

	FORMATO ÚNICO DE INVENTARIO DOCUMENTAL															GSO-GD-FO-026	
	PROCESO DE GESTIÓN DOCUMENTAL																
	REFERENCIA - ACUERDO No. 001 DE 2004 AGN															VERSIÓN: 2	

ENTIDAD REMITENTE	
ENTIDAD PRODUCTORA	FONDO NACIONAL DEL AHORRO S.A.
UNIDAD ADMINISTRATIVA:	VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL
OFICINA PRODUCTORA:	GERENCIA DE CIBERSEGURIDAD - ASEGURAMIENTO INFORMATICO
OBJETO:	ENTREGA DE DOCUMENTOS A GERENCIA DE CONTRATACION

REGISTRO DE ENTRADA			
AÑO	MES	DIA	N° T
N° T: Número de transferencia			

NO° DE ORDEN	CÓDIGOS			NOMBRE DE LA SERIE, SUBSERIE O ASUNTOS	NOMBRE DE LA UNIDAD DOCUMENTAL	FECHAS EXTREMAS		SOPORTE O FORMATO		FÍSICO						ELECTRÓNICO			FRECUENCIA DE CONSULTA	OBSERVACIONES
	CÓDIGO OFICINA	SERIE	SUBSERIE			(dd-mm-aaaa)		Físico	Electrónico	UNIDAD DE CONSERVACIÓN						Ubicación	Cantidad de documentos	Tamaño de los documentos		
						Inicial	Final			PAPEL				OTRO						
										Caja	Carpeta	Tomo	Número de folios	Tipo	Cantidad					
1	1501	13	3	Contrato prestación de servicios	Contrato No. 173-2023 CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA - Soportes Informe Seguimiento para pago Nro.35 factura Nro. FE43 orden de pago No. 5300437522	20-jun-25	7-jul-25		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	279	12,5 MB		

Autorizado por:	Jessebell Cristina Mejias Linares	Entregado por:	Jessebell Cristina Mejias Linares	Recibido por:	
Cargo:	Auxiliar Administrativo 01	Cargo:	Auxiliar Administrativo 01	Cargo:	
Firma:		Firma:		Firma:	
Lugar:	Bogotá D.C.	Lugar:	Bogotá D.C.	Lugar:	
Fecha:	30-07-2025	Fecha:	30/07/2025	Fecha:	

	INFORME DE SEGUIMIENTO Y DE EVALUACIÓN CONTRACTUAL		Código: GLC-CONT-FO-016	
	PROCESO CONTRATACION		Versión: 1	

INFORME No	35	FACTURA No	FECHA	
No. DE ACEPTACIÓN:		1000056459 / 1000056461	20 dd	06 mm
			25 aaaa	

1. GENERALIDADES DEL CONTRATO

CONTRATO No 173 DE 2023 TIPO DE CONTRATO Prestación de servicios
(Número de Contrato) (Año de suscripción) (Prestación de servicios, interventoría, consultoría, Comento)

ORDENADOR DEL GASTO SANDRA MILENA BURGOS BELTRAN SECRETARIA GENERAL
(Nombre del ordenador del Gasto) (Cargo del ordenador del Gasto)

CONTRATISTA CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA
(Escriba el nombre o razón social del contratista)

TIPO DE INTERVENTORIA Y/O SUPERVISIÓN: ☒ INDIVIDUAL ☐ COLEGIADA

INTERVENTOR Y/O SUPERVISOR Juan Sebastian Cardenas Hernández
(Escriba nombre del supervisor o interventor del contrato) (Escriba nombre del supervisor o interventor del contrato)

APOYO SUPERVISIÓN Enrique Alfredo Arrazola Montes Frank Leonardo Ortiz Vela
(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 UNIDAD DE CIBERSEGURIDAD QUE PROPORCIONE SERVICIOS DE SEGURIDAD INTEGRADOS AL FONDO NACIONAL DEL AHORRO

DEPENDENCIA EJECUCIÓN CONTRATO VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL
(Gerencia de Estrategia TI y aseguramiento informatico) (Indique el nombre de la dependencia responsable del contrato)

PLAZO DE EJECUCIÓN DEL CONTRATO 24 Meses
(Indique en este espacio el número de días o de meses para ejecutar el contrato)

FECHA DE INICIACIÓN DEL CONTRATO 22 DE dic DE 2023
(Día) (Mes) (Año)

FECHA DE TERMINACIÓN DEL CONTRATO 21 DE dic DE 2025
(Día) (Mes) (Año)

REGISTRO PRESUPUESTAL No. 5400001604 - 6200000102 - 5400001890 - 6200000115

VALOR DEL CONTRATO

TREINTA Y SEIS MIL CUATROCIENTOS NOVENTA Y NUEVE MILLONES QUINIENTOS OCHENTA Y TRES MIL SEISCIENTOS DIEZ PESOS MONEDA CORRIENTE (\$36.499.583.610,00) M/CTE INCLUIDO IVA Y DEMÁS CONTRIBUCIONES A LAS QUE HAYA LUGAR.

ADICIÓN NRO: 1 DIECINUEVE MIL NOVECIENTOS VEINTIDOS MILLONES NOVECIENTOS OCHENTA Y SIETE MIL CUATROCIENTOS NOVENTA Y TRES PESOS M/CTE (\$19.922.987.493)

El valor del presente contrato es hasta la suma DE CINCUENTA Y SEIS MIL CUATROCIENTOS VEINTIDÓS MILLONES QUINIENTOS SETENTA Y UN MIL CIENTO TRES PESOS M/CTE (\$56.422.571.103)

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

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><th colspan="2">PRÓRROGAS</th></tr> <tr> <th>No.</th><th>PLAZO</th></tr> <tr><td> </td><td> </td></tr> </table>	PRÓRROGAS		No.	PLAZO			<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><th colspan="3">ADICIONES</th></tr> <tr> <th>No.</th><th>VALOR</th><th>RP</th></tr> <tr> <td>1</td><td>\$ 19.922.987.493</td><td>5400001890</td></tr> </table>	ADICIONES			No.	VALOR	RP	1	\$ 19.922.987.493	5400001890	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><th colspan="3">SUSPENSIONES</th></tr> <tr> <th>No</th><th>DESDE</th><th>HASTA</th></tr> <tr><td> </td><td> </td><td> </td></tr> </table>	SUSPENSIONES			No	DESDE	HASTA			
PRÓRROGAS																										
No.	PLAZO																									
ADICIONES																										
No.	VALOR	RP																								
1	\$ 19.922.987.493	5400001890																								
SUSPENSIONES																										
No	DESDE	HASTA																								

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 46.188.140.481,00	81,86%
Valor del pago aprobado con el presente informe	\$ 260.372.000,00	0,46%
VALOR TOTAL EJECUTADO	\$ 46.448.512.481,00	82,32%
Porcentaje de ejecución presupuestal programado a la fecha		82,36%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,04%

OBSERVACIONES

Cuenta 35: Pago de Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A y Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A. **Periodo del 22 de marzo 2025 al 21 de abril 2025**
La diferencia en la ejecución Presupuestal se presenta por cobros de ANS en cuentas 3 y 4.

(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	100%
Porcentaje de ejecución de actividades realizado a la fecha	100%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CONTRATO	0%

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

*La fase de ejecución corresponde a desarrollo de Software de propiedad del FNA

SI ☐ NO ☒

*Si corresponde a Software del FNA marque la fase correspondiente

Investigación ☐ Desarrollo ☐

OBSERVACIONES

Se realizó el debido seguimiento de los Acuerdos de Niveles de Servicio establecidos para el CTO 173 de 2023, encontrando que el contratista cumplió con todas las actividades estipuladas contractualmente sin que se dé lugar a ninguna penalización.

(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 CTO 173 de 2023 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 valor de DOSCIENTOS SESENTA MILLONES TRESCIENTOS SETENTA Y DOS MIL PESOS MCTE (\$ 260.372.000).

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 ESTRATEGIA TI Y ASEGURAMIENTO INFORMATICO, EN SU CONDICIÓN DE SUPERVISOR DEL CONTRATO No. 173 DEL 2023

CERTIFICA:

Que CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA, identificado con NIT. No 901781625-1, entregó un informe de las actividades desarrolladas en el período, dando de esta manera cumplimiento a las obligaciones contenidas en el Contrato No. 173 del 2023.

ANEXOS PRESENTE INFORME

ANEXO	No FOLIOS	DESCRIPCION
Certificado pago Seguridad Social ☒	PDF	Certificaciones, planilla pago parafiscales
Informes ☒	PDF	Informe de Supervisión Informe Gestión Proveedor
Actas ☒	PDF	Acta Seguimiento Mensual ANS
OTROS ☒	PDF	Pre-factura Certificación Cuenta Bancaria Rut's Resolución Facturación Certificación Cumplimiento Circular SFC

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

Veinte

20

días del mes de

junio

de

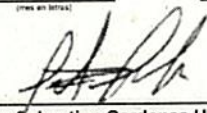
2025

(Se en letras)

(Se en números)

(mes en letras)

(Año)


Juan Sebastian Cardenas HernándezGerente Estrategia TI y aseguramiento informatico
Supervisor CTO173-2023
Revisó y aprobó: Frank Leonardo Ortiz Vela - Jonathan Escobar Rodriguez - Enrique Alfredo Arrazola Montes Apoyos a la supervisión

Estadística de datos	Cantidad
Registros transferidos	8

Cl.doc. : RE (Factura bruto) Documento normal					
Reg.prelim.por		NTUIRAN	Contab.por		MRINCONZ
N° doc.	5100001275	Sociedad	1000	Ejercicio	2025
Fe.docum.	24.06.2025	Fecha contab.	24.06.2025	Período	06
Calc.impuestos	☒				
Referen.	43				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202506260793743				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	244,364,592-
2	86	2511950101	CXP PROVED EM/RF		W0	183,638,420
3	91	5130950114	SERV DE APOYO TEMP		W0	0
4	86	2511950101	CXP PROVED EM/RF		W0	76,733,580
5	91	5130950408	GESTION Y MON SGSI		W0	0
6	50	2519051101	SERVICIO 3.5%			7,658,000-
7	50	2519053801	RTE IVA TARIFA GENER			6,235,800-
8	50	2519054408	SERVICIOS 304 BOGOTA			2,113,608-



CONSORCIO UNIDAD DE
CIBERSEGURIDAD FNA
NIT 901.781.625-1
CALLE 99 10 19
Tel: (601) 5527210
Bogotá - Colombia
contadorjunior@mnemo.com



Factura electrónica de venta
No. FE 43

Señores	Fondo Nacional de Ahorro SA		
NIT	899.999.284-4	Teléfono	(601) 3810150 - Ext. 000
Dirección	CR 12 65 11	Ciudad	Bogotá - Colombia

Fecha y hora Factura	
Generación	24/06/2025, 08:34
Expedición	24/06/2025, 08:50
Vencimiento	24/07/2025

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A Contrato 173-2023 N° de aceptación1000056459 / 1000056461	1.00	0.00	183,638,420.00
2	Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados. Contrato 173-2023 N° de aceptación N°1000056459 / 1000056461	1.00	0.00	76,733,580.00

Total items: 2

Valor en Letras:

Doscientos sesenta millones trescientos setenta y dos mil pesos m/cte

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2025-07-24 por \$ 260,372,000.00

Observaciones:

Total Bruto	218,800,000.00
IVA 19%	41,572,000.00
Total a Pagar	260,372,000.00

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 18764085737391 aprobado en 20241219 prefijo FE desde el número 33 al 5000 Vigencia: 12 Meses**
Responsable de IVA - Actividad Económica 6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Tarifa 9.66
CUFE: b1ef7fe920ab0c1490933e28cbe04f63d2654857ef177881bd61c9b34cdc06c5c92fd2b911cba6c68b4616651b4e15a0

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA
NIT 901.781.625-1

CERTIFICA QUE:

HUMBERTO DE JESUS VELEZ CASTRO, mayor de edad, residente en la ciudad de Bogotá D.C., identificado con C.C. No. 8.770.446 expedida en Soledad-Atlántico, obrando en calidad de Representante legal del **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA**, identificado con el NIT No. 901.781.625-1, de conformidad con lo establecido en el documento de conformación del CONSORCIO en mención, medio del presente me permito **CERTIFICAR**, que el CONSORCIO no tiene empleados a cargo vinculados para el proyecto del Contrato No. 173-2023, suscrito entre el **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA** y el **FONDO NACIONAL DEL AHORRO SA**, razón por la cual no estamos obligados a realizar pagos por concepto de seguridad social y parafiscales, como quiera que el personal del proyecto se encuentra vinculado directamente por **MNEMO COLOMBIA S.A.S.** con una participación del 49%, **MNEMO CYBER SEC SAS** con una participación del 50% y **MNEMO EVOLUTION & INTEGRATION SERVICES SAS** con una participación del 1%.

Para constancia de lo anterior se firma en Bogotá a los Once (11) días del mes de Junio de dos mil veinticinco (2025).

Atentamente,



HUMBERTO DE JESUS VELEZ CASTRO

Representante Legal **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA**

C.C. No. 8.770.446 expedida en Soledad-Atlántico.

Dirección: Calle 99 No. 10 - 19 Oficina 502 Edificio Trade Center de Bogotá D.C.

Teléfono: 6913133 - 310 8569109

Correo electrónico: h.dejesusvelez@mnemo.com



**CERTIFICACIÓN DE CUMPLIMIENTO ARTÍCULO 50 LEY 789 DE 2002 Y LEY 828 DE 2003 -
PERSONA JURÍDICA.**

HUMBERTO DE JESUS VELEZ CASTRO, identificado con cédula de ciudadanía No. **8.770.446** de Soledad - Atlántico, y con Tarjeta Profesional No. 61.061-T de la Junta Central de Contadores de Colombia, en mi condición de Revisor Fiscal de la sociedad extranjera con sucursal en Colombia **MNEMO EVOLUTION & INTEGRATION SERVICES SA**, identificada con NIT 901.306.687-2, debidamente inscrito en la Cámara de Comercio de Bogotá D.C., luego de examinar de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico que la sucursal en mención **NO CUENTA CON PERSONAL VINCULADO EN COLOMBIA** por lo que no tiene obligaciones pendientes durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de presentación de la propuesta para el presente proceso de selección, por los conceptos de salud, pensiones, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002. Dada en Bogotá D.C., a los Once (11) días del mes de Junio de 2025.

A handwritten signature in black ink, appearing to read 'H. Velez Castro', written over a horizontal dashed line.

HUMBERTO DE JESUS VELEZ CASTRO

C.C. 8.770.446 de Soledad – Atlántico

T.P. No. 61.061-T de la Junta Central de Contadores de Colombia

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

61061-T

HUMBERTO DE JESUS VELEZ CASTRO
C.C. 8770446
RES. INSCRIPCION 98 DEL 20/06/1998
UNIVERSIDAD AUTONOMA DEL CARIBE

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

251625 69149



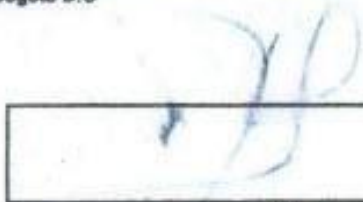
Identificación Plástica C.A. 180017/0118

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Esta tarjeta es el único documento que lo acredita como Contador Público de acuerdo con lo establecido en la Ley 43 de 1990. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (57)(1) 6444450 o devolverla a la UAE – Junta Central de Contadores a la Calle 96 No. 9 A – 21 Bogotá D.C.



FIRMA

EL SUSCRITO REVISOR FISCAL

C E R T I F I C A

Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO CYBER SEC SAS**, con NIT **901.447.968-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, D.C., dedicada a la actividad de desarrollo de sistemas informáticos CIIU 6201, durante el período de los **ÚLTIMO SEIS MESES**, presentó el pago de los aportes al sistema de seguridad social y parafiscales y se pudo verificar que la administración ha cumplido con lo establecido en norma.

Que los registros presentados se encuentran debidamente soportados con los documentos internos y externos que respaldan los pagos a la seguridad social y parafiscales.

Esta certificación se expide por el Revisor Fiscal **JAIRO DAVID TOVAR LOZANO**, identificado C.C. 1.018.408.876 de Bogotá y T.P. 232325-T, para el único fin consagrado en la norma mencionada anteriormente.

En constancia de lo anterior, firmo en la ciudad de Bogotá, D.C., a los (11) Once días del mes de Junio de 2025.

At.



JAIRO DAVID TOVAR LOZANO

Revisor Fiscal T.P. 232325-T

C.C.1.018.408.876 de Bogotá

Cel.3017710213

contadorjunior@mnemo.com

EL SUSCRITO REVISOR FISCAL

C E R T I F I C A

Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO COLOMBIA S.A.S., con NIT 900.396.176-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, D.C., dedicada a la actividad de desarrollo de sistemas informáticos CIIU 6201, durante el período de los **ÚLTIMO SEIS MESES**, presentó el pago de los aportes al sistema de seguridad social y parafiscales y se pudo verificar que la administración ha cumplido con lo establecido en norma.

Que los registros presentados se encuentran debidamente soportados con los documentos internos y externos que respaldan los pagos a la seguridad social y parafiscales.

Esta certificación se expide por el Revisor Fiscal **JOSÉ IGNACIO SALAZAR GÓMEZ**, identificado C.C. 14.239.581 de Ibagué y T.P. 27.398-T, para el único fin consagrado en la norma mencionada anteriormente.

En constancia de lo anterior, firmo en la ciudad de Bogotá, D.C., a los (11) Once días del mes de Junio de 2025.

At.



JOSE IGNACIO SALAZAR GOMEZ

Revisor Fiscal T.P. 27.398-T

C.C. 14.239.581 de Ibagué – Cel. 3158889246 joseignaciosago@hotmail.com

DATOS GENERALES DEL APORTANTE									
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF	
NIT 901447968	1	MNEMO CYBER SEC SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CL 99 10 19	BOGOTA-BOGOTA D.E.	5527210	Si	

DATOS GENERALES DE LA LIQUIDACION									
Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Días Mora	Valor
2025-04	2025-05	1483846404	9486048533	E	2025/05/16	2025/05/15	BANCO DAVIVIENDA	0	\$47,127,000

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES																PENSION		SALUD		CCF		RIESGOS		PARAFISCALES			
No.	Identificación	Nombre	ing	ret	de	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (37 Afiliados)																														
Centro de Trabajo: CENTRO TRABAJO 1 (36 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (36 Afiliados)																														
1	CC	80180206	AMAZO RAMIREZ WALTER JAIR																	230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	SI
2	CC	1015425546	CAITA CORREA CHRISTIAM GERMAN										X							25-14	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	SI
3	CC	1015425546	CAITA CORREA CHRISTIAM GERMAN																	25-14	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	SI
4	CC	1070981128	COLLAZOS FONSECA MATEO																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	SI
5	CC	1018423823	CORTES GUTIERREZ ALFREDO ALEJANDRO	X																230201	8	EPS008	8	CCF24	8	14-25	8	0.522%	8	SI
6	CC	80169118	COY FRANCO JOHAN MANUEL	X																230201	8	EPS017	8	CCF24	8	14-25	8	0.522%	8	SI
7	CC	79619776	ENCISO ALARCON JOHN JAIRO																	230301	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	SI
8	CC	91180662	GARRIDO PRADA YEINSON ALBERTO	X																230301	8	MIN001	8	CCF24	8	14-25	8	0.522%	8	SI
9	CC	80048819	JARAMILLO RAMIREZ MIGUEL ANGEL	X																25-14	8	EPS008	8	CCF24	8	14-25	8	0.522%	8	SI
10	CC	1024460422	JIMENEZ JIMENEZ BRAYAN STEVEN									X								25-14	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	SI
11	CC	1193390038	LIZARAZO HERNANDEZ ANDREY JAVIER																	230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	SI
12	CC	1015474263	LOZANO ESCAMILLA JOHAN ALEXIS									X								25-14	27	EPS008	27	CCF24	27	14-25	27	0.522%	27	SI
13	CC	1015474263	LOZANO ESCAMILLA JOHAN ALEXIS										X							25-14	3	EPS008	3	CCF24	0	14-25	3	0.000%	0	SI
14	CC	1019138524	MALLAMA MEJIA JOHNNY ALBEIRO									X								230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	SI
15	CC	1016017636	MARTIN GONZALEZ GUSTAVO ADOLFO	X																25-14	23	EPS002	23	CCF24	23	14-25	23	0.522%	23	SI
16	CC	13871620	MARTINEZ CARREÑO HECTOR MANUEL																	230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	SI
17	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																	230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	SI
18	CC	80182122	MEDINA ROJAS EDWIN FERNEY	X															X	231001	22	EPS005	22	CCF24	22	14-25	22	0.522%	22	SI
19	CC	1018453849	MERCHAN SANCHEZ LUISA FERNANDA									X								230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	SI
20	CC	1012373695	MONTERO BARRETO SINDY JOHANNA									X								230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	SI
21	CC	1023937645	MORENO DIAZ WENDY JOHANNA									X								230301	28	EPS017	28	CCF24	28	14-25	28	0.522%	28	SI
22	CC	1023937645	MORENO DIAZ WENDY JOHANNA										X							230301	2	EPS017	2	CCF24	0	14-25	2	0.000%	0	SI
23	CC	1233901826	MOYAN SANTANA CRISTIAN CAMILO									X								230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	SI

[illegible]

DATOS GENERALES DEL APORTANTE										
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 901447968	1	MNEMO CYBER SEC SAS		B - MENOS DE 200 COTIZANTES		PRINCIPAL	CL 99 10 19	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION										
Periodo		Clave		Tipo	Fecha		Pago			
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor	
2025-04	2025-05	1483846404	9486048533	E	2025/05/16	2025/05/15	BANCO DAVIVIENDA	0	\$47,127,000	
RESUMEN DE PAGO										
RIESGO		CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR	
AFP (ADMINISTRADORAS: 5)					37	\$29,534,100	\$0	\$0	\$29,534,100	
COLFONDOS	231001	800,227,940	6	3	\$2,460,500	\$0	\$0	\$2,460,500		
COLPENSIONES	25-14	900,336,004	7	10	\$9,135,200	\$0	\$0	\$9,135,200		
PORVENIR	230301	800,224,808	8	13	\$8,294,100	\$0	\$0	\$8,294,100		
PROTECCION	230201	800,229,739	0	9	\$7,912,400	\$0	\$0	\$7,912,400		
SKANDIA	230901	800,253,055	2	2	\$1,731,900	\$0	\$0	\$1,731,900		
ARL (ADMINISTRADORAS: 1)					37	\$998,700	\$0	\$0	\$998,700	
COLMENA	14-25	800,226,175	3	37	\$998,700	\$0	\$0	\$998,700		
CCF (ADMINISTRADORAS: 1)					37	\$7,203,000	\$0	\$0	\$7,203,000	
COMPENSAR	CCF24	860,066,942	7	37	\$7,203,000	\$0	\$0	\$7,203,000		
EPS (ADMINISTRADORAS: 9)					37	\$8,570,600	\$0	\$0	\$8,570,600	
CAPITAL SALUD	EPSC34	900,298,372	9	1	\$137,600	\$0	\$0	\$137,600		
COMPENSAR	EPS008	860,066,942	7	8	\$1,358,400	\$0	\$0	\$1,358,400		
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	2	\$591,800	\$0	\$0	\$591,800		
FAMISANAR	EPS017	830,003,564	7	6	\$983,200	\$0	\$0	\$983,200		
FOSYGA	MIN001	901,037,916	1	3	\$705,400	\$0	\$0	\$705,400		
NUEVA E.P.S.	EPS037	900,156,264	2	2	\$325,300	\$0	\$0	\$325,300		
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	\$166,600	\$0	\$0	\$166,600		
SALUD TOTAL	EPS002	800,130,907	4	6	\$1,344,000	\$0	\$0	\$1,344,000		
SANITAS	EPS005	800,251,440	6	8	\$2,958,300	\$0	\$0	\$2,958,300		
ICBF (ADMINISTRADORAS: 1)					2	\$492,400	\$0	\$0	\$492,400	
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	2	\$492,400	\$0	\$0	\$492,400		
SENA (ADMINISTRADORAS: 1)					2	\$328,200	\$0	\$0	\$328,200	
SENA	PASENA	899,999,034	1	2	\$328,200	\$0	\$0	\$328,200		
TOTAL					37	\$47,127,000	\$0	\$0	\$47,127,000	

DATOS GENERALES DEL APORTANTE									
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF	
NIT 900396176	1	MNEMO COLOMBIA SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si	

DATOS GENERALES DE LA LIQUIDACION									
Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco		Valor
2025-04	2025-05	1486672857	9486044751	E	2025/05/20	2025/05/16	BANCO BBVA COLOMBIA S.A.		\$164,669,900

LIQUIDACION DETALLADA DE APORTES																																
EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS		PARAFISCALES				
No.	Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF		
SUCURSAL: PRINCIPAL (97 Afiliados)																																
Centro de Trabajo: ACTIVIDADES EN CLIENTE VISITA / TRASLADOS (20 Afiliados)																																
Ciudad: BOGOTA Depto: BOGOTA D.E. (20 Afiliados)																																
1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																	230201	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si		
2	CC	93387321	ARANA REYES JAMES GUSTAVO																	25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No		
3	CC	67016350	BOCANEGRA VALBUENA ANA MARIA								X									25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	No		
4	CC	1122651302	CARO ROA JONATHAN																	230301	27	EPS005	27	CCF24	27	14-25	27	1.044%	27	Si		
5	CC	1122651302	CARO ROA JONATHAN												X					230301	3	EPS005	3	CCF24	3	14-25	3	0.000%	3	Si		
6	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																	230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si		
7	CC	1013592039	EMBUS IPIA JULIAN ANDRES																	231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No		
8	CC	6319789	ESPAÑA MOSQUERA JESUS ARBEY																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No		
9	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																	25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si		
10	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO																	231001	13	EPS005	13	CCF24	13	14-25	13	1.044%	13	Si		
11	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO												X					231001	17	EPS005	17	CCF24	17	14-25	17	0.000%	17	Si		
12	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si		
13	CC	79865487	PUENTES CASTRO DAVID EDUARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si		
14	CC	79717549	RODRIGUEZ JOHN FERNANDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si		
15	CC	80791790	ROJAS ARIAS RICARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No		
16	CC	80066361	ROMERO ARCHILA DANIEL DARIO																	230201	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si		
17	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																	230901	27	EPS005	27	CCF24	27	14-25	27	1.044%	27	Si		
18	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI											X						230901	3	EPS005	3	CCF24	0	14-25	3	0.000%	0	Si		
19	CC	24659147	VALDES RAMIREZ ALBA LIBIA																	0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No			
20	CC	79950164	VARGAS HINCAPIE FERNANDO								X									230301	28	EPS002	28	CCF24	28	14-25	28	1.044%	28	Si		
21	CC	79950164	VARGAS HINCAPIE FERNANDO												X					230301	2	EPS002	2	CCF24	2	14-25	2	0.000%	2	Si		
22	CC	1032410736	VARGAS HINCAPIE HENRY																	230301	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No		
23	CC	1022411758	VARGAS LEON MARIA CAMILA																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si		
24	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																	0	EPS002	30	0	0	0	0.000%	0	0	No			
Centro de Trabajo: ADMINISTRACION (73 Afiliados)																																
Ciudad: BOGOTA Depto: BOGOTA D.E. (73 Afiliados)																																

25	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO																25-14	24	EPS005	24	CCF24	24	14-25	24	0.522%	24		Si
26	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO							X									25-14	6	EPS005	6	CCF24	6	14-25	6	0.000%	6		Si
27	CC	1023953140	ARIAS NATALIA MELIZA							X									230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30		Si
28	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER																231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
29	CC	1023978779	BARRERA PACHECO YURANY PAOLA																230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
30	CC	1026295259	BEJARANO QUIROGA ANDRES FELIPE							X									25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
31	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER																230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30		Si
32	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN																230301	27	EPS002	27	CCF24	27	14-25	27	0.522%	27		Si
33	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN								X								230301	3	EPS002	3	CCF24	3	14-25	3	0.000%	3		Si
34	CC	1113858520	CAMACHO PIRA CRISTIAN ALEXANDER							X									25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
35	CC	1122512867	CAMPOS MARTINEZ JUAN ALEJANDRO							X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
36	CC	1034973743	CASTILLO IDROBO JHON FABER	X														X	230301	4	EPS002	4	CCF24	4	14-25	4	0.522%	4		Si
37	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID							X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
38	CC	80731020	DESALVADOR RESTREPO MARCELO																25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
39	CC	1012976046	DIAZ MARIN CAMILO ARTURO							X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
40	CC	80102292	DIAZ TORRES CHRISTIAN ALEXANDER																230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
41	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER																25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
42	CC	1001326677	GOMEZ PARRA CRISTIAN CAMILO							X									230201	30	EPS001	30	CCF24	30	14-25	30	0.522%	30		Si
43	CC	1019009180	GOMEZ ROJAS YENNY PAOLA																230301	19	EPS037	19	CCF24	19	14-25	19	0.522%	19		Si
44	CC	1019009180	GOMEZ ROJAS YENNY PAOLA								X								230301	11	EPS037	11	CCF24	11	14-25	11	0.000%	11		Si
45	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO							X									25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
46	CC	1002811541	GRAJALES GUTIERREZ JESSICA ALEJANDRA																25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
47	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN																230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
48	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL							X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
49	CC	1010840818	GUEVARA GUANCHA ERWIN SANTIAGO							X									25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
50	CC	1082874657	GUEVARA RIZZO SANTIAGO								X								230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
51	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES																230201	22	EPS005	22	CCF24	22	14-25	22	0.522%	22		No
52	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES									X							230201	8	EPS005	8	CCF24	8	14-25	8	0.000%	8		No
53	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
54	CC	1023949411	HOYOS PEREZ LINA KATERINE																230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30		Si
55	CC	1099374748	LEAL GOMEZ DANIELA																230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
56	CC	52953219	LEON CERON MARIA ALEXANDRA																231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
57	CC	1069769484	LOPEZ ZAMORA JUAN DAVID																230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si

[illegible]

Página 4 de 5

DATOS GENERALES DEL APORTANTE											
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal		Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS		B - MENOS DE 200 COTIZANTES		PRINCIPAL		CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION											
Periodo		Clave		Tipo	Fecha		Pago				
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco		Dias Mora	Valor	
2025-04	2025-05	1486672857	9486044751	E	2025/05/20	2025/05/16	BANCO BBVA COLOMBIA S.A.		0	\$164,669,900	
RESUMEN DE PAGO											
RIESGO		CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES		VALOR A PAGAR	
AFP (ADMINISTRADORAS: 5)					91	\$89,057,200	\$0	\$0	\$89,057,200		
COLFONDOS		231001	800,227,940	6	7	\$9,793,300	\$0	\$0	\$9,793,300		
COLPENSIONES		25-14	900,336,004	7	19	\$21,184,200	\$0	\$0	\$21,184,200		
PORVENIR		230301	800,224,808	8	36	\$27,499,500	\$0	\$0	\$27,499,500		
PROTECCION		230201	800,229,739	0	26	\$25,990,200	\$0	\$0	\$25,990,200		
SKANDIA		230901	800,253,055	2	3	\$4,590,000	\$0	\$0	\$4,590,000		
ARL (ADMINISTRADORAS: 1)					93	\$4,445,800	\$0	\$0	\$4,445,800		
COLMENA		14-25	800,226,175	3	93	\$4,445,800	\$0	\$0	\$4,445,800		
CCF (ADMINISTRADORAS: 1)					93	\$23,544,800	\$0	\$0	\$23,544,800		
COMPENSAR		CCF24	860,066,942	7	93	\$23,544,800	\$0	\$0	\$23,544,800		
EPS (ADMINISTRADORAS: 10)					98	\$39,051,200	\$0	\$0	\$39,051,200		
ALIANSAUD EPS (ANTES COLMEDICA)		EPS001	830,113,831	0	3	\$2,222,100	\$0	\$0	\$2,222,100		
CAPITAL SALUD		EPSC34	900,298,372	9	1	\$134,400	\$0	\$0	\$134,400		
COMPENSAR		EPS008	860,066,942	7	16	\$3,280,900	\$0	\$0	\$3,280,900		
EPS SURA (ANTES SUSALUD)		EPS010	800,088,702	2	4	\$539,000	\$0	\$0	\$539,000		
FAMISANAR		EPS017	830,003,564	7	11	\$2,053,700	\$0	\$0	\$2,053,700		
FOSYGA		MIN001	901,037,916	1	7	\$3,394,500	\$0	\$0	\$3,394,500		
FOSYGA RÉGIMEN DE EXCEPCIÓN		MIN002	901,037,916	1	1	\$200,000	\$0	\$0	\$200,000		
NUEVA E.P.S.		EPS037	900,156,264	2	7	\$1,152,600	\$0	\$0	\$1,152,600		
SALUD TOTAL		EPS002	800,130,907	4	9	\$3,279,700	\$0	\$0	\$3,279,700		
SANITAS		EPS005	800,251,440	6	39	\$22,794,300	\$0	\$0	\$22,794,300		
ICBF (ADMINISTRADORAS: 1)					10	\$5,142,600	\$0	\$0	\$5,142,600		
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR		PAICBF	899,999,239	2	10	\$5,142,600	\$0	\$0	\$5,142,600		
SENA (ADMINISTRADORAS: 1)					10	\$3,428,300	\$0	\$0	\$3,428,300		
SENA		PASENA	899,999,034	1	10	\$3,428,300	\$0	\$0	\$3,428,300		
TOTAL					98	\$164,669,900	\$0	\$0	\$164,669,900		

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

Acta N°	67	Tema:	Reunión de revisión de ANS, contrato 173 de 2023 Adición 2024, *Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A *Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados.
Fecha:	23/05/2025	Ubicación:	Virtual.
Hora inicio:	10:00 am	Hora fin:	11:00 am

Objetivo	Reunión de revisión de ANS, contrato 173-2023 para la evaluación de los ítems de integración de fuentes de seguridad y entrega de cinco modelos predefinidos y adaptados a las fuentes de seguridad del FNA para la solución de ciber analítica.		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	Dependencia	Cargo	¿Asistió?
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático FNA	Profesional 3	Si
Frank Leonardo Ortiz	Gerencia de Estrategia de TI y Aseguramiento Informático FNA	Asesor ejecutivo	Si
María Camila Vargas	Mnemo	Apoyo a la Gerencia del Proyecto	Si
Cesar Pinto	Mnemo	Gerente de Proyecto Mnemo	Si

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

1. TEMAS TRATADOS

Revisión cumplimiento de ANS para de integración de fuentes de seguridad y entrega de cinco modelos predefinidos y adaptados a las fuentes de seguridad del FNA correspondiente a la solución de ciber analítica.

2. RESUMEN DE LOS ACUERDOS

ACUERDO NIVELES DE SERVICIO

- Anexo 2 - Acuerdo de Niveles de Servicio CIBER ANALITICA V1

1. DOCUMENTACIÓN CONTRACTUAL

Se realiza la entrega de los documentos asociados a integración de fuentes de seguridad y entrega de cinco modelos predefinidos y adaptados a las fuentes de seguridad del FNA correspondiente a la solución de ciber analítica.

2. Documentación Mensual o cuando se requiera

Asegurar el cumplimiento de los procedimientos, políticas, normas y directrices establecidas por el FNA.

Documentación Mensual	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
2.1. Informe técnico con el detalle de la Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A. 2.3. Informe técnico con el detalle de los cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados con base en el Gobierno del dato	Cumplimiento de tiempo establecido para los entregables correspondientes a cada una de las etapas del contrato. Por cada 5 incumplimientos → 0,5% del valor de la facturación mensual que se irán acumulando.	0	0	0	Ninguna

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

previamente establecido, en el entorno provisionado para la entidad. 2.5. Diagrama de arquitectura actual que incluye las Características técnicas de HW y SW de la plataforma, El cual deberá ser entregado durante el 2do mes contado a partir de la legalización del contrato. 2.9. Manuales de Usuario, técnico, configuración e instalación de los componentes de la plataforma de ciber analítica.						
---	--	--	--	--	--	--

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

2. SISTEMA DE GESTIÓN DE CALIDAD

Se da cumplimiento al uso de los formatos y procedimientos del FNA.

Sistema de Gestión de Calidad					
Asegurar el cumplimiento de los procedimientos, políticas, normas y directrices establecidas por el FNA.					
Sistema de Gestión de Calidad	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
Cumplimiento en procedimientos, políticas, normas y directrices establecidas por el FNA.	A partir de 1 incumplimiento en procedimientos, políticas, normas y directrices	0	0	0	Ninguna

Observación: De acuerdo con lo validado no se presentaron llamados de atención por parte de FNA, y se dio cumplimiento a los procedimientos y políticas indicadas por FNA.

3. CUMPLIMIENTO DEL CRONOGRAMA

El avance en el cronograma para los ítems de implementación de la solución de ciber analítica bajo el contrato 173-2023. a corte de la fecha de finalización de acuerdo con la última versión del cronograma, corresponde al 100% esperado vs 97 % real, con una desviación del 3% dados los inconvenientes técnicos presentados en la integración de algunas fuentes puntuales. Cabe anotar que se generó una versión 2 de cronograma de común acuerdo entre la supervisión del contrato de parte de FNA (Mónica Grand) , el director comercial de Consorcio unidad de ciberseguridad FNA (Ricardo Rojas) y director de operaciones del Consorcio unidad de ciberseguridad FNA (Henry Vargas), dada la extensión de licenciamiento de la solución de ciber analítica y el cambio en las fechas de implementación de las soluciones a implementar, compromiso descrito en el acta # 35 con nombre GEGPFO001ACTADEREUNION_FNA 173-2023.



GEGPFO001ACTADE
REUNION_FNA 173-2

De acuerdo con lo anterior la evaluación del cumplimiento de cronograma va atado a estas nuevas fechas acordadas con esta nueva versión, descritas en detalle a continuación:

% completado	% completado esperadoT1	Nombre de tarea	Duración	Comienzo	Fin
97%	100%	Datafabric	88 días	jue 26/12/24	vie 02/05/25
100%	100%	Planeación	21 días	vie 27/12/24	mar 28/01/25
100%	100%	Evaluación inicial y planificación	8 días	lun 13/01/25	mié 22/01/25
100%	100%	Identificar las fuentes de datos	2 días	jue 23/01/25	vie 24/01/25

	FORMATO ACTA DE REUNIÓN		Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD		Versión: 1

100%	100%	Analizar los flujos de datos actuales y los puntos de integración	2 días	lun 27/01/25	mar 28/01/25
100%	100%	Generacion - Plan de trabajo y Cronograma Ciber Analítica	10 días	vie 27/12/24	lun 13/01/25
100%	100%	Entrega - Plan de trabajo y Cronograma Ciber Analítica	0 días	lun 13/01/25	lun 13/01/25
97%	100%	Implementación	87 días	jue 26/12/24	mié 30/04/25
100%	100%	Configuración y disponibilización	21 días	jue 26/12/24	mar 28/01/25
100%	100%	Adquisición de licenciamiento	5 días	jue 26/12/24	jue 02/01/25
100%	100%	Definición y adquisición del Dominio	1 día	vie 03/01/25	vie 03/01/25
100%	100%	Definición y adquisición de certificado	5 días	mar 07/01/25	lun 13/01/25
100%	100%	Aprovisionamiento tenant AWS	3 días	mié 08/01/25	vie 10/01/25
100%	100%	Aprovisionamiento instancias virtuales	4 días	lun 13/01/25	jue 16/01/25
100%	100%	Instalación Base stratio	3 días	vie 17/01/25	mar 21/01/25
100%	100%	Instalación de Modulos	4 días	mié 22/01/25	lun 27/01/25
100%	100%	Informe de configuración y disponibilización de los entornos de trabajo	3 días	mié 22/01/25	vie 24/01/25
100%	100%	Entrega de licenciamiento - certificación emitida por el proveedor	0 días	vie 03/01/25	vie 03/01/25
100%	100%	Entrega - Acta de entrada en producción de la plataforma de ciber analítica	0 días	mar 28/01/25	mar 28/01/25
100%	100%	Integración de fuentes	32 días	vie 14/02/25	vie 28/03/25
100%	100%	Comunicaciones	11 días	vie 14/02/25	jue 27/02/25
100%	100%	Solicitud direccionamiento interno para gateway	1 día	vie 14/02/25	vie 14/02/25
100%	100%	Entrega de direccionamiento para gateway	3 días	sáb 15/02/25	mar 18/02/25
100%	100%	Control de cambios VPN	5 días	jue 20/02/25	mié 26/02/25
100%	100%	Creación VPN	1 día	jue 27/02/25	jue 27/02/25
100%	100%	Integracion de fuentes de datos	21 días	vie 28/02/25	vie 28/03/25
100%	100%	Cifrado	7 días	lun 17/03/25	mar 25/03/25
100%	100%	Vigilancia (IOC)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	DAM (IBM Guardium)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	WAF (FortiWeb)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Malware Lab (IOC)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Evaluación de seguridad (Vuln)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Análisis de código (Vuln)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Protección de endpoints (Trendmicro)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	XDR (Trendmicro)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	SOAR (Qradar)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Protección web (Proxy)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Inteligencia de Amenazas (IOC)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	IPS (Trendmicro TippingPoint)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	DNS (Infoblox Bloxone)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	NDR (Darktrace)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Sandbox (Trendmicro Deep dicoverly analyzer)	7 días	vie 28/02/25	lun 10/03/25

	FORMATO ACTA DE REUNIÓN		Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD		Versión: 1

100%	100%	Gobernanza (DLP)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Protección en la nube (CASB)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Seguridad de correo electrónico (Dark trace Email)	7 días	vie 28/02/25	lun 10/03/25
100%	100%	SOC	7 días	vie 28/02/25	lun 10/03/25
100%	100%	Generacion - Informe tecnico con el detalle de la Integración de las fuentes	3 días	mié 26/03/25	vie 28/03/25
100%	100%	Entrega - Informe tecnico con el detalle de la Integración de las fuentes	0 días	vie 28/03/25	vie 28/03/25
100%	100%	Gobierno del dato	58 días	vie 31/01/25	mié 23/04/25
100%	100%	Listar fuentes, dominios de datos y vincularlos a un modelo taxonómico	4 días	vie 31/01/25	mié 05/02/25
100%	100%	Identificar responsables participantes del gobierno del dato	5 días	jue 06/02/25	mié 12/02/25
100%	100%	Establecer el modelo taxonómico/base de los datos	14 días	jue 13/02/25	lun 03/03/25
100%	100%	Definir la taxonomía, glosario y reglas para el Gobierno del Dato	12 días	mar 04/03/25	mié 19/03/25
100%	100%	Analizar la situación actual para entender brechas y oportunidades.	5 días	jue 20/03/25	mié 26/03/25
100%	100%	Definir roles y responsables (políticas)	5 días	jue 27/03/25	mié 02/04/25
100%	100%	Crear una ontología asociada (estructura conceptual de datos)	5 días	jue 03/04/25	mié 09/04/25
100%	100%	Generación de informe de gobierno	8 días	jue 10/04/25	mié 23/04/25
100%	100%	Entrega informe de gobierno del dato	0 días	mié 23/04/25	mié 23/04/25
100%	100%	Configuracion de Casos de Uso (Modelos)	59 días	jue 06/02/25	mié 30/04/25
100%	100%	Implementación C.U.1 Gestión unificada de amenazas	31 días	jue 06/02/25	mié 19/03/25
100%	100%	Recibir csv de datos iniciales	4 días	jue 06/02/25	mar 11/02/25
100%	100%	Identificar las fuentes y conectores	2 días	mar 18/02/25	mié 19/02/25
100%	100%	Definición de KPI's	2 días	vie 21/02/25	lun 24/02/25
100%	100%	Arquitectura del pipeline de datos	3 días	mar 18/02/25	jue 20/02/25
100%	100%	Arquitectura del modelo de datos	3 días	mar 18/02/25	jue 20/02/25
100%	100%	Extracción y carga de datos deltas	13 días	lun 24/02/25	mié 12/03/25
100%	100%	Transformación de datos	2 días	lun 17/03/25	mar 18/03/25
100%	100%	Construcción de dashboards	2 días	mar 18/03/25	mié 19/03/25
100%	100%	Implementación C.U.2 Patrones de ataque	38 días	jue 06/02/25	vie 28/03/25
100%	100%	Recibir csv de datos iniciales	6 días	jue 06/02/25	jue 13/02/25
100%	100%	Identificar las fuentes y conectores	8 días	mar 18/02/25	jue 27/02/25
100%	100%	Modelado de patrones de autenticaciones y accesos	31 días	sáb 15/02/25	vie 28/03/25
100%	100%	Entendimiento de los datos	6 días	sáb 15/02/25	vie 21/02/25
100%	100%	Transformación de datos	5 días	lun 24/02/25	vie 28/02/25
100%	100%	Modelado y evaluación	5 días	lun 03/03/25	vie 07/03/25
100%	100%	Consumo del modelo	10 días	lun 10/03/25	vie 21/03/25
100%	100%	Dashboard	5 días	lun 24/03/25	vie 28/03/25
100%	100%	Modelado de patrones de tráfico de red anómalo	19 días	vie 14/02/25	mar 11/03/25

