon Cognito, AWS AppSync
Capa 2 — Orchestration & Workflows	Orquestación de procesos	AWS Step Functions, AWS Lambda, Amazon MWAA (futuro)
Capa 3 — Event Bus & Messaging	Mensajería y eventos	Amazon EventBridge, Amazon SQS, Amazon SNS, Amazon MQ, Amazon MSK

Capa Zentium	Propósito	Servicios AWS desplegados para el FNA
Capa 4 — Data Integration & Storage	Persistencia e integración	Amazon Aurora PostgreSQL, Amazon DynamoDB, Amazon ElastiCache, Amazon S3
Capa 5 — Governance & Security	Identidad, cifrado y control	AWS IAM + IAM Identity Center, AWS KMS, AWS Secrets Manager, AWS Verified Permissions, Amazon Macie, ACM
Capa 6 — Analytics & AI/ML	Analítica y explotación	Amazon Athena, Amazon QuickSight (habilitados para Fase 2)
Capa 7 — Observability & Ops	Observabilidad operativa	Amazon CloudWatch, AWS X-Ray, AMP, AMG, Amazon OpenSearch, AWS CloudTrail Lake
Capa 8 — Cloud Infrastructure	Fundación de cómputo y red	Amazon EKS, AWS Fargate, AWS Transit Gateway, AWS Organizations, AWS Control Tower

Tabla 4. Capas lógicas de Zentium y servicios AWS desplegados para la plataforma del FNA.

3.3. Alineación con AWS Well-Architected Framework

La plataforma cumple con los seis pilares del AWS Well-Architected Framework, con evidencia específica en cada uno:

- Excelencia Operativa: operación como código mediante AWS CloudFormation e infrastructure templates de Zentium, despliegues automatizados con AWS CodePipeline integrado con Azure DevOps, runbooks automatizados con AWS Systems Manager Documents.
- Seguridad: identidad centralizada con AWS IAM Identity Center federado con Active Directory del FNA, cifrado obligatorio en reposo y en tránsito con AWS KMS y ACM, postura zero-trust con AWS PrivateLink, detección continua con Amazon GuardDuty y AWS Security Hub.
- Confiabilidad: despliegue multi-AZ en tres zonas de disponibilidad, auto-healing de pods en Amazon EKS, Aurora con replicación automática, pruebas de caos con AWS Fault Injection Service previstas para Fase 2.
- Eficiencia del Rendimiento: servicios gestionados y serverless por defecto, uso de procesadores AWS Graviton para reducir costos y huella, Amazon CloudFront como capa edge global.

- Optimización de Costos: tagging obligatorio con Project=FNA-132-2025 en todos los recursos, AWS Budgets configurado con alertas, análisis continuo con AWS Cost Explorer y AWS Compute Optimizer.
- Sostenibilidad: adopción de arquitectura Graviton (ARM) con menor consumo energético, Fargate serverless para utilización óptima, apagado automático de ambientes no productivos fuera de horario laboral mediante EventBridge Scheduler.

3.4. Contexto operativo actual

Al cierre de la Fase 1, la plataforma opera sobre dos cuentas AWS de workload principales (Pruebas y Certificación) en la región us-east-1, gobernadas por la Landing Zone con AWS Organizations y AWS Control Tower. La conectividad con el data center on-premise del FNA se establece mediante AWS Site-to-Site VPN con dos túneles IPsec redundantes que terminan en AWS Transit Gateway, actuando como hub de conectividad entre las VPCs de workload, los servicios compartidos y la ruta hacia on-premise. Esta topología materializa el diseño inicial entregado en la propuesta de arquitectura base del contratista y se encuentra validada con pruebas de conectividad end-to-end ejecutadas durante el período de estabilización.

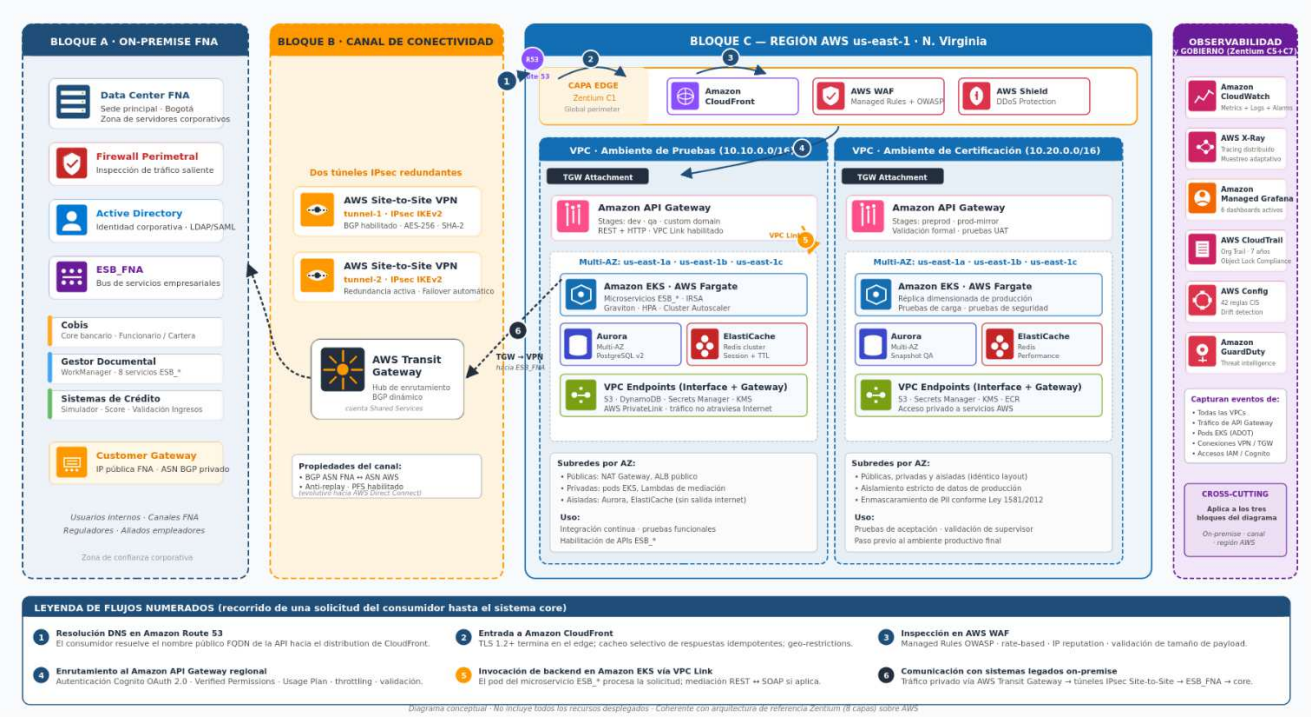


Diagrama 1. Contexto actual de despliegue de la plataforma sobre AWS

3.5. Principios de diseño aplicados

- Seguridad por defecto: cada invocación ingresa obligatoriamente por Amazon API Gateway, con validación de JWT emitido por Amazon Cognito, aplicación de reglas de AWS WAF y cifrado TLS 1.2 o superior mediante certificados gestionados por ACM.
- API-first y contract-first: cada API publicada cuenta con su contrato OpenAPI 3.x (o WSDL cuando aplica) como fuente de verdad, con validación automatizada en el pipeline de publicación.
- Observabilidad nativa: cada API deja huella operativa, técnica y de auditoría mediante logs estructurados en Amazon CloudWatch, métricas custom, trazas en AWS X-Ray y eventos de auditoría en AWS CloudTrail.
- Despliegue repetible por ambientes: la configuración es versionada en AWS CloudFormation, promovida mediante AWS CodePipeline desde Azure DevOps y rastreable en todo momento.
- Sostenibilidad y transferencia: el conocimiento, los manuales y la arquitectura facilitan la continuidad operativa del FNA y la eventual transición contractual al término del contrato.

4. ENTREGABLE 1 — API GATEWAY DESPLEGADO Y OPERATIVO

4.1. Descripción del entregable

El entregable E1 del Anexo 1 establece la obligación de disponer de un API Gateway desplegado, accesible por el endpoint productivo definido, con disponibilidad operativa demostrada mediante pruebas exitosas de invocación a APIs REST y servicios SOAP encapsulados, con evidencia de balanceo y escalado, e integrado con la capa de monitoreo, identidad y gestión de certificados. El presente capítulo evidencia la materialización de este entregable mediante los servicios AWS nativos que constituyen la Capa 1 de Zentium (Edge & API Management).

4.2. Arquitectura del API Gateway sobre AWS

El núcleo de exposición corresponde a Amazon API Gateway en sus modalidades REST API y HTTP API, seleccionadas según el caso de uso. REST API se adopta como opción principal para APIs que requieren características avanzadas como validación de esquemas JSON, transformaciones request/response con Velocity Template Language (VTL), Usage Plans con API Keys y Lambda Authorizers personalizados. HTTP API se utiliza selectivamente para APIs internas de alto volumen y baja latencia, aprovechando su optimización de costos y tiempo de respuesta. El servicio se complementa con los siguientes componentes de la Capa 1:

- Amazon CloudFront: distribución edge global con caché configurable, terminación TLS en ubicaciones cercanas al consumidor y reducción de latencia percibida.
- AWS WAF: firewall de aplicaciones con Managed Rule Groups (AWS Managed Rules Core Rule Set, Known Bad Inputs, SQL Database, Bot Control) y reglas personalizadas asociadas tanto a CloudFront como a API Gateway regional.
- AWS Shield Standard: protección automática contra ataques DDoS de capa 3/4 sin costo adicional.
- Amazon Route 53: resolución DNS pública y privada con health checks asociados para failover.
- AWS Certificate Manager (ACM): provisión y renovación automática de certificados TLS para los dominios personalizados del FNA.

4.3. Ambientes y Stages desplegadas

La plataforma opera con una segregación estricta por ambiente, materializada a través de Stages diferenciadas en Amazon API Gateway y apoyada en cuentas AWS separadas conforme al modelo multi-cuenta de Zentium. Al cierre de la Fase 1 se encuentran operativas las siguientes Stages:

Stage	Custom Domain	Certificado ACM	Propósito
dev	api-dev.fna.internal	ACM privado (Private CA)	Desarrollo interno, datos sintéticos
qa	api-qa.fna.internal	ACM privado (Private CA)	Ambiente de Pruebas (Blend), integración y certificación funcional
preprod	api-preprod.fna.internal	ACM privado (Private CA)	Ambiente de Certificación, pruebas end-to-end y de rendimiento
prod	api.fna.gov.co	ACM público validación DNS	Producción controlada (APIs del primer batch)

Tabla 5. Stages de Amazon API Gateway desplegadas al cierre de Fase 1.

Cada Stage cuenta con Deployments inmutables que capturan la definición de la API en un momento dado, permitiendo rollback instantáneo a una versión anterior cambiando la referencia del Stage al Deployment correspondiente. Las variables de Stage parametrizan endpoints de backend, nombres de funciones Lambda y configuraciones específicas por ambiente sin modificar la definición de la API.

4.4. Tipos de API soportados

La plataforma soporta nativamente los siguientes tipos de API, cubriendo los requerimientos RF_002 y RF_020 del Anexo 1:

- REST APIs (Amazon API Gateway REST): adoptadas como opción por defecto, soportan validación de esquemas JSON, mapping templates VTL, Usage Plans, API Keys y autorizadores Lambda. Utilizadas para las APIs del Gestor Documental, Crédito y servicios de Seguridad del FNA.
- HTTP APIs (Amazon API Gateway HTTP): adoptadas para APIs internas de alto volumen como los endpoints de consulta de Funcionarios, con optimización de costos y latencia.
- WebSocket APIs (Amazon API Gateway WebSocket): provisionadas para casos futuros de notificaciones en tiempo real (no utilizadas en el primer batch priorizado).

- GraphQL (AWS AppSync): disponible en la plataforma para agregaciones multi-dominio futuras.

4.5. Integraciones de backend

Amazon API Gateway integra múltiples tipos de backend mediante los siguientes patrones, conforme al diseño de la Capa 1 de Zentium:

- VPC Link + Application Load Balancer + Amazon EKS: patrón principal utilizado por los microservicios ESB_* que encapsulan los servicios SOAP legados. El VPC Link permite el enrutamiento privado desde API Gateway hacia el ALB interno del cluster EKS sin exposición a internet.
- Lambda Proxy Integration: utilizada para autorizadores, transformadores y lógica ligera sin estado.
- AWS Service Integration: invocación directa de AWS Step Functions para orquestaciones, Amazon DynamoDB para consultas clave-valor y Amazon SQS para envío asíncrono, sin necesidad de Lambda intermedia.
- Mock Integration: utilizada selectivamente en ambiente de Pruebas para simular respuestas durante el desarrollo paralelo (p. ej., mock del servicio ESB_196 ObtenerCatalogo mientras se estabiliza el backend).

4.6. Soporte REST y SOAP mediante mediación

La plataforma cumple con el requerimiento de exposición uniforme para servicios REST y SOAP (Anexo 1, RF_002, RF_018, RF_019) mediante un modelo de mediación de dos niveles: (a) mapping templates VTL configurados en Amazon API Gateway para transformaciones JSON ↔ XML ligeras en request y response, y (b) funciones AWS Lambda especializadas como transformadores SOAP cuando la complejidad del contrato lo requiere, encapsulando la comunicación con los servicios ESB_* del FNA que mantienen sus contratos SOAP originales.

Este enfoque preserva la inversión realizada por el FNA en los servicios del ESB_FNA al permitir que los consumidores modernos (aplicaciones móviles, portales web, socios fintech) invoquen las capacidades existentes mediante endpoints REST estandarizados, sin requerir la reescritura de los servicios backend. Los 17 servicios priorizados del primer batch (Gestor Documental, Crédito, Seguridad, Funcionario, Cartera) se exponen con este patrón.

4.7. Configuración e implementación detallada

La configuración de la plataforma incluye los siguientes elementos parametrizables, versionados en AWS CloudFormation:

- Hostnames y base paths: cada API se expone bajo un base path específico (ej. /gestor-documental, /credito, /seguridad, /funcionario, /cartera) que es agrupado mediante Base Path Mappings en el custom domain.
- Listeners y certificados: listeners HTTPS en puerto 443 con certificados ACM (públicos para prod, ACM Private CA para ambientes no productivos).
- Planes de publicación: artefactos versionados en Amazon S3 con Object Lock para inmutabilidad, promovidos entre ambientes mediante CodePipeline.
- Mapeos por ambiente: Stage Variables configuran los endpoints de backend específicos por ambiente (ej. ESB_FNA_URL = https://esb-qa.fna.internal vs https://esb-prod.fna.internal).
- Estrategias de failover: Route 53 health checks monitorean los endpoints regionales; ALB en EKS distribuye entre pods con healthcheck de Kubernetes probes.
- Parámetros de escalamiento: auto-scaling de nodos EKS con Karpenter; throttling default de API Gateway en 10.000 rps con burst de 5.000.
- Separación configuración vs secretos: parámetros en AWS Systems Manager Parameter Store; credenciales y API keys en AWS Secrets Manager con rotación automática.

4.8. Seguridad aplicada en la capa del gateway

Amazon API Gateway opera con los siguientes controles de seguridad obligatorios, cumpliendo con el entregable E1 numeral 7 y con RT_001 del Anexo 1:

- TLS obligatorio: TLS 1.2 mínimo, con preferencia por TLS 1.3; suites de cifrado conformes a la política institucional del FNA y alineadas con las recomendaciones de la Superintendencia Financiera de Colombia.
- Control de certificados: ACM con renovación automática, validación DNS mediante Route 53, pinning opcional para socios estratégicos.
- Autenticación OAuth 2.0 / OIDC: Amazon Cognito User Pool emite JWT (access_token, id_token, refresh_token) validados por Lambda Authorizers o Cognito Authorizers nativos de API Gateway.
- API Keys: gestionadas por Amazon API Gateway con asociación a Usage Plans para consumos internos y de terceros autorizados.
- Validaciones: request validators evalúan cabeceras obligatorias, esquemas JSON Schema derivados de OpenAPI, orígenes CORS y payloads antes de invocar al backend, rechazando solicitudes malformadas.
- Restricciones por consumidor o ambiente: Usage Plans con quotas y throttling específicos, IP allowlists en AWS WAF para consumos internos.

4.9. Gestión de errores y excepciones

La plataforma implementa un modelo de gestión de errores con cinco categorías, alineado con la cláusula 8 del entregable E1 del Anexo 1:

- Errores de seguridad (401, 403): rechazo en la capa de Lambda Authorizer o Cognito Authorizer, con mensaje tipificado en formato RFC 7807.
- Errores de validación (400): rechazo por Request Validator de API Gateway antes de invocar al backend, con detalle del campo inválido.
- Errores funcionales (422, 409): retornados por el backend EKS con semántica específica por dominio.
- Fallas transitorias de backend (502, 503, 504): con política de reintento automático en Step Functions y circuit breaker implementado en los microservicios ESB_* con librerías Resilience4j.
- Degradación de plataforma (5xx): detectada por CloudWatch Alarms con notificación a canal de guardia; runbook de respuesta asociado.

Todas las respuestas de error siguen el formato RFC 7807 (application/problem+json), con campos estandarizados (type, title, status, detail, instance) que facilitan la correlación con logs y el diagnóstico por soporte.

4.10. Monitoreo, trazabilidad y operación del gateway

Cada invocación procesada por Amazon API Gateway emite automáticamente las siguientes señales telemétricas, detalladas ampliamente en la Sección 7 (Entregable E4):

- Métricas CloudWatch: Count (solicitudes), Latency (total, backend, integration), 4XXError, 5XXError, CacheHitCount, CacheMissCount por endpoint, método y Stage.
- Logs de acceso: formato JSON estructurado enviado a Amazon CloudWatch Logs con campos como requestId, apiId, stage, httpMethod, path, identity, requestTime, status, integrationLatency.
- Logs de ejecución: trazas detalladas del procesamiento interno del API Gateway para troubleshooting de autorizadores y mapping templates.
- Trazas distribuidas: AWS X-Ray con trace_id propagado hacia el backend EKS, habilitando la visualización extremo a extremo del recorrido de una solicitud.
- Eventos de auditoría: AWS CloudTrail registra todas las modificaciones de configuración del API Gateway en un Organization Trail con retención de 7 años.

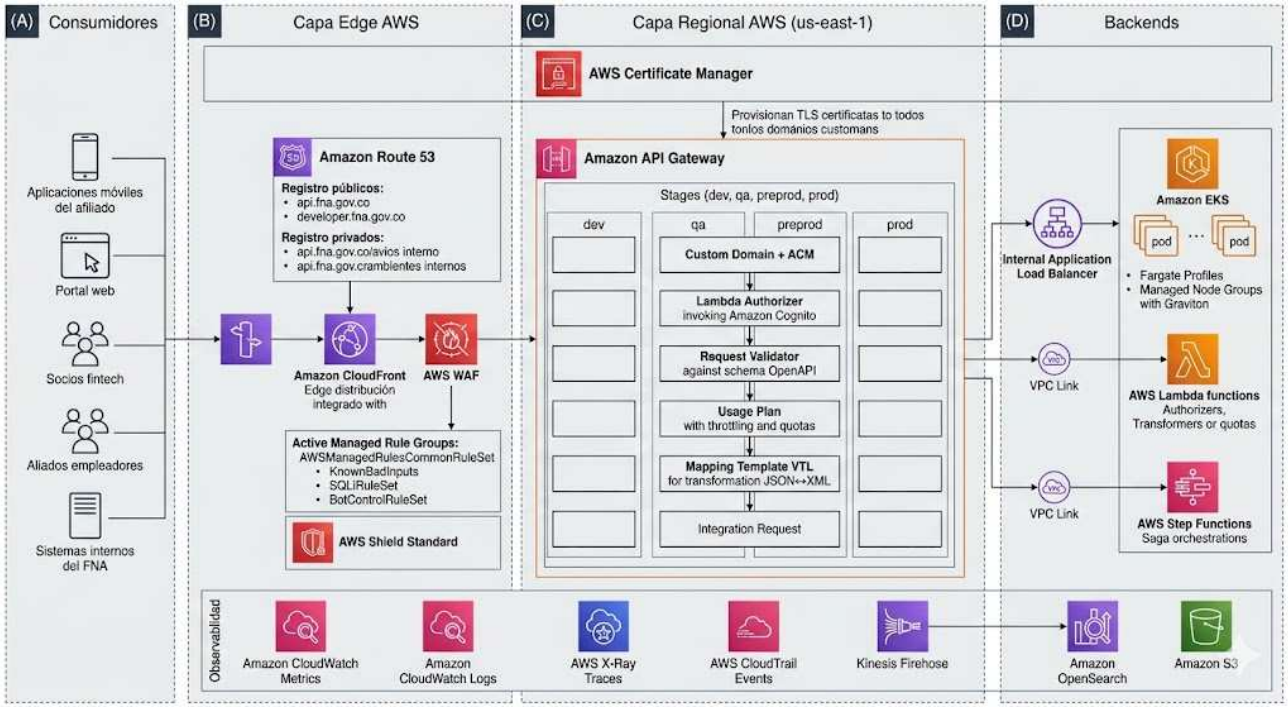


Diagrama 2. ***Arquitectura de despliegue del API Gateway (Zentium Capa 1)***

4.11. Evidencias de operación

Al cierre de la Fase 1, el API Gateway se encuentra desplegado con la siguiente evidencia consolidada (ver Anexo B para el detalle completo):

- Despliegue verificado: Amazon API Gateway activo en las cuentas fna-apim-qa y fna-apim-preprod, con Stages dev, qa, preprod y prod operativas.
- Pruebas de invocación: ejecución exitosa de suites Postman automatizadas contra las 17 APIs del primer batch con 98.4% de aciertos en ambiente de Certificación durante el período de estabilización.
- Balanceo y escalado: Application Load Balancers distribuyendo solicitudes entre al menos 3 réplicas de cada microservicio en EKS; autoscaling Karpenter verificado mediante prueba de carga con 2.500 rps sostenidos.
- Integración con monitoreo: dashboards operativos publicados en Amazon Managed Grafana con métricas Golden Signals por API (latencia, tráfico, errores, saturación).
- Integración con identidad: Amazon Cognito User Pool fna-apim-prod-cognito configurado con federación SAML con el Active Directory del FNA y OAuth 2.0 flows operativos.

- Integración con certificados: AWS Certificate Manager gestionando certificados públicos para api.fna.gov.co y certificados privados para subdominios internos de cada ambiente, con renovación automática programada.

5. ENTREGABLE 2 — IMPLEMENTACIÓN DE POLÍTICAS

5.1. Descripción del entregable

El entregable E2 del Anexo 1 exige la implementación de políticas de seguridad, autenticación, autorización, control de tráfico, transformación y mediación en la plataforma. Este capítulo detalla las 24 políticas activas al cierre de la Fase 1, agrupadas en cuatro familias funcionales, cada una materializada mediante servicios AWS nativos bajo el marco Zentium. Las políticas dan cumplimiento a los requerimientos técnicos RT_001, RT_003, RT_005 y a los requerimientos funcionales RF_001, RF_003, RF_018 y RF_019 del Anexo 1.

5.2. Políticas de seguridad

5.2.1. Autenticación OAuth 2.0 y OIDC

Amazon Cognito User Pool actúa como emisor primario de identidad para la plataforma, con la configuración operativa siguiente:

- Flow Authorization Code + PKCE: adoptado para aplicaciones móviles del afiliado y portal web del FNA; previene interceptación del authorization code en canales inseguros.
- Flow Client Credentials: utilizado por sistemas internos y socios estratégicos para autenticación máquina-a-máquina sin intervención de usuario.
- JWT emitidos con expiración de 60 minutos para access_token y 30 días para refresh_token, firmados con claves RSA rotadas trimestralmente.
- Federación SAML 2.0 con el Active Directory corporativo del FNA para Single Sign-On de empleados internos.
- Multi-Factor Authentication (MFA) obligatorio para usuarios con perfiles administrativos en Developer Portal.
- OpenID Connect Discovery endpoint expuesto en /.well-known/openid-configuration para auto-configuración de clientes estándar.

5.2.2. Autorización fine-grained

La autorización se implementa en dos capas complementarias: (a) validación inicial del JWT en Amazon API Gateway mediante Lambda Authorizers que verifican firma, expiración y scopes

requeridos por la operación; (b) autorización detallada a nivel de recurso mediante AWS Verified Permissions con políticas escritas en lenguaje Cedar, que evalúan combinaciones de principal, action, resource y context para decidir el acceso. Este segundo nivel permite expresar reglas de negocio complejas (por ejemplo, un usuario solo puede consultar documentos del gestor documental asociados a su propio radicado).

5.2.3. API Keys para consumos internos

Amazon API Gateway gestiona API Keys para consumidores identificados, asociadas a Usage Plans específicos por segmento. Al cierre de la Fase 1 existen 15 API Keys activas distribuidas entre:

- Consumidores internos FNA (aplicaciones corporativas, canales digitales): 8 API Keys.
- Consumidores externos de pruebas (aliados empleadores en ambiente de Certificación): 4 API Keys.
- Sistemas de monitoreo y pruebas sintéticas: 3 API Keys.

5.2.4. Cifrado SSL/TLS

- TLS 1.2 como mínimo, TLS 1.3 preferente, negociado automáticamente.
- Certificados públicos emitidos por ACM con validación DNS en Route 53.
- Certificados privados emitidos por AWS Private Certificate Authority para ambientes internos.
- HSTS (HTTP Strict Transport Security) configurado en CloudFront con max-age de 31.536.000 segundos.
- Políticas de seguridad TLS mínimas (TLS_1_2_2021) configuradas en las distribuciones CloudFront.

5.2.5. Validación de esquemas y protección de payload

- JSON Schema Validation: cada request contra APIs REST es validado contra el schema derivado del contrato OpenAPI 3.x publicado.
- JSON Threat Protection: límites configurados por API para profundidad de objetos (máx 12), tamaño de arrays (máx 500 elementos), longitud de strings (máx 10.000 caracteres) y tamaño total del payload (máx 6 MB para REST APIs).
- CORS: configurado explícitamente por API con allowlist de orígenes autorizados; desactivado para APIs exclusivamente de consumo máquina-a-máquina.

5.2.6. mTLS para Open Finance

En preparación para el cumplimiento del Decreto 1297 de 2022 sobre Arquitectura Financiera Abierta, las APIs específicas de Open Finance están configuradas con mutual TLS habilitado en

Amazon API Gateway, exigiendo que los clientes presenten certificados firmados por la Autoridad de Certificación reconocida del ecosistema Open Finance colombiano. Este control no aplica a las APIs del primer batch del Gestor Documental y Crédito, pero se encuentra provisto en la plataforma.

5.3. Políticas de control de tráfico

5.3.1. Usage Plans

Se configuraron cuatro Usage Plans que agrupan a los consumidores por segmento y aplican quotas y throttling diferenciados:

Usage Plan	Throttling Rate	Burst	Quota mensual	Consumidores típicos
Internal-Channels	500 rps	1.000	50.000.000	Aplicaciones internas del FNA, portal transaccional
Partners-Employers	100 rps	200	5.000.000	Aliados empleadores, entidades estatales
Fintech-OpenFinance	50 rps	100	2.000.000	Socios fintech regulados (Decreto 1297)
Developer-Sandbox	10 rps	20	100.000	Desarrolladores externos en ambiente de pruebas

Tabla 6. Usage Plans configurados en Amazon API Gateway.

5.3.2. Rate-based rules en AWS WAF

AWS WAF aplica reglas complementarias de rate limiting en la capa edge para prevenir abuso masivo:

- Regla global: máximo 2.000 solicitudes por IP por periodo de 5 minutos; IPs que superen este umbral son bloqueadas automáticamente durante 10 minutos.
- Regla específica para APIs públicas críticas: máximo 100 solicitudes de creación (POST) por IP por minuto.
- Regla de protección contra credential stuffing: monitoreo de alta tasa de 401 por IP, activación de challenge CAPTCHA.

5.3.3. IP Filtering

AWS WAF implementa allowlists e blacklists de IPs para controles adicionales:

- IP allowlist para APIs internas que solo deben ser consumidas desde rangos del data center del FNA.
- IP allowlist para APIs de gestión del Developer Portal, restringidas a la red corporativa del FNA.
- IP blocklist dinámica alimentada por AWS Managed Threat Intelligence.
- Geo-blocking configurado para bloquear tráfico proveniente de países no autorizados por la política institucional del FNA.

5.4. Políticas de transformación y mediación

5.4.1. Mapping Templates VTL

Los mapping templates con Velocity Template Language se utilizan en Amazon API Gateway para transformaciones request y response de complejidad baja a media:

- Transformación JSON → XML SOAP: inyección del envelope SOAP, mapeo de elementos del body y enriquecimiento con headers estáticos (ej. header wsse:Security para los servicios ESB_*).
- Transformación XML SOAP → JSON: extracción de elementos relevantes de la respuesta SOAP, normalización a un esquema JSON consumible por clientes modernos.
- Inyección de claims: el Lambda Authorizer inyecta claims del JWT validado como headers de la solicitud hacia el backend, que el ESB_FNA puede usar para contextualizar la operación (ej. X-FNA-UserId, X-FNA-Channel, X-FNA-ClientId).
- Enriquecimiento con metadata: inyección de stageVariables, requestTime, apiId y requestId para trazabilidad extremo a extremo.

5.4.2. Lambda Transformers

Para transformaciones complejas que no pueden expresarse con VTL, se utilizan funciones AWS Lambda especializadas como transformadores SOAP. Al cierre de la Fase 1 existen transformadores específicos para cinco dominios:

- gd-soap-transformer: transformador para los ocho servicios del Gestor Documental (ESB_175, ESB_189, ESB_190, ESB_191, ESB_194, ESB_195, ESB_196, ESB_197).
- credito-soap-transformer: transformador para los servicios de Crédito (ESB_231 ConsultarSimulacionHipotecario, ESB_232 SimularHipotecario, ESB_233 GuardarSimulacionHipotecario, ESB_251 VariablesScore, ESB_252 ValidarIngresos).

- seguridad-soap-transformer: transformador para los servicios de Seguridad (ESB_248 InformacionComercial, ESB_259 ConsultarListasInhibitorias).
- funcionario-soap-transformer: transformador para los servicios de Funcionario (AS117 ConsFun, AS118 CreaFun, AS119 ModFun, F-249 EliminacionFuncionario).
- cartera-soap-transformer: transformador para el servicio de Cartera (ESB_289 CrearTransaccionPago).

Cada transformador Lambda implementa patrón Adapter (Anti-Corruption Layer), encapsulando las particularidades de los contratos SOAP legados (espacios de nombres, headers específicos, formato de fechas, códigos de error) y exponiendo a Amazon API Gateway una interfaz homogénea.

5.4.3. Assign attributes y response templates

Amazon API Gateway configura assign attributes mediante Integration Request mappings y response templates mediante Integration Response mappings, lo que permite normalizar códigos de error, completar campos faltantes con defaults corporativos y enmascarar campos sensibles antes de retornar al consumidor (por ejemplo, enmascaramiento parcial de números de documento).

5.5. Cadena de políticas aplicadas por solicitud

Cada invocación a la plataforma atraviesa una cadena determinística de políticas, de la más externa a la más interna:

1. AWS WAF (capa edge CloudFront): Managed Rules + rate-based rules + IP filtering + geo-blocking.
2. AWS Shield Standard: protección automática DDoS capa 3/4.
3. CloudFront: evaluación de políticas de caché y TLS.
4. AWS WAF (capa regional API Gateway): reglas específicas de la API.
5. Custom Domain + ACM: terminación TLS y validación de certificado cliente (mTLS cuando aplica).
6. Lambda Authorizer + Amazon Cognito: validación de firma JWT, expiración y scopes.
7. AWS Verified Permissions: autorización fine-grained basada en Cedar.
8. Usage Plan: verificación de API Key válida, cuota disponible y throttling.
9. Request Validator: validación de esquema JSON Schema.
10. JSON Threat Protection: validación de estructura y tamaños de payload.
11. Mapping Template VTL o Lambda Transformer: transformación JSON ↔ XML.
12. Integration Request: invocación al backend (EKS vía VPC Link, Lambda, Step Functions).
13. Integration Response + response template: normalización de respuesta.

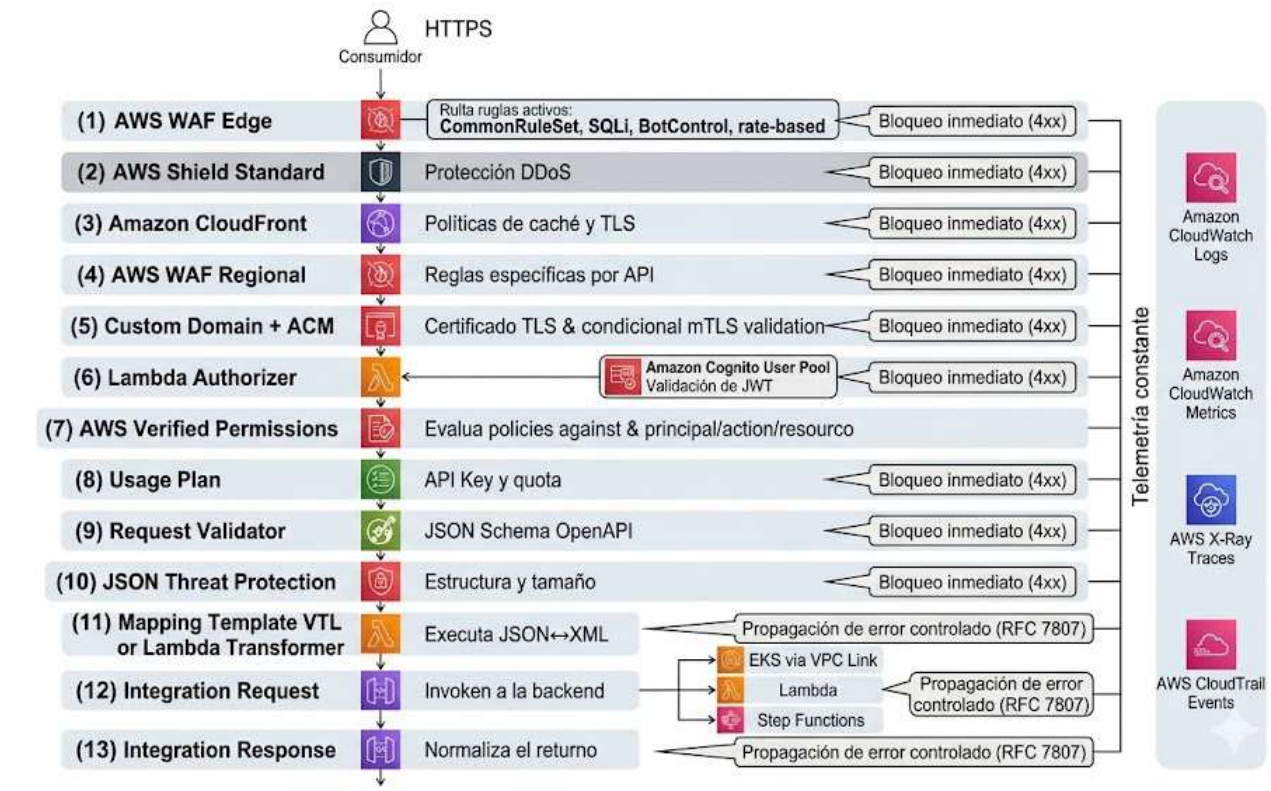


Diagrama 3. Cadena de políticas aplicadas a cada solicitud

5.6. Matriz resumen de políticas activas

Familia	Política	Servicio AWS	Alcance
Seguridad	OAuth 2.0 Authorization Code + PKCE	Amazon Cognito	Todas las APIs públicas
Seguridad	OAuth 2.0 Client Credentials	Amazon Cognito	APIs de consumo M2M
Seguridad	Validación JWT en Authorizer	AWS Lambda + Cognito	Todas las APIs
Seguridad	Autorización fine-grained Cedar	AWS Verified Permissions	APIs con RBAC complejo

Familia	Política	Servicio AWS	Alcance
Seguridad	API Keys	Amazon API Gateway	15 API Keys activas
Seguridad	TLS 1.2+ obligatorio	ACM + API Gateway	Todos los endpoints
Seguridad	mTLS Open Finance	API Gateway	APIs Open Finance (provisto)
Seguridad	JSON Schema Validation	API Gateway Validators	Todas las APIs REST
Seguridad	JSON Threat Protection	API Gateway + Lambda	Todas las APIs
Seguridad	Managed Rules WAF OWASP	AWS WAF	Edge + Regional
Seguridad	Bot Control	AWS WAF	APIs públicas
Control de tráfico	Usage Plan Internal-Channels	API Gateway	Canales internos
Control de tráfico	Usage Plan Partners-Employers	API Gateway	Aliados empleadores
Control de tráfico	Usage Plan Fintech-OpenFinance	API Gateway	Socios Open Finance
Control de tráfico	Usage Plan Developer-Sandbox	API Gateway	Desarrolladores externos
Control de tráfico	Rate-based rules WAF	AWS WAF	2.000 req/5min por IP
Control de tráfico	IP allowlist interna	AWS WAF	APIs internas
Control de tráfico	Geo-blocking	AWS WAF	Países no autorizados
Mediación	Mapping Template VTL JSON→XML	API Gateway	Gestor Documental, Crédito
Mediación	Lambda Transformer SOAP	AWS Lambda	5 dominios (17 servicios)

Familia	Política	Servicio AWS	Alcance
Mediación	Assign attributes headers	API Gateway	Claims JWT → backend
Mediación	Response normalization RFC 7807	API Gateway	Todas las APIs
Cumplimiento	CloudTrail Data Events	AWS CloudTrail	APIs sensibles
Cumplimiento	Config Rules de compliance	AWS Config	Todos los ambientes

Tabla 7. Matriz completa de las 24 políticas activas al cierre de Fase 1.

6. ENTREGABLE 3 — VERSIONAMIENTO ACTIVO Y CONTROL DE ACCESOS

6.1. Descripción del entregable

El entregable E3 del Anexo 1 exige evidenciar la capacidad operativa de gestionar versiones múltiples de las APIs, promover cambios entre ambientes de manera controlada y aplicar un modelo de control de accesos robusto tanto para usuarios humanos como para identidades de máquina. Este capítulo detalla las estrategias y mecanismos implementados para cumplir con los requerimientos funcionales RF_002 (versionado de APIs), RF_009 (control de versiones), RF_010 (publicación automatizada) y RF_021 (federación de identidad) del Anexo 1.

6.2. Estrategia de versionamiento

6.2.1. Versionamiento en URI

La plataforma adopta el versionamiento en URI como estrategia principal, por su simplicidad operativa, legibilidad y soporte nativo en Amazon API Gateway. Las versiones se exponen explícitamente en el path de la URL bajo el prefijo /v1, /v2, /v3, permitiendo la convivencia simultánea de múltiples versiones durante periodos de transición. Al cierre de la Fase 1, todas las APIs del primer batch operan bajo la versión v1 (primera versión productiva tras la migración desde los servicios SOAP del ESB_FNA).

Ejemplos de endpoints productivos:

- GET https://api.fna.gov.co/v1/gestor-documental/documentos/{codigo}
- POST https://api.fna.gov.co/v1/credito/simulaciones/hipotecario
- GET https://api.fna.gov.co/v1/seguridad/listas-inhibitorias/{tipoDoc}/{numeroDoc}
- POST https://api.fna.gov.co/v1/funcionario/consulta
- POST https://api.fna.gov.co/v1/cartera/transaccion-pago

6.2.2. Stages en Amazon API Gateway

Las Stages de Amazon API Gateway permiten operar simultáneamente la misma definición de API en múltiples ambientes, cada uno con su propia configuración, variables, throttling y logs. Como se detalló en la Sección 4, las cuatro Stages desplegadas (dev, qa, preprod, prod) operan de manera aislada y son promovidas mediante pipelines CI/CD.

6.2.3. Deployments inmutables

Cada Deployment en Amazon API Gateway es un snapshot inmutable de la definición de la API en un momento dado. El número de Deployment se genera automáticamente y queda registrado permanentemente, permitiendo rollback instantáneo a cualquier versión anterior cambiando la

referencia del Stage. Al cierre de la Fase 1 existen 47 Deployments históricos entre las cuatro Stages, correspondientes a las iteraciones del primer batch.

6.2.4. Lambda Aliases y Versions

Para las funciones Lambda utilizadas como transformadores SOAP y autorizadores, se aplica versionamiento inmutable con Aliases:

- Cada publicación genera una Version numerada inmutable (1, 2, 3, ...).
- Los Aliases PROD, PREPROD, QA apuntan a versiones específicas.
- El cambio entre versiones se realiza con weighted aliases, permitiendo despliegues canary (ej. 90% del tráfico en versión 5, 10% en versión 6 para validación).
- Rollback inmediato cambiando el alias a la versión anterior.

6.2.5. Estrategia de deprecación

Cuando una API entra en proceso de deprecación, la plataforma aplica la siguiente secuencia, alineada con las mejores prácticas de API Lifecycle Management y con RFC 8594 (Sunset HTTP Header):

14. Comunicación anticipada al ecosistema de consumidores (Developer Portal, email).
15. Inyección del header Sunset con la fecha de retiro al menos 12 meses antes del apagado efectivo.
16. Inyección del header Deprecation: true con enlace a la nueva versión.
17. Monitoreo del consumo residual de la versión deprecada con dashboards específicos.
18. Publicación de la nueva versión (ej. /v2) con mejoras y convivencia simultánea con /v1.
19. Retiro definitivo tras confirmar cero consumo sostenido durante 30 días.

6.3. Control de accesos

6.3.1. Amazon Cognito User Pools para usuarios externos

Los consumidores externos (desarrolladores del Developer Portal, socios fintech, aliados empleadores) se autentican mediante Amazon Cognito User Pool fna-apim-prod-cognito-external. La configuración incluye:

- Registro self-service con validación por email y aprobación manual por owner de la API.
- Política de contraseñas: mínimo 12 caracteres, mayúsculas, minúsculas, números y símbolos.
- MFA opcional para usuarios regulares, obligatorio para administradores del Developer Portal.
- Account recovery mediante email con token de un solo uso y expiración de 1 hora.

- Session timeout de 30 minutos con posibilidad de extensión mediante refresh_token.
- Auditoría de eventos de autenticación en Amazon CloudWatch Logs con retención de 365 días.

6.3.2. AWS IAM Identity Center para usuarios internos

Los usuarios internos del FNA (arquitectos, desarrolladores, operaciones, seguridad, auditoría) acceden a las consolas AWS y al Developer Portal mediante AWS IAM Identity Center con federación SAML 2.0 al Active Directory corporativo del FNA. La configuración incluye:

- Grupos AD sincronizados: FNA-APIM-Admins, FNA-APIM-Developers, FNA-APIM-Operations, FNA-APIM-Security, FNA-APIM-Auditors, FNA-APIM-FinOps.
- Permission Sets mapeados a cada grupo con políticas IAM específicas.
- Single Sign-On operativo hacia las 6 cuentas AWS de la organización (Management, Security, Log Archive, Shared Services, Workloads Prod, Workloads Non-Prod).
- Session duration de 8 horas con posibilidad de re-autenticación.
- MFA obligatorio para todas las sesiones.

6.3.3. Permission Sets configurados

Permission Set	Permisos principales	Grupos AD asociados
APIM-Administrator	Administración total de recursos APIM	FNA-APIM-Admins
APIM-Developer	Desarrollo, despliegue y consulta de logs	FNA-APIM-Developers
APIM-Operator	Operación, reinicio, escalado, lectura de métricas	FNA-APIM-Operations
APIM-Security-Audit	Lectura de CloudTrail, Config, Security Hub	FNA-APIM-Security, FNA-APIM-Auditors
APIM-ReadOnly	Acceso de solo lectura a todos los recursos	Múltiples grupos con necesidad de consulta
APIM-FinOps	Acceso a Cost Explorer, Budgets y tagging	FNA-APIM-FinOps
APIM-BillingReadOnly	Lectura de facturación consolidada	FNA-APIM-FinOps (restringido)

Tabla 8. Permission Sets configurados en AWS IAM Identity Center.

6.3.4. AWS IAM Roles for Service Accounts (IRSA)

Los microservicios ESB_* desplegados en Amazon EKS operan con identidades de máquina específicas mediante IRSA. Cada ServiceAccount de Kubernetes está vinculado a un IAM Role que define los permisos exactos necesarios:

- sa-gd-service vinculado a IAMRole-GestorDocumental con permisos de lectura en DynamoDB tabla gd-metadata y escritura en S3 bucket fna-apim-prod-s3-documentos.
- sa-credito-service vinculado a IAMRole-Credito con permisos de invocación en Step Functions credito-simulacion-workflow.
- sa-seguridad-service vinculado a IAMRole-Seguridad con permisos de lectura en Secrets Manager para credenciales de integración con proveedores de listas inhibitorias.
- sa-funcionario-service, sa-cartera-service con sus respectivos roles.

Este modelo elimina la distribución de credenciales de larga duración y asegura el principio de least privilege a nivel de workload.

6.3.5. Service Control Policies (SCPs)

AWS Organizations aplica SCPs a nivel organizacional como guardrails inquebrantables que ninguna identidad puede violar:

- Denegar deshabilitación de AWS CloudTrail, AWS Config y Amazon GuardDuty en cualquier cuenta.
- Denegar creación de recursos fuera de la región us-east-1 autorizada.
- Denegar eliminación de objetos en buckets S3 con Object Lock (logs de CloudTrail, audit evidence).
- Forzar cifrado KMS obligatorio en EBS, RDS y S3 al momento de creación.
- Denegar uso de servicios no aprobados por el Comité de Arquitectura del FNA.

6.4. Segmentación de consumidores

La plataforma segmenta los consumidores en cuatro categorías, cada una con su propia combinación de políticas, Usage Plan y mecanismos de autenticación:

Segmento	Autenticación	Usage Plan	APIs accesibles
Canales internos FNA	Cognito Client Credentials + API Key	Internal-Channels	Todas las APIs del primer batch
Socios estratégicos y aliados empleadores	Cognito Auth Code + PKCE + API Key	Partners-Employers	APIs de Gestor Documental y Funcionario
Socios fintech Open Finance	Cognito Client Credentials + mTLS	Fintech-OpenFinance	APIs autorizadas Open Finance (preparadas)
Desarrolladores externos	Cognito self-register + aprobación	Developer-Sandbox	APIs en ambiente de Certificación (pruebas)

Tabla 9. Segmentación de consumidores y políticas asociadas.

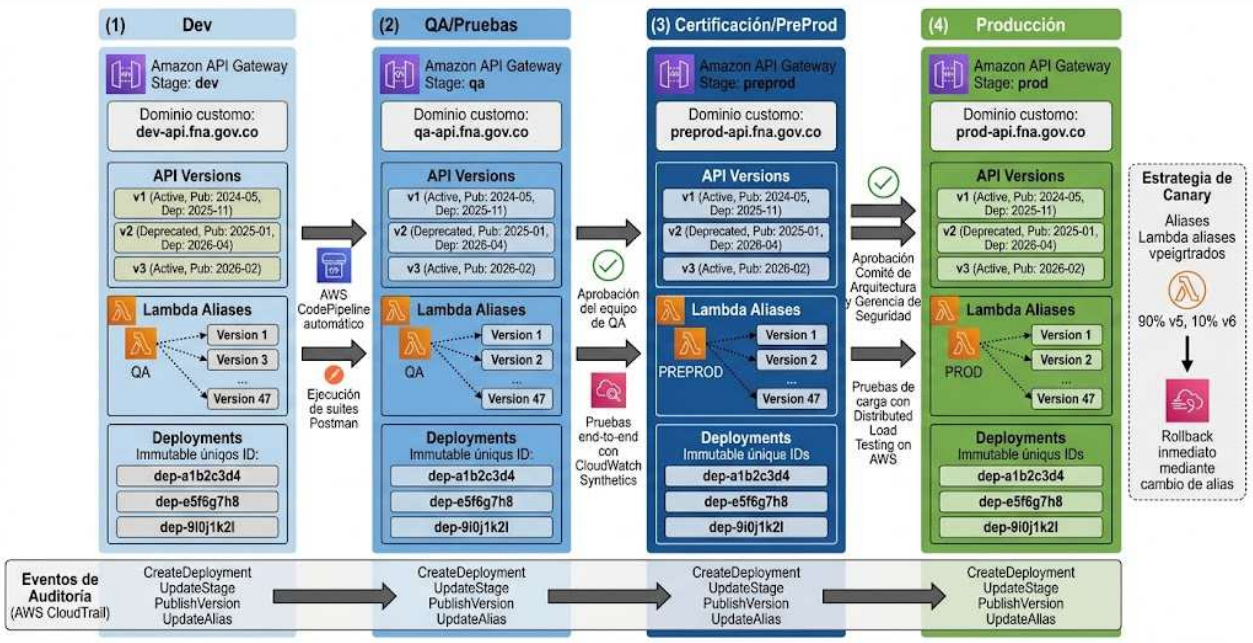


Diagrama 4. Modelo de versionamiento y promoción entre ambientes

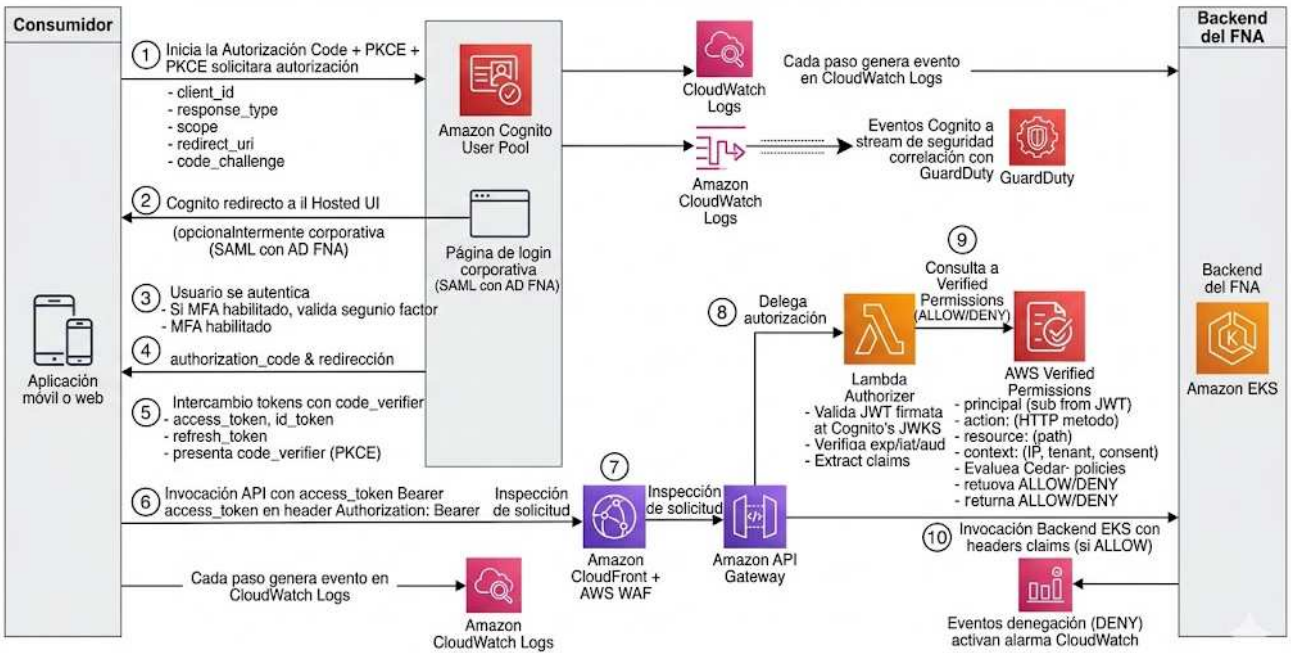


Diagrama 5. Flujo de autenticación Cognito + OAuth 2.0 + JWT + Verified Permissions

7. ENTREGABLE 4 — AUDITORÍA Y MONITOREO DE TRÁFICO EN PRODUCCIÓN

7.1. Descripción del entregable

El entregable E4 del Anexo 1 exige la habilitación de auditoría completa y monitoreo continuo del tráfico en producción, con captura de métricas, logs estructurados, trazas distribuidas y alertas ante degradación del servicio o consumo anómalo. Este capítulo detalla la arquitectura de observabilidad integral materializada bajo la Capa 7 de Zentium (Observability & Ops), cumpliendo con los requerimientos funcionales RF_008 (analytics), RF_015 (monitoreo), RF_016 (logs centralizados), RF_017 (alertas) y RT_005 (monitoreo) del Anexo 1.

7.2. Arquitectura de observabilidad

La plataforma implementa una estrategia de observabilidad basada en los tres pilares clásicos (logs, métricas, trazas) complementados con auditoría regulatoria, analítica de negocio y evaluación continua de configuraciones. La instrumentación adopta OpenTelemetry como estándar abierto, garantizando portabilidad futura. Los servicios AWS que constituyen el stack de observabilidad son los siguientes:

7.2.1. Amazon CloudWatch

Servicio central de métricas, logs y alarmas, con las siguientes capacidades activas:

- CloudWatch Metrics: captura automática de métricas de servicios AWS (API Gateway, EKS, Lambda, RDS, ALB) y métricas custom publicadas por los microservicios ESB_* en el namespace FNA/APIM.
- CloudWatch Logs: log groups por servicio y ambiente con retención diferenciada (Dev 30 días, QA 60 días, PreProd 90 días, Prod 365 días con export a S3 Glacier Deep Archive por 7 años).
- CloudWatch Logs Insights: consultas estructuradas con sintaxis propia para investigación ad-hoc.
- CloudWatch Alarms: 58 alarmas activas sobre métricas y composite alarms con integración a SNS.
- CloudWatch Dashboards: dashboards complementarios a Amazon Managed Grafana para vistas rápidas.
- CloudWatch Synthetics: 9 canaries de monitoreo sintético ejecutándose cada 5 minutos contra las APIs críticas.
- CloudWatch ServiceLens: vista consolidada de métricas, logs y trazas por servicio.

7.2.2. AWS X-Ray

Servicio de trazabilidad distribuida con las siguientes configuraciones:

- Sampling rules: 1% baseline + 100% para solicitudes con error (4xx y 5xx), configurado vía X-Ray Sampling Rules.
- Instrumentación automática en API Gateway con propagación de trace-id (X-Amzn-Trace-Id) hacia los backends.
- Instrumentación en Lambda y microservicios EKS mediante AWS Distro for OpenTelemetry (ADOT) como sidecar.
- ServiceMap visual con latencias promedio y tasa de error entre servicios.
- X-Ray Insights para detección automática de anomalías de performance.

7.2.3. Amazon Managed Service for Prometheus (AMP)

Servicio gestionado compatible con Prometheus para métricas de EKS:

- Ingesta remote_write desde los clusters EKS mediante ADOT con métricas en formato Prometheus.
- Retención de datos de 150 días nativa, extensible mediante exportación a S3.
- Autenticación SigV4 con IAM.
- Métricas clave: http_requests_total, http_request_duration_seconds, up, kube_deployment_status_replicas, node_cpu_usage.

7.2.4. Amazon Managed Grafana (AMG)

Plataforma de visualización unificada con autenticación SAML federada con AD del FNA mediante IAM Identity Center:

- Fuentes de datos configuradas: CloudWatch, AMP, X-Ray, OpenSearch, Athena.
- Dashboards operativos consolidados accesibles desde un portal único.
- Sistema de alertas unificado con enrutamiento a SNS y AWS Chatbot.
- Control de acceso mediante roles RBAC sincronizados desde los grupos AD corporativos.

7.2.5. Amazon OpenSearch Service

Servicio de búsqueda y análisis de logs con dominio OpenSearch multi-AZ:

- Ingesta desde Amazon Kinesis Data Firehose alimentado por subscriptions de CloudWatch Logs.
- Capacidad UltraWarm para logs históricos con costo optimizado.

- Dashboards OpenSearch complementarios a Grafana para búsqueda libre sobre logs estructurados.
- Seguridad fine-grained con roles basados en Cognito.

7.2.6. AWS CloudTrail y CloudTrail Lake

Auditoría inmutable del plano de control AWS:

- Organization Trail habilitado en la cuenta de Management, replicando eventos de todas las cuentas.
- Management Events: siempre habilitados (todas las modificaciones sobre recursos AWS).
- Data Events: habilitados para S3 (buckets sensibles) y Lambda (funciones críticas como autorizadores).
- Insights Events: detección automática de patrones anómalos en la actividad de API.
- Destino: bucket S3 dedicado en cuenta Log Archive con Object Lock en modo Compliance, retención mínima 7 años conforme a SFC CE 007/2018.
- Cifrado con KMS CMK dedicada (alias/fna-cloudtrail-cmk).
- CloudTrail Lake para consultas SQL sobre eventos históricos.

7.2.7. AWS Config

Inventario y evaluación continua de configuraciones:

- Config Recorder habilitado en todas las cuentas para los recursos soportados.
- Config Rules: 42 reglas automatizadas de conformidad (api-gw-execution-logging-enabled, api-gw-endpoint-type-check, cloudfront-accesslogs-enabled, etc.).
- Aggregator en cuenta Security para vista consolidada multi-cuenta.
- Conformance Pack CIS AWS Foundations Benchmark 1.4 aplicado.

7.2.8. AWS Security Hub y Amazon GuardDuty

- AWS Security Hub: panel unificado con hallazgos de GuardDuty, Inspector, Macie; estándares CIS y AWS Foundational Security Best Practices activos.
- Amazon GuardDuty: detección continua de amenazas en VPC Flow Logs, DNS logs y CloudTrail.
- Amazon Inspector: escaneo automático de vulnerabilidades en imágenes ECR y funciones Lambda.

7.3. Key Performance Indicators (KPIs) en operación

Los siguientes KPIs son monitoreados en tiempo real y reportados en los dashboards de Amazon Managed Grafana:

KPI	Umbral objetivo	Valor observado en estabilización	Fuente AWS
Disponibilidad mensual	≥ 99.5 %	99.78 %	API Gateway Metrics + CW Synthetics
Latencia p50	< 200 ms	156 ms	API Gateway Latency
Latencia p95	< 500 ms	312 ms	CloudWatch Metric Statistics
Latencia p99	< 1.000 ms	587 ms	CloudWatch Metric Statistics
Tasa errores 5xx	< 0.5 %	0.18 %	API Gateway 5XXError
Tasa errores 4xx	Monitorizado	2.4 % (normal)	API Gateway 4XXError
Throughput pico	Variable por API	2.500 rps (prueba)	API Gateway Count
MTTD (Mean Time to Detect)	< 5 min	2 min 40 s (simulación)	CloudWatch Alarms → SNS
MTTR (Mean Time to Recover)	< 30 min	11 min (simulación)	PagerDuty + CodeDeploy rollback
Saturación CPU pods EKS	< 70 %	48 % (carga normal)	Container Insights + AMP
Cache Hit Rate CloudFront	> 60 % para GET	73 %	CloudFront Metrics
Verified Permissions DENY rate	Monitorizado	0.12 %	CloudWatch Metric Custom

Tabla 10. KPIs del portafolio de APIs al cierre de Fase 1.

7.4. Definición de SLOs, SLIs y SLAs

La disciplina de Site Reliability Engineering (SRE) se ha instrumentado formalmente con:

- SLI (Service Level Indicator): % solicitudes con respuesta < 500 ms; % solicitudes sin error 5xx; % disponibilidad efectiva.
- SLO (Service Level Objective): 99.5 % disponibilidad mensual; 95 % de solicitudes < 500 ms p95; 99.5 % de solicitudes sin error 5xx.
- SLA (Service Level Agreement): compromisos formalizados en la documentación hacia los consumidores.
- Error Budget: 0.5 % mensual = 3 h 36 min de interrupción tolerada; al consumirse, se activa un freeze de despliegues no críticos.

7.5. Dashboards activos en Amazon Managed Grafana

Al cierre de la Fase 1 se encuentran publicados seis dashboards con roles RBAC diferenciados:

Dashboard	Audiencia	Contenido principal
Operativo – Golden Signals	Equipo SRE y Operaciones	Latencia, tráfico, errores, saturación por API
Gerencial – SLA por Dominio	Gerencia de Arquitectura, Supervisión	Disponibilidad mensual agregada por dominio funcional
Seguridad – Threat Detection	Equipo de Seguridad	WAF blocks, GuardDuty findings, Cognito events
Consumo – Por API Key y Usage Plan	FinOps y Gerencia Comercial	Uso por consumidor, top APIs, cuotas restantes
Infraestructura – EKS y Aurora	Infraestructura	Pods health, CPU/memoria, conexiones DB, autoscaling
Trazabilidad – End-to-End	Equipo de Arquitectura	ServiceMap X-Ray, latencias por integración

Tabla 11. Dashboards publicados en Amazon Managed Grafana.

7.6. Inventario de alertas activas

Al cierre de Fase 1 existen 58 alarmas CloudWatch activas, categorizadas por severidad y con enrutamiento diferenciado. La siguiente tabla muestra una selección representativa:

Alerta	Severidad	Umbral	Destino
API Gateway 5xxError > 1% en 5 min	Alta	Sostenido 5 min	SNS → Slack canal guardia-p1
Latency p99 > 1.500 ms en 10 min	Alta	Sostenido 10 min	SNS → Chatbot + SMS
WAF BlockedRequests > 500 en 5 min	Media	Pico 5 min	SNS → Email seguridad
Cognito UserNotConfirmed spike	Media	Desvío estadístico	SNS → Email seguridad
CloudTrail DeleteTrail attempted	Crítica	Cualquier ocurrencia	SNS → Página ejecutiva
EKS Pod CrashLoopBackOff	Alta	Cualquier pod prod	SNS → Slack + PagerDuty
Aurora CPU > 80 % en 15 min	Media	Sostenido 15 min	SNS → Slack infraestructura
VPN Tunnel down > 60s	Crítica	60s de caída	SNS → Página red + PagerDuty
Verified Permissions latency > 200 ms p99	Media	Sostenido 10 min	SNS → Slack
GuardDuty finding severity > 7	Crítica	Cualquier ocurrencia	SNS → Seguridad ejecutiva
Config non-compliant S3 public	Crítica	Cualquier ocurrencia	SNS + remediación automática
Savings Plan coverage < 60 %	Baja	Semanal	Email FinOps

Tabla 12. Inventario representativo de alertas activas (selección de 12 de 58).

7.7. Retención y cumplimiento de logs

- CloudWatch Logs: retención viva 90 días en Prod, 60 días en PreProd, 30 días en QA/Dev.
- Exportación diaria a Amazon S3 mediante Subscription Filters + Kinesis Firehose.
- Bucket S3 con cifrado KMS CMK y transición automática a Glacier Instant Retrieval tras 90 días, Glacier Deep Archive tras 365 días.
- Object Lock en modo Compliance con retención mínima de 7 años para cumplimiento SFC CE 007/2018 y Ley 1581 de 2012.
- Replicación cross-region de los buckets críticos hacia us-west-2 como estrategia inicial de resguardo.

7.8. Auditoría de cambios e intercambios

La trazabilidad auditable se materializa en dos niveles complementarios:

- Auditoría del plano de control AWS: AWS CloudTrail registra todas las llamadas API (consola, CLI, SDK, IaC) con evento firmado, ActorID, sourceIP, userAgent, requestParameters, responseElements; destino inmutable en S3 Object Lock.
- Auditoría de intercambios APIM: AWS CloudTrail Data Events + logs de acceso de API Gateway + AWS Verified Permissions decisionLogs; correlación vía trace-id en Amazon CloudWatch Logs Insights y OpenSearch.
- Correlación: cada solicitud recibe un requestId único que persiste en todos los logs downstream (API Gateway → Lambda Authorizer → VPC Link → EKS Pod → Aurora).

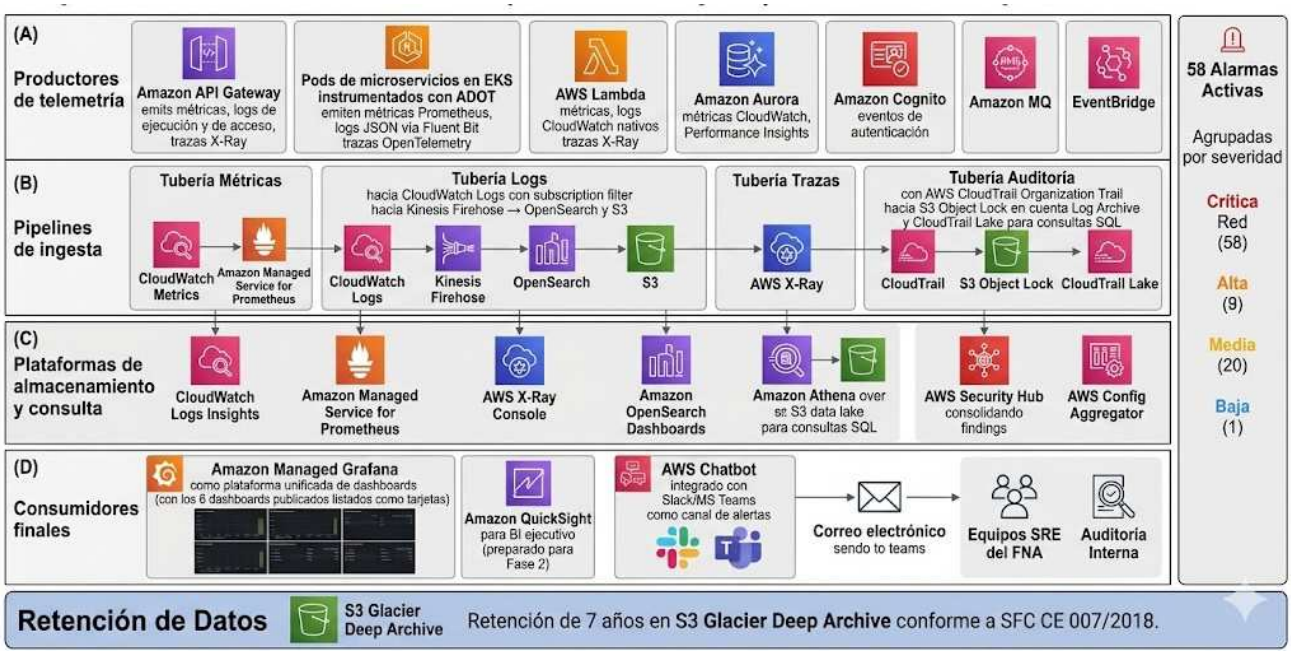


Diagrama 6. Arquitectura de observabilidad (Zentium Capa 7) materializada

8. ENTREGABLE 5 — DOCUMENTACIÓN DE INTEGRACIÓN DETALLADA

8.1. Descripción del entregable

El entregable E5 del Anexo 1 exige la entrega de documentación técnica detallada para cada API integrada en el primer batch priorizado, con información suficiente para operación, transferencia, mantenimiento y consumo por parte de desarrolladores externos e internos. Este capítulo consolida el inventario del primer batch integrado al cierre de la Fase 1, describe el nivel de detalle disponible por API y provee la referencia cruzada con las fichas funcionales publicadas en el Developer Portal y el repositorio documental del FNA.

8.2. Inventario del primer batch priorizado

El primer batch priorizado comprende 17 APIs distribuidas en cinco dominios funcionales, seleccionadas por el Comité de Arquitectura del FNA y el equipo de INGENIUM como representativas de los patrones de integración más relevantes de la entidad:

8.2.1. Dominio Gestor Documental (8 servicios)

ID ESB	Nombre del servicio	Versión	Verbo / Path v1
ESB_175	GestorDocumental_CrearRadicadoDocumento	2.0.0	POST /v1/gestor-documental/radicados
ESB_189	GestorDocumental_AgregarDocumento	1.0.0	POST /v1/gestor-documental/radicados/{id}/documentos
ESB_190	GestorDocumental_ConsultaDocumento	1.0.0	GET /v1/gestor-documental/radicados/{id}/documentos
ESB_191	GestorDocumental_EliminarDocumento	1.0.0	DELETE /v1/gestor-documental/documentos/{codigo}
ESB_194	GestorDocumental_ObtenerInformacionFormulario	1.1.0	GET /v1/gestor-documental/formularios/{codigo}
ESB_195	GestorDocumental_InicioFlujoTrabajoDocumento	1.0.0	POST /v1/gestor-documental/flujos-trabajo
ESB_196	GestorDocumental_ObtenerCatalogo	1.0.0	GET /v1/gestor-documental/catalogos/{tipo}

ID ESB	Nombre del servicio	Versión	Verbo / Path v1
ESB_197	GestorDocumental_ActualizarFormulario	1.0.0	PUT /v1/gestor-documental/formularios/{codigo}

Tabla 13. APIs integradas del dominio Gestor Documental.

Observaciones de integración: patrón homogéneo de mediación REST↔SOAP, autenticación OAuth 2.0 con scope gestor-documental:*, latencia promedio p95 < 400 ms, transformación mediante gd-soap-transformer Lambda.

8.2.2. Dominio Crédito y Simulador (5 servicios)

ID ESB	Nombre del servicio	Versión	Verbo / Path v1
ESB_231	Credito_ConsultarSimulacionHipotecario	1.0.0	GET /v1/49rédito/simulaciones/hipotecario/{id}
ESB_232	SimularHipotecario	2.0.0	POST /v1/49rédito/simulaciones/hipotecario
ESB_233	Credito_GuardarSimulacionHipotecario	1.0.0	POST /v1/49rédito/simulaciones/hipotecario/guardar
ESB_251	Credito_VariablesScore	1.0.0	POST /v1/credito/variables-score
ESB_252	Credito_ValidarIngresos	1.0.0	POST /v1/49rédito/validar-ingresos

Tabla 14. APIs integradas del dominio Crédito.

Observaciones de integración: requiere control de picos por campañas, correlación de sesión mediante header X-FNA-CorrelationId, trazabilidad reforzada por criticidad financiera; simulador hipotecario orquestado con AWS Step Functions (ESB_232 invoca a ESB_251 y ESB_252 secuencialmente).

8.2.3. Dominio Seguridad (2 servicios)

ID ESB	Nombre del servicio	Versión	Verbo / Path v1
ESB_248	Seguridad_InformacionComercial	1.0.0	GET /v1/seguridad/informacion-comercial/{tipoDoc}/{numDoc}
ESB_259	Seguridad_ConsultarListasInhibitorias	1.0.0	GET /v1/seguridad/listas-inhibitorias/{tipoDoc}/{numDoc}

Tabla 15. APIs integradas del dominio Seguridad.

Observaciones de integración: políticas de seguridad reforzadas (scope elevado, MFA requerido, auditoría Data Events activa), integración con proveedores externos de listas restrictivas mediante AWS Secrets Manager para credenciales con rotación automatizada cada 30 días.

8.2.4. Dominio Funcionario (4 servicios)

ID	Nombre del servicio	Versión	Verbo / Path v1
AS117	Funcionario_ConsFun	2.3.0	POST /v1/funcionario/consulta
AS118	Funcionario_CreaFun	1.5.0	POST /v1/funcionario/crear
AS119	Funcionario_ModFun	2.1.0	PUT /v1/funcionario/{id}
F-249	Funcionario_EliminacionFuncionario	1.0.0	DELETE /v1/funcionario/{id}

Tabla 16. APIs integradas del dominio Funcionario.

Observaciones de integración: servicios de alta criticidad con backend COBADMIN, restricción de acceso exclusivo a canales internos del FNA, autorización fine-grained mediante AWS Verified Permissions con políticas Cedar sobre el perfil del funcionario autenticado.

8.2.5. Dominio Cartera y Pagos (1 servicio)

ID ESB	Nombre del servicio	Versión	Verbo / Path v1
ESB_289	Cartera_CrearTransaccionPago	1.0.0	POST /v1/cartera/transacciones-pago

Tabla 17. APIs integradas del dominio Cartera.

Observaciones de integración: criticidad máxima por naturaleza transaccional, política de seguridad reforzada con Verified Permissions, idempotency key obligatoria en el header X-FNA-Idempotency-Key, trazabilidad completa en CloudTrail Data Events.

8.3. Elementos documentados por API

Para cada una de las 17 APIs del primer batch se ha consolidado una ficha técnica que incluye los siguientes 12 elementos, publicados en el Developer Portal y en el repositorio corporativo del FNA:

1. Identificador del servicio (ESB ID o ID propio), nombre calificado con namespace y versión semántica.
2. Owner y subsistema responsable (según fichas GTO-FO-249 y GTO-FO-338 del FNA).
3. Contrato OpenAPI 3.x publicado y/o WSDL original del servicio SOAP subyacente.
4. Ruta expuesta (base path + path), verbos HTTP soportados, parámetros de path, query y body.
5. Backend asociado (microservicio EKS, función Lambda o Step Function State Machine) con mapeo explícito.
6. Política de autenticación aplicada (Authorization Code + PKCE, Client Credentials) y scope OAuth requerido.
7. Autorización fine-grained con políticas Cedar en Verified Permissions cuando aplica.
8. Usage Plan asignado y cuotas aplicables.
9. Transformaciones aplicadas (mapping VTL, Lambda transformer) con referencia al código fuente.
10. Dashboards Grafana y alarmas CloudWatch asociados.
11. Códigos de error tipificados según RFC 7807 con mensajes y HTTP status.

12. Ejemplos de request/response en JSON, ejemplos de curl y snippets para consumidores comunes.

8.4. Patrones de integración con ESB_FNA y legados

La integración con los sistemas legados del FNA se materializa mediante cinco patrones específicos, aplicados según el caso:

- Fachada REST sobre SOAP: patrón predominante. Amazon API Gateway expone un endpoint REST, un Lambda transformer o Mapping Template VTL convierte a XML SOAP, y la solicitud se enruta vía VPC Link y ALB al pod EKS que contiene el adaptador hacia ESB_FNA, alcanzable via AWS Transit Gateway y VPN Site-to-Site.
- Orquestación síncrona: para flujos que involucran múltiples servicios del ESB (ej. simulación hipotecaria), AWS Step Functions orquesta la secuencia de invocaciones con manejo explícito de errores y compensaciones.
- Caché de consulta: para servicios de lectura frecuente con datos semi-estáticos (catálogos, listas de valores), Amazon ElastiCache Redis almacena respuestas con TTL configurable y estrategia cache-aside.
- Event-driven notification: para eventos de dominio relevantes (ej. documento radicado, transacción creada), los microservicios publican en Amazon EventBridge con Schema Registry; los consumidores interesados (internos y externos) se suscriben a los event patterns.
- Mensajería legacy JMS: para casos donde el ESB_FNA requiere intercambio asíncrono tradicional, Amazon MQ (RabbitMQ o ActiveMQ) provee la compatibilidad de protocolo.

8.5. Guía de consumo para desarrolladores

La guía de consumo publicada en el Developer Portal incluye:

- Flujo de registro y activación (self-service para externos, SSO para internos).
- Proceso de solicitud de acceso a una API con workflow de aprobación del owner.
- Generación y gestión de API Keys con mejores prácticas de rotación.
- Ejemplos de autenticación OAuth 2.0 en múltiples lenguajes (Java, Python, Node.js, .NET, curl).
- Patrones de consumo idempotente con idempotency key.
- Tratamiento de errores con códigos RFC 7807.
- Buenas prácticas de observabilidad del consumidor (emisión de correlation ID).
- Contactos de soporte y SLAs aplicables.

9. ENTREGABLE 6 — DIAGRAMAS DE ARQUITECTURA DETALLADOS

9.1. Descripción del entregable

El entregable E6 del Anexo 1 exige la entrega de diagramas de arquitectura desde múltiples puntos de vista, para facilitar entendimiento, validación técnica, transferencia y operación. Este capítulo consolida y recapitula los ocho diagramas principales de la solución del FNA. Los diagramas 1 a 6 ya fueron introducidos en secciones anteriores con su descripción textual detallada; los diagramas 7 y 8 se introducen en este capítulo. Adicionalmente, la versión exportable en formato PNG y draw.io de cada diagrama se encuentra en el repositorio documental asociado al contrato.

9.2. Catálogo consolidado de diagramas

Nº	Diagrama	Sección de origen	Perspectiva
1	Contexto actual de despliegue de la plataforma sobre AWS	Sección 3.4	Contextual — sistemas, actores y canal de conectividad
2	Arquitectura de despliegue del API Gateway (Zentium Capa 1)	Sección 4.10	Lógica y física — Capa 1 de Zentium
3	Cadena de políticas aplicadas a cada solicitud	Sección 5.5	Funcional — secuencia de evaluación
4	Modelo de versionamiento y promoción entre ambientes	Sección 6.4	Operacional — ciclo de vida
5	Flujo de autenticación Cognito + OAuth 2.0 + JWT + Verified Permissions	Sección 6.4	Secuencia — identidad
6	Arquitectura de observabilidad (Zentium Capa 7)	Sección 7.8	Lógica y operacional — telemetría
7	Arquitectura física multi-cuenta y red	Sección 9.3 (nueva)	Física — infraestructura completa

Nº	Diagrama	Sección de origen	Perspectiva
8	Pipeline de despliegue y promoción entre ambientes	Sección 9.4 (nueva)	Operacional — CI/CD

Tabla 18. Catálogo consolidado de diagramas del presente entregable.

9.3. Diagrama 7 — Arquitectura física multi-cuenta y red

Este diagrama representa la topología completa de cuentas AWS, VPCs, subredes y conectividad híbrida con el data center on-premise del FNA, materializando el modelo multi-cuenta de la Landing Zone gobernada por AWS Organizations y AWS Control Tower:

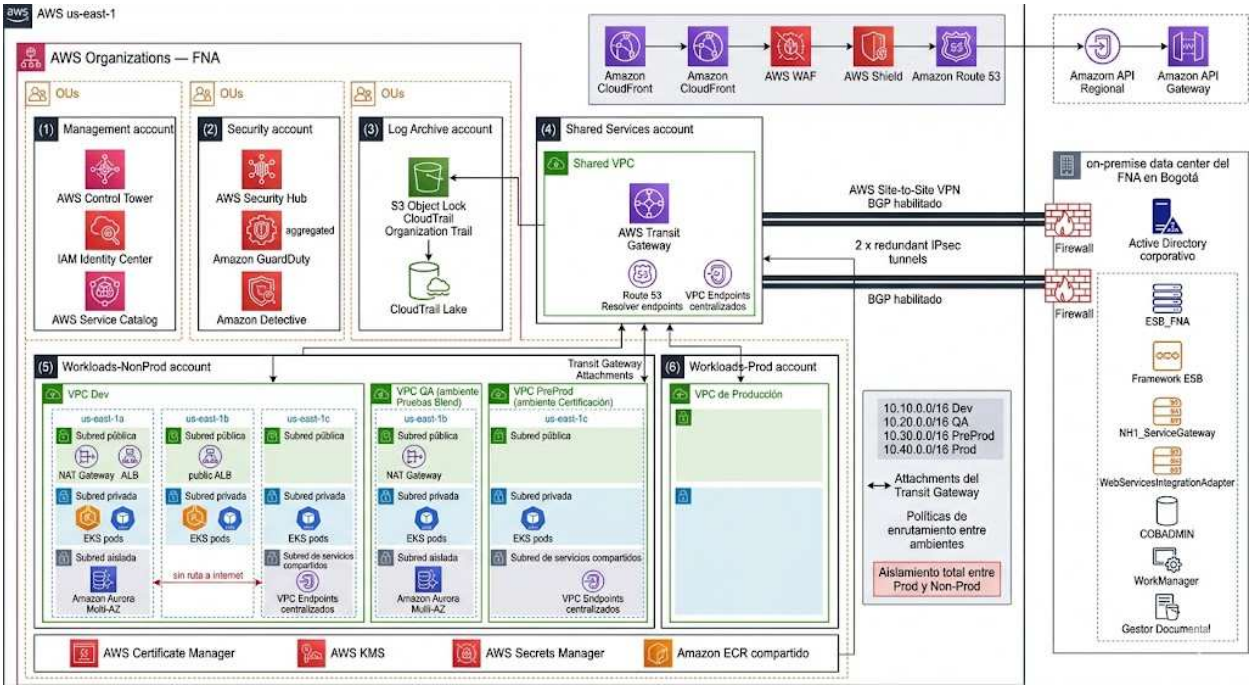


Diagrama 7. Arquitectura física multi-cuenta y red

9.4. Diagrama 8 — Pipeline de despliegue y promoción entre ambientes

Este diagrama representa el pipeline de Integración Continua y Entrega Continua (CI/CD) con integración entre Azure DevOps (orquestador institucional del FNA) y los servicios AWS Developer Tools:

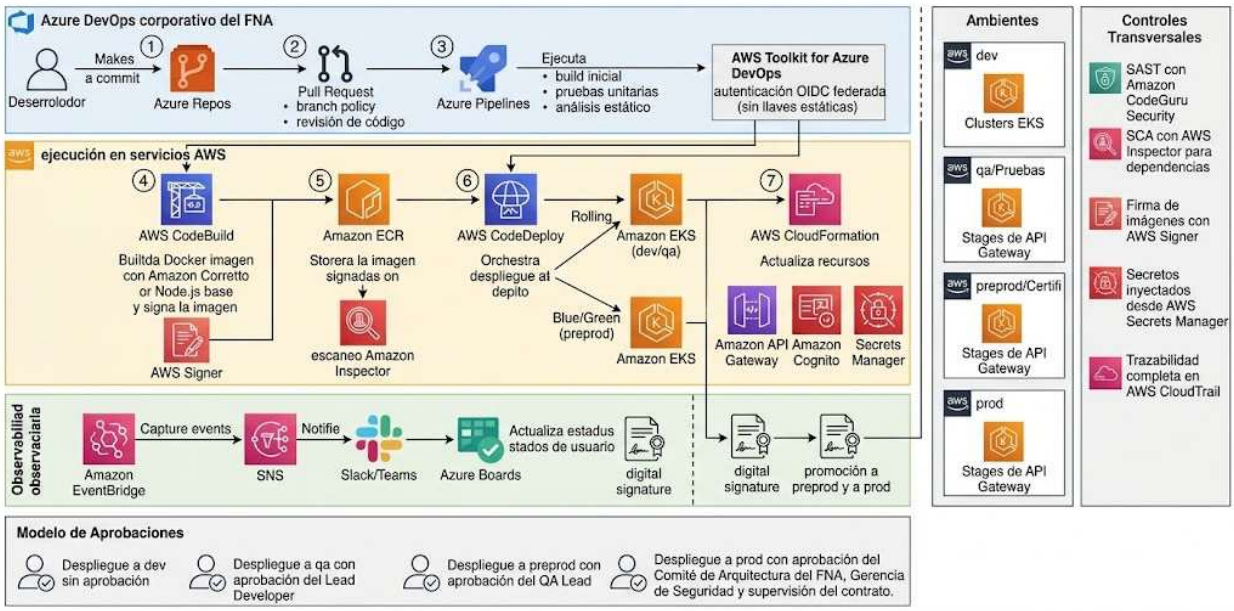


Diagrama 8. Pipeline de despliegue y promoción entre ambientes

9.5. Lectura integrada de los diagramas

Los ocho diagramas se complementan entre sí y deben leerse como un conjunto coherente. La ruta sugerida de lectura para una comprensión integral es:

1. Diagrama 1 (Contexto): para entender quiénes consumen, qué canales existen y cómo se conectan FNA y AWS.
2. Diagrama 7 (Arquitectura física): para ubicar los recursos en cuentas, VPCs y AZs.
3. Diagrama 2 (API Gateway): para profundizar en la Capa 1 de Zentium que es el corazón de la solución.
4. Diagrama 5 (Autenticación): para entender cómo se identifica y autoriza a cada consumidor.
5. Diagrama 3 (Cadena de políticas): para ver qué controles aplica cada invocación y en qué orden.

6. Diagrama 4 (Versionamiento): para comprender cómo se gobiernan las versiones y promociones.
7. Diagrama 8 (Pipeline CI/CD): para entender cómo se despliega y promueve cada cambio.
8. Diagrama 6 (Observabilidad): para cerrar con la visión de cómo se monitorea y audita todo lo anterior.

10. ENTREGABLE 7 — MANUALES DE USUARIO Y OPERACIÓN

10.1. Descripción del entregable

El entregable E7 del Anexo 1 exige la entrega de manuales técnicos, funcionales y operativos que permitan a los equipos del FNA operar, mantener y evolucionar la plataforma de manera autónoma al término del contrato. Este capítulo consolida los manuales entregados, organizados en cuatro bloques: manual de usuario del Developer Portal, manual de operación para equipos de infraestructura y SRE, manual de gestión de consumidores y runbooks operativos. Los manuales completos se encuentran como anexos electrónicos y en el repositorio documental del contrato; a continuación se presenta su estructura y contenido principal.

10.2. Manual de usuario del Developer Portal

El Developer Portal constituye la experiencia primaria para los desarrolladores y consumidores que integran las APIs del FNA. El manual correspondiente guía al usuario a través del ciclo completo, desde el registro hasta el consumo productivo:

10.2.1. Registro y activación

- Acceso al Developer Portal mediante https://developer.fna.gov.co (usuarios externos) o mediante SSO corporativo (usuarios internos con credenciales AD).
- Para usuarios externos: formulario de self-registration con validación por email; aprobación manual por el administrador del Developer Portal o por el owner de la API suscrita.
- Para usuarios internos: redirección automática a la página de autenticación SAML del FNA, con obtención de permisos según grupo AD al cual pertenezca.
- Política de contraseñas, MFA opcional/obligatorio según perfil y procedimiento de recuperación descrito.

10.2.2. Exploración del catálogo de APIs

- Búsqueda por nombre, dominio funcional o tag.
- Filtros por nivel de acceso (público, interno, privado) y estado de la API (activa, beta, deprecada).
- Vista detallada de cada API con contrato OpenAPI 3.x renderizado en Swagger UI o ReDoc, ejemplos, códigos de error y SDKs sugeridos.

10.2.3. Suscripción y gestión de API Keys

- Solicitud de suscripción a una API con selección del Usage Plan deseado.

- Workflow de aprobación: notificación al owner de la API, decisión en consola del portal, notificación al solicitante.
- Generación automática de API Key tras aprobación, visible una única vez al usuario (el usuario debe guardarla; si la pierde debe rotarla).
- Procedimiento de rotación de API Key sin interrupción del servicio (grace period de 24 h para migración).

10.2.4. Consumo de APIs

- Construcción del flujo OAuth 2.0 Authorization Code + PKCE o Client Credentials según tipo de consumidor.
- Obtención del access_token del endpoint /oauth2/token de Cognito.
- Invocación de la API con headers Authorization: Bearer {access_token} y x-api-key: {api-key}.
- Validación de respuestas tipificadas RFC 7807 y mejores prácticas ante errores.
- Implementación de idempotencia en operaciones POST mediante el header X-FNA-Idempotency-Key.

10.2.5. Visualización del consumo personal

- Dashboard del desarrollador mostrando solicitudes exitosas y erróneas por API y por día.
- Cuota disponible del Usage Plan en tiempo real.
- Últimos errores recientes con referencia al requestId para soporte.

10.3. Manual de operación para infraestructura y SRE

Dirigido a los equipos responsables de la operación sostenida de la plataforma. Los capítulos principales son:

10.3.1. Acceso a las cuentas AWS

- Procedimiento de autenticación a AWS IAM Identity Center con credenciales AD corporativas.
- Selección de cuenta (Management, Security, Log Archive, Shared Services, Workloads Prod, Workloads Non-Prod) y Permission Set apropiado.
- Uso de AWS CLI v2 con SSO profile para acceso programático seguro sin access keys.
- MFA obligatorio, session timeout de 8 horas.

10.3.2. Ubicación de recursos en la consola AWS

Guía visual para localizar cada componente de la plataforma:

- Amazon API Gateway: cuenta workload correspondiente, región us-east-1, navegación por APIs → Stages → Deployments.
- Amazon EKS: cuenta workload, cluster fna-apim-{env}-eks-gateway-cluster, recursos gestionados con kubectl mediante el comando aws eks update-kubeconfig.
- Amazon Cognito: cuenta Shared Services, User Pool fna-apim-prod-cognito-external.
- AWS WAF: cuenta Shared Services, Web ACLs por Stage.
- Amazon Managed Grafana: cuenta Shared Services, workspace fna-apim-grafana.

10.3.3. Procedimiento de despliegue de una nueva versión de API

20. Desarrollo en rama feature/* en Azure Repos.
21. Pull Request con revisión por Lead Developer y aprobación.
22. Azure Pipelines ejecuta build, pruebas unitarias y SAST.
23. AWS CodeBuild construye imagen Docker y la firma.
24. Amazon ECR almacena la imagen con escaneo Inspector.
25. AWS CodeDeploy despliega a Dev automáticamente; aprobación para ambientes superiores.
26. Validación mediante CloudWatch Synthetics canaries automáticas.
27. Publicación de la nueva Stage y actualización del custom domain tras validación.

10.3.4. Procedimiento de rollback

- Opción 1 (inmediata): en la consola de API Gateway, cambiar el Deployment al que apunta la Stage al Deployment anterior conocido como estable; cambio instantáneo (< 30 s).
- Opción 2 (función Lambda): cambiar el Alias PROD al Version anterior; efecto inmediato.
- Opción 3 (infraestructura): rollback automático ejecutado por CloudFormation ante fallo de Change Set.
- Documentar el incidente en el sistema de tickets y ejecutar post-mortem con lecciones aprendidas.

10.3.5. Consulta de logs y trazas

- Amazon CloudWatch Logs Insights: acceder a la consola, seleccionar log group /aws/apigateway/{apiId}, ejecutar consulta con filtros por requestId o status code.
- AWS X-Ray: consultar ServiceMap, filtrar por trace-id propagado en las respuestas API mediante header X-Amzn-Trace-Id.

- Amazon Managed Grafana: dashboard Trazabilidad – End-to-End para correlacionar métricas y trazas.
- Amazon OpenSearch Dashboards: búsqueda libre sobre logs estructurados con filtros por campos.

10.3.6. Gestión de alertas y runbooks

- Amazon Managed Grafana: consulta de alarmas activas, silenciamiento temporal y acknowledge.
- Integración con AWS Chatbot: canales Slack/Teams configurados por severidad.
- Ejecución de runbooks documentados en AWS Systems Manager Documents (ssm:StartAutomationExecution).

10.3.7. Gestión de secretos

- AWS Secrets Manager: consola para rotación manual ante compromiso sospechado.
- Verificación de rotación automática programada (cada 30 días por default).
- Auditoría de accesos a secretos vía CloudTrail.

10.3.8. Gestión de certificados

- AWS Certificate Manager: consulta del estado de cada certificado, fecha de expiración y renovación automática.
- Procedimiento ante emisión de nuevo certificado para dominios adicionales.
- Validación DNS en Route 53.

10.4. Manual de gestión de consumidores

Dirigido al administrador del Developer Portal y a los owners de APIs. Incluye:

- Creación manual de API Keys para consumidores estratégicos desde la consola de API Gateway.
- Asignación de API Keys a Usage Plans y configuración de overrides específicos.
- Revocación inmediata ante incidente de seguridad: proceso de emergencia documentado.
- Rotación planificada periódica con plantilla de comunicación al consumidor.
- Análisis de consumo por consumidor con dashboards dedicados en Grafana.
- Gestión de cambios en cuotas y throttling con workflow de aprobación.

10.5. Runbooks operativos

Los siguientes 11 runbooks están documentados y automatizados donde es posible mediante AWS Systems Manager Automation Documents:

ID	Runbook	Disparador	Acción automatizada
RB-001	Incremento anómalo de latencia p99	Alarm CW latency > 1.5s 10min	Notifica + recolecta traces X-Ray + snapshot EKS
RB-002	Incremento de errores 5xx	Alarm 5XX > 1% 5min	Notifica + analiza logs + rollback si persiste
RB-003	Saturación de throttling	Throttled requests > 100/min	Notifica + evaluación de escalar Usage Plan
RB-004	Falla de autenticación Cognito	Spike de 401 > 5% 5min	Notifica + verifica JWKS + check AD federation
RB-005	Pérdida de conectividad VPN	Tunnel down > 60s	Página crítica + failover a tunnel secundario
RB-006	Failover entre AZs	EKS node group AZ outage	Karpenter reaprovisiona en AZs restantes
RB-007	Rotación de emergencia de API Key	Notificación de compromiso	Revoca + genera nueva + comunica
RB-008	Rollback de deployment defectuoso	Post-deploy check fail	CodeDeploy rollback automático
RB-009	GuardDuty finding severity > 7	Finding recibido	Notifica + aísla recurso + preserva evidencia
RB-010	WAF block anómalo alto	WAF blocked > 500/5min	Notifica + análisis patrón + ajuste reglas
RB-011	Aurora storage > 80 %	CW Alarm storage usage	Notifica + auto-scale storage (hasta 128 TB)

Tabla 19. Runbooks operativos documentados.

10.6. Plan de continuidad operativa

Al cierre de la Fase 1 se encuentra formalizado el plan de continuidad operativa con los siguientes elementos:

- Ventanas de mantenimiento pactadas: martes 22:00–00:00 y domingos 02:00–06:00, hora de Colombia, con comunicación previa 72 h de anticipación.
- Equipo de guardia 24×7 durante Fase 2 con modelo de turnos rotativos, cubriendo los horarios hábiles y no hábiles definidos en el Anexo 1.
- Escalamiento por severidad: Nivel 1 (soporte primario), Nivel 2 (ingeniería de plataforma), Nivel 3 (arquitectura + vendor support AWS Enterprise).
- SLAs de atención para Fase 2: P1 Crítico ≤ 30 min, P2 Alto ≤ 2 h, P3 Medio ≤ 8 h, P4 Bajo ≤ 24 h.
- Contactos principales: coordinador técnico INGENIUM, líder SRE FNA, gerencia de seguridad FNA, AWS TAM (Technical Account Manager).

SOLUCIÓN

11.1. Descripción del entregable

El entregable E8 del Anexo 1 exige la entrega de un documento de arquitectura que consolide las decisiones, patrones y estructuras técnicas que sustentan la solución. El Documento de Arquitectura de Referencia completo (RAD API Manager AWS FNA-132-2025) fue entregado previamente al FNA como insumo técnico del contrato, con 89 páginas, 15 tablas, 8 diagramas y 8 ADRs. El presente capítulo consolida la síntesis arquitectónica, las decisiones adoptadas durante la implementación de la Fase 1 y las referencias cruzadas con los requerimientos del Anexo 1, actuando como el resumen ejecutivo arquitectónico del cierre de Fase 1.

11.2. Síntesis arquitectónica consolidada

La solución materializa íntegramente la arquitectura de referencia Zentium sobre Amazon Web Services, extendiendo y operacionalizando el diseño inicial entregado por el contratista al FNA. Las ocho capas lógicas de Zentium se han instanciado con servicios AWS nativos exclusivamente, conformando una plataforma cloud-native serverless-first, event-driven y zero-trust, gobernada por

Infrastructure as Code y desplegada bajo una Landing Zone multi-cuenta controlada por AWS Organizations y AWS Control Tower.

El núcleo de exposición y gobierno corresponde a Amazon API Gateway como servicio central de la Capa 1 Edge & API Management, complementado por Amazon CloudFront, AWS WAF, AWS Shield, Amazon Cognito y AWS AppSync. La capa de cómputo se sustenta en Amazon EKS con Fargate Profiles para los microservicios ESB_*, complementada por AWS Lambda para autorizadores y transformadores SOAP, y AWS Step Functions para orquestaciones Saga. La observabilidad integral se soporta en el stack 100% AWS de CloudWatch, X-Ray, AMP, AMG, OpenSearch y CloudTrail Lake.

11.3. Decisiones arquitectónicas clave adoptadas durante la Fase 1

Las siguientes decisiones arquitectónicas (Architecture Decision Records) se tomaron y documentaron durante la ejecución de la Fase 1, complementando las ADRs generales del RAD entregado previamente:

ADR-F1-001: Adopción íntegra de la arquitectura de referencia Zentium

Contexto: Se requiere una arquitectura de referencia AWS-nativa, coherente, documentada y alineada con Well-Architected que soporte el alcance contractual del FNA.

Decisión: Adoptar Zentium como arquitectura de referencia base para todo el despliegue, con sus 8 capas lógicas materializadas exclusivamente mediante servicios AWS gestionados.

Consecuencias: Alta consistencia arquitectónica entre componentes, reducción de la carga de decisiones ad-hoc, alineación natural con Well-Architected; posible curva de aprendizaje para el equipo del FNA respecto a servicios avanzados como Verified Permissions y Managed Grafana.

ADR-F1-002: Amazon API Gateway REST como núcleo del API Manager

Contexto: Se requiere un API Gateway con Usage Plans, validación de esquemas, mapping templates y autorizadores, exigidos por los requerimientos técnicos del Anexo 1 y por la naturaleza SOAP de los backends del ESB_FNA.

Decisión: Desplegar Amazon API Gateway REST APIs como núcleo; reservar HTTP APIs para casos internos de alto volumen y latencia estricta.

Consecuencias: Costo mayor por solicitud que HTTP APIs, compensado por las capacidades ricas; gestión unificada del portafolio; compatibilidad total con los servicios ESB_* legados del FNA.

ADR-F1-003: Amazon Cognito como IdP para usuarios externos y federación SAML con AD FNA

Contexto: Se requiere autenticación OAuth 2.0/OIDC para consumidores externos y Single Sign-On para usuarios internos con su identidad corporativa, cumpliendo exclusividad AWS.

Decisión: Desplegar Amazon Cognito User Pool como IdP primario de usuarios externos, y configurar federación SAML con el Active Directory del FNA para empleados internos mediante IAM Identity Center.

Consecuencias: Dependencia de un servicio gestionado AWS, mitigada por uso de estándares abiertos (OIDC, SAML, JWT); eliminación de gestión de contraseñas propias para externos; integración natural con el AD del FNA.

ADR-F1-004: Amazon EKS con Fargate Profiles como plataforma de cómputo para microservicios ESB_*

Contexto: Los requerimientos técnicos del Anexo 1 exigen orquestación de contenedores Docker con Kubernetes. Se busca minimizar la carga operativa preservando flexibilidad.

Decisión: Adoptar Amazon EKS con Fargate Profiles para la mayoría de microservicios y Managed Node Groups con procesadores Graviton para workloads de alto throughput.

Consecuencias: Alta disponibilidad nativa, ahorro operativo frente a EKS self-managed, portabilidad estándar K8s; costos variables según carga, trazados mediante tags y Cost Explorer.

ADR-F1-005: Observabilidad basada en stack 100% AWS (CloudWatch + AMP + AMG + OpenSearch)

Contexto: Se requiere observabilidad integral cumpliendo con la exclusividad AWS de la arquitectura Zentium y con los requisitos del entregable E4.

Decisión: Adoptar stack AWS nativo: Amazon CloudWatch para métricas y logs base, Amazon Managed Prometheus para métricas EKS, Amazon Managed Grafana como visualización unificada, Amazon OpenSearch como búsqueda libre sobre logs.

Consecuencias: Evita vendor lock-in a Datadog/ELK/New Relic; integración nativa con IAM, KMS y Organizations; costo optimizable con lifecycles de logs y tiers de OpenSearch.

ADR-F1-006: CloudTrail Organization Trail con retención 7 años y S3 Object Lock Compliance

Contexto: Se requiere trazabilidad inmutable y retención prolongada para cumplimiento con SFC CE 007/2018 y Ley 1581/2012.

Decisión: Habilitar CloudTrail Organization Trail en todas las cuentas, con destino en bucket S3 dedicado en cuenta Log Archive con Object Lock en modo Compliance y retención mínima de 7 años.

Consecuencias: Garantiza evidencia auditable para SFC y auditoría interna; costo predecible con lifecycle a Glacier Deep Archive; requiere doble control para eliminar eventualmente (privilegios segregados).

ADR-F1-007: Azure DevOps como orquestador externo y AWS Developer Tools como ejecutor

Contexto: El FNA ha institucionalizado Azure DevOps como plataforma de CI/CD (numeral IX Anexo 1). La integración con servicios AWS debe respetar este estándar.

Decisión: Operar Azure Repos, Azure Pipelines y Azure Boards como plataforma primaria, con AWS Toolkit for Azure DevOps y OIDC federation (sin access keys estáticas) para delegar la ejecución técnica a AWS CodeBuild, AWS CodeDeploy y AWS CloudFormation.

Consecuencias: Mayor complejidad inicial, compensada por respeto al estándar institucional y aprovechamiento de inversiones existentes; elimina credenciales de larga vida mediante OIDC.

ADR-F1-008: AWS Verified Permissions con Cedar para autorización fine-grained

Contexto: Se requiere autorización contextual avanzada (evaluación de principal, action, resource, context) para APIs sensibles como transacciones de pago y consulta de listas inhibitorias.

Decisión: Adoptar AWS Verified Permissions con políticas escritas en Cedar, invocadas desde el Lambda Authorizer tras validación exitosa del JWT.

Consecuencias: Expresividad superior a políticas IAM puras, velocidad de evaluación sub-10ms p99, auditoría estructurada de decisiones; curva de aprendizaje de Cedar para el equipo FNA, mitigada por transferencia de conocimiento.

11.4. Patrones arquitectónicos adoptados

- Serverless-first: priorización de servicios gestionados sin servidor (API Gateway, Lambda, Step Functions, Fargate, DynamoDB On-Demand) para eliminar la gestión de instancias.
- Event-driven: comunicación asíncrona via Amazon EventBridge como bus corporativo, con Schema Registry para contratos tipados.
- Zero-trust: cada invocación se autentica y autoriza con múltiples capas (WAF, Cognito, Verified Permissions); cero tráfico interno confiado por defecto.
- Multi-cuenta: segregación de responsabilidades y radio de impacto mediante AWS Organizations + Control Tower.
- Database-per-service: cada microservicio gestiona su propio almacén de datos (Aurora, DynamoDB) sin acoplamiento con otros.
- Anti-Corruption Layer: Lambda transformers encapsulan las particularidades de los servicios SOAP legados, exponiendo interfaces REST limpias.
- Strangler Fig: migración gradual desde el ESB_FNA preservando los servicios existentes y encapsulándolos en APIs modernas.
- Infrastructure as Code: toda la infraestructura versionada en AWS CloudFormation; cero cambios manuales en Prod.

11.5. Trazabilidad con requerimientos del Anexo 1

La siguiente tabla consolida la cobertura de los requerimientos funcionales (RF) y técnicos (RT) del Anexo 1 por la implementación entregada en Fase 1:

ID	Requerimiento (resumen)	Estado Fase 1	Servicios AWS
RF_001	API Gateway robusto con enrutamiento	Cumplido	Amazon API Gateway + CloudFront + WAF
RF_002	Soporte REST/SOAP, versionado	Cumplido	API Gateway Stages + VTL + Lambda transformers
RF_003	Gestión de políticas	Cumplido	API Gateway + WAF + Cognito + Verified Permissions
RF_004	Adaptadores para integración con legados	Cumplido	Lambda adapters + Amazon MQ + Step Functions
RF_005	Bus de Integración JMS/AMQP	Cumplido	Amazon MQ (RabbitMQ)
RF_006	Developer Portal con autoservicio	Cumplido	CloudFront + S3 + Cognito + API Gateway
RF_007	Gestión de consumidores	Cumplido	Cognito + API Keys + Usage Plans
RF_008	Analytics y dashboards	Cumplido	CloudWatch + AMP + AMG + Athena/QuickSight (prep)
RF_009	Control de versiones APIs	Cumplido	API Gateway Deployments + Lambda Aliases
RF_010	Publicación automatizada	Cumplido	CodePipeline + CodeDeploy + CloudFormation
RF_011	Gestión de contenedores	Cumplido	Amazon EKS + ECR
RF_012	Orquestación de contenedores	Cumplido	EKS + Fargate + Karpenter
RF_013	Escalabilidad horizontal	Cumplido	HPA + Cluster Autoscaler + Application Auto Scaling

ID	Requerimiento (resumen)	Estado Fase 1	Servicios AWS
RF_014	Integración CI/CD	Cumplido	CodePipeline + CodeBuild + CodeDeploy + Azure DevOps
RF_015	Monitoreo de APIs	Cumplido	CloudWatch + X-Ray + Container Insights
RF_016	Gestión de logs centralizada	Cumplido	CloudWatch Logs + OpenSearch + Firehose
RF_017	Alertas y notificaciones	Cumplido	CloudWatch Alarms + SNS + Chatbot
RF_018	Soporte OpenAPI/WSDL/XSD	Cumplido	API Gateway OpenAPI import + validators
RF_019	Transformación JSON↔XML	Cumplido	API Gateway VTL + Lambda transformers
RF_020	WebSockets y gRPC	Provisto	API Gateway WebSocket + AppSync + ALB gRPC
RF_021	Federación de identidad	Cumplido	Cognito + IAM Identity Center + SAML
RF_022	Cifrado y gestión de secretos	Cumplido	KMS + Secrets Manager + Parameter Store
RF_023	Alta disponibilidad y failover	Cumplido	Multi-AZ + Aurora + Route 53 + Resilience Hub
RT_001	API Gateway seguro y escalable	Cumplido	API Gateway + WAF + Shield + CloudWatch
RT_002	Enrutamiento dinámico	Cumplido	API Gateway + Route 53 + CloudFront
RT_003	Control de tráfico	Cumplido	API Gateway Usage Plans + WAF rate-based

ID	Requerimiento (resumen)	Estado Fase 1	Servicios AWS
RT_004	Transformación contenido/protocolos	Cumplido	API Gateway VTL + Lambda + EventBridge
RT_005	Autenticación, autorización y monitoreo	Cumplido	Cognito + IAM + CloudTrail + Security Hub

Tabla 20. Matriz de trazabilidad de los 28 requerimientos del Anexo 1 al cierre de Fase 1.

11.6. Conformidad con AWS Well-Architected Framework

La plataforma cumple con los seis pilares del AWS Well-Architected Framework con evidencia específica:

Pilar Well-Architected	Evidencia al cierre de Fase 1
Excelencia Operativa	Infrastructure as Code, CI/CD Azure DevOps + AWS Developer Tools, 11 runbooks automatizados
Seguridad	Zero-trust, Cognito + MFA, KMS CMK, Verified Permissions, WAF + Shield, GuardDuty, Security Hub
Confiabilidad	Multi-AZ, Aurora Multi-AZ, Karpenter autoscaling, EKS auto-healing, 2 túneles VPN redundantes
Eficiencia del Rendimiento	Serverless-first, Graviton, CloudFront edge, caché ElastiCache, API Gateway caching
Optimización de Costos	Tagging obligatorio, AWS Budgets, Compute Optimizer, apagado programado Non-Prod
Sostenibilidad	Graviton ARM, Fargate right-sized, lifecycle S3, cero sobreaprovisionamiento

Tabla 21. Evidencia de conformidad con AWS Well-Architected Framework.

11.7. Conformidad normativa

- SFC Circular Externa 007/2018 (ciberseguridad): CloudTrail 7 años, GuardDuty, Security Hub, WAF, MFA obligatorio para administradores, segregación de ambientes.
- SFC Circular Externa 029/2014: cifrado extremo a extremo, control de acceso robusto, trazabilidad integral.
- Ley 1581/2012 y Decreto 1377/2013 (Habeas Data): Macie para clasificación PII, KMS para cifrado, derechos ARCO habilitados en aplicación, retención definida.
- Ley 1273/2009 (delitos informáticos): registro forense con CloudTrail + Detective.
- Decreto 1297/2022 (Open Finance): preparación con mTLS, Cognito, registro auditable (APIs Open Finance provisionadas).
- OWASP API Security Top 10: controles WAF + Verified Permissions + validadores + threat protection.
- Políticas GR-SI-MN-SGSI del FNA: hardening, gestión de vulnerabilidades, desarrollo seguro, seguridad de proveedores.

12. REQUERIMIENTOS NO FUNCIONALES Y ATRIBUTOS DE CALIDAD

12.1. Propósito y alcance

El presente capítulo consolida y presenta los Requerimientos No Funcionales (RNF) que dan forma a los atributos de calidad de la solución de API Manager implementada para el Fondo Nacional del Ahorro (FNA). Su propósito es servir como anexo técnico de la Arquitectura de Solución, documentando de manera estructurada los criterios de calidad bajo los cuales fue diseñada, desplegada y verificada la plataforma Zentium, así como las tácticas arquitectónicas y los componentes que sustentan su cumplimiento.

Los atributos de calidad abordados son Seguridad, Escalabilidad, Disponibilidad, Rendimiento, Mantenibilidad y Operabilidad, Interoperabilidad e Integración, y Trazabilidad y Monitoreo. Estos constituyen el conjunto de capacidades transversales que la solución debe garantizar para soportar de forma confiable la exposición y gobierno de las APIs del FNA. Cada atributo se describe mediante el alcance de la revisión, las tácticas de arquitectura aplicadas, la realización a través de componentes estructurales y el estado de conformidad alcanzado.

Además, el capítulo se complementa con la vista de Arquitectura de Solución presentada en la sección final, donde se identifican los componentes que materializan cada uno de los atributos de calidad descritos.

Para efectos de lectura del presente capítulo y de los capítulos 13 y 14, los ambientes TEST, CERT y PROD corresponden, respectivamente, a los ambientes de Pruebas (QA), Certificación (PreProd) y Producción descritos en la Sección 3.4 y en los indicadores de la Sección 1.2.

12.2. Seguridad

Tabla 22. Atributo de calidad — Seguridad.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Seguridad** La seguridad es el atributo de calidad más crítico del proyecto. El FNA gestiona información sensible de millones de ahorradores colombianos. La arquitectura implementa una estrategia de defensa en profundidad con múltiples capas de control: autenticación, autorización, cifrado, aislamiento de red, protección contra abuso y auditoría completa.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) El API Manager soporta integración con proveedores de identidad externos mediante estándares como OpenID Connect, permitiendo centralizar la autenticación de usuarios para el acceso a la consola de administración y portal de desarrolladores. Adicionalmente, la plataforma incorpora controles de autorización basados en roles, habilitando perfiles diferenciados para administración, publicación y consumo de APIs. (2) Cifrado en Tránsito: todo el tráfico externo termina en TLS en el AWS ALB. Los certificados son gestionados por AWS Certificate Manager. La VPN Site-to-Site IPSec cifra el canal entre la infraestructura AWS y el datacenter del FNA. La comunicación intra-cluster también va cifrada.

	(3) Aislamiento de Red (Network Segmentation): cada ambiente (TEST/CERT/PROD) opera en su propio namespace Kubernetes con Network Policies que restringen el tráfico entre namespaces. MongoDB, Redis y ElasticSearch no están expuestos fuera del cluster. Solo el ALB tiene reglas de ingreso externas. (4) Rate Limiting y Protección contra Abuso: Redis 7.x implementa el motor de rate limiting del Gateway. Las políticas de quota se aplican por suscripción. Capacidad de lista negra / blanca de IPs mediante políticas de IP Filtering aplicables por API o a nivel global del Gateway. (5) Auditoría y Trazabilidad: ElasticSearch captura el log completo de cada petición (timestamp, consumidor, API, código de respuesta, latencia). La consola registra todas las acciones de gestión con datos de usuario y timestamp. Los registros son inmutables con retención configurable. (6) Gestión de Secretos: credenciales y llaves almacenadas en Kubernetes Secrets cifrados con KMS de AWS. AWS IAM controla los accesos de pods a recursos AWS siguiendo el principio de mínimo privilegio. Las API Keys son únicas y revocables individualmente sin impacto a otros consumidores. (7) Autenticación hacia Backends (Upstream Security): las APIs publicadas en la Solución consumen los servicios del FNA utilizando el mismo mecanismo de autenticación definido por los servicios del

	bus existente — usuario/contraseña, tokens o headers configurados individualmente por servicio. El Gateway propaga de forma segura estas credenciales hacia los backends sin exponerlas al consumidor externo, preservando la integración con los sistemas legados del FNA sin requerir cambios en los backends ni en el bus.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: Solución Gateway (punto de aplicación de políticas), AWS ALB (terminación TLS), VPN IPSec (cifrado canal FNA-AWS), Redis (rate limiting), ElasticSearch (auditoría), Kubernetes Secrets + KMS (gestión de secretos) y AWS IAM (identidades). - Flujo de seguridad: [Consumidor] → HTTPS → [AWS ALB / TLS] → [Solución Gateway: valida JWT/OAuth, aplica rate limit via Redis, registra log en OS] → [FNA via VPN IPSec]. - Aislamiento: namespace — sin tráfico cruzado por Network Policy. Componentes de datos (MongoDB, Redis y ElasticSearch) solo son accesibles desde dentro del cluster en el ambiente de Pruebas. En los ambientes de Certificación y Producción, al operar como servicios gestionados fuera del clúster, únicamente se comunican de forma interna a través de la red VPC de AWS.
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. Todos los controles de seguridad requeridos por el Anexo Técnico están implementados y activos en los tres ambientes.**

12.3. Escalabilidad

Tabla 23. Atributo de calidad — Escalabilidad.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Escalabilidad** La arquitectura está diseñada para escalar de forma horizontal y vertical sin interrupciones de servicio, soportando el crecimiento en número de APIs publicadas, consumidores activos y volumen de tráfico. La estrategia se fundamenta en microservicios sin estado que permiten escalado elástico e independiente por componente.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Microservicios sin estado: cada componente de la Solución (Gateway, Management API, Portal API) es un Deployment Kubernetes sin estado. La ausencia de estado en el Gateway permite añadir réplicas instantáneamente sin coordinación, garantizando escalado elástico. (2) Escalado horizontal automático (HPA): HorizontalPodAutoscaler configurado en los Deployments del Gateway — escala réplicas automáticamente cuando el uso de CPU supera el umbral definido (70%). AWS EKS Cluster Autoscaler aprovisiona nodos EC2 adicionales cuando los pods no encuentran capacidad. (3) **Escalado vertical por componente:** MongoDB y ElasticSearch soportan ajuste de resource limits/requests vía kubectl patch en el ambiente de Pruebas, en el ambiente de Certificación y Productivo puede ser configurado desde los servicios de ElasticSearch (AWS OpenSearch) y en la nube de MongoDB Atlas respectivamente. Amazon EBS con

	AllowVolumeExpansion habilitado permite ampliar el almacenamiento persistente sin recrear los StatefulSets. (4) Distribución Multi-AZ y Alta Disponibilidad: nodos EKS distribuidos en múltiples Zonas de Disponibilidad de AWS us-east-1. AWS ALB balancea tráfico entre réplicas en diferentes AZ sin punto único de falla. Redis en modo Cluster activo garantiza disponibilidad del rate limiting incluso ante pérdida de un nodo.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: AWS EKS (Kubernetes gestionado), HorizontalPodAutoscaler (escalado automático), AWS Cluster Autoscaler (nodos EC2), Amazon EBS + CSI (almacenamiento escalable), AWS ALB (balanceo Multi-AZ) y Redis Cluster (alta disponibilidad de caché). - Flujo de escalado: [Incremento de tráfico] → [HPA detecta CPU > 70%] → [Nuevos pods Gateway] → [Si sin capacidad: Cluster Autoscaler → nuevo nodo EC2] → [ALB distribuye tráfico entre réplicas en AZ-1, AZ-2]. - Estado verificado: 9 pods en Running en los tres ambientes. Configuración de réplicas activa en PROD con mínimo 2 réplicas del Gateway para garantizar disponibilidad continua.
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. Arquitectura elástica verificada con pods en Running en los tres ambientes.**

	HPA, Cluster Autoscaler y Multi-AZ configurados y operativos.

12.4. Disponibilidad

Tabla 24. Atributo de calidad — Disponibilidad.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Disponibilidad** La arquitectura garantiza la continuidad del servicio de gestión de APIs ante fallos de componentes individuales, actualizaciones y mantenimientos. El objetivo de disponibilidad en producción es mayor o igual a 99.9%, equivalente a menos de 8.7 horas de indisponibilidad anual.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Réplicas múltiples activas: el Gateway opera con mínimo 2 réplicas en producción. La pérdida de un pod no interrumpe el servicio: el ALB redirige el tráfico a las réplicas sanas automáticamente. (2) Health Checks (liveness y readiness probes): configurados en todos los pods. Kubernetes reinicia automáticamente pods en fallo y no redirige tráfico a pods no listos hasta que superen el readiness check. (3) Rolling Updates sin downtime: las actualizaciones de versión se despliegan gradualmente, reemplazando pods uno a uno mientras se valida la salud del nuevo despliegue. Rollback instantáneo disponible vía kubectl rollout undo ante cualquier fallo.

	(4) Ambientes independientes TEST/CERT/PROD: los cambios se validan progresivamente antes de llegar a producción, minimizando el riesgo de incidentes. Un fallo en TEST o CERT no tiene impacto en el ambiente productivo. (5) AWS ALB con health checks activos: el balanceador retira automáticamente del pool los nodos EKS o pods que no respondan correctamente a los health checks configurados.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: Solución Gateway (múltiples réplicas), AWS ALB (balanceo + health checks), Kubernetes (liveness/readiness probes, rolling updates), AWS EKS Multi-AZ (tolerancia a fallo de zona) y 3 ambientes independientes (pipeline de promoción). - Flujo de fallo y recuperación: [Pod Gateway falla] → [Kubernetes detecta via liveness probe] → [Reinicia pod automáticamente] → [ALB retira pod del pool hasta que readiness probe pase] → [Tráfico fluye sin interrupción a réplicas sanas]. - Estado verificado: todos los pods en Running. URLs de los tres ambientes activas y respondiendo: test.apimanager.fna.gov.co · cert.apimanager.fna.gov.co · prod.apimanager.fna.gov.co.
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. Todos los pods verificados en estado Running. Alta disponibilidad habilitada**

	con réplicas múltiples, health probes y ALB operativos en producción.

12.5. Rendimiento

Tabla 25. Atributo de calidad — Rendimiento.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Rendimiento** La arquitectura minimiza la latencia añadida por el Gateway en el camino de cada petición de API, garantizando throughput adecuado para el volumen de servicios del FNA. Las decisiones de diseño priorizan el procesamiento no bloqueante y el uso de caché para operaciones frecuentes.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Caché con Redis 7.x: actúa como capa de caché para respuestas de APIs configuradas con cache policy, reduciendo la carga en los sistemas backend del FNA. El rate limiting se resuelve en memoria Redis (sub-milisegundo) sin añadir latencia perceptible al camino de la petición. (2) Analytics asíncrono (non-blocking): la ingesta de logs y métricas en ElasticSearch se realiza de forma asíncrona. El procesamiento de analytics no afecta la latencia del Gateway en el camino crítico. Reportes y dashboards consumen datos de ES sin impacto en el Gateway productivo. (3) Connection Pooling: el Gateway mantiene connection pools hacia los backends del FNA, eliminando el overhead de establecer nuevas conexiones TCP/TLS por cada petición.