	FORMATO ACTA DE REUNIÓN		Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD		Versión: 1

100%	100%	Entendimiento de los datos	4 días	vie 14/02/25	mié 19/02/25
100%	100%	Transformación de datos	4 días	mié 19/02/25	lun 24/02/25
100%	100%	Modelado y evaluación	4 días	lun 24/02/25	jue 27/02/25
100%	100%	Consumo del modelo	4 días	vie 28/02/25	mié 05/03/25
100%	100%	Dashboard	4 días	jue 06/03/25	mar 11/03/25
100%	100%	Modelado de patrones de privilegios y configuraciones	20 días	lun 24/02/25	vie 21/03/25
100%	100%	Entendimiento de los datos	4 días	lun 24/02/25	jue 27/02/25
100%	100%	Transformación de datos	4 días	vie 28/02/25	mié 05/03/25
100%	100%	Modelado y evaluación	4 días	jue 06/03/25	mar 11/03/25
100%	100%	Consumo del modelo	4 días	mié 12/03/25	lun 17/03/25
100%	100%	Dashboard	4 días	mar 18/03/25	vie 21/03/25
100%	100%	Implementación C.U.3 Movimientos laterales	37 días	vie 14/02/25	vie 04/04/25
100%	100%	Recibir csv de datos iniciales	1 día	vie 14/02/25	vie 14/02/25
100%	100%	Identificar las fuentes y conectores	1 día	lun 17/02/25	lun 17/02/25
100%	100%	Modelado de patrones de procesos anómalos	37 días	vie 14/02/25	vie 04/04/25
100%	100%	Entendimiento de los datos	6 días	vie 14/02/25	vie 21/02/25
100%	100%	Transformación de datos	11 días	jue 20/02/25	jue 06/03/25
100%	100%	Modelado y evaluación	7 días	vie 07/03/25	lun 17/03/25
100%	100%	Consumo del modelo	7 días	mar 18/03/25	mié 26/03/25
100%	100%	Dashboard	7 días	jue 27/03/25	vie 04/04/25
100%	100%	Implementación C.U.4 Evaluación de riesgos	36 días	jue 06/02/25	mié 26/03/25
100%	100%	Recibir csv de datos iniciales	6 días	jue 06/02/25	jue 13/02/25
100%	100%	Identificar las fuentes y conectores	6 días	mié 12/02/25	mar 18/02/25
100%	100%	Definición de KPI's	6 días	lun 17/02/25	lun 24/02/25
100%	100%	Transformación de datos	12 días	vie 21/02/25	lun 10/03/25
100%	100%	Construcción de dashboards	12 días	mar 11/03/25	mié 26/03/25
100%	100%	Implementación C.U.5 Correlacionador de eventos	31 días	lun 17/03/25	mié 30/04/25
100%	100%	entendimiento de los datos	5 días	lun 17/03/25	vie 21/03/25
100%	100%	transformación de datos	5 días	lun 24/03/25	vie 28/03/25
100%	100%	modelado y evaluación	5 días	lun 31/03/25	vie 04/04/25
100%	100%	consumo del modelo	5 días	lun 07/04/25	vie 11/04/25
100%	100%	dashboard	8 días	lun 14/04/25	vie 25/04/25
100%	100%	<i>Etapas cierre modelos</i>	3 días	lun 28/04/25	mié 30/04/25
95%	100%	Entregables	87 días	jue 26/12/24	mié 30/04/25
100%	100%	Entregables Caso de Uso	28 días	jue 20/03/25	mié 30/04/25
100%	100%	Generación Informe Tecnico Modelo probado documentado y disponibilizado	28 días	jue 20/03/25	mié 30/04/25
100%	100%	Entrega informe tecnico modelo Caso de uso 1 con su respectiva disponibilización	0 días	mié 30/04/25	mié 30/04/25
100%	100%	Generación Informe Tecnico Modelo probado documentado y disponibilizado	26 días	lun 24/03/25	mié 30/04/25

	FORMATO ACTA DE REUNIÓN		Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD		Versión: 1

100%	100%	Entrega informe tecnico modelo de caso de uso 2 con su respectiva dispinibilización	0 días	mié 30/04/25	mié 30/04/25
100%	100%	Generación informe Tecnico Modelo probado documentado y disponibilizado	16 días	lun 07/04/25	mié 30/04/25
100%	100%	Entrega informe tecnico modelo caso de uso 3 con su respectiva disponibilización	0 días	mié 30/04/25	mié 30/04/25
100%	100%	Generación informe Tecnico Modelo probado documentado y disponibilizado	23 días	jue 27/03/25	mié 30/04/25
100%	100%	Entrega informe tecnico modelos Caso de uso 4 con su respectiva disponibilización	0 días	mié 30/04/25	mié 30/04/25
100%	100%	Generación informe tecnico modelo probado documentado y disponibilizado	3 días	lun 28/04/25	mié 30/04/25
100%	100%	Entrega informe tecnico modelo Caso de uso 5 con su respectiva disponibilización	0 días	mié 30/04/25	mié 30/04/25
100%	100%	Diagramas de Arquitectura	75 días	vie 27/12/24	vie 11/04/25
100%	100%	Generación Diagrama Nivel 0	60 días	vie 27/12/24	vie 21/03/25
100%	100%	Generación Diagrama Nivel 1	60 días	vie 27/12/24	vie 21/03/25
100%	100%	Generación Diagrama Nivel 2	60 días	vie 27/12/24	vie 21/03/25
100%	100%	Generacion - Diagrama de arquitectura actual que incluye las Características técnicas de HW y SW de la plataforma	15 días	lun 24/03/25	vie 11/04/25
100%	100%	Entrega - Informe Diagrama de arquitectura (Topologia)	0 días	vie 11/04/25	vie 11/04/25
89%	100%	Otros Entregables	76 días	jue 26/12/24	vie 11/04/25
70%	100%	Generacion - Plan de tranferencia de conocimiento y manuales	75 días	vie 27/12/24	vie 11/04/25
70%	100%	Entrega - Plan de tranferencia de conocimiento y manuales	0 días	vie 11/04/25	vie 11/04/25
100%	100%	Generacion - Plan de continuidad de operación del servicio	45 días	vie 27/12/24	vie 28/02/25
100%	100%	Entrega - Plan de continuidad de operación del servicio	0 días	vie 28/02/25	vie 28/02/25
100%	100%	Generación hoja de vida de los equipos que conforman la plataforma	60 días	vie 27/12/24	vie 21/03/25
95%	100%	Entrega - hoja de vida d elos equipos que conforman la plataforma	0 días	vie 21/03/25	vie 21/03/25
95%	100%	Alistamiento - Manuales de usuario, tecnico, configuración	60 días	vie 27/12/24	vie 21/03/25
90%	100%	Entrega - Manuales de usuario, tecnico, configuración	0 días	jue 26/12/24	jue 26/12/24
0%	0%	Cierre etapa implementacion Ciberanalitica	1 día	vie 02/05/25	vie 02/05/25

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

CUMPLIMIENTO DE CRONOGRAMA					
El proveedor deberá hacer entrega de un cronograma donde se plasmen todas las actividades el contrato.					
Sistema de Gestión de Calidad	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
Ejecución de actividades según lo establecido en el cronograma del contrato. Máximo 2 días de atraso en la fecha de ejecución con respecto a la planeada en el cronograma para el corte que se defina	Por cada 3 incumplimientos → 0,5% del valor de la facturación mensual que se irán acumulando.	0	0	0	Ninguna

Medición:

88 días equivale al 100% para la etapa de implementación de la solución de ciber analítica de acuerdo con cronograma, es decir que 1 día equivale al 1,14 %, por lo cual un retraso del 4% equivale a 2,63 días de retraso.

De acuerdo con ello no hay penalidad, teniendo en cuenta que la aplicación del 0,5% de ans debería excederse en más de 6 días de retraso en el cronograma.

4. DISPONIBILIDAD DEL SERVICIO

Este ítem no aplica para la evaluación del ítem a evaluar en esta acta de ans, dado a que se está evaluando la etapa de implementación en los ítems de Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A y entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados.

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

5. RECURSO HUMANO

5. Disponibilidad del recurso humano					
Garantizar que el personal asignado por el proveedor cumpla tanto con los perfiles definidos en el Anexo Técnico, como con la disponibilidad allí pactada.					
Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
Garantizar que el personal asignado por el proveedor cumpla tanto con los perfiles definidos en el Anexo 1 Especificaciones Técnicas Adición	Por cada dos (2) incumplimientos → 1% del valor de la facturación mensual que se irán acumulando.	0	0	0	

6. TIEMPO DE REMEDIACIÓN DE VULNERABILIDADES

Este ítem no aplica para la evaluación del ítem a evaluar en esta acta de ans

7. TIEMPO DE SOLUCIÓN DE INCIDENTES, SOPORTES Y REQUERIMIENTOS

Este ítem no aplica para la evaluación del ítem a evaluar en esta acta de ans

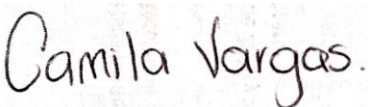
8. DETERMINACIÓN DEL VALOR A FACTURAR

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A	\$ 154.318.000,00	\$ 0,00	\$ 154.318.000,00	\$ 29.320.420,00	183.638.420,00
Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados	\$ 64.482.000,00	\$ 0,00	\$ 64.482.000,00	\$ 12.251.580,00	76.733.580,00
TOTAL	\$ 218.800.000,00	\$ 0,00	\$ 218.800.000,00	\$ 41.572.000,00	\$ 260.372.000,00

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

3. COMPROMISOS PACTADOS

DESCRIPCIÓN	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO

ELABORÓ	APROBÓ
 Cesar Pinto Gerente de Proyecto Consorcio unidad de ciberseguridad FNA	 Enrique Arrazola Apoyo a la supervisión 173-2023 Gerencia de Estrategia de TI y Aseguramiento Informático
APROBÓ	APROBÓ
 Maria Camila Vargas Apoyo a la gerencia del Proyecto Consorcio unidad de ciberseguridad FNA	 Frank Ortiz Apoyo a la supervisión 173-2023 Gerencia de Estrategia de TI y Aseguramiento Informático



FONDO NACIONAL DEL AHORRO
VICEPRESIDENCIA DE TECNOLOGIA Y
TRANSFORMACION DIGITAL
SUPERVISIÓN CTO 173 - 2023

SUPERVISIÓN AL CONTRATO No. 173 de 2023
FONDO NACIONAL DEL AHORRO
Informe No. 35

1. Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad para la plataforma de CiberAnalítica.
2. Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados, para la plataforma de CiberAnalítica.

OBJETO: Contratar unidad de ciberseguridad que proporcione servicios de seguridad integrados al fondo nacional del ahorro

Bogotá, D.C. junio de 2025



1. INTRODUCCIÓN

El presente informe de supervisión del CTO 173 de 2023, cuyo objeto es *"Contratar unidad de ciberseguridad que proporcione servicios de seguridad integrados al fondo nacional del ahorro"*, suscrito entre el FNA y CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA, describe el resumen de las actividades realizadas por cada una de las partes y las observaciones resultado de la labor de seguimiento que se han encontrado respecto al Contrato 173 de 2023.

2. RESUMEN EJECUTIVO

En cumplimiento al apoyo a la supervisión asignada por la Jefatura de la Gerencia de Estrategia TI y Aseguramiento Informático del FONDO NACIONAL DEL AHORRO, se realizó el seguimiento a las actividades conforme a lo establecido en el CTO 173 de 2023. El presente informe tiene como fin el análisis realizado en cuanto al cumplimiento de los hitos referente a:

1. Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DE AHORRO S.A, para la plataforma de CiberAnalítica.
2. Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados, para la plataforma de CiberAnalítica.

3. OBJETIVO DEL INFORME

Realizar seguimiento a los servicios y entregables acorde con lo contratado en el CTO 173 de 2023.

4. OBJETIVOS ESPECÍFICOS DEL INFORME

- Realizar seguimiento a las actividades contratadas y ejecutadas durante el periodo.
- Expedir constancia del cumplimiento a cargo del contratista previo al pago de la factura.
- Identificar las observaciones o desviaciones de las actividades realizadas con el fin de definir los planes de acción para su mitigación o eliminación.

5. INFORME DE AVANCE

De acuerdo con lo establecido en el CTO 173 de 2023, se realiza el seguimiento, control y verificación de los hitos referente a:

1. Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DE AHORRO S.A, para la plataforma de CiberAnalítica.
2. Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados, para la plataforma de CiberAnalítica.

ACTIVIDADES REALIZADAS

Referente al hito No.1 se adjunta el informe **“FNA - Ciber analítica - Fuentes de Informacion.PDF”**, que se centra en describir los procesos, herramientas, y configuraciones establecidas para la captura, normalización y almacenamiento inicial de datos desde diversas fuentes, como archivos en SFTP, tablas en PostgreSQL y APIs externas. Estas fuentes proveen información esencial que sirve como base para la construcción de casos de uso actuales y futuros, asegurando que los datos ingresados estén listos para análisis avanzado, correlación de eventos y monitoreo en tiempo real.

Dentro de este alcance se detallan los flujos de trabajo diseñados para la ingesta de fuentes de datos requeridas en la plataforma de analítica. Así mismo, incluye la orquestación de procesos integrales que abarcan desde la extracción inicial hasta el almacenamiento optimizado en un entorno HDFS, proporcionando información estructurada y transformada en formatos eficientes como Parquet. Estas actividades aseguran la calidad, integridad y disponibilidad de los datos para las distintas aplicaciones de ciberseguridad.

Los aspectos principales cubiertos en este informe incluyen:

1. Extracción de fuentes SFTP: Procesos escalables para la captura de grandes volúmenes de datos en formato JSON mediante workflows organizados por particiones diarias.
2. Normalización de datos: Transformación de datos no estructurados a representaciones tabulares para facilitar su posterior uso en big data.

-
3. Definición de tablas y almacenamiento: Filtrado, estructuración y escritura de datos en tablas clasificadas según las distintas áreas funcionales (SOC, DAM, Gobernanza, etc.), optimizando su disponibilidad en un sistema centralizado dentro del HDFS.
 4. Conexión a bases de datos Postgres: Ingesta de tablas mediante módulos de descubrimiento, virtualización y persistencia, asegurando compatibilidad e integración en la plataforma.
 5. Consumo de APIs externas: Captura de datos relevantes de inteligencia de amenazas en tiempo real para su análisis, almacenaje y aplicación en otros sistemas de la plataforma.

Con respecto al hito No.2, el alcance de esta iniciativa incluyo diseñar, desarrollar e implementar una solución integral de analítica avanzada de ciberseguridad, utilizando plataformas de datos robustas y flexibles como Datafabric Rocket y Datafabric Discovery. Los casos de uso descritos en este documento ilustran aplicaciones específicas destinadas a gestionar amenazas, identificar patrones de ataque, analizar movimientos laterales, evaluar riesgos y mejorar la capacidad de correlación avanzada del SOC (Centro de Operaciones de Seguridad).

La solución cubre los siguientes aspectos principales (Casos de uso):

1. **Gestión Unificada de Amenazas:** Centraliza, integra y transforma fuentes de datos clave (p. ej., logs SIEM, análisis de vulnerabilidades, riesgos de usuarios) para visibilizar amenazas críticas mediante tableros de control interactivos.
2. **Identificación de Movimientos Laterales:** Detecta actividades sospechosas que podrían ser indicadoras de brechas en la seguridad interna, como conexiones HTTP inusuales, comportamiento de redes internas o descargas de scripts sospechosos asociadas a uso de herramientas como PsExec.
3. **Patrones de Ataque:** Señala indicadores relacionados con potenciales cadenas de ataque o comportamiento malicioso repetitivo, asegurando que la detección abarque incluso los escenarios más complejos, como pruebas de penetración o ataques en tiempo real.
4. **Evaluación Integral de Riesgos:** Proporciona una visión centralizada y jerárquica (Nodos, Segmentos, Capas y DEFCON) del nivel de riesgo, apoyándose en fuentes homogéneas y fórmulas de ponderación adaptativas.
5. **Correlación Avanzada:** Fortalece el monitoreo proporcionado por el SOC al relacionar eventos aislados, transformando información aparentemente inofensiva en una visión holística de potenciales amenazas operativas.

Para lo cual se entrega el informe “**FNA - Ciber analítica - informe técnico Casos de Uso.PDF**” y los casos de uso implementados, donde se describen los detalles técnicos más relevantes de cada caso de uso, incluyendo las fuentes de



**FONDO NACIONAL DEL AHORRO
VICEPRESIDENCIA DE TECNOLOGIA Y
TRANSFORMACION DIGITAL
SUPERVISIÓN CTO 173 - 2023**

datos, los procesos de integración/transformación desarrollados en Datafabric Rocket, y el producto resultante en forma de tableros de control disponibilizados mediante Datafabric Discovery, a saber:

1. FNA - Caso de Uso 1 Gestion Unificada Amenazas.PDF
2. FNA - Caso de Uso 2 Patrones de Ataque.PDF
3. FNA - Caso de Uso 3 Movimientos Laterales.PDF
4. FNA - Caso de Uso 4 Evaluación Integral de Riesgos.PDF
5. FNA - Caso de Uso 5 correlación Avanzada.PDF

5.1 INFORMACIÓN DE AVANCE PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 46.188.140.481,00	81,86%
Valor del pago aprobado con el presente informe	\$ 260.372.000,00	0,46%
VALOR TOTAL EJECUTADO	\$ 46.448.512.481,00	82,32%
Porcentaje de ejecución presupuestal programado a la fecha		82,36%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,04%

Por lo cual se concluye que se verificaron cada una de las actividades y entregables definidos en el cronograma de actividades del proyecto, así como los compromisos y observaciones establecidas en las reuniones de seguimiento y relacionadas en las respectivas actas; concluyendo que el avance del proyecto está acorde con lo establecido en el CTO 173 de 2023.

5.2 CONCEPTO SUPERVISION

El contratista cumplió a satisfacción con los hitos referentes a:

1. Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DE AHORRO S.A, para la plataforma de CiberAnalítica.

2. Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados, para la plataforma de CiberAnalítica.

Porcentaje de ejecución proyectado	100%
Porcentaje de ejecución realizado	100%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	0%

6. NIVELES DE SERVICIO

Se realizó el debido seguimiento de los Acuerdos de Nivel de Servicio establecidos para el CTO 173 de 2023, encontrando que el contratista cumplió con todas las actividades estipuladas contractualmente sin que se de lugar a ninguna penalización.

7. VERIFICACIÓN DE ENTREGABLES

Para el desarrollo de las actividades ejecutadas el contratista ha facilitado los siguientes entregables producto de las actividades gestionadas y acordadas en el cronograma de trabajo:

Seguimiento a Entregables del Periodo				
Nº.	Nombre del entregable	Criterio de aceptación	Fecha de entrega	Observaciones
1	FNA - Ciber analítica - Fuentes de Informacion.PDF	Bueno	Mayo 2025	Ninguna
2	FNA - Ciber analítica - informe técnico Casos de Uso.PDF	Bueno	Mayo 2025	Ninguna
3	FNA - Caso de Uso 1 Gestion Unificada Amenazas.PDF	Bueno	Mayo 2025	Ninguna
4	FNA - Caso de Uso 2 Patrones de Ataque.PDF	Bueno	Mayo 2025	Ninguna
5	FNA - Caso de Uso 3	Bueno	Mayo 2025	Ninguna

	Movimientos Laterales.PDF FNA - Caso de Uso 4 Evaluación Integral de Riesgos.PDF			
6	FNA - Caso de Uso 5 correlación Avanzada.PDF	Bueno	Mayo 2025	Ninguna

Se define que, para la facturación del pago del periodo reportado, el contratista debe entregar junto a la prefectura los siguientes documentos:

- Certificación de cumplimiento circulares de la Superintendencia financiera de Colombia
- Certificación de pagos de prestaciones sociales y aportes parafiscales
- Informe de Gestión del Contratista o Acta de entrega formal
- RUT Actualizado
- Certificación Bancaria
- Acta de ANS de la actividad

8. CONCLUSIÓN

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 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 valor de **DOSCIENTOS SESENTA MILLONES TRESCIENTOS SETENTA Y DOS MIL PESOS MCTE (\$ 260,372,000).**

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



**FONDO NACIONAL DEL AHORRO
VICEPRESIDENCIA DE TECNOLOGIA Y
TRANSFORMACION DIGITAL
SUPERVISIÓN CTO 173 - 2023**

Se firma a los 19 días del mes de junio de 2025.

JUAN SEBASTIAN CARDENAS
Gerente Estrategia TI y Aseguramiento
Informático
Supervisor CTO 173 de 2023

ENRIQUE A. ARRAZOLA MONTES
Profesional 03
Apoyo supervisión CTO 173 de 2023

JONATHAN ESCOBAR RODRIGUEZ
Profesional Universitario 2
Apoyo a la Supervisión CTO 173 de 2023

FRANK LEONARDO ORTIZ VELA
Asesor Ejecutivo
Apoyo supervisión CTO 173 de 2023

Caso de Uso 1

Gestión Unificada de Amenazas

MN_EMO



Gestión Unificada de Amenazas

Este documento describe los detalles técnicos más relevantes del caso de uso 1 de Gestión Unificada de Amenazas, incluyendo las fuentes de datos, los procesos de integración/transformación desarrollados en Datafabric Rocket, y el producto resultante en forma de tableros de control disponibilizados mediante Datafabric Discovery.

A través de esta solución, se logra una visión integral de las amenazas de seguridad, vulnerabilidades y riesgos, permitiendo una gestión proactiva de la seguridad informática.

Fuentes de Datos



Logs SIEM

Eventos que representan actividades de diferentes dispositivos en el tiempo, incluyendo tráfico interno o externo. Proviene de dispositivos firewalls de borde, WAF y DNS.



Indicadores de Compromiso

Conjunto de IPs entregadas por la herramienta TreatQ, detectadas como fuentes o destinos potencialmente peligrosos, con una calificación de riesgo asociada.



Análisis de Vulnerabilidades

Análisis periódicos sobre activos críticos para identificar y mitigar oportunidades de acceso no autorizado a datos y servicios del FNA.



Riesgo de Usuarios y Activos Críticos

Logs del directorio activo analizados por una plataforma intermedia y lista de activos críticos identificados mediante IP.

Transformaciones de Datos



ETL Principal

Extrae logs del SIEM, los cruza con indicadores de compromiso y activos críticos para entregar estadísticas de amenazas identificadas con su criticidad.



ETL de Riesgo de Usuarios

Procesa información de riesgo de usuarios para dar soporte al tablero de control correspondiente. Se ejecuta diariamente.



ETL de Análisis de Vulnerabilidades

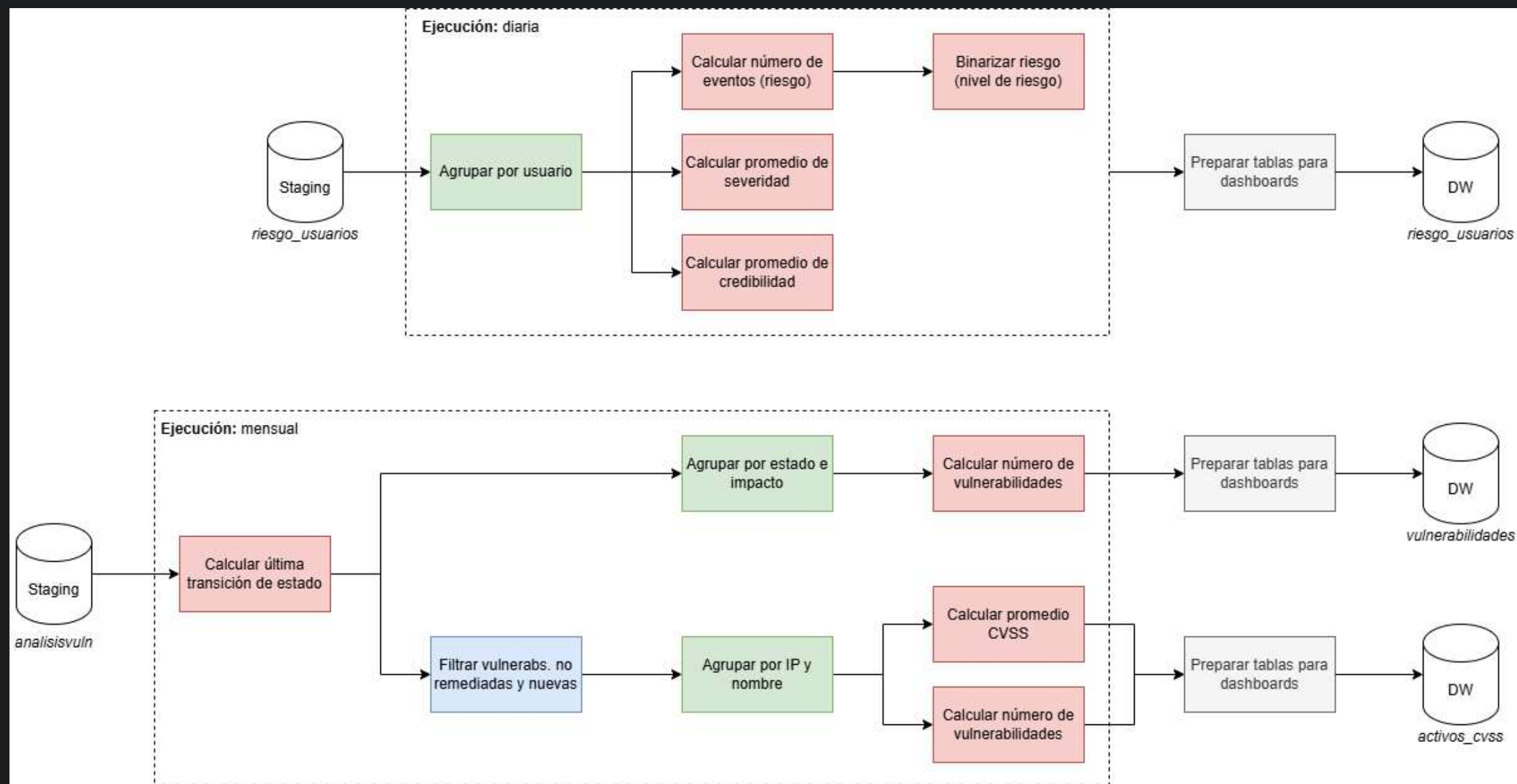
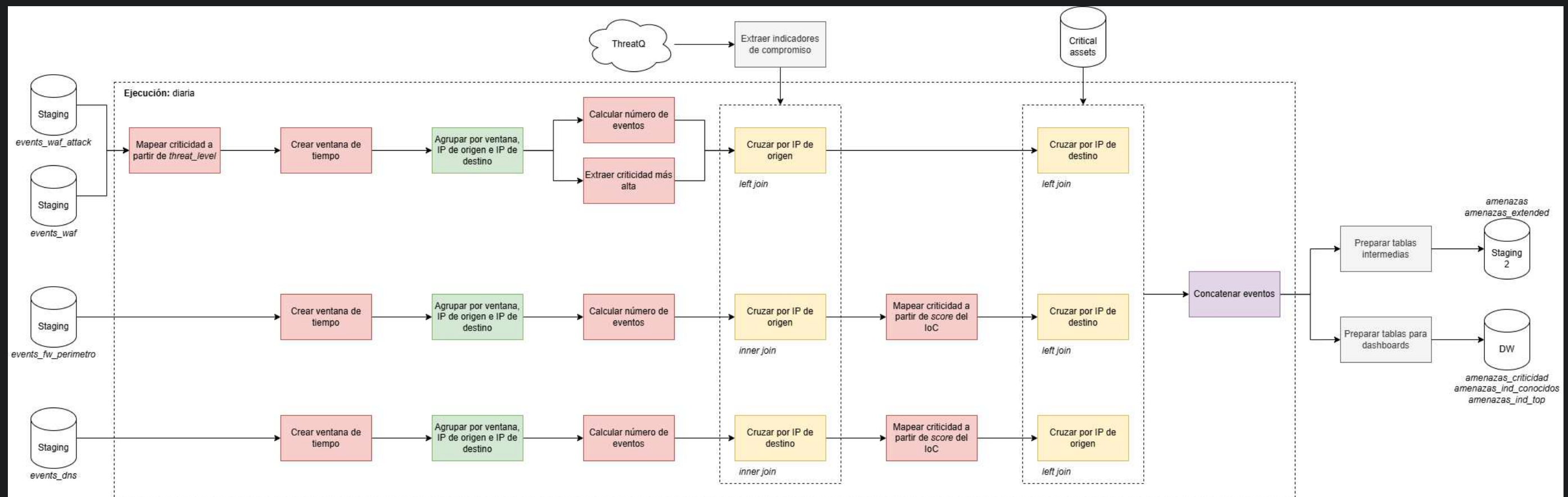
Actualizado mensualmente, modifica tablas que afectan tanto a los tableros como a otros ETLs.



ETL de Criticidad de Activos

Depende de la información de los ETLs 1 y 3, asignando una calificación actualizada a cada activo crítico.

Los bloques en rojo representan cálculos a nivel de registro, los verdes agrupaciones, los amarillos cruces de tablas, los azules filtros, los morados concatenación de tablas y los grises procesos complementarios.



MNEMO

Tablero de Estadísticas Generales

Visión General

Proporciona una visión general de las potenciales amenazas provenientes de diferentes tipos de dispositivos expuestos a internet como firewalls, WAF y DNS.

Análisis Temporal

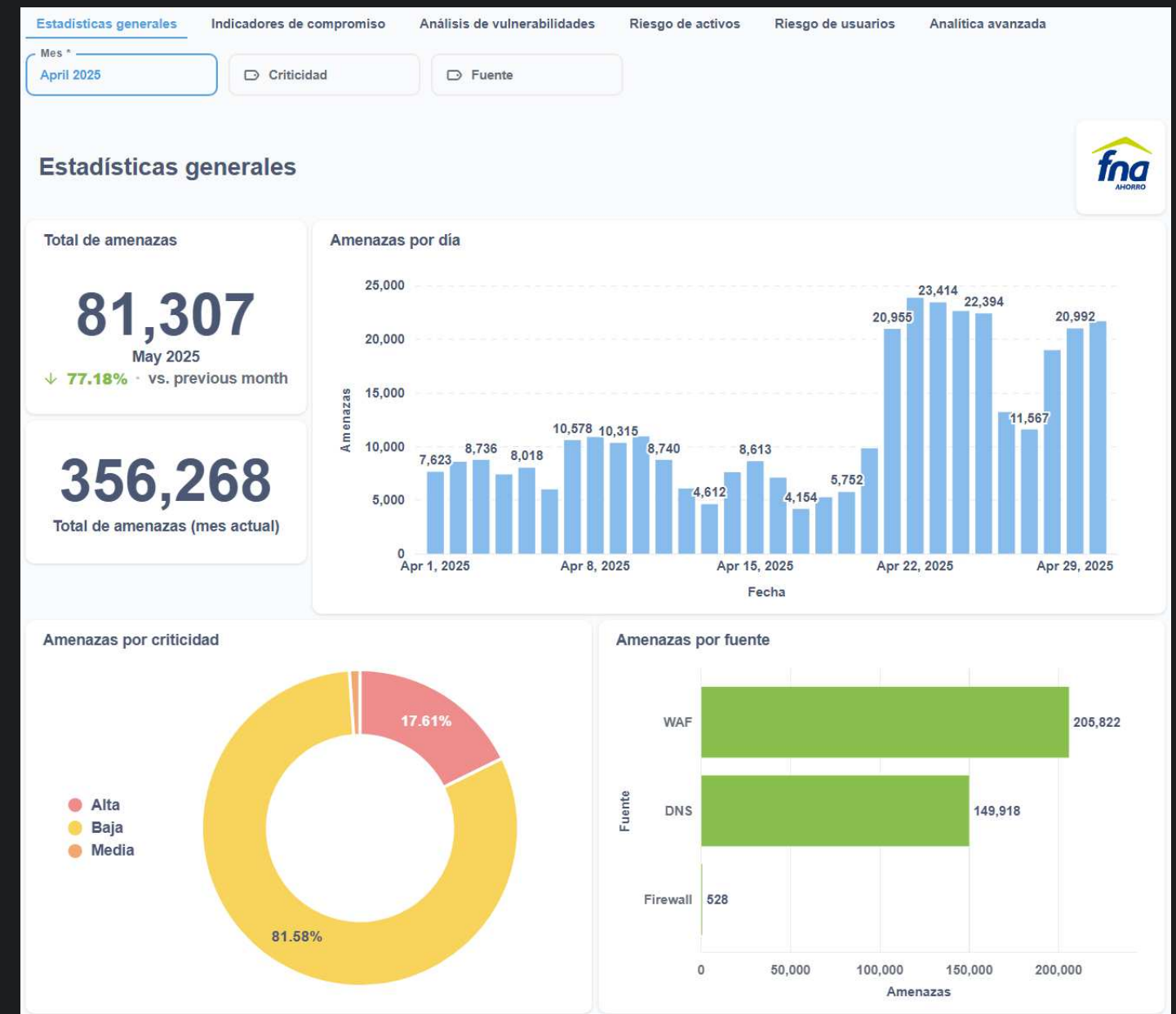
Visualiza el comportamiento cuantitativo de las amenazas a través del tiempo, su fuente y la criticidad (baja, media, alta) atribuida.

Información Agregada

Muestra el total de amenazas detectadas respecto al mes anterior, incluyendo su cambio a nivel porcentual.

Filtros Disponibles

Permite al usuario enfocar su análisis en un subgrupo de fuentes o criticidades mediante filtros específicos.



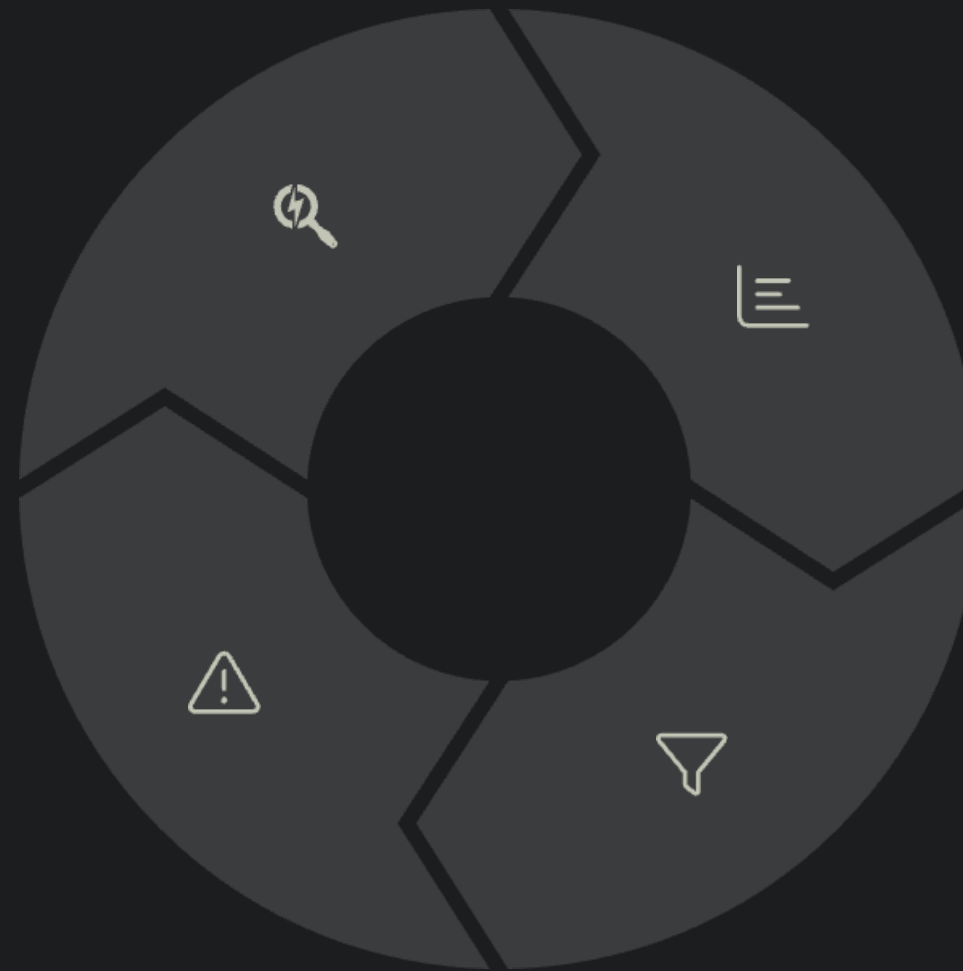
Tablero de Indicadores de Compromiso

Análisis de Amenazas

Del total de amenazas, cuántas provienen de indicadores de compromiso conocidos y desconocidos.

Calificación de Riesgo

Incluye la calificación de riesgo otorgada a cada indicador de compromiso, tomada directamente desde ThreatQ.

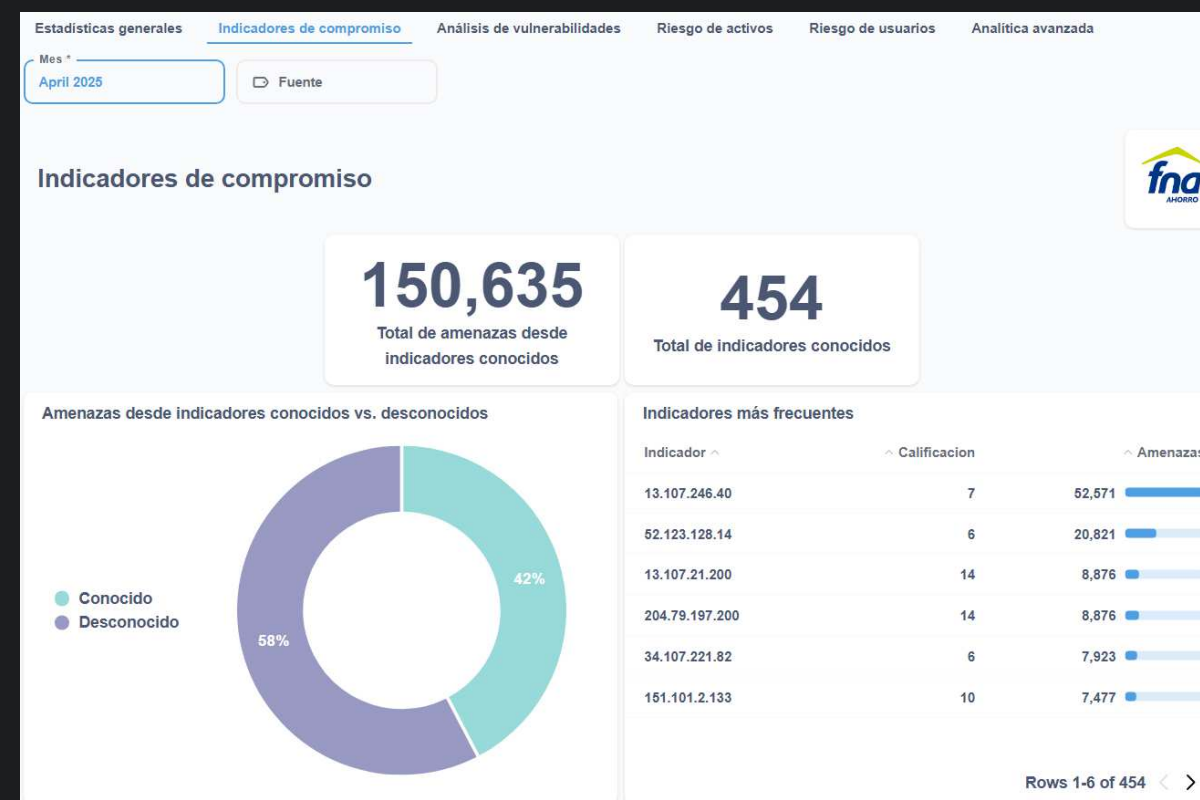


Frecuencia de Indicadores

Cuántos y cuáles son los indicadores de compromiso más frecuentes en la ventana de tiempo seleccionada.

Filtrado por Fuente

Los análisis pueden enfocarse a una fuente particular según las necesidades del usuario.



Tablero de Análisis de Vulnerabilidades

G+

Vulnerabilidad Nueva

Vulnerabilidades detectadas por primera vez en el análisis mensual.

!

Vulnerabilidad No Remediada

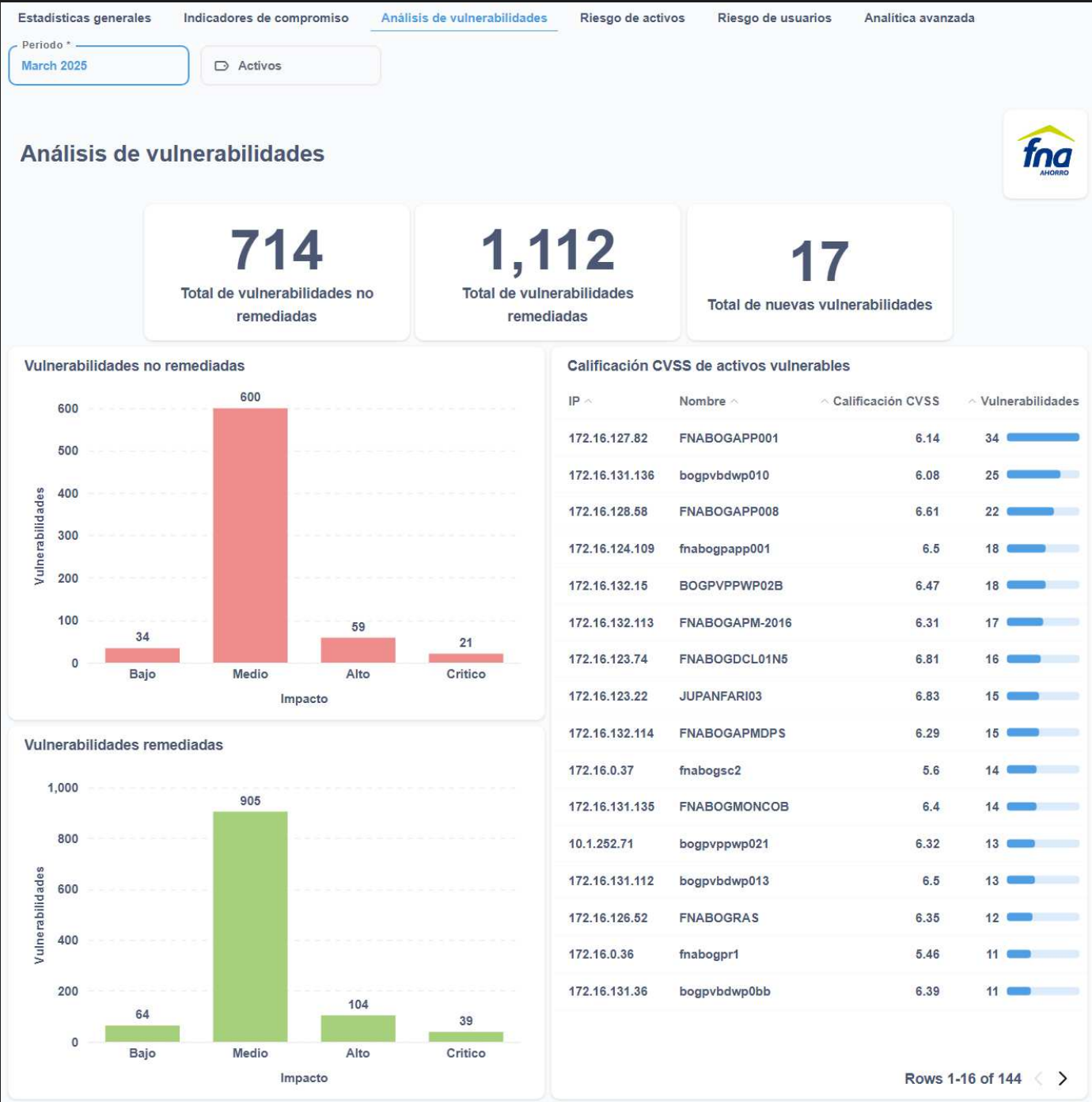
Vulnerabilidades que persisten desde análisis anteriores y aún no han sido solucionadas.