	AWS ALB opera con keep-alive habilitado hacia los pods del Gateway. (4) Escalado horizontal reactivo: ante picos de carga, el HPA aumenta réplicas del Gateway antes de que la latencia se degrade, garantizando tiempos de respuesta estables bajo demanda variable.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: Redis 7.x (caché de respuestas y rate limiting), ElasticSearch (analytics asíncrono), Solución Gateway (connection pooling hacia backends FNA) y AWS ALB (keep-alive, distribución de carga). - Flujo de petición optimizado: [Consumidor] → [ALB keep-alive] → [Gateway: valida JWT en memoria, comprueba rate limit en Redis ~0.5ms, sirve desde caché si aplica] → [Backend FNA via pool de conexiones persistentes] → [Log asíncrono a ElasticSearch sin bloquear respuesta]. - Optimización de analytics: el Gateway envía eventos de log a un buffer interno que drena a ElasticSearch de forma periódica y asíncrona, garantizando que ningún pico de escritura en ES afecte la latencia de las APIs productivas.
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. Arquitectura optimizada para baja latencia con Redis, procesamiento asíncrono de métricas y connection pooling hacia el bus del FNA.**

12.6. Mantenibilidad y Operabilidad

Tabla 26. Atributo de calidad — Mantenibilidad y Operabilidad.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Mantenibilidad y Operabilidad** La arquitectura facilita la operación diaria, actualización y diagnóstico de la plataforma sin requerir acceso directo a infraestructura. La Console web, los tres ambientes independientes y la centralización de logs garantizan que el equipo del FNA pueda gestionar el ciclo de vida de sus APIs de forma autónoma y controlada.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Infraestructura como Código (IaC): el despliegue de todos los componentes en EKS se gestiona mediante manifiestos Kubernetes versionados, garantizando reproducibilidad, auditabilidad y capacidad de recrear cualquier ambiente en caso de desastre. (2) Tres ambientes independientes (TEST/CERT/PROD): permiten el ciclo completo de prueba, validación y promoción de cambios. Ninguna modificación llega a producción sin haber pasado por los ambientes previos. Reducción drástica del riesgo operativo. (3) Console de Administración web: la gestión del ciclo de vida de APIs (publicación, versioning, deprecación, planes, suscripciones) no requiere acceso SSH ni conocimiento de infraestructura. Operación accesible para el equipo técnico del FNA.

	(4) Logs centralizados en ElasticSearch: diagnóstico rápido de incidentes sin acceso a pods individuales. Búsqueda por API, consumidor, código de error o rango de tiempo. Dashboards nativos en la Console de la Solución. (5) Rolling updates y rollback: cualquier versión defectuosa puede revertirse en segundos mediante kubectl rollout undo. Actualizaciones sin ventanas de mantenimiento ni downtime.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: Solución Console (gestión web del ciclo de vida), Kubernetes manifiestos versionados (IaC), ElasticSearch (logs centralizados), 3 ambientes independientes (pipeline TEST → CERT → PROD) y kubectl rollout (rolling updates y rollback). - Pipeline de cambios: [Desarrollo/cambio] → [Despliegue en TEST] → [Validación funcional] → [Promoción a CERT] → [Certificación QA] → [Promoción a PROD vía rolling update sin downtime] → [Monitoreo post-despliegue en dashboards ES]. - Operación diaria: el equipo del FNA gestiona APIs desde la Console web (publicar, versionar, crear planes, aprobar suscripciones) sin depender del equipo DevOps para operaciones rutinarias. Solo cambios de infraestructura requieren acceso al cluster.

Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. Operación centralizada verificada vía Console web. Tres ambientes activos con pipeline de promoción operativo. Logs disponibles en ElasticSearch.**

12.7. Interoperabilidad e Integración

Tabla 27. Atributo de calidad — Interoperabilidad e Integración.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Interoperabilidad e Integración** La solución centraliza la exposición y consumo de los servicios del FNA, independientemente del protocolo o tecnología de los sistemas backend. Permite integrar consumidores internos, externos y ciudadanos con los servicios institucionales de forma estandarizada, segura y gobernada.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Soporte multi-protocolo: el Gateway soporta REST/HTTP, REST/HTTPS y capacidad de extensión para SOAP y GraphQL mediante policies de transformación. Los backends del FNA pueden mantenerse en sus protocolos actuales mientras el Gateway expone interfaces modernas estandarizadas. (2) Integración con el datacenter FNA via VPN IPSec: la VPN Site-to-Site conecta la infraestructura AWS con el datacenter del FNA. El Gateway enruta peticiones al bus de servicios del FNA sin exponerlos a redes públicas. (3) Portal del Desarrollador con OpenAPI/Swagger: expone documentación interactiva de todas las APIs publicadas. Facilita la adopción por equipos internos del FNA, proveedores externos y desarrolladores de aplicaciones ciudadanas. (4) Policy Engine sin modificación de código: las políticas del Gateway

	(transformación de headers, reescritura de URLs, inyección de parámetros de seguridad, conversión de formatos) son configurables por API desde la Console sin tocar el código de los backends del FNA. (5) Compatibilidad con Autenticación del Bus Existente: la Solución es transparente al mecanismo de autenticación utilizado por cada servicio del bus del FNA. Los backends son consumidos con las mismas credenciales que ya usan (usuario/contraseña, tokens o headers específicos por servicio), configuradas de forma segura en las políticas del Gateway. Esto permite onboardear servicios existentes sin modificar los contratos ni la infraestructura del bus, acelerando la adopción de la plataforma de APIs.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: Solución Gateway (policy engine multi-protocolo), VPN IPSec FNA-AWS (integración datacenter), Solución Portal (catálogo OpenAPI), AWS ALB (entrada HTTPS unificada para todos los consumidores) y Solución Console (configuración de policies). - Flujo de integración: [Consumidor externo/interno] → [HTTPS → ALB] → [Gateway: aplica policy de transformación si aplica] → [VPN IPSec] → [Bus de servicios FNA interno (SOAP/REST/legado)] → [Respuesta transformada al consumidor en formato estandarizado].

	- Conectividad FNA verificada: VPN IPSec activa (tunnel establecido y probado).
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme con dispensa — VPN activa en TEST. Acceso a CERT y PROD pendiente de habilitación por FNA. Portal y Gateway operativos.**

12.8. Trazabilidad y Monitoreo

Tabla 28. Atributo de calidad — Trazabilidad y Monitoreo.

Revisión de arquitectura (RNF): atributo de calidad del sistema.	**Trazabilidad y Monitoreo** La arquitectura provee visibilidad completa del tráfico de APIs, el comportamiento de los consumidores y las acciones de gestión. ElasticSearch como motor de analytics garantiza que el FNA pueda auditar cualquier transacción y detectar anomalías en tiempo real.
Alcance de la revisión: tácticas puntuales de arquitectura para el cumplimiento del atributo.	(1) Logs estructurados por transacción: ElasticSearch almacena un registro por cada petición procesada por el Gateway: timestamp, consumidor, API invocada, plan, código HTTP, latencia y payload resumido. Búsqueda y filtrado en tiempo real desde la Console. (2) Dashboards de analytics nativos: la Console de la Solución provee dashboards de tráfico por API, tasa de error, latencia percentil (p50/p95/p99) y top consumidores. Actualizados en tiempo real sin herramientas externas. (3) Alertas configurables: la plataforma puede emitir notificaciones cuando una API supera su tasa de error, latencia o quota definida. Integrable con sistemas de alertas del FNA (email, webhooks). (4) Auditoría de gestión: todas las acciones sobre la plataforma (publicar, modificar, eliminar una API; crear planes; aprobar suscripciones) quedan registradas con usuario, timestamp y

	detalle de la acción. Inmutable y consultable desde la Console.
Realización de la consideración: descripción de la implementación mediante componentes estructurales y sus relaciones.	- Componentes involucrados: ElasticSearch (OpenSearch) 8.x (motor de logs y analytics), Solución Console (dashboards, alertas, auditoría de gestión) y Solución Gateway (generación de eventos de log por transacción, non-blocking). - Flujo de trazabilidad: [Petición al Gateway] → [Procesamiento (auth, rate limit, routing)] → [Respuesta al consumidor] → [Evento de log enviado asíncronamente a ElasticSearch] → [Disponible en dashboards de la Console en tiempo real]. - Estado verificado: ElasticSearch activo en los tres ambientes. Ingesta de logs activa desde el Gateway. Dashboard de analytics accesible desde la Console en prod.apimanager.fna.gov.co.
Estado de Conformidad: Conforme — Cumple plenamente. No conforme. Conforme con dispensa.	**Conforme — Cumple plenamente. ElasticSearch operativo con ingesta de logs activa en los tres ambientes. Dashboards de analytics y auditoría de gestión disponibles en la Console.**

12.9. Vista de arquitectura de la solución

La presente sección presenta la vista general de la arquitectura de la solución del API Manager, mostrando los componentes que la conforman y la forma en que se relacionan entre sí. El diagrama permite identificar los componentes técnicos que dan cumplimiento a los requerimientos no funcionales descritos en las secciones anteriores, como capas de red, plataforma de cómputo, gateway, motores de caché y analítica, repositorios de datos y servicios gestionados de AWS. De esta manera, cada atributo se materializa en uno o varios componentes visibles en la arquitectura, asegurando la trazabilidad entre los requerimientos definidos y la solución implementada.

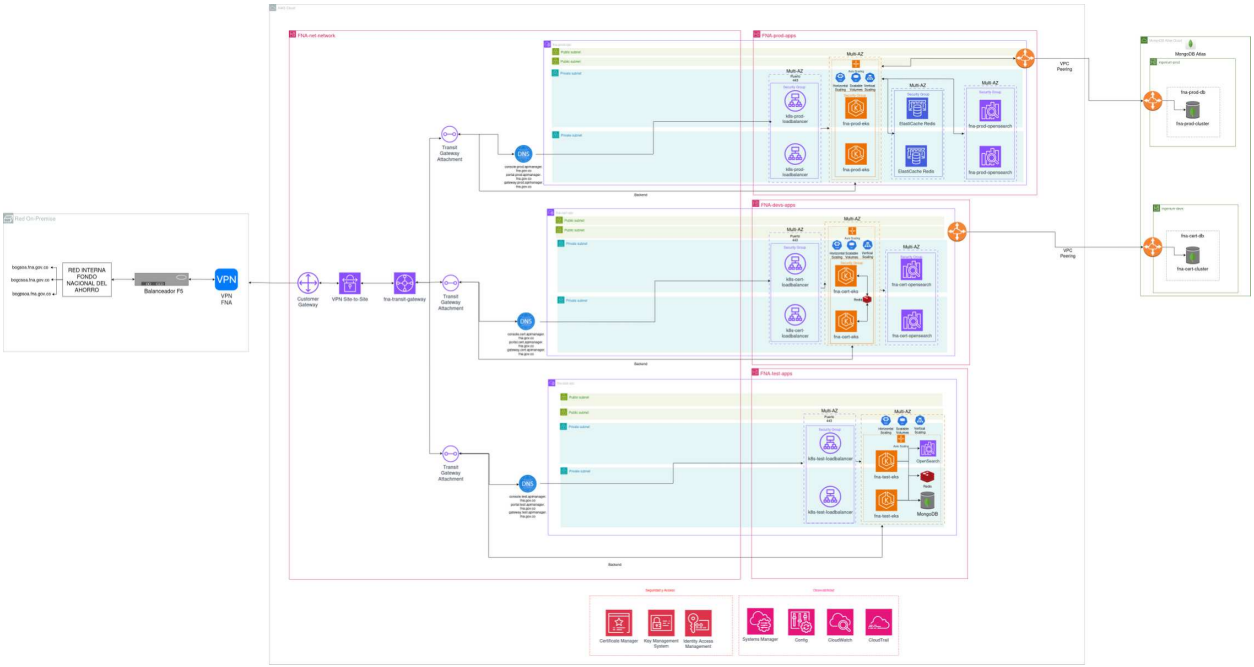


Ilustración 1. Vista general de la arquitectura de solución del API Manager.

13. CUMPLIMIENTO DE REQUERIMIENTOS FUNCIONALES Y TÉCNICOS

El presente capítulo consolida la matriz de cumplimiento de los requerimientos funcionales (RF_001 a RF_023) y de los requerimientos técnicos (RT) definidos en el Anexo 1 — Especificaciones Técnicas, indicando para cada requerimiento la respuesta de la plataforma y la evidencia asociada. Las evidencias referenciadas (Imagen 1 a Imagen 53) se presentan de forma íntegra en la Sección 13.3, con hipervínculos internos desde las matrices de cumplimiento. Los requerimientos marcados

como “No aplica contractualmente” corresponden a capacidades excluidas del alcance del contrato; el requerimiento RF_009 (SSL/TLS con certificados de validación extendida) se registra como pendiente por parte del FNA.

13.1. Requerimientos funcionales

ID REQ	DESCRIPCIÓN	Evidencia del cumplimiento (Pantallazo o Metadata)
RF_001	API Gateway: La plataforma debe contar con un API Gateway robusto que centralice la gestión de tráfico hacia las APIs. Este Gateway debe ser capaz de manejar tanto APIs REST como SOAP y de enrutar las solicitudes adecuadamente, independientemente del tipo de protocolo utilizado.	*Imagen 1* *Imagen 2*
RF_002	Versionado de APIs: Debe ser posible gestionar múltiples versiones de una misma API (por ejemplo, v1, v2, v3) y definir políticas de acceso específicas para cada versión. Este mecanismo debe estar integrado con la infraestructura de control de tráfico.	Imagen 3 Imagen 4 Imagen 5 Imagen 6

RF_003	Gestión de Endpoints - La plataforma debe ser capaz de administrar múltiples endpoints de manera eficiente, permitiendo que cada API pueda tener diferentes puntos de entrada para servicios internos, externos, o incluso entornos diferenciados como desarrollo, pruebas, y producción. - **Ejemplo de Endpoint: REST**: `https://api.company.com/v1/resource` - **Ejemplo de Endpoint SOAP**: `https://api.company.com/v1/service?wsdl`	Imagen 7 Imagen 8 Imagen 9 Imagen 10
RF_004	Integración con Sistemas Legados** - Debe permitir la creación de adaptadores o conectores para integrarse con sistemas legados, utilizando tecnologías como **ESB (Enterprise Service Bus)** o **Middleware**. Estos adaptadores deben permitir la conversión entre los formatos de datos legados y los formatos modernos (JSON, XML).	La plataforma de API MANAGER se conecta al bus existente del FNA a través de VPN Site-to-Site IPSec sin requerir la construcción de adaptadores ESB adicionales. El Gateway actúa como capa de exposición y gobierno sobre los servicios existentes del bus, los cuales son consumidos con sus protocolos nativos. La transformación de formatos (RF_019) se gestiona mediante policies de transformación del Gateway cuando aplica. La creación de un ESB o middleware adicional no aplica contractualmente. *Imagen 11*

RF_005	- La plataforma debe incluir un **Bus de Integración de Mensajes (MOM)** para integrar diferentes sistemas usando protocolos estándar como **JMS (Java Message Service)** o **AMQP**.	No aplica contractualmente
RF_006	Autenticación y Autorización** - **OAuth 2.0 / OpenID Connect**: La plataforma debe ser capaz de manejar autenticación con OAuth 2.0 para APIs RESTful. Además, debe poder integrar soluciones de **Single Sign-On (SSO)** utilizando OpenID Connect para gestionar el acceso de usuarios en sistemas distribuidos.	Imagen 12 Imagen 13
RF_007	**Autenticación de Clientes (API Keys)**: Permitir que los clientes de las APIs se autentiquen mediante el uso de **API Keys** para restringir el acceso a recursos sensibles.	Imagen 14 Imagen 15 Imagen 16
RF_008	**Políticas de Acceso Granulares**: Definir políticas de autorización por usuario, rol, y recurso. Además, las políticas deben permitir la gestión de permisos para entornos específicos (desarrollo, staging, producción).	Imagen 17 Imagen 18 Imagen 19

RF_009	Seguridad de Comunicación** - **SSL/TLS**: Todos los tráficos hacia las APIs deben ser cifrados mediante SSL/TLS (con certificados de validación extendida). Las políticas deben permitir la revalorización periódica de certificados para prevenir vulnerabilidades.	Pendiente por parte de la FNA
RF_010	**Cifrado de Datos en Reposo**: Garantizar que todos los datos almacenados, especialmente aquellos sensibles como credenciales y tokens de acceso, sean cifrados utilizando estándares de la industria como AES-256.	Imagen 20 Imagen 21 Imagen 22
RF_011	Control de Tráfico (Rate Limiting y Throttling)** - **Limitación de tasa por API/Cliente**: La plataforma debe ser capaz de definir límites de tráfico (requests por minuto/por hora) a nivel de API o cliente. Este mecanismo de **Rate Limiting** debe permitir configuraciones tanto globales como específicas por endpoint.	Imagen 23 Imagen 24

RF_012	**Circuit Breaker**: Implementación de patrones de **circuit breaker** para prevenir sobrecargas y mantener la estabilidad del sistema frente a picos de tráfico inesperados.	Imagen 25 Imagen 26 Imagen 27 Imagen 28
RF_013	Auditoría y Monitoreo de Seguridad** - **Registros de Auditoría**: La plataforma debe generar logs detallados de acceso a las APIs, que incluyan la autenticación, la autorización, las acciones realizadas y los errores generados. Estos logs deben estar cifrados y ser fácilmente accesibles para auditorías.	Imagen 29 Imagen 30 Imagen 31 Imagen 32
RF_014	**Alertas de Seguridad**: Generación de alertas automáticas ante cualquier intento de acceso no autorizado o patrones de tráfico anómalos (ej. acceso excesivo desde una misma IP).	Imagen 33 Imagen 34
RF_015	Despliegue y Gestión de Entornos** - **CI/CD (Integración Continua / Despliegue Continuo)**: La plataforma debe integrarse con pipelines de CI/CD para facilitar la automatización de despliegues de APIs. Se debe permitir la integración con herramientas como Jenkins, GitLab CI, o Azure	No aplica contractualmente

	DevOps.	
RF_016	**Entornos Isolados**: La plataforma debe permitir crear entornos aislados para pruebas, staging, y producción, con mecanismos de propagación de cambios controlados.	Imagen 35 Imagen 36 Imagen 37
RF_017	Desactivación y Retiro de APIs** - La plataforma debe permitir la desactivación de versiones antiguas de una API sin interrumpir a los consumidores actuales. Esto se puede hacer mediante el uso de **políticas de deprecación** donde los consumidores sean notificados antes de la retirada definitiva.	Imagen 38 Imagen 39
RF_018	Compatibilidad con REST y SOAP** - **REST**: Debe ser compatible con la especificación **OpenAPI** (Swagger), permitiendo la importación y exportación de definiciones de API en formato YAML o JSON. - **SOAP**: Debe ser capaz de gestionar servicios web SOAP utilizando	Imagen 40 Imagen 41 Imagen 42

	WSDL para la definición de servicios y **XSD** para la validación de esquemas de datos.	
RF_019	Transformación de Datos** - **Mediadores de Transformación**: La plataforma debe ofrecer mediadores que permitan la conversión de formatos de datos, como **transformación de JSON a XML** o **XML a JSON**, para asegurar la interoperabilidad entre sistemas heterogéneos.	Imagen 43 Imagen 44 Imagen 45
RF_020	Soporte para Protocolos Adicionales** - **WebSockets y gRPC**: Además de REST y SOAP, la plataforma debe ser capaz de manejar comunicaciones bidireccionales en tiempo real mediante **WebSockets**, así como soportar **gRPC** para aplicaciones que requieran comunicaciones rápidas y eficientes en protocolos HTTP/2.	No aplica contractualmente
RF_021	Escalabilidad Horizontal** - **Escalabilidad Dinámica**: La plataforma debe ser capaz de escalar horizontalmente, permitiendo la adición de nodos	Imagen 46 Imagen 47

	adicionales para manejar el aumento de carga, sin requerir tiempo de inactividad.	
RF_022	**Microservicios**: La plataforma debe estar basada en una arquitectura de microservicios que permita distribuir los servicios y las responsabilidades, asegurando que el rendimiento no se vea afectado a medida que crece el volumen de tráfico.	No aplica contractualmente El API Manager internamente está basado en microservicios, pero no se construyen microservicios para el FNA
RF_023	Alta Disponibilidad** - **Clústeres y Failover**: Debe ser posible configurar clústeres de servidores con capacidades de failover automático. En caso de que un nodo falle, otro nodo debe tomar el control de manera transparente para los usuarios. **Despliegue Multizona**: Soporte para despliegues multizona (distribuidos geográficamente) para asegurar que la plataforma continúe funcionando incluso si un centro de datos falla.	*Imagen 48*

Tabla 29. Matriz de cumplimiento de requerimientos funcionales (RF_001–RF_023).

13.2. Requerimientos técnicos

Las siguientes matrices consolidan el cumplimiento de los requerimientos técnicos del Anexo 1, organizados por componente de la plataforma.

13.2.1. API Gateway

ID REQ	Descripción	
RT_001	El **API Gateway** será el componente central que manejará el enrutamiento de solicitudes, autenticación, autorización, control de acceso, transformación de datos, y logging de todas las interacciones hacia y desde las APIs. Es el primer punto de contacto para las solicitudes externas e internas. **Características Clave**: - **Rendimiento**: Debe ser capaz de manejar grandes volúmenes de tráfico, asegurando alta disponibilidad y baja latencia. - **Seguridad**: Implementación de autenticación y autorización, incluyendo OAuth 2.0, API keys, JWT (JSON Web Tokens), y protección contra ataques comunes (DDoS, inyección SQL, etc.). - **Escalabilidad**: Soporte para el escalado horizontal (agregar más instancias de API Gateway en función de la carga) y balanceo de carga automático. - **Logging y Monitoreo**: Integración con herramientas de	Todas las configuraciones se gestionan desde el API Manager, que se encarga de exponer el Gateway. *Imagen 1* *Imagen 2* Imagen 12 Imagen 13 Imagen 46 Imagen 47 Imagen 29 Imagen 30 Imagen 31 Imagen 32

	logging (como **ELK Stack**, **Splunk**) y monitoreo (como **Prometheus**, **Grafana**).	
RT_002	**Enrutamiento dinámico de tráfico**: El gateway debe enrutar las solicitudes a diferentes servicios de API según reglas definidas.	Imagen 7 Imagen 8 Imagen 9 Imagen 10 *Imagen 49*
RT_003	**Control de tráfico**: Capacidad para gestionar límites de solicitud, tasas de acceso, y cuotas para evitar abusos del sistema.	Imagen 23 Imagen 24

RT_004	**Transformación de contenido**: Capacidad para modificar o transformar las solicitudes y respuestas, como reescribir cabeceras o cuerpos de solicitud en función de diferentes protocolos.	Imagen 43 Imagen 44 Imagen 45
RT_005	**Gestión de políticas**: Implementación de políticas para autenticación, autorización, monitoreo, control de acceso, etc.	Imagen 17 Imagen 18 Imagen 19

Tabla 30. Cumplimiento de requerimientos técnicos — API Gateway.

13.2.2. Microservicios y contenedores

ID REQ	Descripción	
RT_001	Para asegurar una arquitectura escalable y flexible, cada servicio debe ser independiente, aislado, y fácilmente escalable. Los microservicios serán implementados en contenedores **Docker**, lo que permite la portabilidad y la rápida gestión de versiones.	Los microservicios que componen la plataforma de API Manager (Gateway, Management API, Management UI, Portal API, Portal UI, MongoDB, Redis, Elasticsearch) están desplegados como contenedores independientes y aislados en AWS EKS, el cual utiliza containerd como runtime de contenedores, estándar en Kubernetes moderno. Cada componente opera en su propio pod con recursos configurados de forma independiente. Contractualmente, el alcance de este requerimiento se limita exclusivamente a la implementación y componentes asociados a la plataforma API Manager. *Imagen 50*

RT_002	**Escalabilidad**: Cada microservicio puede escalar de manera independiente según la demanda, manteniendo una arquitectura eficiente y ágil.	Cada componente de API MANAGER puede escalar de forma independiente mediante HorizontalPodAutoscaler en Kubernetes *Imagen 51*
RT_003	**Independencia**: Los microservicios deben ser autónomos, y cada uno manejará un conjunto específico de funciones (como autenticación, facturación, gestión de usuarios, etc.).	Los componentes de api manager operan de forma autónoma: el Gateway maneja el tráfico de APIs, la Management API gestiona la configuración, el Portal expone el catálogo a desarrolladores, y los servicios de datos (MongoDB, Redis, Elasticsearch) cumplen funciones específicas e independientes. Cada componente tiene su propio ciclo de vida, configuración y recursos dentro del clúster EKS *Imagen 50*
RT_004	**Automatización**: Integración con **CI/CD** (Integración Continua y Despliegue Continuo) para automatizar el ciclo de vida de los microservicios.	No aplica contractualmente
RT_005	**Orquestación con Kubernetes**: Utilizar **Kubernetes** como el sistema de orquestación de contenedores, que proporcionará características avanzadas de escalabilidad, recuperación ante fallos, balanceo de carga, y distribución de tráfico entre	*Imagen 48*

	instancias de microservicios.	

Tabla 31. Cumplimiento de requerimientos técnicos — Microservicios y contenedores.

13.2.3. Infraestructura y requisitos de software

ID REQ	Descripción	
RT_001	**Contenedores Docker**: - Docker debe estar instalado y configurado en cada nodo de la infraestructura.	La infraestructura desplegada sobre AWS EKS utiliza containerd como runtime de contenedores, estándar en Kubernetes moderno. Los nodos EC2 del clúster están configurados y activos con soporte completo de contenedores verificado mediante kubectl get pods. *Imagen 52*
RT_002	Todos los microservicios deben ser empacados en imágenes Docker, optimizando los recursos y asegurando su correcta ejecución.	Todos los componentes de la plataforma junto con sus servicios de datos (MongoDB, Redis, Elasticsearch) están desplegados como contenedores en el clúster AWS EKS. Todos en estado Running en los tres ambientes (TEST/CERT/PROD). *Imagen 50*
RT_003	Uso de **Docker Compose** o **Helm Charts** para la gestión de múltiples servicios y su configuración en entornos de desarrollo o producción.	La gestión de los componentes de la plataforma se realiza mediante manifiestos Kubernetes versionados desplegados sobre AWS EKS. *Imagen 50*

RT_004	**Kubernetes** proporcionará la orquestación para la infraestructura de contenedores, asegurando que los microservicios sean distribuidos, escalados y gestionados correctamente.	La orquestación de todos los contenedores se realiza mediante AWS EKS (Kubernetes gestionado). Componentes activos: AWS EKS Cluster, Amazon EC2 (nodos), Amazon EBS + CSI (almacenamiento persistente), Amazon ALB (balanceo de carga). *Imagen 48*
RT_005	Escalabilidad automática**: Kubernetes debe ser configurado para ajustar automáticamente el número de réplicas de los microservicios en función de la demanda de tráfico.	HorizontalPodAutoscaler configurado en los Deployments del Gateway. Escala réplicas automáticamente cuando el uso de CPU supera el 70%. AWS EKS Cluster Autoscaler aprovisiona nodos EC2 adicionales cuando los pods no encuentran capacidad disponible. Arquitectura Multi-AZ activa en us-east-1. *Imagen 51*
RT_006	**Recuperación ante fallos**: Kubernetes debe asegurarse de que los microservicios sean reiniciados en caso de fallos, y de que el tráfico sea redirigido a instancias saludables.	Kubernetes gestiona liveness y readiness probes en todos los pods. Ante fallo de un pod, Kubernetes lo reinicia automáticamente y el ALB lo retira del pool hasta que supere el readiness check. Mínimo 2 réplicas del Gateway en producción garantizan continuidad ante pérdida de un nodo. Rolling updates sin downtime configurados con rollback instantáneo disponible. *Imagen 48*
RT_007	**Gestión de Configuración**: Utilización de **ConfigMaps** y **Secrets** para gestionar configuraciones sensibles (como credenciales de base de datos, claves	Las credenciales y llaves de la plataforma están almacenadas en Kubernetes Secrets cifrados con KMS de AWS. AWS IAM controla los accesos de pods a recursos AWS siguiendo el principio de mínimo privilegio. Las API Keys son únicas y revocables individualmente. ConfigMaps

	API, etc.).	gestionan la configuración no sensible de los componentes del en los tres ambientes. *Imagen 53*

Tabla 32. Cumplimiento de requerimientos técnicos — Infraestructura y requisitos de software.

13.2.4. Bases de datos

ID REQ	Descripción	
RT_001	**API Gateway y Servicio de Middleware**: - **Descripción**: Para la integración con sistemas externos y legados, la plataforma debe ser capaz de manejar diferentes protocolos (HTTP/HTTPS, SOAP, JMS, AMQP, etc.). Para esto, se pueden utilizar tecnologías de middleware como **Apache Camel** o **MuleSoft ESB**, que permiten la integración y orquestación de diversos servicios y sistemas en una arquitectura distribuida.	La plataforma de API Manager gestiona el tráfico sobre protocolos HTTP/HTTPS y SOAP, conforme al alcance definido. Imagen 40 Imagen 41 Imagen 42

Tabla 33. Cumplimiento de requerimientos técnicos — Bases de datos.

13.2.5. Integración y adaptabilidad

ID REQ	Descripción	
RT_001	**API Gateway y Servicio de Middleware**: - **Descripción**: Para la integración con sistemas externos y legados, la plataforma debe ser capaz de manejar diferentes protocolos (HTTP/HTTPS, SOAP, JMS, AMQP, etc.). Para esto, se pueden utilizar tecnologías de middleware como **Apache Camel** o **MuleSoft ESB**, que permiten la integración y orquestación de diversos servicios y sistemas en una arquitectura distribuida.	La plataforma de API Manager gestiona el tráfico sobre protocolos HTTP/HTTPS y SOAP, conforme al alcance definido. Imagen 40 Imagen 41 Imagen 42

Tabla 34. Cumplimiento de requerimientos técnicos — Integración y adaptabilidad.

13.2.6. Adaptabilidad

ID REQ	Descripción	
RT_001	La solución debe ser **flexible** para poder integrarse con sistemas y aplicaciones existentes en la organización (CRM, ERP, bases de datos legacy, etc.).	La plataforma de API Manager provee la capa de exposición y gobierno sobre los servicios del bus existente del FNA, a través de las APIs definidas, sin requerir modificación de los sistemas backend. *Imagen 11*
RT_002	API First Design**: Se debe fomentar un enfoque de Desarrollo centrado en las APIs para garantizar que todos los servicios expuestos sean fácilmente accesibles y escalables.	La plataforma implementa un modelo de gobierno centralizado de APIs, habilitando cada servicio registrado, fomentando el diseño y consumo orientado a APIs. *Imagen 1*

RT_003	Estrategias de Migración**: Considerar un plan de migración progresivo desde sistemas legacy a soluciones basadas en API para evitar interrupciones en los servicios.	No aplica contractualmente

Tabla 35. Cumplimiento de requerimientos técnicos — Adaptabilidad.

13.3. Evidencias de cumplimiento

A continuación se presentan las evidencias de cumplimiento (Imagen 1 a Imagen 53) referenciadas en las matrices de las Secciones 13.1 y 13.2, organizadas por requerimiento.

1. **Requerimientos funcionales:**

RF_001

Imagen 1
UI consola de la solución api mánager

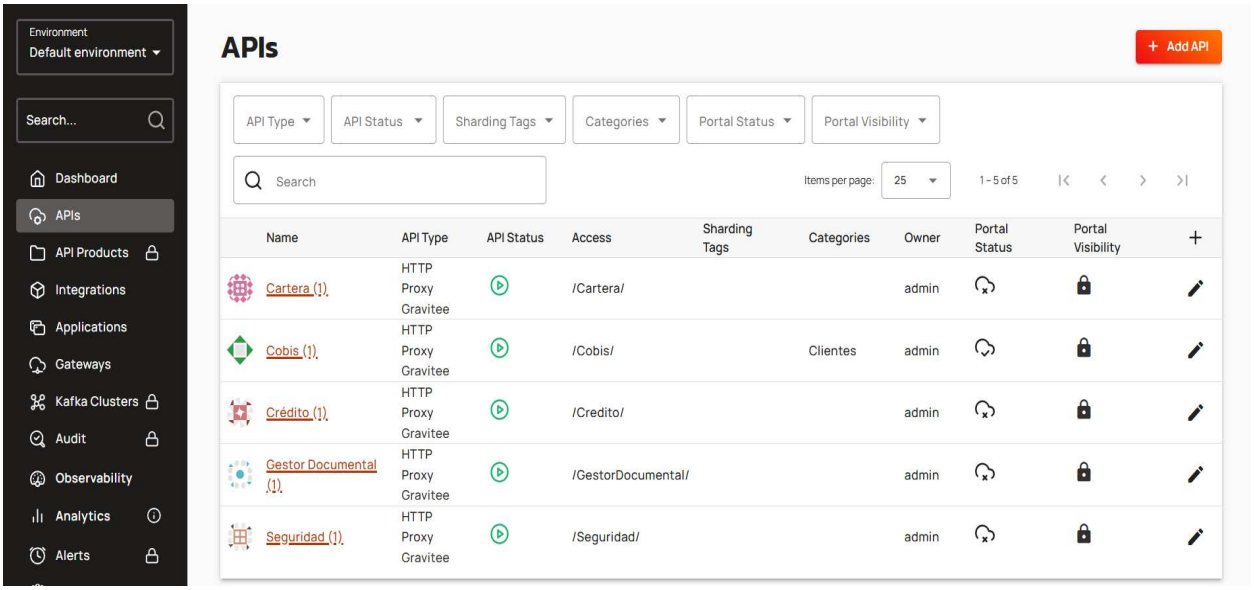
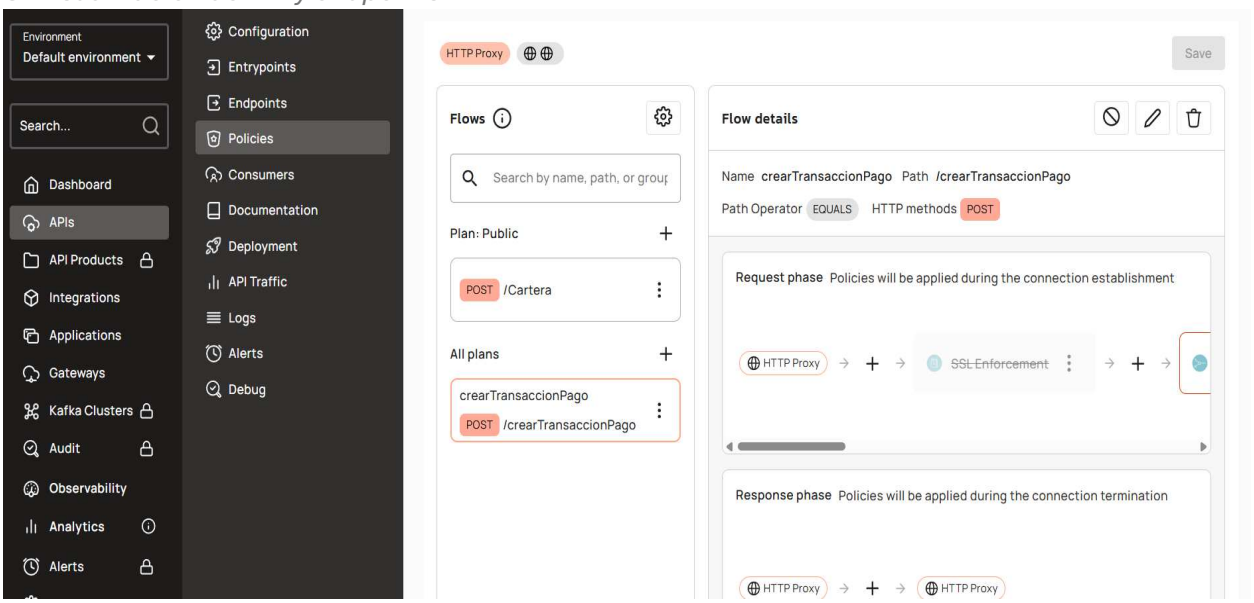


Imagen 2
UI Visualización de API y endpoints



RF_002

Imagen 3
UI Creación de versionado de API

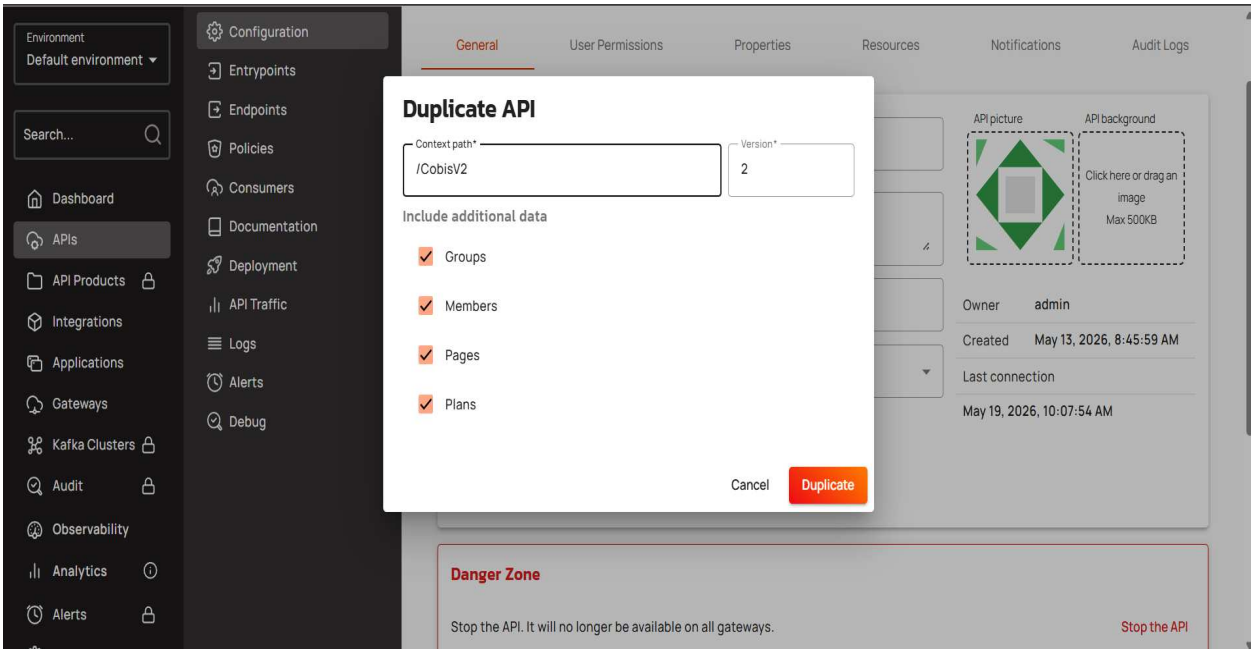


Imagen 4
UI Creación de versionado de API

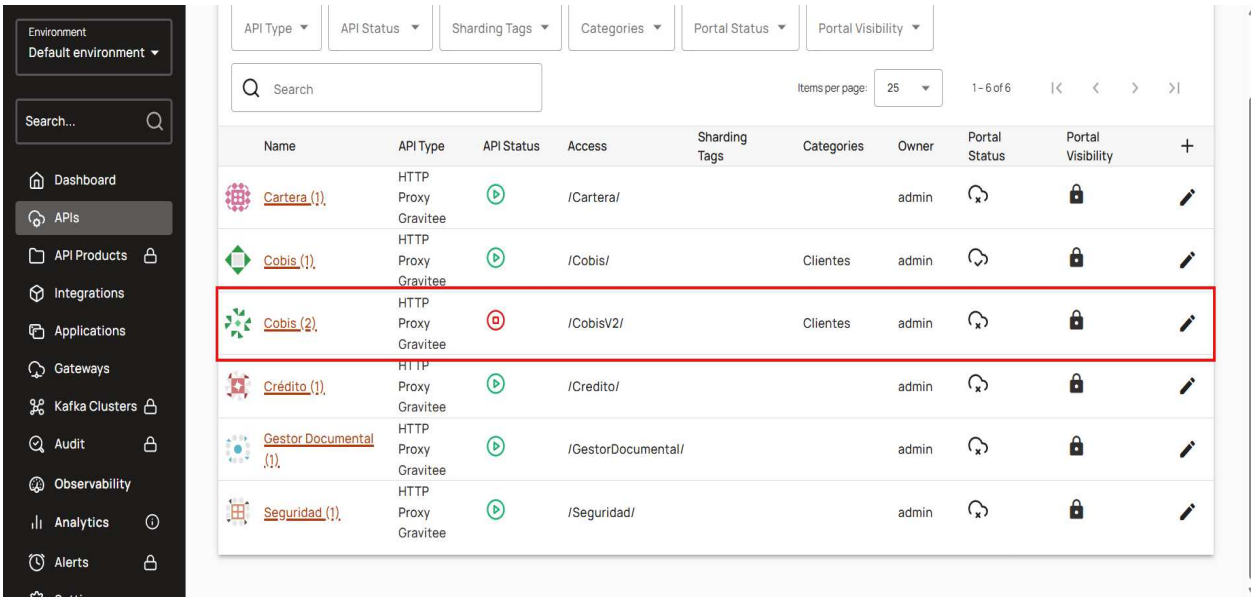


Imagen 5
UI Validación de versionado de API

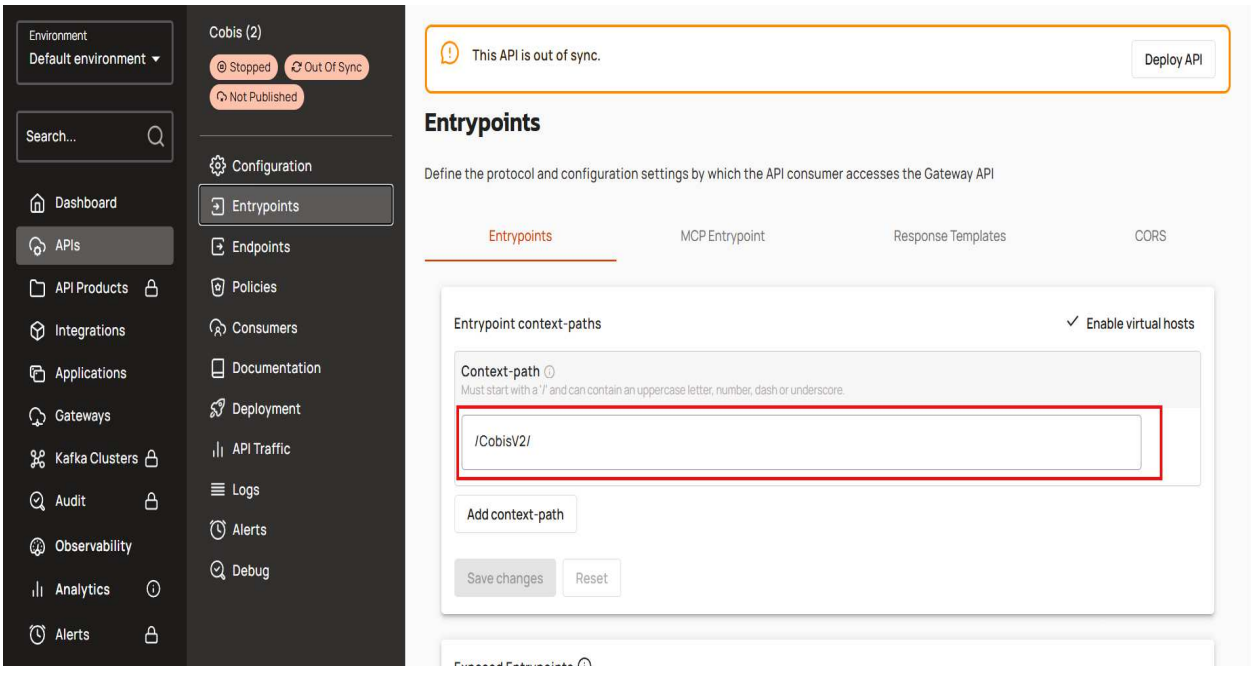


Imagen 6
UI Validación de políticas de versionado de API

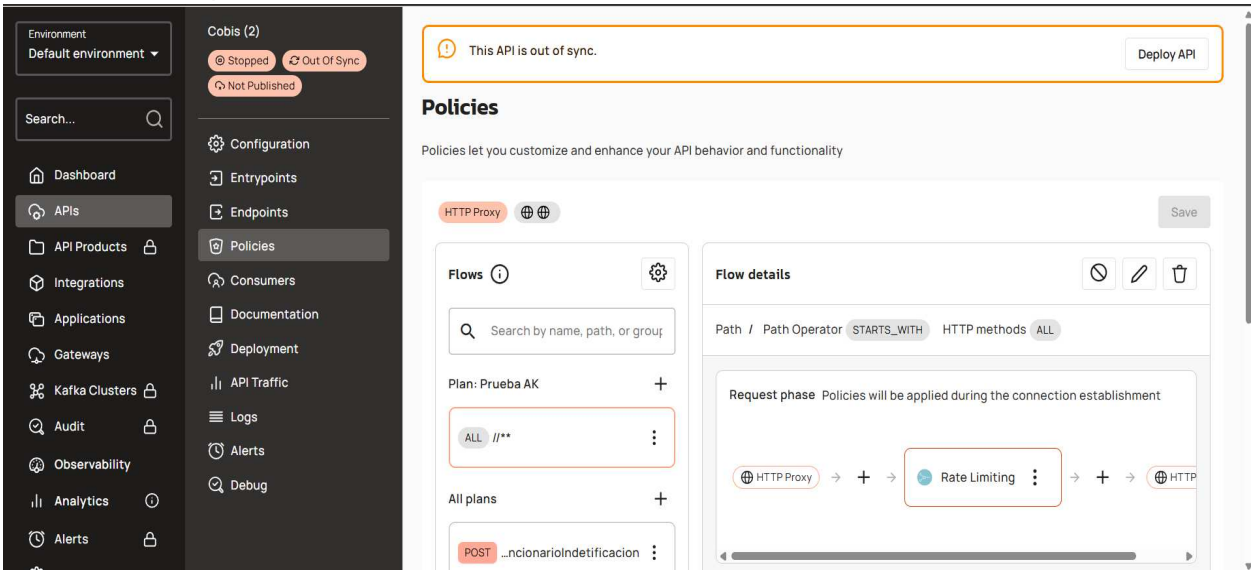


Imagen 7
UI Gestión de endpoints del API

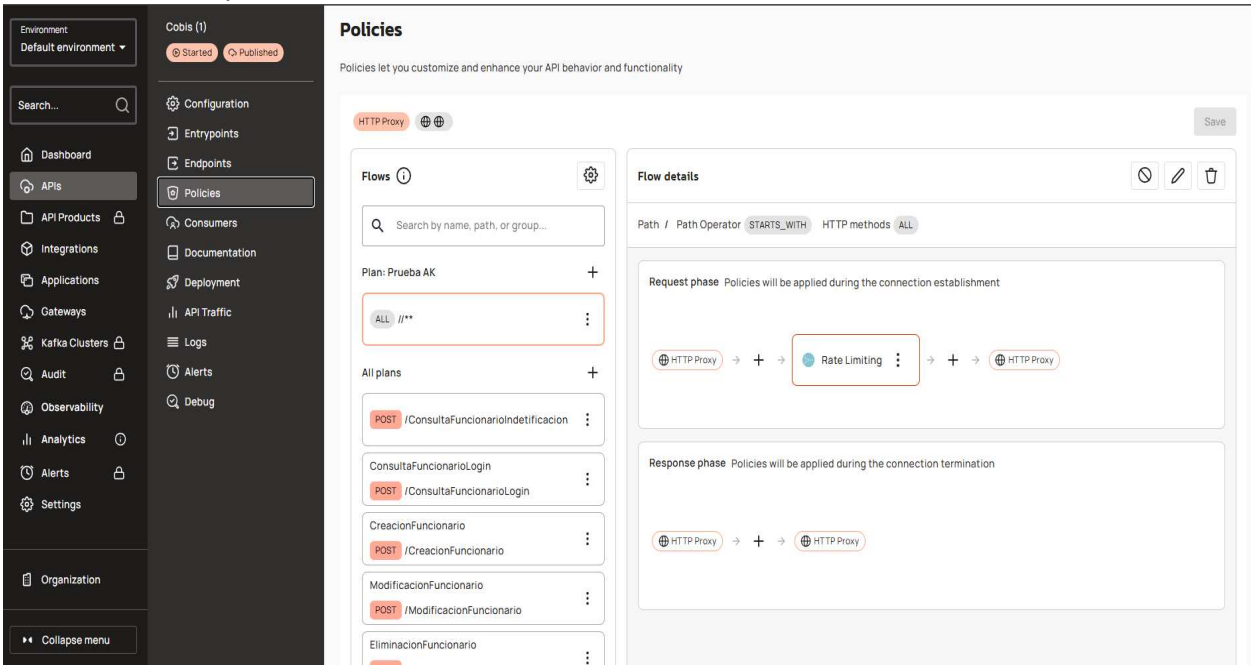


Imagen 8
UI Gestión de endpoints del API

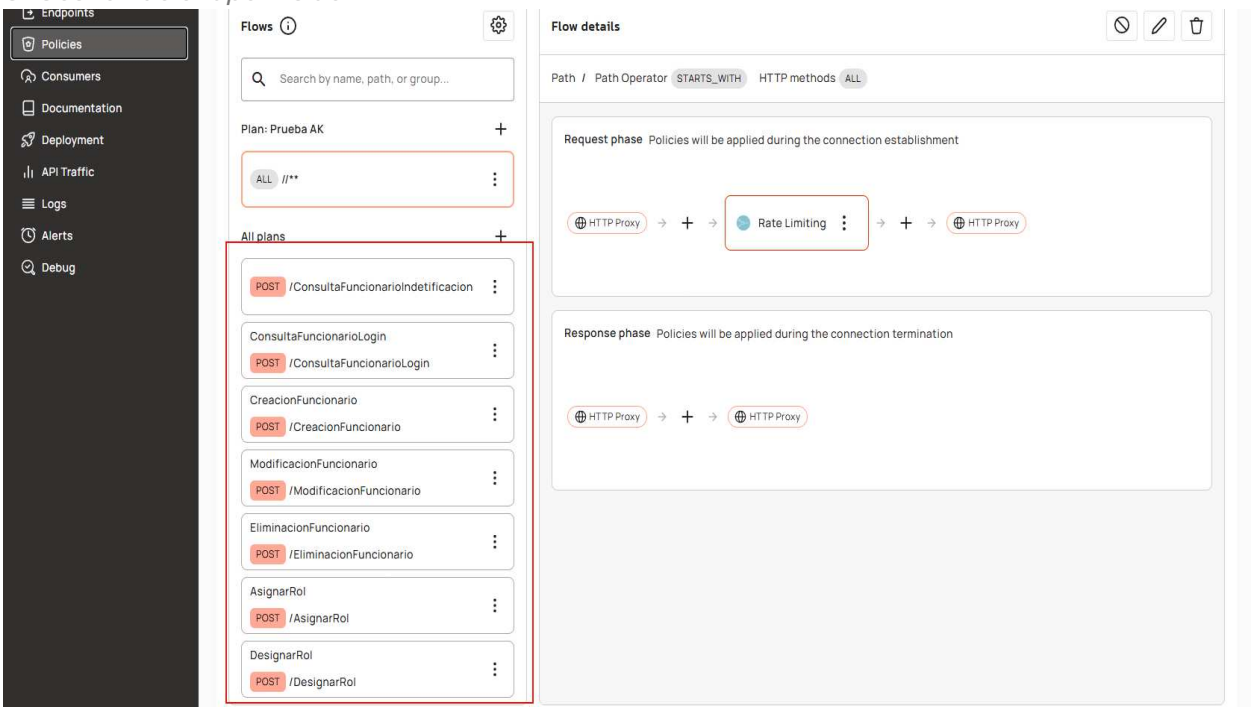


Imagen 9
UI Gestión de prefijo del API

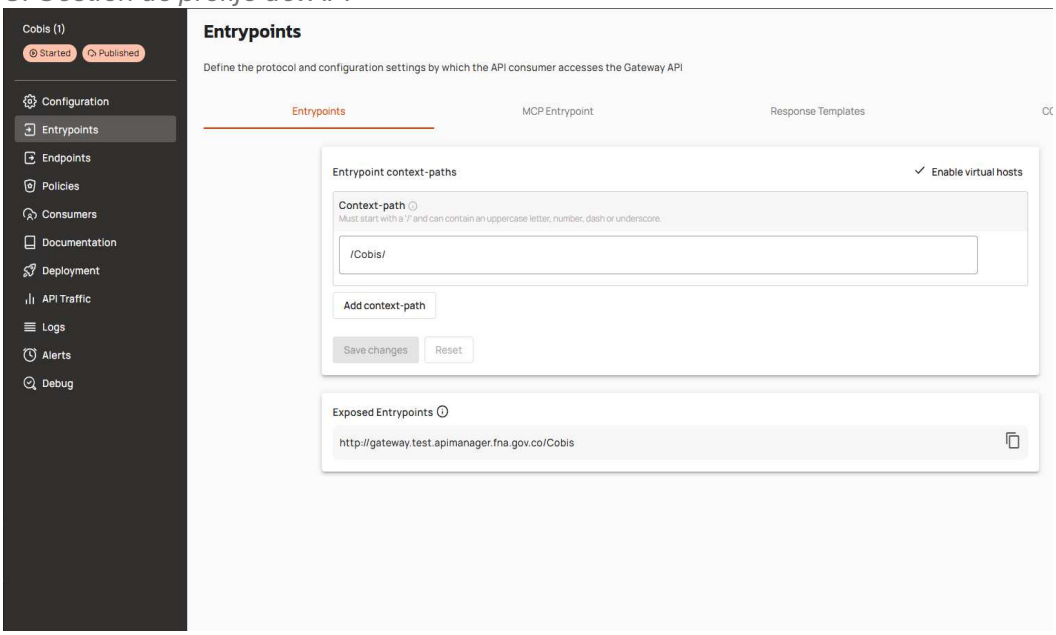
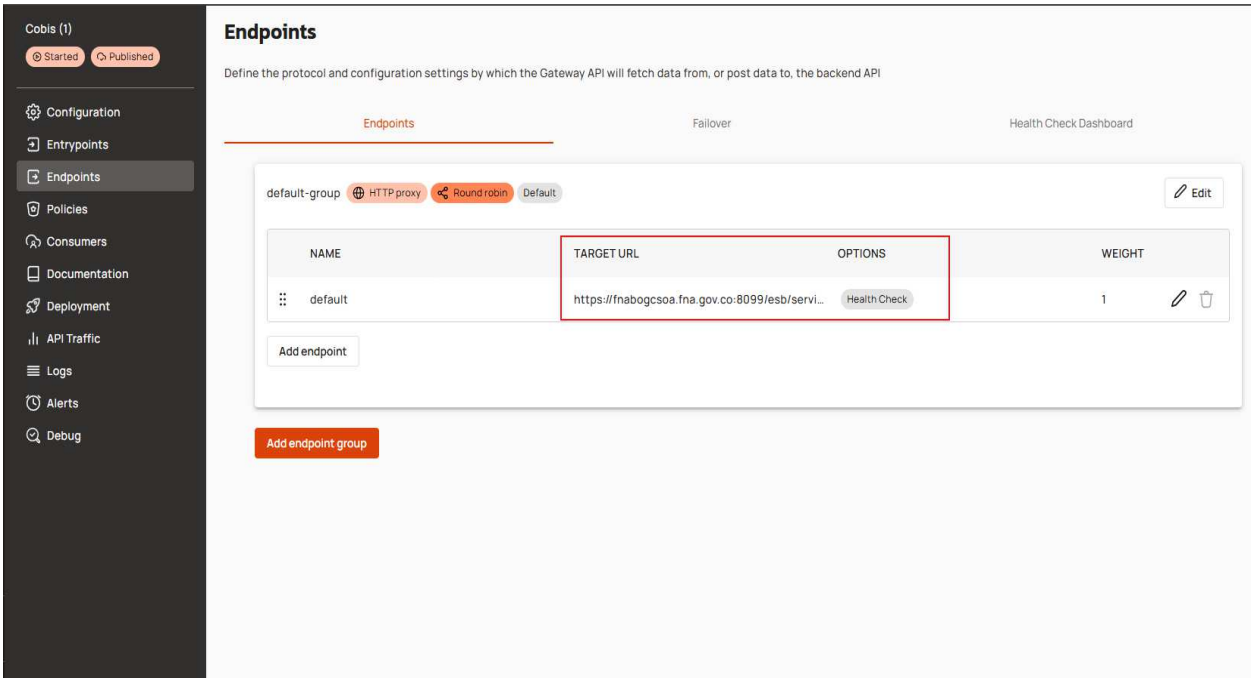
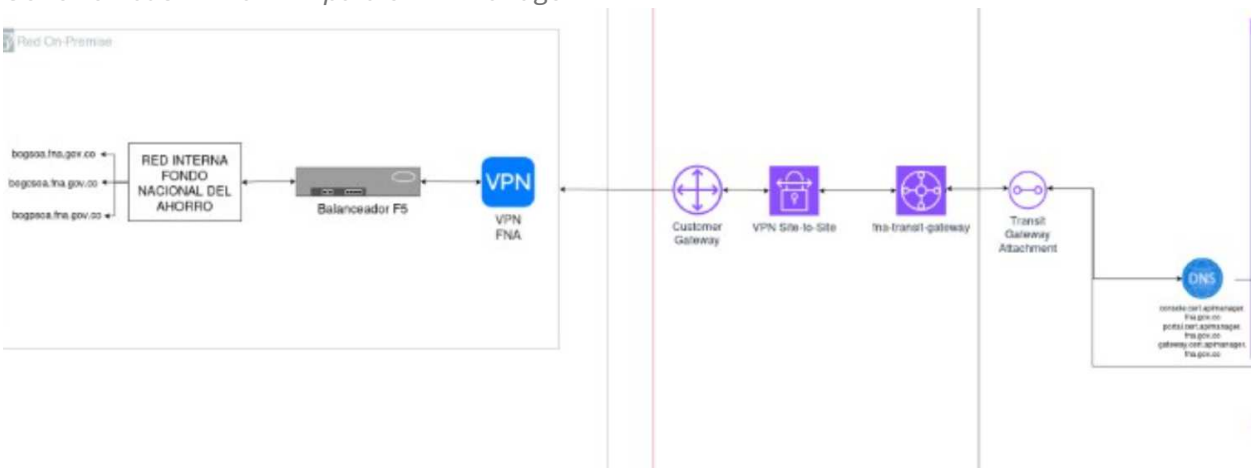