✓

Vulnerabilidad Remediada

Vulnerabilidades que han sido solucionadas y dejarán de considerarse en análisis futuros.

El tablero muestra la lista de activos críticos con vulnerabilidades abiertas, el promedio de la calificación CVSS otorgada a cada vulnerabilidad y el total de vulnerabilidades abiertas para el mes actual. El usuario puede localizar un activo por su IP y ver su detalle de calificación y vulnerabilidades.



Rows 1-16 of 144

Tablero de Riesgo de Activos



Calificación CVSS

Vulnerabilidades del mes anterior

2

Indicadores de Compromiso

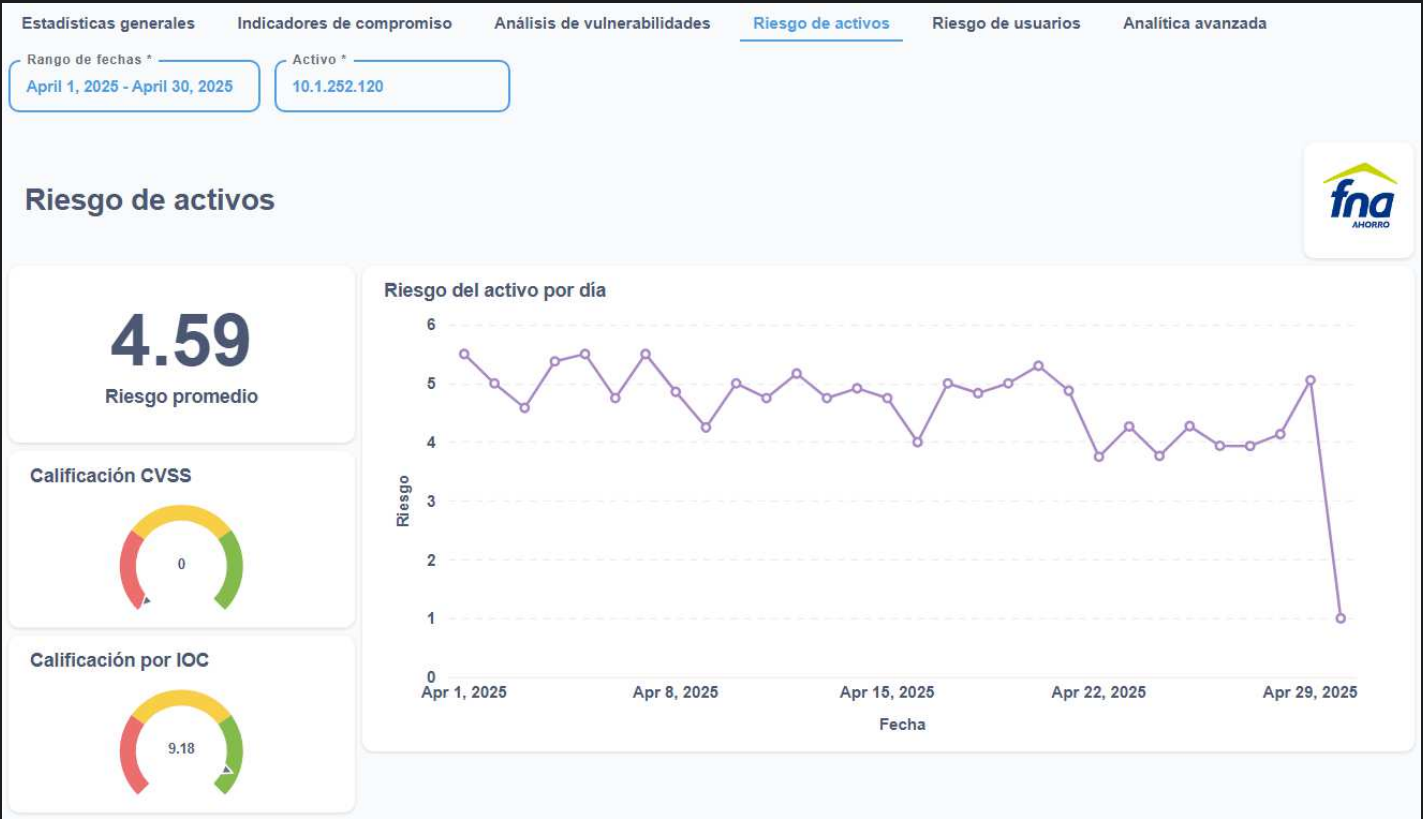
Promedio de calificaciones relacionadas al activo



Cálculo de Riesgo

Promedio de ambas calificaciones

El tablero se centra en un activo particular que puede ser localizado mediante su IP. Para mayor interpretabilidad, se muestran tanto el valor final de riesgo como los valores de calificación que lo componen. También se visualiza el riesgo promedio en el tiempo del mismo activo seleccionado.



Tablero de Riesgo de Usuarios

0-5

DNS

Escala de Riesgo

Rango en el que se califica el riesgo diario de cada usuario

Fuente Principal

Eventos analizados por plataforma intermedia

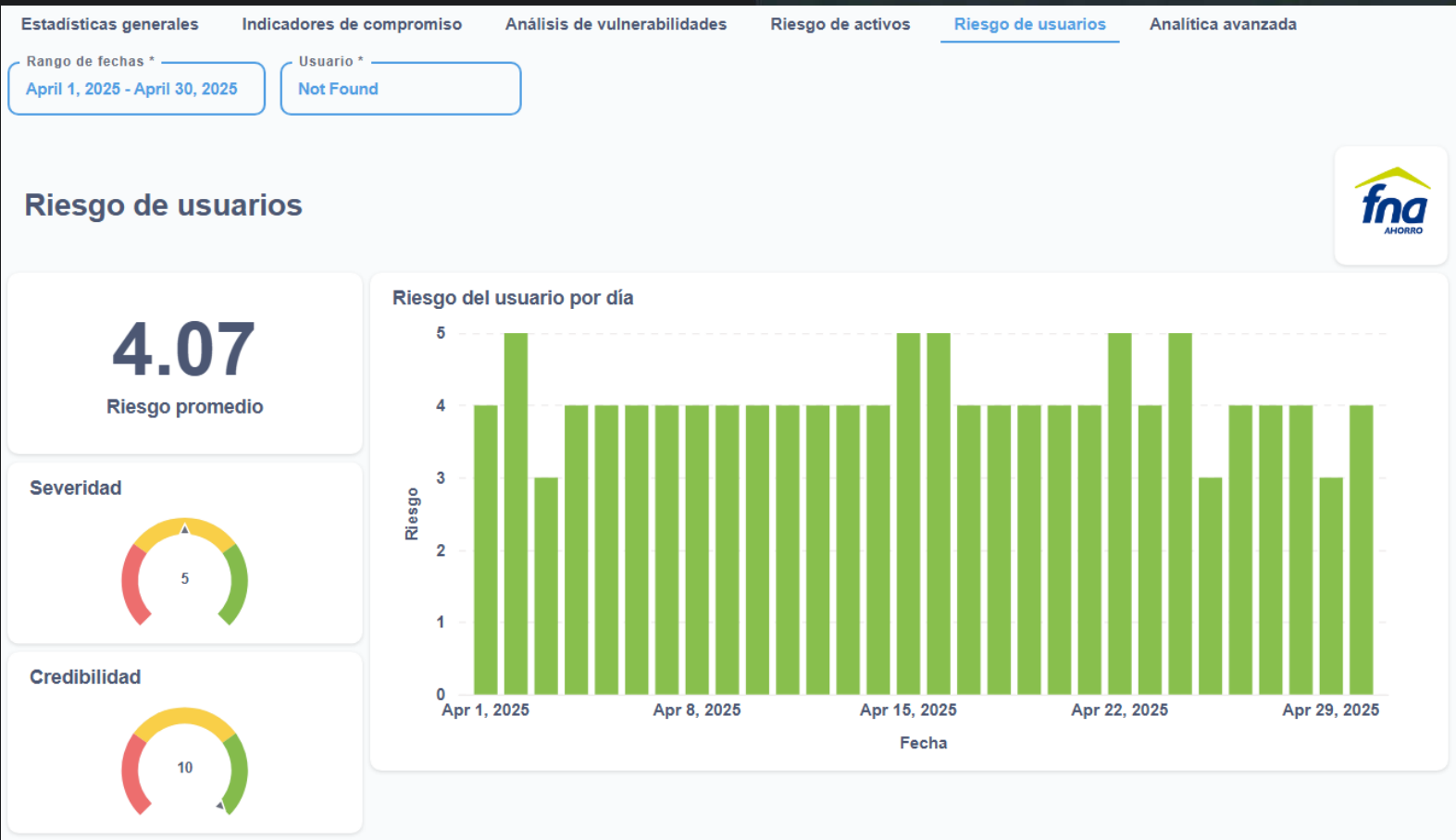
2

Métricas Adicionales

Severidad y credibilidad promedio de eventos

Similar al tablero de riesgo de activos, este tablero se centra en un usuario particular que puede ser localizado mediante su nombre único. El riesgo se calcula a partir de la frecuencia de eventos entregados por la plataforma intermedia, que también proporciona una severidad y credibilidad para cada evento.

MNEMO



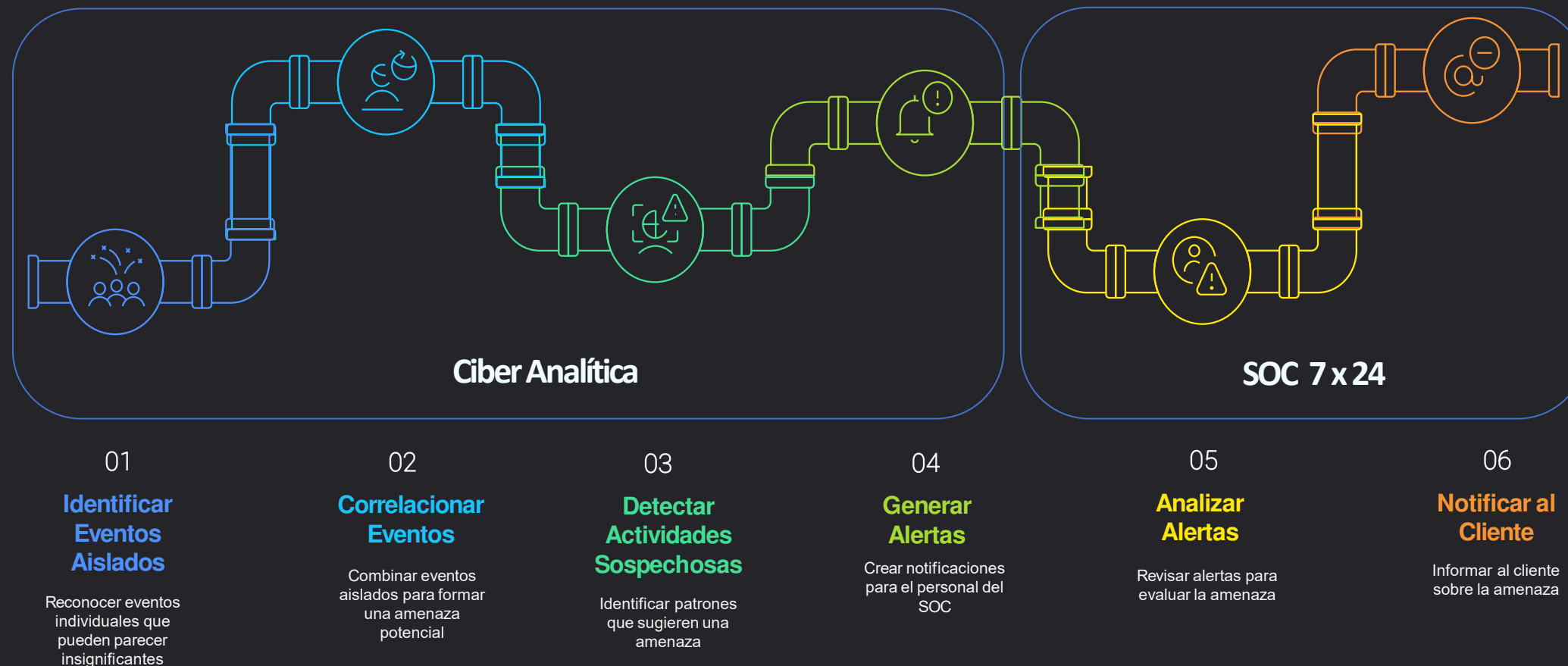
CASO DE SO 2

PATRONES DE ATAQUE

MN_EMO



Interoperabilidad Casos de Uso con el servicio SOC



El proceso de correlación avanzada se inicia con la identificación de eventos aislados, a menudo insignificantes por sí mismos, pero que en conjunto pueden representar una amenaza significativa. Esta capacidad permite a nuestro sistema de ciber analítica detectar actividades sospechosas seguidas de tareas administrativas en endpoints, generando alertas que el personal del SOC, operativo 24/7, puede analizar rápidamente.

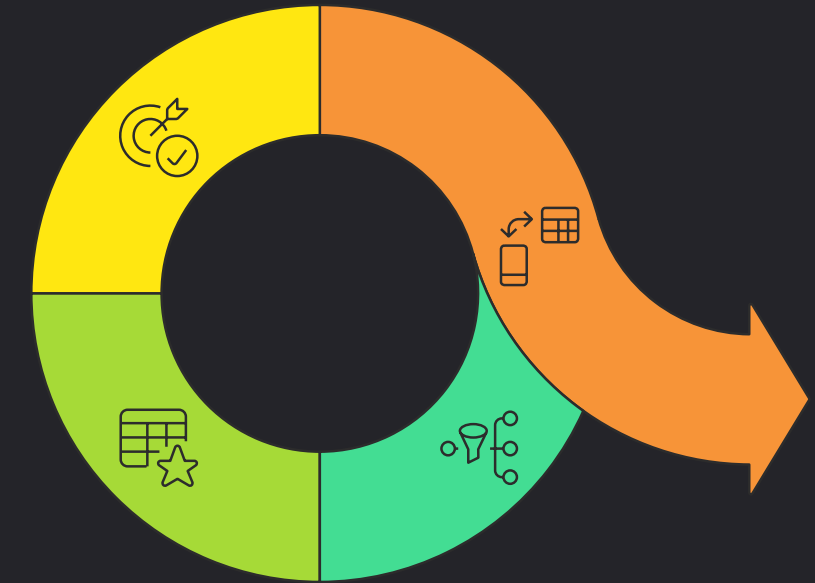
¡PATRONES DE ATAQUE

Múltiples indicadores de cadena de ataque se activan cuando un dispositivo exhibe comportamientos que indican una posible amenaza. Esto se observa frecuentemente en pruebas de penetración, pero también ocurre durante ataques reales.

Acción recomendada: Identifique los dispositivos de origen y su participación en la actividad para determinar si representa una amenaza real para la red. Si los ataques están autorizados, etiquete el dispositivo como "dispositivo de seguridad" para inhibir futuras alertas.

Este modelo se activará cuando se alcance una puntuación objetivo de 6 dentro de un período de 6000 segundos. La puntuación se compone de 17 componentes diferentes, cada uno con sus propios filtros específicos.

Ciclo de activación del modelo



1

Aplicar modelos

Aplicar modelos con filtros

2

Calcular puntuación

Calcular la puntuación total

3

Alcanzar puntuación objetivo

Verificar si se alcanza la puntuación objetivo

4

Activar modelo

Activar el modelo si se alcanza la puntuación

Componente 1: Attack and Recon Tools



Este componente se activa cuando se detectan herramientas de ataque y reconocimiento en la red. Para que se considere una amenaza, debe cumplir con cinco filtros específicos dentro de un período de 45 minutos.



Dirección solo saliente

El tráfico debe ser únicamente de salida desde la red interna.



Sin etiqueta de seguridad

La fuente interna no debe estar etiquetada como "Dispositivo de seguridad".



Sin etiqueta de puerta

La fuente interna no debe estar etiquetada como "Puerta".



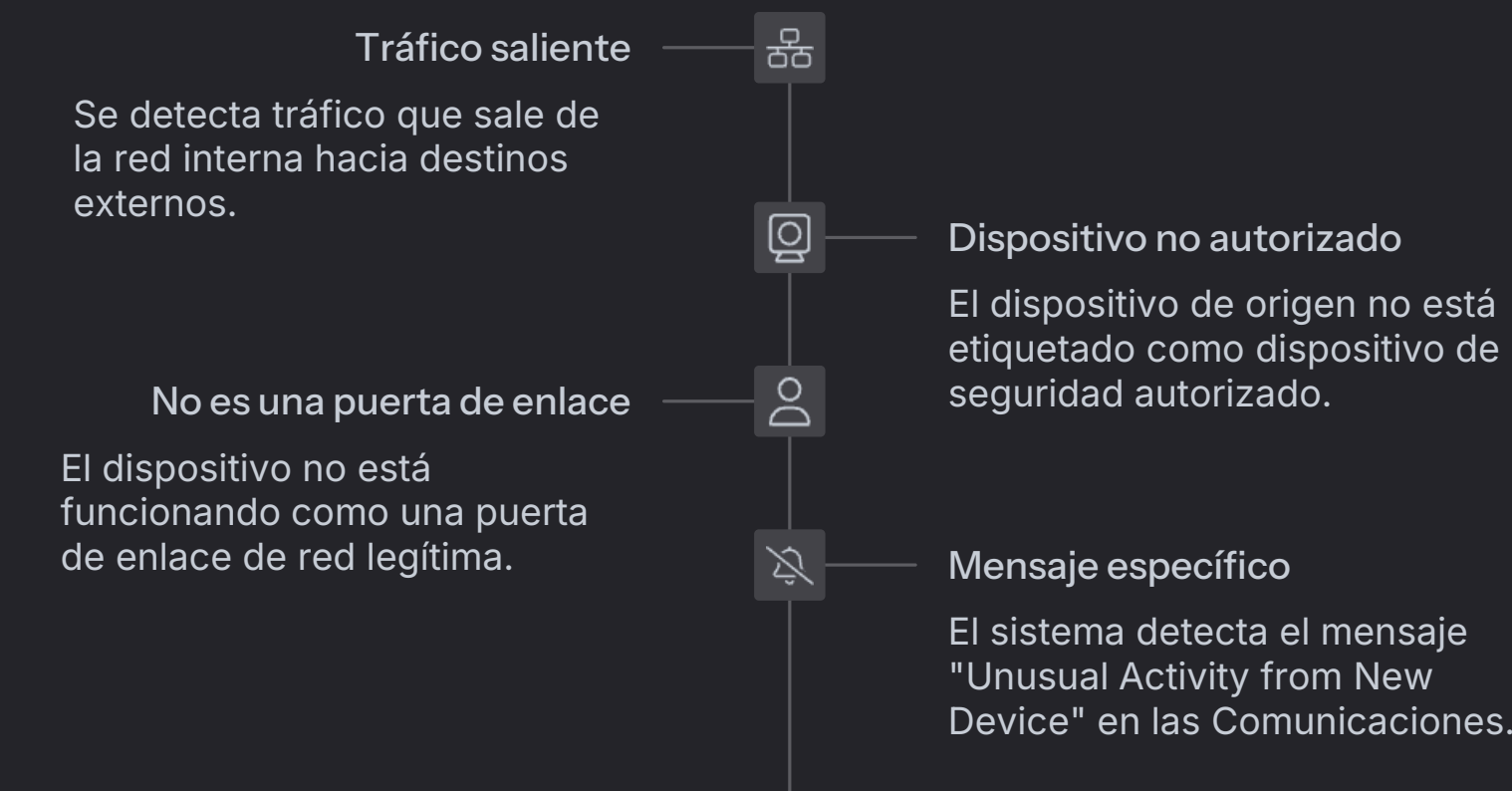
Sin etiqueta de apoderado

La fuente interna no debe estar etiquetada como "Apoderado".

El mensaje debe contener específicamente "Attack and Recon Tools" para que este componente contribuya a la puntuación objetivo.

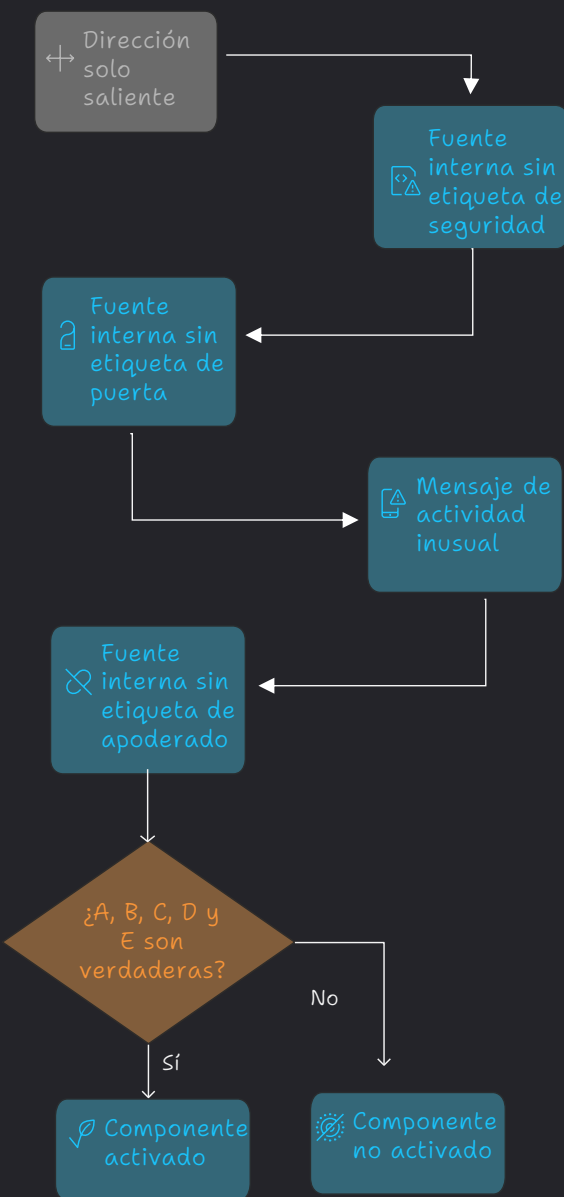
Componente 2: Unusual Activity from New Device

Este componente monitoriza actividades inusuales procedentes de dispositivos nuevos en la red. Para activarse, debe cumplir con cinco condiciones específicas en un período de 30 minutos.



Este componente es crucial para identificar nuevos dispositivos que podrían estar comprometidos o ser utilizados para actividades maliciosas en la red.

Proceso de Activación de Componente



Componente 3: AT Service

El tercer componente se centra en la detección del uso del servicio AT, una herramienta que puede ser utilizada legítimamente para programar tareas, pero también es frecuentemente explotada por atacantes para ejecutar comandos maliciosos.

Período de detección

Este componente debe detectarse dentro de un período de 20 minutos para contribuir a la puntuación objetivo del modelo de amenaza.

Condiciones de filtrado

Al igual que otros componentes, requiere que el tráfico sea saliente, que el dispositivo no esté etiquetado como de seguridad, puerta o apoderado.

Indicador específico

El mensaje debe contener específicamente "AT Service" para que este componente se active y contribuya a la puntuación general.

La detección del servicio AT puede indicar intentos de establecer persistencia en sistemas comprometidos o la ejecución de comandos programados como parte de un ataque más amplio.

Componente 4: New or Unusual Remote Command Execution

Este componente detecta la ejecución de comandos remotos inusuales o nuevos en la red. La ejecución remota de comandos es una técnica común utilizada por atacantes para controlar sistemas comprometidos y ejecutar código malicioso.



La detección temprana de ejecución de comandos remotos inusuales es crucial para identificar y detener ataques en sus etapas iniciales, antes de que el atacante pueda establecer un control completo sobre los sistemas comprometidos.

Componente 5: WinRM

El quinto componente se centra en la detección de actividades relacionadas con Windows Remote Management (WinRM), un servicio que permite la administración remota de sistemas Windows y que puede ser explotado por atacantes para movimiento lateral.



Servicio legítimo con riesgo

WinRM es un servicio legítimo que puede ser abusado



Ventana de detección

30 minutos para detectar actividad sospechosa



Filtros de seguridad

Requiere cumplir 5 condiciones específicas

WinRM permite a los administradores gestionar sistemas remotamente, pero también puede ser utilizado por atacantes para ejecutar comandos, transferir archivos y establecer persistencia en sistemas comprometidos. La detección de actividades inusuales relacionadas con WinRM puede indicar un intento de movimiento lateral dentro de la red.

Componente 6: Scan

Este componente detecta actividades de escaneo en la red, una fase crítica en la cadena de ataque donde los atacantes buscan sistemas vulnerables, puertos abiertos y servicios accesibles para planificar sus siguientes movimientos.



Reconocimiento activo

Detecta intentos de mapeo de la red y descubrimiento de activos vulnerables mediante técnicas de escaneo.



Ventana de 30 minutos

El componente monitoriza actividades de escaneo durante un período de 30 minutos para identificar patrones sospechosos.



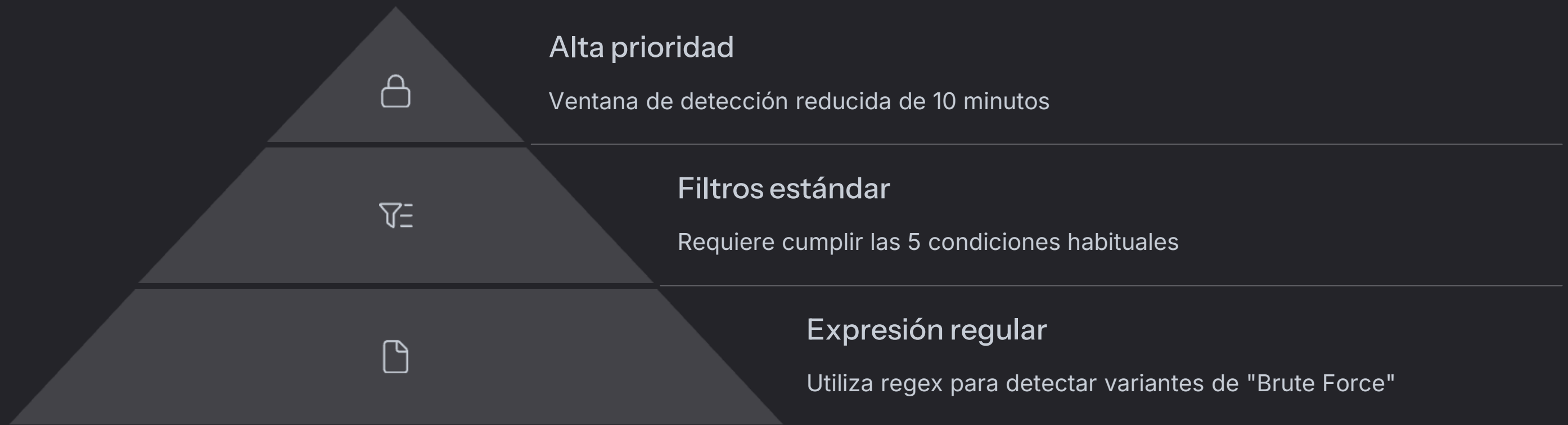
Filtros específicos

Requiere tráfico saliente y que el dispositivo no esté etiquetado como dispositivo de seguridad, puerta o apoderado.

Las actividades de escaneo son a menudo el primer indicador visible de un posible ataque, ya que los atacantes necesitan recopilar información sobre la red objetivo antes de intentar explotar vulnerabilidades específicas. La detección temprana de estos escaneos puede permitir a los equipos de seguridad implementar medidas defensivas antes de que ocurra un compromiso.

Componente 7: Brute Force

El séptimo componente se centra en la detección de ataques de fuerza bruta, donde los atacantes intentan acceder a sistemas mediante pruebas sistemáticas de múltiples combinaciones de credenciales hasta encontrar las correctas.



Los ataques de fuerza bruta son métodos comunes para comprometer cuentas y sistemas. Este componente utiliza una expresión regular específica (`/._Brute\[\\s-\]?Force._/i`) para detectar diferentes variantes de mensajes relacionados con ataques de fuerza bruta, permitiendo una identificación más precisa de estos intentos.

La detección temprana de estos ataques es crucial para proteger las credenciales y prevenir accesos no autorizados a sistemas críticos.

Componente 8: New or Uncommon Service Control

Este componente detecta la creación o modificación de servicios inusuales o poco comunes en los sistemas, una técnica frecuentemente utilizada por atacantes para establecer persistencia y garantizar que su malware se ejecute automáticamente.

5

Minutos

Ventana de tiempo muy reducida para
detección rápida

5

Filtros

Condiciones que deben cumplirse
simultáneamente

1

Mensaje específico

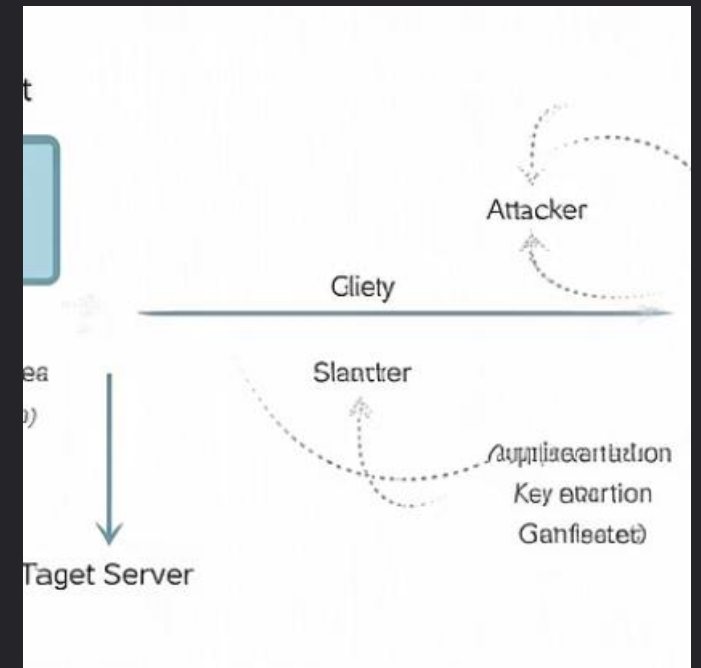
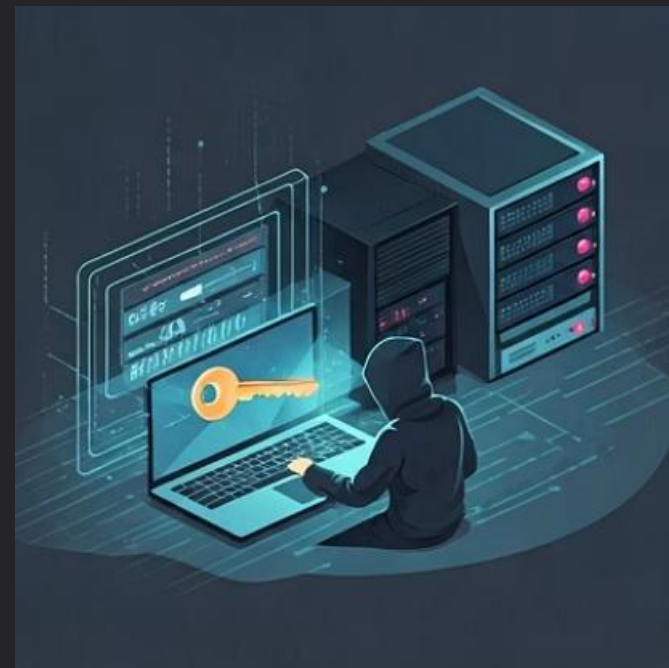
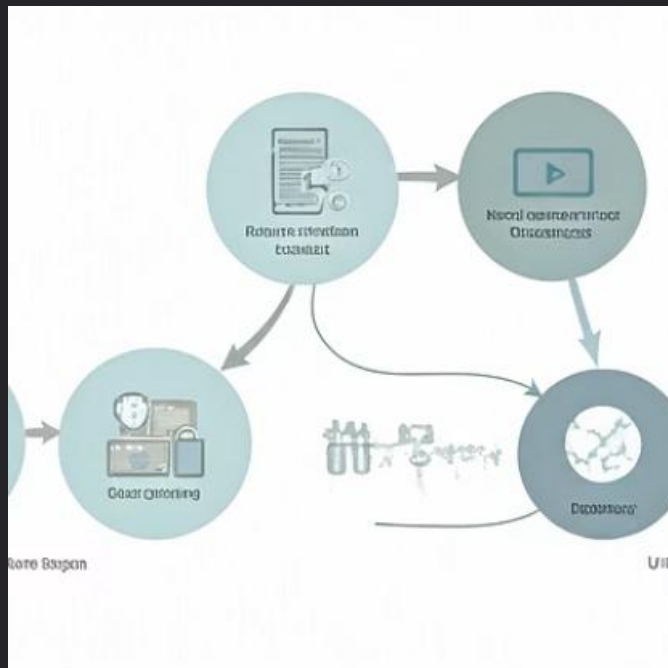
"New or Uncommon Service Control"
debe estar presente

La manipulación de servicios del sistema es una técnica de persistencia común utilizada por atacantes. Al crear o modificar servicios, pueden garantizar que su código malicioso se ejecute automáticamente cuando el sistema se inicia o en respuesta a eventos específicos.

La ventana de tiempo extremadamente corta de 5 minutos para este componente refleja la criticidad de detectar rápidamente estas modificaciones antes de que el atacante pueda establecer un control permanente sobre el sistema.

Componente 9: Kerberos Failures

El noveno componente monitoriza fallos en la autenticación Kerberos, que pueden indicar intentos de explotación de vulnerabilidades en este protocolo de autenticación, como ataques de Pass-the-Hash, Pass-the-Ticket o Kerberoasting.



Los fallos de Kerberos deben detectarse en un período de 10 minutos y cumplir con los cinco filtros estándar para contribuir a la puntuación objetivo. Estos fallos pueden ser indicativos de varios tipos de ataques avanzados contra la infraestructura de autenticación de Windows.

La detección temprana de estos patrones puede ayudar a identificar intentos de elevación de privilegios y movimiento lateral dentro de entornos Windows antes de que los atacantes obtengan acceso a recursos críticos.

Componente 10: Unusual Internal Connections

Este componente detecta conexiones internas inusuales que pueden indicar movimiento lateral dentro de la red. El movimiento lateral es una técnica utilizada por atacantes para expandir su acceso después de comprometer un sistema inicial.



Sistema comprometido

Punto de entrada inicial



Movimiento lateral

Expansión a otros sistemas



Objetivo de alto valor

Acceso a datos sensibles

Este componente tiene una ventana de detección de 30 minutos y requiere que se cumplan los cinco filtros estándar. El mensaje debe contener específicamente "Unusual Internal Connections" para que este componente contribuya a la puntuación objetivo.

Las conexiones internas inusuales pueden manifestarse como accesos a sistemas que normalmente no se comunican entre sí, conexiones en horarios atípicos, o patrones de tráfico anómalos que difieren del comportamiento normal de la red.

Componente 11: Tunnel

El undécimo componente se centra en la detección de túneles de comunicación, que son canales encubiertos utilizados por atacantes para exfiltrar datos o mantener comunicaciones persistentes con sistemas comprometidos, evadiendo los controles de seguridad.

Ventana de tiempo	60 minutos (la más larga)
Filtros requeridos	5 filtros estándar
Mensaje específico	"Tunnel" debe estar presente
Dirección del tráfico	Solo saliente
Exclusiones	No etiquetado como dispositivo de seguridad, puerta o apoderado

Los túneles pueden implementarse de diversas formas, como túneles DNS, HTTP, ICMP o mediante protocolos cifrados. Estos canales permiten a los atacantes mantener el control de los sistemas comprometidos y extraer información sensible sin ser detectados por los mecanismos de seguridad tradicionales.

La ventana de tiempo extendida de 60 minutos refleja la naturaleza a menudo intermitente o de bajo volumen de este tipo de tráfico, que puede requerir un período de observación más largo para su detección efectiva.

Componente 12: Reverse DNS Sweep

Este componente detecta barridos de DNS inverso, una técnica de reconocimiento utilizada por atacantes para mapear la red objetivo mediante la resolución de direcciones IP a nombres de host, revelando información sobre la estructura y nomenclatura de la red.



Patrones de consulta

Múltiples consultas DNS inversas desde una misma fuente en un corto período de tiempo pueden indicar un barrido sistemático de la red.

Los barridos de DNS inverso son una forma de reconocimiento pasivo que puede pasar desapercibida en muchas redes. La detección de estos patrones puede proporcionar una alerta temprana sobre actividades de reconocimiento que preceden a ataques más directos.



Maapeo de red

Los atacantes utilizan la información obtenida para crear un mapa detallado de la infraestructura objetivo, identificando servidores y servicios críticos.



Detección temprana

La ventana de detección de 10 minutos permite identificar rápidamente esta actividad de reconocimiento antes de que el atacante obtenga demasiada información.

Componente 13: New Admin Credentials on Client

El decimotercer componente detecta la aparición de nuevas credenciales administrativas en sistemas cliente, lo que puede indicar una escalada de privilegios o el uso de credenciales robadas para obtener acceso administrativo a sistemas comprometidos.

Compromiso inicial

El atacante obtiene acceso a un sistema con privilegios limitados mediante phishing, explotación de vulnerabilidades u otras técnicas.

Escalada de privilegios

Utiliza técnicas para obtener o crear credenciales administrativas, permitiéndole un control total sobre el sistema comprometido.

Expansión de acceso

Con privilegios administrativos, puede desactivar defensas, instalar malware persistente y acceder a recursos protegidos.

Este componente tiene una ventana de detección de 15 minutos y requiere que el mensaje contenga específicamente "New Admin Credentials on Client". Los filtros estándar también deben cumplirse para que este componente contribuya a la puntuación objetivo.

La aparición de nuevas credenciales administrativas, especialmente en sistemas cliente que normalmente no deberían tener usuarios con privilegios elevados, es un fuerte indicador de actividad maliciosa.

Componente 14: Unusual Internal Remote Desktop

Este componente detecta el uso inusual de conexiones de Escritorio Remoto dentro de la red interna, una técnica comúnmente utilizada por atacantes para el movimiento lateral y el control de sistemas comprometidos.

Dos variantes de detección

Este componente es único porque puede activarse por dos mensajes diferentes: "Unusual Internal Remote Desktop" o "Active Remote Desktop Tunnel". Ambos indican el uso potencialmente malicioso de servicios de escritorio remoto.

La ventana de detección es de 15 minutos, lo que permite una respuesta relativamente rápida a este tipo de actividad sospechosa.

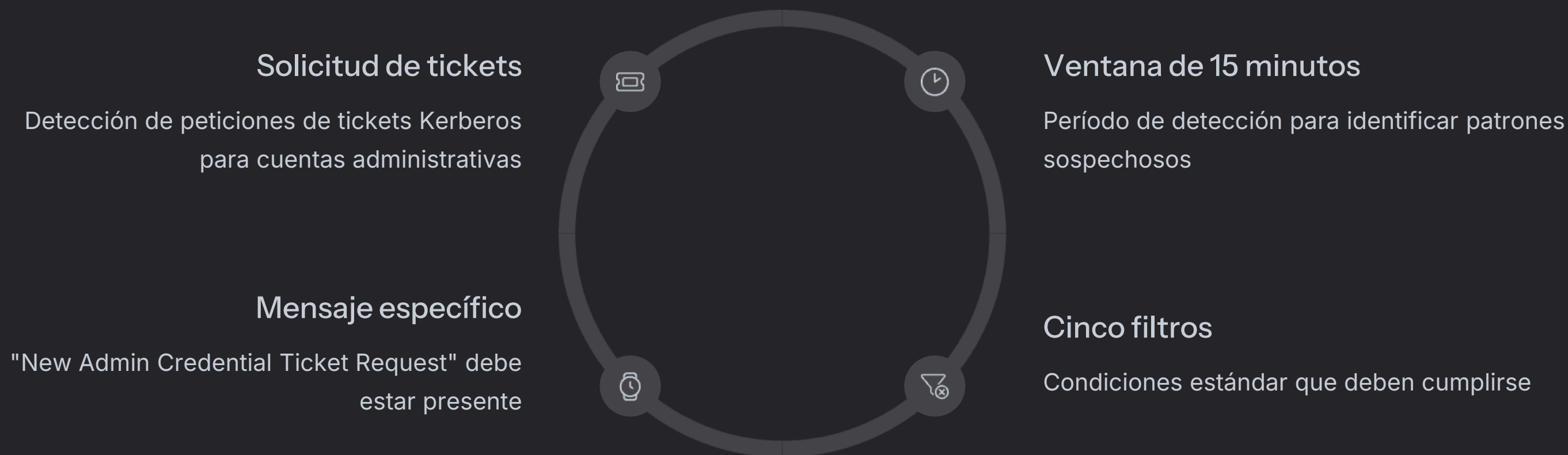
Este componente tiene seis filtros en lugar de los cinco estándar, añadiendo una capa adicional de especificidad para reducir los falsos positivos. La detección de estas actividades es crucial para identificar a atacantes que utilizan herramientas legítimas para fines maliciosos, una técnica conocida como "living off the land".



Las conexiones de Escritorio Remoto son legítimas en muchos entornos empresariales, pero su uso inusual o desde fuentes inesperadas puede indicar que un atacante está utilizando estas herramientas administrativas para moverse lateralmente dentro de la red.

Componente 15: New Admin Credential Ticket Request

El decimoquinto componente se centra en la detección de solicitudes de tickets de credenciales administrativas nuevas, lo que puede indicar intentos de obtener tickets Kerberos para cuentas privilegiadas mediante técnicas como Kerberoasting o Pass-the-Ticket.



Los tickets Kerberos son fundamentales para la autenticación en entornos Windows. Los atacantes pueden intentar obtener tickets para cuentas privilegiadas para elevar sus privilegios o acceder a recursos protegidos. La detección de solicitudes inusuales de tickets puede ayudar a identificar estos intentos antes de que se produzca un compromiso completo.

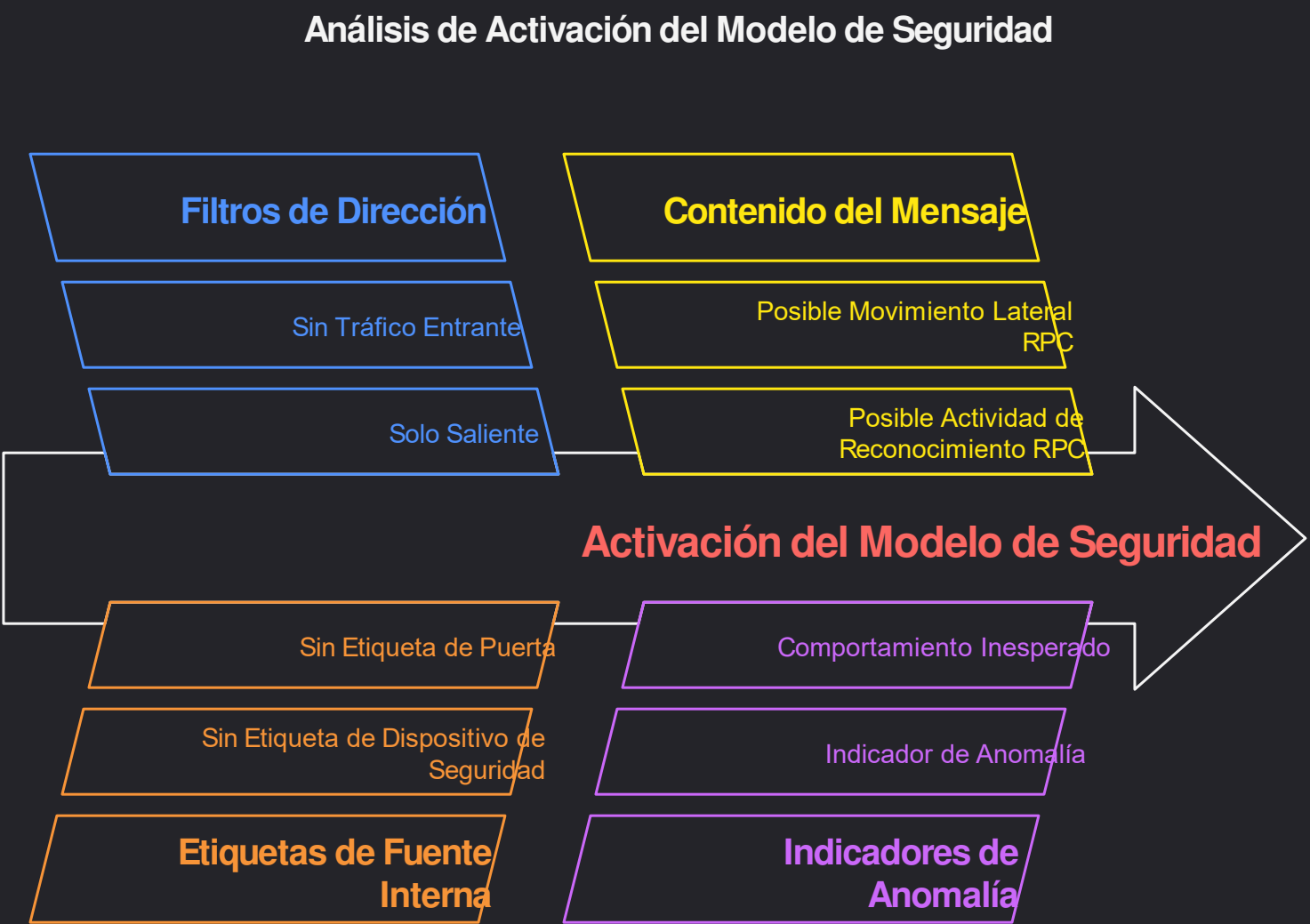
Componente 16: Possible RPC Lateral Movement

Este componente detecta posible movimiento lateral mediante llamadas a procedimiento remoto (RPC), una técnica avanzada utilizada por atacantes para ejecutar código en sistemas remotos y expandir su control dentro de la red comprometida.