Imagen 10
UI Gestión de ambientes o backend del API



RF_004

Imagen 11
Conexión bus FNA a VPN para el API Manager



RF_006

Imagen 12
UI Gestión de planes mTLS, JWT, 0Auth2, API Key

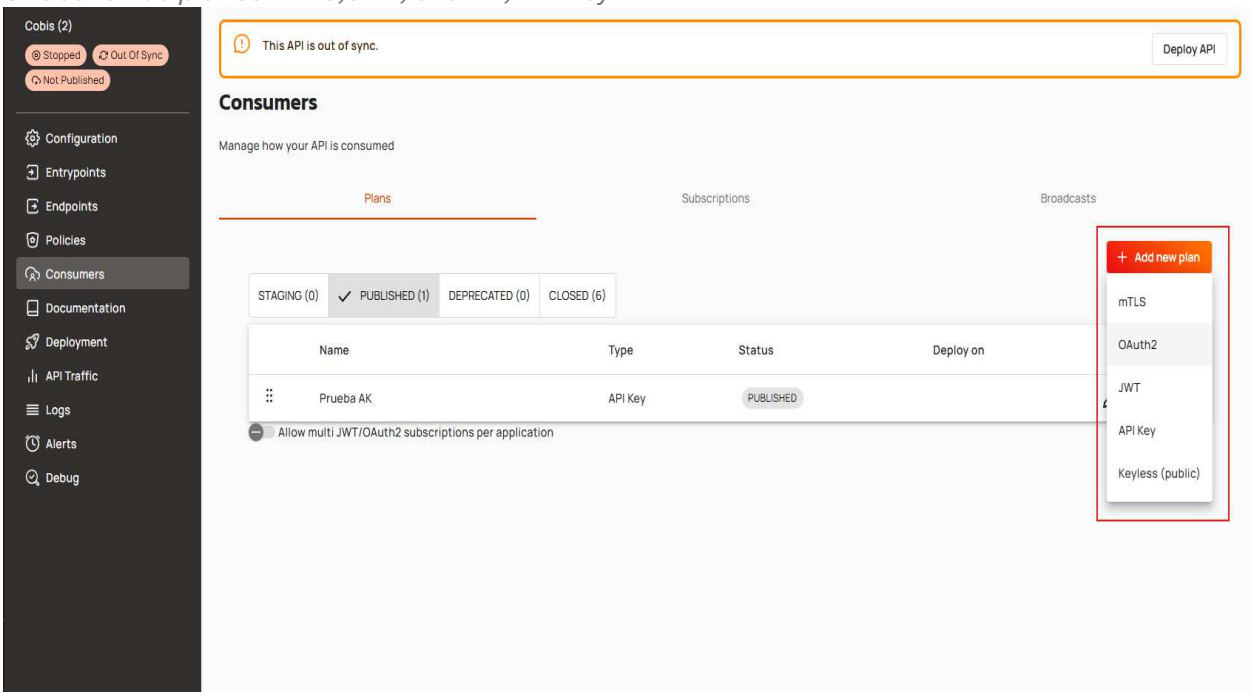
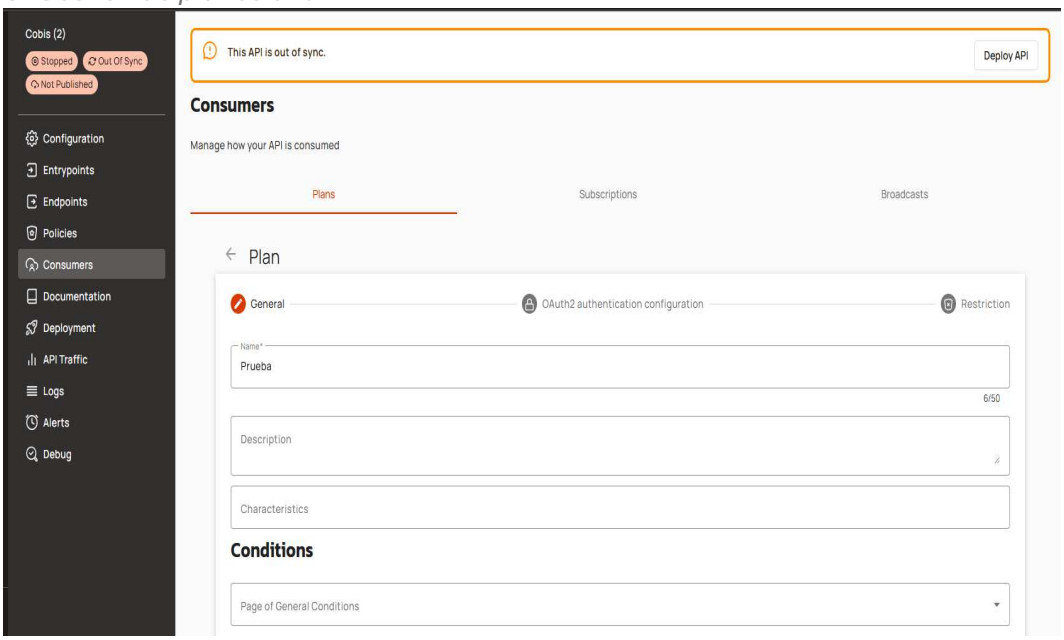


Imagen 13
UI Gestión de planes 0Auth2



RF_007

Imagen 14

UI Gestión de planes API Key por aplicaciones

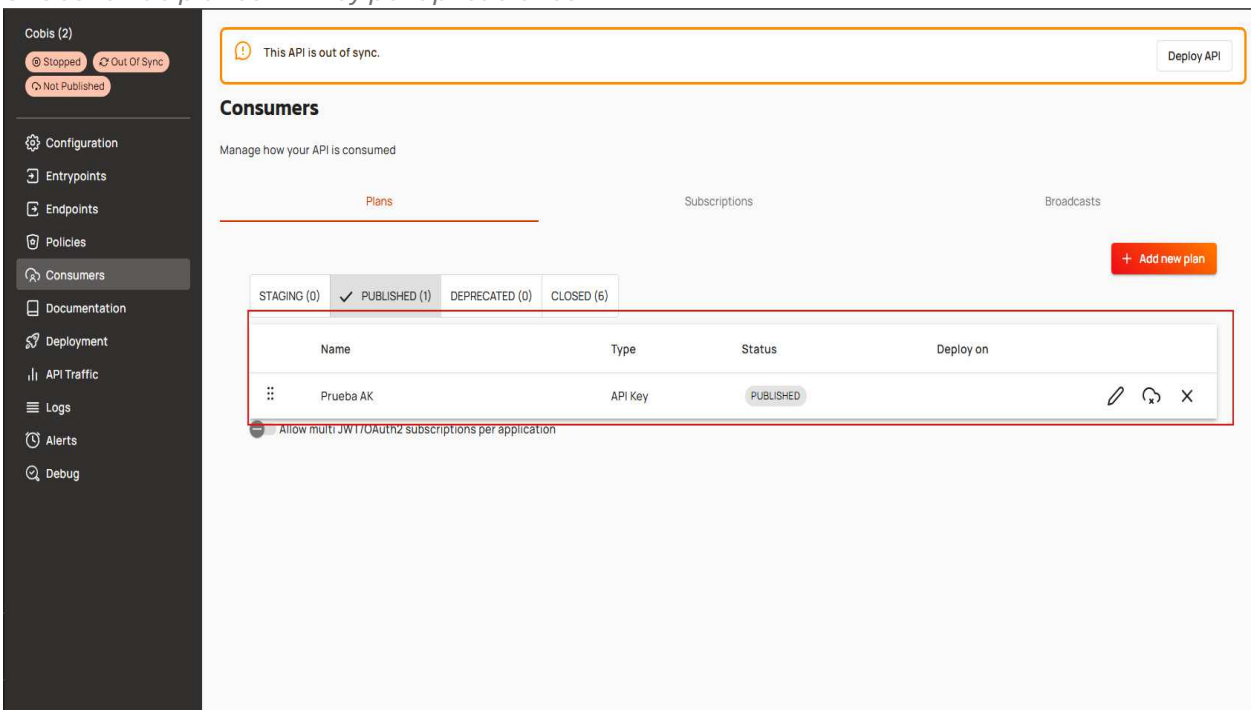


Imagen 15

UI Gestión de planes API Key por suscriptiones

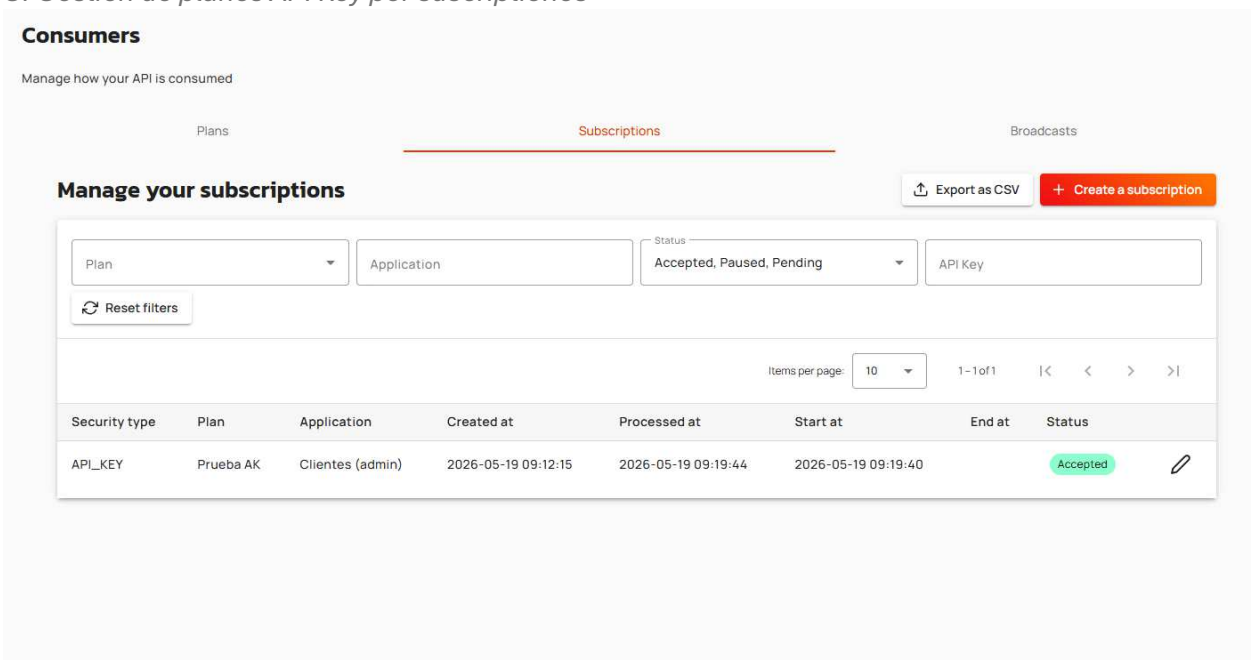
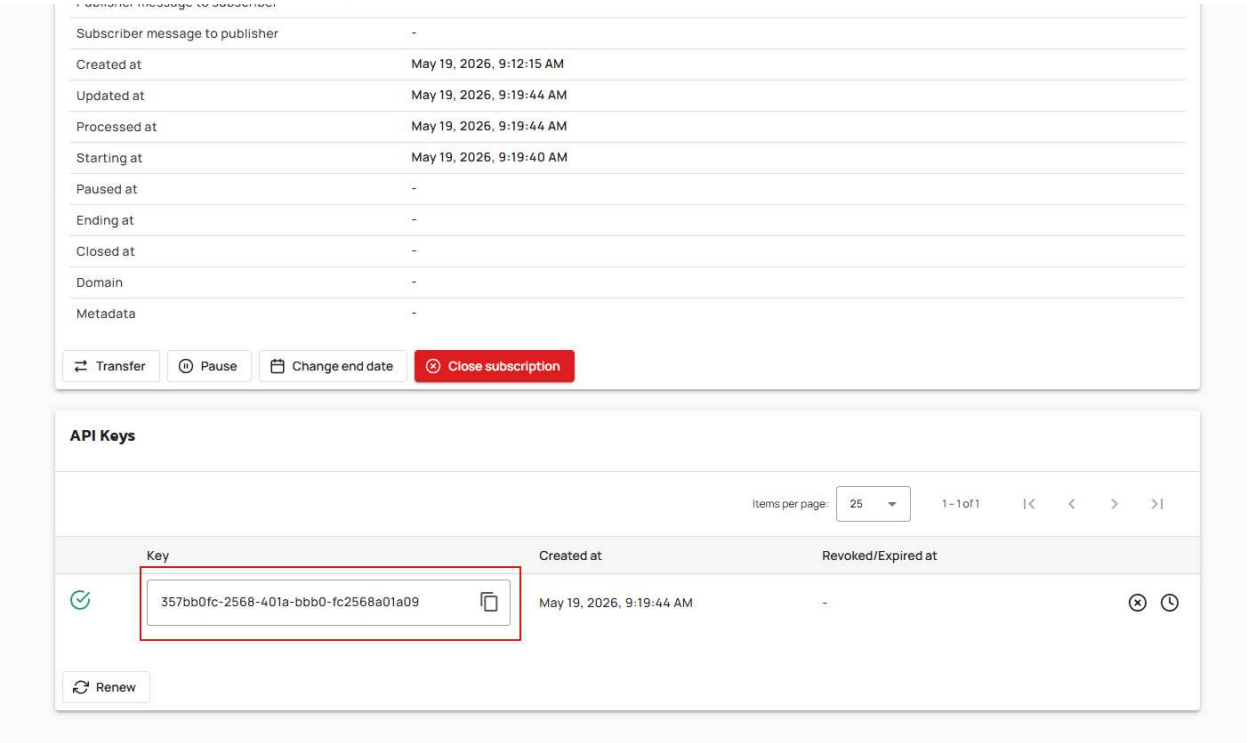


Imagen 16
UI Gestión de planes API Key value



RF_008

Imagen 17
UI Gestión de usuarios

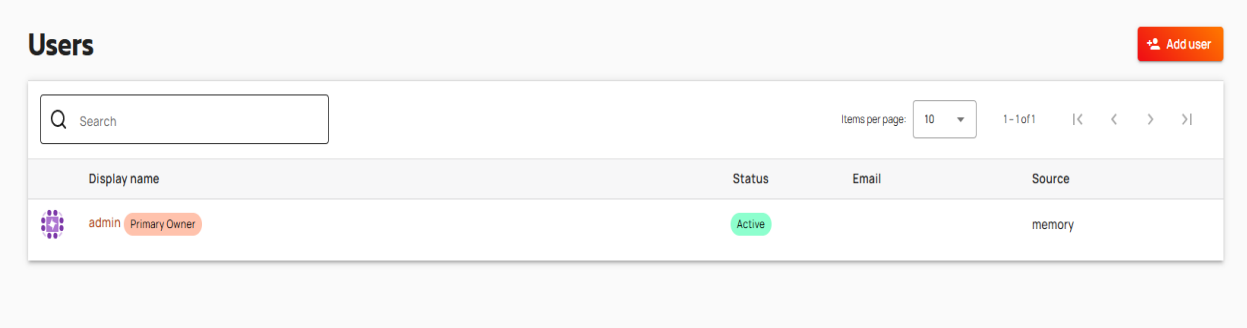


Imagen 18
UI Gestión de roles de usuarios

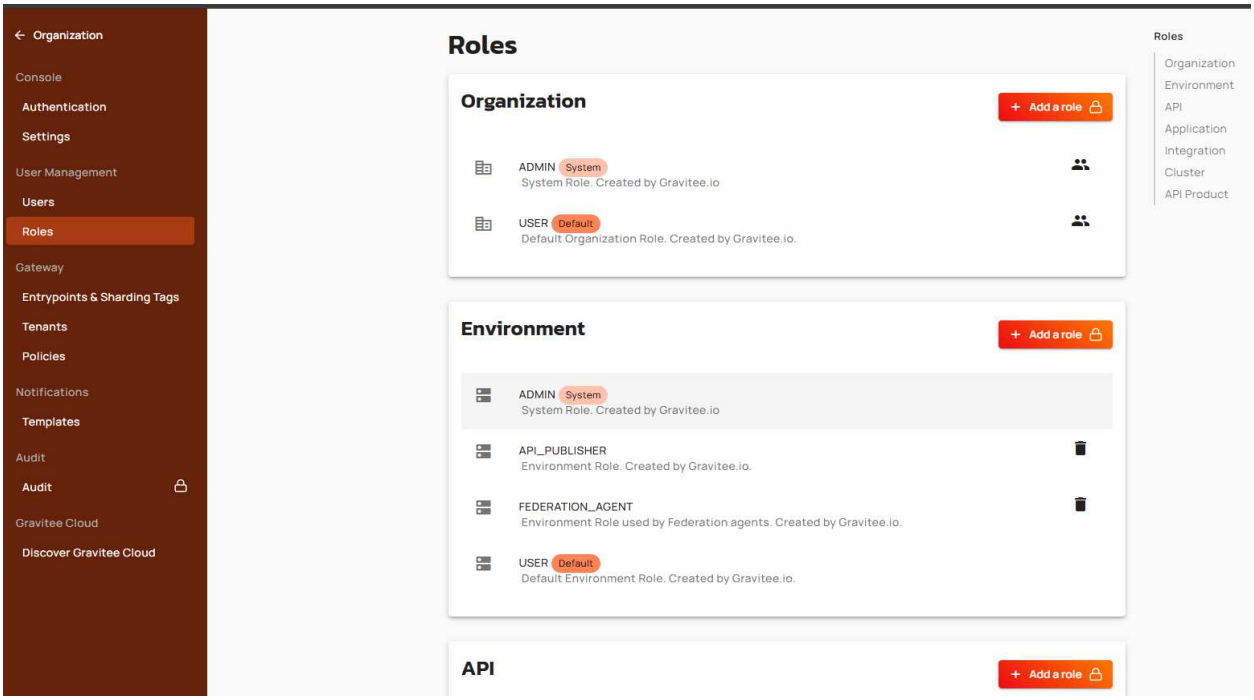
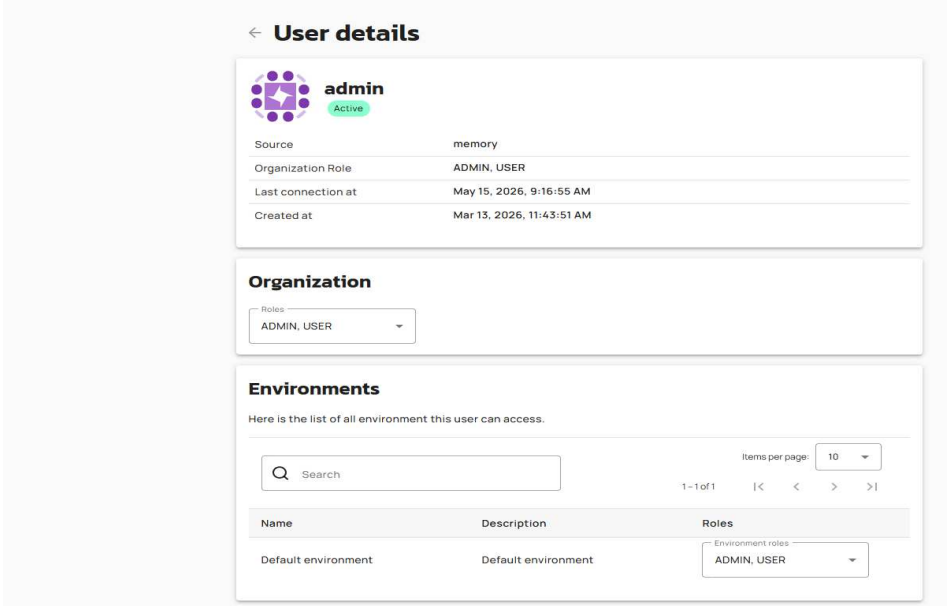


Imagen 19
UI Gestión de permisos por usuario



RF_010

Imagen 20
UI información de encriptación AWS OpenSearch

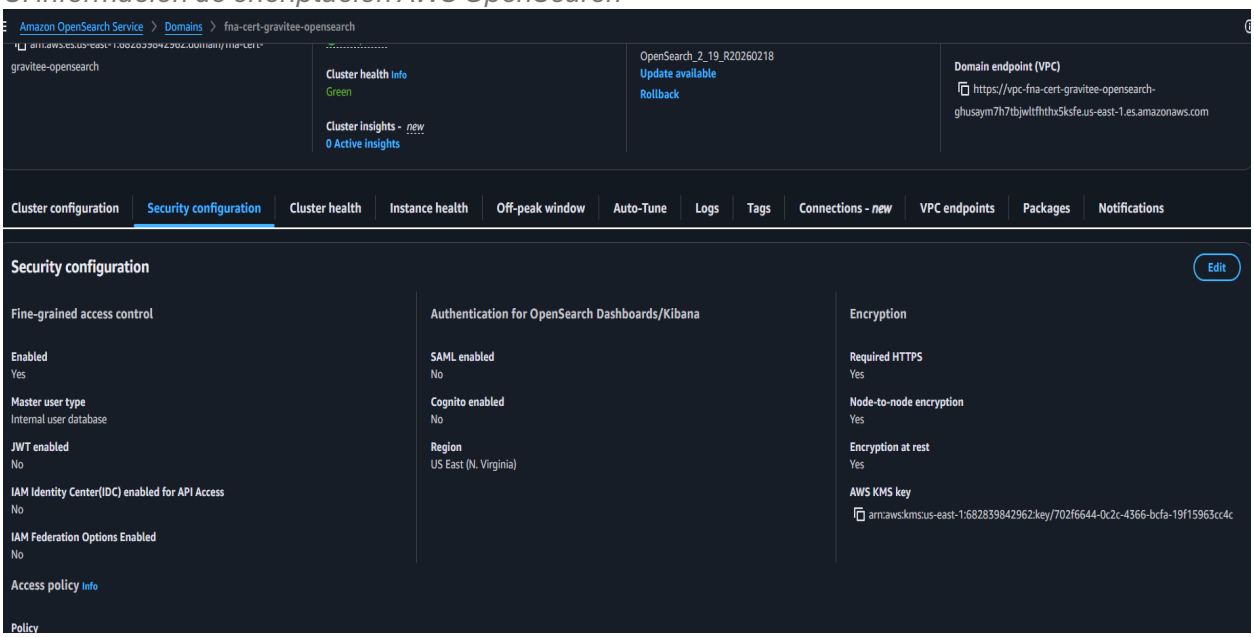


Imagen 21
UI información de encriptación en sitio AWS OpenSearch

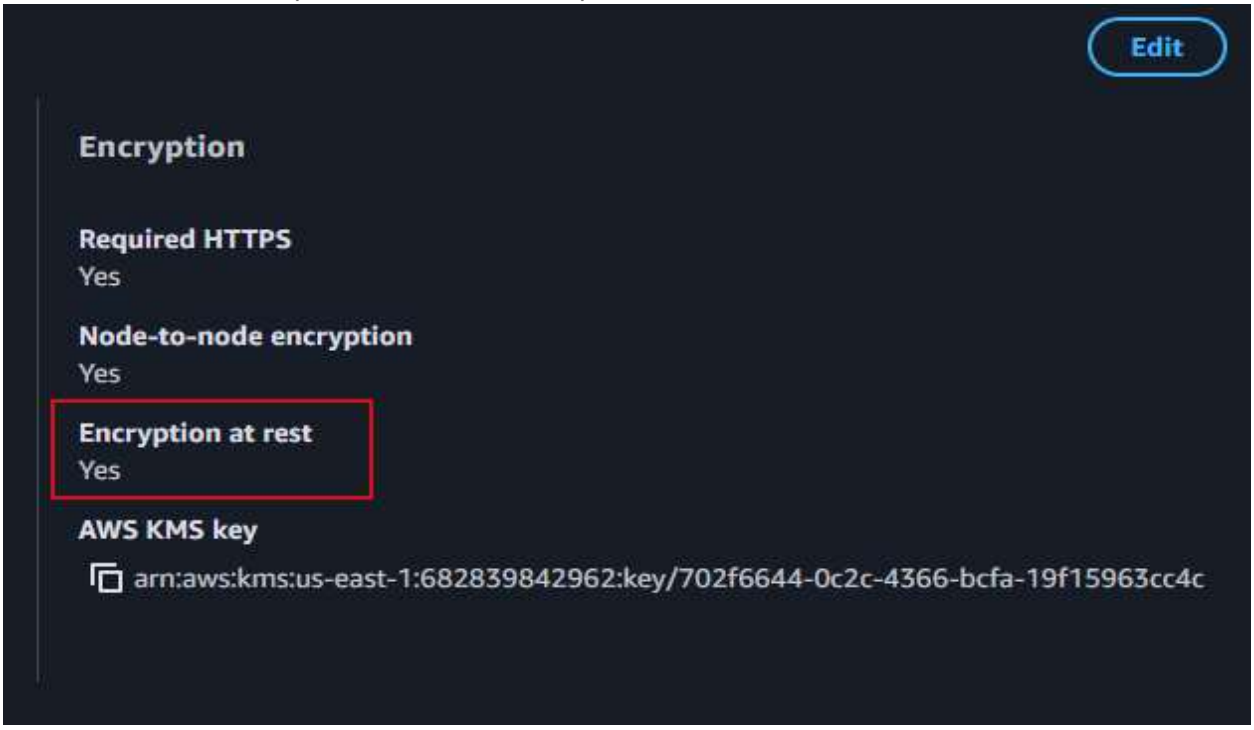
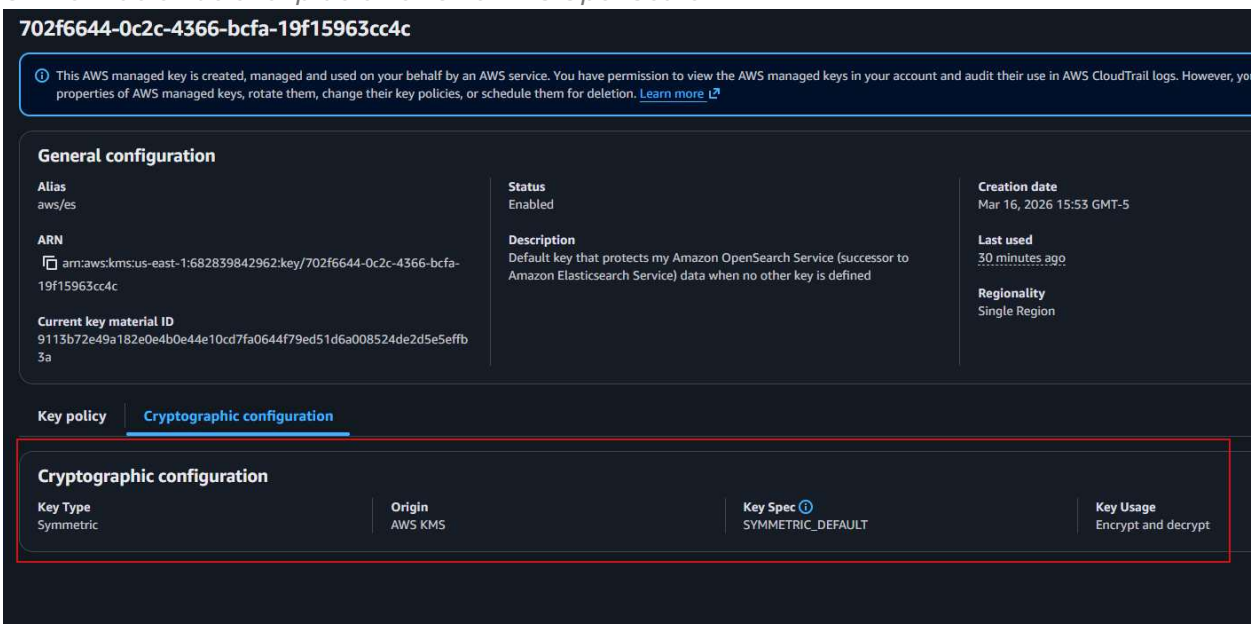


Imagen 22
UI información de encriptación en sitio AWS OpenSearch



RF_011

Imagen 23
UI manejo de rate limit por API y por endpoint con políticas

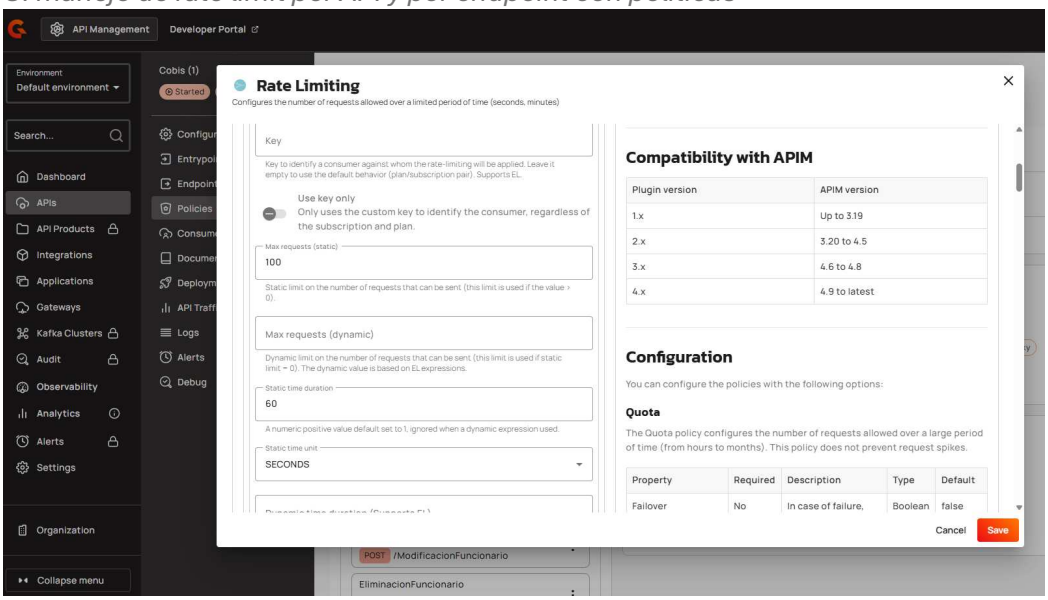
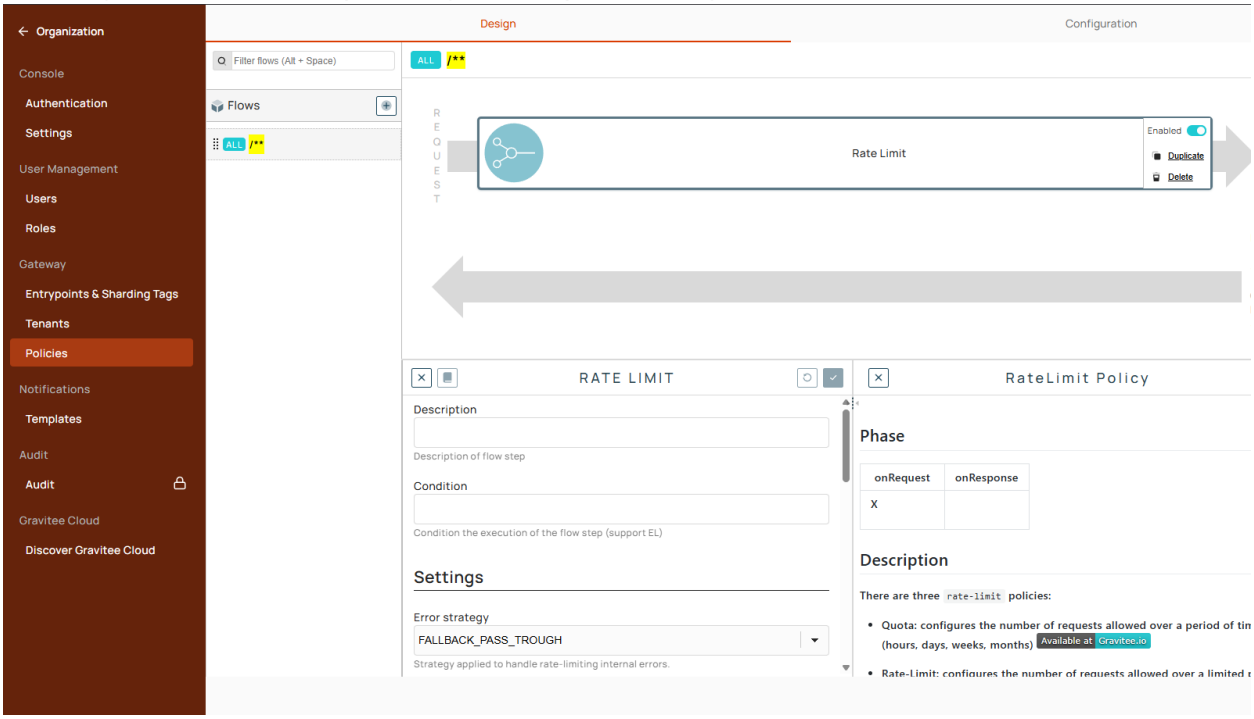


Imagen 24
UI manejo de rate limit con política global en panel de organización



RF_012

Imagen 25
UI activación y manejo de tolerancia a fallos

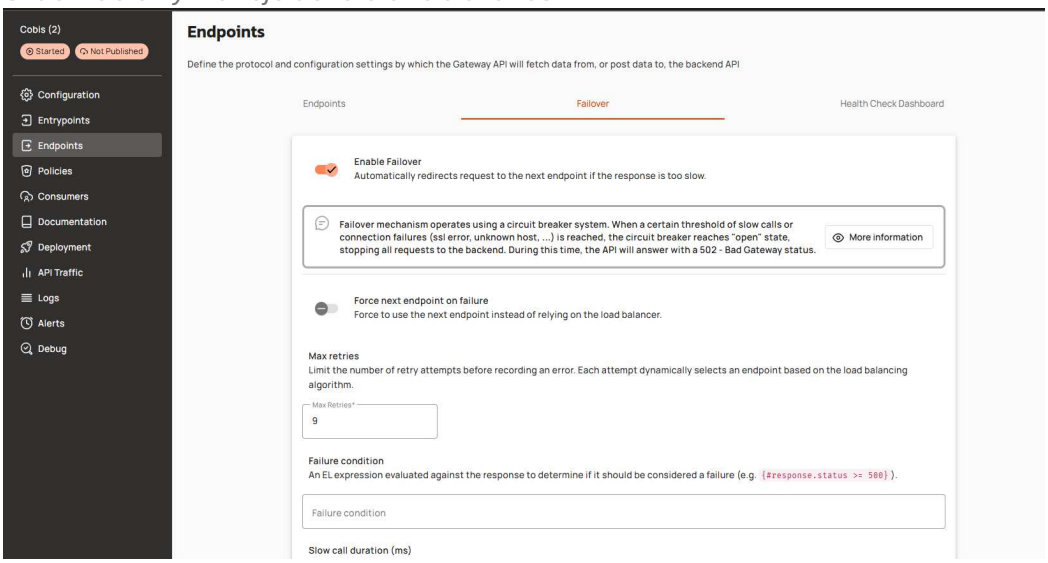


Imagen 26
UI configuración y manejo de tolerancia a fallos

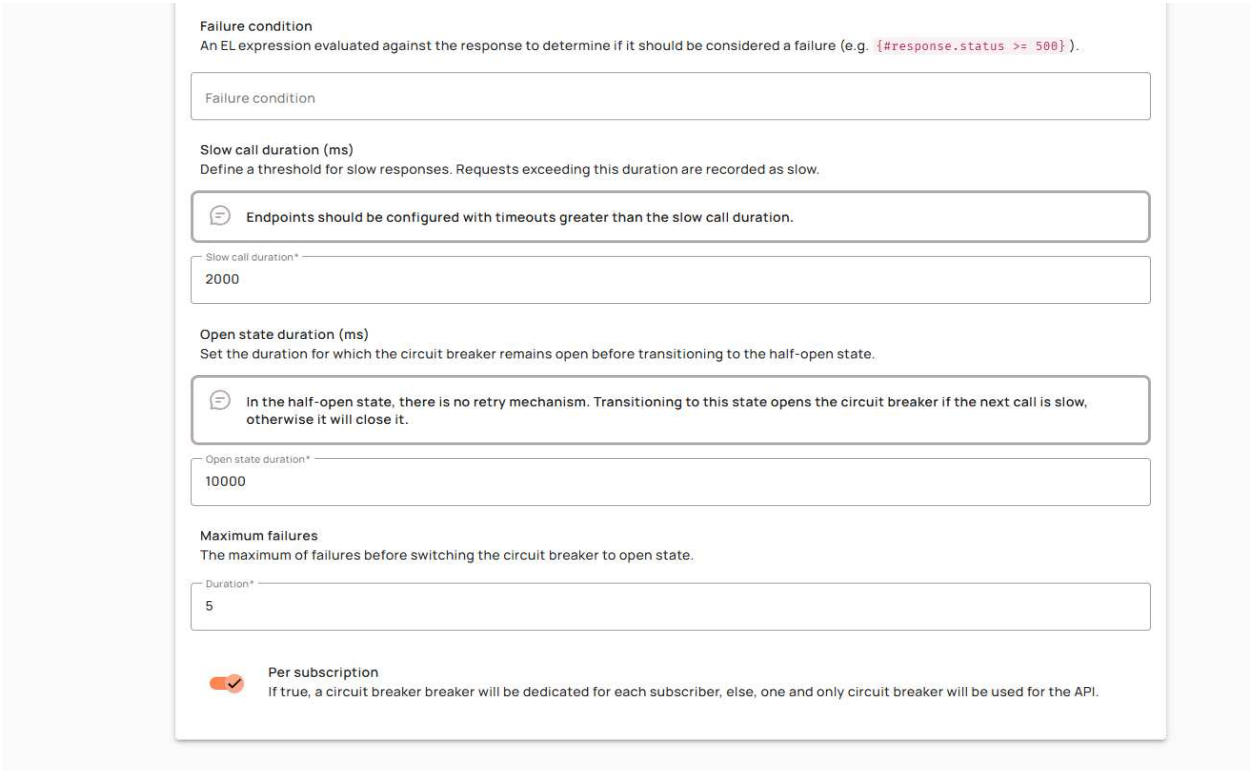


Imagen 27
UI configuración y manejo de tolerancia a fallos

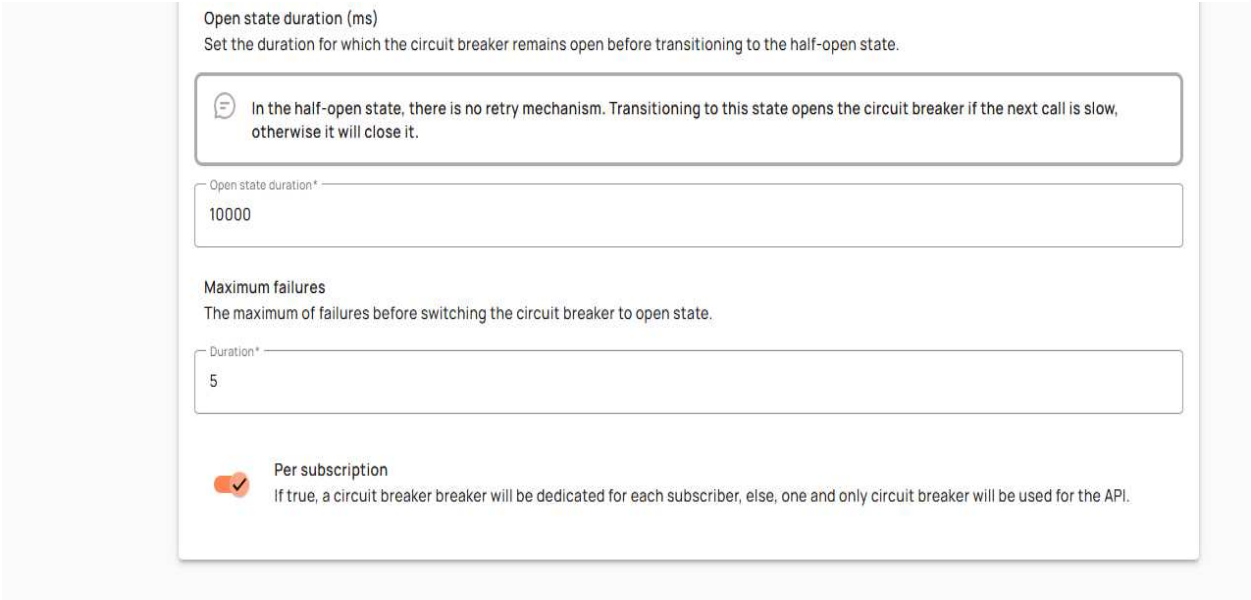
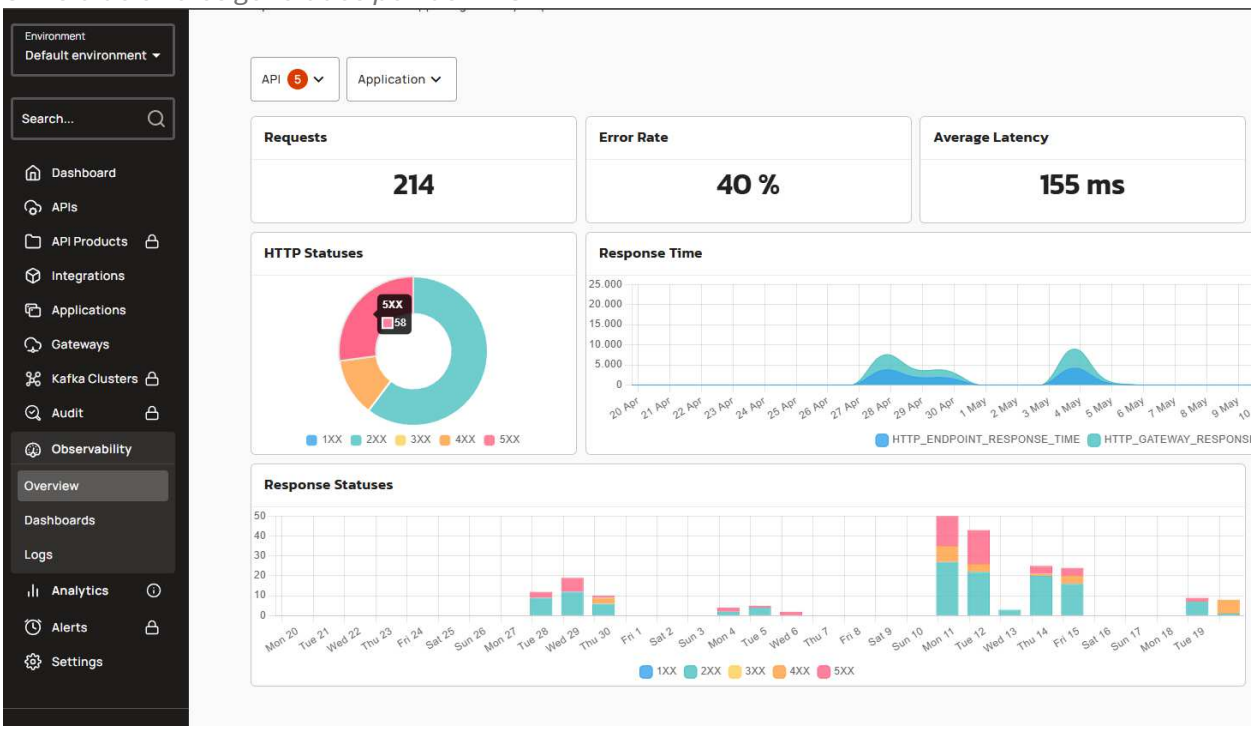


Imagen 28
UI vista de errores generados por las APIS



RF_013

Imagen 29
UI vista de logs generados por las APIS

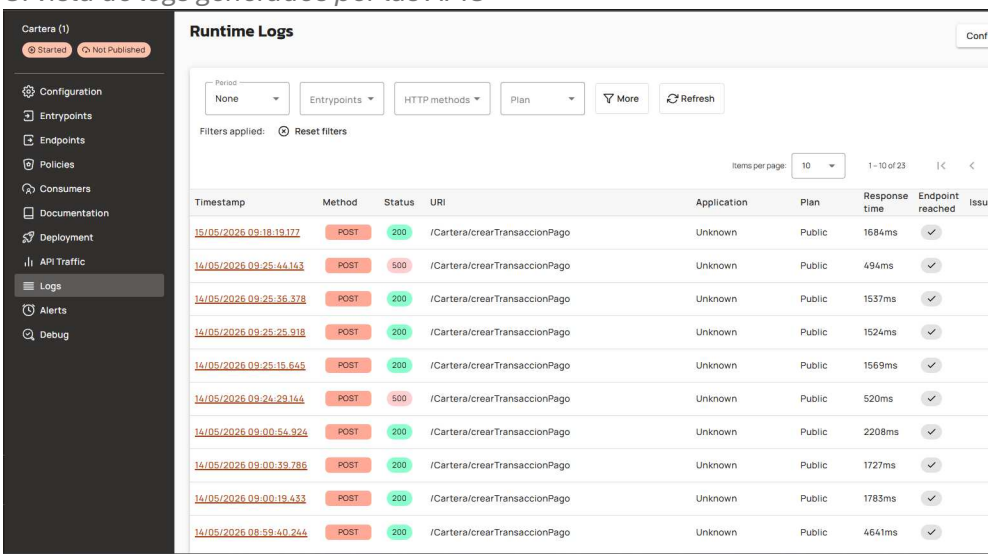


Imagen 30
UI vista de logs generados por las APIS

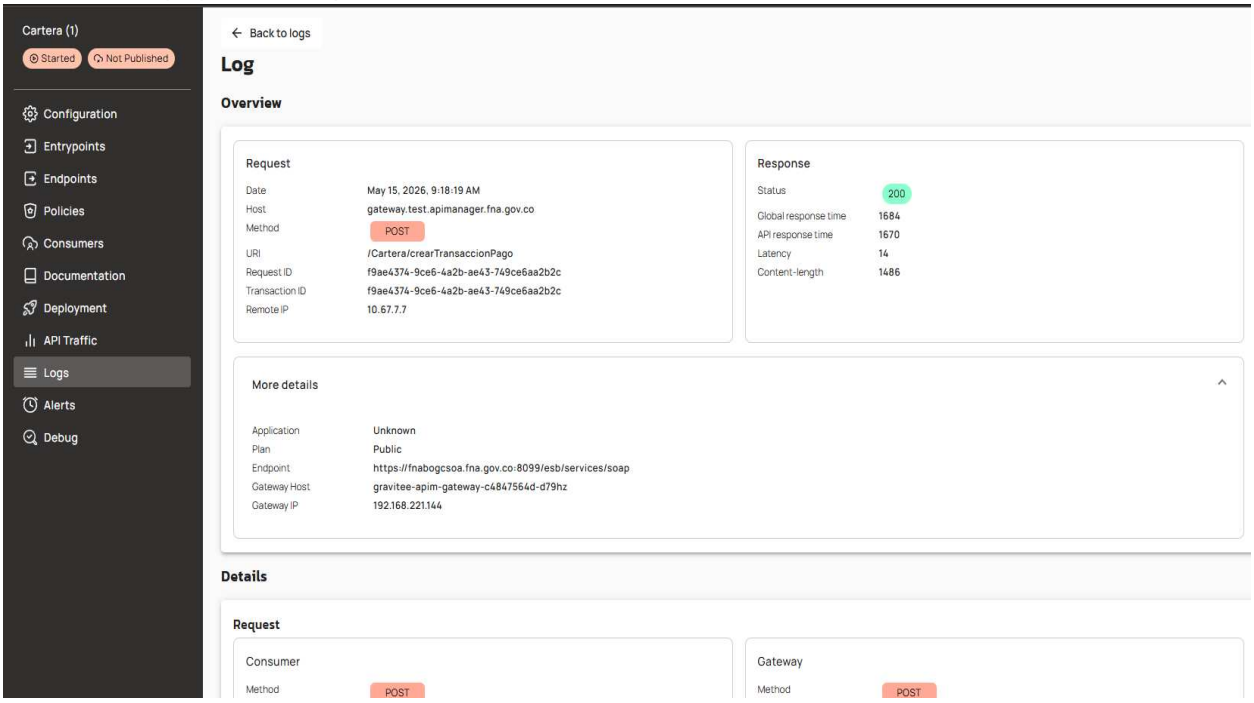


Imagen 31
UI vista de logs generados por las APIS

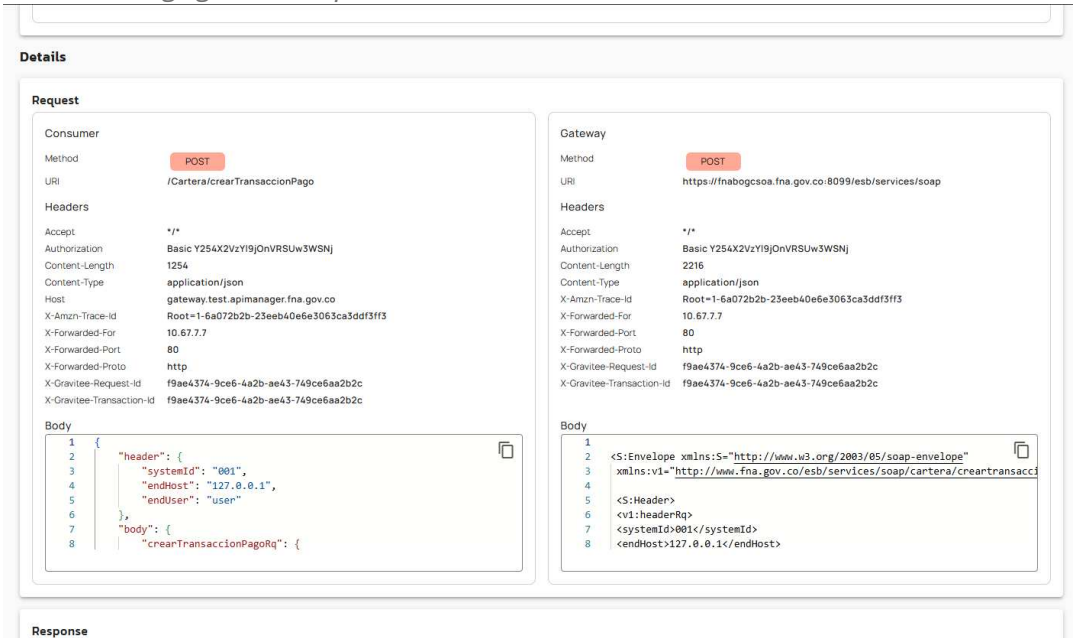
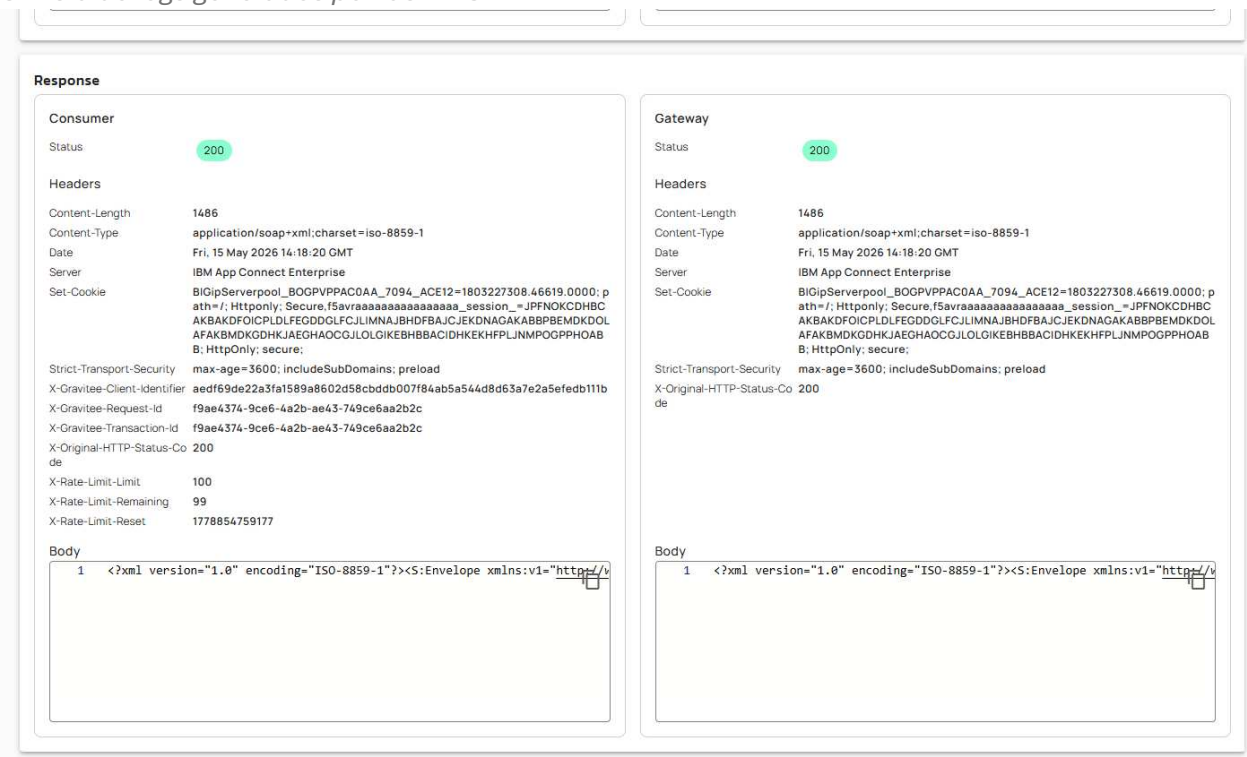


Imagen 32
UI vista de logs generados por las APIS



RF_014

Imagen 33
UI vista de alertas tipo de errores generados por API

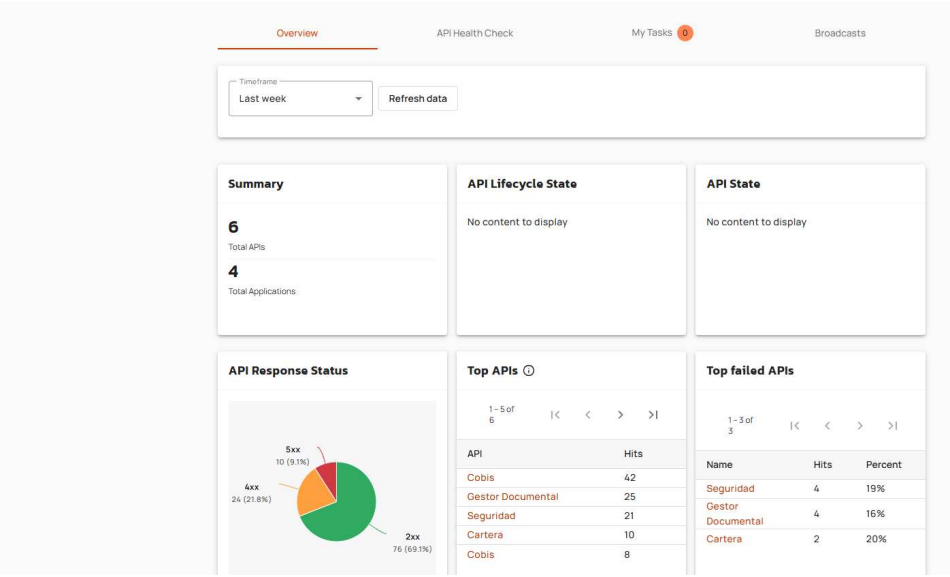
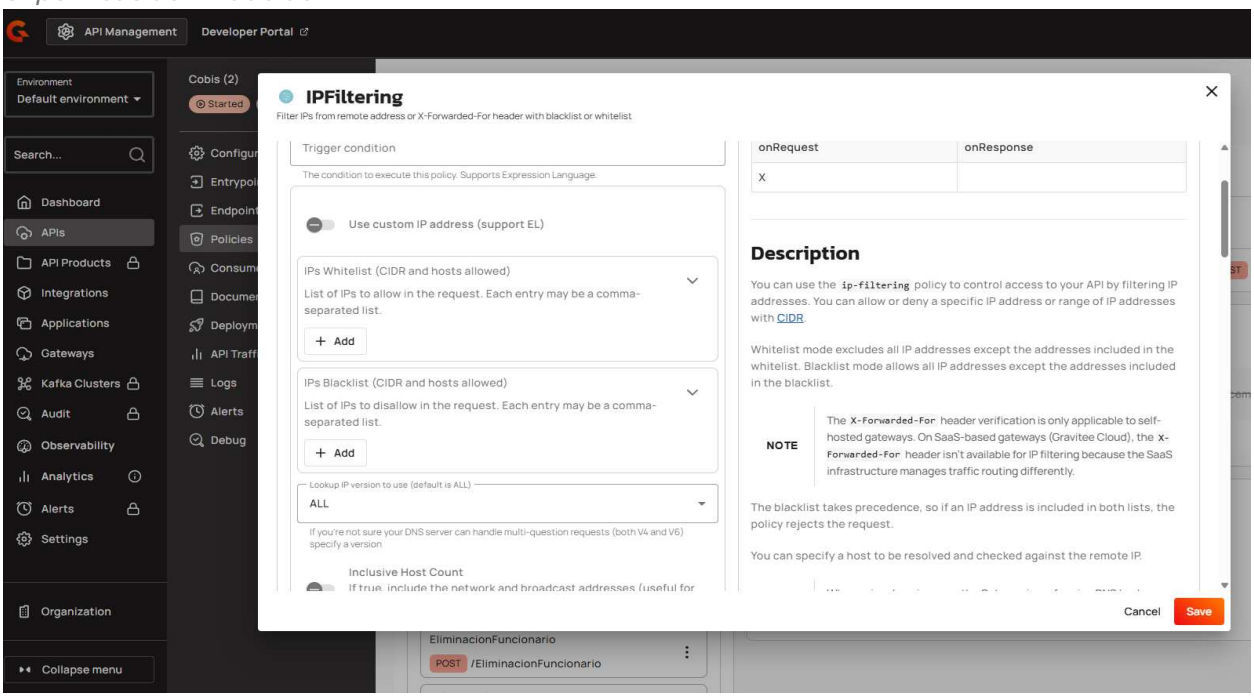


Imagen 34
UI políticas de filtrado de IP



RF_016

Imagen 35
UI entorno de test o certificación

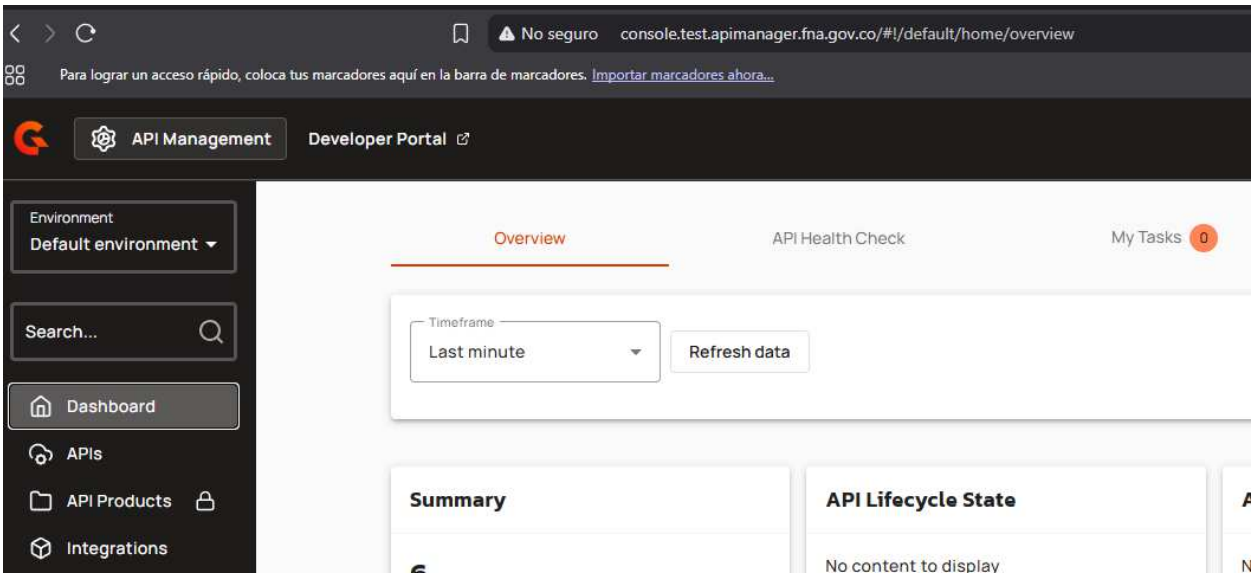


Imagen 36
UI entorno de producción

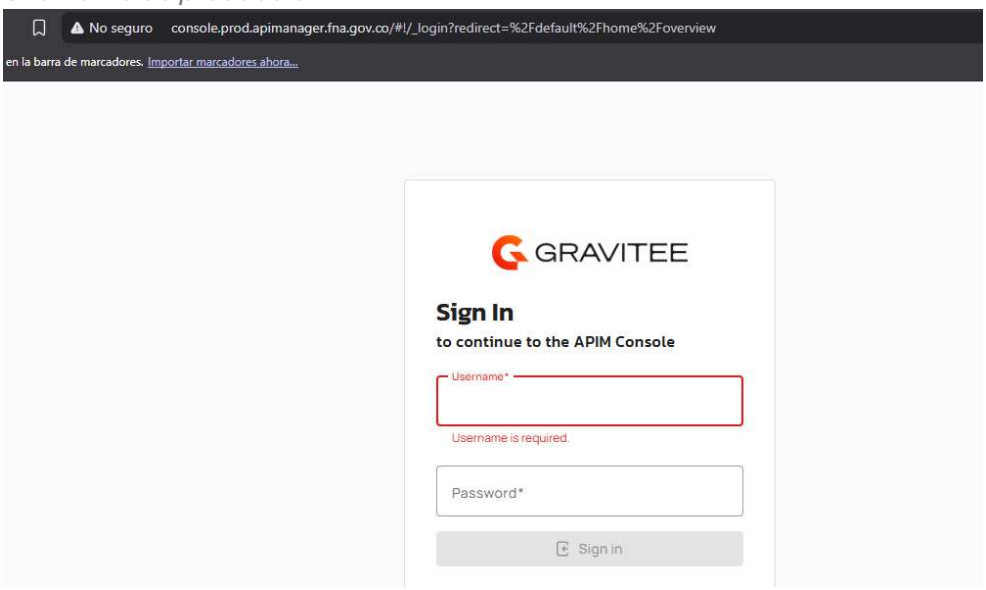
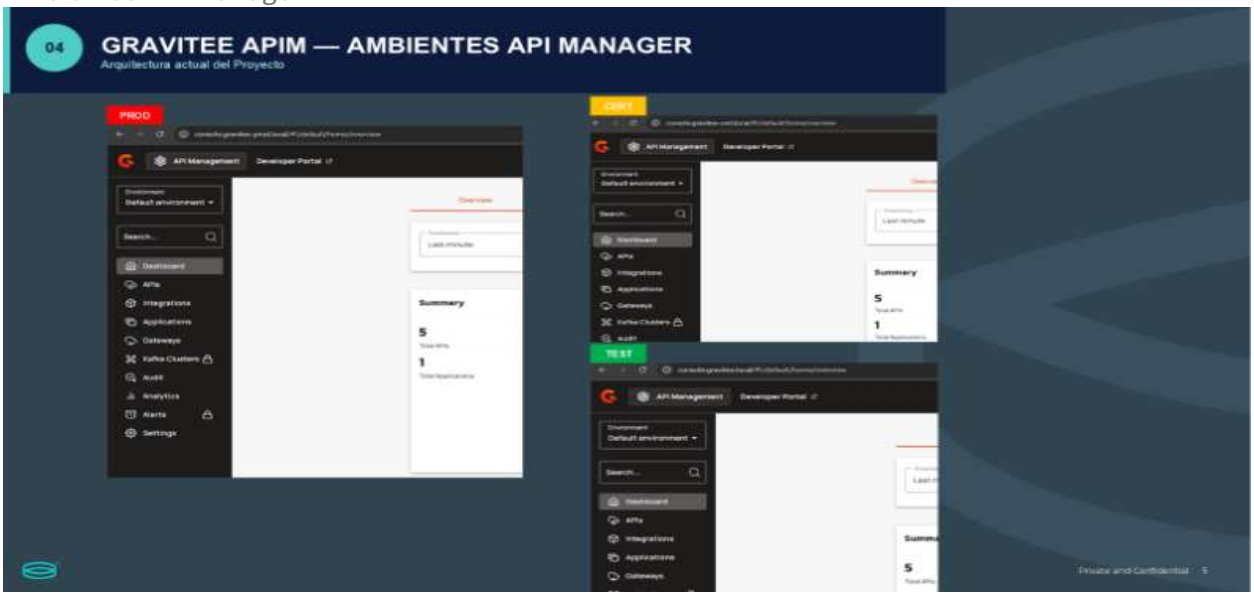


Imagen 37
Ambientes API Manager



RF_017

Imagen 38
UI Versionado de APIS

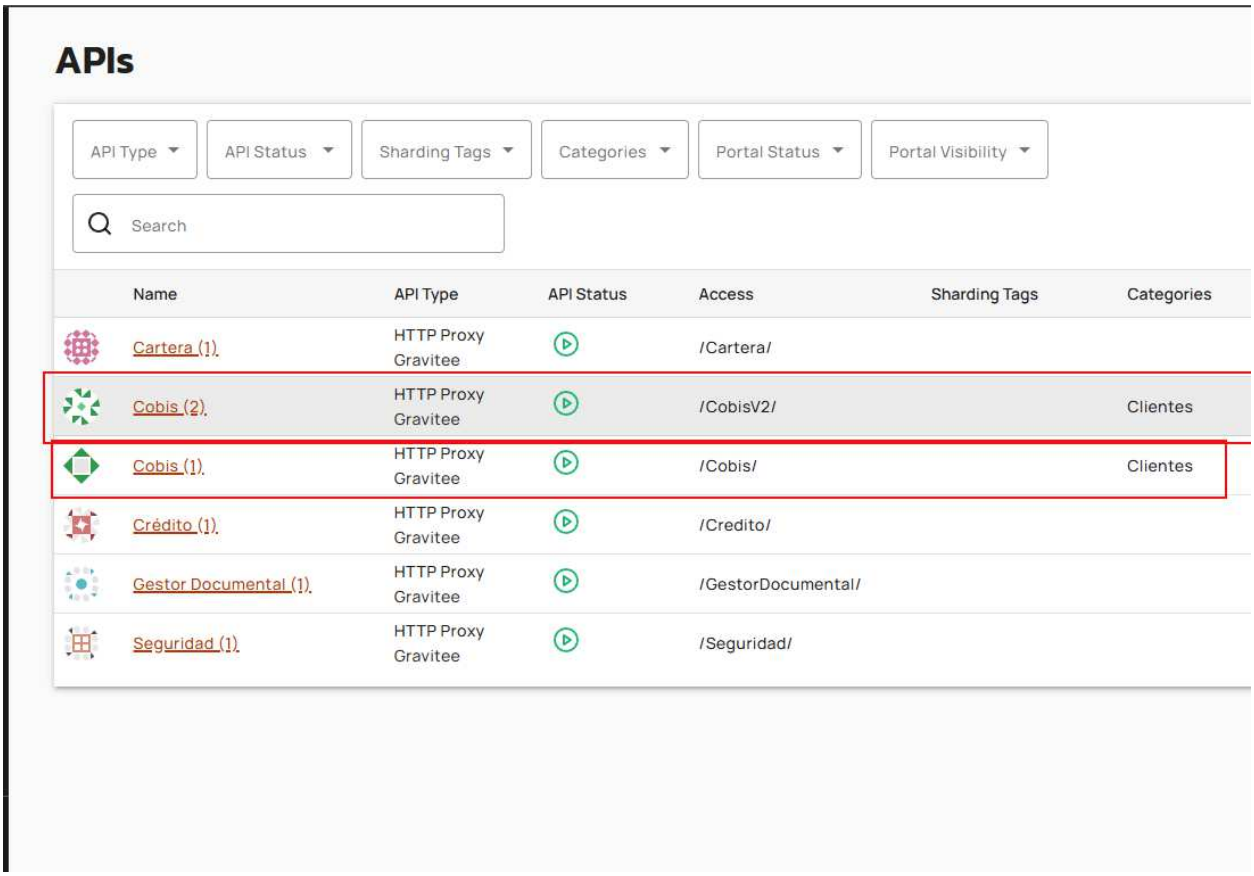
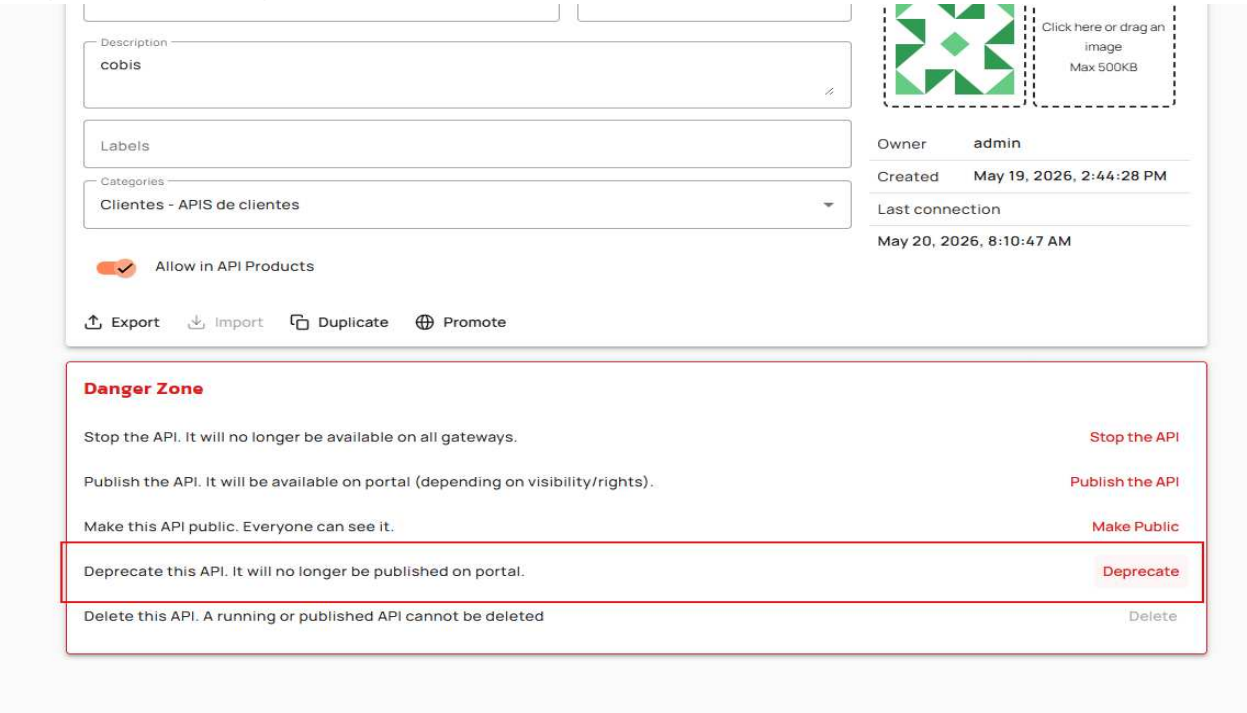


Imagen 39
UI opciones de manejo de API



RF_018

Imagen 40
UI manejo de consumo JSON

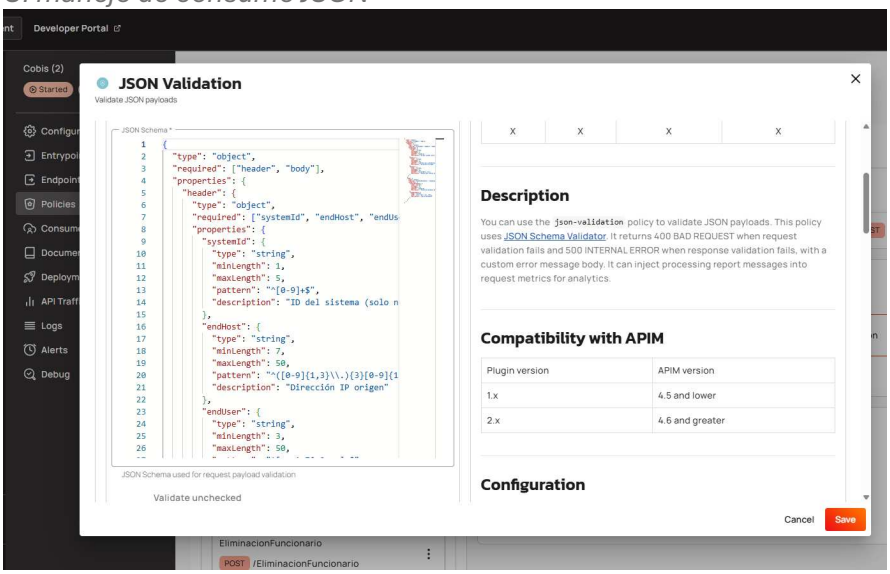
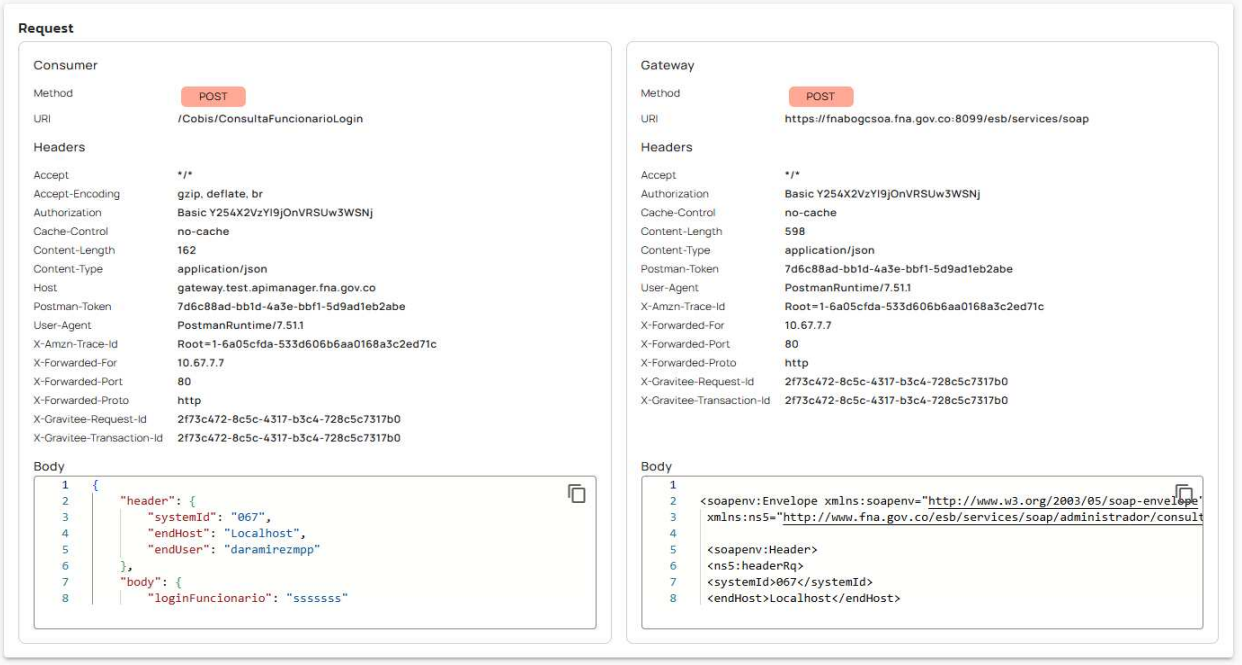


Imagen 41
UI consumo JSON



Request

Consumer

Method	POST
URI	/Cobis/ConsultaFuncionarioLogin

Headers

Accept	*/*
Accept-Encoding	gzip, deflate, br
Authorization	Basic Y254X2VzYI9jOnVRSUw3WSNj
Cache-Control	no-cache
Content-Length	162
Content-Type	application/json
Host	gateway.test.apimanager.fna.gov.co
Postman-Token	7d6c88ad-bb1d-4a3e-bbf1-5d9ad1eb2abe
User-Agent	PostmanRuntime/7.51.1
X-Amzn-Trace-Id	Root=1-6a05cfda-533d606b6aa0168a3c2ed71c
X-Forwarded-For	10.67.7.7
X-Forwarded-Port	80
X-Forwarded-Proto	http
X-Gravitee-Request-Id	2f73c472-8c5c-4317-b3c4-728c5c7317b0
X-Gravitee-Transaction-Id	2f73c472-8c5c-4317-b3c4-728c5c7317b0

Body

```
{
    "header": {
        "systemId": "067",
        "endHost": "Localhost",
        "endUser": "daramirezmpp"
    },
    "body": {
        "loginFuncionario": "sssssss"
```

Gateway

Method	POST
URI	https://fnabogcsoa.fna.gov.co:8099/esb/services/soap

Headers

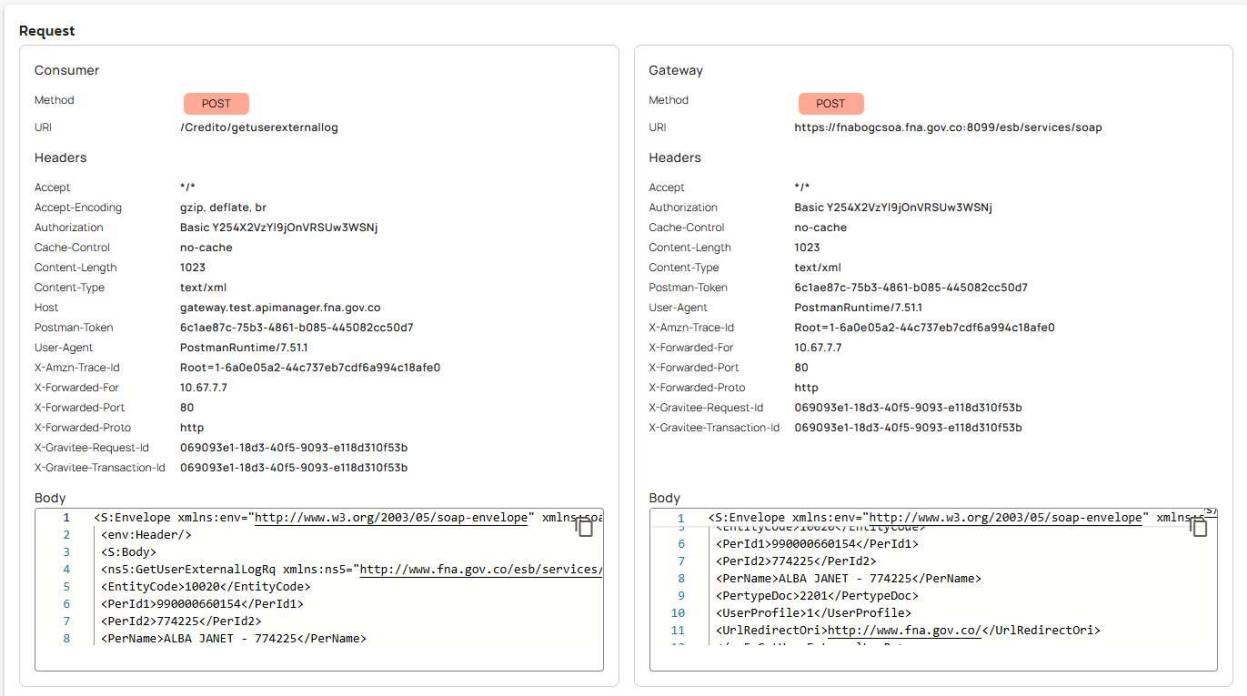
Accept	*/*
Authorization	Basic Y254X2VzYI9jOnVRSUw3WSNj
Cache-Control	no-cache
Content-Length	598
Content-Type	application/json
Postman-Token	7d6c88ad-bb1d-4a3e-bbf1-5d9ad1eb2abe
User-Agent	PostmanRuntime/7.51.1
X-Amzn-Trace-Id	Root=1-6a05cfda-533d606b6aa0168a3c2ed71c
X-Forwarded-For	10.67.7.7
X-Forwarded-Port	80
X-Forwarded-Proto	http
X-Gravitee-Request-Id	2f73c472-8c5c-4317-b3c4-728c5c7317b0
X-Gravitee-Transaction-Id	2f73c472-8c5c-4317-b3c4-728c5c7317b0

Body

```
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:ns5="http://www.fna.gov.co/esb/services/soap/administrador/consult

<soapenv:Header>
<ns5:headerRq>
<systemId>067</systemId>
<endHost>Localhost</endHost>
```

Imagen 42
UI consumo XML



Request

Consumer

Method	POST
URI	/Credito/getuserexternallog

Headers

Accept	*/*
Accept-Encoding	gzip, deflate, br
Authorization	Basic Y254X2VzYI9jOnVRSUw3WSNj
Cache-Control	no-cache
Content-Length	1023
Content-Type	text/xml
Host	gateway.test.apimanager.fna.gov.co
Postman-Token	6c1ae87c-75b3-4861-b085-445082cc50d7
User-Agent	PostmanRuntime/7.51.1
X-Amzn-Trace-Id	Root=1-6a0e05a2-44c737eb7cdf6a994c18afe0
X-Forwarded-For	10.67.7.7
X-Forwarded-Port	80
X-Forwarded-Proto	http
X-Gravitee-Request-Id	069093e1-18d3-40f5-9093-e118d310f53b
X-Gravitee-Transaction-Id	069093e1-18d3-40f5-9093-e118d310f53b

Body

```
<S:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" xmlns:soa
<env:Header/>
<S:Body>
<ns5:GetUserExternalLogRq xmlns:ns5="http://www.fna.gov.co/esb/services/
<EntityCode>10020</EntityCode>
<PerId1>990000660154</PerId1>
<PerId2>774225</PerId2>
<PerName>ALBA JANET - 774225</PerName>
```

Gateway

Method	POST
URI	https://fnabogcsoa.fna.gov.co:8099/esb/services/soap

Headers

Accept	*/*
Authorization	Basic Y254X2VzYI9jOnVRSUw3WSNj
Cache-Control	no-cache
Content-Length	1023
Content-Type	text/xml
Postman-Token	6c1ae87c-75b3-4861-b085-445082cc50d7
User-Agent	PostmanRuntime/7.51.1
X-Amzn-Trace-Id	Root=1-6a0e05a2-44c737eb7cdf6a994c18afe0
X-Forwarded-For	10.67.7.7
X-Forwarded-Port	80
X-Forwarded-Proto	http
X-Gravitee-Request-Id	069093e1-18d3-40f5-9093-e118d310f53b
X-Gravitee-Transaction-Id	069093e1-18d3-40f5-9093-e118d310f53b

Body

```
<S:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" xmlns:ns
<PerId1>990000660154</PerId1>
<PerId2>774225</PerId2>
<PerName>ALBA JANET - 774225</PerName>
<PertypeDoc>2201</PertypeDoc>
<UserProfile>1</UserProfile>
<UrlRedirectOri>http://www.fna.gov.co/</UrlRedirectOri>
```

RF_019

Imagen 43

UI política de transformación JSON a SOAP mapeo de datos

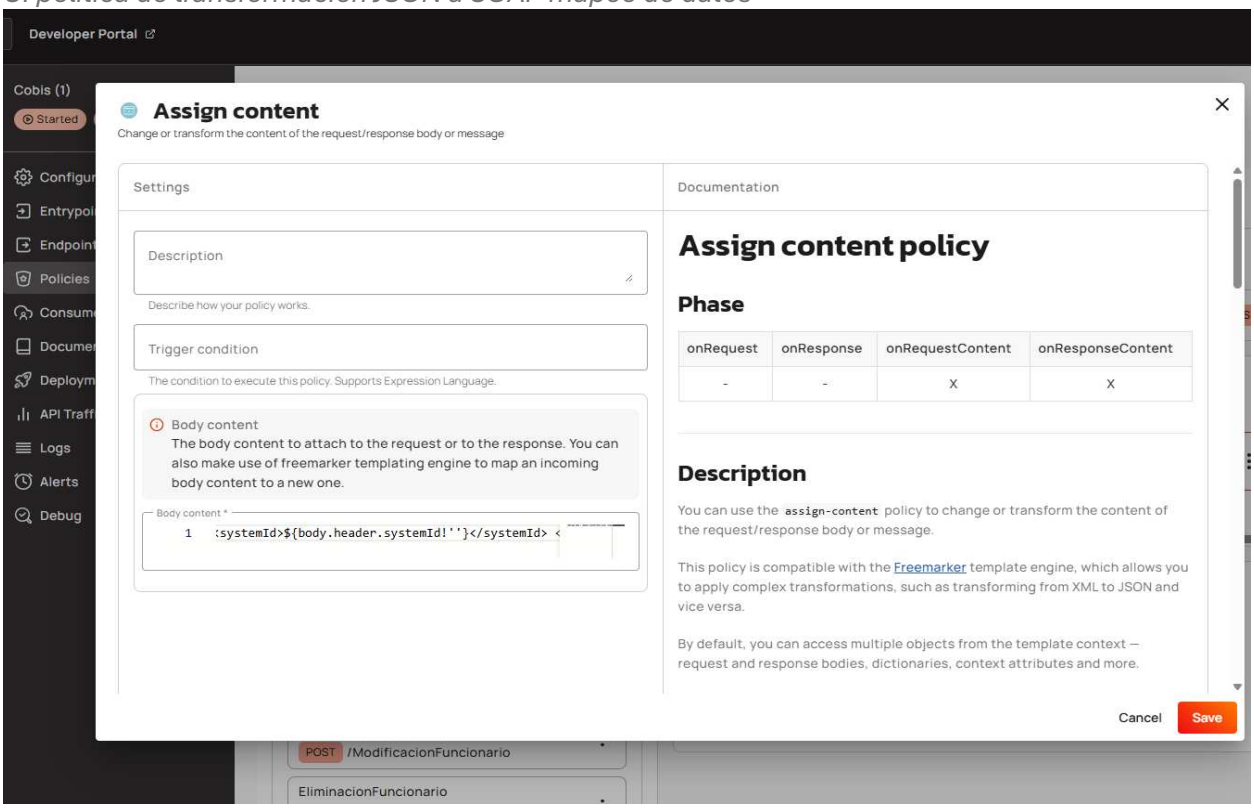


Imagen 44
UI política de transformación JSON a XML

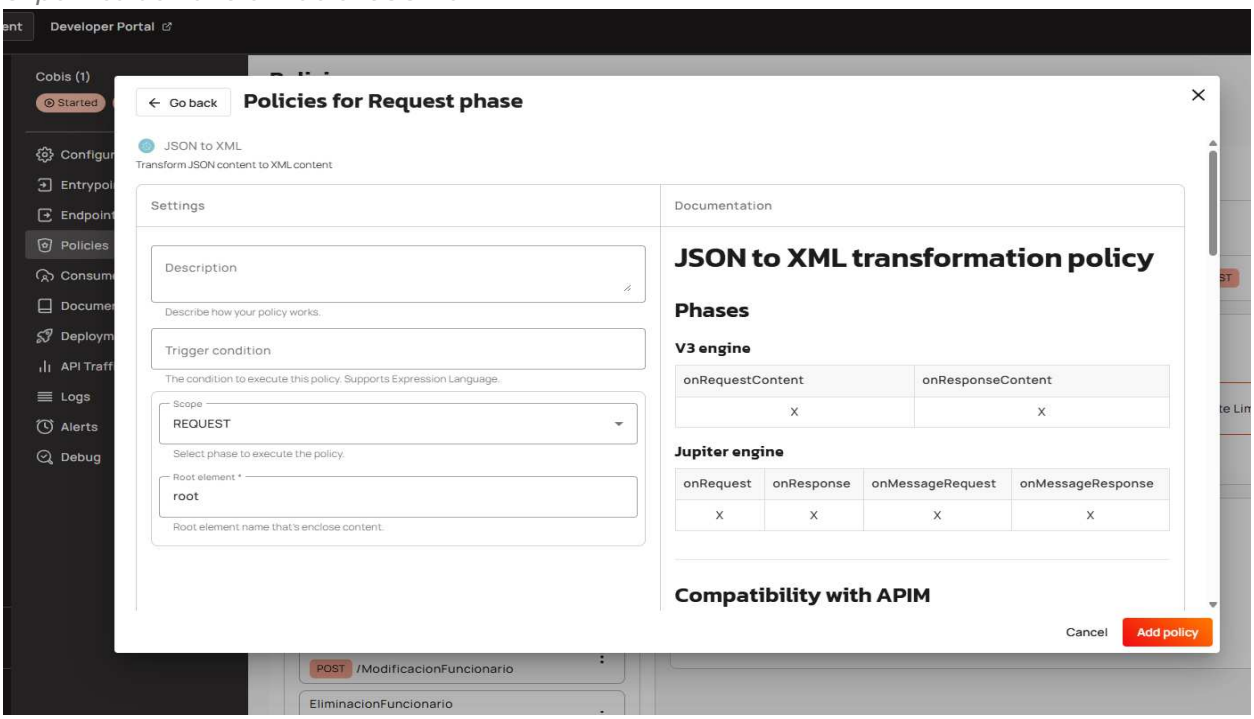
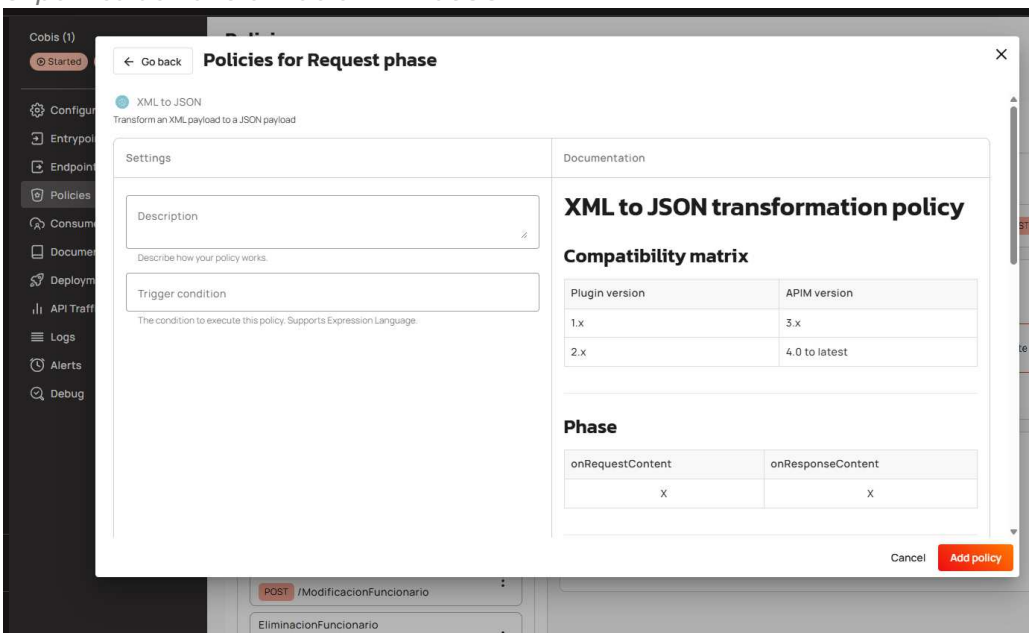


Imagen 45
UI política de transformación XML a JSON



RF_021

Imagen 46

UI Kubernete activo en AWS con nodos auto escalables

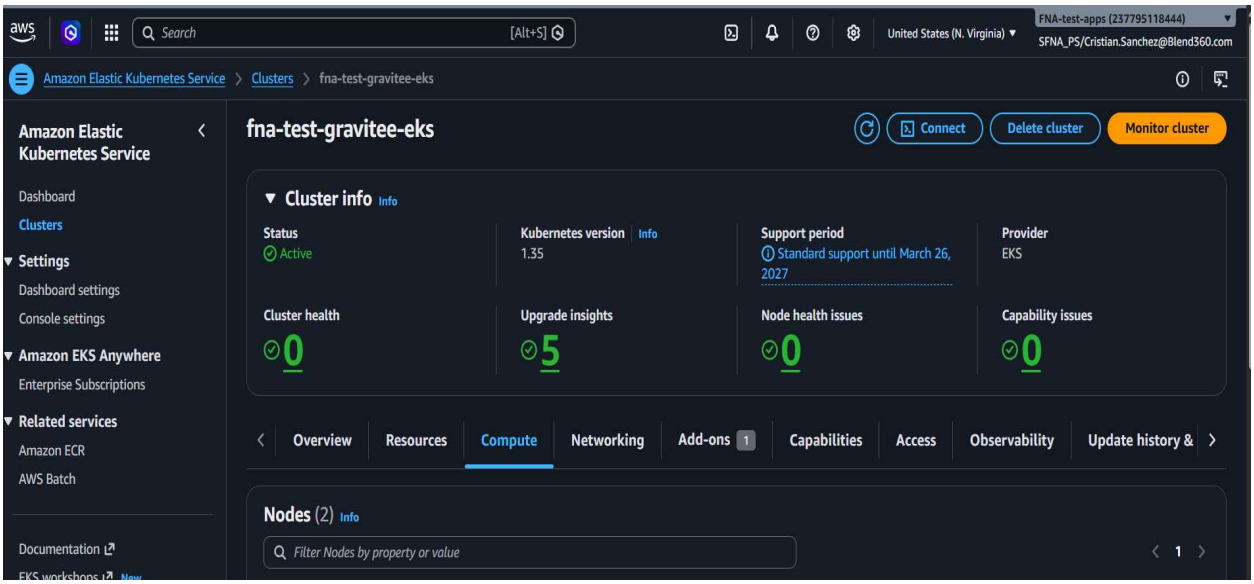
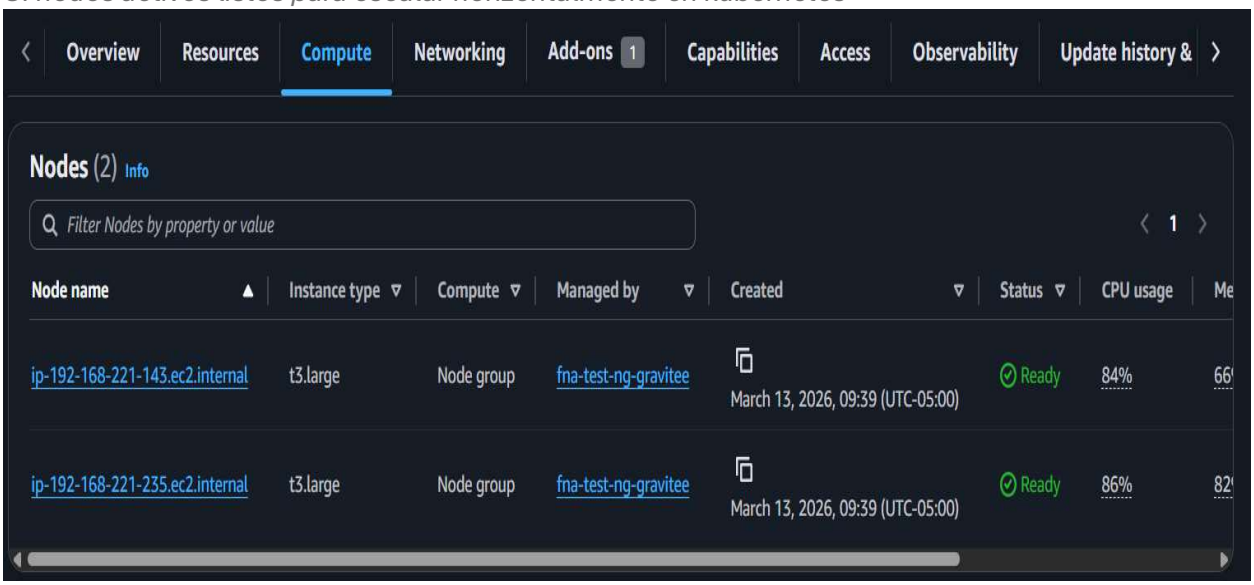


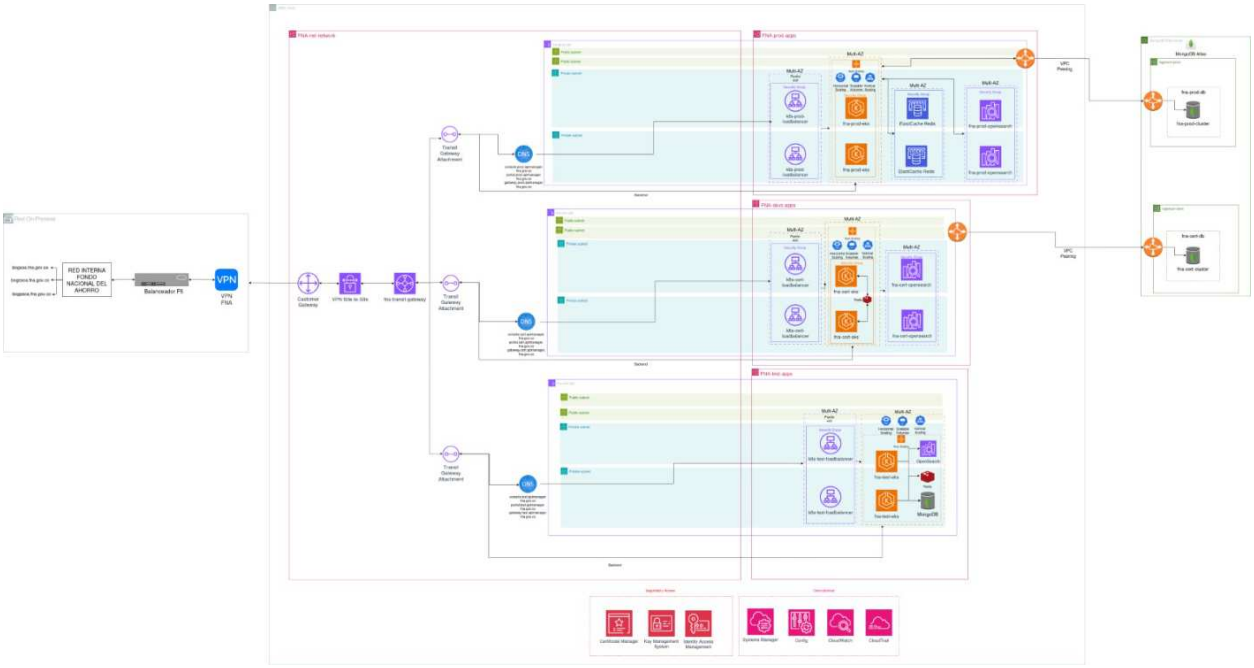
Imagen 47

UI nodos activos listos para escalar horizontalmente en kubernetes



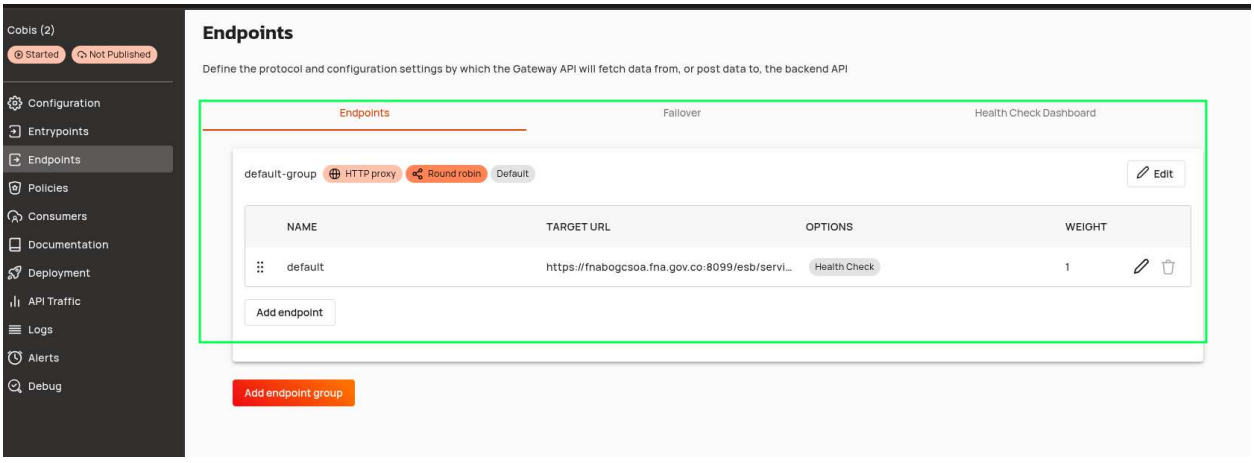
RF_023

Imagen 48
Diagrama de arquitectura API Manager.



3. API GATEWAY

RT_002
Imagen 49
Ui API MANAGER Endpoints



4. MICROSERVICIOS Y CONTENEDORES

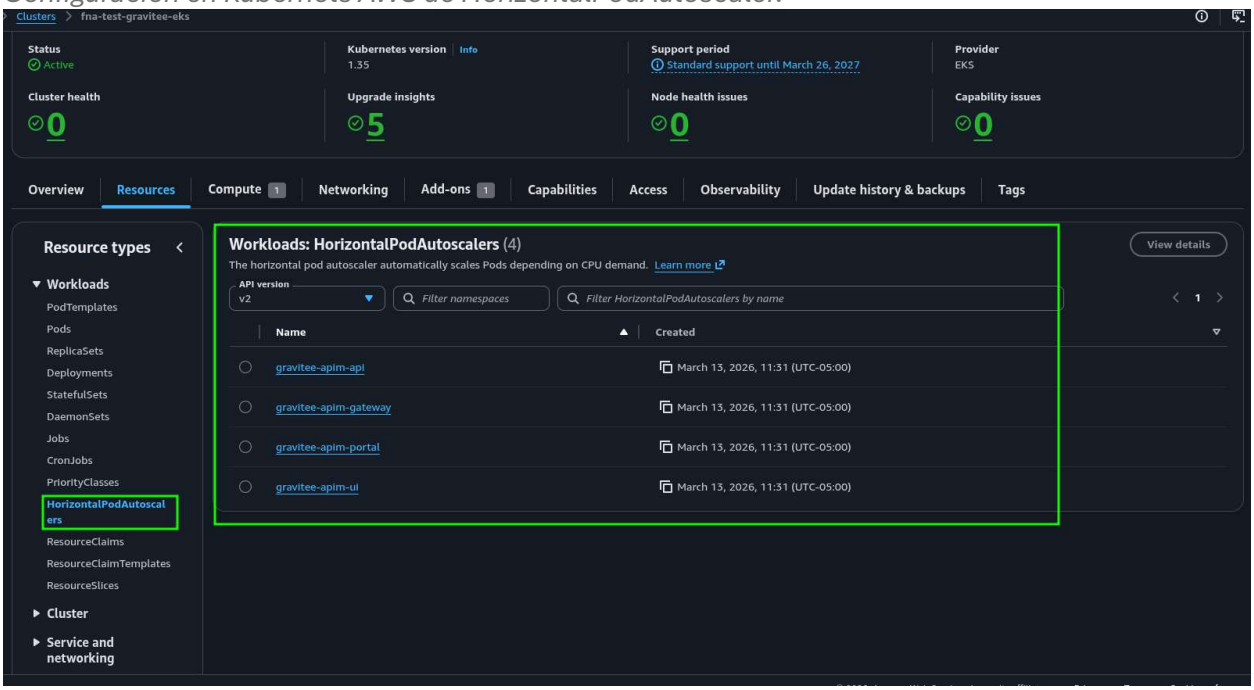
RT_001

Imagen 50
kubectl get pods: todos los componentes de la plataforma API Manager (incluyendo MongoDB, Redis y Elasticsearch) Corriendo.



RT_002

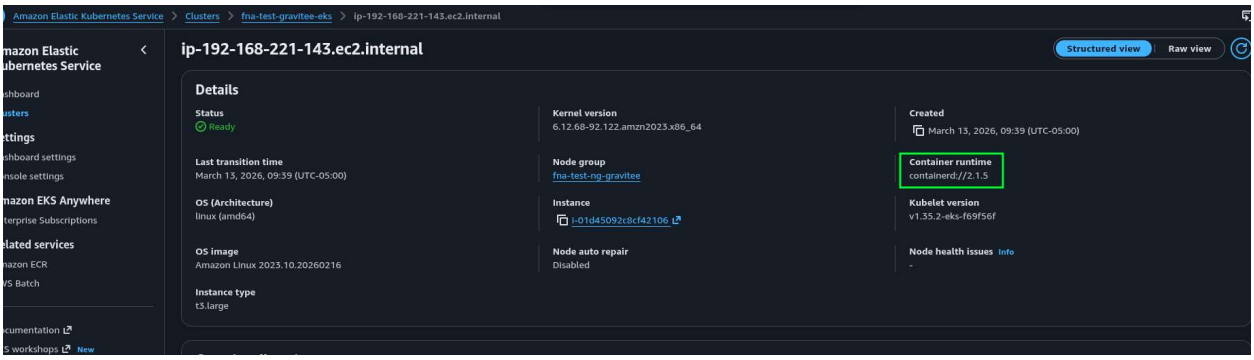
Imagen 51
Configuración en Kubernets AWS de HorizontalPodAutoscaler.



5. **INFRAESTRUCTURA Y REQUISITOS DE SOFTWARE**

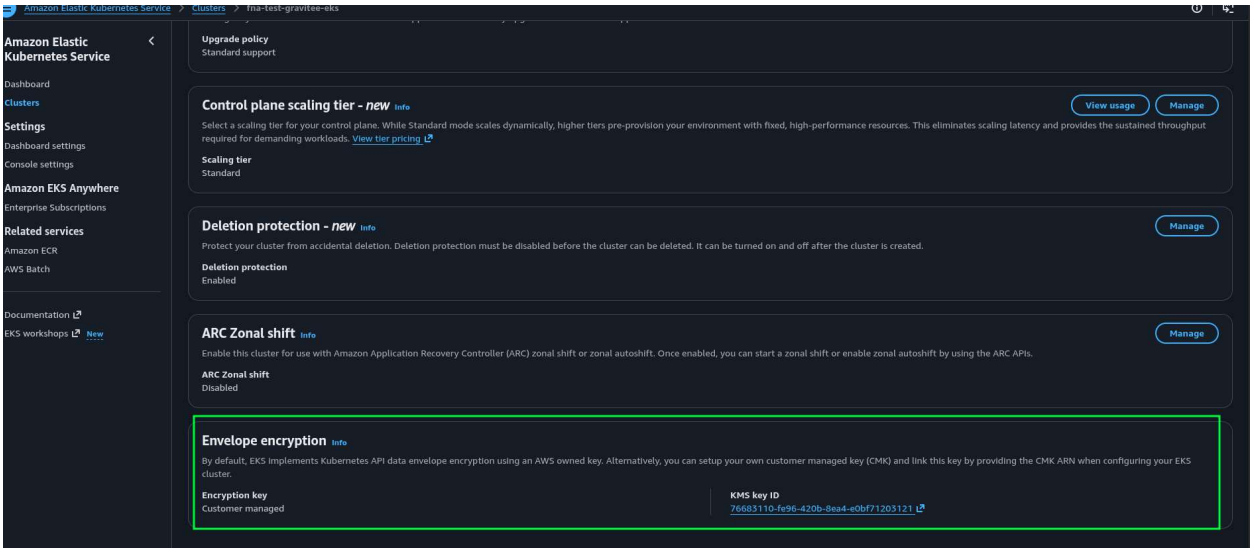
RT_001

Imagen 52
Kubernets en AWS con containerd como runtime de contenedores



RT_007

Imagen 53
Kubernetes Secrets cifrados con KMS de AWS.



14. HISTÓRICO DE PRUEBAS Y VALIDACIONES DE SERVICIOS

14.1. Alcance del histórico de pruebas

El presente capítulo consolida el histórico de pruebas y validaciones realizadas sobre los servicios (APIs) expuestos a través de la plataforma API Manager del Fondo Nacional del Ahorro (FNA). Su finalidad es dejar registro trazable de la ejecución y los resultados de las pruebas de conexión y estabilización efectuadas durante la fase de integración de los servicios, sirviendo como evidencia técnica y como insumo para las etapas posteriores.

Se presentan los servicios expuestos a través del API Manager, agrupados en 5 dominios funcionales/APIs (Cobis, Seguridad, Cartera, Gestor Documental y Crédito). Cada servicio se invocó mediante Postman sobre el Gateway del API Manager y para cada uno se registró la información general del servicio, la respuesta obtenida y la evidencia de ejecución.

Las pruebas aquí consolidadas se ejecutaron mediante invocaciones sobre el Gateway de la plataforma en el ambiente de Desarrollo/QA, como parte de las actividades de conexión y estabilización de los servicios del primer batch priorizado descrito en la Sección 8. El histórico registra 21 operaciones de servicio con resultado satisfactorio, agrupadas según el backend de origen. El grupo Cobis corresponde a los servicios del dominio Funcionario (backend COBADMIN) e

incluye, además de las operaciones del inventario contractual (consulta, creación y modificación de funcionario), las operaciones complementarias DesignarRol, AsignarRol y ConsultaFuncionarioLogin, validadas durante la estabilización del mismo backend. El servicio ValidarIngresos (ESB_252), que en el inventario de la Sección 8 pertenece al dominio Crédito, se reporta en este histórico dentro del grupo de pruebas de Seguridad; el grupo Crédito incluye adicionalmente el servicio GetUserExternalLog (ESB_155), probado durante la fase de estabilización. Los servicios AgregarDocumento (ESB_189), VariablesScore (ESB_251) y EliminacionFuncionario (F-249) no hacen parte de este histórico. Estas agrupaciones son de carácter operativo y no modifican el inventario contractual de 17 APIs del primer batch descrito en la Sección 8 y en el Anexo C.

14.2. Resumen de los servicios probados

Tabla 36. Resumen de los servicios probados

Dominio / API	Cantidad de servicios	Resultado
Cobis	6	Satisfactorio
Seguridad	3	Satisfactorio
Cartera	1	Satisfactorio
Gestor Documental	7	Satisfactorio
Crédito	4	Satisfactorio
Total	21	—

14.3. Servicio Cobis

14.3.1. ConsultaFuncionarioIdentificacion

Tabla 37. Información general – ConsultaFuncionarioIdentificacion

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	ConsultaFuncionarioIdentificacion

Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 38. Respuesta – ConsultaFuncionarioIdentificacion

Campo	Valor
númeroDocumento	1117534447
tipoDocumento	CC
código	10247
nombre	ANGIE KATERINE VERA
códigoSexo	F
login	akvera
clave	ZZZZZZ
códigoOficina	49
códigoDepartamento	49
códigoCargo	62

códigoEstadoFuncionario	V
fechaIngreso	2022-07-05
fechaRetiro	2024-05-24

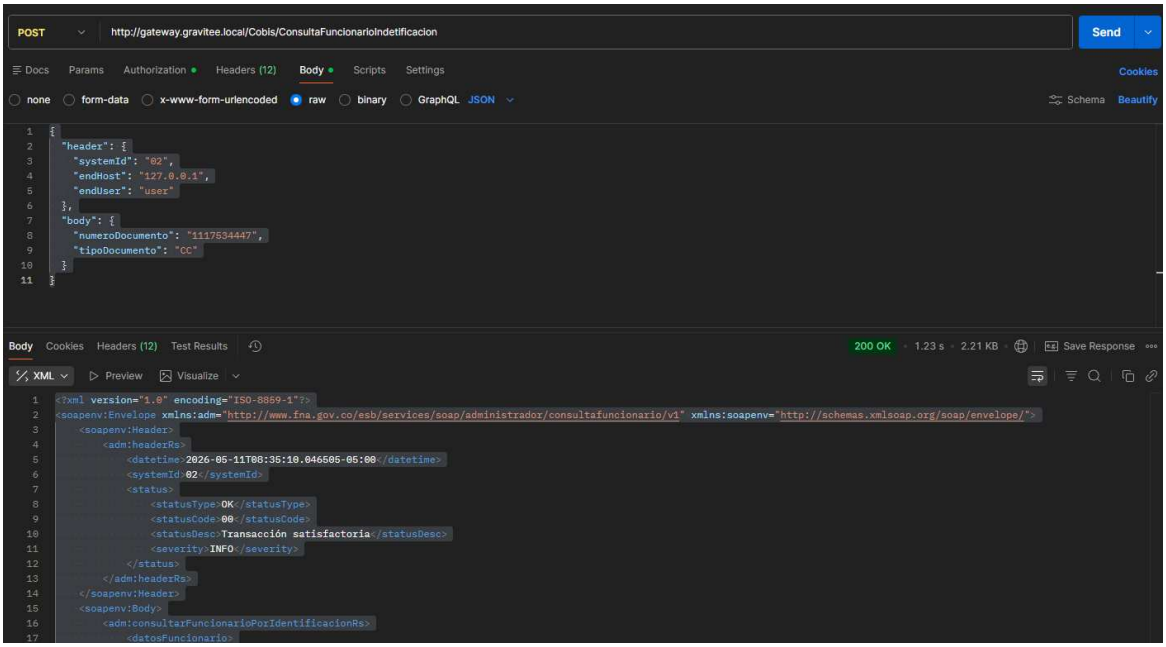


Ilustración 2. ConsultaFuncionarioIdentificacion

14.3.2. CreacionFuncionario

Tabla 39. Información general – CreacionFuncionario

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	CreacionFuncionario
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11

Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 40. Respuesta – CreacionFuncionario

Campo	Valor
código	18120
datetime	2026-05-11T08:36:47
systemId	001
statusType	OK
statusDesc	Transacción satisfactoria

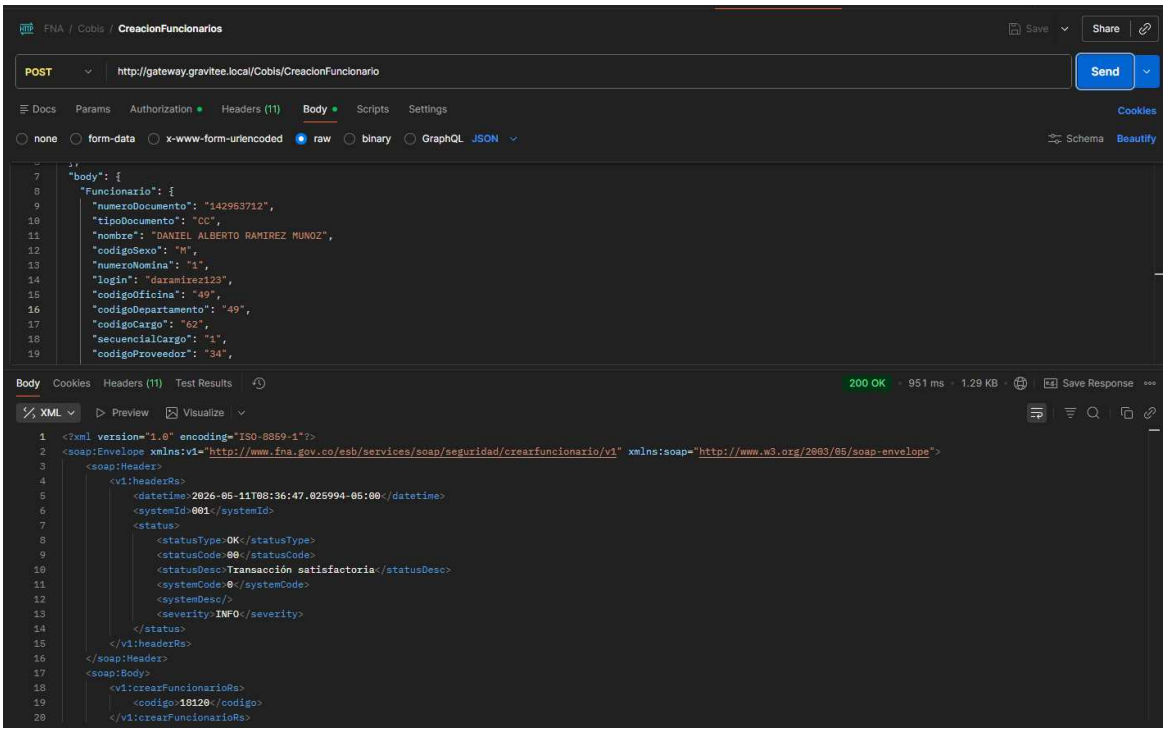


Ilustración 3. CreacionFuncionario

14.3.3. ModificacionFuncionario

Tabla 41. Información general – ModificacionFuncionario

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	ModificacionFuncionario
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP

- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 42. Respuesta – ModificacionFuncionario

Campo	Valor
clientTransactionID	Generado dinámicamente
datetime	2026-05-11T08:44:42
systemId	74
statusType	OK
statusDesc	Transacción satisfactoria

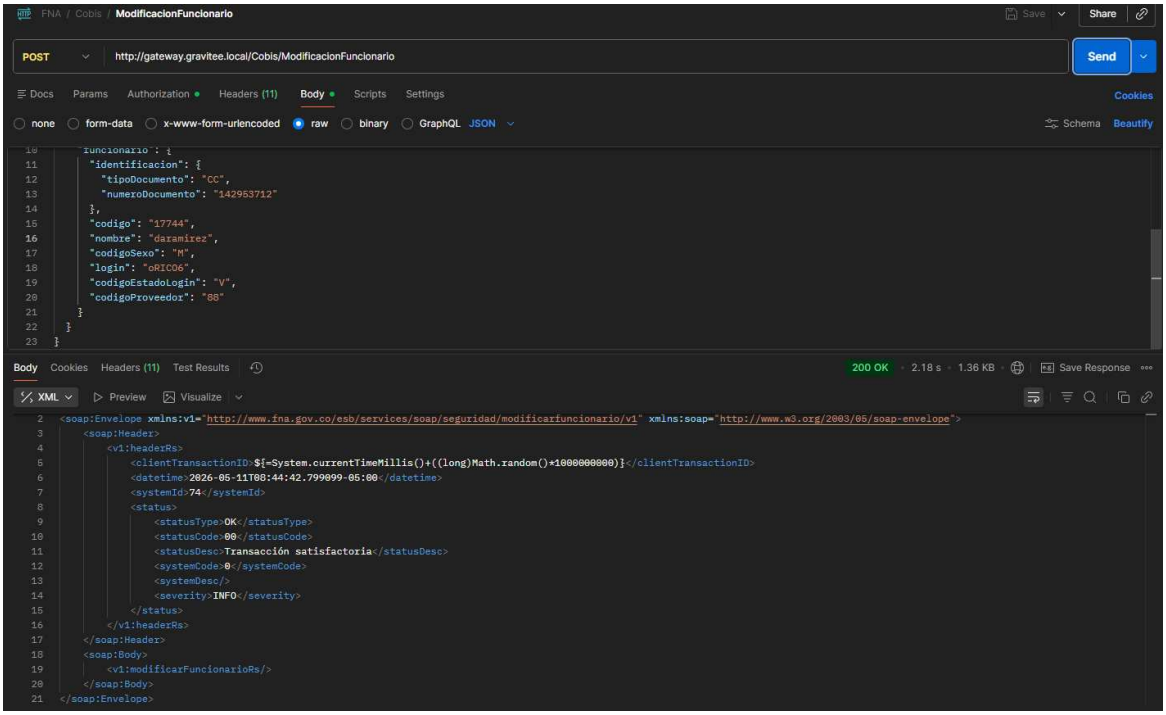


Ilustración 4. ModificacionFuncionario

14.3.4. DesignarRol

Tabla 43. Información general – DesignarRol

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	DesignarRol
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 44. Respuesta – DesignarRol

Campo	Valor
clientTransactionID	Generado dinámicamente
datetime	2026-05-11T09:32:24
systemId	001
statusType	OK
statusDesc	Transacción satisfactoria