Este componente es uno de los más complejos, con siete filtros en total y múltiples combinaciones de activación. Puede activarse si se detecta "Possible RPC Lateral Movement" o "Possible RPC Recon Activity", siempre junto con "Anomaly Indicator" y cumpliendo los filtros estándar.

La ventana de detección es de 60 minutos, lo que refleja la naturaleza a menudo intermitente o de bajo volumen de este tipo de actividad. Las llamadas RPC son legítimas en entornos Windows, pero su uso inusual o desde fuentes inesperadas puede indicar actividad maliciosa.

La detección de este tipo de movimiento lateral es crucial para identificar ataques avanzados que utilizan protocolos y servicios legítimos para evitar la detección.



Componente 17: Suspicious New User Agents

El último componente detecta agentes de usuario nuevos y sospechosos, que pueden indicar el uso de herramientas automatizadas, scripts personalizados o software malicioso para interactuar con sistemas y aplicaciones web.



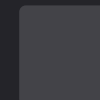
Identificación de herramientas

Los agentes de usuario revelan información sobre el software utilizado para conectarse a servicios web, permitiendo identificar herramientas inusuales o maliciosas.



Ventana de 15 minutos

Período de detección relativamente corto para identificar rápidamente estas anomalías en el tráfico web.



Filtros estándar

Requiere cumplir las cinco condiciones habituales para contribuir a la puntuación objetivo.

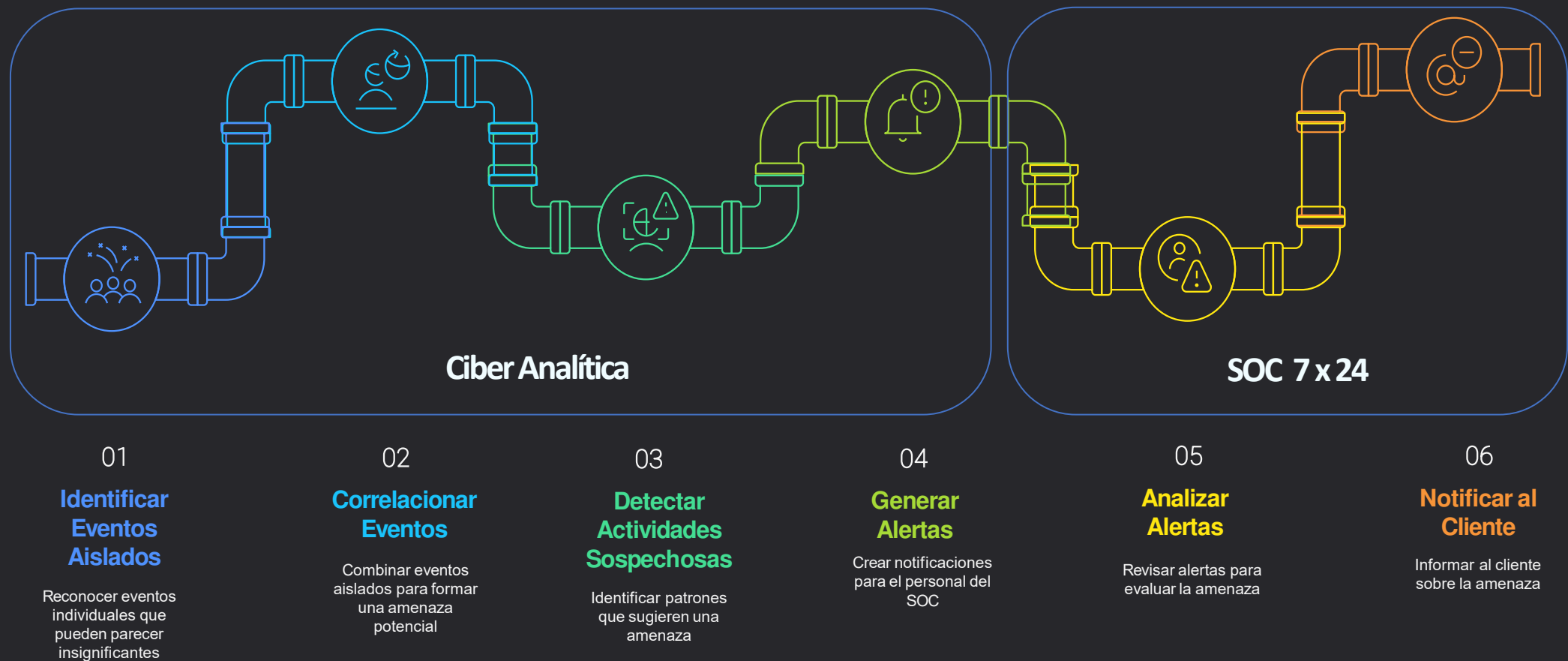
Los agentes de usuario son cadenas que identifican el navegador, sistema operativo u otra aplicación que se utiliza para acceder a un servicio web. Los atacantes a menudo utilizan agentes de usuario personalizados o inusuales cuando emplean herramientas automatizadas para escanear vulnerabilidades, realizar ataques de fuerza bruta o explotar vulnerabilidades web.

La detección de agentes de usuario sospechosos puede proporcionar una alerta temprana sobre actividades maliciosas dirigidas a aplicaciones y servicios web dentro de la organización.

CASO DE USO 3
MOVIMIENTOS
LATERALES

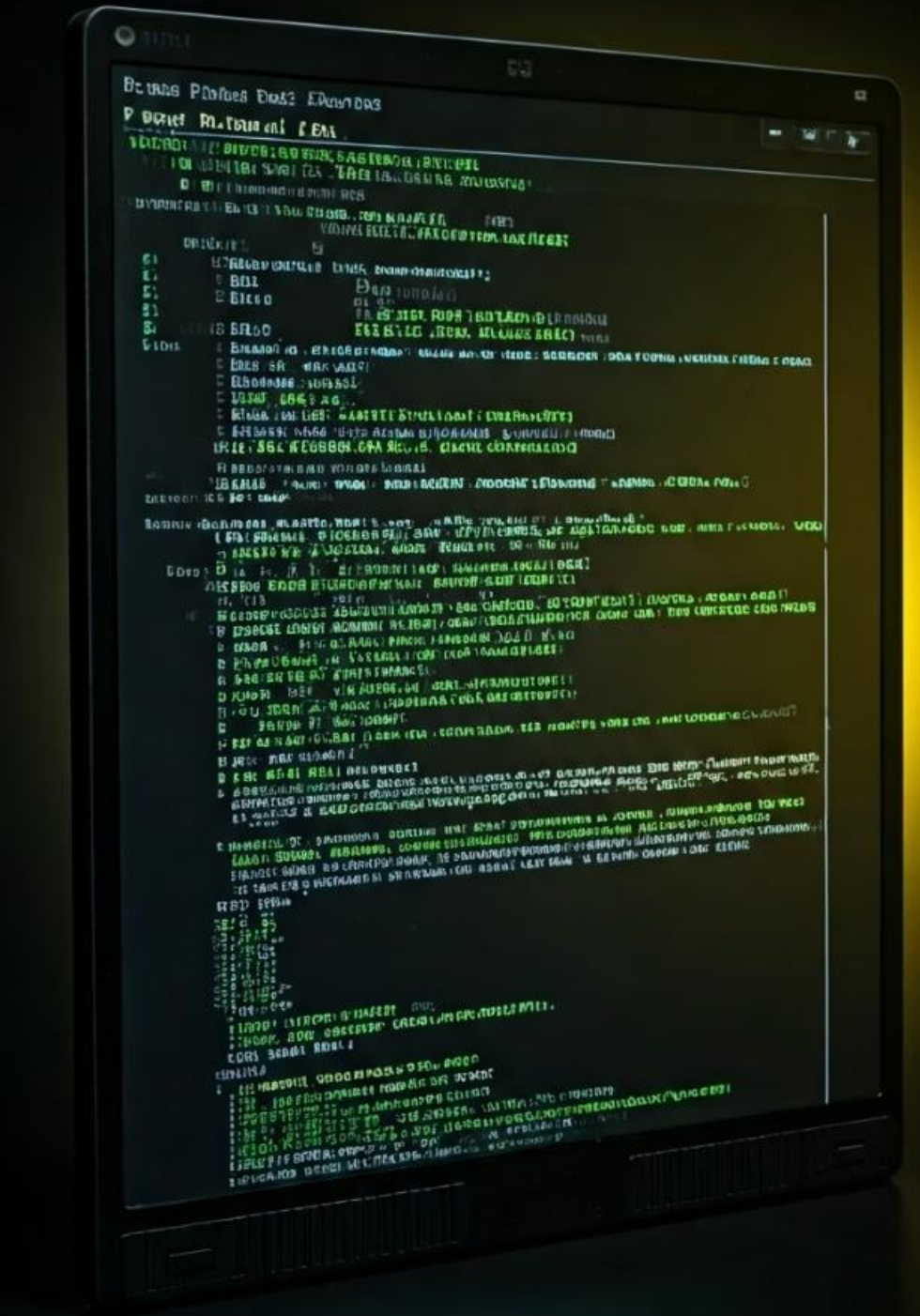
MN_EMO

Interoperabilidad Casos de Uso con el servicio SOC



El proceso de correlación avanzada se inicia con la identificación de eventos aislados, a menudo insignificantes por sí mismos, pero que en conjunto pueden representar una amenaza significativa. Esta capacidad permite a nuestro sistema de ciber analítica detectar actividades sospechosas seguidas de tareas administrativas en endpoints, generando alertas que el personal del SOC, operativo 24/7, puede analizar rápidamente.

Uso sospechoso interno de protocolo web





Uso Interno Sospechoso del Protocolo Web

Se busca detectar un patrón inusual en un dispositivo interno que establece conexiones nuevas o atípicas sobre HTTP y SSL/TLS inválidas hacia máquinas internas, acompañado de un volumen inesperado de tráfico interno.

Este comportamiento es característico de ataques internos drive-by que configuran receptores de comando y control (C2) en puertos HTTP no estándar o intentos de explotación de aplicaciones web alojadas.

Se recomienda investigar la actividad de los dispositivos de origen y destino para validar si esta conducta es legítima o maliciosa.



Descripción general

Un dispositivo estable conexiones HTTP nuevas o inusuales y conexiones SSL/TLS no válidas a una máquina interna, junto con un volumen inesperado de conexiones internas. Este patrón de actividad se ha observado en ataques drive-by internos donde se configura un receptor C2 en un puerto HTTP no estándar, o durante intentos de explotación contra aplicaciones web alojadas internamente. Acción: Investigue la actividad de los dispositivos de origen y destino y compruebe si esta actividad es la esperada por el dispositivo.

Condiciones de activación

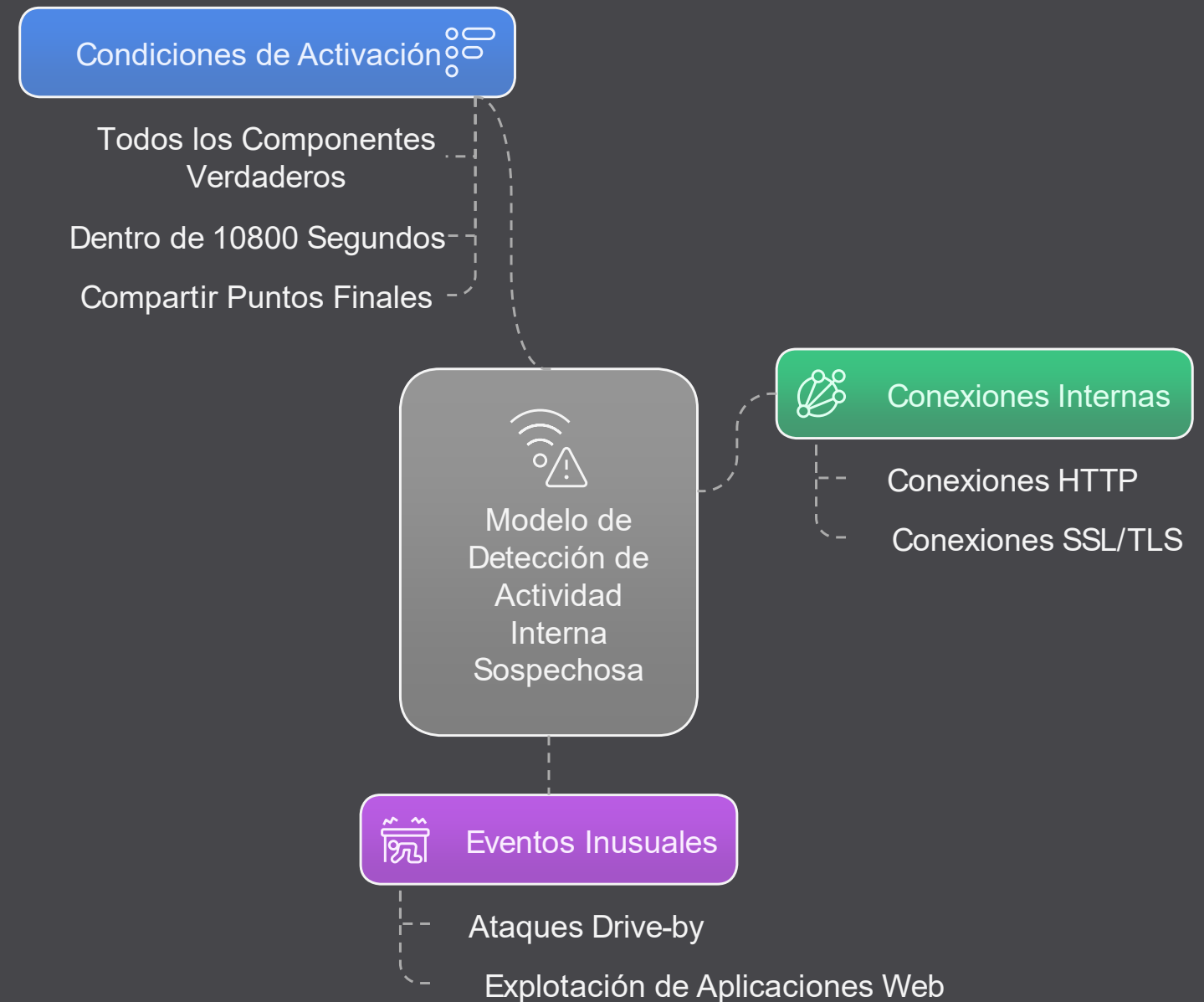
Este modelo se activará si: todos los componentes son verdaderos

Componentes que activaran este modelo:

1. Cualquier conexión interna (8 filtros)
2. Cualquier conexión interna (11 filtros)
3. Cualquier evento de actividad inusual (3 filtros)

Todos los componentes deben activarse dentro de esta cantidad de segundos 10800

Todos los componentes deben compartir puntos finales (endpoints)



Proceso de Activación de Conexión Interna



Componente 1: Conexiones Internas con Filtros Específicos

Filtros esenciales

- Conexión solo saliente
- Puerto destino 443
- Protocolo no es SSL ni Desconocido
- No es conexión a través de proxy

Protocolos y puertos

- Protocolo TCP
- Protocolo de aplicación no HTTPS
- Puerto origen distinto de 18000

La activación se da solo cuando todos estos filtros coinciden simultáneamente en un lapso máximo de 60 minutos.

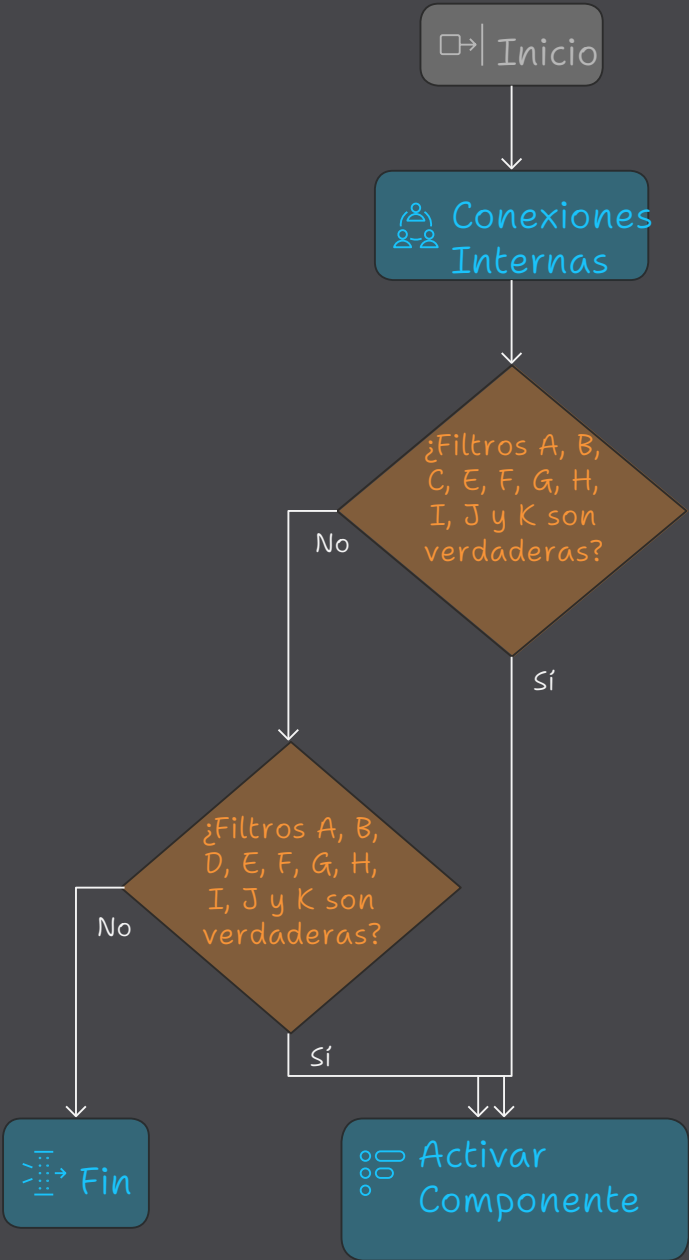
Esta combinación ayuda a identificar conexiones internas con tráfico cifrado aparente pero sin usar protocolos esperados, lo que puede indicar tráfico malicioso encubierto.

Componente 2: Conexiones Internas Filtros Detallados

- Características de la conexión
Conexiones internas salientes, nuevas, con protocolo HTTP, y tamaño de datos significativos en subida y bajada.
- Condiciones específicas
Agentes de usuario que no corresponden a software legítimo comúnmente usado (por ejemplo, no coincide con agentes internos).
- Etiquetas de seguridad
Ni el dispositivo origen ni destino poseen etiquetas de dispositivo de seguridad, sugiriendo dispositivos no gestionados.
- Filtros adicionales
URL no corresponde a patrones predefinidos y puerto origen es diferente de 18000.

Estos filtros permiten aislar actividades internas anómalas que potencian la detección de tráfico no autorizado o mal configurado en la red.

Filtro	Descripción
[A] A	Dirección solo saliente
[B] B	El protocolo de aplicación es HTTP
[C] C	Nueva conexión
[D] D	Conectividad inusual > 80
[E] E	Tamaño individual de bajada > 0
[F] F	Tamaño individual de subida > 0
[Ga] G	No coincide con la expresión regular del agente de usuario
[H] H	El destino interno carece de etiqueta de seguridad
[Ii] I	La fuente interna carece de etiqueta de seguridad
[Js] J	No coincide con la expresión regular de la URL
	Puerto de origen != 18000



Componente 3: Eventos de Actividad Inusual Relevantes

Métricas detectadas

Actividad anómala comprobada a través de métricas específicas, enfocadas en conexiones internas.

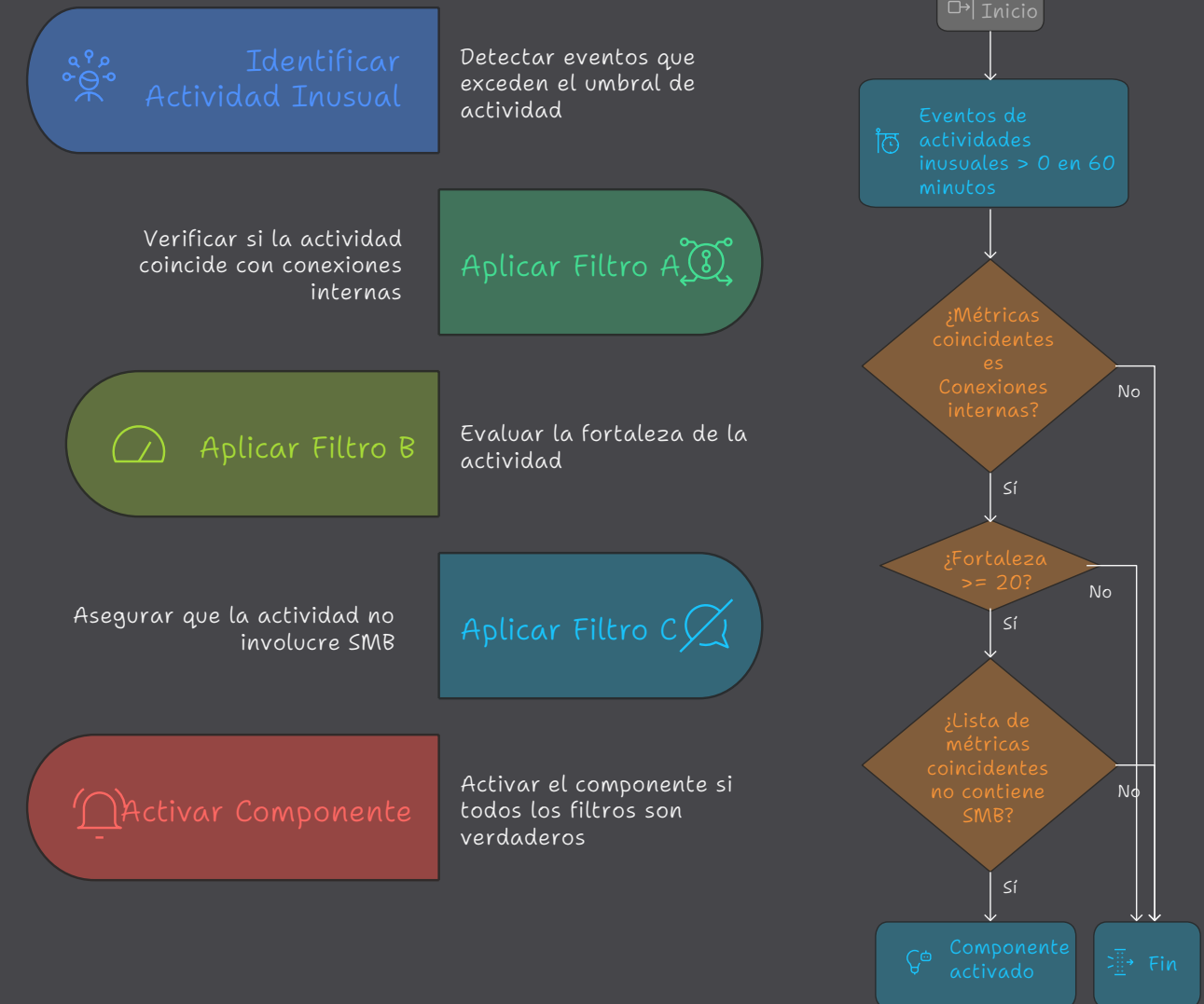
- Eventos de conexiones internas mayores que cero en 60 minutos
- Fortaleza mínima de 20 para considerarse relevante
- Exclusión de tráfico SMB para evitar falsos positivos

Importancia para análisis

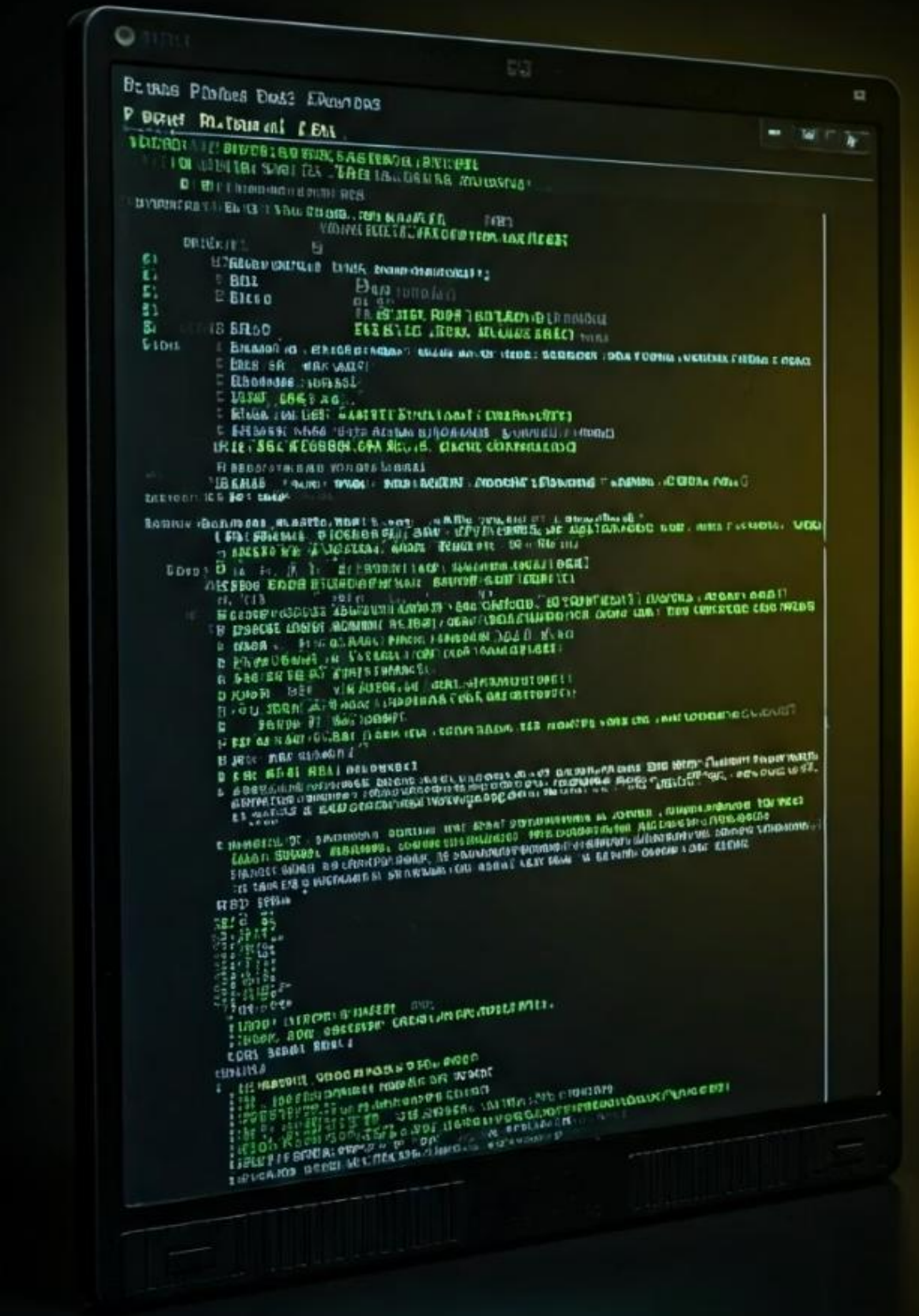
La fuerte correlación entre estas métricas permite priorizar alertas con mayor probabilidad de representar amenazas reales, facilitando investigaciones eficientes.

Se recomienda integrar estos indicadores con los otros componentes para una detección robusta de intrusiones internas.

Secuencia de Detección de Actividad Inusual



PsExec entrante y descarga de scripts





Detección de PsExec Entrante y Descarga de Scripts Sospechosos

El uso de PsExec, una herramienta legítima para administración remota vía SMB, puede ser aprovechado por atacantes para movimientos laterales en redes corporativas. Recientemente, se identificó un dispositivo que descargó un archivo de script sospechoso en una sesión controlada mediante PsExec, lo que podría indicar una amenaza activa.

Este modelo de detección se activa cuando se cumplen estrictas condiciones relacionadas con tráfico SMB y conexiones externas, permitiendo un monitoreo preciso para prevenir accesos no autorizados y actividad maliciosa.



Proceso de Detección de Actividad Sospechosa



Identificar Actividad SMB

Detectar cualquier actividad relacionada con SMB en la red.



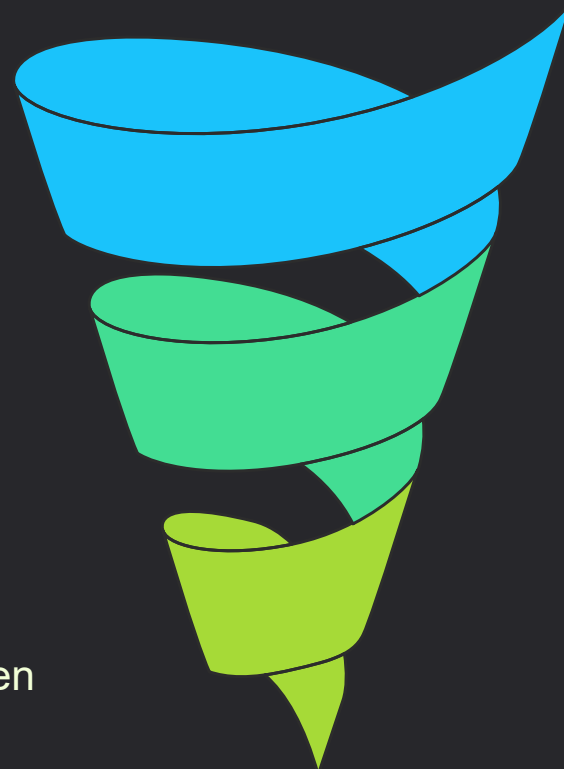
Detectar Conexiones Externas

Identificar cualquier conexión externa iniciada por el dispositivo.



Verificar Secuencia de Eventos

Asegurar que los eventos ocurran en el orden correcto y dentro de un plazo de 3600 segundos.



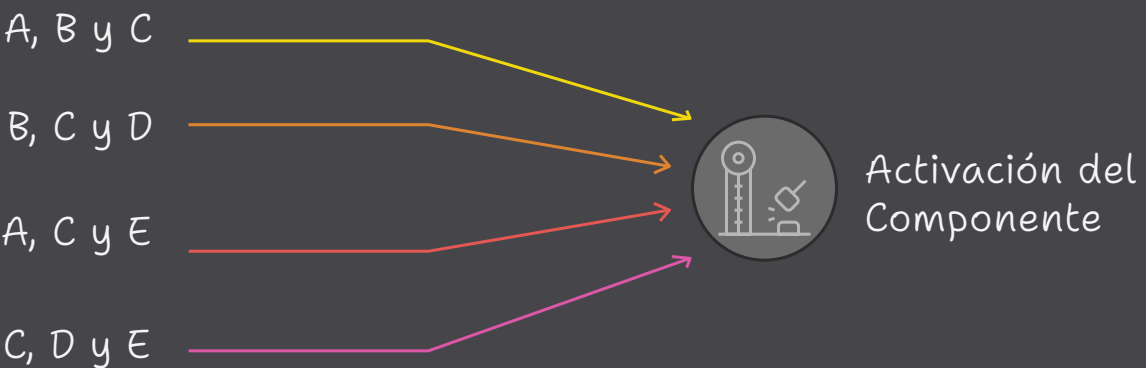
PsExec y Descarga de Scripts Sospechosos

El uso de PsExec, una herramienta legítima para administración remota vía SMB, puede ser aprovechado por atacantes para movimientos laterales en redes corporativas. Recientemente, se identificó un dispositivo que descargó un archivo de script sospechoso en una sesión controlada mediante PsExec, lo que podría indicar una amenaza activa.

Indicadores de Actividad Sospechosa



Convergencia de Condiciones



Componentes y Condiciones de Activación: Tráfico SMB Anómalo

Filtros para SMB

- Mensajes que contienen "psexesvc" o referencian nuevo uso de PyMEs
- Conexiones entrantes únicas según dirección
- Detección de patrones específicos mediante expresiones regulares
- Alto uso inusual de SMB > 50 en 5 minutos

Condiciones de Activación

Este componente se activa cuando combinaciones específicas de filtros se cumplen simultáneamente, como A+B+C o C+D+E, entre otras. Así se asegura que la alerta se active sólo ante anomalías concretas y no falsos positivos.

Componentes y Condiciones de Activación: Conexiones Externas Sospechosas

1

Filtros para conexiones externas

- Puntos finales externos raros detectados > 95
- URL que coinciden con expresiones regulares de comandos maliciosos
- Direcciones solo salientes exclusivas
- Puertos que no son estándar para correo (diferentes de 25)
- Edad del destino < 4 días
- Nombre de host no confiable

2

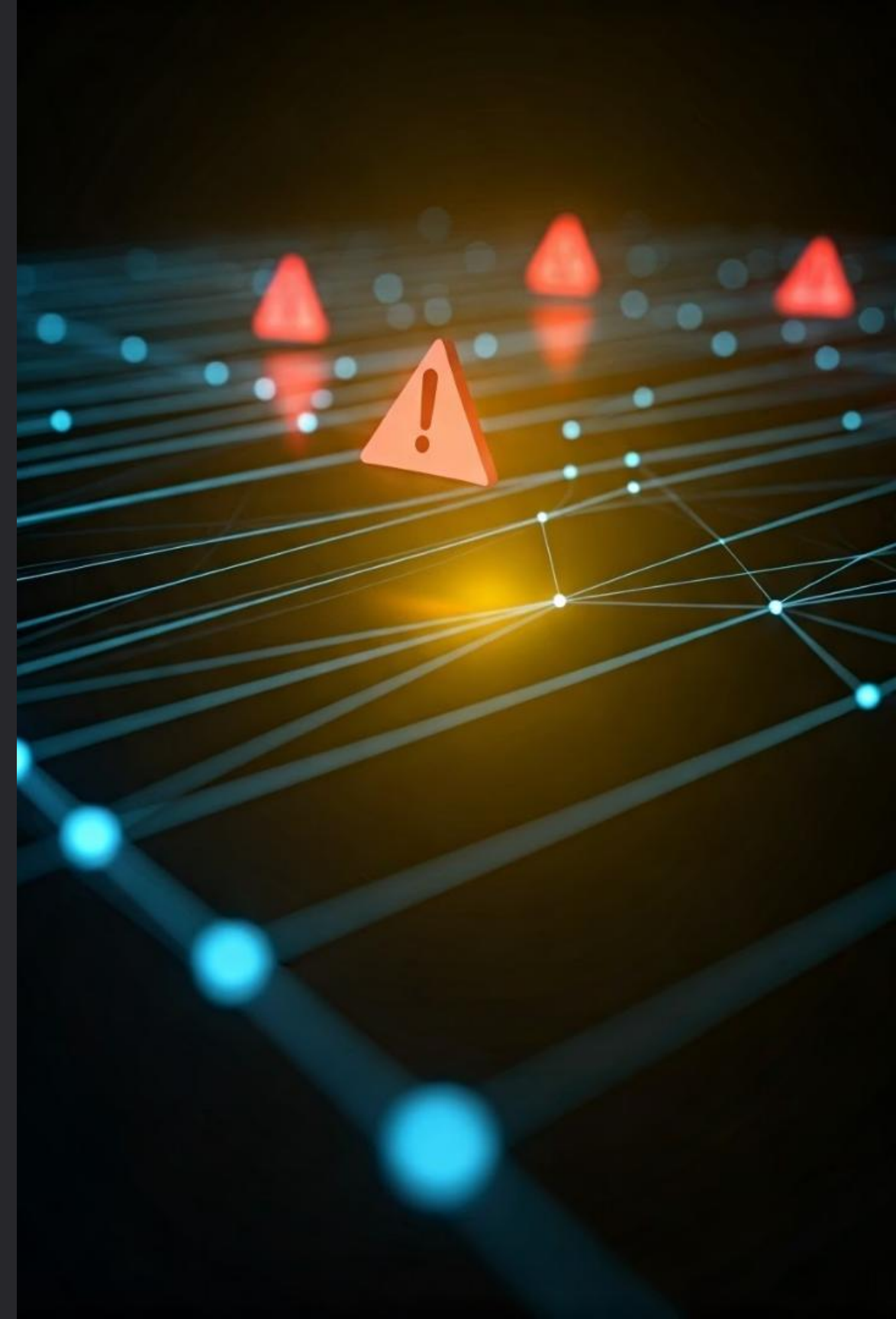
Activación del componente

El modelo exige que todas las condiciones A, B, C, D, E y F sean verdaderas para activar esta alerta, garantizando que la detección sea específica a comportamientos externos inusuales y potencialmente maliciosos.

Análisis de Actividades Sospechosas con PSEXec



Detección de Movimiento Lateral y Actividad C2



Detección de Movimiento Lateral y Actividad C2

El movimiento lateral y la actividad C2 (Command and Control) son indicadores de posibles vulnerabilidades activas en dispositivos conectados a la red. Cuando se detecta una secuencia de este tipo, es fundamental revisar las alertas del modelo relacionado para determinar si este comportamiento es esperado.

Es importante examinar también cualquier conexión a endpoints externos poco comunes, ya que estos pueden ser señales de actividad sospechosa que requiere atención inmediata. La detección temprana de estos patrones es crucial para prevenir compromisos de seguridad más graves.



Condiciones de Activación del Modelo



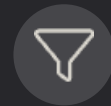
Puntuación Objetivo

Se requiere alcanzar una puntuación objetivo de 5 dentro de un período de 129.600 segundos (36 horas).



Activación

El modelo se activará cuando se alcance la puntuación objetivo mediante la combinación de los componentes mencionados.



Componentes Contribuyentes

Cuatro componentes principales con múltiples filtros: Modelo más de 2 en 24 horas (11 filtros), Modelo más de 1 en 1 hora (13 filtros), Cualquier modelo (11 filtros), y Modelo más de 1 en 24 horas (12 filtros).

Proceso de Activación de Componentes



Coincidencia de Expresión Regular

Los mensajes coinciden con patrones predefinidos



Contenido de Mensaje

Los mensajes contienen palabras clave específicas



Incidencia de Modelo

Los mensajes alcanzan un umbral de incidencia



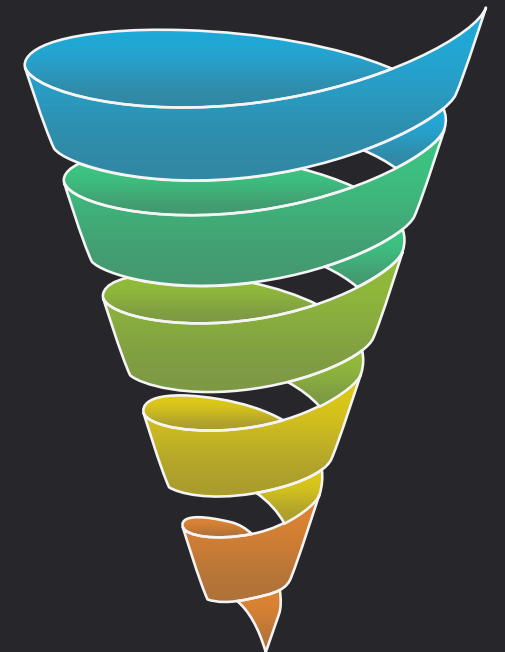
Etiquetado de Fuente

Las fuentes internas están etiquetadas

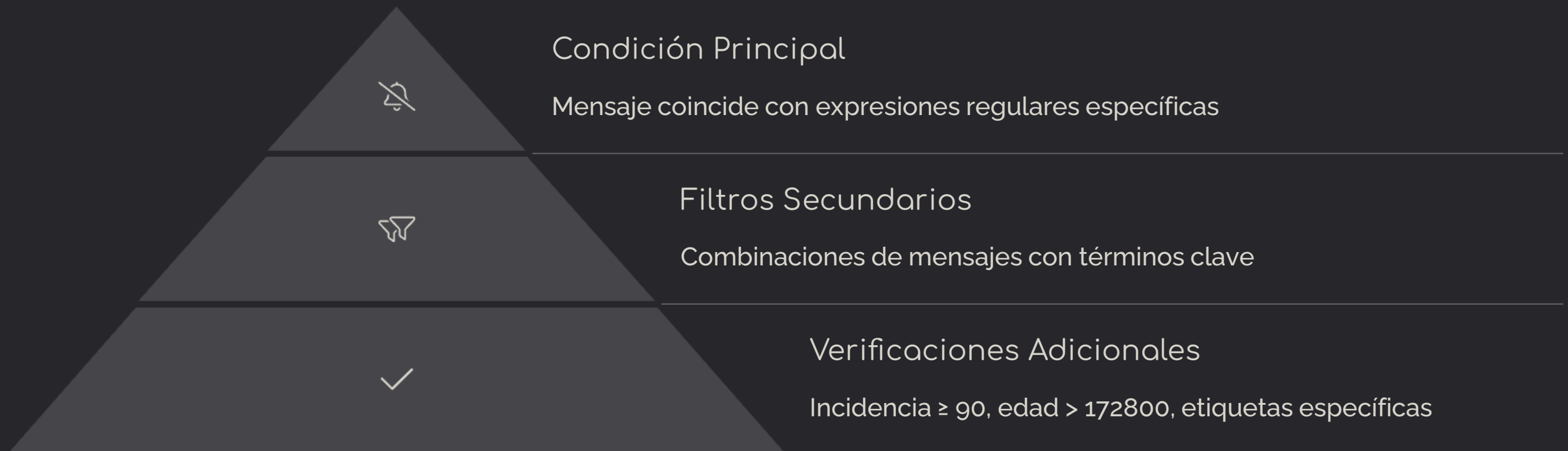


Edad de la Fuente

Las fuentes cumplen con un criterio de edad



Componente: Modelo más de 2 en 24 horas



Este componente utiliza 11 filtros diferentes (A-K) y se activará cuando se cumplan combinaciones específicas de estos filtros. Por ejemplo, cuando A, B, G, H e I son verdaderos simultáneamente, o cuando A, C, G, H e I son verdaderos, entre otras combinaciones posibles.

Los filtros incluyen coincidencias con expresiones regulares, presencia de términos como "Rare external", "New Endpoint", "Beacon", y verificaciones sobre la edad de la fuente y etiquetas específicas.

- Coincidencia con expresiones regulares específicas
- Ausencia de "Activity Identifier" y "Anomaly Indicator"
- Presencia de términos como "SMB", "RPC", "Brute Force"

- Mensajes sobre "Compromise / Ransomware"
- Mensajes sobre "Anomalous File / Internal"
- Coincidencia con expresiones de alta prioridad

- Incidencia nueva o poco común ≥ 90
- Fuente sin etiqueta "Agentes de usuario en conflicto"
- Edad de la fuente > 172800
- Fuente sin etiqueta "Dispositivo"

Community Monitoring

01:00	13:00	05:00	22:00	02:00
Enchiladas	100g	Enchiladas	100g	Enchiladas
Banana con queso	100g	Banana con queso	100g	Banana con queso
Don't know	0	Don't know	0	Don't know

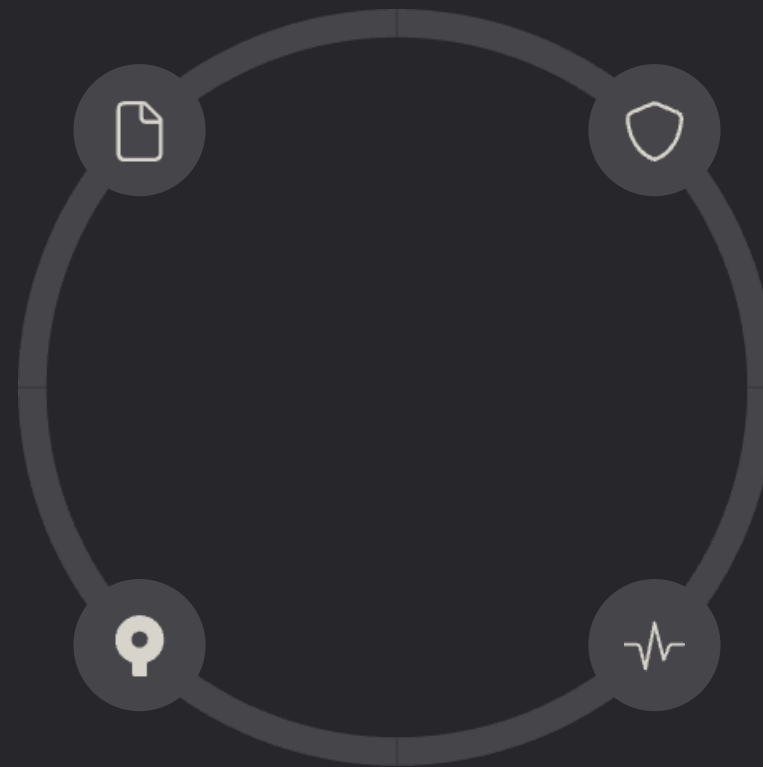
Componente: Cualquier modelo

Filtros de Archivos

Detección de archivos anómalos, EXE, SMB, descargas sospechosas

Requisitos de Fuente

Incidencia ≥ 90 , sin etiquetas específicas, edad > 172800



Filtros de Seguridad

Compliance, SMB Drive Write, Compromise/Ransomware

Filtros de Actividad

Actividad inusual, operaciones de escritura sospechosas

Este componente utiliza 11 filtros (A-K) y se activará cuando se cumplan combinaciones específicas. Por ejemplo, cuando A, B, C, H, I, J y K son verdaderas simultáneamente, o cuando E, H, I, J y K son verdaderas, entre otras combinaciones posibles.

Componente: Modelo más de 1 en 24 horas

Filtros de Mensajes	Coincidencia con expresiones regulares, términos como "Rare external", "New Endpoint", "Beacon"
Verificaciones de Seguridad	Incidencia nueva o poco común ≥ 90 , mensajes con "External Windows", "to Rare Endpoint"
Requisitos de Fuente	Sin etiqueta "Agentes de usuario en conflicto", edad > 172800
Requisito Adicional	Campos de mensajes únicos (filtro L)

Este componente utiliza 12 filtros (A-L) y se activará cuando se cumplan combinaciones específicas. La diferencia clave con el primer componente es la adición del filtro L "Campos de mensajes únicos", que debe ser verdadero en todas las combinaciones de activación.

Las combinaciones de activación incluyen A, B, G, H, I y L verdaderas simultáneamente, o A, C, G, H, I y L verdaderas, entre otras posibilidades específicas.



Caso de uso 4: Evaluación integral de riesgos

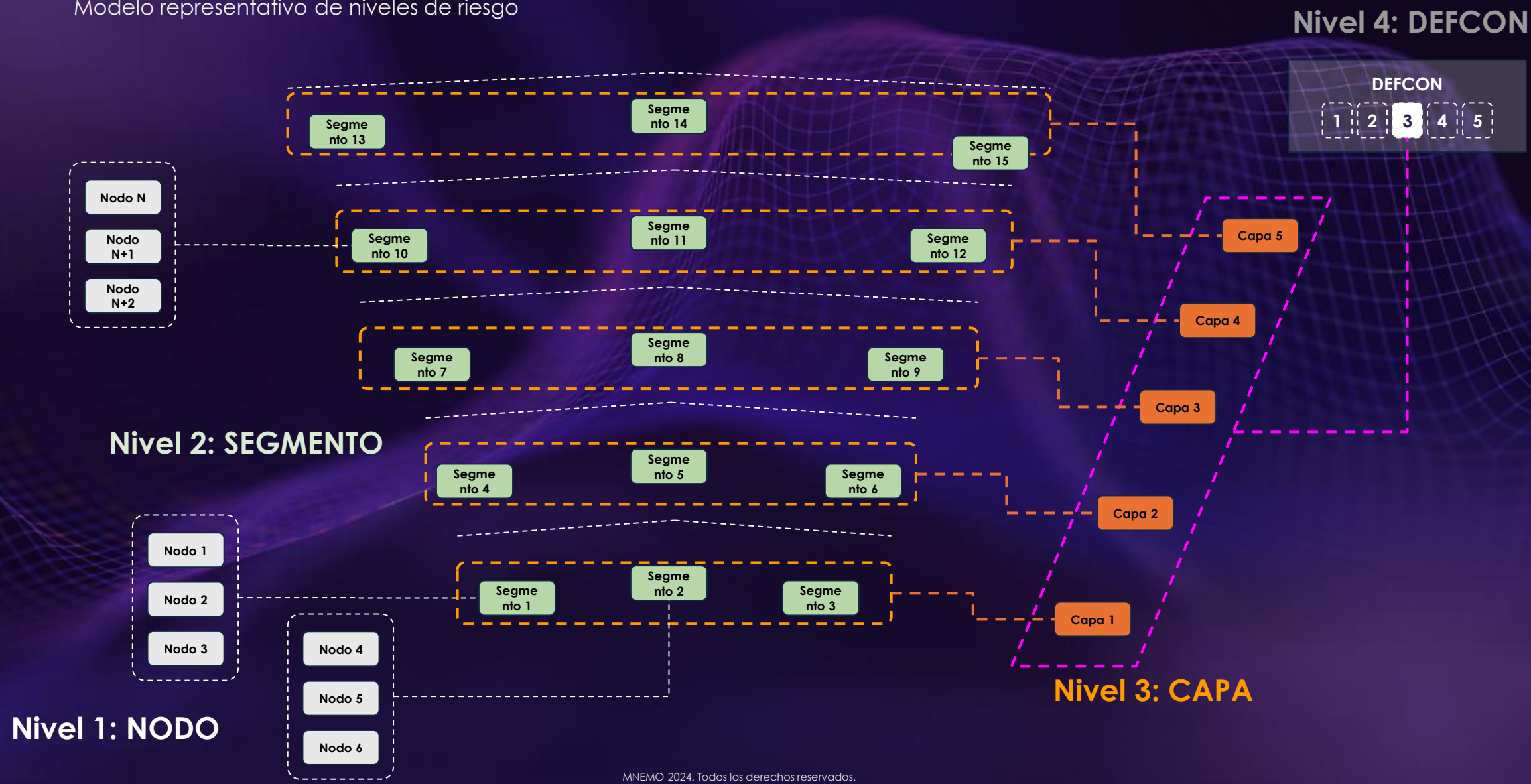
1. Definición conceptual del caso de uso
2. Arquitectura lógica del caso de uso
3. Requisitos y fuentes de datos
4. Arquitectura técnica
5. Productos del caso de uso

Modelo integral de riesgo que centraliza y agrega toda la posición de seguridad en 4 niveles (nodos -servicios-, segmentos -agregan servicios de alcance cercano o complementario-, capas -agregan segmentos con una cercanía a la infraestructura similar, 5 niveles- y DEFCON -indicador global agregado del riesgo-.

Fuentes de datos involucradas

- Cada nodo consume información de uno o varios servicios generando un valor de riesgo.

Modelo representativo de niveles de riesgo



Lógica de cálculo de los niveles agregado: **CAPA EXOS**

Capa	Fórmula Capa:pesos de los segmentos	Niveles de clasificación capa	Segmento	Fórmula Segmento:pesos de los nodos	Niveles de clasificación segmento	Nodo
EXOS	(Digital Monitoring Risk x 0,40) + (E-crime Monitoring Risk x 0,40) + (Threat Monitoring Risk x 0,20)	● %50 > = 5 (Suma de alertas críticas, altas) ● Entre 40% y 49% = 4 - Muy alto ● Entre 30% y 39% = 3 - Alto ● Entre 20% y 29% = 2 - Medio ● %19 < = 1 - Bajo	Digital Monitoring	(Brand Sentiment Risk x 0,60) + (Social Monitoring Risk x 0,30) + (External application Risk x 0,10)	● %90 > = 5 - Crítico ● Entre %80 y 89% = 4 - Muy Alto ● Entre 60% y 79% = 3 - Alto ● Entre 30% y 59% = 2 - Medio ● %30% < = 1 Bajo	Brand Sentiment
						Social Monitoring
						External Application Monitor
			E-crime Monitoring	(Critical Information Risk x 0,30) + (Domain Attacks Risk x 0,70)	● %40 > = 5 (Suma de alertas críticas, altas) ● Entre 30% y 39% = 4 - Muy alto ● Entre 20% y 29% = 3 - Alto ● Entre 10% y 19% = 2 - Medio ● %9 < = 1 - Bajo	Critical information leaks
						Domain attacks
			Threats Monitoring	(Intelligence Preventive Risk x 0,30) + (CyberFraud x 0,70)	● %60 > = 5 (Suma de alertas críticas, altas) ● Entre 50% y 59% = 4 - Muy alto ● Entre 40% y 49% = 3 - Alto ● Entre 30% y 39% = 2 - Medio ● %29 < = 1 - Bajo	Cyberfraud
						Intelligence Preventive

Lógica de cálculo de los niveles agregado: **CAPA THERMOS**

Capa	Fórmula Capa:pesos de los segmentos	Niveles de clasificación capa	Segmento	Fórmula Segmento:pesos de los nodos	Niveles de clasificación segmento	Nodo
THERMOS	(Corporate Intelligence x 0,45) + (Cloud x 0,45) + (Third Parties x 0,10)	• %50 > = 5 (Suma de alertas críticas, altas) • Entre 40% y 49% = 4 - Muy alto • Entre 30% y 39% = 3 - Alto • Entre 20% y 29% = 2 - Medio • %19 < = 1 - Bajo	Corporate Intelligence	(Risk Scoring Status x 0,80) + (VIP Fingerprint x 0,10) + (Infrastructure Fingerprint x 0,10)	• %70 > = 5 - Crítico • Entre %60 y 69% = 4 - Muy Alto • Entre 50% y 59% = 3 - Alto • Entre 40% y 49% = 2 - Medio • %39% < = 1 Bajo	Risk Scoring Status
						VIP Fingerprint
						Infrastructure Fingerprint
			Cloud	(Vulnerabilities & Weaknesses Riskx 0,70) + (Attacks and Threat Behavior Risk x 0,30)		Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
			Third Parties	(Risk Scoring Status x 0,50) + (CyberReputation Risk x 0,30) + (Vulnerabilities & Weaknesses Risk x 0,20)	• %90 > = 5 - Crítico • Entre %80 y 89% = 4 - Muy Alto • Entre 60% y 79% = 3 - Alto • Entre 30% y 59% = 2 - Medio • %30% < = 1 Bajo	Risk Scoring Status
						CyberReputation Risk
						Vulnerabilities & Weaknesses Risk

Lógica de cálculo de los niveles agregado: **CAPA MESOS**

Capa	Fórmula Capa:pesos de los segmentos	Niveles de clasificación capa	Segmento	Fórmula Segmento:pesos de los nodos	Niveles de clasificación segmento	Nodo
MESOS	(Exposure monitoring x 0,25) + (Operation Availability x 0,60) + (Vulnerability Intelligence x 0,15)	• %50 >= 5 • Entre 40% y 49% = 4 - Muy alto • Entre 30% y 39% = 3 - Alto • Entre 20% y 29% = 2 - Medio • %19 <= 1 - Bajo	Exposure monitoring	(Applications x 0,50) + (communications x 0,25) + (services x 0,25)	• %90 >= 5 - Crítico • Entre %80 y 89% = 4 - Muy Alto • Entre 60% y 79% = 3 - Alto • Entre 30% y 59% = 2 - Medio • %30% <= 1 Bajo	Applications
						Communications
						Services
			Operation Availability	(Applications x 0,50) + (communications x 0,25) + (services x 0,25)		Applications
						Communications
						Services
			Vulnerability Intelligence	(Early detection x 0,90 + Risk landscapes x 0,10)		Early detection
						Risk Landscape

Lógica de cálculo de los niveles agregado: **CAPA STRATOS**

Capa	Fórmula Capa:pesos de los segmentos	Niveles de clasificación capa	Segmento	Fórmula Segmento:pesos de los nodos	Niveles de clasificación segmento	Nodo
STRATOS	(External Application Security x 0,33) + (External Communication Security x 0,33) + (External Services Security x 0,33)	● %50 > = 5 ● Entre 40% y 49% = 4 - Muy alto ● Entre 30% y 39% = 3 - Alto ● Entre 20% y 29% = 2 - Medio ● %19 < = 1 - Bajo	External Applications Security	(Vulnerabilities & Weaknesses Riskx 0,25) + (Attacks and Threat Behavior Risk x 0,75)	● %90 > = 5 - Crítico ● Entre %80 y 89% = 4 - Muy Alto ● Entre 60% y 79% = 3 - Alto ● Entre 30% y 59% = 2 - Medio ● %30% < = 1 Bajo	Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
			External Communication Security	(Vulnerabilities & Weaknesses Risk x 0,25) + (Attacks and Threat Behavior Risk x 0,75)		Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
			External Services Security	Weaknesses Riskx 0,25) + (Attacks and Threat Behavior Risk x 0,75)		Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk

Lógica de cálculo de los niveles agregado: **CAPA TROPOS**

Capa	Fórmula Capa:pesos de los segmentos	Niveles de clasificación capa	Segmento	Fórmula Segmento:pesos de los nodos	Niveles de clasificación segmento	Nodo
TROPOS	(Infrastructure security x 0,33) + (Identity security x 0,33) + (Data security x 0,33)	• %50 > = 5 Crítico • Entre 40% y 49% = 4 - Muy alto • Entre 30% y 39% = 3 - Alto • Entre 20% y 29% = 2 - Medio • %19 < = 1 - Bajo	Infrastructure Security	(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)	• %90 > = 5 - Crítico • Entre %80 y 89% = 4 - Muy Alto • Entre 60% y 79% = 3 - Alto • Entre 30% y 59% = 2 - Medio • %30% < = 1 Bajo	Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
						CounterIntelligence & Deception
			External Communication Security	(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)	• %90 > = 5 - Crítico • Entre %80 y 89% = 4 - Muy Alto • Entre 60% y 79% = 3 - Alto • Entre 30% y 59% = 2 - Medio • %30% < = 1 Bajo	Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
						CounterIntelligence & Deception
			Data Security	(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)	• %90 > = 5 - Crítico • Entre %80 y 89% = 4 - Muy Alto • Entre 60% y 79% = 3 - Alto • Entre 30% y 59% = 2 - Medio • %30% < = 1 Bajo	Vulnerabilities & Weaknesses Risk
						Attacks and Threat Behavior Risk
						CounterIntelligence & Deception

Lógica de cálculo de los niveles agregado: **DEFCON**

	Fórmula DEFCON :pesos de las capas	Niveles de clasificación DEFCON
DEFCON	$(\text{Capa EXOS} \times 0,2) + (\text{Capa THERMOS} \times 0,2) + (\text{Capa MESOS} \times 0,2) + (\text{Capa STRATOS} \times 0,2) + (\text{Capa TROPOS} \times 0,2)$	• %80 > = 5 Crítico • Entre 60% y 79% = 4 - Muy alto • Entre 40% y 69% = 3 - Alto • Entre 20% y 29% = 2 - Medio • %19 < = 1 - Bajo

CU4:
Evaluación integral de riesgos > 3. Requisitos y fuentes de datos

Identificación de servicios activos en cliente, fuente de origen y fórmula de cálculo de riesgo

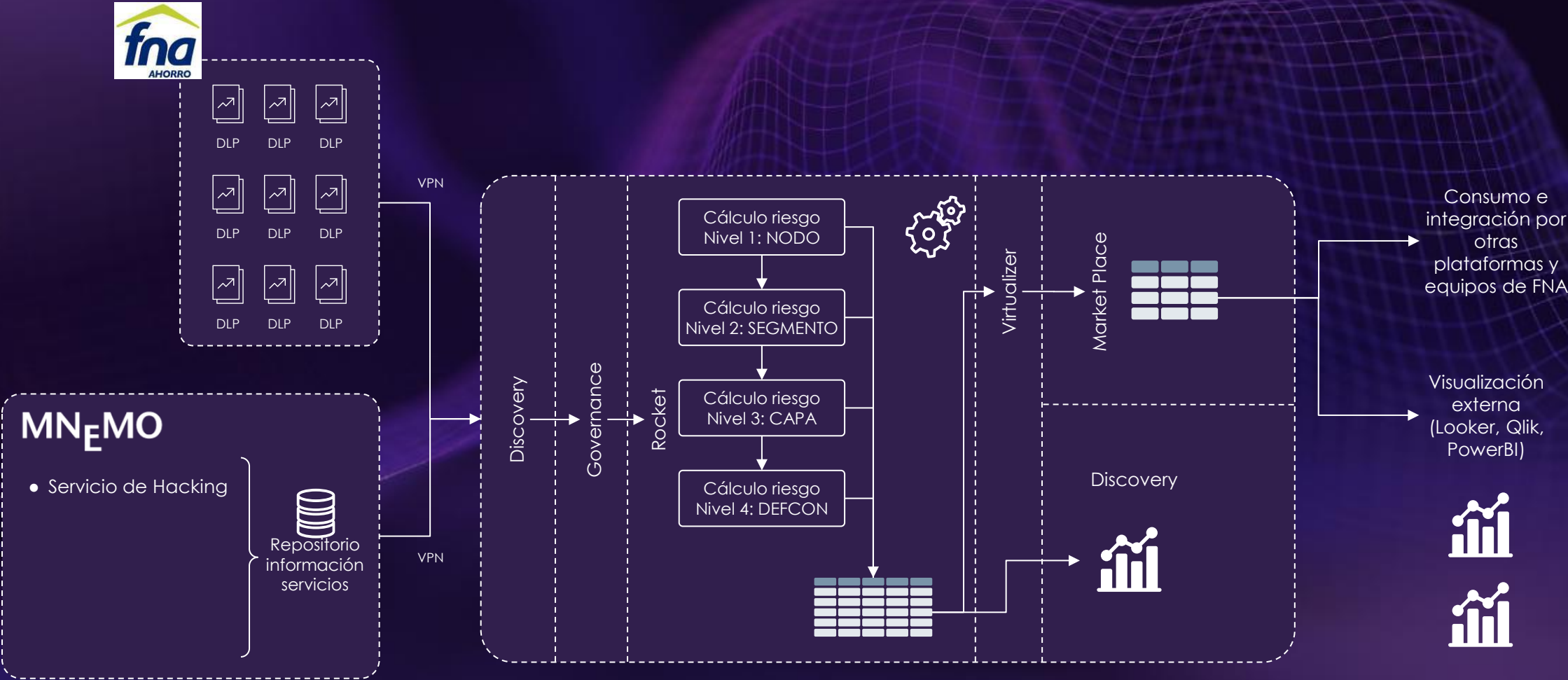
Capa	Segmento	Nodo	Activo en cliente	Fuente de datos	Fórmula de cálculo de riesgo
EXOS	Digital Monitoring	Brand Sentiment	OK	Servicio de vigilancia de medios digitales	# detecciones criticidad >=3 / #total de detecciones
		Social Monitoring	OK	Servicio de vigilancia RRSS	# detecciones criticidad >=4 / #total de detecciones
		External Application Monitor	OK	Servicio de vigilancia APK	# detecciones criticidad >=3 / #total de detecciones
	E-crime Monitoring	Critical information leaks	OK	Servicios de vigilancia de bajas/credenciales/credenciales de terceros	((# detecciones criticidad bajas >=3 / #total de detecciones bajas) + (# detecciones criticidad credenciales>=3 / #total de detecciones credenciales) + (# detecciones criticidad terceros >=3 / #total de detecciones terceros)) /3
		Domain attacks	OK	Servicio de vigilancia de dominios	# detecciones criticidad >=3 / #total de detecciones
	Threats Monitoring	Cyberfraud			
		Intelligence Preventive	OK	Servicio de alerta preventiva	# detecciones criticidad >=4 / #total de detecciones
THERMOS	Corporate Intelligence	Risk Scoring Status			
		VIP Fingerprint			
		Infrastructure Fingerprint			
	Cloud	Vulnerabilities & Weaknesses Risk			
		Attacks and Threat Behavior Risk			
	Third Parties	Risk Scoring Status			
		CyberReputation Risk			
		Vulnerabilities & Weaknesses Risk			
MESOS	Exposure monitoring	Applications			
		Communications			
		Services			
	Operation Availability	Applications			
		Communications			
		Services			
	Vulnerability Intelligence	Early detection	OK	Servicio de alerta temprana	# detecciones criticidad >=7 / #total de detecciones
		Risk Landscape	OK		

CU4:
Evaluación integral de riesgos > 3. Requisitos y fuentes de datos

Identificación de servicios activos en cliente, fuente de origen y fórmula de cálculo de riesgo

Capa	Segmento	Nodo	Activo en cliente	Fuente de datos	Fórmula de cálculo de riesgo
STRATOS	External Applications Security	Vulnerabilities & Weaknesses Risk	OK	AC-EH-PortalesPub	# registros con criticidad = 5 / # total de registros
		Attacks and Threat Behavior Risk	OK		
	External Communication Security	Vulnerabilities & Weaknesses Risk	OK	AV Portales Pub-ECVW	# registros con valor "Alto" (5) / # total de registros
		Attacks and Threat Behavior Risk	OK		
	External Services Security	Vulnerabilities & Weaknesses Risk			
		Attacks and Threat Behavior Risk			
TROPOS	Infrastructure Security	Vulnerabilities & Weaknesses Risk	OK	Servicio de análisis de vulnerabilidades	(# vul. riesgo >7) # total de vulnerabilidades
		Attacks and Threat Behavior Risk	OK		
		CounterIntelligence & Deception			
	Identity Security	Vulnerabilities & Weaknesses Risk	OK		
		Attacks and Threat Behavior Risk	OK		
		CounterIntelligence & Deception			
	Data Security	Vulnerabilities & Weaknesses Risk			
		Attacks and Threat Behavior Risk			
		CounterIntelligence & Deception			

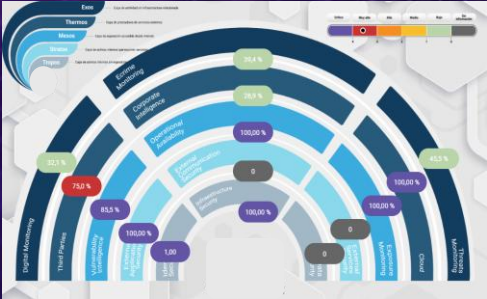
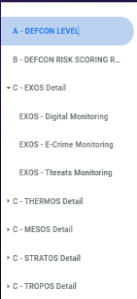
CU4:
Evaluación integral de riesgos > 4. Arquitectura técnica



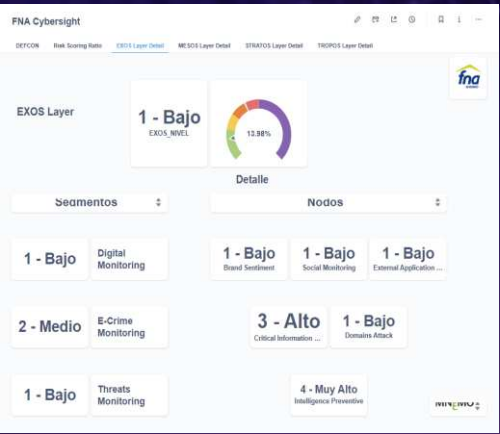
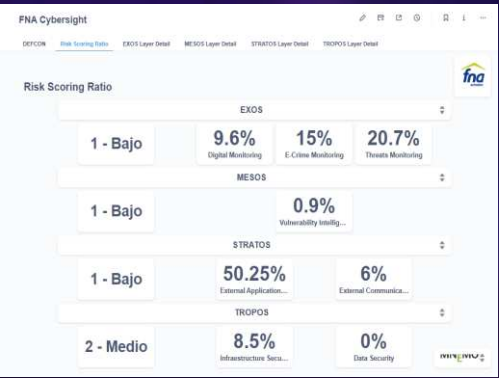
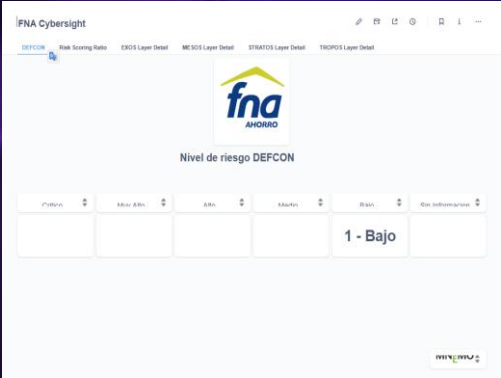
CU4:
Evaluación integral de riesgos > 5. Productos del caso de uso

Dashboards que muestran el riesgo en los distintos niveles del modelo, diversos diseños en base al BI seleccionado.

Versión Looker
Studio
(BI Externo)



Versión Stratio
Data Fabric
(BI Interno)



Caso de uso 4: Evaluación integral de riesgos

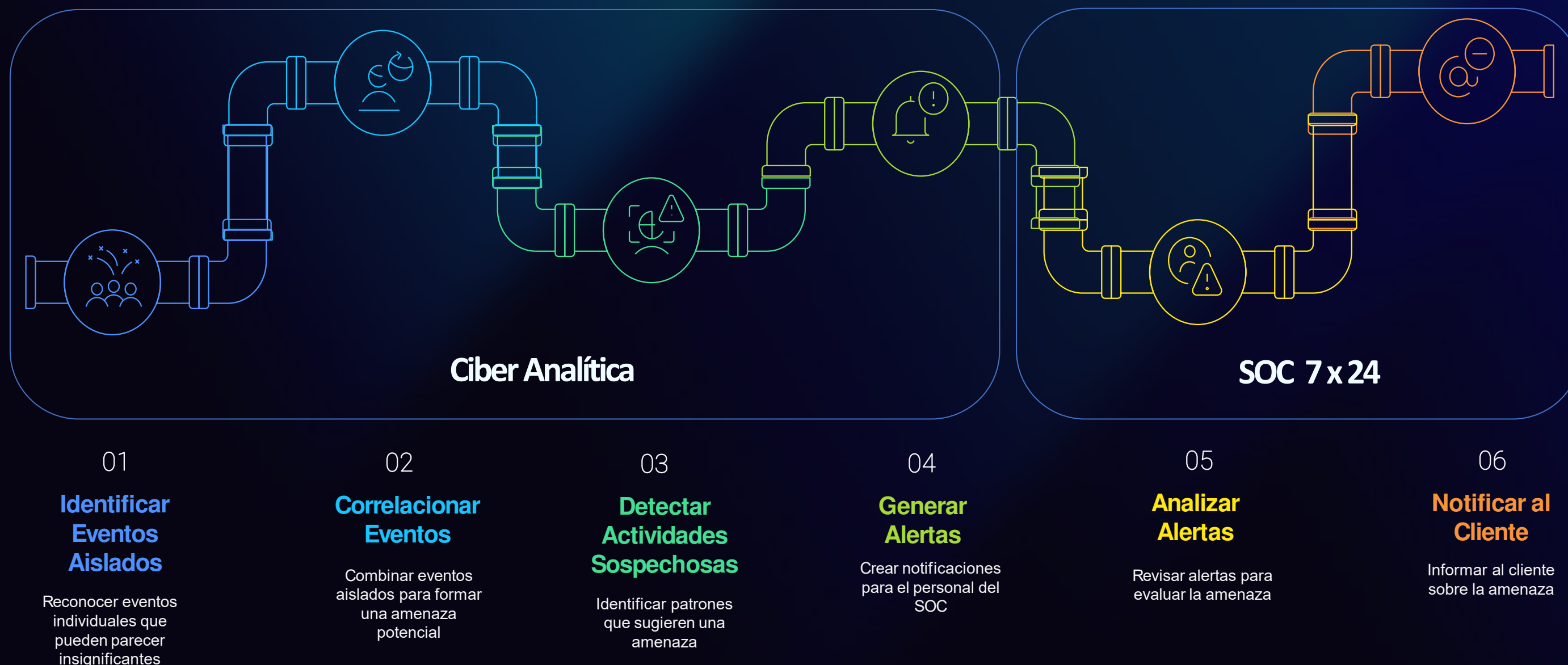
Data & AI

CASO DE USO 5
CORRELACION
AVANZADA

MN_EMO

MN_EMO

Interoperabilidad Casos de Uso con el servicio SOC

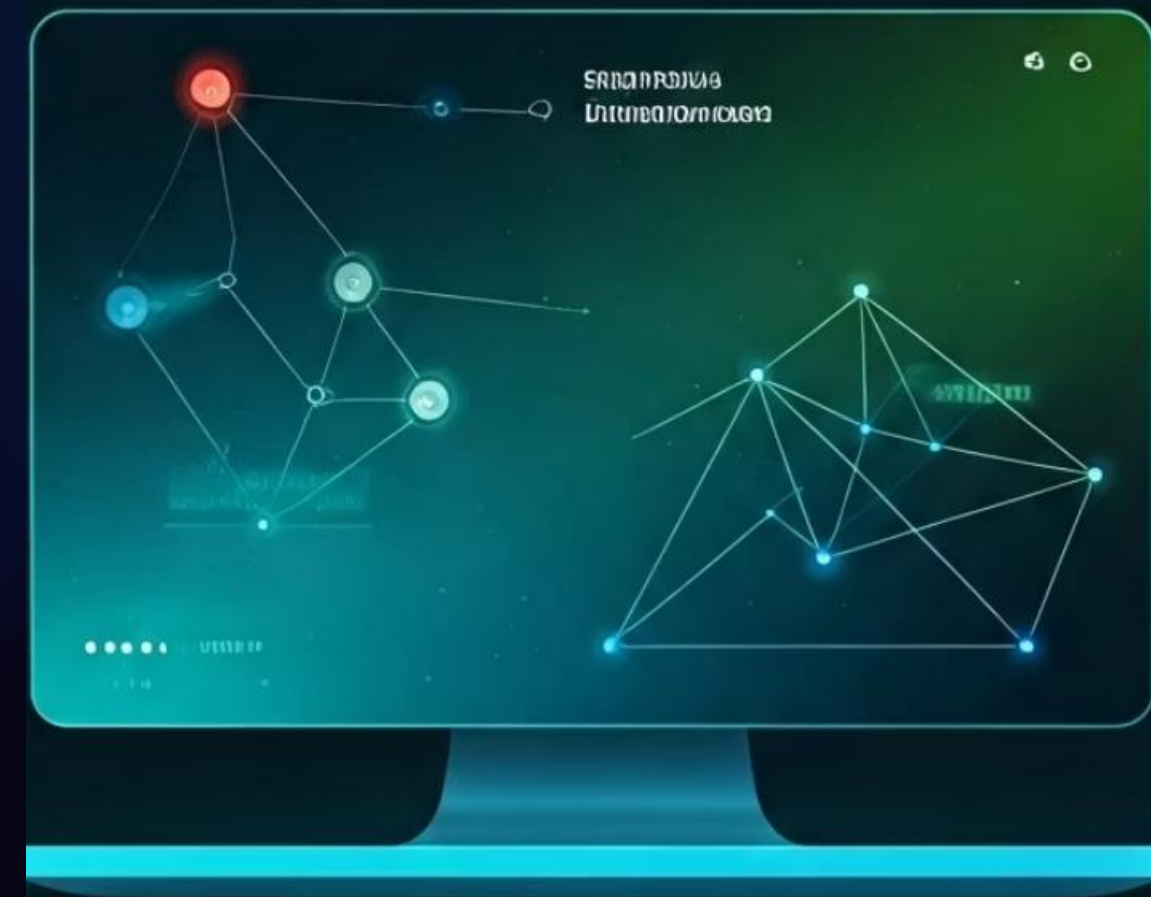


El proceso de correlación avanzada se inicia con la identificación de eventos aislados, a menudo insignificantes por sí mismos, pero que en conjunto pueden representar una amenaza significativa. Esta capacidad permite a nuestro sistema de ciber analítica detectar actividades sospechosas seguidas de tareas administrativas en endpoints, generando alertas que el personal del SOC, operativo 24/7, puede analizar rápidamente.

Caso de uso correlación avanzada

Esta presentación detalla una regla de correlación avanzada diseñada para detectar actividades sospechosas seguidas de tareas de administración en el mismo sistema. La regla se activa cuando, tras detectar comportamientos potencialmente maliciosos, se realizan acciones administrativas como descargar archivos, modificar derechos de usuario o ejecutar comandos con privilegios elevados.

La lógica general establece que la regla se ejecuta cuando se detecta una coincidencia de "Administración habitual de endpoints" al menos una vez en los 10 minutos posteriores a cualquier "Actividad sospechosa en puntos finales" con el mismo identificador. A continuación, exploraremos en detalle los componentes y criterios específicos que conforman esta regla de correlación.



Lógica Detallada de la Regla

Componentes Generales

La regla se activa cuando se detecta una actividad sospechosa seguida de una tarea de administración de endpoint en el mismo sistema.

Condición Temporal

La administración habitual de endpoints debe coincidir al menos 1 vez en los 10 minutos posteriores a la detección de la actividad sospechosa.

Identificación

Ambos eventos deben estar relacionados con el mismo identificador para establecer la correlación entre ellos.

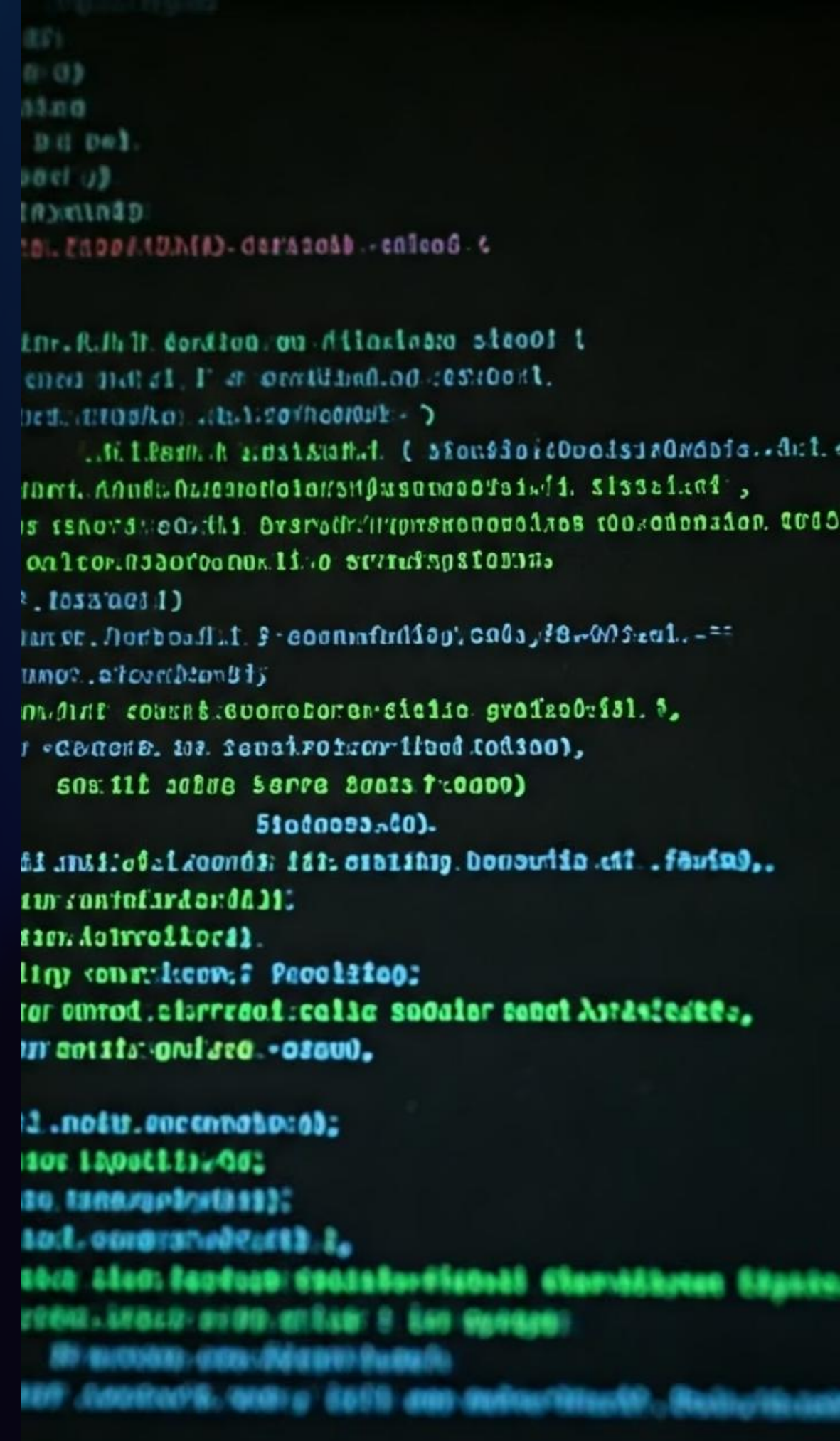
La lógica detallada de esta regla se compone de dos bloques principales: "Administración habitual de endpoints" y "Actividades sospechosas en puntos finales". Cada uno de estos bloques agrupa múltiples criterios específicos que, al cumplirse en la secuencia temporal establecida, desencadenan la alerta de seguridad.

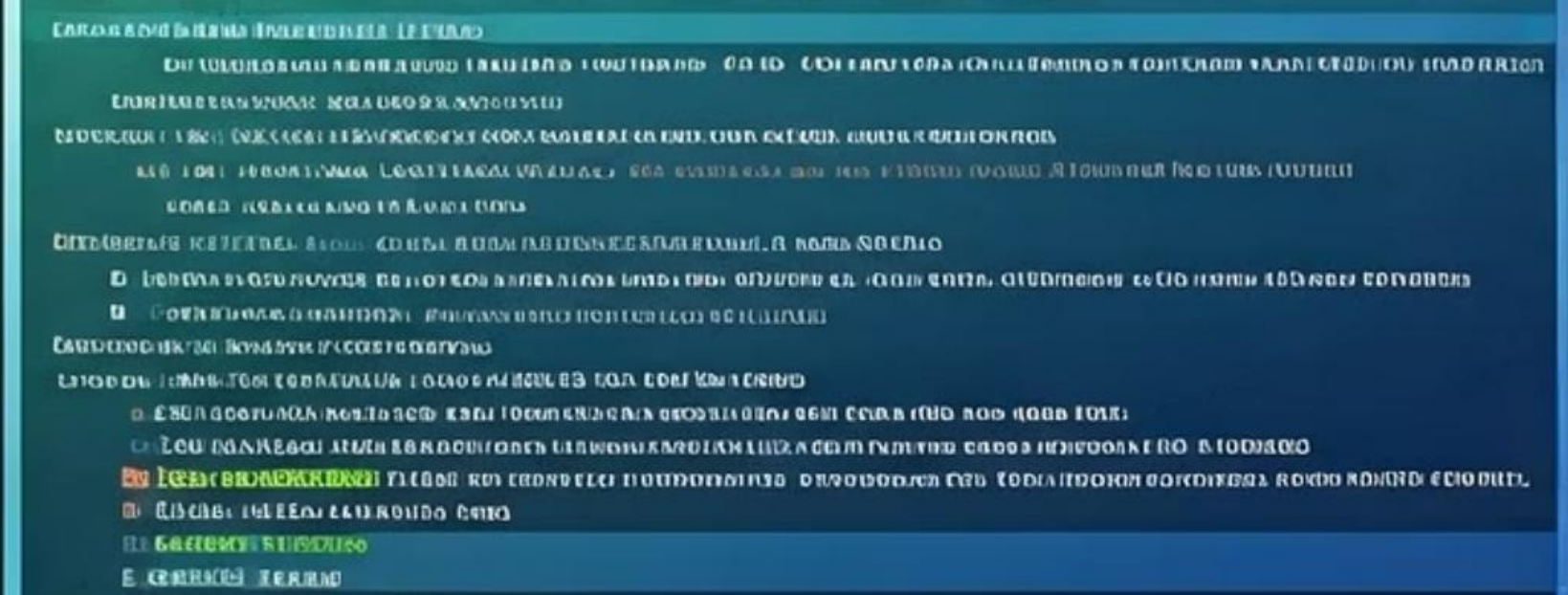


Privilegios de administrador añadidos (Unix)

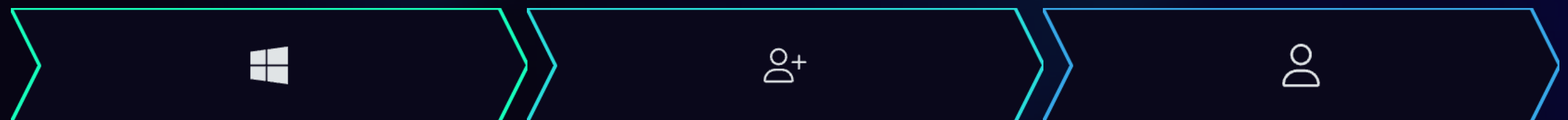
- 1 Sistema Operativo**
El evento debe ocurrir en un sistema Unix.
- 2 Categoría del Evento**
La categoría del evento debe ser Authentication.Group Member Add Success.
- 3 Aplicación**
La aplicación utilizada debe ser usermod.
- 4 Grupo**
El nombre del grupo debe ser sudo.

Este criterio específico dentro del bloque "Administración habitual de endpoints" detecta cuando se añaden privilegios de administrador en sistemas Unix. La detección se basa en la combinación de eventos de autenticación relacionados con la adición de miembros a grupos, específicamente cuando se utiliza el comando usermod para añadir usuarios al grupo sudo, otorgándoles así privilegios elevados en el sistema.





Privilegios de administrador añadidos (Windows)



Fuente del Evento

Microsoft Windows Security Event
Log

Categoría del Evento

Authentication.Group Member Added

Grupo Objetivo

Administrators o Administradores

Este criterio detecta la adición de privilegios de administrador en sistemas Windows. Se activa cuando el registro de eventos de seguridad de Windows detecta que un usuario ha sido añadido al grupo "Administrators" o "Administradores", lo que le otorga control total sobre el sistema operativo.

La detección de este tipo de eventos es crucial ya que la elevación de privilegios es una técnica común utilizada por atacantes después de obtener acceso inicial a un sistema, permitiéndoles realizar acciones con mayores permisos y potencialmente comprometer todo el entorno.

Privilegios de administrador eliminados (Windows)

Fuente del Evento

El evento debe ser detectado por Microsoft Windows Security Event Log, que registra todos los cambios relacionados con la seguridad en sistemas Windows.

Este criterio detecta cuando se eliminan usuarios del grupo de administradores en sistemas Windows. Aunque puede parecer una acción de reducción de privilegios positiva, en contexto con actividades sospechosas previas podría indicar intentos de ocultar acciones maliciosas o crear cuentas alternativas con privilegios mientras se eliminan usuarios legítimos.

Categoría del Evento

La categoría específica debe ser Authentication.Group Member Removed, indicando que un miembro ha sido eliminado de un grupo de seguridad.

Grupo Objetivo

El nombre del grupo afectado debe ser específicamente "Administrators", lo que indica cambios en los privilegios administrativos del sistema.