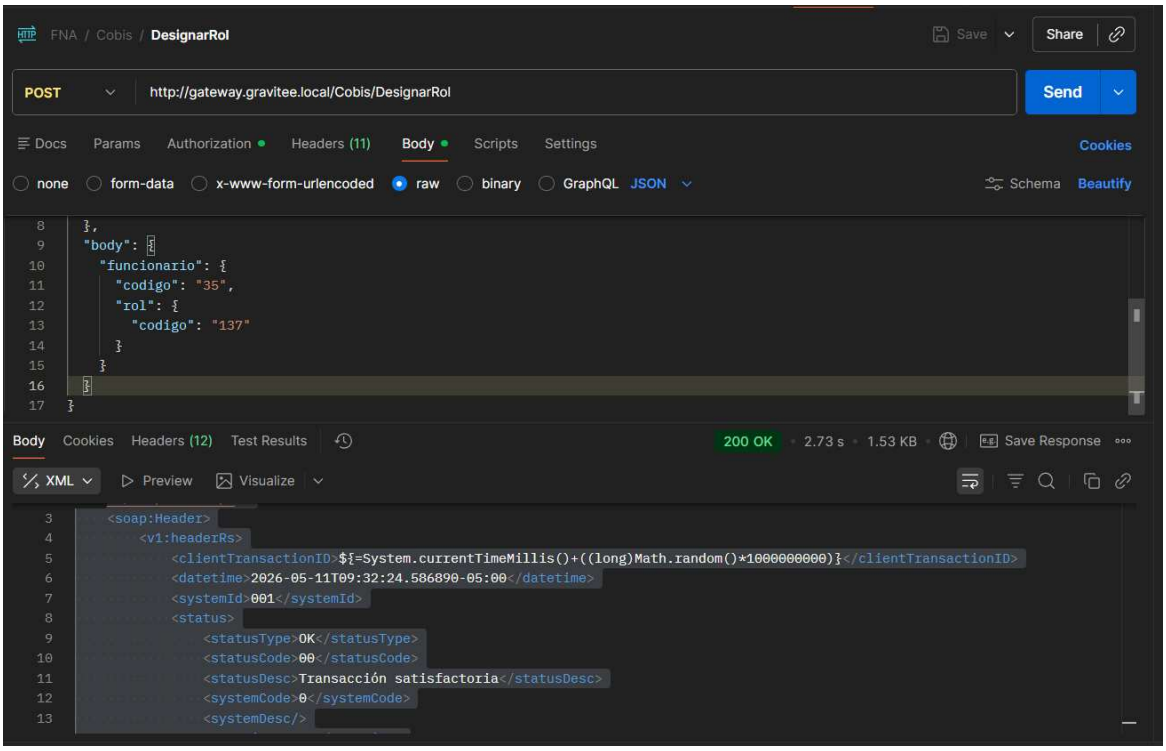


Ilustración 5. DesignarRol

14.3.5. AsignarRol

Tabla 45. Información general – AsignarRol

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	AsignarRol
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

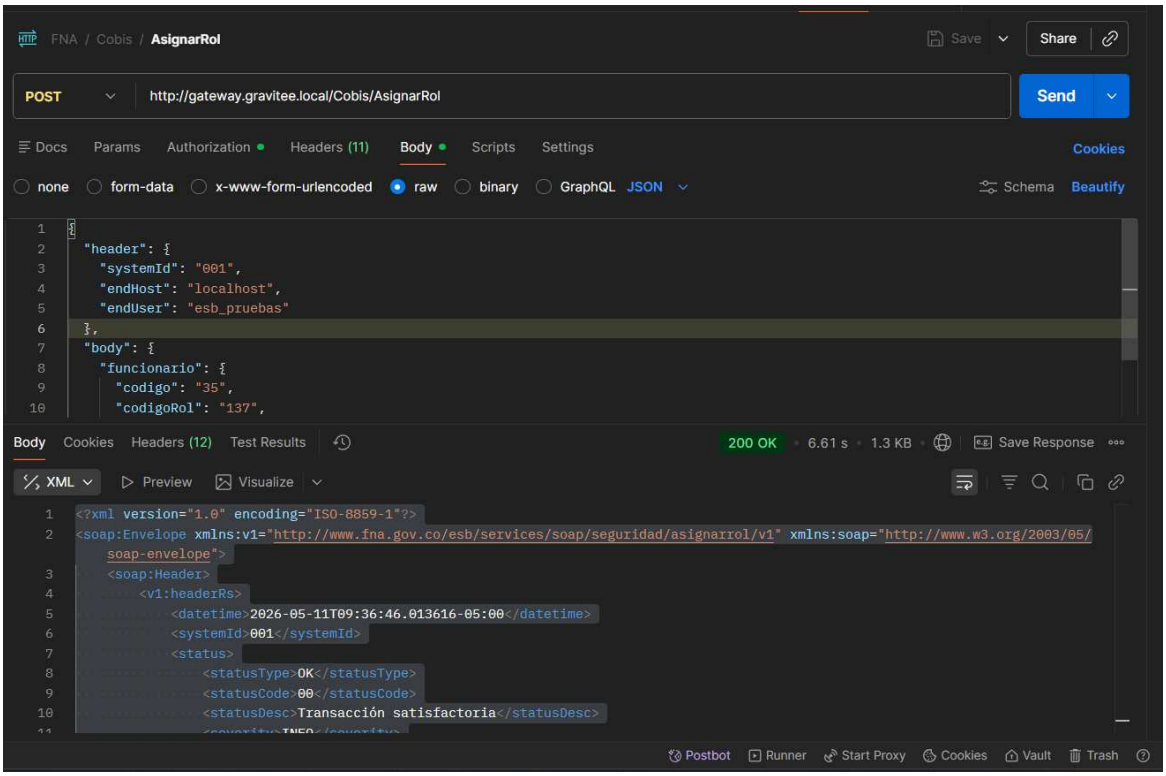


Ilustración 6. AsignarRol

14.3.6. ConsultaFuncionarioLogin

Tabla 46. Información general – ConsultaFuncionarioLogin

Campo	Valor
Proyecto	Cobis - API Management
Servicio / API	ConsultaFuncionarioLogin
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

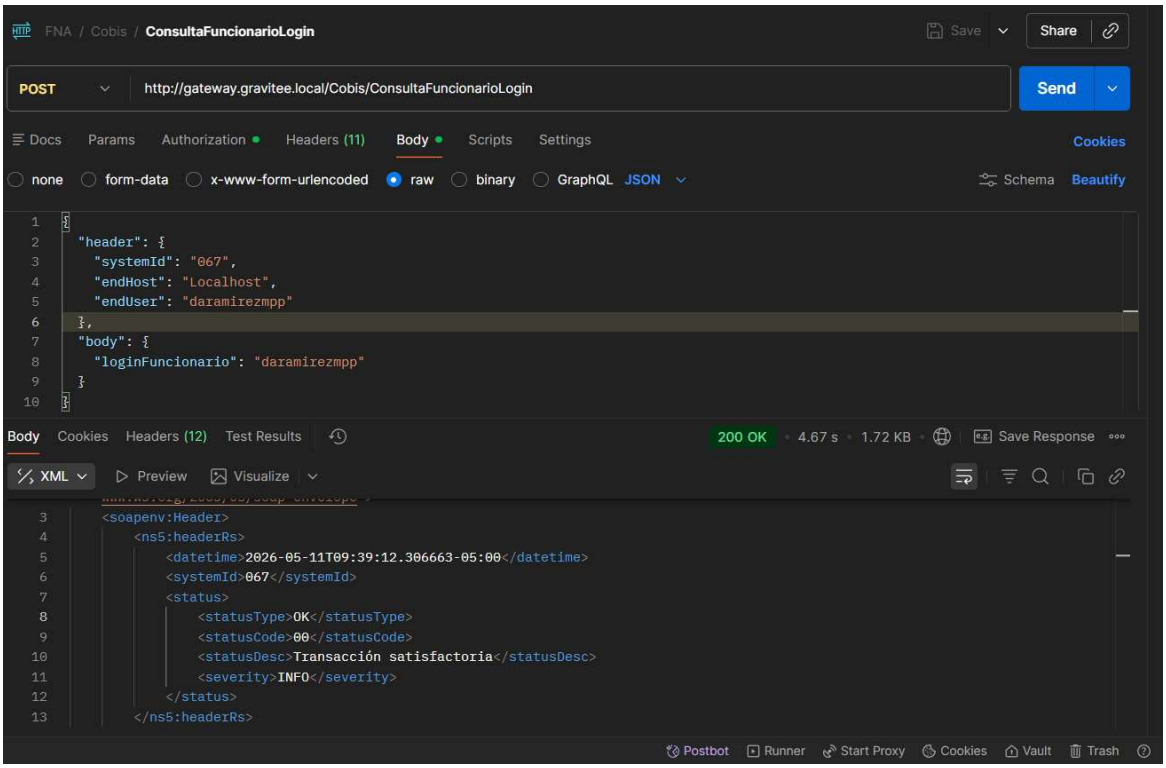


Ilustración 7. ConsultaFuncionarioLogin

14.4. Servicios Seguridad

14.4.1. ConsultarListasInhibitorias

Tabla 47. Información general – ConsultarListasInhibitorias

Campo	Valor
Proyecto	Seguridad - API Management
Servicio / API	consultarlistasinhibitorias
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 48. Respuesta – ConsultarListasInhibitorias

Campo	Valor
reportadoPorId	N
reportadoPorNombre	N
datetime	2026-05-11T11:12:38
systemId	094
statusType	OK
statusDesc	Transacción satisfactoria

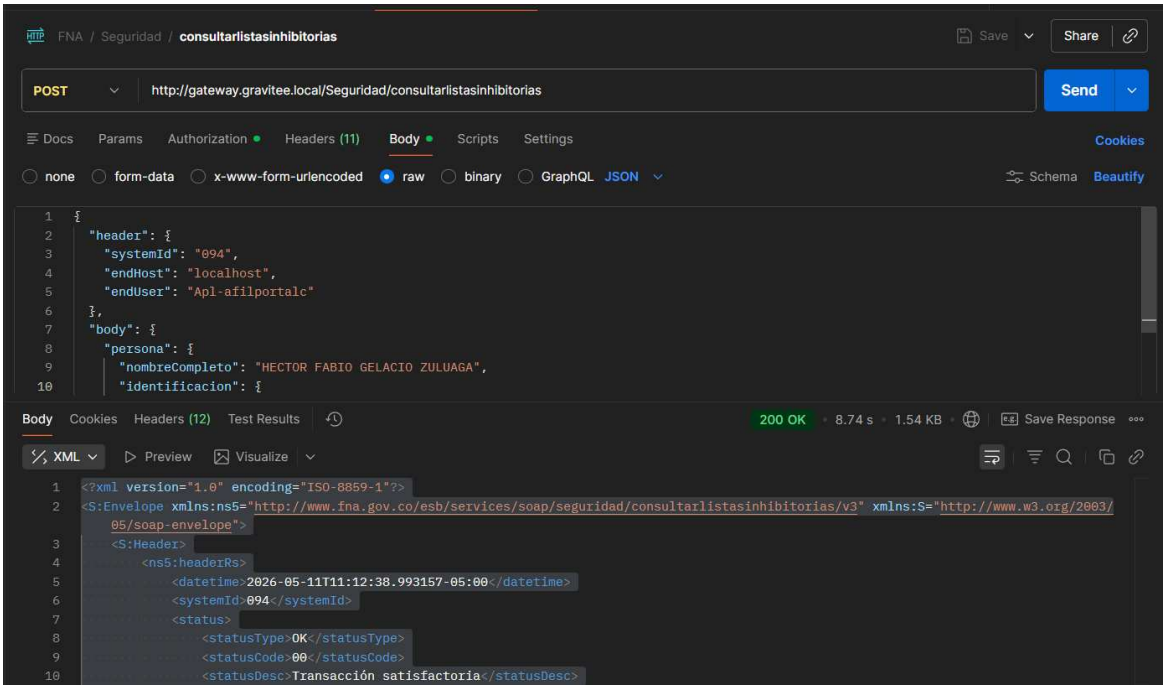


Ilustración 8. ConsultarListasInhibitorias

14.4.2. InformacionComercial

Tabla 49. Información general – InformacionComercial

Campo	Valor
Proyecto	Seguridad - API Management
Servicio / API	InformacionComercial
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Tipo de respuesta: XML embebido (CIFIN)
- Resultado general:

Tabla 50. Respuesta – InformacionComercial

Campo	Valor
systemId	067
status	OK
statusCode	00
statusDesc	Transacción satisfactoria

datetime	2026-05-11T11:14:52

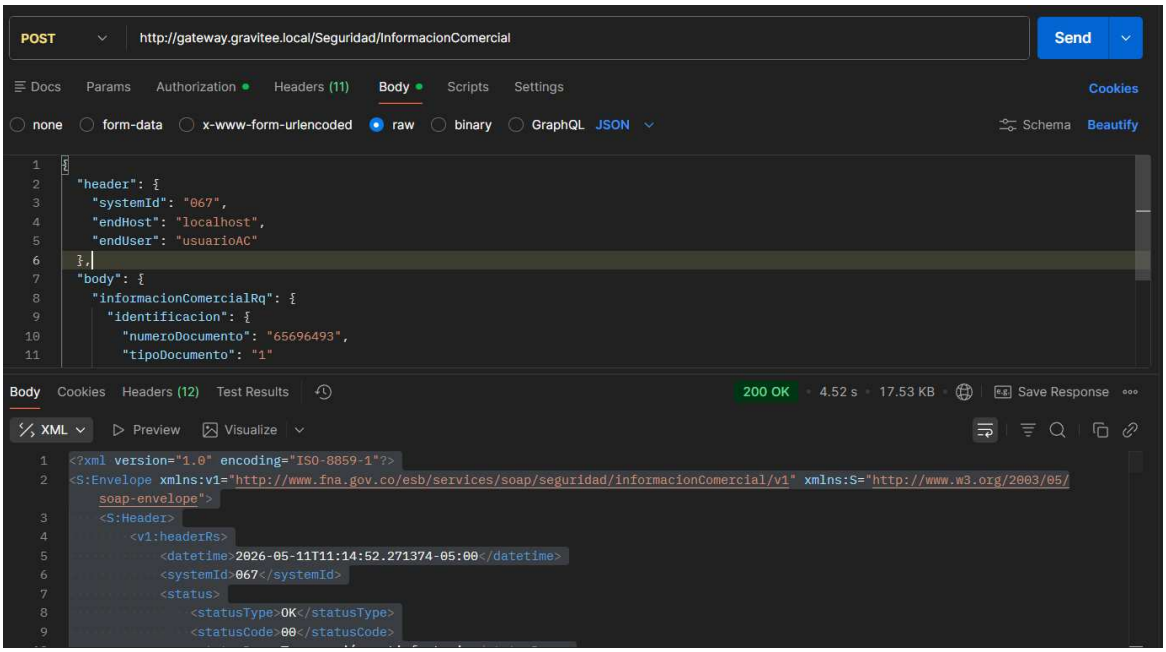


Ilustración 9. InformacionComercial

14.4.3. ValidarIngresos

Tabla 51. Información general – ValidarIngresos

Campo	Valor
Proyecto	Seguridad - API Management
Servicio / API	ValidarIngresos
Método	POST
Tipo	SOAP (XML)
Fecha	2026-05-11
Ambiente	Desarrollo / QA

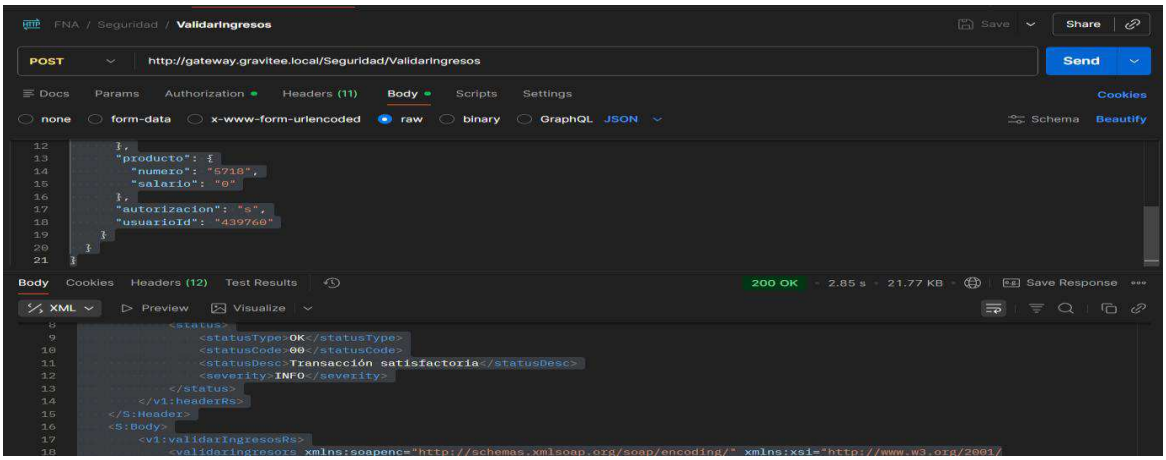


Ilustración 10. ValidarIngresos

14.5. Servicios Cartera

14.5.1. CrearTransaccionPago

Tabla 52. Información general – CrearTransaccionPago

Campo	Valor
Proyecto	Cartera - Pagos
Servicio / API	crearTransaccionPago
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 53. Respuesta – CrearTransaccionPago

Campo	Valor

estadoTransaccion	SUCCESS
numeroTransaccion	71486035
urleCollect	https://test1.e-collect.com/d_ecollectplus/Portfolio/Pay.aspx?WsPm=674B2F33664D43424F4E414B41332F6D6E77345273773D3D
tiempoUtilidad	0
fechaTransaccion	2026-05-11T11:26:11.8879914-05:00
codigoMoneda	N/A
monto	0.00
impuestoMonto	0.00
tasaCambio	0.00
referenciaPago	N/A
codigoConcepto	N/A
descripcionConcepto	N/A
codigoEstadoTransaccion	N/A
codigoResultadoPeticion	N/A
codigoComercio	N/A

codigoTrazabilidad	N/A

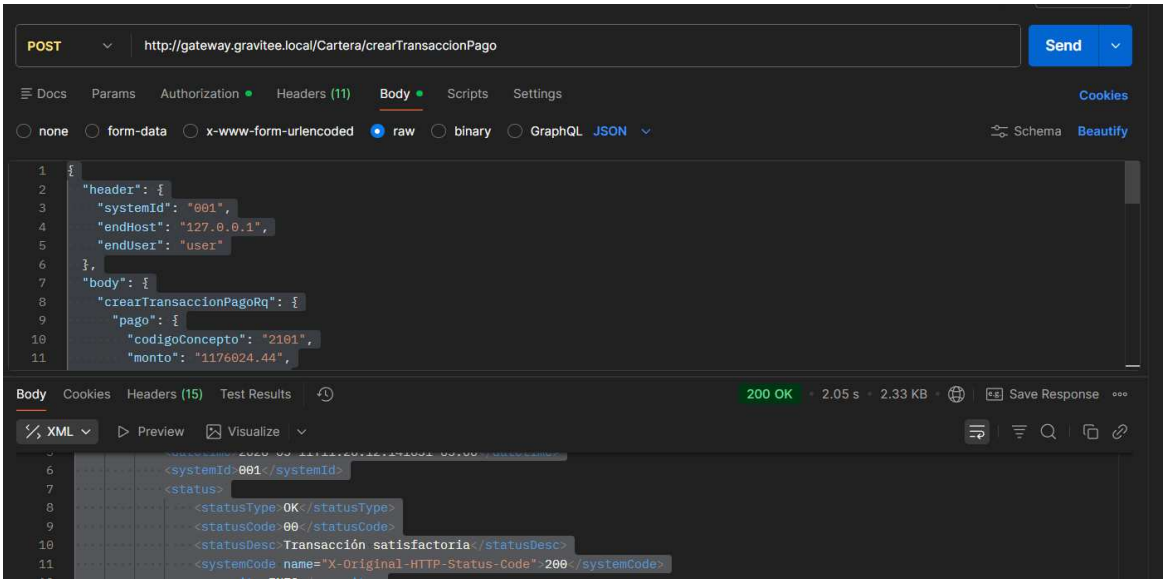


Ilustración 11. CrearTransaccionPago

14.6. Servicios Gestor Documental

14.6.1. consultaDocumento

Tabla 54. Información general – consultaDocumento

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	consultaDocumento
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO

- Datos principales devueltos:

Tabla 55. Respuesta – consultaDocumento

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
mensaje	OK
exitoso	true
datetime	2026-05-12T15:51:56.356594-05:00
systemId	108

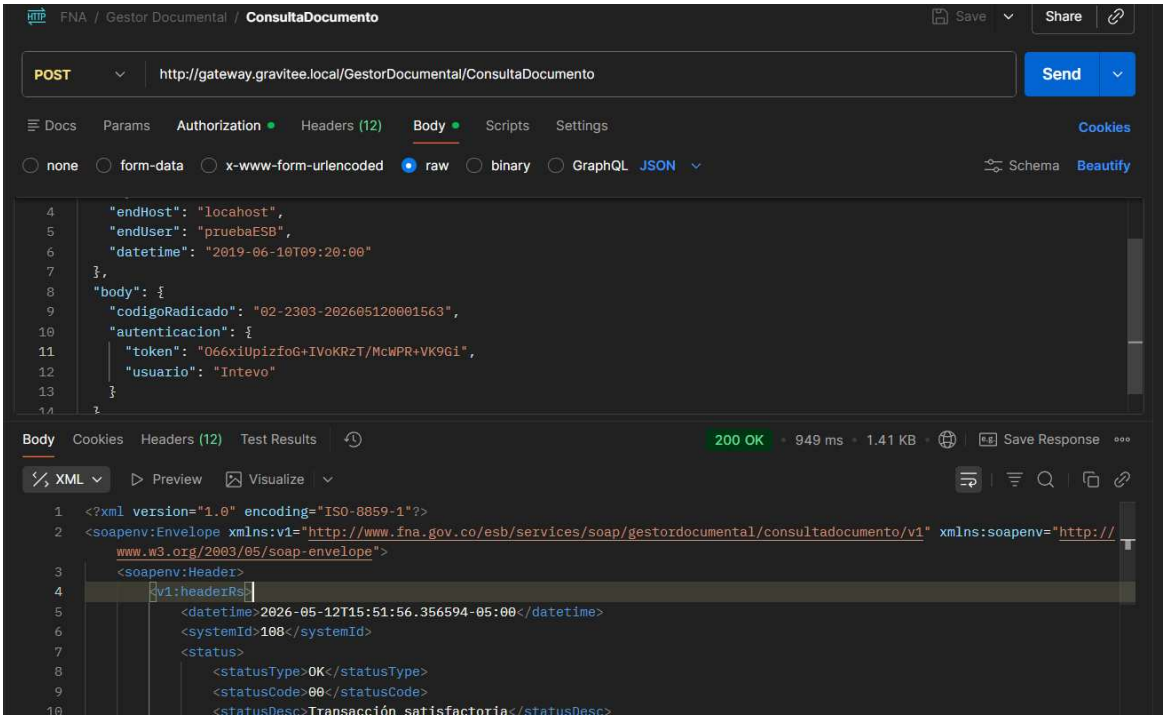


Ilustración 12. consultaDocumento

14.6.2. EliminarDocumento

Tabla 56. Información general – EliminarDocumento

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	eliminarDocumento
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 57. Respuesta – EliminarDocumento

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
mensaje	OK
exitoso	true
datetime	2026-05-12T16:00:22.197827-05:00

systemId	108
clientTransactionID	${=System.currentTimeMillis()}

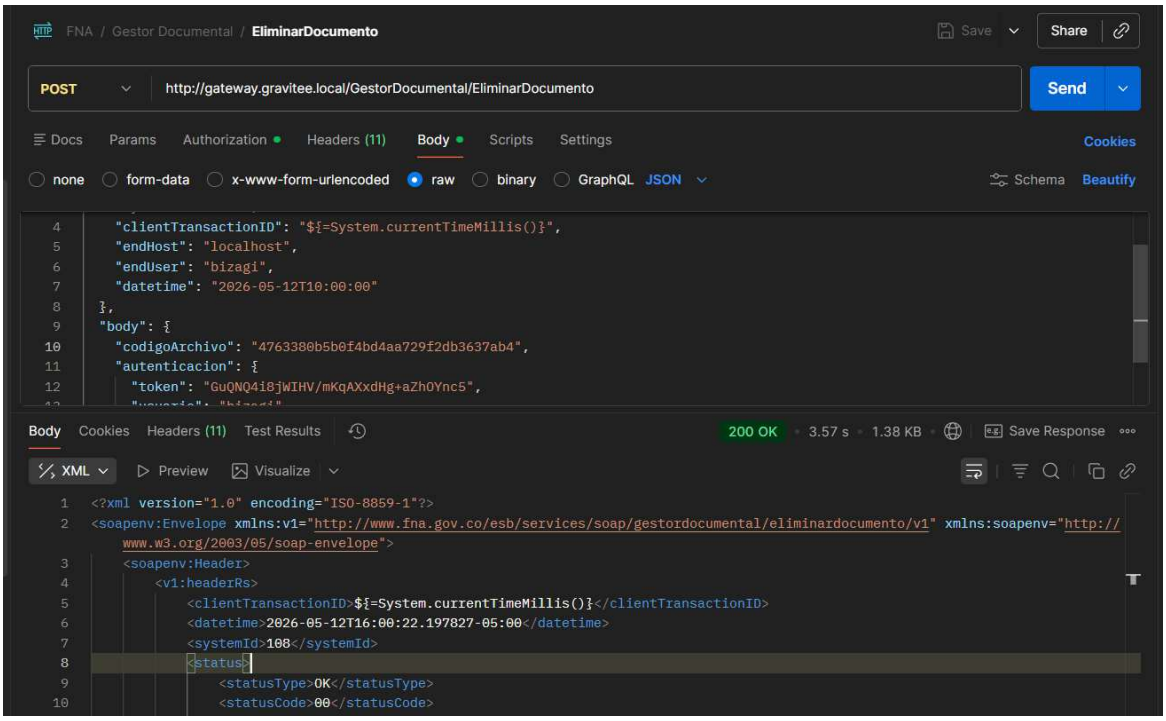


Ilustración 13. EliminarDocumento

14.6.3. ObtenerInformacionFormulario

Tabla 58. Información general – ObtenerInformacionFormulario

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	obtenerInformacionFormulario
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP

- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 59. Respuesta – ObtenerInformacionFormulario

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
clientTransactionID	${=System.currentTimeMillis()+((int)Math.random()*200000000)}
datetime	2026-05-12T16:03:23.244593-05:00
systemId	070
mensaje	OK
exitoso	true

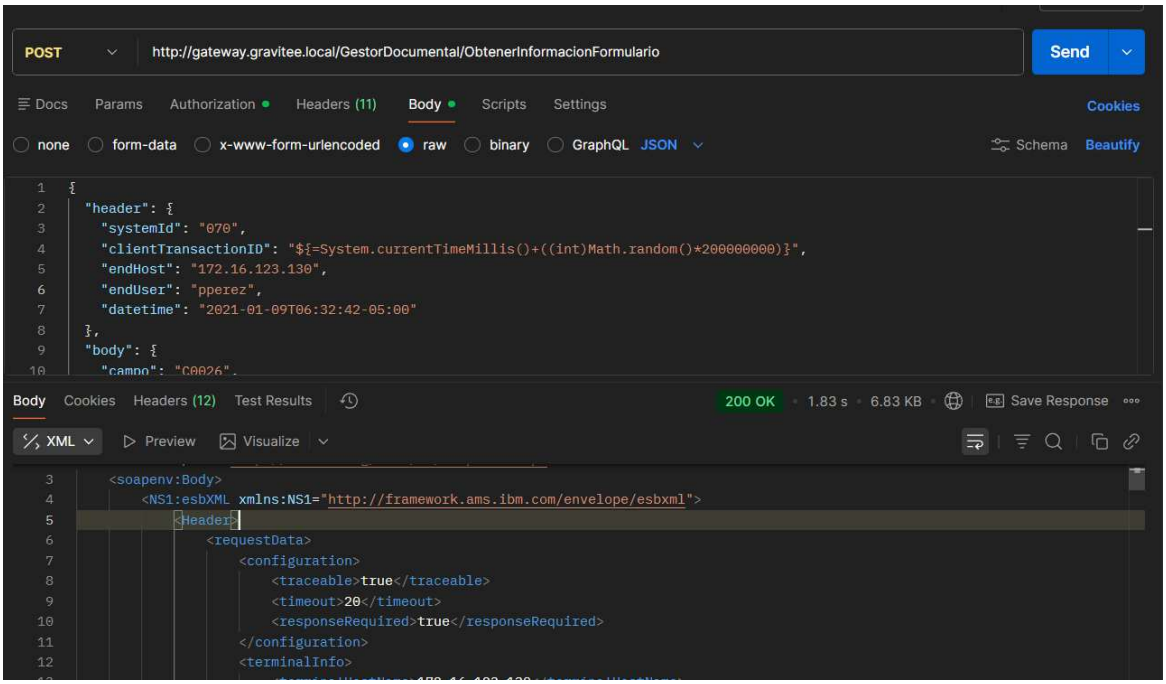


Ilustración 14. ObtenerInformacionFormulario

14.6.4. InicioFlujoTrabajoDocumento

Tabla 60. Información general – InicioFlujoTrabajoDocumento

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	inicioFlujoTrabajoDocumento
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 61. Respuesta – InicioFlujoTrabajoDocumento

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
clientTransactionID	TX-1715539123001
datetime	2026-05-12T16:00:10.196471-05:00
systemId	070
codigoArchivo	4763380b5b0f4bd4aa729f2db3637ab4
mensaje	OK
exitoso	true
idFlujoTrabajo	-1

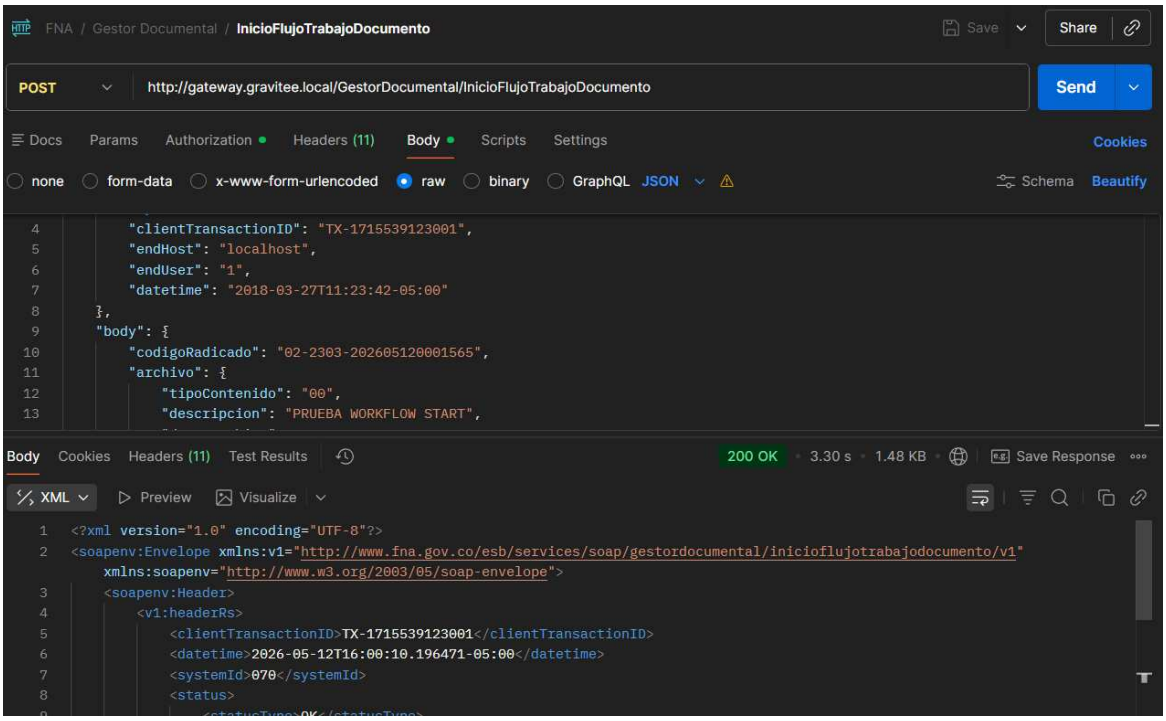


Ilustración 15. InicioFlujoTrabajoDocumento

14.6.5. ObtenerCatalogo

Tabla 62. Información general – ObtenerCatalogo

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	obtenerCatalogo
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 63. Respuesta – ObtenerCatalogo

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
clientTransactionID	${=System.currentTimeMillis()+((int)Math.random()*200000000)}
datetime	2026-05-12T16:10:50.735706-05:00
systemId	070
mensaje	OK
exitoso	true

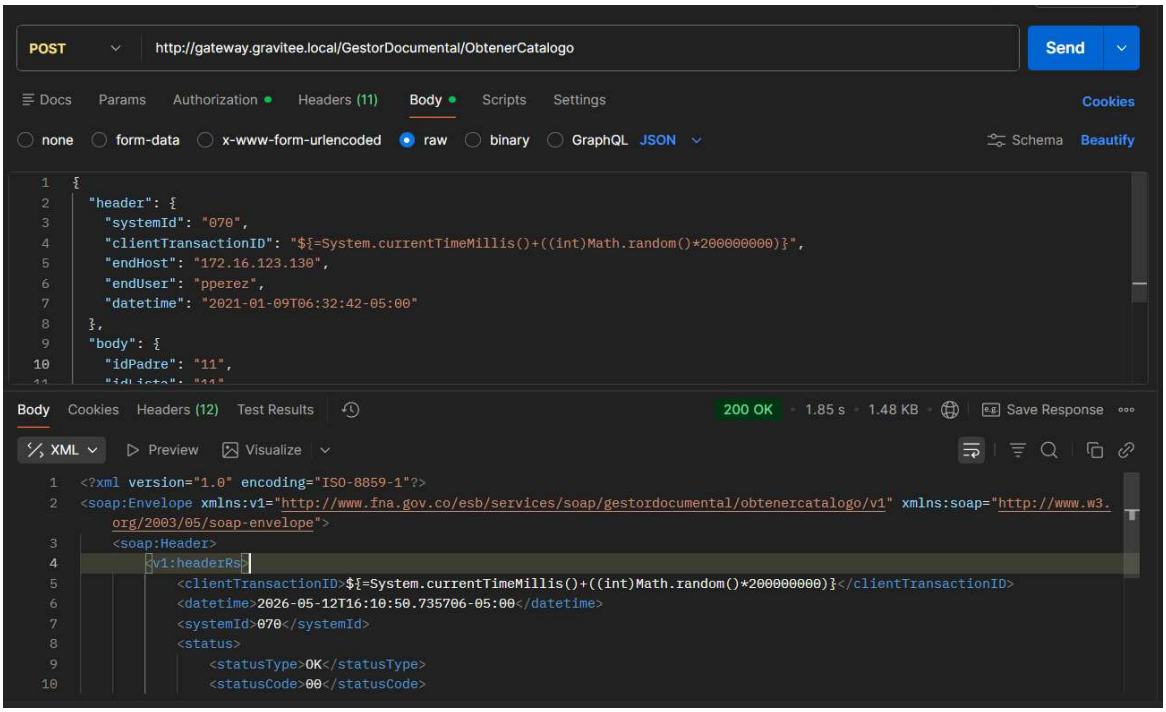


Ilustración 16. ObtenerCatalogo

14.6.6. ActualizarFormulario

Tabla 64. Información general – ActualizarFormulario

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	actualizarFormulario
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 65. Respuesta – ActualizarFormulario

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
clientTransactionID	${=System.currentTimeMillis()}
datetime	2026-05-12T16:12:47.155876-05:00
systemId	070

mensaje	OK
filas	1
exitoso	true

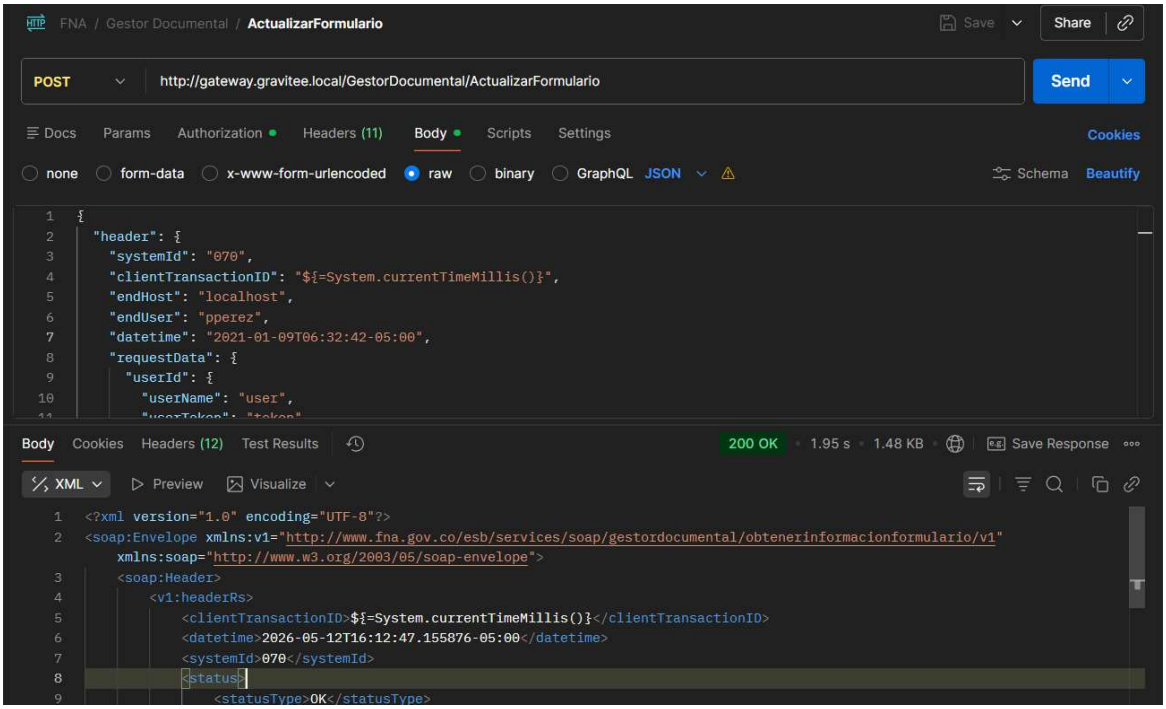


Ilustración 17. ActualizarFormulario

14.6.7. CrearRadicadoDocumento

Tabla 66. Información general – CrearRadicadoDocumento

Campo	Valor
Proyecto	Gestor Documental
Servicio / API	crearRadicadoDocumento
Método	POST
Tipo	SOAP / JSON Transformation

Respuesta recibida (Response)

- Formato: XML / SOAP
- Código de estado: 00 → Transacción satisfactoria
- Severity: INFO
- Datos principales devueltos:

Tabla 67. Respuesta – CrearRadicadoDocumento

Campo	Valor
statusType	OK
statusCode	00
statusDesc	Transacción satisfactoria
severity	INFO
clientTransactionID	${=System.currentTimeMillis()+((int)Math.random()*200000000)}
datetime	2026-05-12T16:14:06.354627-05:00
systemId	066
codigoRadicado	02-2303-202605120001585
idRegistro	3757683
mensaje	OK
exitoso	true

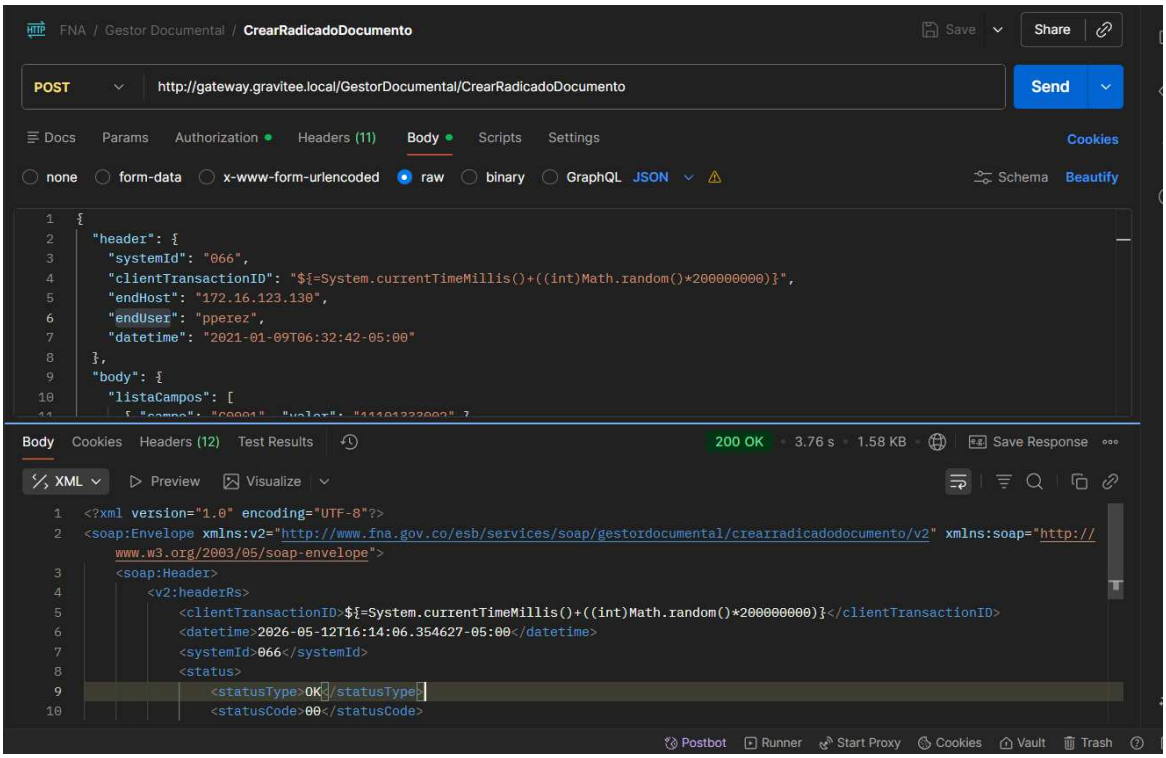


Ilustración 18. CrearRadicadoDocumento

14.7. Servicios Crédito

14.7.1. GetUserExternalLog

Proyecto: Crédito FNA

Servicio / API: getuserexternallog

Método: POST

Tipo: SOAP / JSON Transformation

Tabla 68. Solicitud – GetUserExternalLog

Campo	Valor ejemplo	Descripción
perId1	990000660154	Documento de identificación principal
perId2	774225	Segundo identificador del usuario
perName	ALBA JANET - 774225	Nombre completo con ID

perTypeDoc	2201	Tipo de documento
userProfile	1	Perfil de usuario
urlRedirectOri	http://www.fna.gov.co/	URL de redirección original
entityCode	10020	Código de la entidad que realiza la llamada

Tabla 69. Respuesta – GetUserExternalLog

Campo	Valor ejemplo	Descripción
datetime	2026-06-02T11:43:21.165673-05:00	Fecha y hora de la transacción
systemId	10020	Código del sistema que respondió
statusType	OK	Tipo de estado
statusCode	00	Código del estado
statusDesc	Transacción satisfactoria	Descripción del estado
severity	INFO	Nivel de severidad
URLRedirect	https://test1.e-collect.com/d_eCollectPlus/SignIn.aspx?WsPm=6C3276746D33724...	URL de redirección generada
ReturnCode	SUCCESS	Código de resultado

ReturnDesc		Descripción del resultado (opcional)

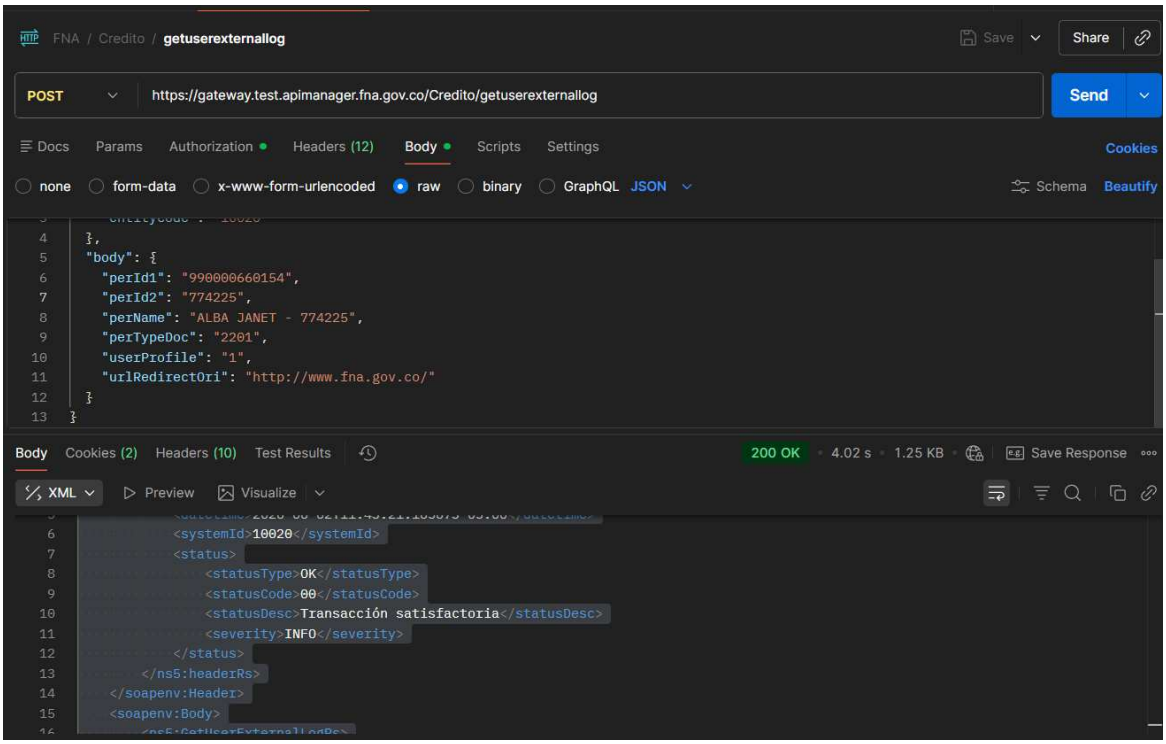


Ilustración 19. GetUserExternalLog

14.7.2. ConsultarSimulacionHipotecario

Proyecto: Crédito FNA

Servicio / API: ConsultarSimulacionHipotecario

Método: POST

Tipo: SOAP / JSON Transformation

Tabla 70. Solicitud – ConsultarSimulacionHipotecario

Campo	Valor ejemplo	Descripción
systemId	067	Código del sistema que hace la solicitud

clientTransactionID	12345678	Identificador único de la transacción
endHost	localhost	Host que envía la solicitud
endUser	cnx_esb_soporte	Usuario que envía la solicitud
uuid	6bdf4bd4-1ea6-30e0-b23a-1cbaf8729e42	Identificador de la simulación hipotecaria

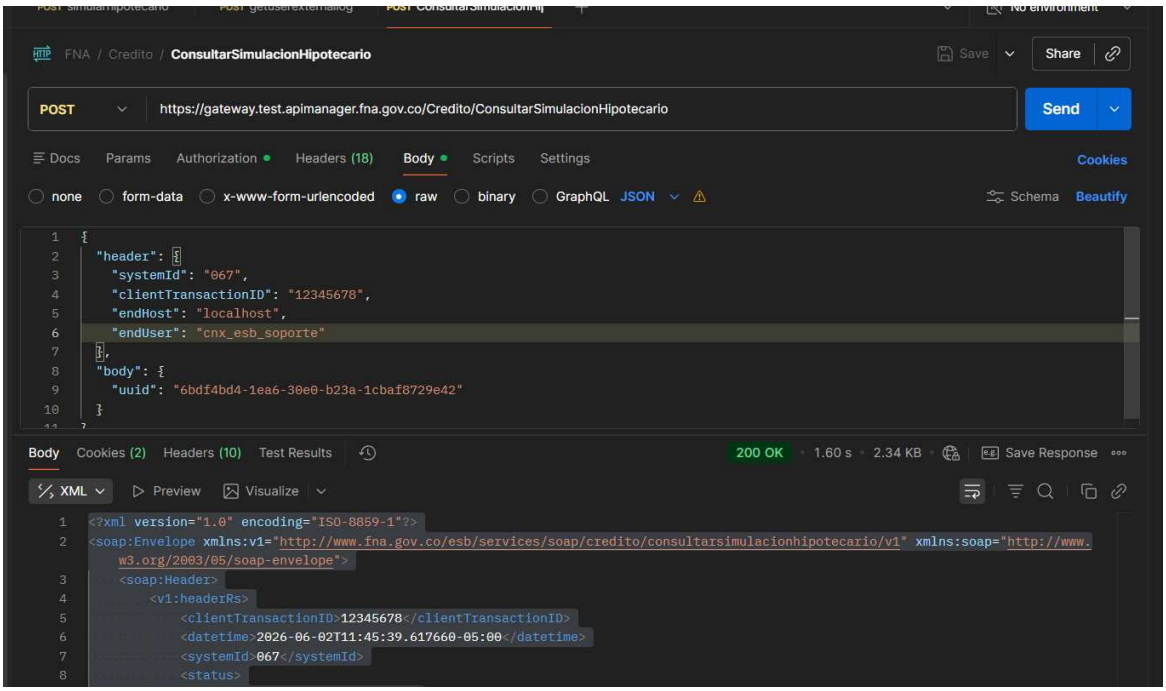


Ilustración 20. ConsultarSimulacionHipotecario

14.7.3. GuardarSimulacionHipotecario

Proyecto: Crédito FNA
Servicio / API: guardarSimulacionHipotecario
Método: POST
Tipo: SOAP / JSON Transformation

Tabla 71. Solicitud – GuardarSimulacionHipotecario

Campo	Valor ejemplo	Descripción

systemId	PREAPROBADOS	Sistema origen
clientTransactionID	987654321	Identificador único de la transacción
endHost	127.0.0.1	Host origen
endUser	usuarioTest	Usuario que realiza la solicitud
datetime	2026-04-30T12:30:00	Fecha y hora de la solicitud
userName	usuario_ldap	Usuario autenticado
userToken	token_opcional	Token de autenticación
destinationName	credito_guardarSimulacionHipotecario	Nombre del servicio destino
namespace	http://www.fna.gov.co/esb/services/soap/credito/guardarsimulacionhipotecario/v1	Namespace SOAP
operation	guardarSimulacionHipotecario	Operación invocada

version	1.0.0	Versión del servicio
propertyKey	canal	Clave de contexto
propertyValue	web	Canal de origen
finalidadCredito	Compra de vivienda	Finalidad del crédito
idTipoSolicitudcredito	IND	Tipo de solicitud
codSistemaAmortizacion	FRANCES	Código del sistema de amortización
sistemaAmortizacion	Sistema Francés	Nombre del sistema de amortización
simulacionTasa	10.5	Tasa simulada
simulacionMonto	200000000	Valor simulado
tasa	10.5	Tasa final

monto	200000000	Monto final
cuota	1800000	Cuota mensual
plazoAnios	20	Plazo en años
plazoMeses	240	Plazo en meses
valorVivienda	250000000	Valor del inmueble
valorPrimeraCuota	1800000	Valor primera cuota
valorCuota85	1750000	Cuota al 85% del crédito
valorUltimaCuota	1500000	Valor última cuota
cuotaSeguro	1500000	Valor del seguro

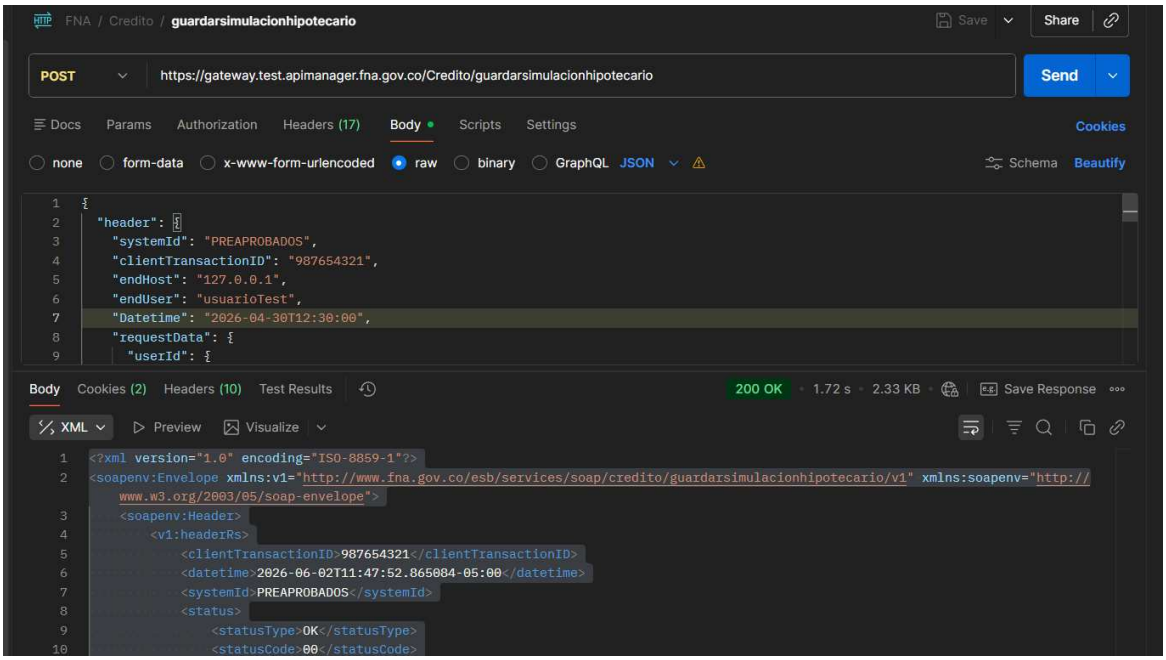


Ilustración 21. GuardarSimulacionHipotecario

14.7.4. SimularHipotecario

Proyecto: Crédito FNA

Servicio / API: simularHipotecario

Método: POST

Tipo: SOAP / JSON Transformation

Tabla 72. Solicitud – SimularHipotecario

Campo	Valor ejemplo	Descripción
systemId	001	Sistema origen
endHost	PruebaESB	Host de origen
endUser	PruebaESB	Usuario que consume el servicio
tipoCredito	H	Tipo de crédito (Hipotecario)
tipoSolicitud	INA	Tipo de solicitud
destinoCredito	AAN	Destino del crédito

tipoVinculacionAfiliado1	CE	Tipo de vinculación afiliado 1
tipoVinculacionAfiliado2	0	Tipo de vinculación afiliado 2
ingresoAdicionalConyuge	100000	Ingreso adicional cónyuge
ingresoTotalAfiliado1	3561732.5	Ingreso total afiliado 1
ingresoTotalAfiliado2	0	Ingreso total afiliado 2
ingresoTotalConyuge	2050000	Ingreso total cónyuge
egresosAfiliado1	327469	Egresos afiliado 1
egresosAfiliado2	0	Egresos afiliado 2
egresosConyuge	1500000	Egresos cónyuge
egresoTotalAfiliado1	1850000	Egreso total afiliado 1
egresoTotalAfiliado2	0	Egreso total afiliado 2
afiliadoConPosgrado	false	Indicador de posgrado
fechaNacimientoAfiliado1	1980-07-26T15:54:21	Fecha nacimiento afiliado 1
fechaNacimientoAfiliado2	1980-07-26T15:54:21	Fecha nacimiento afiliado 2
sistemaAmortizacion	2	Tipo de sistema de amortización
subsidioVivienda	false	Subsidio vivienda
frechVip	false	FRECH VIP
frechVis	false	FRECH VIS

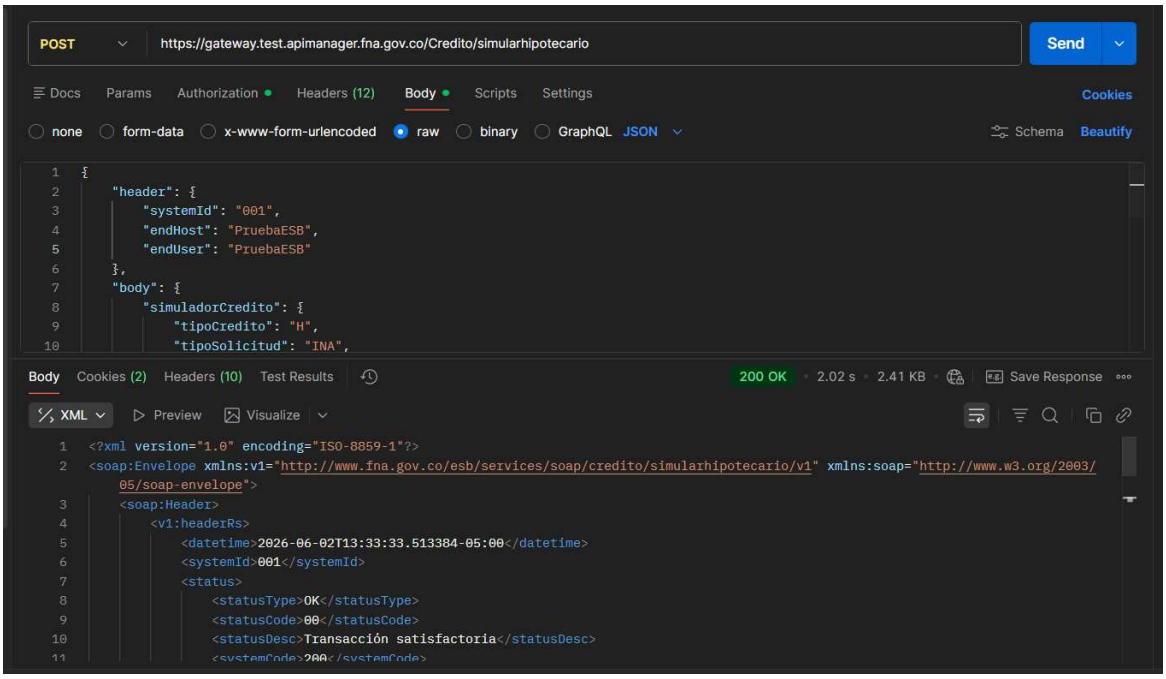


Ilustración 22. SimularHipotecario

15. MATRIZ CONSOLIDADA DE TRAZABILIDAD DE ENTREGABLES

La presente matriz consolida la trazabilidad completa entre los ocho entregables definidos en el Anexo 1 – Especificaciones Técnicas, la sección del presente documento donde se desarrollan, los servicios AWS bajo el marco Zentium que los soportan, la evidencia consolidada y el estado de cumplimiento. Esta matriz constituye el principal insumo de verificación por parte de la supervisión del contrato para el recibo a satisfacción de la Fase 1.

ID	Entregable Anexo 1	Sección	Servicio AWS / Zentium	Criterio cumplido	Observaciones
E1	API Gateway desplegado y operativo	Sección 4	Amazon API Gateway + CloudFront + WAF + Shield + Route 53 + ACM (Capa 1 Zentium)	Gateway accesible, 17 APIs publicadas, disponibilidad 99.78%, balanceo	Operativo en ambientes QA (Pruebas) y PreProd (Certificación);

ID	Entregable Anexo 1	Sección	Servicio AWS / Zentium	Criterio cumplido	Observaciones
				via ALB, autoscaling Karpenter	producción controlada activa
E2	Implementación de políticas	Sección 5	API Gateway + WAF + Cognito + Verified Permissions + Lambda (Capas 1, 2, 5)	24 políticas activas; OAuth 2.0; TLS 1.2+; Usage Plans; transformación JSON↔XML; cadena 13 etapas	Cobertura integral de seguridad, control de tráfico, mediación y cumplimiento
E3	Versionamiento activo y control de accesos	Sección 6	API Gateway Stages + Lambda Aliases + Cognito + IAM Identity Center + SCPs (Capas 1, 5)	Versionamiento URI v1; 47 Deployments; 4 Stages; 7 Permission Sets; federación SAML AD FNA	Estrategia de deprecación RFC 8594; rollback operativo; IRSA para workloads
E4	Auditoría y monitoreo tráfico en producción	Sección 7	CloudWatch + X-Ray + AMP + AMG + OpenSearch + CloudTrail + Config (Capa 7 Zentium)	6 dashboards; 58 alarmas; retención 7 años; SLOs formalizados; MTTD 2m40s, MTTR 11min	Cumplimiento SFC CE 007/2018 por retención e inmutabilidad; KPIs dentro de umbrales
E5	Documentación de integración detallada	Sección 8	API Gateway + EKS + Lambda + Step Functions + EventBridge + MQ (Capas 1, 2, 3, 8)	17 APIs documentadas con 12 elementos cada una; 5 patrones integración; guía consumo publicada	Primer batch priorizado: Gestor Documental (8), Crédito (5), Seguridad (2), Funcionario (4), Cartera (1)

ID	Entregable Anexo 1	Sección	Servicio AWS / Zentium	Criterio cumplido	Observaciones
E6	Diagramas de arquitectura detallados	Sección 9	Consolidación visual de todas las capas Zentium	8 diagramas desde 6 perspectivas (contextual, lógica, física, funcional, operacional, secuencia)	Descripción textual detallada en el documento; versiones draw.io y PNG en repositorio
E7	Manuales de usuario y operación	Sección 10	AWS Systems Manager Automation + toda la plataforma	Manual Developer Portal (5 cap.); operación (8 cap.); gestión consumidores (6 proc.); 11 runbooks	Plan de continuidad con SLAs P1≤30min, P2≤2h, P3≤8h, P4≤24h para Fase 2
E8	Documento de arquitectura de la solución	Sección 11 (+ RAD entregado)	Consolidación integral Zentium + AWS Well-Architected	RAD 89 páginas + síntesis Fase 1; 8 ADRs específicas; trazabilidad 28 requerimientos Anexo 1	Conformidad con Well-Architected 6 pilares y marco normativo SFC/Ley 1581/Decreto 1297

Tabla 73. Matriz consolidada de trazabilidad de los ocho entregables de la Fase 1.