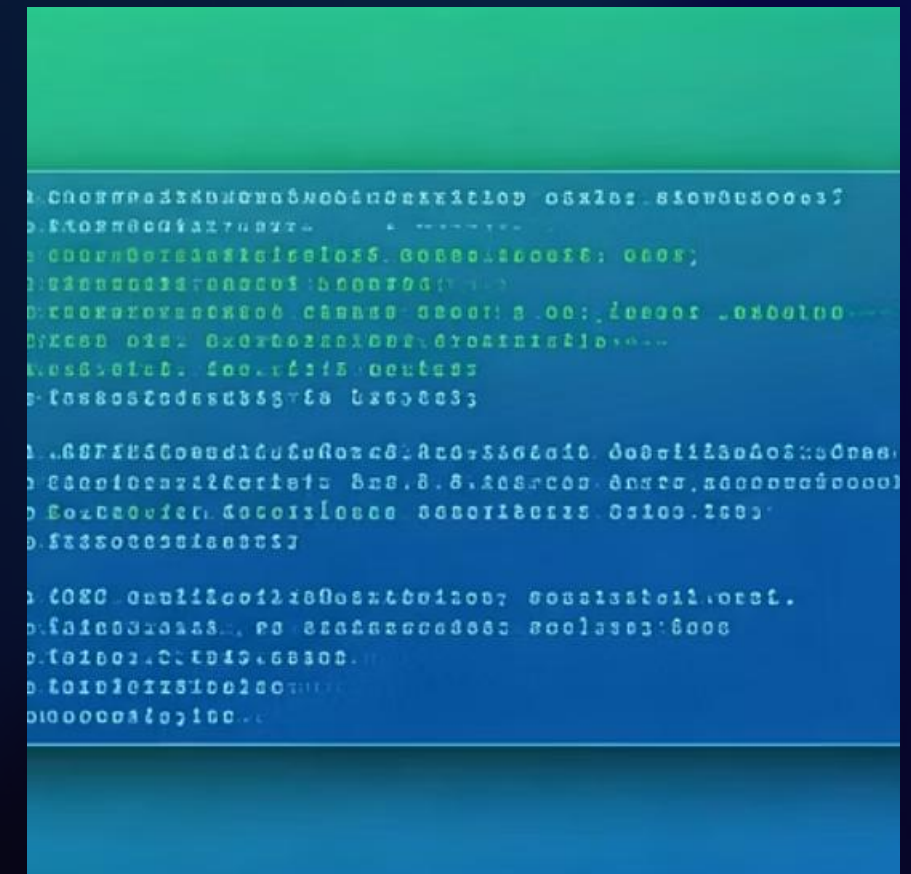
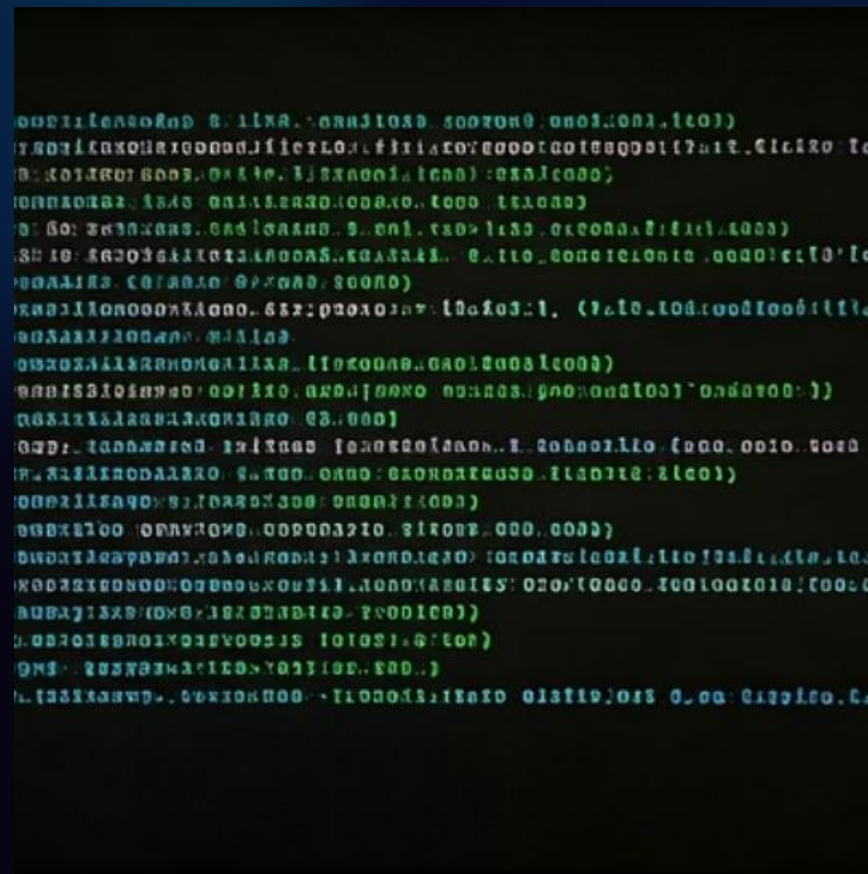
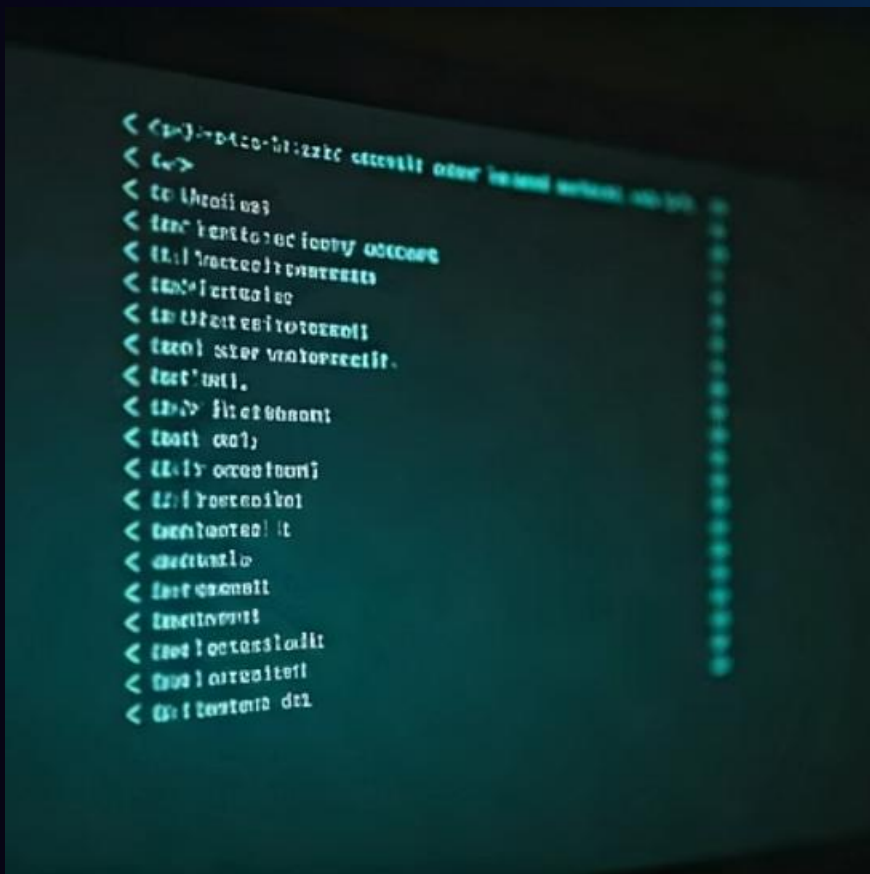
Descargar utilidades en eventos



Este criterio detecta cuando se utilizan herramientas comunes para descargar archivos desde Internet en sistemas de punto final. Las utilidades como wget, curl, bitsadmin y certutil son legítimas pero frecuentemente abusadas por atacantes para descargar malware o herramientas adicionales después de comprometer un sistema.

La monitorización de estas actividades es esencial ya que representan un vector común para la segunda fase de un ataque, donde el adversario intenta establecer persistencia o expandir su acceso.

Descubrimiento de grupo o cuenta



Este criterio detecta intentos de descubrir información sobre grupos y cuentas de usuario en el sistema. Se activa cuando se ejecutan comandos específicos diseñados para enumerar usuarios y grupos, como "whoami", "groups", "net localgroup", o consultas LDAP.

El descubrimiento de cuentas es una táctica común en la fase de reconocimiento de un ataque, donde los adversarios intentan identificar cuentas privilegiadas que podrían ser objetivos para el movimiento lateral o la escalada de privilegios. La detección temprana de estas actividades de reconocimiento puede ayudar a prevenir ataques más avanzados.

Archivo o carpeta ocultos creados

3

Sistemas Operativos

Windows, Linux, HP-UX, Solaris, AIX, Mac
OS X, IBM i

1

Categoría

System.File Created

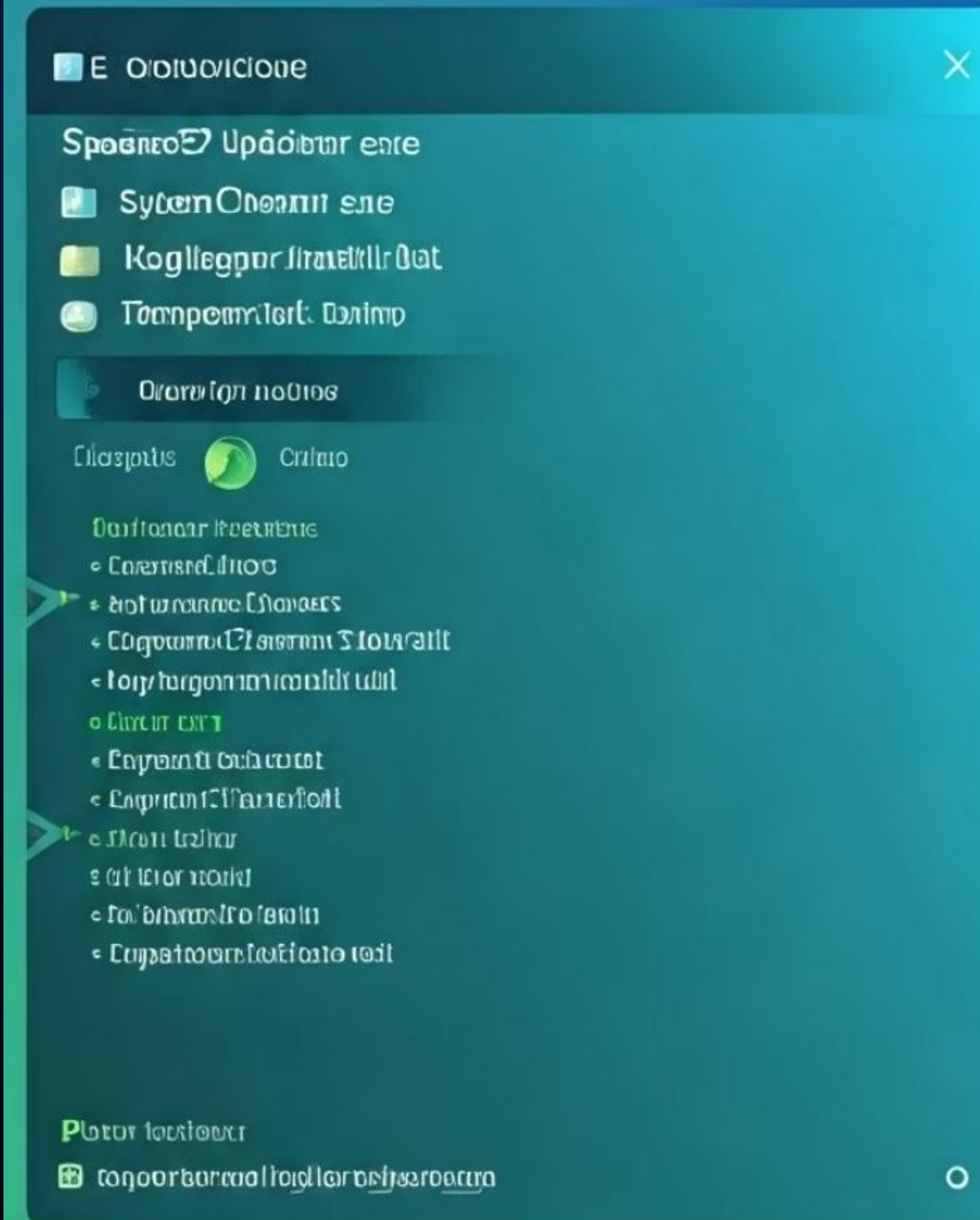
2

Patrones

Archivos que comienzan con punto o tienen atributos ocultos

Este criterio detecta la creación de archivos o carpetas ocultos en sistemas operativos. En Unix/Linux, los archivos ocultos comienzan con un punto (.), mientras que en Windows pueden tener atributos específicos de archivo oculto. La regla utiliza expresiones regulares para identificar nombres de archivo que comienzan con punto o tienen codificaciones específicas que indican atributos ocultos.

La creación de archivos ocultos es una técnica común utilizada por atacantes para ocultar malware, herramientas de persistencia o datos robados, dificultando su detección durante análisis forenses o escaneos de seguridad rutinarios.



Descubrimiento de políticas de contraseñas (Unix)



Archivos Monitorizados

La regla detecta accesos a archivos críticos de configuración de políticas de contraseñas en sistemas Unix, incluyendo
`/etc/pam.d/common-password,`
`/etc/pam.d/system-auth,`
`/etc/security/pwquality.conf`
y `/etc/login.defs`.



Categoría del Evento

Se monitoriza específicamente la categoría `Audit.Command Execution Attempt`, que registra intentos de ejecutar comandos en el sistema.



Método de Detección

La detección se realiza mediante expresiones regulares que identifican comandos que acceden o consultan los archivos de configuración de políticas de contraseñas.

Este criterio identifica intentos de descubrir información sobre las políticas de contraseñas en sistemas Unix. Los atacantes suelen buscar esta información para entender las restricciones de contraseñas y planificar ataques de fuerza bruta más efectivos o identificar posibles debilidades en la configuración de seguridad.

Descubrimiento de políticas de contraseñas (Windows)



Plataforma

Microsoft Windows Security Event Log es la fuente de los eventos monitorizados, capturando todas las actividades relacionadas con la seguridad del sistema.



Categoría

System.Process Creation Success es la categoría específica que registra la creación exitosa de nuevos procesos en el sistema operativo.



Comando

Se detectan específicamente variaciones del comando "net accounts", que muestra información sobre políticas de contraseñas del sistema o dominio.

Este criterio detecta intentos de descubrir información sobre las políticas de contraseñas en sistemas Windows. El comando "net accounts" proporciona detalles sobre la configuración de seguridad de contraseñas, como la longitud mínima, requisitos de complejidad, historial y períodos de expiración.

Los atacantes utilizan esta información para adaptar sus ataques de fuerza bruta o identificar configuraciones débiles que podrían ser explotadas. La detección de estas actividades de reconocimiento puede ser un indicador temprano de un posible ataque en desarrollo.

Ejecutar como superusuario u otro usuario (Unix)



Verificación de Sistema

El evento debe ocurrir en un sistema operativo Unix



Categoría del Evento

System.Process Creation Success



Verificación de Identidad

Audit ID diferente del Effective User ID

Este criterio detecta cuando un proceso se ejecuta con privilegios de otro usuario en sistemas Unix. La regla verifica que el ID de auditoría (el usuario que inició la acción) sea diferente del ID de usuario efectivo (el usuario con cuyos privilegios se ejecuta el proceso), excluyendo los procesos comunes como su, sudo, sh y bash.

Esta técnica es frecuentemente utilizada por atacantes para escalar privilegios o ejecutar comandos maliciosos con los permisos de usuarios más privilegiados después de comprometer una cuenta de menor nivel.

Ejecutar como superusuario u otro usuario (Windows)

Fuente del Evento

Microsoft Windows Security Event Log, que registra todos los eventos relacionados con la seguridad del sistema operativo Windows.

Esta fuente proporciona información detallada sobre la creación de procesos y los contextos de seguridad en los que se ejecutan.

Categoría del Evento

System.Process Creation Attempt o System.Process Creation Success, que capturan los intentos y ejecuciones exitosas de nuevos procesos.

Estas categorías son fundamentales para monitorizar la actividad de ejecución en el sistema.

Tipo de Elevación

Token Elevation Type debe estar presente y ser uno de los valores '%%1937' o '%%1938', que indican elevación de privilegios.

Estos códigos específicos representan diferentes tipos de elevación de privilegios en Windows.

Este criterio detecta cuando un proceso se ejecuta con privilegios elevados en sistemas Windows. El tipo de elevación de token indica si un proceso se está ejecutando con privilegios administrativos completos o limitados, siendo una característica clave del Control de Cuentas de Usuario (UAC) de Windows.

Cuenta de usuario añadida (Unix)



Este criterio detecta la creación de nuevas cuentas de usuario en sistemas Unix. La regla se activa cuando se registran eventos de la categoría Authentication.User Account Added y la aplicación utilizada coincide con los comandos useradd o adduser, que son las herramientas estándar para crear usuarios en sistemas Unix.

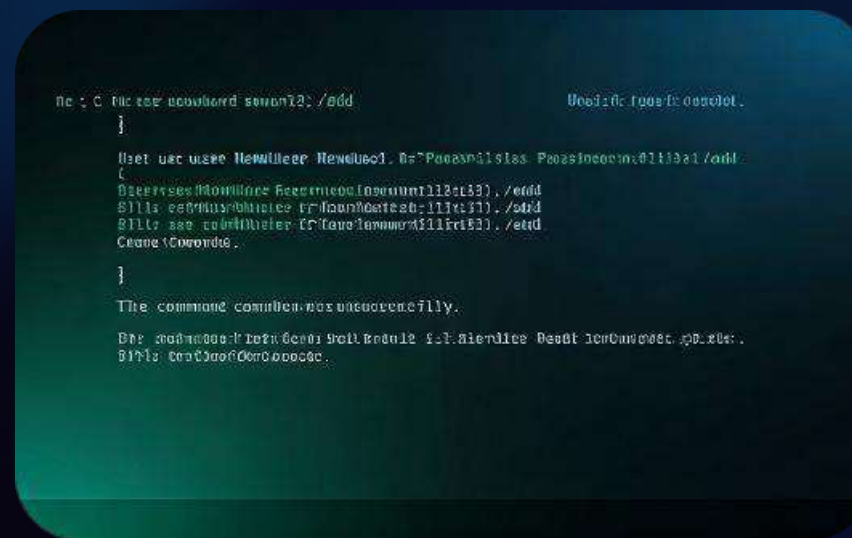
La creación de cuentas de usuario no autorizadas es una técnica común utilizada por atacantes para establecer persistencia en sistemas comprometidos, permitiéndoles mantener el acceso incluso si se descubren y remedian otras vías de entrada.

Cuenta de usuario añadida (Windows)



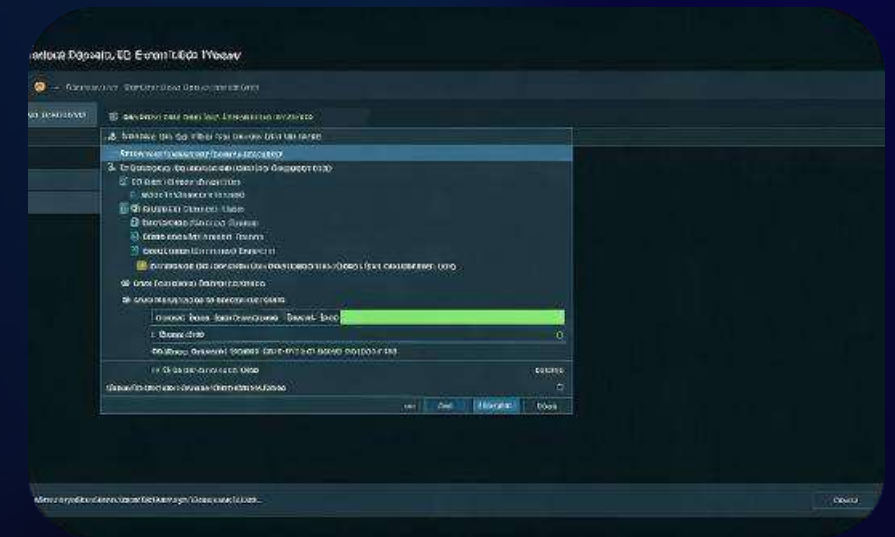
Interfaz de Administración

La creación de usuarios en Windows puede realizarse a través de interfaces gráficas como el Panel de Control o herramientas administrativas, pero todas generan el mismo tipo de evento de seguridad.



Línea de Comandos

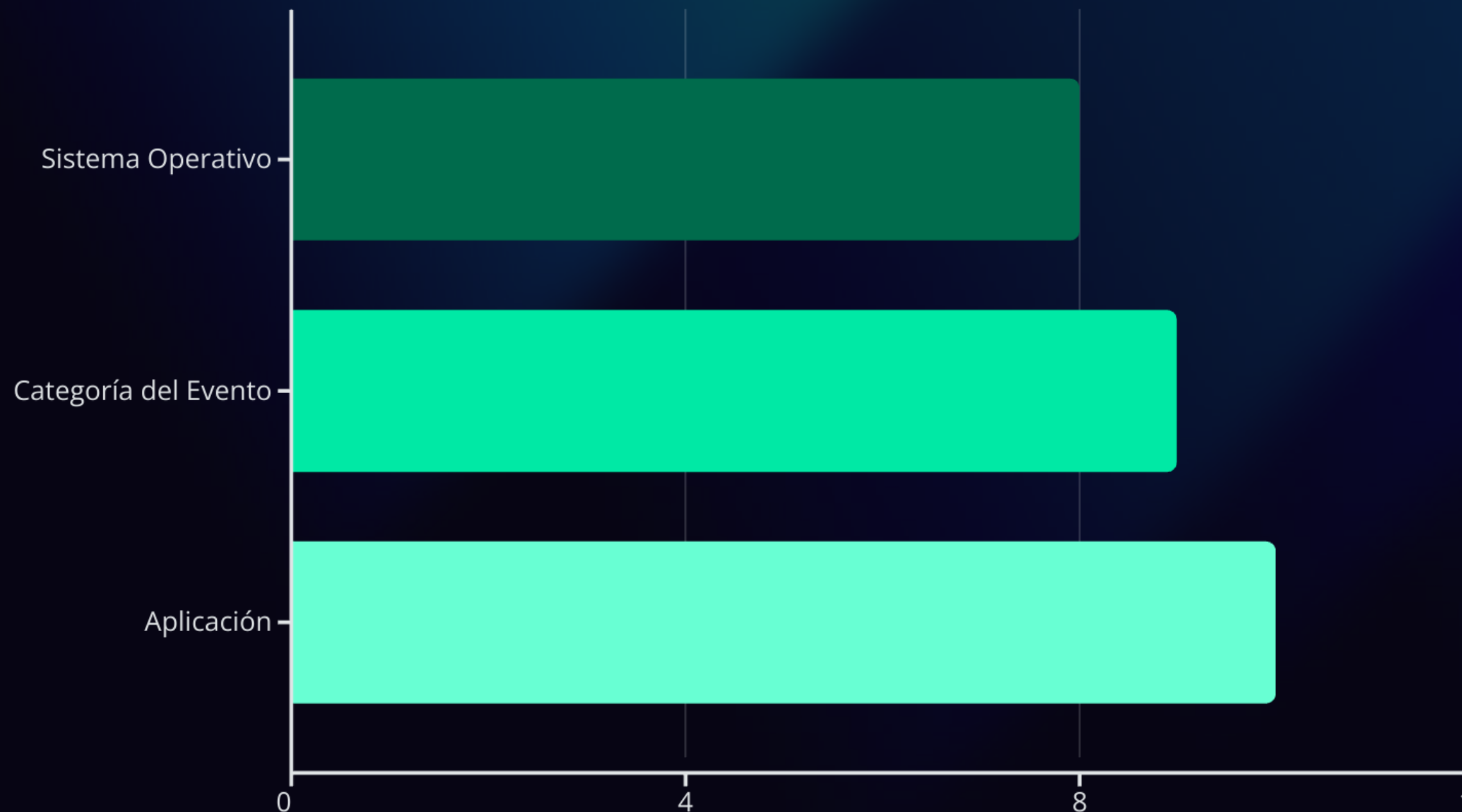
Los atacantes suelen preferir métodos de línea de comandos como "net user" para crear cuentas, ya que pueden ejecutarse remotamente o a través de scripts automatizados durante un ataque.



Registro de Eventos

La regla detecta específicamente el QID 5000892, que corresponde a un evento de auditoría exitosa de creación de cuenta de usuario en el registro de seguridad de Windows.

Cuenta de usuario eliminada (Unix)



Este criterio detecta la eliminación de cuentas de usuario en sistemas Unix. La regla se activa cuando se registran eventos de la categoría Authentication.User Account Removed y la aplicación utilizada coincide con los comandos userdel o deluser, que son las herramientas estándar para eliminar usuarios en sistemas Unix.

La eliminación de cuentas de usuario puede ser parte de actividades legítimas de administración, pero también puede indicar intentos de ocultar actividades maliciosas o eliminar cuentas legítimas para causar interrupciones. En el contexto de esta regla de correlación, es especialmente relevante cuando ocurre después de actividades sospechosas.

Cuenta de usuario eliminada (Windows)



Fuente del Evento

Microsoft Windows Security Event Log es la fuente primaria de detección, capturando todos los eventos relacionados con la gestión de cuentas de usuario en el sistema.



Identificador Específico

El QID 5000897 corresponde específicamente a un evento de auditoría exitosa de eliminación de cuenta de usuario en Windows.



Contexto de Seguridad

La eliminación de cuentas requiere privilegios administrativos, por lo que este evento también puede indicar que el atacante ya ha obtenido acceso elevado al sistema.

Este criterio detecta la eliminación de cuentas de usuario en sistemas Windows. La eliminación de cuentas puede ser parte de una estrategia para ocultar actividades maliciosas, eliminar usuarios legítimos para causar interrupciones, o limpiar rastros después de crear y utilizar cuentas temporales para actividades maliciosas.

En el contexto de la regla de correlación, la eliminación de cuentas después de actividades sospechosas puede ser un fuerte indicador de compromiso y requiere investigación inmediata.

Permiso de archivo modificado

	Sistemas Compatibles Windows, Linux, HP-UX, Solaris, AIX, Mac OS X, IBM i
	Categoría del Evento System.Process Creation Success
3	Proceso Específico chmod (cambio de modo de archivo)
	Parámetros Técnicos Audit ID presente y Call Type igual a 268

Este criterio detecta modificaciones en los permisos de archivos en sistemas operativos. Se centra específicamente en el uso del comando chmod, que es la herramienta estándar para cambiar permisos de archivos en sistemas Unix. La regla verifica que el ID de auditoría esté presente y que el tipo de llamada sea 268, que corresponde a operaciones de cambio de permisos.

La modificación de permisos de archivos puede ser utilizada por atacantes para hacer ejecutables archivos maliciosos, ocultar archivos de usuarios normales, o cambiar la configuración de seguridad de archivos críticos del sistema.

Actividad de descarga de archivos de PowerShell

Fuente del Evento	Microsoft Windows Security Event Log
Categoría	Audit.Command Execution Success
Comandos Monitorizados	Invoke-WebRequest, Start-BitsTransfer, DownloadFile, DownloadString
Método de Detección	Expresiones regulares que identifican patrones de comandos de descarga

Este criterio detecta el uso de PowerShell para descargar archivos desde Internet. La regla monitoriza comandos específicos como Invoke-WebRequest, Start-BitsTransfer y métodos de la clase System.Net.WebClient como DownloadFile y DownloadString, que son comúnmente utilizados para transferir archivos.

PowerShell es una herramienta legítima pero frecuentemente abusada por atacantes debido a su potencia y flexibilidad. La descarga de archivos mediante PowerShell puede indicar la introducción de malware, scripts maliciosos o herramientas de post-explotación en un sistema comprometido.

Actividad de carga de archivos de PowerShell



Este criterio detecta el uso de PowerShell para cargar archivos a servidores remotos. La regla monitoriza específicamente el uso del método UploadFile, que forma parte de las clases de red de .NET y permite enviar archivos a servidores web u otros destinos remotos.

La carga de archivos puede indicar exfiltración de datos, donde un atacante intenta extraer información sensible del sistema comprometido. Esta actividad es particularmente preocupante cuando ocurre después de otras actividades sospechosas, ya que podría representar la fase final de un ataque donde se extraen los datos robados.

Descubrimiento de directorios (Unix)



Comando ls

El comando ls con opciones específicas para listar directorios es uno de los métodos monitorizados. La regla detecta variantes como "ls -d" o "ls -r" que se utilizan específicamente para enumerar directorios.



Comando find

El uso del comando find con la opción "-type d" para buscar específicamente directorios también es detectado por esta regla. Este método permite búsquedas más exhaustivas y personalizadas de la estructura de directorios.



Impacto en seguridad

El descubrimiento de directorios permite a los atacantes mapear la estructura del sistema, identificar ubicaciones de archivos sensibles y planificar movimientos laterales dentro de la red comprometida.

Descubrimiento de directorios (Windows)

1

Fuente

Microsoft Windows Security Event
Log

2

Categoría

Audit.Command Execution Success

3

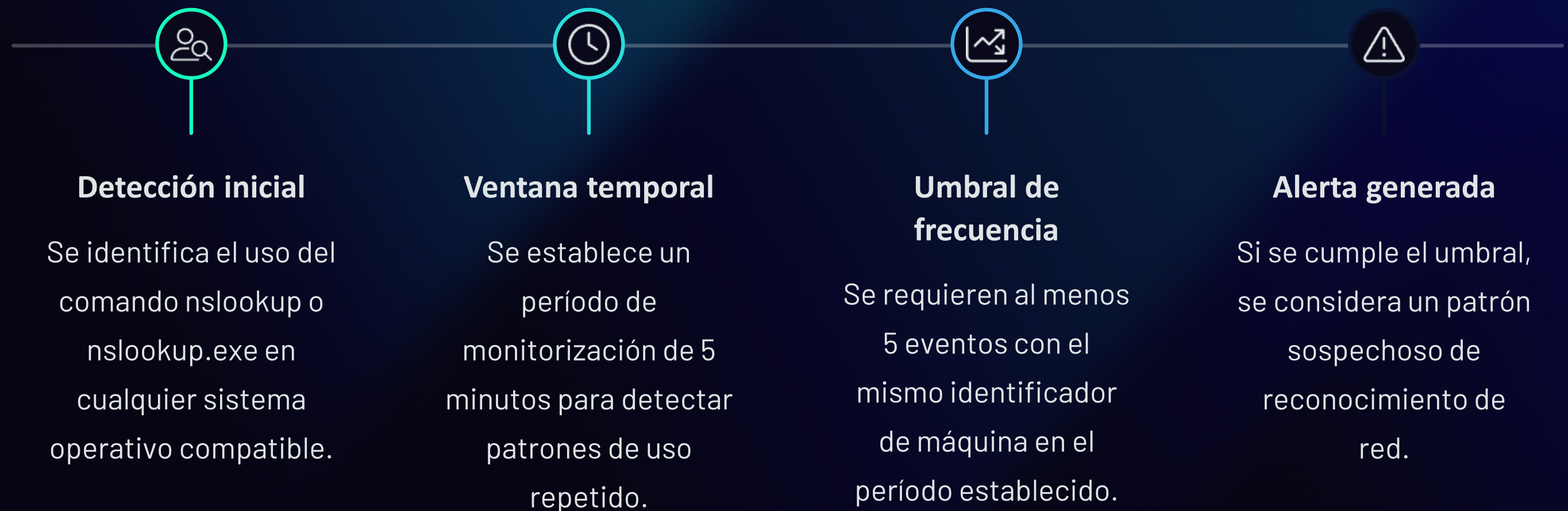
Comandos

Get-ChildItem con opción -Recurse o
bucles ForEach

Este criterio detecta actividades de descubrimiento de directorios en sistemas Windows utilizando PowerShell. La regla monitoriza específicamente el uso del cmdlet Get-ChildItem (alias dir o ls en PowerShell) con la opción -Recurse, o construcciones de bucle ForEach que iteran a través de directorios para enumerar su contenido.

El descubrimiento de directorios es una técnica común en la fase de reconocimiento de un ataque, donde los adversarios intentan mapear la estructura de archivos del sistema para identificar datos valiosos, configuraciones sensibles o posibles vectores de ataque adicionales. La detección temprana de estas actividades puede ayudar a prevenir el acceso no autorizado a información sensible.

Uso repetido de Nslookup



Este criterio detecta el uso repetido de la herramienta nslookup, que se utiliza para consultar servidores DNS y obtener información sobre dominios y direcciones IP. La regla se activa cuando se detectan al menos 5 usos de nslookup desde la misma máquina en un período de 5 minutos.

El uso frecuente de nslookup puede indicar actividades de reconocimiento de red, donde un atacante intenta identificar sistemas, servicios o infraestructura dentro de la red comprometida o en redes externas. Este comportamiento es particularmente sospechoso cuando ocurre en sistemas que normalmente no realizan este tipo de consultas.

Eliminación de varios archivos en el sistema de endpoints

Sistemas Monitorizados

Windows, Linux, HP-UX, Solaris, AIX, Mac OS X, IBM i y otros sistemas operativos compatibles con el registro de eventos de seguridad.

Categoría del Evento

System.File Deleted, que captura específicamente las operaciones de eliminación de archivos en el sistema de archivos.

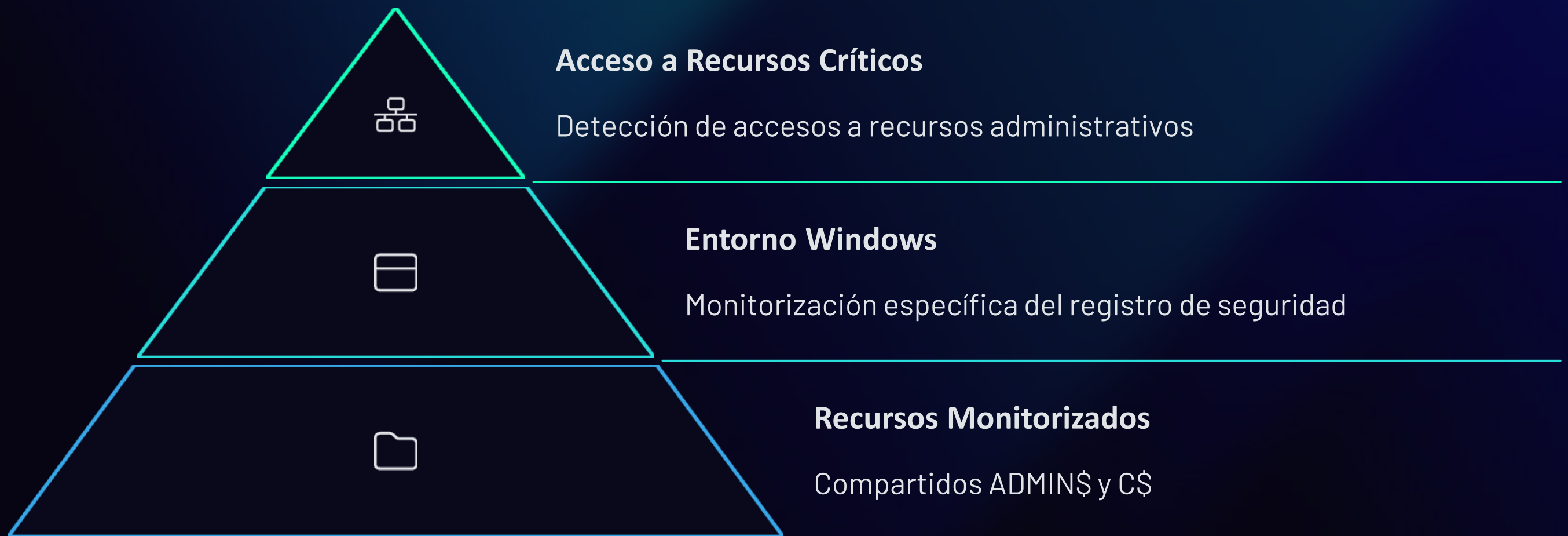
Umbral de Detección

Al menos 3 eventos de eliminación de archivos desde la misma máquina en un período de 10 minutos, excluyendo archivos temporales específicos.

Este criterio detecta la eliminación de múltiples archivos en sistemas de punto final. La regla monitoriza eventos de la categoría System.File Deleted y se activa cuando se detectan al menos 3 eliminaciones de archivos desde la misma máquina en un período de 10 minutos, excluyendo ciertos tipos de archivos temporales o de respaldo.

La eliminación masiva de archivos puede indicar intentos de destrucción de evidencia, actividades de limpieza después de un ataque, o incluso ataques de ransomware que eliminan los archivos originales después de cifrarlos. Este comportamiento es particularmente sospechoso cuando ocurre después de otras actividades anómalas en el sistema.

Acceso a recurso compartido administrativo



Este criterio detecta accesos a recursos compartidos administrativos en sistemas Windows. La regla monitoriza específicamente el QID 5001108, que corresponde a eventos de auditoría exitosa de acceso a objetos de recursos compartidos de red, centrándose en los recursos ADMIN\$ y C\$.

Los recursos compartidos administrativos son puntos de acceso privilegiado que permiten la administración remota de sistemas Windows. El acceso a estos recursos requiere credenciales administrativas y puede indicar movimiento lateral dentro de una red, administración remota legítima, o acceso no autorizado con credenciales comprometidas de alto privilegio.

Actividades sospechosas en puntos finales

El segundo componente principal de la regla de correlación es "Actividades sospechosas en puntos finales". Este bloque define una amplia gama de comportamientos potencialmente maliciosos que, cuando van seguidos de tareas administrativas, pueden indicar un compromiso de seguridad.

Entre las actividades sospechosas monitorizadas se incluyen: comunicación con hosts potencialmente hostiles, descubrimiento de actividades de volcado de credenciales, modificación de permisos de archivos críticos, desactivación de herramientas de seguridad, detección de indicadores de compromiso maliciosos, posible secuestro de DLL o COM, enmascaramiento de procesos, comportamientos asociados con ransomware, y muchas otras técnicas utilizadas comúnmente por atacantes.

La detección de estas actividades, especialmente cuando van seguidas de acciones administrativas en el mismo sistema, proporciona una señal de alerta temprana de posibles compromisos de seguridad que requieren investigación inmediata.



Actividades sospechosas en puntos finales

Este componente define las actividades consideradas sospechosas en endpoints, que cuando son seguidas por tareas de administración, activan la regla de correlación avanzada. Estas actividades son indicativas de posibles compromisos de seguridad y requieren atención inmediata.



Sistemas operativos

Las actividades sospechosas pueden detectarse en múltiples sistemas operativos, incluyendo Microsoft Windows, Linux, Unix, Solaris, AIX, Mac OS X e IBM i.



Reglas de correlación

Se aplican numerosas reglas específicas para identificar comportamientos sospechosos, desde comunicación con hosts potencialmente hostiles hasta detección de ransomware.



Indicadores de compromiso

El sistema busca IOCs maliciosos, comportamientos de herramientas como Cobalt Strike, y patrones de actividad asociados con amenazas conocidas.

Reglas de correlación específicas

Las reglas de correlación específicas para actividades sospechosas abarcan un amplio espectro de comportamientos maliciosos potenciales, desde comunicaciones con hosts hostiles hasta indicadores de ransomware y herramientas de ataque conocidas.



Estas reglas incluyen detección de comunicación con hosts potencialmente hostiles, actividades de volcado de credenciales, modificación de permisos de archivos críticos, desactivación de herramientas de seguridad, detección de IOCs maliciosos, posible secuestro de COM o DLL, enmascaramiento de procesos, comportamientos de ransomware como Maze o REvil, y uso de herramientas de reconocimiento, entre muchas otras amenazas específicas.

MNEMO

NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD



FUENTES DE DATOS
CIBER ANALÍTICA

Tabla de contenido

Contenido

CONTENIDO DE ESTE DOCUMENTO.....	4
ALCANCE.....	4
FUENTES DE INFORMACIÓN CYBER ANÁLITICA	5
1.1 Proceso ingesta archivos en SFTP:.....	5
1.2 Proceso normalización datos del SFTP:	9
1.3 Proceso de definición de tablas desde el origen del SFTP:.....	11
1.3.1 DAM :.....	16
1.3.2 Gobernanza:	18
1.3.3 PAM :	20
1.4 Proceso ingesta Tablas Postgres:.....	22
1.4.1 FNA_Fuentes	23
1.4.2 Fuente Vigilancia - vigcredencialesemp	24
1.4.3 Fuente Vigilancia - vigcredencialesterceros	27
1.4.4 Fuente Vigilancia - vigdominios.....	29
1.4.5 Fuente Vigilancia – vigrss.....	31
1.4.6 Fuente Vigilancia - vigmediosdigitales	33
1.4.7 Fuente Malware Lab - alertaspreventivas.....	35
1.4.8 Fuente Malware Lab - alertastempranas	37
1.4.9 Fuente Evaluación de Seguridad	39
1.4.10 Fuente Análisis de código.....	41
1.4.11 Fuente Protección de Endpoints / En la Nube / Web / SandBox.....	43
1.4.12 Fuente XDR.....	44
1.4.13 Fuente SOAR	46
1.4.14 Fuente WAF – waf_attack.....	49
1.4.15 Fuente WAF – events waf	51
1.4.16 Fuente IPS	53
1.4.17 Fuente DNS.....	55
1.4.18 Fuente NDR	57

- 1.4.19 Fuente Seguridad de Correo Electrónico 59
- 1.4.20 Fuente Cifado 62
- 1.4.21 Fuente Inteligencia de Amenazas : 64
- 1.5 Tablas almacenadas en HDFS: 67

CONTENIDO DE ESTE DOCUMENTO

En el ámbito de la analítica de ciberseguridad, la ingesta y procesamiento de fuentes de datos representa la primera etapa crucial para desarrollar casos de uso con impacto estratégico. Este documento se centra en describir los procesos, herramientas, y configuraciones establecidos para la captura, normalización y almacenamiento inicial de datos desde diversas fuentes, como archivos en SFTP, tablas en PostgreSQL y APIs externas. Estas fuentes proveen información esencial que sirve como base para la construcción de casos de uso actuales y futuros, asegurando que los datos ingresados estén listos para análisis avanzado, correlación de eventos y monitoreo en tiempo real.

ALCANCE

El objetivo de este documento es detallar los flujos de trabajo diseñados para la ingesta de fuentes de datos requeridas en la plataforma de analítica. El alcance incluye la orquestación de procesos integrales que abarcan desde la extracción inicial hasta el almacenamiento optimizado en un entorno HDFS, proporcionando información estructurada y transformada en formatos eficientes como Parquet. Estas actividades aseguran la calidad, integridad y disponibilidad de los datos para las distintas aplicaciones de ciberseguridad.

Los aspectos principales cubiertos en este documento incluyen:

Extracción de fuentes SFTP: Procesos escalables para la captura de grandes volúmenes de datos en formato JSON mediante workflows organizados por particiones diarias.

Normalización de datos: Transformación de datos no estructurados a representaciones tabulares para facilitar su posterior uso en big data.

Definición de tablas y almacenamiento: Filtrado, estructuración y escritura de datos en tablas clasificadas según las distintas áreas funcionales (SOC, DAM, Gobernanza, etc.), optimizando su disponibilidad en un sistema centralizado dentro del HDFS.

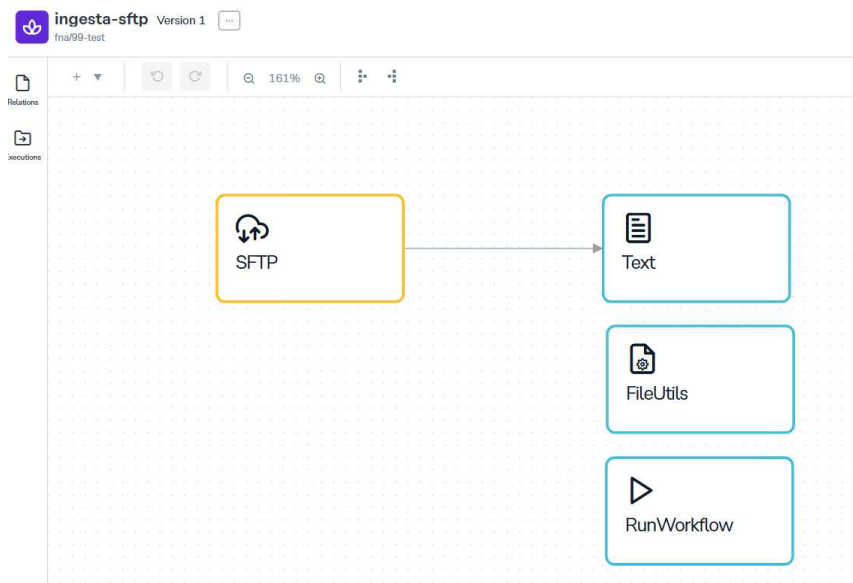
Conexión a bases de datos Postgres: Ingesta de tablas mediante módulos de descubrimiento, virtualización y persistencia, asegurando compatibilidad e integración en la plataforma.

Consumo de APIs externas: Captura de datos relevantes de inteligencia de amenazas en tiempo real para su análisis, almacenaje y aplicación en otros sistemas de la plataforma.

FUENTES DE INFORMACIÓN CYBER ANÁLITICA

1.1 Proceso ingesta archivos en SFTP:

En el SFTP existe un proceso que dispone la información diaria en chunks de información lo que por cada cierta cantidad de información se dispone un archivo .txt pero que internamente en la información su estructura es un formato JSON. Dada la cantidad de información diaria, los archivos diarios se dividen en 10 Sub-Carpetas para dejar una carga a la hora de llevar la información a la plataforma de Stratio. Por lo que cada carpeta es un Workflow independiente, a continuación, se mostrará el flujo y su funcionamiento:



La caja SFTP contiene la información de la ubicación de las Sub-carpetas desde donde extraeremos la información.

×

Input - SFTP

Name and description

Configuration

GenAI metadata

Security

Schema

Execution

Writer (1)

SFTP File Type *

TXT

SFTP Host *

172.16.132.67

SFTP Port *

22

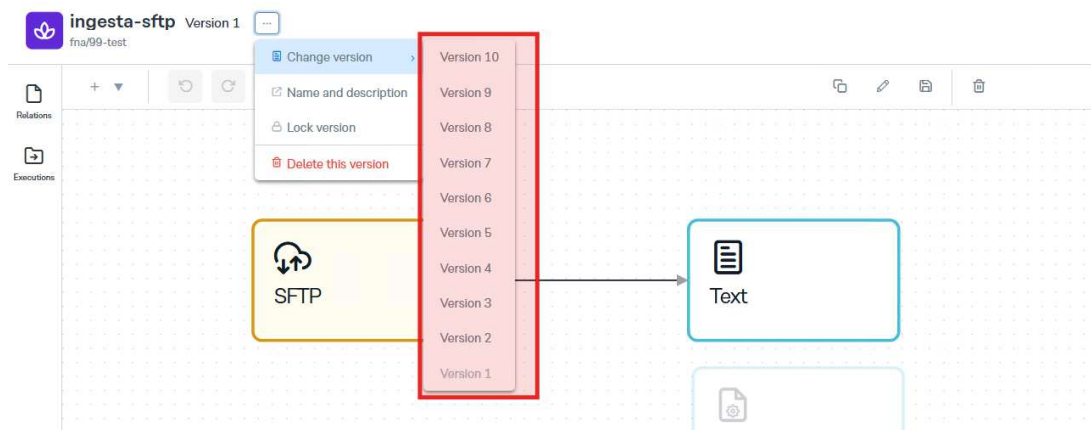
SFTP Path *

/C:/opt/output/20250414/01/

☐ Don't use HDFS for temporary files

Aquí debemos configurar el tipo de archivos que vamos a extraer, la IP , el puerto y la ruta/directorio en el SFTP donde se encuentran almacenados los archivos en este caso cómo tenemos la siguiente ruta “/C:/opt/output/20250414/01/” observamos que es de la fecha 2025-04-14 y que es la partición 01 de ese día.

Cómo debíamos replicar este mismo ejercicio para los otros 9 lo que se hizo fue versionar el Workflow y cada versión contiene su correspondiente partición.



La caja del SFTP también posee un componente de seguridad donde se almacenan las credenciales de la conexión :

×

Input - SFTP

Name and description

Configuration

GenAI metadata

Security

Schema

☐ TLS enabled

☐ User/pass from Vault enabled

Username

Password

Por cuestiones de seguridad en esta documentación no se dejan visibles pero en la plataforma quedarán usables y configurables por los desarrolladores.

Por último, del nodo SFTP surge una conexión hacia una caja de tipo OUTPUT de TXT. Que se encargará de enviar la información extraída del SFTP en el HDFS de la plataforma de Stratio. Aquí tenemos que considerar dos puntos clave, en la caja SFTP tenemos la opción de escritura (writer) que es donde le vamos a dar un nombre a la tabla :

×

Input - SFTP

Name and description

Configuration

GenAI metadata

Security

Schema

Execution

Writer (1)

Debug

▼ Text

Table name

20250414

Discard table name

Save mode *

Overwrite

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

En este caso el nombre de la tabla será 20240414 , además cómo es el primer flujo que se ejecuta este ejecuta en modo overwrite es decir sobre-escritura (borra todo lo que tiene y empieza de nuevo con lo que se guarda) en las siguientes versiones del workflow se tiene este parámetro en append dado que queremos apilar más información.

Ahora buen la ruta en donde será guardada la tabla se encuentra en la caja de TXT

×

Output - Text

Name and description

Configuration

Schema

Execution

Path *

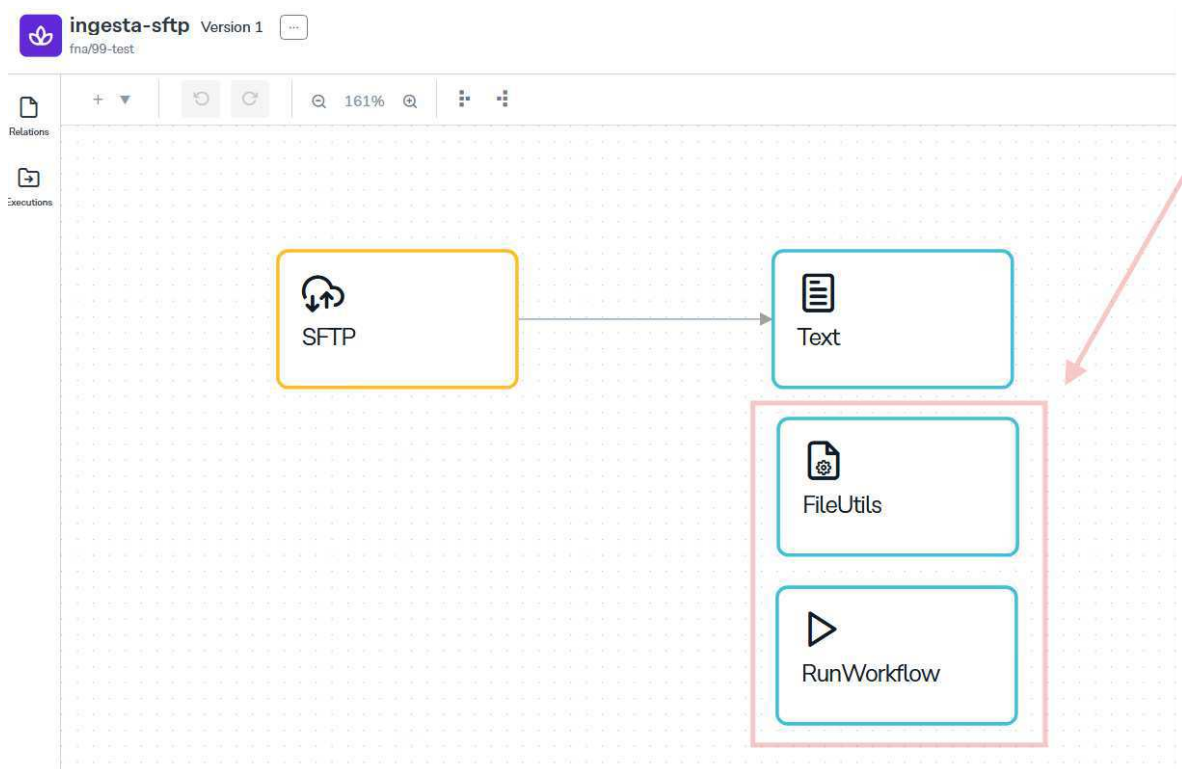
/test/logs_orig/

Text save properties

+

Add element

Por último dado que la extracción del SFTP requiere que se copien inicialmente los datos para luego se cargados se crean unas copias temporales para lo que utilizaremos el nodo de FileUtils para hacer que una vez finalizado el workflow se encargue de borrar las temporales (Dado que cuando se extraigan los nuevos datos no va a dejar descargarlos)

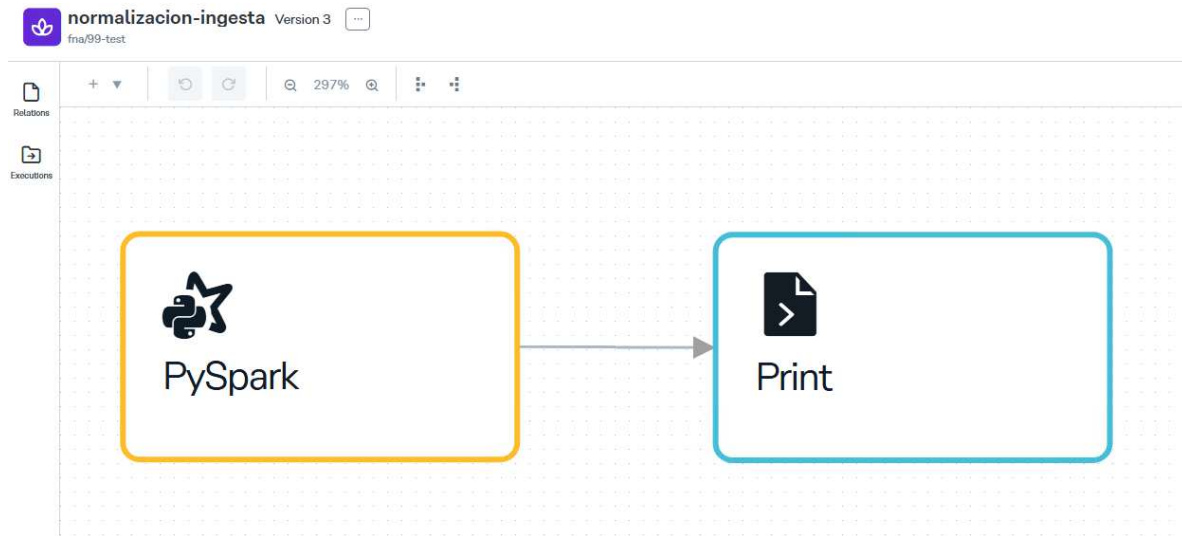


Por último, necesitamos encadenar las ejecuciones para que cuando finalice una inicie la otra y eso lo logramos con la caja de RunWorkflow. Donde el siguiente flujo a ejecutarse será la versión 2, y así sucesivamente cada flujo llevará al siguiente :

La configuración es muy sencilla, el envía la ejecución del flujo siguiente una vez finalice el actual y en los parámetros le decimos que debe heredar las características de Spark y de parámetros que el primer flujo utilizó.

1.2 Proceso normalización datos del SFTP:

Una vez los datos se ingestan en la plataforma debemos llevar la información a un formato tabular y almacenado en un formato más optimizado para big data (Parquet) por lo que se ejecuta un proceso con Pyspark para leer los txt como archivos JSON e ir dando forma tabular a los datos que se requieren:



Al inicio se solicita al proceso leer el HDFS y listar los archivos .TXT en la carpeta indicada :

×

Input - PySpark

□

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

PySpark input function *

```

1 from pyspark.sql import *
2 from pyspark.sql.functions import *
3 from pyspark.sql.types import *
4 from pyspark.sql.functions import regexp_extract, regexp_replace, col, get_json_object
5 from pyspark.sql.types import StructType, StructField, StringType, IntegerType
6
7
8 def pyspark_input(spark, param_dict):
9     """
10     :param spark: SparkSession
11     :param param_dict: Input dictionary
12     :return: Valid DataFrame
13     """
14
15     # 1. Configuración inicial: HDFS y listado de ficheros
16     hadoop_conf = spark._sc._jsc.hadoopConfiguration()
17     fs = spark._sc._jvm.org.apache.hadoop.fs.FileSystem.get(hadoop_conf)
18     stat = fs.listStatus(spark._sc._jvm.org.apache.hadoop.fs.Path("/test/logs_orig/20250414"))
19     files = [s.getPath().toString() for s in stat if s.getPath().toString().endswith(".txt")]
20
21     # 2. Datos de salida
22     output_path = "hdfs://hdfs.fnacyber-datastores/fna/fuentes/ORIGEN/TABULAR_borrar"
23
24     # 4. Definir mapeo de campos JSON a columnas
25     fields = [
26         ("type", "$.type"),
27         ("category", "$.category"),
28         ("protocolID", "$.protocolID"),
29         ("sev", "$.sev"),
30         ("enc", "$.enc")
31     ]

```

Luego definimos los nombres que le daremos a los campos y su ubicación en el JSON :

4. Definir mapeo de campos JSON a columnas

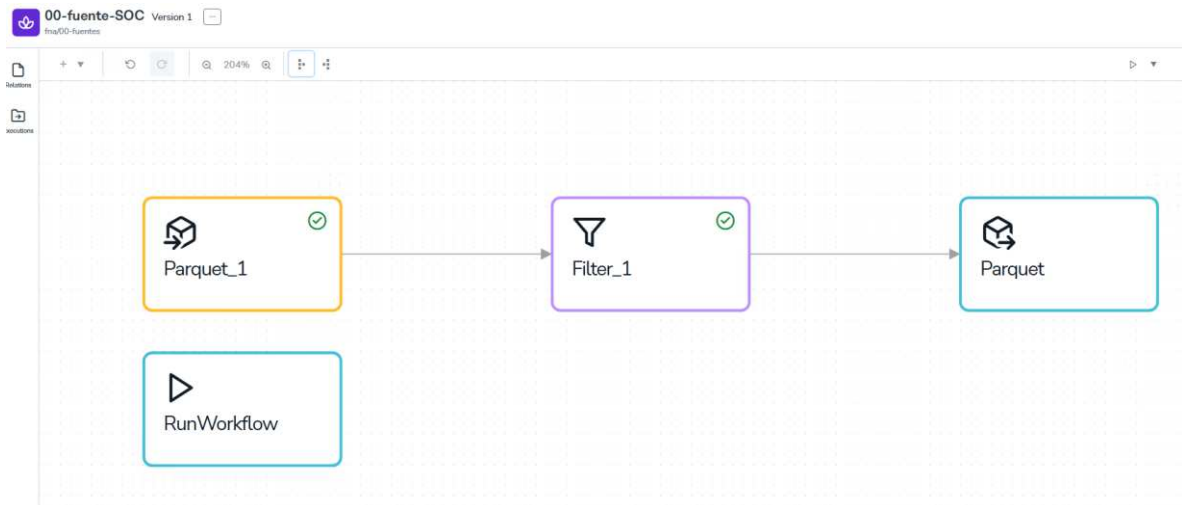
```
fields = [
    ("type", "$.type"),
    ("category", "$.category"),
    ("protocolID", "$.protocolID"),
    ("sev", "$.sev"),
    ("src", "$.src"),
    ("dst", "$.dst"),
    ("srcPort", "$.srcPort"),
    ("dstPort", "$.dstPort"),
    ("relevance", "$.relevance"),
    ("credibility", "$.credibility"),
    ("startTimeEpoch", "$.startTimeEpoch"),
    ("startTimeISO", "$.startTimeISO"),
    ("storageTimeEpoch", "$.storageTimeEpoch"),
    ("storageTimeISO", "$.storageTimeISO"),
    ("devTimeEpoch", "$.devTimeEpoch"),
    ("devTimeISO", "$.devTimeISO"),
    ("srcPreNATPort", "$.srcPreNATPort"),
    ("dstPreNATPort", "$.dstPreNATPort"),
    ("srcPostNATPort", "$.srcPostNATPort"),
    ("dstPostNATPort", "$.dstPostNATPort"),
    ("hasIdentity", "$.hasIdentity"),
    ("eventCnt", "$.eventCnt"),
    ("srcIPLoc", "$.srcIPLoc"),
    ("dstIPLoc", "$.dstIPLoc"),
    ("hasOffense", "$.hasOffense"),
    ("domainID", "$.domainID"),
    ("eventName", "$.eventName"),
    ("lowLevelCategory", "$.lowLevelCategory"),
    ("highLevelCategory", "$.highLevelCategory"),
    ("eventDescription", "$.eventDescription"),
    ("logSource", "$.logSource"),
```

Por último se realiza una limpieza de la información y nos centramos para leer el json en un formato entendible para usar las definiciones anteriores para extraer los datos y así poder crear una tabla que podremos ir añadiéndole registros hasta crear nuestra tabla completa permitiendo guardarlo en la ruta indicada e el HDFS como un append a la tabla TABULAR en formato Parquet.

Al final, se realiza una limpieza de la caché y los objetos para no llenar la memoria y que el proceso pueda finalizar sin problemas.

1.3 Proceso de definición de tablas desde el origen del SFTP:

Luego de tener la información de los logs provenientes del SFTP en formato tabular, se definieron una serie de filtros para definir algunas de las tablas de interés :



Este tipo de flujos tienen la misma estructura lo único que cambia es el filtro, la ruta donde se almacenan y el nombre de la tabla:

El parquet es donde se encuentra almacenada la información

×
Input - Parquet_1

Name and description

Configuration

GenAI metadata

Schema

Execution

Debug

Path *

/fna/fuentes/ORIGEN/TABULAR

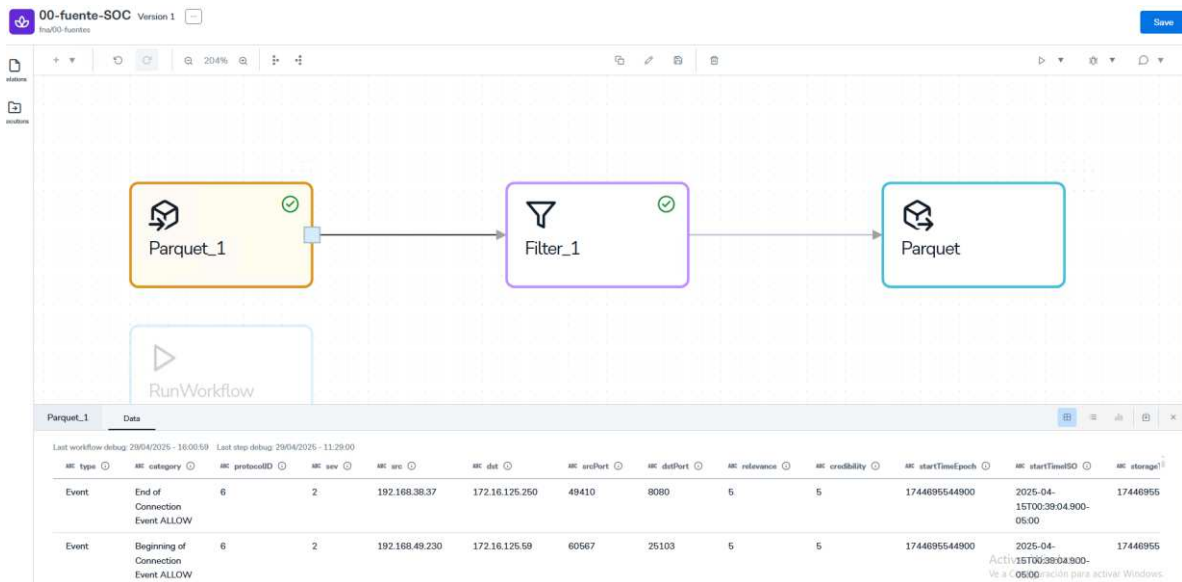
Read mode

☒ Default
 ☐ Document

Optional properties

[⊕ Add element](#)

Aquí vemos que en la ruta /fna/fuentes/ORIGEN/ se encuentra la tabla llamada TABULAR , tenemos una vista preliminar si ejecutamos el debug de la plataforma :



El Filter es un filtro a nivel Spark SQL :

Transformation - Filter_1

Schemas

- Parquet_1

Filter expression

```

1 logSourceType == 'Cisco Firepower Threat Defense' AND
2 logSource in ( 'BOGPFVPCP001_172.31.1.96_FW_BORDER-1', 'BOGPFVPCP003_172.31.1.98_FW_SERVIDORES1',
3               'BOGPFVPCP002_172.31.1.102_FW_VPN', 'CiscoFirepowerThreatDefense @ 172.31.1.101',
4               'CiscoFirepowerThreatDefense @ 172.31.1.97 _FW_BORDER-2', 'CiscoFirepowerThreatDefense @ 172.31.1.99')

```

☐ Quote automatically sql sentence before execution

Configuration

- GenAI metadata
- Schema
- Execution
- Writer (1)
- Debug

En este Filter al ser el penultimo nodo, aquí se debe definir en la opción Writer el nombre de la tabla en formato Overwrite:

×

Transformation - Filter_1

Name and description

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Debug

▼ Parquet

Table name

SOC

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

Luego tenemos el Output de Parquet donde definiremos la ruta donde se almacenará la tabla :

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/

Parquet save properties

⊕ Add element

Finalmente, tenemos el RunWorkflow que encarga de lanzar el siguiente flujo de la lista (lo que nos permite automatizar el proceso).

A continuación veamos que los datos están almacenados en formato parquet en el HDFS de la plataforma en la ruta “/fna/fuentes/SOC”

RocketProjectsCatalogFile BrowserIntelligence

File Browser

Filter file or directory...

Upload fileNew folder

/ fna / fuentes / SOC

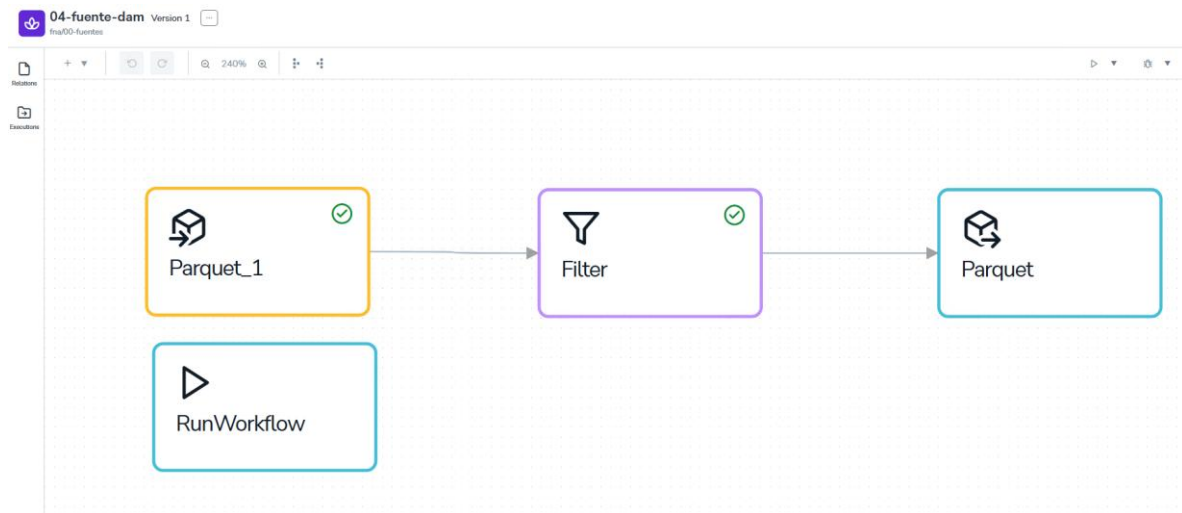
	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.84 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:12
☐	part-00001-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.66 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:22
☐	part-00002-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.65 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:29
☐	part-00003-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.27 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:39
☐	part-00004-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.28 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:47
☐	part-00005-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	9.9 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:02:55
☐	part-00006-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	9.69 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:03:03
☐	part-00007-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	10.05 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:03:10
☐	part-00008-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	9.82 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:03:19
☐	part-00009-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	9.82 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:03:26
☐	part-00010-216f54f2-63dc-4280-878d-048a607208db-c...	parquet	9.4 MB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:03:35

También tenemos una vista de los datos de SOC :

id	id: domainID	id: eventName	id: lowLevelCategory	id: highLevelCategory	id: eventDescription	id: logSource	id: srcNetName	id: dstNetName	id: logSourceType
0		End of Connection Event Allow	Firewall Permit	Access	End of Connection Event was allowed.	BOGFFFWCP003_172.31.1.98_FW_SERVIDORES1	RED_FNA.RED_FNA	RED_FNA.RED_FNA	Cisco Firepower Threat Defense
0		Beginning of Connection Event Allow	Firewall Permit	Access	Beginning of Connection Event was allowed.	BOGFFFWCP003_172.31.1.98_FW_SERVIDORES1	RED_FNA.RED_FNA	RED_FNA.RED_FNA	Cisco Firepower Threat Defense
0		No matching connection for ICMP	Suspicious ICMP Protocol Usage	Suspicious Activity	ICMP error packets were dropped by the security appliance because the ICMP error messages are not related to any session already established in the security appliance.	BOGFFFWCP003_172.31.1.98_FW_SERVIDORES1	RED_FNA.RED_FNA	RED_FNA.RED_FNA	Cisco Firepower Threat Defense
0		Built translation	Firewall Session Opened	Access	A TCP, UDP, or ICMP address translation slot was created. The slot translates the source socket from the local side to the global side. In reverse, the slot	CiscoFirepowerThreatDefense @ 172.31.1.97_FW_BORDE-2	RED_FNA.RED_FNA	other	Cisco Firepower Threat Defense

Para este tipo de flujos tenemos a la fuente SOC que es la que vimos en el ejemplo, pero también tenemos :

1.3.1 DAM :



Donde el origen de los datos es el mismo (los logs del SFTP) pero se aplica un filtro correspondiente a los datos de DAM :

×

Transformation - Filter

Name and description

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Debug

Schemas

▶ Parquet_1

Filter expression

```

1 logSourceType == 'SafeNet DataSecure/KeySecure' AND
2 logSource in ( 'BOGPVPLP00E_172.16.132.87_IBM_GUARDIUM',
3               'BOGPVPLP00F_172.16.132.88_IBM_GUARDIUM' )

```

☐ Quote automatically sql sentence before execution

Para el almacenamiento (Output) no solo debemos definir la ruta sino también el nombre de la tabla, en este caso la tabla se llamará DAM y se reescribirá la tabla cada vez que el flujo sea ejecutado.

×

Transformation - Filter

Name and description

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Debug

▼ Parquet

Table name

DAM

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By ('.' separated)

Number of partitions

List of columns for repartition

Y la ruta donde se almacenará la tabla :

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/

Parquet save properties

⊕ Add element

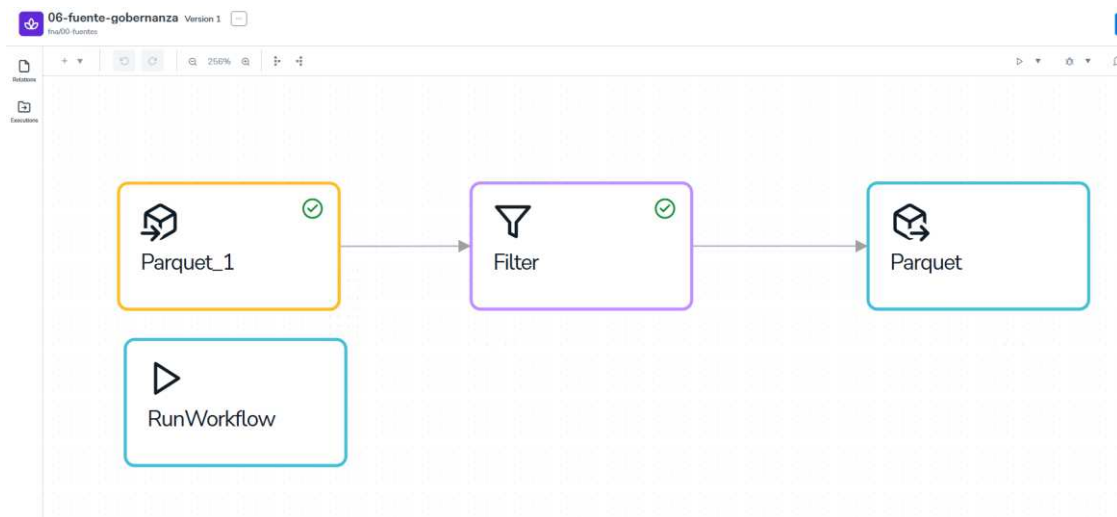
Ahora validemos que existan datos en la tabla dentro del HDFS :

File Browser							
Filter file or directory...							
fna / fuentes / DAM							
☐	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.84 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:51
☐	part-00001-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.95 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:52
☐	part-00003-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.9 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:53
☐	part-00004-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.76 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:54
☐	part-00005-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.89 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:54
☐	part-00006-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.68 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:55
☐	part-00007-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.11 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:56
☐	part-00008-61805b33-f7eb-4e6b-857a-1b1a7f5e505f-c0...	parquet	11.81 KB	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:50:56

Por último, demos una vista a los datos de la tabla:

src_domainID	src_eventName	src_lowLevelCategory	src_highLevelCategory	src_eventDescription	src_logSource	src_srcNetName	src_dstNetName	src_logSourceType
0	unknown	Unknown	Unknown	unknown	BOGPVPLP00E_172.16.132.87_IBM_GUARDIUM	RED_FNA.RED_FNA	RED_FNA.RED_FNA	SafeNet DataSecure/KeySecure
0	Rol 1 Eliminacion Usuarios	Asset User Deleted	Asset Profiler	Rol 1 Eliminacion Usuarios	BOGPVPLP00E_172.16.132.87_IBM_GUARDIUM	RED_FNA.RED_FNA	RED_FNA.RED_FNA	SafeNet DataSecure/KeySecure
0	Rol 1 Eliminacion Usuarios	Asset User Deleted	Asset Profiler	Rol 1 Eliminacion Usuarios	BOGPVPLP00E_172.16.132.87_IBM_GUARDIUM	RED_FNA.RED_FNA	RED_FNA.RED_FNA	SafeNet DataSecure/KeySecure
0	Rol 1 Eliminacion Usuarios	Asset User Deleted	Asset Profiler	Rol 1 Eliminacion Usuarios	BOGPVPLP00E_172.16.132.87_IBM_GUARDIUM	RED_FNA.RED_FNA	RED_FNA.RED_FNA	SafeNet DataSecure/KeySecure

1.3.2 Gobernanza:



Donde el origen de los datos es el mismo (los logs del SFTP) pero se aplica un filtro correspondiente a los datos de Gobernanza:

Transformation - Filter

Schemas

Parquet_1

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Filter expression

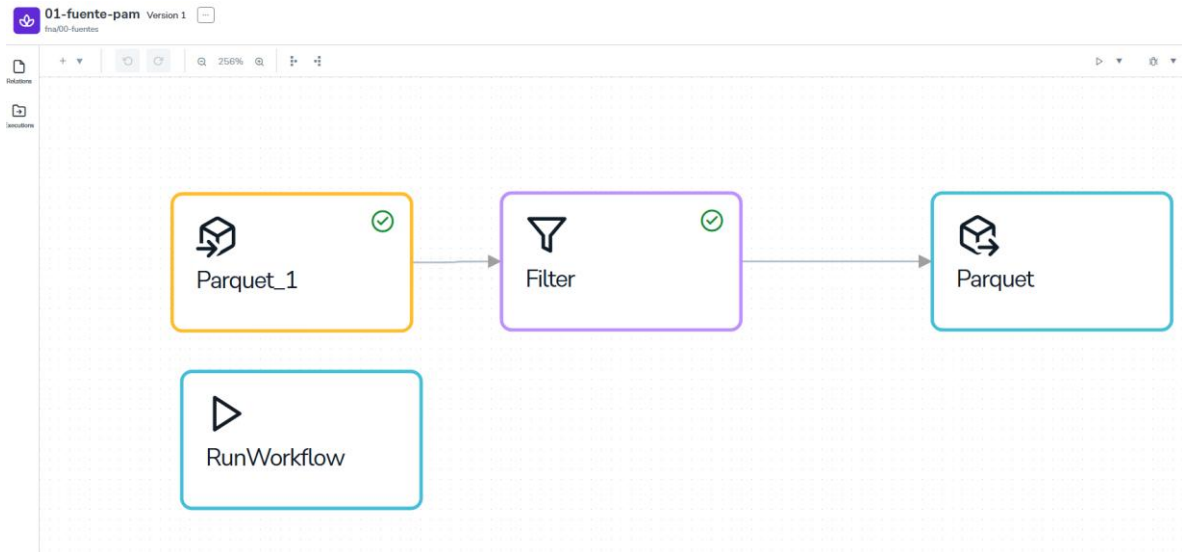
```
1 logSource in ( 'Forcepoint DLP - 172.16.127.84' )
```

☐ Quote automatically sql sentence before execution

Por último, demos una vista a los datos de la tabla GOBERNANZA:

IdentUserName	isoTimeFormat	LogSource	LogSourceGroup	LogSourceIdentifier	LogSourceType	LowLevelCategory	Name	Payload
	yyyy-MM-ddTHH:mm:ss.SSSZ	Forcepoint DLP - 172.16.127.84	FNA	172.16.127.84	Universal CEF	Unknown	DefaultProfile	CEF:0 Forcepoint Forcepoint DLP 10.2.0 2582301; phone=5731764341728;text=PARA+ACTIVAR+L/ype=phone_number&app_absent=0 frame=C Provoed Detection for Web File Uploads suser=Nefer , Endpoint HTTPS analyzedBy=Policy Engine FNAB tyType=MEDIUM sourceIp=VRE-PA-SMR-3403.7 00:28:27.181 destinationHosts=api.whatsapp.coi
	yyyy-MM-ddTHH:mm:ss.SSSZ	Forcepoint DLP - 172.16.127.84	FNA	172.16.127.84	Universal CEF	Unknown	DefaultProfile	CEF:0 Forcepoint Forcepoint DLP 10.2.0 2582432; phone=5731764341728;text=PARA+ACTIVAR+L/ype=phone_number&app_absent=0 frame=C Provoed Detection for Web File Uploads suser=Nefer , Endpoint HTTPS analyzedBy=Policy Engine FNAB tyType=MEDIUM sourceIp=VRE-PA-SMR-3403.7 05:28:27.181 destinationHosts=api.whatsapp.coi
	yyyy-MM-ddTHH:mm:ss.SSSZ	Forcepoint DLP - 172.16.127.84	FNA	172.16.127.84	Universal CEF	Unknown	DefaultProfile	Activar Windows CEF:0 Forcepoint Forcepoint DLP 10.2.0 2582607; hone=573172168014 frame=C User/igamboalD Web File Uploads suser=Rodrigo Isaac Gamba N

1.3.3 PAM :



Donde el origen de los datos es el mismo (los logs del SFTP) pero se aplica un filtro correspondiente a los datos de PAM:

×

Transformation - Filter

🔍

▼

Schemas

Name and description

►

Parquet_1

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Debug

Filter expression

```

1 logSourceType == 'Cyber-Ark Vault' AND
2 logSource in ( 'Cyber-Ark_Vault -172.16.132.138-BOGPVCHM008' )

```

☐ Quote automatically sql sentence before execution

Para el almacenamiento (Output) no solo debemos definir la ruta sino también el nombre de la tabla, en este caso la tabla se llamará PAM y se reescribirá la tabla cada vez que el flujo sea ejecutado:

×

Transformation - Filter

Name and description

Configuration

GenAI metadata

Schema

Execution

Writer (1)

Debug

▼ Parquet

Table name

PAM

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Y la ruta donde se almacenará la tabla :

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/

Parquet save properties

⊕ Add element

Ahora validemos que existan datos en la tabla dentro del HDFS :

File Browser							
Filter file or directory... Upload file							
📁 / fna / fuentes / PAM							
☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	16.95 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:11
☐	part-00001-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	16.2 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:14
☐	part-00002-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	17.31 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:15
☐	part-00003-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	16.17 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:17
☐	part-00004-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	16.11 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:18
☐	part-00005-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	17.07 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:19
☐	part-00006-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	18.11 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:20
☐	part-00007-35f196b-ea85-4249-9170-bb0632801845-c...	parquet	15.87 KB	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:21

Por último, demos una vista a los datos de la tabla PAM:

EventName	LowLevelCategory	HighLevelCategory	EventDescription	LogSource	SrcNetName	DestNetName	LogSourceType	
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Set Password - Cyber-Ark	Password Change Succeeded	Authentication	Set Password - Cyber-Ark	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Set Password - Cyber-Ark	Password Change Succeeded	Authentication	Set Password - Cyber-Ark	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot
Open File - Cyber-Ark	FileTransfer Opened	Application	Cyber-Ark identifica la apertura de un archivo	Cyber-Ark_Vault -172.16.132.138-BOGPVCNWP00B	RED_FNA,RED_FNA	RED_FNA,RED_FNA	Cyber-Ark Vault	Ot

1.4 Proceso ingesta Tablas Postgres:

Para ingestar las tablas provenientes del postgres se orquestaron flujos por cada tabla para llevar el control y el orden de la información ingestada en la plataforma. La conexión se realizó desde el agente de autodescubrimiento que permite desde el módulo de Governance ver toda la información disponible en la base de datos y desde este mismo módulo se crean vistas técnicas con las tablas de interés que luego podrán ser consumida dentro de la plataforma como parte de una colección.

Vista de la metadata del postgres descubierta por el agente de autodescubrimiento.

Name	Alias	Type	Last updated
public.activos_criticos	--	Table	28 Apr 2025, 15:10
public.alertaspreventivas	--	Table	10 Apr 2025, 19:00
public.alertastempranas	--	Table	11 Apr 2025, 19:00
public.analisiscodigo	--	Table	24 Apr 2025, 10:37
public.analisisvuln	--	Table	09 Apr 2025, 19:00
public.correlacionavanzada	--	Table	25 Apr 2025, 19:00
public.events_casb	--	Table	24 Apr 2025, 10:37
public.events_cifrado	--	Table	23 Apr 2025, 19:00

Se creó una colección y en ella desde la vista técnica (Technial View) se agregaron las tablas de interés:

Asset name	Last updated
FNA_analytics	01 Apr 2025
FNA_cybersight	24 Mar 2025
FNA_data	01 Apr 2025
FNA_FUENTES	28 Apr 2025
shakedown_governance	13 Feb 2025

1.4.1 FNA_Fuentes

Dentro de esta colección se encuentra una gran cantidad de fuentes que hacen parte de los requerimientos iniciales, a continuación presentamos cada una de estas.

Vista de las tablas añadidas a la vista de negocio:

Asset Name	View Type	Last Updated
public_alertastempranas	Table view	15 Apr 2025,11:29
public_analisiscodigo	Table view	24 Apr 2025,10:42
public_analisisvuln	Table view	15 Apr 2025,11:34
public_correlacionavanzada	Table view	28 Apr 2025,15:13
public_criticidadactivos	Table view	28 Apr 2025,15:10
public_events_casb	Table view	24 Apr 2025,10:44
public_events_cifrado	Table view	24 Apr 2025,10:31
public_events_dns	Table view	24 Apr 2025,12:28
public_events_email	Table view	24 Apr 2025,10:32

Una vez las tablas se encuentran gobernadas, ya podemos hacer uso de ellas mediante el virtualizador de datos de la plataforma (mediante el catálogo en Rocket, en consultas desde Discovery o en ETLs desde los Workflows de Rocket). En este punto los datos no se encuentran aún persistidos, es decir, almacenados al interior de la plataforma y por ende cada consulta va directamente a la fuente origen y esta no es una buena práctica en el desarrollo de aplicaciones de datos. Por lo que por cada tabla se generó una ETL (Workflow) para persistir la información de dichas tablas en el HDFS de la plataforma.

En el proyecto fna de Rocket existe la carpeta 00-fuentes que contiene todos los Workflows correspondientes a estas ingestas alcanzando cerca de 30 tablas:

Assets

Search...

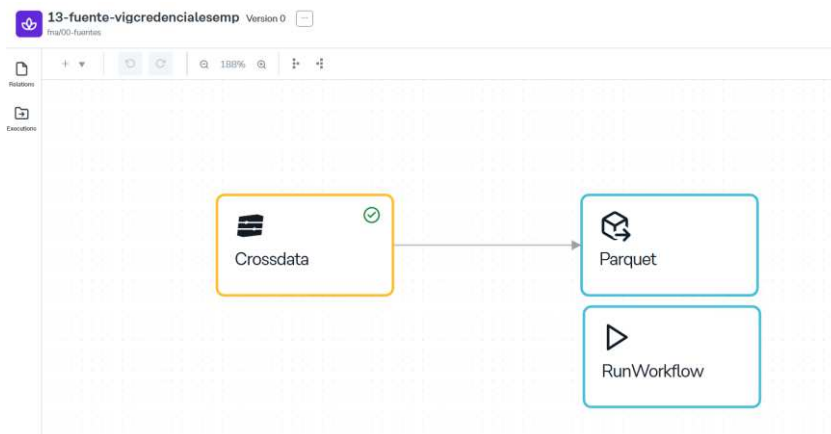
/ 00-fuentes

	Name	Type
☐	23-fuente-events_IPS	Hybrid
☐	24-fuente-analisiscodigo	Hybrid
☐	25-fuente-events_ndr	Hybrid
☐	26-fuente-events_email	Hybrid
☐	27-fuente-events_trendmicro	Hybrid
☐	28-fuente-events_xdr	Hybrid
☐	29-fuente-events_soar	Hybrid

Admin project

1.4.2 Fuente Vigilancia - vigcredencialesemp

Se va a explicar al detalle cada uno de los componentes de este tipo de Workflows para la primera tabla de VIGILANCIA llamada vigcredencialesemp , para el resto de tablas provenientes del postgres se explicará qué flujo es, las rutas, nombre de la tabla, la muestra de dónde quedaron almacenados los datos y una muestra de los datos:



Estos workflows se componen de 3 nodos un nodo Input, y dos nodos output . El nodo input lee los datos gobernados utilizado el virtualizador llamado crossdata , extrae la información enviándola hacia el HDFS en formato Parquet . El último nodo RunWorkflow se encarga de esperar a que este flujo finalice y lanza el siguiente en este caso lanza un flujo con la siguiente tabla a ingestar.

Veamos el nodo Crossdata :

En la opción writer estará el nombre de la tabla :

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

vigcredencialesemp

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/VIGILANCIA

Parquet save properties

[Add element](#)

Una vez ejecutado el Workflow veremos los datos en el HDFS que la fuente de VIGILANCIA se compone de 5 tablas:

/ fna / fuentes / VIGILANCIA

☐	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	vigapk	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:00:47
☐	vigcredencialesmp	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:01:27
☐	vigcredencialesterceros	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:02:17
☐	vigdominios	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:02:59
☐	vigmediosdigitales	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:03:46
☐	vigrrss	directory	-	execution-ident...	supergroup	rw-r-xr-x	29 Apr 2025 - 1:04:27

A continuación veamos que en la carpeta de la tabla vigcredencialesmp tenemos datos:

Rocket Projects Catalog File Browser Intelligence

File Browser

Filter file or directory...