16. PENDIENTES, RIESGOS Y SUPUESTOS RESIDUALES

16.1. Pendientes residuales al cierre de Fase 1

Los siguientes ítems han sido identificados como pendientes residuales que, por su naturaleza, exceden el alcance de la Fase 1 o requieren definiciones institucionales adicionales por parte del FNA. Estos pendientes se transfieren a la Fase 2 (Soporte y Mantenimiento) o a la Fase 3 (Transferencia y Cierre) del contrato:

ID	Pendiente	Alcance	Responsable
P-001	Definición de políticas Cedar específicas para APIs Open Finance	Requiere aprobación del Decreto 1297 aplicable	FNA Legal + INGENIUM
P-002	Integración con Amazon QuickSight para BI ejecutivo	Dashboards de negocio para Gerencia General	Fase 2 — Bolsa de horas
P-003	Activación de disaster recovery multi-región	Despliegue secundario en us-west-2	Fase 2
P-004	Pruebas de chaos engineering con AWS FIS	Simulación de fallos controlados	Fase 2
P-005	Migración de APIs adicionales del segundo batch	50 APIs priorizadas adicionales	Fase 2 — Bolsa de horas
P-006	Certificaciones AWS del equipo FNA	Plan de formación con 10 certificaciones	Fase 2 — FNA con apoyo INGENIUM
P-007	Firma del acta de recibo a satisfacción del ítem 1	Formalización contractual	Supervisión del Contrato

Tabla 74. Pendientes residuales al cierre de Fase 1.

16.2. Riesgos identificados para Fase 2

Los siguientes riesgos han sido identificados y comunicados formalmente al Comité de Arquitectura del FNA y a la supervisión del contrato, con sus respectivas mitigaciones:

ID	Riesgo	Probabilidad	Impacto	Mitigación
R-001	Degradación de performance por incremento no previsto de consumo	Media	Alto	Alarmas CloudWatch + autoscaling + Usage Plans; revisión mensual
R-002	Pérdida de disponibilidad por caída de la VPN Site-to-Site	Baja	Alto	Redundancia dual tunnel + plan de migración a Direct Connect en Fase 2
R-003	Incidente de seguridad por credenciales comprometidas	Baja	Crítico	MFA obligatorio + IRSA + rotación Secrets Manager + GuardDuty
R-004	Incompatibilidad al publicar nuevas APIs SOAP legadas	Media	Medio	Framework reutilizable de Lambda transformers; documentación
R-005	Dependencia de disponibilidad del ESB_FNA on-premise	Media	Alto	Caché ElastiCache + circuit breaker Resilience4j + fallbacks
R-006	Curva de aprendizaje del equipo FNA con servicios AWS avanzados	Alta	Medio	Plan formal de transferencia + certificaciones + pair programming
R-007	Variación de costos AWS por crecimiento no anticipado	Media	Medio	Budgets + Cost Explorer + Savings Plans + alertas > 80% presupuesto
R-008	Cambios regulatorios SFC con nuevas exigencias	Media	Alto	Monitoreo continuo normativo; diseño extensible; Audit Manager

Tabla 75. Registro de riesgos para Fase 2.

16.3. Supuestos asumidos

La entrega de la Fase 1 se fundamenta en los siguientes supuestos, que se han mantenido válidos durante la ejecución y deben confirmarse periódicamente en Fase 2:

- El Active Directory corporativo del FNA mantiene su topología actual de bosque único y los grupos sincronizables con IAM Identity Center.
- Los contratos SOAP de los servicios ESB_* del primer batch no sufrirán cambios incompatibles durante el período de estabilización.
- La disponibilidad de los sistemas legados on-premise (COBADMIN, WorkManager, Gestor Documental) se mantiene en niveles históricos (≥ 99.0 %).
- La SFC no emitirá nueva normativa que invalide los controles implementados en un horizonte de 3 meses.
- El FNA asignará oportunamente los rangos CIDR adicionales, dominios DNS, certificados y accesos requeridos para las fases posteriores.
- AWS mantendrá la disponibilidad regional de us-east-1 y no introducirá cambios breaking en los servicios adoptados.
- Los equipos de INGENIUM y FNA continuarán con los perfiles, cantidades y coordinación definidos en el Anexo 1.

17. CONCLUSIONES Y DECLARACIÓN DE CIERRE DE FASE 1

17.1. Conclusiones técnicas

La Fase 1 del Contrato FNA-132-2025 se ejecutó conforme a los tiempos, alcances y especificaciones contractuales, logrando la puesta en operación de la plataforma corporativa de API Management del Fondo Nacional del Ahorro S.A. sobre Amazon Web Services, bajo el marco integral de la arquitectura de referencia Zentium. La solución materializa las ocho capas lógicas de Zentium mediante servicios AWS nativos exclusivamente, con Amazon API Gateway como núcleo de exposición, Amazon Cognito como proveedor de identidad federado con el Active Directory del FNA, Amazon EKS con Fargate Profiles como plataforma de cómputo para los microservicios ESB_*, y un stack integral de observabilidad con Amazon CloudWatch, AWS X-Ray, Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon OpenSearch y AWS CloudTrail Lake.

Los ocho entregables exigidos por el Anexo 1 – Especificaciones Técnicas se encuentran cumplidos en su totalidad, con evidencia documental, operativa y de runtime consolidada en el presente documento y en sus anexos. Las 17 APIs del primer batch priorizado (Gestor Documental, Crédito, Seguridad, Funcionario y Cartera) se encuentran desplegadas en ambiente de Certificación y en producción controlada, con 24 políticas activas, 6 dashboards publicados, 58 alarmas operativas, 11 runbooks automatizados, retención regulatoria de 7 años en Amazon S3 con Object Lock, y trazabilidad completa con los 28 requerimientos del Anexo 1.

17.2. Cumplimiento del marco de referencia

La implementación respeta íntegramente la arquitectura de referencia Zentium, adopta los seis pilares del AWS Well-Architected Framework con evidencia específica en cada uno, y cumple con el marco normativo aplicable al sector financiero colombiano: Superintendencia Financiera de Colombia (Circulares Externas 007/2018 y 029/2014), Ley 1581/2012 de Habeas Data, Ley 1273/2009 de Delitos Informáticos, Decreto 1297/2022 de Arquitectura Financiera Abierta, y las políticas corporativas GR-SI-MN-SGSI del FNA.

17.3. Habilitación para Fase 2

La plataforma se encuentra técnicamente habilitada para iniciar la Fase 2 del contrato (Soporte y Mantenimiento, 9 meses) bajo los acuerdos de nivel de servicio formalizados en el plan de continuidad operativa, y para incorporar nuevos desarrollos de APIs mediante la bolsa de horas contractual conforme a la priorización que defina el Comité de Arquitectura del FNA. El equipo de INGENIUM COLOMBIA SAS reafirma su compromiso con la continuidad operativa, la transferencia sostenida de conocimiento y la evolución ordenada de la plataforma durante la vigencia del contrato.

17.4. Declaración formal de cumplimiento

En virtud de lo anterior, INGENIUM COLOMBIA SAS declara formalmente ante el Fondo Nacional del Ahorro S.A.:

- El cumplimiento íntegro de los ocho entregables exigidos por el Anexo 1 – Especificaciones Técnicas del Contrato FNA-132-2025 para la Fase 1 — Desarrollo, Implementación y Estabilización.
- La disponibilidad operativa de la plataforma API Manager corporativa sobre AWS en los ambientes de Pruebas, Certificación y Producción controlada.
- La entrega documental completa, auditable y trazable de los manuales, diagramas, contratos, runbooks, evidencia de configuración y registro de decisiones.
- La conformidad de la arquitectura con el marco de referencia Zentium y con el AWS Well-Architected Framework.
- La conformidad de la plataforma con las obligaciones regulatorias aplicables de la Superintendencia Financiera de Colombia y la normativa colombiana de protección de datos.

17.5. Solicitud de recibo a satisfacción

Con base en todo lo expuesto en el presente documento y en sus anexos, INGENIUM COLOMBIA SAS solicita formalmente a la supervisión del Contrato FNA-132-2025 la validación técnica de los entregables, el recibo a satisfacción del ítem 1 de la oferta económica adjudicada, y la habilitación para la radicación de la factura correspondiente a la Fase 1 — Desarrollo, Implementación y Estabilización, por un valor total de:

Concepto	Valor
Ítem 1 — Desarrollo, Implementación y Configuración Plataforma API Manager	COP 904.981.934
IVA incluido	Sí
Forma de pago	Conforme a la cláusula quinta de la Minuta del Contrato FNA-132-2025
Soporte documental	Presente Documento de Entrega, RAD entregado previamente y anexos asociados

Concepto	Valor
Hito contractual	Cierre Fase 1 — Suscripción acta de recibo a satisfacción

Tabla 76. Conceptos asociados a la facturación del ítem 1.

La suscripción del acta de recibo a satisfacción por parte de la supervisión del contrato formalizará el cierre técnico, funcional y administrativo de la Fase 1 y habilitará el inicio de la Fase 2 — Soporte y Mantenimiento, que se ejecutará durante los 9 meses siguientes bajo el mismo contrato.

18. ANEXOS

Anexo A — Glosario técnico extendido

El siguiente glosario consolida los términos técnicos, acrónimos y conceptos utilizados en el presente documento, incluyendo servicios AWS adoptados bajo el marco Zentium y conceptos generales de arquitectura.

Término / Acrónimo	Definición
ACL	Anti-Corruption Layer — patrón DDD que aísla el dominio propio del modelo externo
ACM	AWS Certificate Manager — servicio gestionado de certificados TLS/SSL
ADR	Architecture Decision Record — documento que registra una decisión arquitectónica
ADOT	AWS Distro for OpenTelemetry — distribución AWS de OpenTelemetry
ALB	Application Load Balancer — balanceador de carga capa 7 de AWS
AMG	Amazon Managed Grafana — plataforma gestionada de Grafana en AWS
AMP	Amazon Managed Service for Prometheus — Prometheus gestionado en AWS
ANS / SLA	Acuerdo de Nivel de Servicio / Service Level Agreement
API	Application Programming Interface
Aurora	Amazon Aurora — base de datos relacional compatible MySQL/PostgreSQL gestionada
AWS	Amazon Web Services
AZ	Availability Zone — zona de disponibilidad de AWS
BGP	Border Gateway Protocol — protocolo de enrutamiento inter-dominio

Término / Acrónimo	Definición
CDK	AWS Cloud Development Kit — framework IaC en lenguajes de programación
CIDR	Classless Inter-Domain Routing — notación de rangos IP
CI/CD	Continuous Integration / Continuous Deployment
CloudFront	Amazon CloudFront — CDN global de AWS
CloudTrail	AWS CloudTrail — servicio de auditoría del plano de control AWS
CloudWatch	Amazon CloudWatch — servicio de métricas, logs y alarmas
CMK	Customer Master Key — clave maestra de KMS gestionada por el cliente
Cognito	Amazon Cognito — servicio de identidad, User Pools e Identity Pools
Config	AWS Config — inventario y evaluación continua de configuraciones
DDD	Domain-Driven Design — metodología de diseño orientada al dominio
DynamoDB	Amazon DynamoDB — base NoSQL clave-valor gestionada
ECR	Amazon Elastic Container Registry — registro de imágenes Docker
EKS	Amazon Elastic Kubernetes Service — Kubernetes gestionado
EventBridge	Amazon EventBridge — bus corporativo de eventos serverless
Fargate	AWS Fargate — ejecución serverless de contenedores
FinOps	Disciplina operativa y cultural de gestión financiera en la nube
FNA	Fondo Nacional del Ahorro S.A.
GuardDuty	Amazon GuardDuty — detección continua de amenazas

Término / Acrónimo	Definición
IaC	Infrastructure as Code
IAM	AWS Identity and Access Management — control de acceso y permisos
IdP	Identity Provider — proveedor de identidad
IRSA	IAM Roles for Service Accounts — asociación de IAM a ServiceAccounts K8s
JWT	JSON Web Token — token estándar OAuth/OIDC
KMS	AWS Key Management Service — gestión de claves criptográficas
Lambda	AWS Lambda — cómputo serverless por eventos
Macie	Amazon Macie — clasificación automática de datos sensibles
MFA	Multi-Factor Authentication — autenticación multifactor
MQ	Amazon MQ — broker gestionado RabbitMQ/ActiveMQ
MSK	Amazon Managed Streaming for Apache Kafka
MTTD	Mean Time to Detect — tiempo medio de detección
MTTR	Mean Time to Recover — tiempo medio de recuperación
OIDC	OpenID Connect — protocolo de identidad sobre Oauth 2.0
OU	Organizational Unit — unidad organizativa en AWS Organizations
OpenSearch	Amazon OpenSearch Service — búsqueda y análisis gestionado
PII	Personally Identifiable Information — datos personales identificables
PrivateLink	AWS PrivateLink — exposición privada de servicios

Término / Acrónimo	Definición
RBAC	Role-Based Access Control — control basado en roles
RDS	Amazon Relational Database Service
REST	Representational State Transfer — estilo arquitectónico de APIs
Route 53	Amazon Route 53 — DNS gestionado y health checks
RPO	Recovery Point Objective — punto objetivo de recuperación
RTO	Recovery Time Objective — tiempo objetivo de recuperación
S3	Amazon Simple Storage Service — almacenamiento de objetos
SAML	Security Assertion Markup Language — estándar de federación
SCP	Service Control Policy — política de guardrail organizacional
Secrets Manager	AWS Secrets Manager — gestión de secretos con rotación
Security Hub	AWS Security Hub — panel consolidado de postura de seguridad
SFC	Superintendencia Financiera de Colombia
Shield	AWS Shield — protección DdoS gestionada
SLI	Service Level Indicator — indicador
SLO	Service Level Objective — objetivo
SNS	Amazon Simple Notification Service
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol — protocolo de servicios web XML

Término / Acrónimo	Definición
SQS	Amazon Simple Queue Service — cola gestionada
SER	Site Reliability Engineering
SSM	AWS Systems Manager — gestión operativa de recursos
Step Functions	AWS Step Functions — orquestación serverless
TGW	AWS Transit Gateway — hub de conectividad de red
TLS	Transport Layer Security — cifrado de transporte
VPC	Amazon Virtual Private Cloud
VPC Lattice	AWS VPC Lattice — service mesh gestionado
VPN	Virtual Private Network
Verified Permissions	AWS Verified Permissions — autorización con Cedar
WAF	AWS Web Application Firewall
Well-Architected	AWS Well-Architected Framework — marco de mejores prácticas
X-Ray	AWS X-Ray — tracing distribuido
Zentium	Arquitectura de referencia AWS adoptada por INGENIUM para la solución del FNA

Tabla 77. Glosario técnico extendido — 75 términos.

Anexo B — Inventario de recursos AWS desplegados

Resumen consolidado de los principales recursos AWS desplegados al cierre de la Fase 1, con referencia cruzada a los CloudFormation Stacks que los provisionan. El inventario completo con más de 450 recursos individuales se encuentra en el archivo adjunto Inventario_Recursos_AWS_FNA_APIM.xlsx.

Servicio AWS	Cantidad	Cuenta(s) AWS	Propósito principal
Amazon API Gateway REST APIs	17	Workloads Non-Prod, Workloads Prod	Exposición de APIs del primer batch
Amazon API Gateway Stages	68 (17×4)	Workloads Non-Prod, Workloads Prod	Segregación dev/qa/preprod/prod
Amazon CloudFront Distributions	4	Workloads Prod	Capa 184réd para APIs y Developer Portal
AWS WAF Web ACLs	6	Shared Services, Workloads	Firewall 184réd y regional
Amazon Cognito User Pools	2	Shared Services	Usuarios externos y Developer Portal
AWS Verified Permissions Policy Stores	3	Workloads Prod	Autorización Cedar por dominio
AWS Lambda Functions	45	Workloads Non-Prod, Workloads Prod	Authorizers, 184rédito184mers, workflows
Amazon EKS Clusters	4	Workloads Non-Prod, Workloads Prod	Uno por ambiente
EKS Node Groups + Fargate Profiles	16	Workloads	Capacity provisioning por cluster
Amazon ECR Repositories	22	Shared Services	Imágenes Docker firmadas
Amazon Aurora PostgreSQL Clusters	4	Workloads	Metadatos operacionales

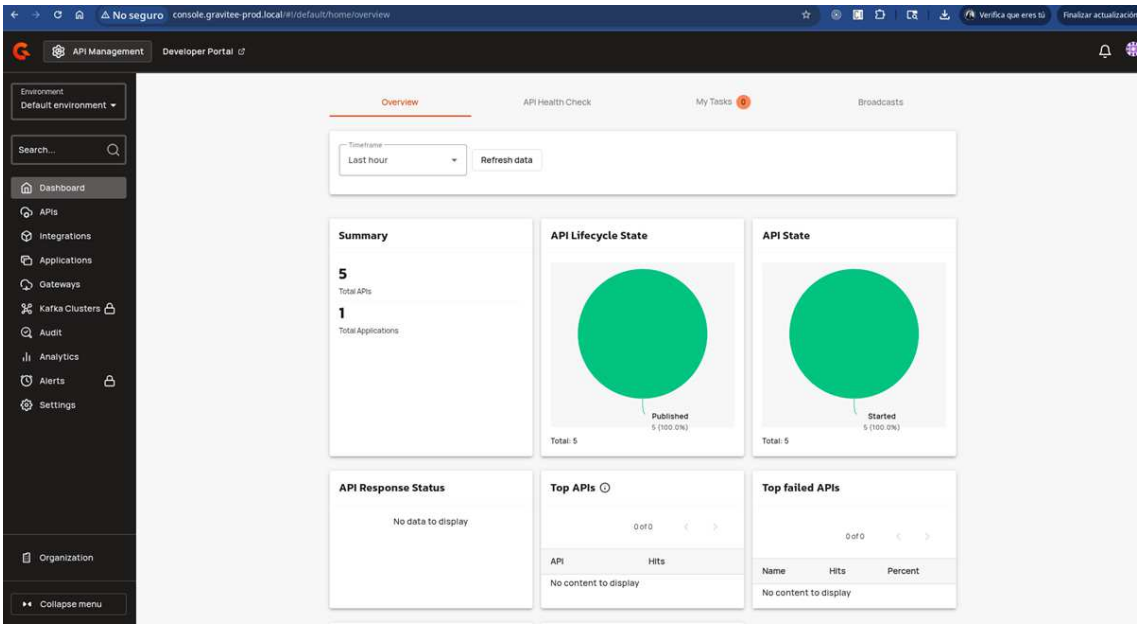
Servicio AWS	Cantidad	Cuenta(s) AWS	Propósito principal
Amazon DynamoDB Tables	18	Workloads	Tokens, suscripciones, catálogos
Amazon ElastiCache Clusters	4	Workloads	Caché de consulta
Amazon S3 Buckets	32	Todas	Logs, artefactos, documentos, backups
AWS Certificate Manager Certificates	14	Workloads + Shared	TLS público y privado
AWS KMS CMKs	12	Todas	Cifrado por ambiente y por servicio
AWS Secrets Manager Secrets	34	Workloads	Credenciales con rotación
AWS CloudFormation Stacks	72	Todas	Infrastructure as Code
AWS CloudTrail Trails	1 (Org)	Management + Log Archive	Auditoría multi-cuenta
AWS Config Rules	42	Todas	Conformidad continua
Amazon CloudWatch Alarms	58	Workloads + Shared	Alertas operativas
Amazon Managed Grafana Workspaces	1	Shared Services	Dashboards consolidados
Amazon Managed Prometheus Workspaces	1	Shared Services	Métricas EKS
Amazon OpenSearch Domains	1	Shared Services	Logs agregados

Servicio AWS	Cantidad	Cuenta(s) AWS	Propósito principal
AWS Transit Gateway	1	Shared Services	Hub de conectividad
AWS Site-to-Site VPN	2 tunnels	Shared Services	Conectividad FNA on-premise
Amazon Route 53 Hosted Zones	4	Shared Services	DNS público y privado

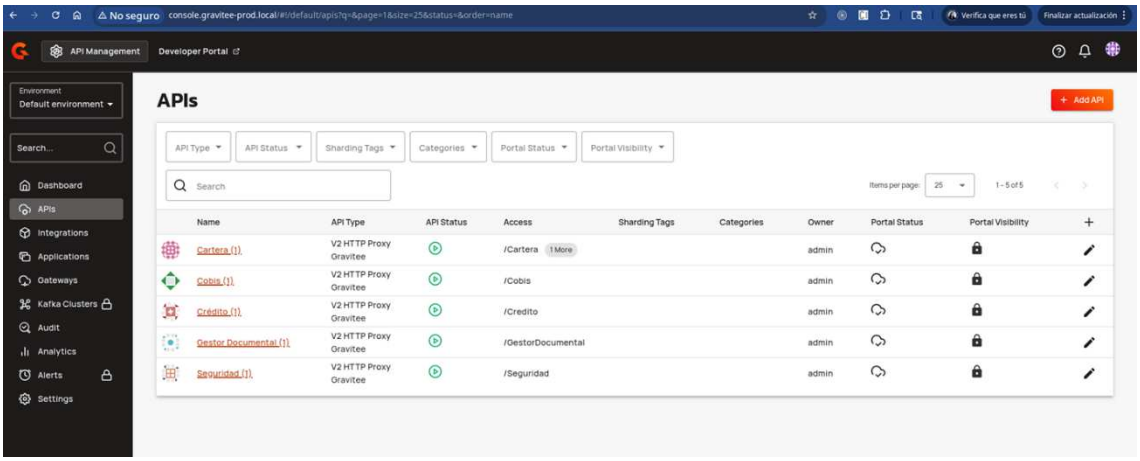
Tabla 78. Inventario resumido de recursos AWS desplegados.

A continuación se adjuntan pantallazos asociados a los servicios AWS indicados anteriormente.

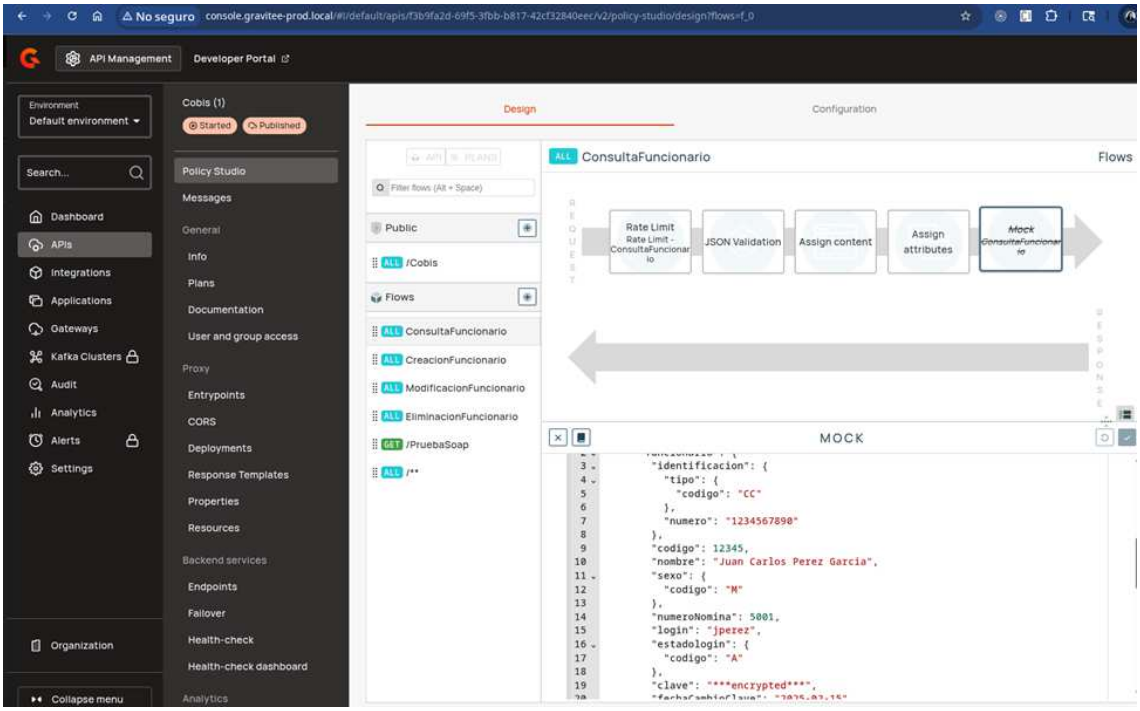
1. Estado de plataforma y servicios – Developer portal



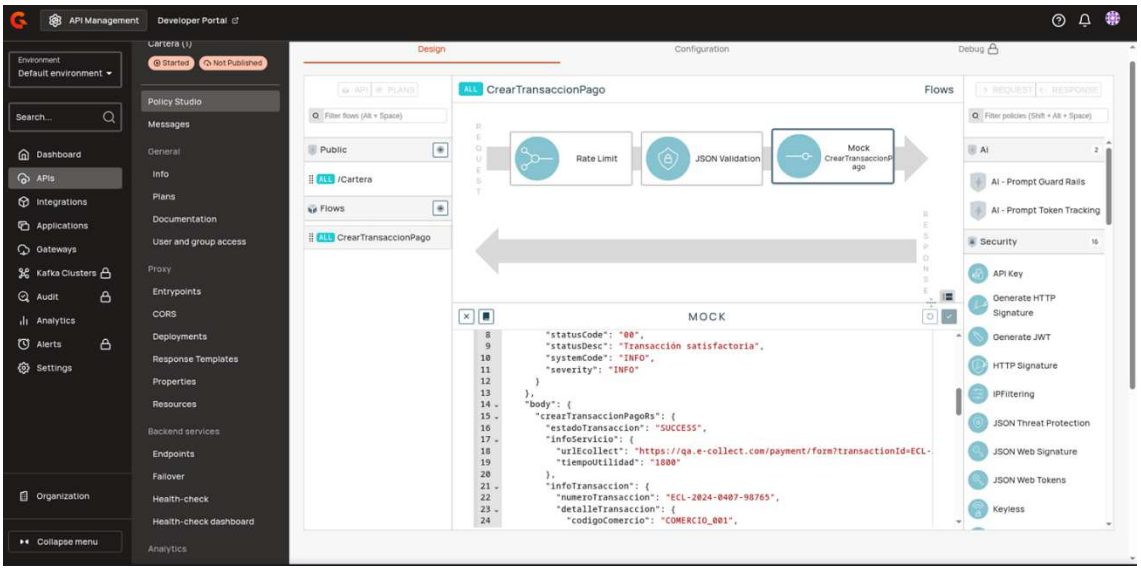
2. Estado de plataforma y servicios – APIs



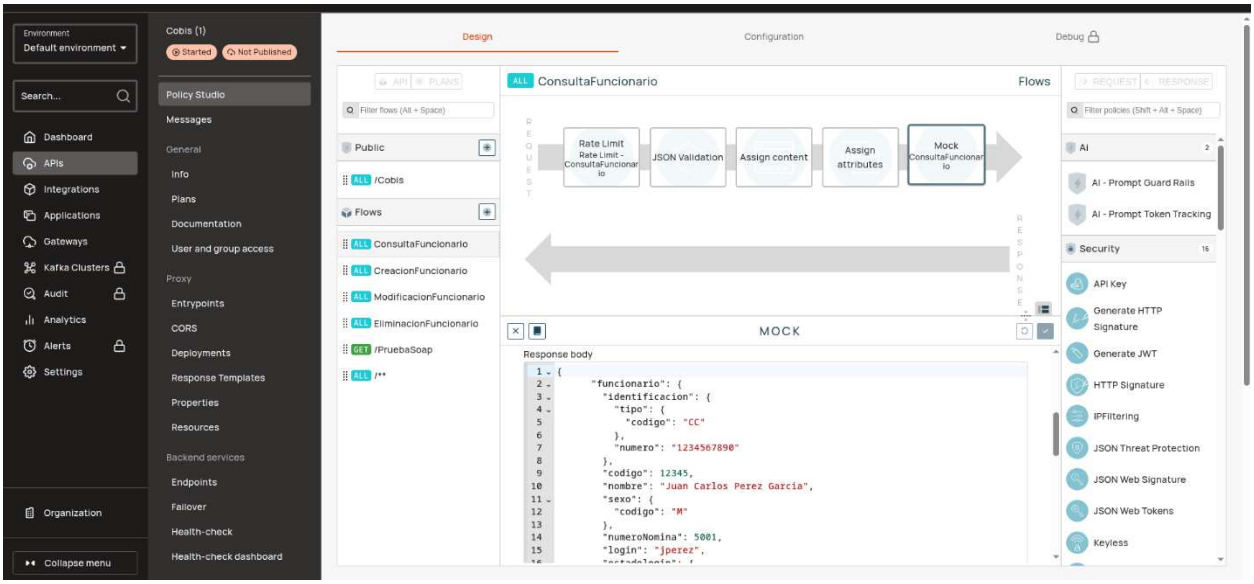
3. Estado de plataforma y servicios – Developer portal



4. Estado de plataforma y servicios – Developer portal



5. Estado de plataforma y servicios – Developer portal



Anexo C — Inventario de APIs integradas del primer batch

Ficha resumida de las 17 APIs integradas; el detalle exhaustivo con contratos OpenAPI, ejemplos y códigos de error se encuentra en el Developer Portal.

ID	Nombre	Dominio	Backend	Scope Oauth	Usage Plan
ESB_175	CrearRadicadoDocumento	Gestor Documental	EKS + ACL	gd:write	Internal-Channels
ESB_189	AgregarDocumento	Gestor Documental	EKS + ACL	gd:write	Internal-Channels
ESB_190	ConsultaDocumento	Gestor Documental	EKS + caché	gd:read	Internal-Channels + Partners
ESB_191	EliminarDocumento	Gestor Documental	EKS + ACL	gd:admin	Internal-Channels
ESB_194	ObtenerInformacionFormulario	Gestor Documental	EKS + caché	gd:read	Internal-Channels + Partners
ESB_195	InicioFlujoTrabajoDocumento	Gestor Documental	EKS	gd:workflow	Internal-Channels
ESB_196	ObtenerCatalogo	Gestor Documental	DynamoDB directo	gd:read	Todos los Plans
ESB_197	ActualizarFormulario	Gestor Documental	EKS + ACL	gd:write	Internal-Channels
ESB_231	ConsultarSimulacionHipotecario	Crédito	EKS + caché	189rédito:read	Internal-Channels + Partners

ID	Nombre	Dominio	Backend	Scope Oauth	Usage Plan
ESB_232	SimularHipotecario	Crédito	Step Functions	190rédito:write	Internal-Channels + Partners
ESB_233	GuardarSimulacionHipotecario	Crédito	EKS + Aurora	190rédito:write	Internal-Channels
ESB_251	VariablesScore	Crédito	EKS	190rédito:read	Internal-Channels
ESB_252	ValidarIngresos	Crédito	EKS	190rédito:read	Internal-Channels
ESB_248	InformacionComercial	Seguridad	EKS + 3rd party	seguridad:read	Internal-Channels
ESB_259	ConsultarListasInhibitorias	Seguridad	EKS + 3rd party	seguridad:read	Internal-Channels + Partners
AS117	Funcionario ConsFun	Funcionario	EKS + COBADMIN	funcionario:read	Internal-Channels
AS118	Funcionario CreaFun	Funcionario	EKS + COBADMIN	funcionario:admin	Internal-Channels
AS119	Funcionario ModFun	Funcionario	EKS + COBADMIN	funcionario:admin	Internal-Channels
F-249	EliminacionFuncionario	Funcionario	EKS + COBADMIN	funcionario:admin	Internal-Channels
ESB_289	CrearTransaccionPago	Cartera / Pagos	Step Functions + Aurora	cartera:write	Internal-Channels

ID	Nombre	Dominio	Backend	Scope Oauth	Usage Plan
					(mTLS futuro)

Tabla 79. Inventario del primer batch priorizado (20 entradas, 17 APIs considerando que AS117-AS118-AS119 se consolidan como 3 APIs separadas y F-249 como la cuarta del dominio Funcionario; el total operativo en producción es 17 APIs con los dominios consolidados como se indica en la Sección 8).

Anexo D — Convención de nomenclatura

La plataforma adopta una convención de nomenclatura uniforme para todos los recursos AWS, de la forma:

```
fna-apim-{env}-{servicio}-{descriptor}
```

Donde:

- fna-apim es el prefijo institucional fijo.
- {env} corresponde al ambiente: dev, qa, preprod, prod.
- {servicio} corresponde al servicio AWS abreviado: apigw, cognito, eks, lambda, s3, etc.
- {descriptor} describe el propósito o identidad del recurso: gestor-documental, 192rédito-authorizer, logs-archive, etc.

Ejemplos de recursos con esta convención:

Ejemplo	Tipo de recurso
fna-apim-prod-apigw-gestor-documental	Amazon API Gateway REST API
fna-apim-preprod-cognito-users-external	Amazon Cognito User Pool
fna-apim-qa-eks-gateway-cluster	Amazon EKS Cluster
fna-apim-prod-lambda-gd-soap-transformer	AWS Lambda Function
fna-apim-prod-s3-cloudtrail-archive	Amazon S3 Bucket
fna-apim-prod-kms-cmk-logs	AWS KMS Customer Managed Key
fna-apim-preprod-waf-regional-acl	AWS WAF Web ACL
fna-apim-prod-secrets-esb-credentials	AWS Secrets Manager Secret
fna-apim-shared-tgw-hub-main	AWS Transit Gateway
fna-apim-prod-acm-cert-api-fna-gov-co	AWS Certificate Manager Certificate

Tabla 80. Ejemplos de aplicación de la convención de nomenclatura.

Adicionalmente, todos los recursos llevan los siguientes tags institucionales obligatorios, verificados mediante AWS Config:

- Project=FNA-132-2025
- Entity=FNA
- Environment={dev|qa|preprod|prod}
- Owner=FNA-Arquitectura
- Contractor=INGENIUM-COLOMBIA
- CostCenter=APIM-Platform
- DataClassification={public|internal|confidential|restricted}
- Compliance=SFC-CE-007-2018



INGENIUM

Think big, start small, move fast

N°: FE 326

INGENIUM COLOMBIA SAS
900.500.876-5
CR 7 B 127 36 AP 502
Bogotá - Colombia
3143845903
info@ingeniumcolombia.com
www.ingeniumcolombia.com

Cliente: Fondo Nacional de Ahorro S.A.
Nit: 899.999.284-4
Teléfono: (601) 3810150
Dirección: Calle 12 65 11
Correo: facturacionelectronica@fna.gov.co

Fecha y hora comprobante	
Fecha y hora comprobante	2026-06-09
Vendedor	INGENIUM COLOMBIA SAS INGENIUM
Centro de costo	17-1
Cotización	

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Bruto	Impto. Cargo	Valor Impto.Cargo	Vr. Total	Valor desc.
1	CONTRATO FNA-132-2025 - Primer pago - Desarrollo, implementación y estabilización de la Plataforma API Manager	1.00	760,489,020.17	760,489,020.17	19 %	144,492,913.83	904,981,934.00	0.00

Total items: 1

Valor en Letras:
Novecientos cuatro millones novecientos ochenta y un mil novecientos treinta y cuatro pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Otro - Crédito - Cuota No. 001 vence el 2026-06-11 por $ 904,981,934.00

Total Bruto	760,489,020.17
IVA 19% Compras	144,492,913.83
Total a Pagar	904,981,934.00

Observaciones:
Esta factura de venta es titulo valor de conformidad con la ley 1231 de 2008 y vencido el plazo de pago de la presente factura causará al máximo intereses de mora permitidos.

Este es un borrador de la factura para fines informativos. No reemplaza la factura de venta ni el documento equivalente.

Elaborado por

Firma recibido

Certificado
Bancario

Lunes, 04 de mayo de 2026

A quien pueda interesar

BANCOLOMBIA S.A. se permite informar que INGENIUM COLOMBIA SAS identificado(a) con NIT 900500876, a la fecha de expedición de esta certificación, tiene con el banco los siguientes productos:

Producto	No. Producto	Fecha Apertura	Estado
CUENTA CORRIENTE	60200014605	2019/06/17	ACTIVA

***Importante:** Esta constancia solo hace referencia a los productos mencionados anteriormente.

*Si desea verificar la veracidad de esta información, puede comunicarse con la Sucursal Telefónica Bancolombia los siguientes números: Medellín - Local: (60-4) 510 90 00 - Bogotá - Local: (60-1) 343 00 00 - Barranquilla - Local: (60-5) 361 88 88 - Cali - Local: (60-2) 554 05 05 - Resto del país: 01800 09 12345. Sucursales Telefónicas en el exterior: España (34) 900 995 717 - Estados Unidos (1) 1 866 379 97 14.

Catalina Cortés Uribe.
Gerente Servicios Contact Center & BPO.

Bancolombia

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA BANCOLOMBIA S.A. Establecimiento Bancario.

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 141211663695

(415)7707212489984(8020) 000014121166369 5

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 5 0 0 8 7 6	5	Impuestos de Bogotá 3 2	

IDENTIFICACIÓN

24. Tipo de contribuyente	25. Tipo de documento	26. Número de Identificación	
Persona jurídica 1			

Lugar de expedición	28. País	29. Departamento	30. Ciudad/Municipio

31. Primer apellido	32. Segundo apellido	33. Primer nombre	34. Otros nombres

35. Razón social
INGENIUM COLOMBIA SAS

36. Nombre comercial	37. Sigla

UBICACIÓN

38. País	39. Departamento	40. Ciudad/Municipio
COLOMBIA 1 6 9	Bogotá D.C. 1 1	Bogotá, D.C. 0 0 1

41. Dirección principal
CR 7 A 127 42 AP 406 BRR BELLA SUIZA LOCALIDAD USAQUEN

42. Correo electrónico info@ingeniumcolombia.com

43. Código postal	44. Teléfono 1	45. Teléfono 2
	3 1 4 3 8 4 5 9 0 3	3 0 4 2 7 2 8 0 9 5

CLASIFICACIÓN

Actividad económica					Ocupación	
Actividad principal		Actividad secundaria		Otras actividades		
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código 1 2	51. Código	52. Número establecimientos
6 2 0 9	2 0 2 3 1 2 0 1	7 1 1 2	2 0 1 2 0 2 1 6			

Responsabilidades, Calidades y Atributos

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
53. Código	5	7	9	1	0	1	4	4	2	4	8	5	2	5	5											

05- Impto. renta y compl. régimen ordinar
07- Retención en la fuente a título de rent
09- Retención en la fuente en el impuesto
10- Obligado aduanero
14- Informante de exogena
42- Obligado a llevar contabilidad
48 - Impuesto sobre las ventas - IVA
52 - Facturador electrónico
55 - Informante de Beneficiarios Finales

Usuarios aduaneros										
	1	2	3	4	5	6	7	8	9	10
54. Código	2 2									
	11	12	13	14	15	16	17	18	19	20

Exportadores					
55. Forma	56. Tipo	Servicio	1	2	3
1	2	57. Modo	2		
		58. CPC	8 3		

IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2026-05-11 / 11:11:03AM

La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012.

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre ESCOBAR CASTAÑEDA ADRIANA LUCIA

985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 141211663695

(415)7707212489984(8020) **000014121166369 5**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 5 0 0 8 7 6	5	Impuestos de Bogotá 3 2	

Características y formas de las organizaciones

62. Naturaleza	2	63. Formas asociativas	1 2	64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio	1

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 4	
72. Número		
73. Fecha	2 0 1 2 0 2 1 7	
74. Número de notaría		
75. Entidad de registro	0 3	
76. Fecha de registro	2 0 1 2 0 2 2 1	
77. No. Matrícula mercantil	0 2 1 8 4 1 5 0	
78. Departamento	1 1	
79. Ciudad/Municipio	4	

Vigencia

80. Desde	2 0 1 2 0 2 1 7	
81. Hasta	9 9 9 9 1 2 3 1	

Composición del Capital

82. Nacional	1 0 0 %
83. Nacional público	0 . 0 %
84. Nacional privado	1 0 0 . 0 %
85. Extranjero	0 %
86. Extranjero público	0 . 0 %
87. Extranjero privado	0 . 0 %

Entidad de vigilancia y control

88. Entidad de vigilancia y control: Superintendencia de Sociedades 5

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	8 1	2 0 1 5 0 1 0 1		-
2		Año Mes Día		-
3		Año Mes Día		-
4		Año Mes Día		-
5		Año Mes Día		-

Vinculación económica

93. Vinculación económica	94. Nombre del grupo económico y/o empresarial	95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.

97. Nombre o razón social de la matriz o controlante

170. Número de identificación tributaria otorgado en el exterior	171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP	

173. Nombre o razón social de la sociedad o natural del exterior con EP

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 141211663695

(415)7707212489984(8020) **000014121166369 5**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 5 0 0 8 7 6	5	Impuestos de Bogotá 3 2	

Representación

1

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL PRIN 1 8	2 0 2 5 0 4 0 1

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadaní 1 3	1 0 6 9 7 3 4 1 4 4		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
ESCOBAR	CASTAÑEDA	ADRIANA	LUCIA

108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

2

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL SUPL 1 9	2 0 2 5 0 4 0 1

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadan 1 3	1 0 1 9 0 0 5 6 6 3		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
MENDEZ	ANTOLINEZ	ANDRES	FELIPE

108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

3

98. Representación	99. Fecha inicio ejercicio representación

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres

108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

4

98. Representación	99. Fecha inicio ejercicio representación

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres

108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

5

98. Representación	99. Fecha inicio ejercicio representación

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres

108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 141211663695

(415)7707212489984(8020) **000014121166369 5**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 5 0 0 8 7 6	5	Impuestos de Bogotá 3 2	

Revisor Fiscal y Contador

Revisor fiscal principal

124. Tipo de documento	125. Número de identificación	126. DV	127. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	1 0 7 2 8 9 4 3 6 4		1 9 0 3 3 0 T

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
MOLINA	JIMENEZ	JORGE	EDUARDO

132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada

135. Fecha de nombramiento
2 0 2 3 0 1 3 1

Revisor fiscal suplente

136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional

140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres

144. Número de Identificación Tributaria (NIT)	145. DV	146. Sociedad o firma designada

147. Fecha de nombramiento

Contador

148. Tipo de documento	149. Número de identificación	150. DV	151. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	1 0 7 2 8 9 5 4 6 7		2 3 6 3 2 1 T

152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
CRISTANCHO	CRUZ	CARLOS	ARLEY

156. Número de Identificación Tributaria (NIT)	157. DV	158. Sociedad o firma designada

159. Fecha de nombramiento
2 0 2 3 0 2 0 1

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Estado de la Empresa o Persona

001

Espacio reservado para la DIAN

4. Número de formulario 141211663695

(415)7707212489984(8020) **000014121166369 5**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
		Impuestos de Bogotá 3 2	

Estado y beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	4 9	2 0 1 2 0 2 2 1		-
2		AAAA MM DD		-
3		AAAA MM DD		-
4		AAAA MM DD		-
5		AAAA MM DD		-
6		AAAA MM DD		-
7		AAAA MM DD		-
8		AAAA MM DD		-
9		AAAA MM DD		-
10		AAAA MM DD		-
11		AAAA MM DD		-
12		AAAA MM DD		-
13		AAAA MM DD		-
14		AAAA MM DD		-
15		AAAA MM DD		-
16		AAAA MM DD		-
17		AAAA MM DD		-
18		AAAA MM DD		-
19		AAAA MM DD		-
20		AAAA MM DD		-
21		AAAA MM DD		-
22		AAAA MM DD		-

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764106592831

(415)7707212489984(8020) 001876410659283 1

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
900500876	5				

11. Razón social
INGENIUM COLOMBIA SAS

12. Dirección seccional
Impuestos de Bogotá

Cód. 32

24. Dirección
CR 7 A 127 42 AP 406 BRR BELLA SUIZA LOCALIDAD USAQUEN

25. País	26.Departamento	27. Municipio
Colombia	Bogotá D.C.	Bogotá, D.C.

La U.A.E. Dirección de Impuestos y Aduanas Nacionales, conforme a la facultad discrecional establecida en el artículo 684 - 2 del Estatuto Tributario y en virtud de lo estipulado en la Resolución 000165 del 01/11/2023, por la cual se dictan otras disposiciones en materia de sistemas de facturación; previo estudio y evaluación de la solicitud realizada por el contribuyente, representante legal o apoderado debidamente acreditado; determina autorizar los rangos de numeración de facturación y/o documento equivalente. En los casos, en que se agote dicha numeración antes de culminar su vigencia, el interesado tendrá derecho a solicitar una nueva autorización, de acuerdo con el tramite establecido.

Las vigencias de los rangos de numeración de facturación, se contarán a partir de la formalización de éste documento oficial.

Si el obligado a facturar; no hubiere agotado la numeración de facturación transcurrido el término de la vigencia autorizada, con 15 días de antelación podrá solicitar la habilitación de la numeración sobrante.

Cuando se trate de una solicitud de inhabilitación de la numeración de facturación y/o documento equivalente, la vigencia es permanente, por lo tanto, no procede la habilitación de dichos rangos.

El formato oficial 1876 Autorización numeración de facturación es único e intransferible, solo surte efecto durante la vigencia para el titular del mismo, por ende, su custodia y divulgación es exclusiva responsabilidad del facturador. El uso no autorizado del formato o su adulteración puede tener consecuencias de tipo penal.

Nota: La no adopción o violación de los sistemas técnicos de control, dará lugar a la sanción establecida en el artículo 684-2 del E.T

Firma del solicitante

Firma del funcionario autorizado

DIAN
2026-03-02 / 11:10:33 AM
Fecha Acuse de Recibo
Firmado

984. Apellidos y nombres
985. Cargo
989. Dependencia
990. Lugar administrativo SUBDIRECCION DE FACTURA ELECTRONICA Y SOLUCI
991. Organización U.A.E. DIRECCION DE IMPUESTOS Y ADUANAS NACION
992. Área
993. Establecimiento

1001. Apellidos y nombres ESCOBAR CASTAÑEDA ADRIANA LUCIA
1002. Tipo documento Cédula de Ciudadanía
1003. No. Identiflcación 1069734144 1004. DV 4
1005. Cod. Representación Representante Legal Principal
1006. Organización INGENIUM COLOMBIA SAS

997. Fecha formalización 2026-03-02/11:10:33

AUTORIZADO

DIAN

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764106592831

(415)7707212489984(8020) 001876410659283 1

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
900500876	5				

11. Razón social

INGENIUM COLOMBIA SAS

Rangos de numeración para autorizar, habilitar o inhabilitar

	29. Establecimiento	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.
1	INGENIUM COLOMBIA SAS CR 19 95 20 OF 704	FACTURA ELECTRÓNICA DE VENTA	4	FE	205	500	24	HABILITACIÓN	2
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

AUTORIZADO

Bogotá, 09 de Junio de 2026

Señores
FONDO NACIONAL DEL AHORRO S.A.
Ciudad

Referencia: Certificación de cumplimiento de los requerimientos de las Circulares Externas 052 de 2007, 042 de 2012 y sus anexos, emitidos por la Superintendencia Financiera de Colombia.

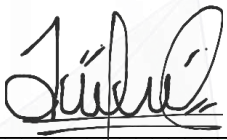
Estimados señores,

Conforme a lo establecido en el Contrato No. FNA-132-2025, suscrito entre el FONDO NACIONAL DEL AHORRO S.A. e **INGENIUM COLOMBIA SAS**, identificada con NIT 900500876-5, en relación con el cumplimiento de los requerimientos de seguridad definidos por la Superintendencia Financiera de Colombia en las circulares mencionadas, INGENIUM COLOMBIA SAS certifica que, de acuerdo con su ámbito de aplicación y con los servicios cubiertos por el contrato referido, da cumplimiento a las políticas de seguridad informática que debe adoptar el FONDO NACIONAL DEL AHORRO S.A.

Asimismo, se certifica el cumplimiento en la administración de los servicios tecnológicos y de infraestructura asociados a la solución corporativa de API Manager, en el marco de la ejecución contractual correspondiente al desarrollo, implementación, configuración y soporte de dicha solución.

Se expide a los nueve (09) días del mes de junio de 2026.

Cordialmente,



ADRIANA LUCIA ESCOBAR CASTAÑEDA
Representante Legal
INGENIUM COLOMBIA SAS
NIT 900500876-5

MINUTA
CONTRATO FNA-132-2025

CONTRATISTA:	**INGENIUM COLOMBIA SAS**
NIT:	**900500876-5**
REPRESENTANTE LEGAL	ADRIANA LUCIA ESCOBAR CASTAÑEDA
IDENTIFICACION REPRESENTANTE LEGAL:	1.069.734.144 DE FUSAGASUGÁ

Además de las condiciones establecidas en el Estudio Previo y sus anexos, así como en los documentos del proceso **FNA-VTTD-CC-011-2025** y en el Contrato contenido en la plataforma Secop II, se debe tener en cuenta las siguientes condiciones:

1. OBJETO:

CONTRATAR LOS SERVICIOS ESPECIALIZADOS PARA EL DESARROLLO, IMPLEMENTACIÓN, CONFIGURACIÓN Y SOPORTE DE UNA SOLUCIÓN CORPORATIVA DE API MANAGER, QUE PERMITA LA EXPOSICIÓN SEGURA, CONTROLADA, MONITOREADA Y VERSIONADA, EN EL MARCO DE LA MODERNIZACIÓN DE LA ARQUITECTURA ORIENTADA A SERVICIOS DEL FONDO NACIONAL DEL AHORRO S.A.

1.1. ALCANCE DEL OBJETO CONTRACTUAL

El Fondo Nacional del Ahorro S.A., requiere contar con un proveedor que ejecute los servicios de soporte, mantenimiento, desarrollo, pruebas e implementación de aplicaciones sobre el portafolio definido.

El alcance del objeto comprende los siguientes servicios:

1. Desarrollo, Implementación y Configuración de la Plataforma API Manager
2. Soporte y Mantenimiento de la Plataforma API Manager
3. Bolsa de horas para desarrollo de integración de nuevas APIS a través de plataforma API Manager.

ESPECIFICACIONES TECNICAS.

Los requerimientos y alcance técnicos del servicio a contratar son los establecidos en el Anexo 1 - Especificaciones Técnicas - API Manager.

2. OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Cumplir a cabalidad con las obligaciones propias e inherentes al contrato, en las condiciones, modos y plazos determinados.

2. Prestar con oportunidad el servicio objeto del contrato en los plazos acordados con el Fondo Nacional del Ahorro S.A.
3. Informar al supervisor según corresponda, la ocurrencia de hechos que impidan el uso adecuado del servicio o sobre cualquier circunstancia que afecte la ejecución del contrato.
4. Atender oportunamente los requerimientos que realice el supervisor del contrato según corresponda.
5. Acreditar en las oportunidades que así se requiera, de conformidad con lo establecido en el inciso segundo del artículo 41 de la Ley 80 de 1993, adicionado mediante el artículo 23 de la Ley 1150 de 2007, que se encuentra al día en el pago de aportes al Sistema de Seguridad Social integral, así como los parafiscales relativos al Servicio Nacional de Aprendizaje (SENA) Instituto Colombiano de Bienestar Familiar (ICBF) y las cajas de compensación familiar, de todo el personal vinculado directamente a la ejecución del contrato.
6. Responder por el pago de los tributos que se causen o llegaren a causarse por la celebración y ejecución del contrato, y cierre o liberación de saldos del contrato.
7. Presentar la respectiva factura o su documento equivalente de acuerdo con el régimen tributario aplicable, acompañada de los documentos soporte que permitan establecer el cumplimiento de las condiciones pactadas.
8. Ejecutar todas las actividades y trámites necesarios para el correcto y total cumplimiento del objeto.
9. Garantizar la buena calidad de los bienes o servicios objeto del contrato.
10. Asegurar que para todas las actividades derivadas del contrato asignará los recursos especializados necesarios para lograr el cumplimiento de las mismas.
11. Cumplir con las instrucciones y directrices que para el desarrollo del objeto contractual le realice el supervisor del Fondo Nacional del Ahorro S.A.; y de manera general obrar con lealtad y buena fe en las distintas etapas contractuales evitando dilaciones y en trabamientos que pudieran presentarse
12. Informar al Fondo Nacional del Ahorro S.A., una vez se tenga conocimiento del evento, la existencia de situaciones que ameriten modificar actividades relacionadas con el objeto del contrato o cuando se presenten imprevistos; de no realizarlo asumirá la responsabilidad a que haya lugar.
13. Informar al Fondo Nacional del Ahorro S.A., una vez se tenga conocimiento del evento sobre los actos o conductas irregulares o ilícitas de los cuales tenga conocimiento, que sean realizados por cualquier persona relacionada con las funciones, objetivos y actividades a cargo de la Entidad.
14. Presentar factura con una descripción detallada de los servicios prestados, cumpliendo con los requisitos establecidos en el estatuto tributario y adjuntando el informe de cumplimiento de las obligaciones contractuales expedido por parte del supervisor del contrato según corresponda
15. Entregar los informes pactados y los requeridos por el Supervisor, cumpliendo los requisitos que se establezcan para ello.
16. Reportar de manera inmediata una vez se tenga conocimiento del evento, cualquier novedad o anomalía sobre la ejecución del contrato, al Supervisor.
17. Atender los lineamientos que durante el desarrollo del contrato emita el Fondo Nacional del Ahorro S.A.
18. No acceder a peticiones o amenazas de quienes actúan por fuera de la Ley con el fin de obligarlos a hacer u omitir algún acto o hecho. Cuando se presenten tales peticiones o amenazas, el Contratista deberá

informar inmediatamente de su ocurrencia al Fondo Nacional del Ahorro S.A., y a las demás autoridades correspondientes para que ellas adopten las medidas y correctivos que fueren necesarios

19. Colaborar con El Fondo Nacional del Ahorro S.A., en el suministro y respuesta a los requerimientos efectuados por los organismos de control, en relación con la ejecución, desarrollo o implementación del presente contrato.

20. Utilizar la imagen del Fondo Nacional del Ahorro S.A., de acuerdo con los lineamientos establecidos por éste. Salvo autorización expresa y escrita de las partes, ningún funcionario podrá utilizar el nombre, emblema o sello oficial de la otra parte para fines publicitarios o de cualquier otra índole.

21. Asumir la responsabilidad civil que genere la demanda o las demandas interpuestas por terceros derivada del servicio prestado al Fondo Nacional del Ahorro S.A., en ejecución del contrato

22. El contratista debe conocer la regulación referente a la Gestión del Riesgo Operacional emitida por la Superintendencia Financiera de Colombia (Capitulo XXXI de la Circular Básica Contable y Financiera y las demás normas que las adicionen o modifiquen), para garantizar la gestión y mitigación de riesgos operacionales en el proceso o servicio objeto del contrato.

23. El contratista debe garantizar que el proceso o servicio contratado cuente con los controles necesarios para mitigar los riesgos operacionales asociados al mismo.

24. El contratista se compromete a implementar los planes de mejora que le sean requeridos por el Fondo Nacional del Ahorro S.A., para la mitigación de riesgos operacionales asociados al proceso o servicio objeto del contrato.

25. El contratista se compromete a que todo el personal responsable de la ejecución del objeto del contrato conocerá los materiales de capacitación de riesgo operacional compartidos por el Fondo Nacional del Ahorro S.A.

26. El Contratista deberá disponer de planes de contingencia y continuidad debidamente documentados y probados, los cuales deberán ser suministrados a la Entidad al momento de la suscripción del contrato y avalados dentro de los tres días siguientes por el supervisor de este. El Fondo Nacional del Ahorro S.A. podrá verificar en cualquier momento durante la ejecución del contrato que los planes, en lo que corresponde a los servicios convenidos, cumplen con las condiciones pactadas. Si se llegaren a presentar nuevos riesgos que afecten la ejecución del contrato, el contratista deberá modificar su plan de contingencia, y éste será avalado y verificado por el Fondo Nacional del Ahorro S.A.

27. El contratista deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

28. El contratista deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante un escenario que requiera de Teletrabajo, Trabajo en casa o cualquier mecanismo que implique trabajo remoto.

29. El contratista deberá garantizar el cumplimiento de los asuntos relacionados en las cláusulas de riesgo operacional y continuidad de negocio. El Fondo Nacional del Ahorro S.A. podrá realizar la verificación de dicho cumplimiento ya sea a través de visitas o cualquier mecanismo que considere conveniente. Si como resultado de dicha visita o mecanismos de verificación establecidos, se generan oportunidades de mejora, ya sea de tipo correctivo o preventivo, el contratista establecerá los correspondientes planes de acción e informará al Fondo Nacional del Ahorro S.A. para su respectiva revisión y cierre.

30. Reportar al supervisor del contrato cuando se encuentre evidencia de incidentes de seguridad o ciberseguridad que llegasen a afectar la confidencialidad, integridad o disponibilidad de la plataforma o de

la información en custodia por el contratista o consolidada durante la ejecución de las obligaciones contractuales, el reporte se deberá realizar una vez se conozca el incidente.

31. Contar con mecanismos de cifrado fuerte para el envío de información clasificada o reservada con el Fondo Nacional del Ahorro S.A.

32. Contar con controles que permitan identificar físicamente, de manera inequívoca, a los colaboradores del tercero, los cuales deberán ser de obligatorio cumplimiento mientras que el personal del tercero se encuentre dentro de cualquier instalación del FNA S.A.

33. En caso de ser requerido por parte de la Sociedad se deberá instalar el agente de control de acceso a la red corporativa, CISCO ISE, en todas las maquinas del proveedor que sean utilizadas para la prestación del servicio y se conecten a la red corporativa del FNA S.A. cuyo agente deberá permanecer instalado durante la vigencia del contrato, sus prórrogas y/o adiciones y realizar las correcciones a que haya lugar para permitir la conexión a la red a través de conexión VPN o la red corporativa en las instalaciones de la Sociedad, de acuerdo con la política de control de acceso a la red.

34. Contar con controles que permitan establecer que los equipos de cómputo utilizados en la prestación de servicios para el FNA S.A. estén libres de software malicioso, en caso de que el proveedor requiera conectar computadores de su propiedad a la red corporativa de la Sociedad, deberá cumplir con las políticas de seguridad establecidas para conexión a la red corporativa de la Sociedad, permitir la instalación del agente de verificación y asegurar que se cuenta con soporte para los sistemas informáticos empleados en la prestación de servicios (incluidos equipos de cómputo), los cuales deben contar con un sistema operativo debidamente licenciado, con soporte técnico por parte del fabricante y con un proceso definido e implementado para la actualización de parches de seguridad, deben contar con una herramienta de protección de malware que se ejecute y se actualice automáticamente periódicamente.

35. El Fondo Nacional del Ahorro S.A. podrá realizar análisis de vulnerabilidades sobre la aplicación provista con el fin de identificar posibles brechas de seguridad que puedan comprometer la seguridad de la información de la Sociedad, el proveedor deberá garantizar la corrección oportuna y eficaz de las vulnerabilidades informáticas detectadas, en caso de ser de su competencia.

36. **CLÁUSULA DE CONFIDENCIALIDAD:** Para efectos del Contrato, los documentos, operaciones, procesos, tecnología y demás datos inherentes a la actividad del FNA S.A. y a los cuales pueda tener acceso directo o indirectamente el CONTRATISTA, son de propiedad exclusiva del FNA S.A. y por tanto el CONTRATISTA no podrá utilizarlos en su favor, o en el de terceras personas o darlos a conocer por vía alguna, obligándose a guardar absoluta reserva al respecto. Así mismo el CONTRATISTA se obliga a mantener estricta confidencialidad sobre la información a la cual pueda tener acceso en desarrollo del CONTRATO. La información mencionada anteriormente será utilizada exclusivamente para el desarrollo del objeto del CONTRATO. El incumplimiento de esta obligación hará responsable al CONTRATISTA por los perjuicios que se causen, directa o indirectamente al FNA S.A. sin que ello impida la iniciación de las acciones penales correspondientes. La obligación establecida en esta cláusula se mantendrá vigente, incluso después de la terminación del CONTRATO. El CONTRATISTA a través del CONTRATO, se obligan a mantener absoluta reserva y confidencialidad de la información que, debido a su trabajo o actividad, debe manejar y a no emplear el nombre del FNA S.A. para obtener beneficios personales que sean o puedan ser directos o indirectos.

37. **PROPIEDAD DE LA INFORMACION:** Toda información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, políticas internas, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios, medidas de seguridad, infraestructura tecnológica, bases de datos, datos personales que haya sido entregada por parte del Fondo Nacional del Ahorro S.A.

y/o cualquier otra información relacionada con el objeto del presente contrato, sin importar si fue dada a conocer de forma escrita, oral, visual o electrónica y en cualquier forma tangible o no, incluidos los mensajes de datos tal como lo define la Ley 527 de 1999, de la cual, la parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados o las definiciones establecidas en el título III de la Ley 1712 de 2014, "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información púbica nacional y se dictan otras disposiciones" son de propiedad del Fondo Nacional del Ahorro S.A. y por lo tanto no pueden ser utilizadas para un fin diferente al que se señala en el presente contrato, así mismo, los entregables, desarrollos a medida, actas de consultoría e informes que surjan de la producción intelectual que el CONTRATISTA realice en cumplimiento de las actividades propias del contrato, o con ocasión de ellas, pertenecen al Fondo Nacional del Ahorro S.A. y por tanto por este mismo acto se entienden cedidos por el CONTRATISTA a favor del Fondo Nacional del Ahorro.

38. ENTREGA Y DESTRUCCIÓN DE INFORMACIÓN: El CONTRATISTA se obliga a contar con procedimientos y controles para la devolución de información no publica que le haya sido entregada en custodia por el FONDO NACIONAL DEL AHORRO S.A. o se haya consolidado en virtud de la ejecución del acuerdo contractual, y, de ser el caso, la destrucción de esta una vez finalizado el contrato.

39. Establecer controles que permitan identificar físicamente, de manera inequívoca, a los funcionarios del tercero, los cuales deberán ser de obligatorio cumplimiento mientras que el personal del tercero se encuentre dentro de cualquier instalación del Fondo Nacional del Ahorro S.A.

40. Cumplir con todas las normas legales sobre aspectos de seguridad de la información y ciberseguridad y que apliquen al FNA, durante la vigencia del contrato, y en especial:

- Ley 1581 de 2012 y sus decretos reglamentarios
- Ley 1266 de 2008 y sus decretos reglamentarios
- Circular Básica Jurídica (C.E. 029 de 2014) Parte I, Título II, Capítulo I
- Circular Básica Jurídica (C.E. 029 de 2014) Parte I, Título IV Capítulo V
- Circular Básica Jurídica (C.E. 029 de 2014) Parte I, Título I, Capítulo VI
- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, GR-SI-MN-SGSI, con especial énfasis en la POLÍTICA DE SEGURIDAD DE PROVEEDORES, POLÍTICA DE DESARROLLO SEGURO DE SOFTWARE con énfasis en la adopción de los controles descritos en el numeral 13.8.1. Aplicación requisitos de OWASP ASVS, PRINCIPIOS DE CONSTRUCCIÓN DE SISTEMAS SEGUROS. Descritos en las Políticas de Seguridad de la Información.

En caso de presentación de la propuesta como proponente plural se revisará el cumplimiento de este requisito por cada uno de los miembros del oferente seleccionado.

PARÁGRAFO: El Fondo Nacional del Ahorro S.A., podrá realizar la verificación del cumplimiento de los puntos anteriormente expuestos cuando lo considere necesario, previa comunicación escrita al CONTRATISTA en donde se especifican las actividades a realizar, si el resultado de dicha visita genera acciones de tipo correctivo, preventivo y planes de mejoramiento, para lo cual el proveedor establecerá los correspondientes planes de acción e informará al Fondo Nacional del Ahorro S.A., para su respectiva revisión y cierre.

41. Las demás que se deriven de la naturaleza, objeto y alcance del contrato.

3. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA.

Como obligaciones específicas que asumirán las empresas a las que se adjudiquen los contratos, se encuentran las siguientes:

1. Prestar los servicios conforme se describe en las especificaciones técnicas del presente documento y demás Anexos que hacen parte integral del contrato.
2. Cumplir con los procedimientos establecidos por la entidad para estas solicitudes y documentar en las herramientas dispuestas para tal fin, todas las acciones ejecutadas.
3. Atender los problemas presentados en ambiente de producción y asegurar la calidad de las soluciones entregadas.
4. Realizar un análisis de la causa raíz del problema reportado para ejecutar la resolución definitiva a través de mantenimientos correctivos.
5. Ejecutar todas las etapas del ciclo de vida de desarrollo (análisis, Desarrollo, desarrollo y pruebas).
6. Diseñar la experiencia de uso que tendrá el usuario final, garantizando el cubrimiento de sus necesidades, usabilidad y tendencias del mercado.
7. Mantener actualizado el inventario de servicios web del Fondo.
8. Realizar periódicamente revisiones sobre la gestión realizada, los indicadores, las metodologías y los procedimientos, que permitan trazar estrategias en conjunto para mejorar el servicio y ser acordadas entre las partes para su implementación.
9. Cumplir con los procedimientos establecidos por la entidad para el soporte, mantenimiento y ciclo de desarrollo del software.
10. Asesorar y apoyar a la entidad en la definición de requerimientos, mínimo producto viable, análisis de impacto, viabilidad funcional y técnica, propuestas de Desarrollo según la arquitectura y Desarrollo de prototipos, de las solicitudes de negocio que ingresan.
11. Validar el impacto de las nuevas solicitudes sobre los requerimientos en curso.
12. Realizar el levantamiento funcional y no funcional de los requerimientos definidos, documento que será la entrada para la estimación entre las partes.
13. Ejecutar las solicitudes que se autoricen por bolsa de desarrollo
14. Contar con personal especializado en todo el ciclo de vida de los requerimientos (analistas, diseñadores, expertos en arquitectura funcional y técnica, seguridad, pruebas, documentadoras, etc.) que le permitan garantizar la calidad de las soluciones entregadas al Fondo Nacional del Ahorro S.A.
15. Entregar en detalle la estimación de esfuerzo requerida, en un modelo de estimación acordado entre las partes (Excel), para atender las solicitudes realizadas, en un tiempo no mayor a cinco (5) días hábiles desde la solicitud acordado con el Fondo Nacional del Ahorro S.A. Deberá sustentar las estimaciones a la entidad para su autorización.
16. Proponer la arquitectura de solución de los requerimientos y proyectos solicitados, con el fin de ser valorados por el equipo de arquitectura del Fondo.
17. Mantener actualizado el inventario del portafolio de APIS del Fondo
18. Implementar en el Fondo Nacional del Ahorro S.A., modelos o procesos de contenerización que permita generar evolución los procedimiento y metodologías de desarrollo de software.
19. Otorgar al Fondo Nacional del Ahorro S.A una garantía sobre los desarrollos desplegados en ambiente de producción durante sesenta (60) días hábiles siguientes a su implementación o partir del inicio de su uso por parte del Fondo según el ciclo del producto, tiempo en el cual se podrán reportar los inconvenientes presentados en la solución ocasionados por el despliegue y deben ser atendidos con prioridad sin generar costos adicionales al Fondo Nacional del Ahorro S.A., sin hacer uso del recurso

humano de la línea base y cumpliendo los ANS establecidos. Una vez finalice esta garantía, si se presentan problemas en producción serán atendidos por el equipo asignado al servicio de soporte y mantenimiento de aplicativos.

20. Apoyar al Fondo en la implementación del empaquetamiento de APIS para ser distribuido y ejecutado en ambientes pre-productivos, mediante el uso de contenedores.

21. Informar al Fondo Nacional del Ahorro S.A la ocupación de todos los recursos asignados al servicio.

4. OBLIGACIONES DEL FONDO NACIONAL DEL AHORRO S.A.

Son obligaciones del Fondo Nacional del Ahorro S.A las siguientes:

1. Pagar al CONTRATISTA el valor del contrato en la forma de pago establecida en el contrato, previa aprobación del supervisor y demás requisitos establecidos.
2. Exigir al CONTRATISTA a través del supervisor la ejecución idónea y oportuna del objeto contractual y velar por el cumplimiento de este.
3. Suministrar la información necesaria que el contratista requiera para la ejecución del contrato.
4. Ejercer el seguimiento técnico, jurídico, administrativo y financiero de la ejecución del contrato a través del supervisor
5. Formular las sugerencias por escrito sobre los asuntos que estime convenientes en el desarrollo del contrato.
6. Las demás obligaciones que surjan de acuerdo con la naturaleza del contrato.

5. VALORES AGREGADOS

De conformidad con los factores ponderables presentados dentro del proceso el contratista se compromete a garantizar durante la ejecución del contrato lo siguiente:

5.1. ASIGNACIÓN DE UN ARQUITECTO DE SOLUCIÓN

Para garantizar la correcta implementación y alineación estratégica de la solución corporativa de API Manager con la visión de transformación digital del Fondo Nacional del Ahorro S.A., así como para cumplir con los estándares de calidad y madurez técnica requeridos en el marco de los proyectos de tecnología de la información, la Entidad otorgará hasta (20) puntos al proponente que ofrezca un Arquitecto de Soluciones con una dedicación del 50% para la supervisión y diseño estratégico del proyecto sin costo el cual realizará las siguientes funciones:

- Definir y proponer la arquitectura de la solución de API Manager, asegurando su alineación con la visión de transformación digital del Fondo, los lineamientos del Plan Estratégico de Tecnología de la Información (PETI) y los estándares de arquitectura empresarial, promoviendo una arquitectura orientada a servicios (SOA) que garantice interoperabilidad, escalabilidad y reutilización de servicios.

- Apoyar en la definición de requerimientos funcionales y no funcionales, proponer prototipos y validar el impacto de nuevas integraciones, asegurando que las soluciones sean viables, escalables y alineadas

con las necesidades del negocio.

- Trabajar de manera conjunta con la Gerencia de Arquitectura e Ingeniería de Software y otros equipos involucrados, asegurando una comunicación efectiva y la alineación estratégica durante todas las etapas del proyecto (desarrollo, implementación, estabilización, soporte y mantenimiento).

El contratista se compromete a garantizar durante la ejecución del contrato el perfil profesional del Arquitecto ofrecido en la propuesta.

En caso, que el Fondo Nacional del Ahorro S.A. o el contratista requiera cambiar el Arquitecto durante la ejecución del contrato, este deberá tener un perfil igual o superior al ofrecido en la propuesta, previa aprobación de la supervisión del contrato.

6. VALOR

La entidad adjudicará un contrato por valor de **MIL CUATROCIENTOS TRES MILLONES SETECIENTOS OCHENTA Y DOS MIL CIENTO CINCUENTA Y OCHO PESOS M/CTE ($ 1.403.782.158,00)** incluye IVA, demás impuestos, tasas y contribuciones a las que haya lugar.

7. FORMA DE PAGO

El Fondo Nacional del Ahorro S.A. pagará al contratista el valor del contrato de la siguiente manera:

Un primer pago correspondiente a la etapa de Desarrollo, implementación y estabilización, previa validación y recibo a satisfacción por parte del supervisor del contrato, conforme a la oferta económica presentada.

Pagos mensuales vencidos, correspondientes a soporte y mantenimiento, previa validación y recibo a satisfacción por parte del supervisor del contrato, conforme a la oferta económica presentada.

La bolsa de horas autorizada para los servicios de construcción de software será pagada de la siguiente manera:

a. Pagos mensuales vencidos, de acuerdo con el servicio efectivamente prestado, previa verificación, cumplimiento y aprobación del supervisor del contrato, conforme el valor establecido en la oferta económica respecto de los unitarios que apliquen para estos ítems.

b. El reconocimiento de estas horas se realizará con fechas de cortes mensual vencido; será prerrequisito la entrega de planes de trabajo detallados de las horas efectivamente ejecutadas aprobados por el Fondo.

c. El consumo de la bolsa de horas se medirá y pagará conforme al valor hora estipulado en el contrato, de acuerdo con la oferta económica presentada por el contratista y los controles definidos por la entidad.

PARÁGRAFO 1: Los valores definitivos serán los resultantes de la oferta del oferente adjudicatario del presente proceso de selección.
PARÁGRAFO 2: Todos los valores deben incluir el IVA y cualquier clase de impuesto o gravamen que se cause o se llegaré a causar; en tal evento EL CONTRATISTA se obliga a asumirlo, así como los costos directos e indirectos que se ocasionen para la ejecución de este.
PARÁGRAFO 3: La factura debe presentarse con el lleno de los requisitos establecidos por el Estatuto Tributario, conforme al mes correspondiente.
PARAGRAFO 4: En caso de facturación electrónica deberán cumplirse todos los archivos electrónicos referente a factura electrónica solamente, al correo electrónico facturacionelectronica@fna.gov.co esto previa validación y entrega de los números de aceptación por el supervisor del contrato, de lo contrario su factura para el mes correspondiente será rechazada por el Fondo Nacional del Ahorro; a esta dirección de correo no se deben enviar soportes y/o anexos en imagen o archivos electrónicos diferentes a la factura electrónica; los soportes y demás anexos se deben seguir radicando en el punto de atención.
PARÁGRAFO 5: Para efectos de los desembolsos de los que trata la presente cláusula, el contratista deberá acreditar el pago de los aportes parafiscales y su afiliación obligatoria y pago actualizado al sistema de seguridad social, salud y pensiones, conforme al artículo 182 de la ley 100 de 1993, a ley 789 de 2002, el decreto 1703 de agosto 2 de 2002, la Leyes 797 y 828 de 2003 y el decreto 510 de 2003, y demás que las adicionen, reglamenten, complementen o modifiquen, so pena de hacerse acreedor a las sanciones establecidas en la misma.
PARÁGRAFO 6: Una vez suscrito el contrato el contratista deberá presentar la certificación de la cuenta bancaria donde se consignarán los recursos derivados del contrato, con fecha de expedición no mayor a 30 días anteriores a la recepción de esta.

8. PLAZO

El Fondo Nacional del Ahorro S.A. ha estimado un plazo de ejecución de (12) meses, contados a partir de la firma del acta de inicio, previo el cumplimiento de los requisitos de perfeccionamiento y ejecución. Los cuales están definidos en las siguientes etapas:

- Desarrollo, implementación y estabilización, con una duración de tres (3) meses contados a partir de la suscripción del acta de inicio

- Soporte y mantenimiento, con una duración de nueve (9) meses contados a partir de la finalización de la etapa de Desarrollo, implementación y estabilización

- Transferencia y Cierre, con una duración de un (1) mes correspondiente al último mes de la etapa de soporte y mantenimiento.

9. LUGAR DE EJECUCIÓN Y DOMICILIO CONTRACTUAL

El objeto del presente contrato se ejecutará en la Ciudad de Bogotá en la sede principal del Fondo Nacional del Ahorro S.A. ubicada en la Carrera 65 No. 11 – 83.

Para todos los efectos contractuales se tendrán como domicilio la ciudad de Bogotá.

10. CONOCIMIENTO DEL CONTRATISTA SOBRE LAS CONDICIONES PARA LA EJECUCIÓN DEL CONTRATO

Se entiende por las partes que EL CONTRATISTA ha hecho sus propias averiguaciones, estudios y proyecciones, y ha analizado las condiciones técnicas, sociales, de orden público, climatológicas, ambientales y las demás circunstancias relevantes bajo las cuales se adelantará la ejecución del contrato. En consecuencia, se considera conocedor de todos los elementos necesarios para tomar la decisión de asumir totalmente, a su riesgo, las obligaciones derivadas del contrato, tal como efectivamente lo hace con la presentación de la oferta y, posteriormente de aceptar su oferta, con la suscripción de este.

11. APROPIACIÓN PRESUPUESTAL

El Fondo Nacional del Ahorro S.A. cuenta para el presente proceso de contratación con el certificado de disponibilidad presupuestal expedido por la Gerencia de Presupuesto del Fondo Nacional del Ahorro que se indica a continuación:

Certificado de Disponibilidad Presupuestal	Fecha	Proyecto	Centro Gestor	Posición Presupuestaria	Valor
10002331	16/09/2025	OPER.000 - proyecto operativo	F0502000 - Gcia Arq e Ing Softw	2.1.3.3.99.05.01 - Transformacion Digit	$1.404.972.158

PARÁGRAFO: Para el presente proceso el valor a comprometer del CDP anteriormente indicado corresponderá a la suma de **MIL CUATROCIENTOS TRES MILLONES SETECIENTOS OCHENTA Y DOS MIL CIENTO CINCUENTA Y OCHO PESOS M/CTE ($ 1.403.782.158,00)** incluye IVA, demás impuestos, tasas y contribuciones a las que haya lugar, correspondiente al valor del contrato adjudicado.

12. OMISIONES

Cualquier omisión, error o vicio en los ítems contenidos en la oferta, en las especificaciones técnicas y demás documentos e información técnica que al momento del estudio para la presentación de la oferta económica debió advertir el oferente o que advirtiéndolo no lo informó oportunamente al Fondo Nacional del Ahorro S.A. antes de la presentación de la OFERTA, será de su responsabilidad exclusiva y, en tal virtud, los mayores costos, atrasos en el cronograma de ejecución, defectos o vicios de la ejecución serán asumidos íntegramente con su patrimonio. Así mismo, las omisiones o errores en el cálculo de su oferta económica y, en general, cualquier otro componente de los precios unitarios, serán de exclusiva responsabilidad del oferente y, por tanto, el Fondo Nacional del Ahorro S.A. no realizará ningún reconocimiento por estos conceptos.

13. MULTAS

MULTA DE APREMIO: Si, de manera previa a la conclusión del trámite de imposición de medidas contractuales, el contratista no ha subsanado las situaciones de Incumplimiento que motivaron el inicio de la actuación, se le impondrá una multa, a manera de apremio estimada de acuerdo con la siguiente formula, por cada día de retraso, sin que se supere el veinte por ciento (20%) del valor total del contrato

$$\text{Porcentaje multa apremio} = \frac{0.5}{\text{No. dias (plazo del contrato en dias)}}$$

Esta multa será independiente de la obligación que le asiste al contratista del FONDO NACIONAL DEL AHORRO S.A. de ponerse al día en el cumplimiento de sus obligaciones.

Parágrafo: Para el valor que resulte del cálculo aritmético del porcentaje de la multa se tomaran dos decimales.

MULTA PUNITIVA: Si, de manera previa al inicio del trámite de imposición de medidas contractuales, o, durante su adelantamiento, el contratista cumple con las obligaciones a su cargo, se le impondrá una multa por el cumplimiento tardío del programa prestacional a su cargo. La cuantía de la multa punitiva habrá de ser menor con respecto a la cuantía de la multa de apremio y salvo estipulación en contrario, el monto de la multa punitiva será un cincuenta por ciento (50%) menor con respecto al valor de la multa de apremio que se le hubiera impuesto al contratista de no haber cumplido las obligaciones a su cargo. Esta multa también se podrá imponer, cuando quiera que se verifique el cumplimiento tardío de las obligaciones a cargo del contratista.

Con el fin de asegurar el cumplimiento de las obligaciones del presente contrato, se acuerda entre las partes que, mediante su firma, EL CONTRATISTA faculta al FONDO NACIONAL DEL AHORRO S.A a hacer efectiva la MULTA DE APREMIO o MULTA PUNITIVA, según sea el caso, por retraso en la ejecución total o parcial de las obligaciones adquiridas en virtud del contrato, así como, por la ejecución de manera tardía, defectuosa, o de forma diferente a como fue pactado o a las normas técnicas que apliquen.

El apremio corresponderá al valor que resulte de la aplicación de la formula planteada en esta cláusula, por cada día de retraso, sin que se supere el veinte por ciento (20%) del valor total del contrato y en todo caso dentro de los términos establecidos en el artículo 867 del Código de Comercio. Si se generan apremios que superen dicho valor, el FONDO NACIONAL DEL AHORRO S.A podrá dar por terminado anticipadamente el Contrato de conformidad con el literal **e** del numeral 8.9.4 del Manual de Contratación, adelantar su liquidación y hacer efectiva la Cláusula Penal Pecuniaria.

En los casos en los que se requiera Personal Mínimo para la ejecución contractual se atendrá a lo siguiente: Así mismo, dado que EL CONTRATISTA deberá mantener durante la ejecución del contrato EL PERSONAL MINIMO requerido en las reglas de participación o el documento que haga sus veces que dieron origen al presente contrato, por cada profesional o técnico que no cumpla con las especificaciones y dedicaciones mínimas requeridas o que no esté laborando o realizando actividades, se faculta a FONDO NACIONAL DEL AHORRO S.A. a exigir al EL CONTRATISTA la suma de veinte (20) salarios mínimos diarios legales vigentes (SMDLV) por cada día calendario que no se cuente con ese personal. Para el efecto, debe contarse con el requerimiento que sobre el particular efectué el supervisor y/o interventoría, de acuerdo con el informe correspondiente. Realizados dos (2) requerimientos al CONTRATISTA, el supervisor y/o interventoría solicitará el inicio de un proceso de incumplimiento parcial del contrato.

PARÁGRAFO: Los apremios que se causen en virtud de lo dispuesto en esta cláusula se harán efectivos, sin perjuicio de la indemnización de perjuicios a que haya lugar pues buscan conminar al CONTRATISTA para el cumplimiento de sus obligaciones y, por lo tanto, no tienen el carácter de estimación anticipada de perjuicios, de manera que pueden acumularse con cualquier forma de indemnización, en los términos previstos en el artículo 1600 del Código Civil.

14. PENAL PECUNIARIA:

Con la firma del presente contrato, se acuerda entre las partes que EL CONTRATISTA faculta al FONDO NACIONAL DEL AHORRO S.A a exigir al CONTRATISTA a título de pena, la suma equivalente al veinte (20%) del valor total del contrato, en caso de incumplimiento de una o varias de las obligaciones a cargo del CONTRATISTA.

El pago del valor acá señalado se considera como indemnización parcial y no definitiva de los perjuicios causados por el posible incumplimiento del **CONTRATISTA**, razón por la cual, **el FONDO NACIONAL DEL AHORRO S.A.** tendrá derecho a obtener del **CONTRATISTA** y/o su GARANTE el pago de la indemnización correspondiente a los demás perjuicios imputables a este como consecuencia de dicho incumplimiento.
La cláusula penal pactada se causará por el solo hecho del incumplimiento y no requerirá de reconvención judicial previa; bastará con el simple retardo imputable al mismo, para generar la obligación de pago de las sumas que correspondan.

El FONDO NACIONAL DEL AHORRO S.A. podrá obtener el pago de la penal pecuniaria mediante el ejercicio de las acciones legales a que haya lugar, ejercidas en contra del **CONTRATISTA** y/o su Garante haciendo efectivo el amparo de Cumplimiento de la Póliza de Cumplimiento ante Entidades Públicas con Régimen Privado de Contratación. El valor de la Cláusula penal pecuniaria pactada se calculará sobre el valor total del contrato, incluidas las modificaciones al valor del mismo, sin perjuicio de lo previsto en el Art. 1596 del Código Civil.

15. PROCEDIMIENTO PARA APLICACIÓN DE LA CLÁUSULA DE MULTAS Y DE LA CLÁUSULA PENAL PECUNIARIA

En garantía del debido proceso, y con el fin de asegurar el derecho de defensa y contradicción de EL CONTRATISTA, se deberá agotar el procedimiento establecido en el formato GLC-CONT-PR-15 o el que se encuentre vigente.

PARAGRAFO PRIMERO: Quienes ejerzan actos de vigilancia y control, deben requerir al contratista para que presente los informes, aclaraciones y explicaciones que consideren pertinentes sobre el desarrollo de la ejecución contractual de los hechos o circunstancias que puedan poner o pongan en riesgo el cumplimiento del contrato o convenio, o cuando tal incumplimiento se presente; actuación que deberá reunir los siguientes requisitos:
a) Los requerimientos deberán hacerse por escrito al contratista, en plazo no superior a lo que la debida diligencia impone. Deberán acumularse por lo menos dos (02) requerimientos previos a la radicación del presunto incumplimiento en la Gerencia de Contratación.
b) En el contenido del requerimiento dirigido al contratista se deben incorporar los hechos, actos o circunstancias sobre los que el supervisor e interventor requiere informes, aclaraciones y explicaciones y

señalar con exactitud las razones y cláusulas por las cuales se considera que puede presentarse un incumplimiento de las obligaciones contractuales a su cargo y de ser pertinente o conducente, los documentos o soportes anexos que a juicio de la supervisión o la interventoría, deben ser allegados para aclarar las situaciones particulares de cada caso.
c) Dentro del mismo texto del requerimiento, el supervisor o interventor debe establecer un plazo prudencial y perentorio para recibir la respuesta por parte del contratista, teniendo en cuenta la gravedad y complejidad del asunto, así como, la naturaleza y cantidad de los documentos solicitados.
d) En los casos en que la garantía de cumplimiento consista en póliza de seguros, una copia del requerimiento al contratista será remitido al garante.
e) Cuando el contratista guarde silencio frente al requerimiento o la respuesta presentada no desvirtúe plenamente el posible incumplimiento, el supervisor o interventor elaborará con destino a la Gerencia de Contratación, un informe pormenorizado de lo sucedido.
f) El informe que el supervisor o interventor rinda deberá ser objeto de análisis por la Gerencia de Contratación, y si encuentran procedente continuar con el procedimiento y seguir con la activación del derecho al pago de sanciones.

PARÁGRAFO SEGUNDO: Las partes acuerdan que, para establecer el valor de la medida a imponer al CONTRATISTA, por concepto de multas, cualquiera de ellas o clausula penal pecuniaria, se aplicará la forma prevista por el FONDO NACIONAL DEL AHORRO S.A. en el presente contrato.

PARÁGRAFO TERCERO: A través de la firma del presente contrato el CONTRATISTA autoriza al FONDO NACIONAL DEL AHORRO S.A. para efectuar la compensación del valor de las medidas que se le impongan como lo señala el numeral 8.8 del Manual de Contratación, a título de multa o cláusula penal pecuniaria, con los montos que el FONDO NACIONAL DEL AHORRO S.A. le adeude con ocasión de la ejecución de este contrato, en los términos de los artículos 1714 y 1715 del Código Civil.

PARÁGRAFO CUARTO: Si no existen sumas con cargo al contrato, que puedan ser compensadas por EL CONTRATISTA, las medidas que se le impongan, a título de apremio o cláusula penal pecuniaria, podrán ser cobradas por vía judicial, dado que se trata de obligaciones claras, expresas y exigibles a cargo de EL CONTRATISTA que prestan mérito ejecutivo. EL CONTRATISTA renuncia al previo aviso o a la reconvención previa para constituirlo en mora.

16. HABEAS DATA Y PROTECCIÓN DE DATOS PERSONALES

El CONTRATISTA se compromete a dar estricto cumplimiento al régimen de protección de datos personales que establecen las leyes 1266 de 2008, 1581 de 2012 y demás normas que las complementen o modifiquen, así como a implementar las medidas técnicas, administrativas y humanas que aseguren que el tratamiento de datos personales cumple con los principios de seguridad, acceso y circulación restringida, confidencialidad y calidad contenidos en la legislación, so pena de incurrir en las sanciones legales correspondientes.

17. SOLUCIÓN DE CONTROVERSIAS

Las partes acuerdan que, para la solución de las diferencias y discrepancias surgidas de la celebración del contrato, su ejecución, desarrollo y/o terminación acudirán al arreglo directo.

18. GARANTÍAS

El contratista deberá presentar dentro de los **cinco (5) días hábiles** siguientes a la firma del contrato, una garantía a **FAVOR DE ENTIDADES PÚBLICAS CON RÉGIMEN PRIVADO DE CONTRATACIÓN** que ampare el cumplimiento de todas y cada una de las obligaciones que surjan a cargo de este frente a la entidad.

Esta garantía podrá consistir en póliza de seguro y deberá contar con los siguientes amparos:

GARANTÍAS CONTRACTUALES		
AMPARO	**PORCENTAJE**	**VIGENCIA**
Cumplimiento	20% del valor del contrato	Con una vigencia igual al plazo de ejecución del contrato y seis (06) meses más.
Pago de salarios y Prestaciones sociales	10% del valor del contrato	Con una vigencia igual plazo de ejecución del contrato y tres (3) años más.
Calidad del servicio	20% del valor del contrato	Con una vigencia igual al plazo de ejecución del contrato y seis (06) meses más.

PARAGRAFO 1: La garantía de cumplimiento deberá encontrarse vigente hasta que culmine la vigencia del contrato; esto es, hasta su liquidación.
PARAGRAFO 2: El contratista debe ajustar las garantías de conformidad con la fecha de suscripción del acta de inicio, con el fin de que los amparos y vigencias correspondan a lo establecido en el presente numeral.
PARAGRAFO 3: Las garantías contractuales se establecieron teniendo en cuenta el valor del contrato versus la cuantificación del porcentaje para cada amparo.
PARAGRAFO 4: En caso de que la garantía sea una póliza de seguro, la póliza deberá contener el siguiente texto de modificación de las condiciones generales de la misma: "*SE REEMPLAZA EL NUMERAL DE LAS CONDICIONES GENERALES DE LA PÓLIZA CORRESPONDIENTE A LA CUANTÍA Y OCURRENCIA POR EL SIGUIENTE TEXTO: CUANTÍA Y OCURRENCIA EN CONCORDANCIA CON LO NORMADO EN EL ARTÍCULO 1077 DEL CÓDIGO DE COMERCIO, LA SOCIEDAD DEBERÁ ACREDITAR LA OCURRENCIA DEL SINIESTRO Y LA CUANTÍA DE LA RECLAMACIÓN.*" El anterior texto debe estar incluido EXPRESAMENTE en la carátula de la póliza.
PARAGRAFO 5: En caso de prorrogarse el plazo de ejecución, deberá ampliarse la vigencia del amparo por el mismo término. Ocurrido cualquier siniestro el Contratista está obligado a restablecer la cobertura completa.
PARAGRAFO 6: Constará por obligación del contrato que acaecido el plazo máximo de presentación de las garantías y el proponente seleccionado no ha presentado las mismas ante la Entidad, se le efectuarán descuentos del 0.01% por cada uno de los días en que permanezca en estado de Incumplimiento en lo que respecta a esta obligación, hasta el valor máximo del 1% del valor del contrato, ello en concordancia con lo estipulado en el numeral 5.8.2 del Manual de Contratación versión 5 del Fondo Nacional del Ahorro S.A.

Así las cosas, en caso de acaecer la condición señalada, la Gerencia de Contratación notificará al área solicitante, para que en el marco de sus funciones como supervisor del contrato proceda con el respectivo descuento.

19. SUFICIENCIA DE LAS GARANTÍAS:

EL CONTRATISTA debe mantener en todo momento de vigencia del contrato la suficiencia de las garantías otorgadas. En consecuencia, en el evento en que el plazo de ejecución del contrato y/o su valor se amplíe o aumente, respectivamente, EL CONTRATISTA deberá ampliar la vigencia de las garantías y/o el valor amparado de las mismas, según sea el caso, como condición previa y necesaria para el pago de las facturas pendientes de pago. De igual modo, EL CONTRATISTA deberá reponer las garantías cuando su valor se afecte por razón de los siniestros amparados. En el caso de los amparos cuya vigencia debe prolongarse con posterioridad al vencimiento del plazo de ejecución del contrato, el valor amparado también debe reponerse cuando el mismo se afecte por la ocurrencia de los riesgos asegurados con posterioridad a tales fechas. El pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, será de cargo exclusivo de EL CONTRATISTA.

20. SUPERVISIÓN:

La supervisión del contrato estará a cargo de la Gerente de Arquitectura e Ingeniería de Software o quien haga sus veces, o quien el ordenador del gasto designe, quien ejercerá el control y seguimiento administrativo, jurídico y financiero y demás que le correspondan al FONDO NACIONAL DEL AHORRO S.A., de conformidad con el Manual de Supervisión vigente en la entidad.

El supervisor está facultado a solicitar informes, aclaraciones y explicaciones sobre el desarrollo de la ejecución contractual y será responsable por mantener informado al FONDO NACIONAL DEL AHORRO S.A. de los hechos o circunstancias que puedan constituir actos de corrupción tipificados como conductas punibles o que puedan poner o pongan en riesgo el cumplimiento del contrato, o cuando tal incumplimiento se presente. En ningún caso goza de la facultad de modificar el contenido y alcance del contrato suscrito entre EL CONTRATISTA y el FONDO NACIONAL DEL AHORRO S.A., ni de eximir, a ninguno de ellos, de sus obligaciones y responsabilidades.

21. INDEMNIDAD:

EL CONTRATISTA se compromete a cumplir con las obligaciones señaladas en el presente contrato, bajo su única responsabilidad y riesgo y mantendrá indemne al FONDO frente a cualquier reclamación judicial o extrajudicial de terceros; por consiguiente, el FONDO en ningún caso responderá por demandas o reclamaciones que puedan presentar sus empleados, asesores o terceros, con ocasión de daños o perjuicios, o respecto del pago de seguros, salarios y prestaciones sociales derivados de la ejecución del presente contrato. Si ello no fuere posible y se presentaren reclamaciones o demandas contra el FONDO, esta entidad podrá comunicar la situación por escrito al CONTRATISTA. En cualquiera de dichas situaciones, EL CONTRATISTA se obliga a acudir en defensa de los intereses del FONDO, para lo cual contratará profesionales idóneos que representen a la entidad y asumirá el costo de los honorarios de éstos, del proceso y de la condena,

si la hubiere. Si el FONDO estima que sus intereses no están siendo adecuadamente defendidos, lo manifestará por escrito al CONTRATISTA, caso en el cual acordará la mejor estrategia de defensa o si el FONDO lo estima necesario, asumirá directamente la misma. En este último caso, el FONDO cobrará y descontará de los saldos a favor del CONTRATISTA todos los costos que implique esa defensa, más un diez por ciento (10%) del valor de estos, por concepto de gastos de administración. Si no hubiere saldos pendientes de pago a favor del CONTRATISTA, el FONDO podrá proceder, para el cobro de los valores a que se refiere este numeral, por la vía ejecutiva, para lo cual este contrato, junto con los documentos en los que se consignen dichos valores, prestará mérito ejecutivo.

22. INEXISTENCIA DE RELACIÓN LABORAL:

Las partes declaran que entre el FONDO y el personal que CONTRATISTA emplee para la ejecución del presente contrato no existe vínculo laboral alguno, en consecuencia, el FONDO únicamente se obliga a pagar a CONTRATISTA las sumas expresamente pactadas, siendo obligación de este cancelar a su costa y bajo su responsabilidad los honorarios y/o salarios, al personal que emplee para la ejecución del contrato.

23. INHABILIDADES E INCOMPATIBILIDADES:

EL CONTRATISTA declara bajo la gravedad del juramento que no existe ningún tipo de inhabilidad o incompatibilidad de las señaladas en la Constitución Nacional o en la Ley que impida la celebración del presente contrato, ni se encuentra reportado como responsable fiscal en el boletín de la Contraloría General de la República, ni en las listas restrictivas. Igualmente declara que en caso de presentarse alguna inhabilidad o incompatibilidad se hará responsable ante el FONDO y ante terceros por los perjuicios que se llegaren a ocasionar. Si llegare a sobrevenir inhabilidad o incompatibilidad CONTRATISTA cederá el contrato, previa autorización escrita del FONDO y si ello no fuere posible renunciará a su ejecución.

24. CONFIDENCIALIDAD E INFORMACIÓN PRIVILEGIADA

El contratista adquiere las obligaciones que se describen a continuación, en relación con la información confidencial y/o privilegiada a la que tenga acceso en el desarrollo del presente contrato: a). Abstenerse en cualquier tiempo de divulgar, parcial o totalmente la Información Confidencial y/o privilegiada a cualquier persona natural o jurídica, entidades gubernamentales o privadas, excepto en los casos que se precisan a continuación: (i). Cuando la información sea solicitada por **FONDO NACIONAL DEL AHORRO S.A**. (ii). En cumplimiento de una decisión judicial en firme, orden, requerimiento o una solicitud oficial expedida bien sea por un tribunal competente, una autoridad u órgano judicial o legislativo con competencia para ello, para lo cual deberá observarse el procedimiento establecido por **FONDO NACIONAL DEL AHORRO S.A.** para dar respuesta a tales decisiones, requerimientos o solicitudes, así como las competencias y delegaciones establecidas para la suscripción de las mismas. (iii). Cuando cualquier autoridad judicial, gubernamental o regulatoria la haya requerido legalmente, siempre y cuando la información confidencial y/o privilegiada se entregue a la mencionada autoridad cumpliendo con los mecanismos de cuidado, protección y manejo responsable de la información estipulados en esta cláusula, previa notificación a **FONDO NACIONAL DEL AHORRO S.A.** , con el fin de que puedan tomar las acciones administrativas y judiciales pertinentes y se observe el procedimiento establecido por **FONDO NACIONAL DEL AHORRO S.A.** para dar respuesta a tales requerimientos, así como las competencias y delegaciones establecidas para la suscripción de los mismos. b).

Abstenerse en cualquier tiempo de utilizar, explotar, emplear, publicar o divulgar la Información Confidencial y/o privilegiada en una forma diferente a la autorizada en esta cláusula. c). Tomar todas las medidas necesarias para que la Información Confidencial y/o privilegiada que le sea suministrada en medio físico o electrónico, se transporte, manipule y mantenga en un lugar seguro y de acceso restringido. d). Instruir a todas aquellas personas que tengan acceso a la Información Confidencial y/o privilegiada sobre la forma de manipulación, utilización, manejo de medidas de seguridad y demás, para que la información subsista bien manejada y protegida. e) El uso de la Información Confidencial y/o privilegiada no otorga derecho ni constituye licencia a **EL CONTRATISTA**, para utilizarla sin observar los principios de la ética profesional, comercial y la competencia leal, ni otorgando, favoreciendo ni beneficiando a cualquier otra persona natural o jurídica. Para ello **EL CONTRATISTA** acuerda expresamente emplear todos los medios a su alcance para impedir esa utilización irregular de la Información Confidencial y/o privilegiada. **PARÁGRAFO PRIMERO**: Para todos los efectos, el término "información confidencial y/o privilegiada", corresponde a la información que entrega **FONDO NACIONAL DEL AHORRO S.A.** para el desarrollo de las actividades propias del contrato, que debe ser cuidada, protegida y tratada de manera responsable por **EL CONTRATISTA**. **PARÁGRAFO SEGUNDO**: El incumplimiento de las obligaciones derivadas de la presente cláusula generará un incumplimiento del contrato. **PARÁGRAFO TERCERO: FONDO NACIONAL DEL AHORRO S.A.** adelantará las acciones judiciales pertinentes contra **EL CONTRATISTA** en el evento que éste, en cualquier tiempo, vulnere el compromiso adquirido en virtud de la presente cláusula.

25. SUSPENSIÓN:

De común acuerdo entre las partes, se podrá suspender la ejecución del contrato, mediante la suscripción de acta, sin que para el efecto del plazo extintivo del mismo se compute el tiempo de suspensión. Para su reinicio, se requerirá un acta en el que conste dicha circunstancia.

26. CESIÓN:

Este contrato se celebra en consideración a la calidad del CONTRATISTA y no podrá cederlo en todo ni en parte a ningún título, sin el consentimiento expreso, previo y escrito del FONDO, para subcontratar total o parcialmente el objeto de este, deberá contar de igual manera con la autorización expresa, previa y escrita del FONDO.

PARÁGRAFO: En el caso que sea autorizada la subcontratación, las partes deberán suscribir anexo con las condiciones autorizadas para tal fin, incluyendo, sin limitarse a ello, el periodo por el cual se autoriza y las condiciones técnicas y económicas provisionales

27. CESIÓN DE LOS DERECHOS ECONÓMICOS DEL CONTRATO:

Los derechos económicos del contrato no podrán cederse en todo ni en parte, a ningún título, sin el consentimiento expreso, previo y escrito del FONDO. En caso de producirse Cesión del contrato, requerirá, para su eficacia, de la suscripción de un documento por parte del cedente, el cesionario y la aprobación expresa del FONDO, de acuerdo con el procedimiento interno del FONDO para tal efecto.

28. CLÁUSULA DE CONFIDENCIALIDAD:

El Encargado se obliga y se compromete, de conformidad con la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, así como cualquier otra norma que las reemplace, modifique o sustituya, a guardar absoluta reserva, confidencialidad y a no divulgar información confidencial que por virtud del contrato sea suministrada por EL FONDO.

Para efectos del Contrato, los documentos, operaciones, procesos, tecnología y demás datos inherentes a la actividad de EL FONDO y a los cuales pueda tener acceso directo o indirectamente el CONTRATISTA, son de propiedad exclusiva del EL FONDO y por tanto el CONTRATISTA no podrá utilizarlos en su favor, o en el de terceras personas o darlos a conocer por vía alguna, obligándose a guardar absoluta reserva al respecto. Así mismo el CONTRATISTA se obliga a mantener estricta confidencialidad sobre la información a la cual pueda tener acceso en desarrollo del CONTRATO. La información mencionada anteriormente será utilizada exclusivamente para el desarrollo del objeto del CONTRATO. El incumplimiento de esta obligación hará responsable al CONTRATISTA por los perjuicios que se causen, directa o indirectamente al EL FONDO sin que ello impida la iniciación de las acciones penales correspondientes. La obligación establecida en esta cláusula se mantendrá vigente, incluso después de la terminación del CONTRATO. El CONTRATISTA a través del CONTRATO, se obligan a mantener absoluta reserva y confidencialidad de la información que, debido a su trabajo o actividad, debe manejar y a no emplear el nombre de EL FONDO para obtener beneficios personales que sean o puedan ser directos o indirectos. En consecuencia y de conformidad con lo mencionado anteriormente, El Encargado declara que: a. Conoce y acepta que la violación de esta obligación lo hará incurrir en las sanciones legales correspondientes y en la terminación inmediata del presente contrato por justa causa y sin indemnización alguna por parte de EL FONDO. b. El incumplimiento por parte del CONTRATISTA de la presente cláusula dará derecho a EL FONDO de exigir resarcimiento de los perjuicios resultantes de dicho incumplimiento. Por lo tanto, el presente acuerdo prestará mérito ejecutivo frente al pago de cualquier otra suma a cargo del EL FONDO. Y se compromete a: a. Tomar las medidas necesarias para que sus empleados y dependientes cumplan con las obligaciones previstas en esta cláusula. b. No retirar de las dependencias de EL FONDO datos y/o información a que tenga acceso, excepto con la autorización escrita de la persona responsable de EL FONDO. El Encargado no divulgará a terceros cualquier tipo de información obtenida en el desarrollo del objeto del contrato sin el consentimiento previo y por escrito de EL FONDO, excepto: a. Aquella información conocida por El Contratista antes de ser revelada bajo el contrato, sin que la misma estuviese sujeta a ninguna obligación de confidencialidad. b. Información publicada o que se publique, o de otra manera esté disponible al público en general y que no haya sido divulgada por EL FONDO. c. Que la revelación y/o divulgación de la información se haga en desarrollo de orden de autoridad competente en ejercicio de sus funciones legales. En este caso, El Contratista se obliga a avisar dentro de los tres (3) días siguientes a la fecha en que le sea notificada la orden, o sea conocida la solicitud, a EL FONDO, para que éste pueda tomar las medidas necesarias para proteger su información confidencial, y de igual manera se compromete a tomar las medidas pertinentes para atenuar los efectos de tal divulgación. La presente cláusula de confidencialidad estará vigente durante todo el término de duración del contrato y a la terminación del mismo, permanecerá vigente a perpetuidad con respecto a la confidencialidad de los datos personales y las bases de datos que las contengan. Estas obligaciones se hacen extensivas a todos los datos personales y/o datos personales sensibles que reciba el CONTRATISTA de EL FONDO o de cualquier tercero con motivo de los Servicios objeto de este Contrato. El CONTRATISTA se obliga a cumplir con la legislación aplicable en materia de protección de datos en posesión de particulares.

29. PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO

EL CONTRATISTA manifiesta bajo la gravedad de juramento, que se entiende prestado con la suscripción del presente contrato, que los ingresos percibidos y recursos que componen su patrimonio no provienen de cualquier delito fuente relacionado con el lavado de activos y financiación del terrorismo, contemplados en el Código Penal Colombiano; de igual manera manifiesta que los recursos recibidos en desarrollo de este contrato no serán destinados a ninguna de las actividades antes descritas. Para efectos de lo anterior, el contratista autoriza expresamente a FONDO NACIONAL DEL AHORRO S.A. , para que consulte los listados, sistemas de información y bases de datos a los que haya lugar y, de encontrar algún reporte, FONDO NACIONAL DEL AHORRO S.A. procederá a adelantar las acciones contractuales y/o legales que correspondan.

EL CONTRATISTA se obliga a realizar todas las actividades encaminadas a asegurar que todos sus socios, administradores, clientes, proveedores, empleados, etc., y los recursos de estos, no se encuentren relacionados o provengan, de actividades ilícitas, particularmente, de las anteriormente enunciadas.

En el debido caso que se detecte que uno de los deudores del FONDO NACIONAL DEL AHORRO S.A. se encuentre vinculado en la lista vinculante ONU y cualesquiera listas restrictivas, se deberá informar de manera inmediata al Oficial de cumplimiento del FONDO NACIONAL DEL AHORRO S.A., así mismo, al interior de la entidad no se podrán ejecutar nuevas operaciones ni recibir dineros nuevos provenientes del deudor, toda vez que dicha operación podría ser producto de la ejecución de una actividad presuntamente delictiva relacionada con el LAFT.

30. RÉGIMEN LEGAL:

El presente contrato se regirá por las disposiciones consagradas en el Manual de Contratación del Fondo Nacional del Ahorro S.A., sin perjuicio de las normas legales aplicables a la materia.

31. LIQUIDACIÓN DEL CONTRATO:

El contrato que resulte del presente proceso de selección será de objeto de liquidación de acuerdo con lo establecido en el Manual de Contratación Vigente al momento de la suscripción del presente contrato; en ese orden, esta deberá realizarse dentro de los seis (6) meses siguientes a la terminación del plazo de ejecución del contrato

Parágrafo: En el evento en que El CONTRATISTA no comparezca a la firma de la liquidación, el FONDO NACIONAL DEL AHORRO S.A. remitirá el documento por correo certificado a la dirección registrada y si no la devolviere firmada dentro del término que se le indique en el oficio remisorio, se procederá a ordenar el archivo del contrato dejando constancia de la situación de este, sin perjuicio del derecho de cada una de las partes de acudir al juez del contrato para la protección de sus intereses.

32. COMPENSACIÓN

Con el fin de asegurar el cumplimiento de las obligaciones del presente contrato, se acuerda entre las partes que, mediante su firma, EL CONTRATISTA faculta al FONDO NACIONAL DEL AHORRO S.A a hacer efectiva

durante la ejecución del contrato, o, al momento de llevar a cabo la etapa de cierre, la compensación de las sumas que por cualquier concepto adeude el contratista, de los pagos que se encuentren pendientes de ser desembolsados. Lo anterior, sin perjuicio de que la Entidad adelante las gestiones administrativas y judiciales correspondientes, en caso de que el valor compensado no alcance a cubrir la totalidad de las acreencias en favor del Fondo.

Parágrafo: Los contratos que sean objeto de compensación deberán ser liquidados y de las sumas compensadas se dejará constancia en el documento de Cierre Contractual que proceda en el contrato respectivo

33. TERMINACIÓN ANTICIPADA

El presente contrato terminará anticipadamente por las siguientes causas: **a)** Por mutuo acuerdo de las partes, caso en el cual se dejará expresa constancia del acuerdo bilateral; **b)** Por muerte de la persona natural o disolución de la persona jurídica, del CONTRATISTA, o de una de las personas naturales o jurídicas que integran el respectivo consorcio o unión temporal; así como por la modificación de los miembros de éstos últimos, sin autorización del FONDO; **c)** En el caso de que El CONTRATISTA o alguno de sus asociados haya incurrido o incurra en actividades que impliquen para el FONDO Riesgo Reputacional; **d)** Por cualquiera de las causales previstas en el ordenamiento jurídico colombiano; **e)** Por la ocurrencia de las causales previstas en la cláusula de terminación anticipada del contrato.

34. CAUSALES DE TERMINACIÓN ANTICIPADA DEL CONTRATO MEDIANTE RESOLUCIÓN EXPRESA

En desarrollo del principio de la voluntad, EL CONTRATISTA se sujeta, acepta y autoriza a EL CONTRATANTE a terminar anticipadamente el contrato en los siguientes eventos:

a. Si durante la ejecución del contrato la persona llegare a presentar alguna investigación de cualquier tipo relacionada con actividades ilícitas, lavado de dinero o financiamiento del terrorismo, o fuese incluida en las listas internacionales vinculantes para Colombia, de conformidad con el derecho internacional (listas de Naciones Unidas – ONU, listas de la Unión Europea – UE y listas de la Oficina de Control de Activos Extranjeros – OFAC), el Fondo Nacional del Ahorro S.A. tendrá derecho de terminar el contrato sin que por este hecho, esté obligado a indemnizar.
b. Cuando se haya celebrado un contrato con persona incursa en causal de inhabilidad o incompatibilidad.
c. No haber logrado el contratista dejar el contrato en estado de ejecución, por: (i) la no presentación del certificado de constitución de la garantía de cumplimiento, o por no haber logrado la corrección de los defectos advertidos, de conformidad con lo señalado en este Manual y en el respectivo contrato; o, (ii) no haber cumplido con otro tipo de requisitos a su cargo, de conformidad con lo señalado en el contrato.
d. Cuando el monto de la totalidad de la remuneración reconocida al Contratista en ejercicio de la cláusula de Acuerdos de Niveles de Servicio (ANS), o de los demás previstos en el contrato, no haya logrado alcanzar, una determinada suma, prefijada en el contrato.
e. Cuando el monto de las multas impuestas alcance el 20% del valor total del contrato.

f. Cuando el CONTRATISTA incurre en un retardo injustificado respecto del cumplimiento de sus obligaciones, calificadas como esenciales según el contrato, y pese a habérsele conminado a su cumplimiento, no ha logrado subsanar dicha situación dentro del término razonable que se le hubiere señalado.
g. Cuando el CONTRATISTA cumple de manera insatisfactoria obligaciones calificadas como esenciales según el contrato, y pese a habérsele conminado a efectuar las correcciones que sean del caso, no ha logrado subsanar dicha situación dentro del término razonable que se le hubiere señalado.
h. Las demás que hayan sido fijadas en el contrato de acuerdo con el entorno que rodea el objeto de la contratación.

35. PROCEDIMIENTO PARA APLICACIÓN DE LA CLAUSULA DE TERMINACIÓN ANTICIPADA DEL CONTRATO MEDIANTE REOLUCIÓN EXPRESA:

En garantía del debido proceso, y con el fin de asegurar el derecho de defensa y contradicción de EL CONTRATISTA, se deberá agotar el procedimiento que se encuentre vigente.

36. DOCUMENTOS:

Hacen parte integral del presente contrato:

1. Los estudios previos del proceso No **FNA-VTTD-CC-011-2025**
2. Anexos.
3. El Certificado de Disponibilidad Presupuestal.
4. La propuesta del oferente con sus respectivos soportes, anexos y formatos.
5. Todos los documentos del proceso.

37. REQUISITOS DE PERFECCIONAMIENTO Y EJECUCIÓN:

El presente contrato se perfeccionará con la aceptación de las partes en la plataforma del Secop II y para su ejecución se requerirá el registro presupuestal y la aprobación de las garantías.

Revisó: Miguel Leonardo Fernández Torres – Profesional Secretaría General
Revisó: Juan Felipe Torres Arango- Profesional Gerencia de Contratación
Proyectó: Yohanna Mesa Ramos – Profesional Gerencia de Contratación

fna FONDO NACIONAL DEL AHORRO	**ACTA DE INICIO DEL CONTRATO**	Código: GLC-CONT-FO-004
	PROCESO DE CONTRATACIÓN	Versión: 1

DEPENDENCIA QUE REALIZA LA SUPERVISIÓN: Gerencia de Arquitectura e Ingeniería de Software	
Información del Contrato	
Contrato No. FNA-132-2025	**Suscrito**: 05 nov 2025
Nombre del contratista: **INGENIUM COLOMBIA SAS**	**NIT o cédula contratista:** **900.500.876-5**
Objeto del contrato: *CONTRATAR LOS SERVICIOS ESPECIALIZADOS PARA EL DESARROLLO, IMPLEMENTACIÓN, CONFIGURACIÓN Y SOPORTE DE UNA SOLUCIÓN CORPORATIVA DE API MANAGER, QUE PERMITA LA EXPOSICIÓN SEGURA, CONTROLADA, MONITOREADA Y VERSIONADA, EN EL MARCO DE LA MODERNIZACIÓN DE LA ARQUITECTURA ORIENTADA A SERVICIOS DEL FONDO NACIONAL DEL AHORRO S.A.*	
Valor del contrato (incluido IVA): MIL CUATROCIENTOS TRES MILLONES SETECIENTOS OCHENTA Y DOS MIL CIENTO CINCUENTA Y OCHO PESOS ($1.403.782.158,00)	
Plazo: Doce (12) Meses	
Fecha aprobación póliza y/o RP: RP: 06/11/2025	

Supervisión: CRISTIAN CAMILO GARCIA PARRA

Para constancia de la presente acta, se firma por los que intervienen a los 29 días del mes de diciembre del año 2025.

POR EL FONDO NACIONAL DEL AHORRO S.A.

CRISTIAN GARCIA PARRA
C.C. 1.094.941.554
Supervisor del Contrato 132-2025

POR EL CONTRATISTA.

ADRIANA LUCÍA ESCOBAR CASTAÑEDA
C.C. 1.069.734.144
Representante Legal
INGENIUM COLOMBIA S.A.S.

División de Presupuesto
Documento de Pago

N° ORDEN DE PAGO	5300426264	**FECHA DE CONTABILIZACIÓN**	25.06.2026
N° DE REFERENCIA	337	**FECHA DE PAGO**	15.07.2026

RESPONSABLE DEL PAGO

NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO
N° IDENTIFICACIÓN	NIT 8999992844

PROVEEDOR	INGENIUM COLOMBIA SAS	**N° IDENTIFICACION**	9005008765

BENEFICIARIO DEL PAGO

NOMBRE COMPLETO	INGENIUM COLOMBIA SA		
N° IDENTIFICACION	9005008765	**TIPO DE IDENTIFICACION**	NIT
FORMA DE PAGO	PAGO ELECTRÓNICO	**CIUDAD**	BOGOTÁ
N° DE CUENTA	60200014605	**BANCO**	BANCOLOMBIA
TIPO DE CUENTA	CUENTA CORRIENTE	**INFORME N°**	CUENTA 1
N° FACTURA PROVEEDOR	FE337 RAD 02-2303-202606250813638		

OBSERVACIONES: FE337 RAD 02-2303-202606250813638.pl444

INFORMACIÓN PRESUPUESTAL

SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO		LERF	RE-L	VALOR
10002331	5400002117	00010	CTO 132-2025	.	1000061970	5105633514	0
10002331	5400002117	00010	CTO 132-2025	.	1000061970	5105633514	904.981.934
						AFECTACIÓN PEDIDO	904.981.934

DETALLE DE LA ORDEN DE PAGO

VALOR TOTAL FAC.	904.981.934,00
DESCUENTOS	55.637.377,00
NOTAS CRÉDITOS	0,00
VALOR A PAGAR	849.344.557,00

Usuario: Jarieth Astrid Rivera Ga
Fecha de impresión: 31.07.2026

Gerencia Tesorería
Documento de Pago

No. ORDEN DE PAGO	337	**FECHA DE CONTABILIZACION**	15-jul-26
No. DOCUMENTO DE PAGO	5300426264	**FECHA DE DOCUMENTO**	15-jul-26
		FECHA DE COMPENSACION	15-jul-26
PROPUESTA	60806	**FECHA DE LA PROPUESTA**	15-jul-26

RESPONSABLE DEL PAGO

NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO		
No. IDENTIFICACIÓN	8999992844	**TIPO DE IDENTIFICACÓN**	NIT
CONCEPTO	GIRO DEFINITIVO AHORRO VOLUNTAR		

DATOS GENERALES

NOMBRE COMPLETO	INGENIUM COLOMBIA SAS		
No. INDENTIFICACION	9005008765	**TIPO DE IDENTIFICACION**	NIT
FORMA DE ENTREGA	PAGO ELECTRÓNICO		
CIUDAD DE ENTREGA	BOGOTÁ		
NUMERO DE CUENTA	60200014605	**TIPO DE CUENTA**	CUENTA CORRIENTE
BANCO	BANCOLOMBIA		
GRAV MOVIMIENTOS FINANCIEROS	0		

BENEFICIARIO DEL PAGO

NOMBRE COMPLETO	INGENIUM COLOMBIA SAS		
No. IDENTIFICACIÓN	9005008765	**TIPO DE IDENTIFICACIÓN**	25
NOMBRE:	INGENIUM COLOMBIA SA		
OBSERVACIONES:	FE337 RAD 02-2303-202606250813638		
NÚMERO DE CUENTA	2511050101	**TIPO DE CUENTA**	CUENTA CORRIENTE
BANCO	BC02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	849.344.557		

DETALLE DE LA ORDEN DE PAGO

NO. DOCUMENTO	NO. FACTURA	IMPORTE	RETENCIÓN	NOMBRE DE LA CUENTA	CENTRO DE COSTO	NO. DE DOCUMENTO PRESUPUESTAL

DETALLE DOCUMENTO DE COMPENSACIÓN

ACREEDOR	DOC.COMP.	REFERENCIA	IMPORTE	TEXTO	PEDIDO	CONTRATO
1004003807	5300426264	337	849.344.557	FE337 RAD 02-2303-202606250813638	5400002117	CTO 132-2025