/ fna / fuentes / VIGILANCIA / vigcredencialesmp

☐	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-e7145030-21a9-497a-ac08-9a7d79d2873e-c...	parquet	9.67 KB	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:01:27
☐	_SUCCESS	file	0 Bytes	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:01:28

Por último si queremos ver una muestra de los datos de la tabla vigcredencialesmp :

id	responsable_email	id_ticket	id_serie	id_mesa	id_fecha_email	id_usuario	id_url_path	id_origen	id_fuente
	Oscar Zambrano	98914	2024	Febrero	45329	fochoa@fna.gov.co	DESCONOCIDO	DeepWeb	Siglit
	Ramiro Ramirez	102537	2024	Marzo	45357	bsaboga@fna.gov.co	DESCONOCIDO	DeepWeb	Siglit
			2024	Marzo	45357	smolina@fna.gov.co	https://login.salesforce.com/	Deepweb	Siglit
			2024	Marzo	45357	smolina@fna.gov.co	https://login.salesforce.com/	Deepweb	Siglit
			2024	Marzo	45357	privera@fna.gov.co	https://wordpress.com/wp-login.php	Deepweb	Siglit
			2024	Marzo	45357	centrodemonitoreo@fna.gov.co	https://accounts.zohoportal.com/accounts/login	Deepweb	Siglit
			2024	Marzo	45357	lvalenzuela@fna.gov.co	https://login.microsoftonline.com/0f415027-a316-4731-b6b3-a40febe43cbc/auth/2/authenticate	Deepweb	Siglit
			2024	Marzo	45357	murreav@fna.gov.co	https://aprende.fna.gov.co	Deepweb	Siglit
	Ramiro Ramirez	104161	2024	Marzo	45389	fburbano@fna.gov.co	https://login.live.com/login.url	Deepweb	Siglit
			2024	Marzo	45389	fburbano@fna.gov.co	https://www.springstep.com/inicio-sesion	Deepweb	Siglit

Ahora veamos en el nodo RunWorkflow que se encarga de lanzar el siguiente flujo apenas finalice el actual:

×

Output - RunWorkflow

Name and description

Configuration

Execution

Run workflow when *

☐ Receive data

☒ After workflow ends

Asset to run

14-fuentes-vigcredencialesterceros - Latest version x

/home/fna/00-fuentes

Modify

Workflow version reference \${xxx} (less priority than asset selector when both are specified)

☐ Unique instance

Contexts

Add element

☐ Forward parent contexts

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

vigcredencialesterceros

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By ('', separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

Ruta de almacenado en el HDFS:

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/VIGILANCIA

Parquet save properties

[Add element](#)

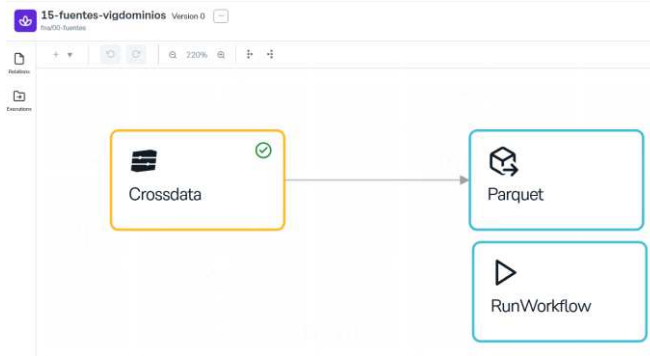
Veamos que los datos están almacenados en el HDFS :

File Browser							
Filter file or directory... Upload file							
🏠 / fna / fuentes / VIGILANCIA / vigcredencialesterceros							
☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-155d2287-e068-478f-ba22-3da24e951783-c...	parquet	68.55 KB	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 10:21:17
☐	._SUCCESS	file	0 Bytes	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 10:21:17

Por último, una vista a los datos ingestados:

#	id	REC numero	REC ticket	REC responsable_emulo	REC ano	REC mes	REC fecha_registro	REC usuario	REC url_path	REC origen	REC fuente	REC eorime	REC
2		5860	145831	Oscar Zambrano	2025	Enero	2025-01-04T05:00:00.000Z	79695838	fna.gov.co	Deep Web			B.
3		5861	145831	Oscar Zambrano	2025	Enero	2025-01-04T05:00:00.000Z	32649249	fna.gov.co	Deep Web			B.
4		5862	145831	Oscar Zambrano	2025	Enero	2025-01-04T05:00:00.000Z	52289338	www.fna.gov.co	Deep Web			B.
5		5863	145831	Oscar Zambrano	2025	Enero	2025-01-04T05:00:00.000Z	1013588270	www.fna.gov.co	Deep Web			B.

1.4.4 Fuente Vigilancia - vigdominios



Origen de los datos (Postgres) :

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_vigdominios

Definición del nombre de la tabla en el HDFS vigdominios, con la opción de reescritura cada vez que se ejecute el Workflow:

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

vigdominios

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

Ruta de almacenado en el HDFS:

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/VIGILANCIA

Parquet save properties

[Add element](#)

Veamos que los datos están almacenados en el HDFS :

File Browser

Filter file or directory...

📁 Upload file

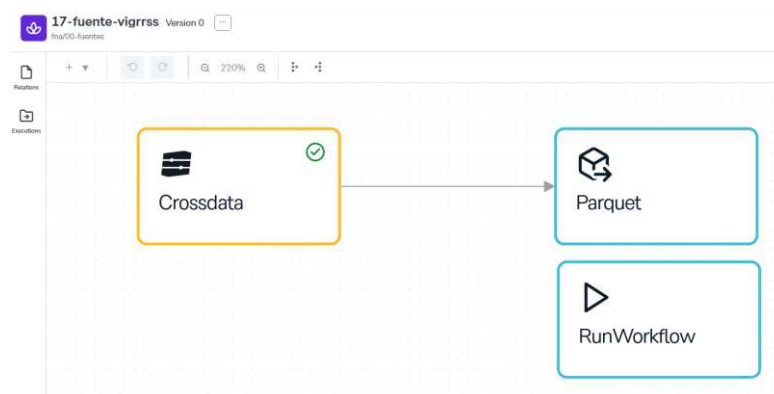
/ fna / fuentes / VIGILANCIA / vigdominios

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-5d96cc80-53e0-4c3c-993f-a78fe6de8fbd-c00...	parquet	5.64 KB	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:02:59
☐	._SUCCESS	file	0 Bytes	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:02:59

Por último, una vista a los datos ingestados:

# id	analista	ticket	mes	fecha_envio	dominio	tipo_dominio	e_crime	criticidad	calificacion
16	Ramiro Ramírez	130277	Septiembre	2024-09-22T14:54:33.890Z	fnaapp.net	Sospechoso		MEDIA	3
31	Camila Lozano	144604	Diciembre	2024-12-24T18:57:16.819Z	fna9.online	Sospechoso		MEDIA	3
2	Ramiro Ramírez	101600	Febrero	2024-02-28T10:12:57.746Z	fna.video	Sospechoso		MEDIA	3
32	David de Salvador	145922	Enero	2025-01-05T20:43:44.553Z	fna.me	Sospechoso		MEDIA	3
3	Ramiro Ramírez	109516	Abril	2024-04-21T12:24:00.110Z	fna.band	Sospechoso		MEDIA	3

1.4.5 Fuente Vigilancia – vigrss



×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_vigrrss

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

vigrss

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/VIGILANCIA

Parquet save properties

[Add element](#)

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

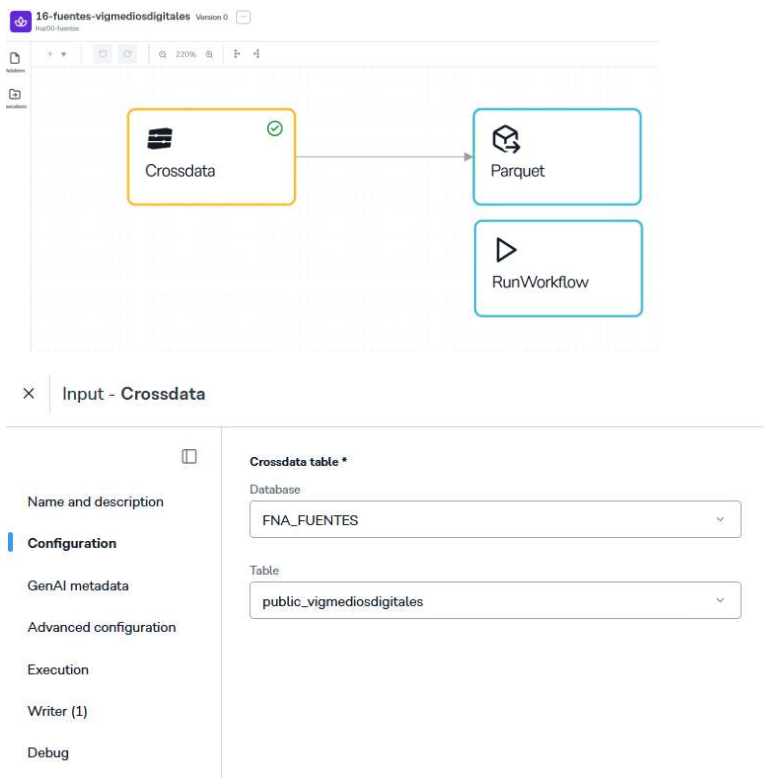
📁

Upload file

🏠 / fna / fuentes / VIGILANCIA / vigrss

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-994b1f8b-8e74-4328-aad1-3ccb4e79b239-c...	parquet	26.09 KB	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:04:27
☐	_SUCCESS	file	0 Bytes	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:04:27

1.4.6 Fuente Vigilancia - vigmediosdigitales



✕

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

vigmediosdigitales

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

✕

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/VIGILANCIA

Parquet save properties

⊕ Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

Upload file

/ fna / fuentes / VIGILANCIA / vigmediosdigitales

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-1ab42524-e069-4e30-b58f0a1fef11-c0...	parquet	17.85 KB	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:03:46
☐	._SUCCESS	file	0 Bytes	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:03:46

url_path

https://caracol.com.co/2025/01/14/credito-vivienda-para-independientes-en-fna-que-papeles-pidon-prestan-hasta-1298-millones/

descripcion

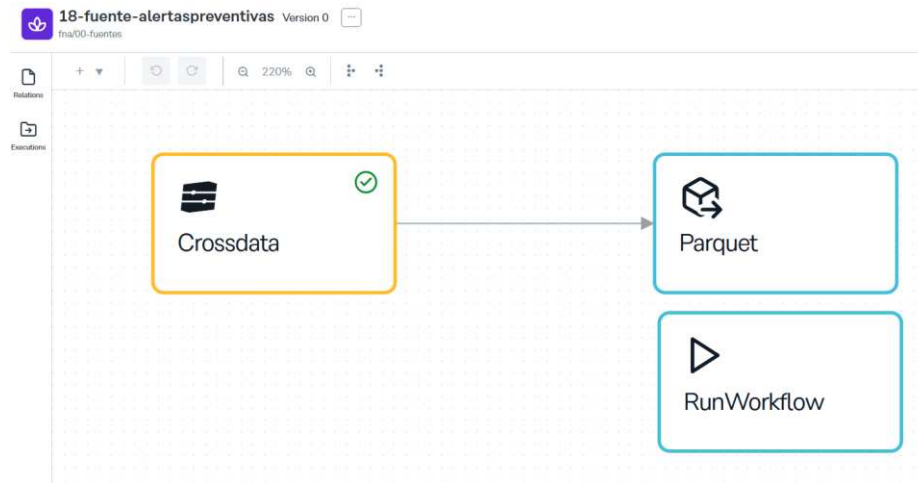
Artículo publicado por el medio "Caracol Radio", donde informa que el Fondo Nacional del Ahorro (FNA) ofrece créditos para vivienda dirigidos tanto a empleados como a independientes, permitiendo "la compra de vivienda nueva o usada, construcción, mejoras o compra de cartera". Los préstamos

tags

Mencion de marca

extra

1.4.7 Fuente Malware Lab - alertaspreventivas



× Input - Crossdata

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_alertaspreventivas

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

alertaspreventivas

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path*

/fna/fuentes/MALWARE_LAB

Parquet save properties

[Add element](#)

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

📁

Upload file

🏠 / fna / fuentes / MALWARE_LAB

☐	↑	Name	Type	Size	Owner	Group	Permissions	Last updated
☐		📁 alertaspreventivas	directory	-	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 10:51:16
☐		📁 alertastempranas	directory	-	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 10:51:57

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

📁

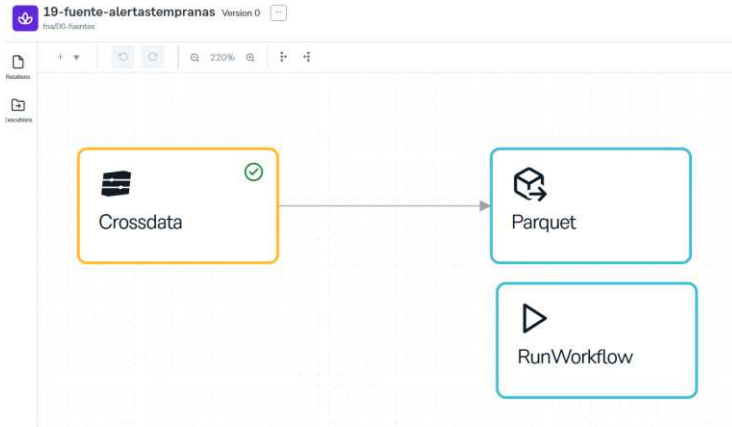
Upload file

🏠 / fna / fuentes / MALWARE_LAB / alertaspreventivas

☐	↑	Name	Type	Size	Owner	Group	Permissions	Last updated
☐		📄 part-00000-1ca603ca-727b-4922-ba5a-2d09f5acbb6ad-c0...	parquet	53.6 KB	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 10:51:16
☐		📄 _SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 10:51:16

#	id	ABC fecha_envio	ABC fuentes	ABC continente	ABC tipologia_malware	ABC numero_tiket	ABC numero_alertas	ABC threat_actor	ABC nombre_malware	ABC criticidad
18		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico
19		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico
20		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico
21		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico
22		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico
23		2025-01-01T05:00:00.000Z	otx-alienvault			145445				Critico

1.4.8 Fuente Malware Lab - alertastempranas



Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_alertastempranas

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Parquet

Table name

alertastempranas

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/MALWARE_LAB

Parquet save properties

[Add element](#)

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

Upload file

/ fna / fuentes / MALWARE_LAB / alertastempranas

☐	↑	Name	Type	Size	Owner	Group	Permissions	Last updated
☐		part-00000-fc57d239-efcf-4ec2-a698-5583ecf925e-c00...	parquet	22.07 KB	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:05:57
☐		_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:05:57

🔍

AK: fecha_reporte

AK: fuente

AK: fecha_fuente

AK: cve_reportada

AK: num_vulnerabilidades

AK: fabricante

AK: producto

AK: ticket_id

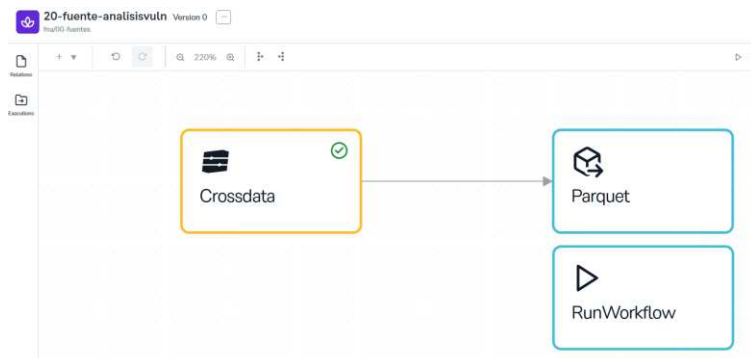
AK: num_alertas

AK: tecnica_mitig

AK: sub_sec

18	2025-01-15T05:00:00.000Z	https://msrc.microsoft.com/update-guide	2025-01-15T05:00:00.000Z	CVE-2025-21172	1	MICROSOFT	Windows 11 Version 24H2 for x64-based Systems	147301
19	2025-01-15T05:00:00.000Z	https://msrc.microsoft.com/update-guide	2025-01-15T05:00:00.000Z	CVE-2025-21173	1	MICROSOFT	Windows 11 Version 23H2 for ARM64-based Systems	147301
21	2025-01-15T05:00:00.000Z	https://msrc.microsoft.com/update-guide	2025-01-15T05:00:00.000Z	CVE-2025-21178	1	MICROSOFT	Windows 11 Version 23H2 for x64-based Systems	147301
22	2025-01-15T05:00:00.000Z	https://msrc.microsoft.com/update-guide	2025-01-15T05:00:00.000Z	CVE-2025-21186	1	MICROSOFT	Windows 11 Version 23H2 for ARM64-based Systems	147301
23	2025-01-15T05:00:00.000Z	https://msrc.microsoft.com/update-guide	2025-01-15T05:00:00.000Z	CVE-2025-21187	1	MICROSOFT	Windows Server 2016	147301

1.4.9 Fuente Evaluación de Seguridad



×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_analisisvuln

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

analisisvuln

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (" separated")

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/EVALUACION_DE_SEGURIDAD

Parquet save properties

[Add element](#)

🔍 Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

📁

Upload file

🏠 / fna / fuentes / EVALUACION_DE_SEGURIDAD

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	📁 analisisvuln	directory	-	execution-identity...	supergroup	rw-r--r-x	29 Apr 2025 - 1:06:46

File Browser

Filter file or directory...

Upload file

/ fna / Fuentes / EVALUACION_DE_SEGURIDAD / analisisvuln

☐	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-9dd88276-7242-434c-9193-448b0517ba0-c...	parquet	58.44 KB	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:06:45
☐	_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:06:46

#	id	ac test	ac id_vuln	ac id_mensaje	ac vulnerabilidad	ac identificador	ac ip	ac nombre	ac puerto	ac protocolo	ac impacto	ac puntaje_cve	ac explotable	a
13	2022		33174	51192	SSL Certificate Cannot Be Trusted	CWE-326	172.16.0.63	FNABOGINF015	636	tcp	Medio	6.5	NO	F
1301	2024-02-01T05:00:00.000Z		37000	51192	SSL Certificate Cannot Be Trusted	CWE-326	172.16.127.146	fnabogwmpw	3126	tcp	Medio	6.5	NO	F
21	2022		33190	45411	SSL Certificate Cannot Be Trusted	CWE-326	172.16.0.69	FNABOGINF010	1002	tcp	Medio	5.3	NO	F

1.4.10 Fuente Análisis de código

Z4-fuente-analisiscodigo Version 0

Buttons

Execution

Crossdata

Parquet

RunWorkflow

Input - Crossdata

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_analisiscodigo

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

analisiscodigo

Discard table name

Save mode *

Overwrite

☐

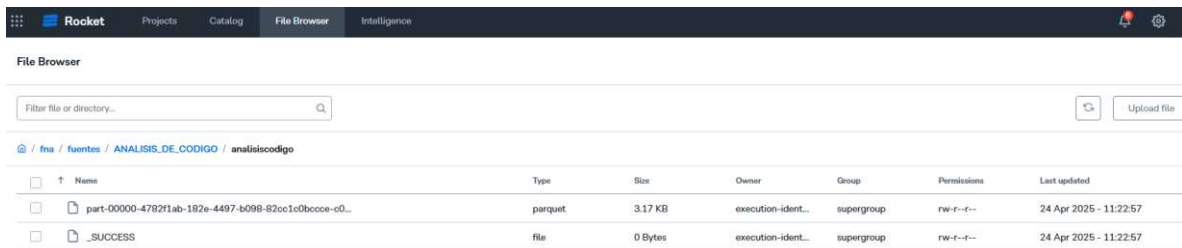
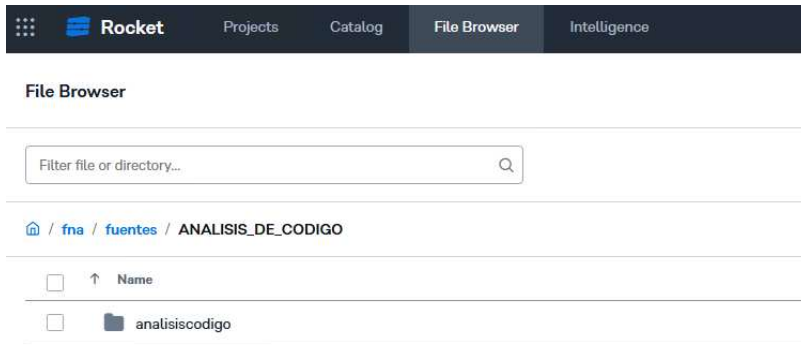
Enable dynamic overwrite partitioning

Partition By (',' separated)

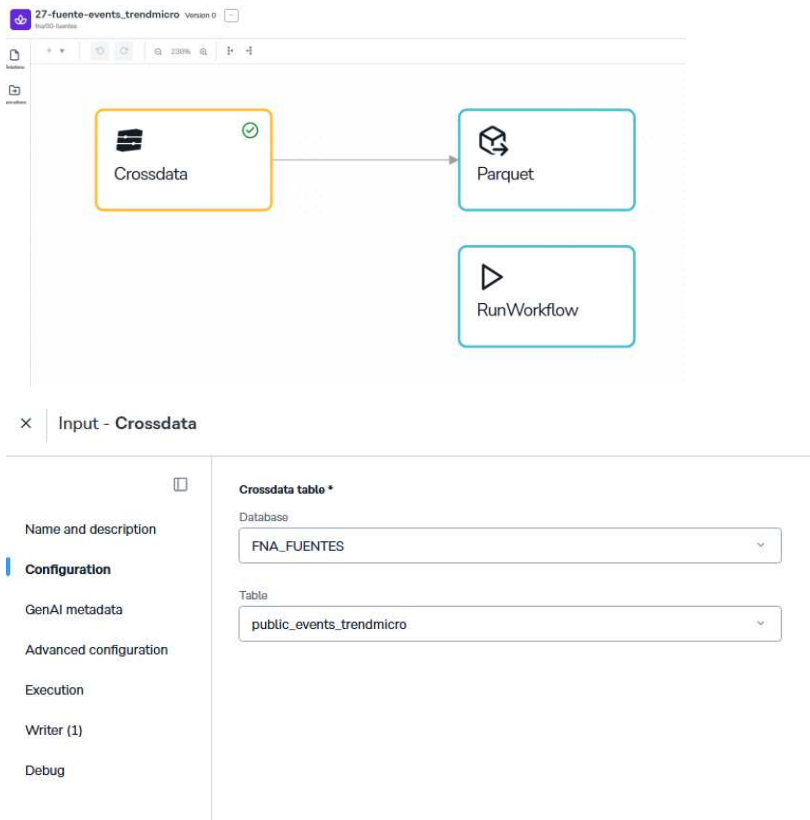
Number of partitions

List of columns for repartition

# id	# servicio	# vulnerabilidad	# criticidad	# calculo
2	Radicacion Credito	Ataque de robot en formulario	Alta	5
3	Radicacion Credito	Implementación incorrecta de reCaptcha	Alta	5
4	Radicacion Credito	Credenciales enviadas en texto plano	Media	3
5	Radicacion Credito	Algoritmos de cifrado obsoletos	Media	3
6	Radicacion Credito	Software con vulnerabilidades conocidas	Media	3
7	Radicacion Credito	Divulgación de información interna	Media	3



1.4.11 Fuente Protección de Endpoints / En la Nube / Web / SandBox



×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

events_trendmicro

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (*, separated)

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/MULTIFUENTE/

Parquet save properties

[Add element](#)

Rocket

ProjectsCatalogFile BrowserIntelligence

File Browser

Filter file or directory...

/fna / fuentes / MULTIFUENTE

☐	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	events_trendmicro	directory	-	execution-identity...	supergroup	rwxr-xr-x	24 Apr 2025 - 12:13:37

date

#

starttime

MC logsource

MC eventname

MC sourceip

MC destinationip

MC destinationport

MC category

MC protocol

MC username

MC action

MC command

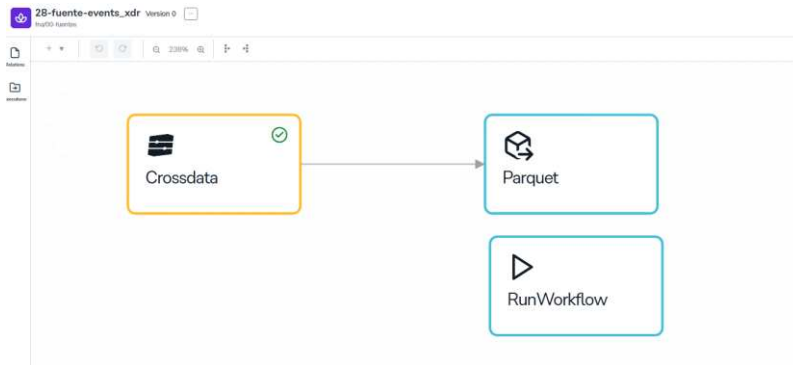
MC commandassociate

2025-03-25	1742906826546	FNA_TrendMicro_ApexCentral	Device Access Control	34.205.5.2	34.205.5.2	0	System Security Access Granted	255	FNA2jogomez	null	null	null
2025-03-25	1742907428671	FNA_TrendMicro_ApexCentral	Device Access Control	34.205.5.2	34.205.5.2	0	System Security Access Granted	255	null	null	null	null
2025-03-25	1742908633225	FNA_TrendMicro_ApexCentral	Device Access Control	34.205.5.2	34.205.5.2	0	System Security Access Granted	255	FNA2jedgarciag	null	null	null
2025-03-25	1742909225362	FNA_TrendMicro_ApexCentral	Device Access Control	34.205.5.2	34.205.5.2	0	System Security Access Granted	255	FNA2alsuarez	null	null	null

Activar Windows

Ve a Configuración para activar Window

1.4.12 Fuente XDR



× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_xdr

× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Parquet

Table name

events_xdr

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (* separated)

Number of partitions

List of columns for repartition

× Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/XDR/

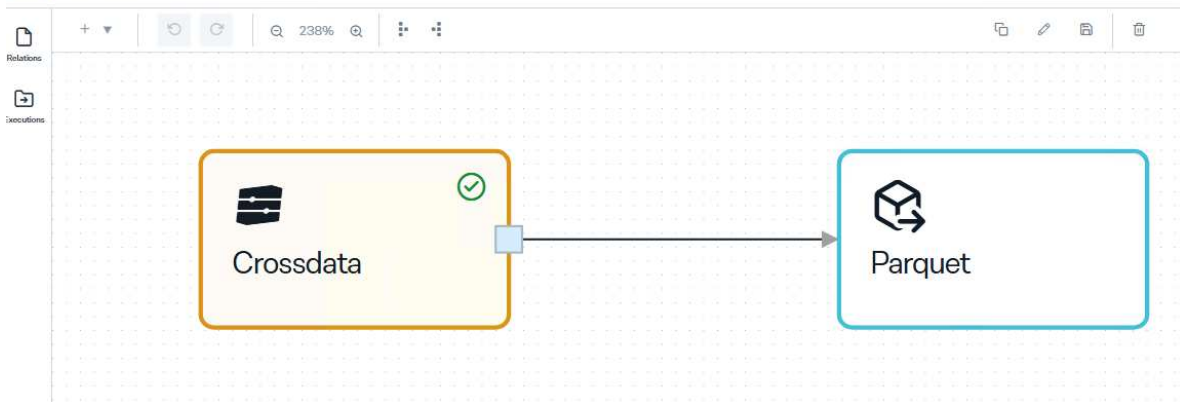
Parquet save properties

[Add element](#)

date	start time	src event name	src ip	src category	src severity	src destination	src tactic name	src technique name	src entity type	src endpoint name	src filename	src event
2025-03-25	1742866066583	Observed Attack Technique	TrendMicroVisionOneCustom @ VisionOneLogSource	Unknown Potential Exploit Attack	169.254.3.5	169.254.3.5	,TA0005,	,T1036,	endpoint	GRB-CNA-02-2315	Uncommon File Path of Executable File,	1
2025-03-25	1742869367042	Observed Attack Technique	TrendMicroVisionOneCustom @ VisionOneLogSource	Unknown Potential Exploit Attack	169.254.3.5	169.254.3.5	,TA0005,	,T1036,	endpoint	GRB-CNA-02-2939	Uncommon File Path of Executable File,	1
2025-03-25	1742869486609	Observed Attack Technique	TrendMicroVisionOneCustom @ VisionOneLogSource	Unknown Potential Exploit Attack	169.254.3.5	169.254.3.5	,TA0005,	,T1036,	endpoint	GEA-TCC-04-2286	Uncommon File Path of Executable File,	1
2025-03-25	1742872464228	Observed Attack Technique	TrendMicroVisionOneCustom @ VisionOneLogSource	Unknown Potential Exploit Attack	169.254.3.5	169.254.3.5	,TA0005,	,T1036,	endpoint	VRE-PE-CAD-3915	Uncommon File Path of Executable File,	1
2025-03-25	1742888027691	Observed Attack Technique	TrendMicroVisionOneCustom @ VisionOneLogSource	Unknown Potential Exploit Attack	169.254.3.5	169.254.3.5	,TA0005,	,T1036,	endpoint	GLE-CNA-02-2216	Uncommon File Path of Executable File,	1

Activar V	Path of Executable File.
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	...
27	...
28	...
29	...
30	...
31	...
32	...
33	...
34	...
35	...
36	...
37	...
38	...
39	...
40	...
41	...
42	...
43	...
44	...
45	...
46	...
47	...
48	...
49	...
50	...
51	...
52	...
53	...
54	...
55	...
56	...
57	...
58	...
59	...
60	...
61	...
62	...
63	...
64	...
65	...
66	...
67	...
68	...
69	...
70	...
71	...
72	...
73	...
74	...
75	...
76	...
77	...
78	...
79	...
80	...
81	...
82	...
83	...
84	...
85	...
86	...
87	...
88	...
89	...
90	...
91	...
92	...
93	...
94	...
95	...
96	...
97	...
98	...
99	...
100	...

29-fuente-events_soar Version 0
fna/00-fuentes



× | Input - Crossdata

Name and description
Configuration
GenAI metadata
Advanced configuration
Execution
Writer (1)
Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_soar

× | Input - Crossdata

Name and description
Configuration
GenAI metadata
Advanced configuration
Execution
Writer (1)
Debug

Parquet

Table name

events_soar

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/SOAR/

Parquet save properties

Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

/ fna / fuentes / SOAR / events_sour

	Name	Type	Size	Owner	Group	Permissions	Last updated
	part-00000-e5a13c30-9c03-438d-840e-bf54affbaf6a-c00...	parquet	5.01 KB	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 16:26:55
	._SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 16:26:55

date	starttime	eventname	eventname	category	sourceip	destinationip	magnitude	eventdescription	apppathinfo	eventcount
2025-03-31	1743439476821	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-03-31	1743439476821	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-03-31	1743450268180	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-03-31	1743450268411	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-04-24	1745505415752	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-04-24	1745505415752	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-04-24	1745505602090	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-04-24	1745505602090	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1
2025-04-24	1745505602090	API request failure	SOAR_Integration_API	SIM User Action	169.254.3.23	10.87.61.56	5	API request failure	/console/estapi/reference_data/sets	1

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

events_attack_WAF

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (';' separated)

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/WAF

Parquet save properties

[Add element](#)

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

📁

Upload file

🏠 / fna / fuentes / WAF

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	📁 events_attack_WAF	directory	-	execution-identity...	supergroup	rwax-x-x	29 Apr 2025 - 1:07:53
☐	📁 events_waf	directory	-	execution-identity...	supergroup	rwax-x-x	29 Apr 2025 - 1:08:41

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

Upload

fna

/

fuentes

/

WAF

/

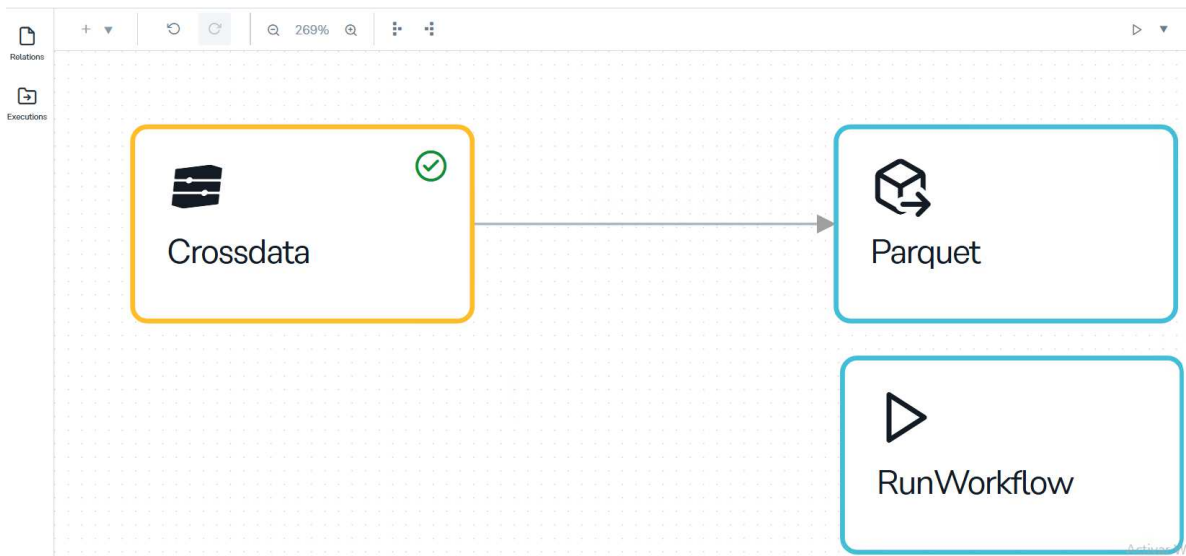
events_attack_WAF

☐	↑	Name	Type	Size	Owner	Group	Permissions	Last updated
☐		part-00000-d68d8ba5-16c8-4875-9833-693d19f5950-c...	parquet	2.46 MiB	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:07:53
☐		_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:07:53

Date	#	StartTime	Qidname	LogsourceName	Lowlevelcategory	Sourceip	Destinationip	Destinationport	Sub_type	Eventtype	Http_host	Main_type
2025-03-26	1742951541741		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.97	10.1.252.120	443	Crawler	attack	fna.gov.co	Known Bots Detection
2025-03-26	1742951542738		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.107	10.1.252.120	443	Crawler	attack	fna.gov.co	Known Bots Detection
2025-03-26	1742951542738		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.96	10.1.252.120	443	Crawler	attack	www.fna.gov.co	Known Bots Detection
2025-03-26	1742951542739		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.110	10.1.252.120	443	Crawler	attack	fna.gov.co	Known Bots Detection
2025-03-26	1742951542739		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.102	10.1.252.120	443	Crawler	attack	www.fna.gov.co	Known Bots Detection
2025-03-26	1742951725857		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.106	10.1.252.120	443	Crawler	attack	www.fna.gov.co	Known Bots Detection
2025-03-26	1742951725857		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.104	10.1.252.120	443	Crawler	attack	www.fna.gov.co	Known Bots Detection
2025-03-26	1742951726855		Alert Deny Event	FortiGate @ 172.16.125.6	Alert	52.159.249.111	10.1.252.120	443	Crawler	attack	www.fna.gov.co	Known Bots Detection
2025-03-26	1742951834923		Firewall Alert	FortiGate @ 172.16.125.6	Alert	177.93.59.71	10.1.254.120	8081	Anonymous Proxy	attack	ivars Winone's	IP Reputation

1.4.15 Fuente WAF – events waf

 **22-fuente-events_waf** Version 0 



×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_waf

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

events_waf

Discard table name

Save mode *

Overwrite

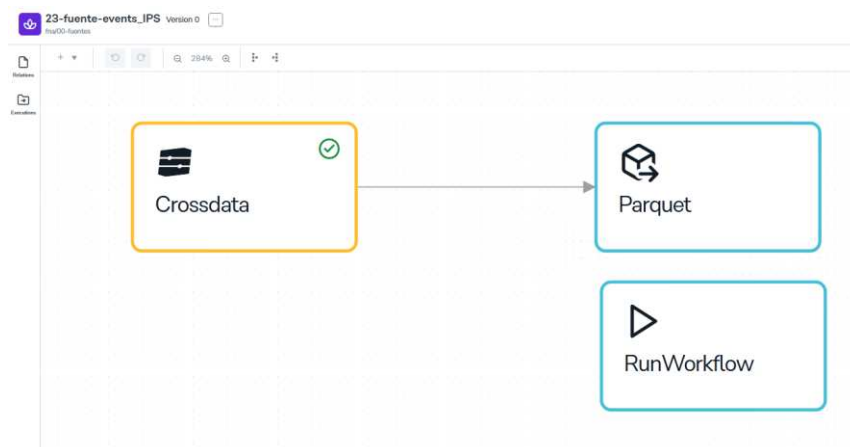
☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

1.4.16 Fuente IPS



× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_ips

× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Parquet

Table name

events_IPS

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/IPS/

Parquet save properties

⊕

Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

🔍

📁

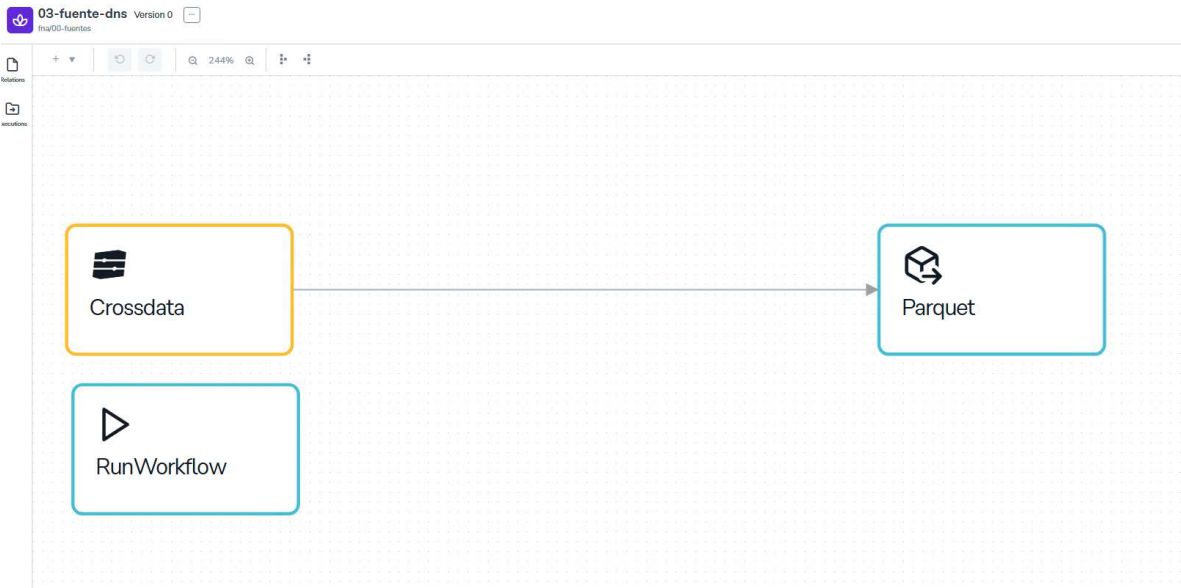
Upload file

📁 / fna / fuentes / IPS / events_IPS

☐	↑	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	📁	part-00000-4ebd0dd6-e41c-4b7c-ad3c-b576ec527a93-c...	parquet	691.27 KB	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:09:26
☐	📄	_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	29 Apr 2025 - 1:09:26

🕒 date	🕒 start time	👤 ac username	👤 ac logoname	🏷️ ac category	📡 ac sourceip	📡 ac sourceport	📡 ac destinationip	📡 ac destinationport	👤 ac username	📊 ac magnitude	📊 ac eventcount
2025-04-23	1745424630558	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	IPS Trendmicro TippingPoint @ 172.16.125.214	Notice	10.2.8.40	56332	172.16.125.33	2533	null	6	1
2025-04-23	1745424590539	3959: HTTP: Cross-Site Scripting (Cookie Manipulation)	IPS Trendmicro TippingPoint @ 172.16.125.214	Cross Site Scripting	192.168.35.31	53614	172.16.127.118	80	null	7	1
2025-04-23	1745424590539	3959: HTTP: Cross-Site Scripting (Cookie Manipulation)	IPS Trendmicro TippingPoint @ 172.16.125.214	Cross Site Scripting	192.168.35.20	63753	172.16.127.118	80	null	7	1

1.4.17 Fuente DNS



× | Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_dns

× | Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Parquet

Table name

events_dns

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/DNS/

Parquet save properties

+ Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

Upload file

/ fna / fuentes / DNS / events_dns

	Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-f23c3fee-5960-461b-8c00-51e0f1d0ec38-c0...	parquet	3.97 MB	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 12:30:22
☐	_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 12:30:22

1.4.18 Fuente NDR

25-fuente-events_ndr

Version 0

fna/00-fuentes

+

▼

↺

↻

🔍

238%

🔍

⋮

⋮

relations

Crossdata

✓

Parquet

RunWorkflow

× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_ndr

× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Parquet

Table name

events_ndr

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/NDR/

Parquet save properties

+

 Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

↻

Upload file

/ fna / fuentes / NDR / events_ndr

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-3cfs2b84-c5o7-443c-99de-e2ada7738226-c...	parquet	14.8 KB	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 11:27:20
☐	_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 11:27:20

⌕ date ⌕	⌕ starttime ⌕	⌕ eventname ⌕	⌕ logsource ⌕	⌕ eventcount ⌕	⌕ sourcip ⌕	⌕ sourceport ⌕	⌕ destinationip ⌕	⌕ destinationport ⌕	⌕ username ⌕	⌕ score ⌕
2025-04-14	1744595662663	Unknown	FNA_Darktrace	1	18.220.154.78	59404	10.1.252.124	8093	24051	62.0
2025-04-14	1744595666253	Unknown	FNA_Darktrace	1	18.220.154.78	47618	10.1.252.122	8093	41422	62.0
2025-04-14	1744615707843	SaaS_Access_Failed Logins from Multiple Rare IPs	FNA_Darktrace	1	172.17.81.61	0	172.17.81.61	0	237662	46.0
2025-04-14	1744622316870	Unknown	FNA_Darktrace	1	222.99.237.249	0	172.17.81.61	0	235401	35.0
2025-04-14	1744630697349	SaaS_Access_Failed Logins from Multiple Rare IPs	FNA_Darktrace	1	172.17.81.61	0	172.17.81.61	0	239333	46.0
2025-04-14	1744636749916	Unknown	FNA_Darktrace	1	10.10.12.55	0	179.196.116	6180	655	50.0
2025-04-14	1744637857610	Unknown	FNA_Darktrace	1	172.17.253.4	0	172.16.0.70	88	205891	62.0

1.4.19 Fuente Seguridad de Correo Electrónico

26-fuente-events_email

Version 0

fna/00-fuentes

Relations

Executions

+

238%

Crossdata

Parquet

RunWorkflow

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_email

× Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

▼ Parquet

Table name

events_email

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

☐ Check if empty dataframe before saving it

× Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/SEGURIDAD_CORREO_ELECTRONICO/

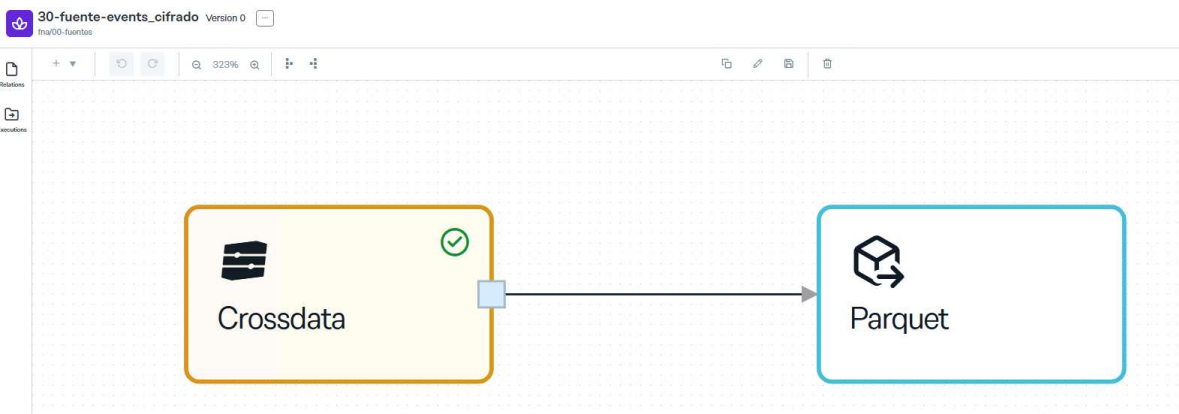
Parquet save properties

[+ Add element](#)

Rocket Projects Catalog File Browser Intelligence							
File Browser							
Filter file or directory...							
📁 / fna / fuentes / SEGURIDAD_CORREO_ELECTRONICO / events_email							
☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	part-00000-d7035067-78cc-4cae-9064-8a3cbacc460b-c...	parquet	180.03 KB	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 11:33:55
☐	_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	24 Apr 2025 - 11:33:56

#	data	starttime	eventname	eventsource	eventdirection	eventsender	eventrecipients	eventsubject	eventsha1hash	event
2025-03-25	1742921223052	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-03-25	1742942708297	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-03-26	1742946977913	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-03-26	1742947106990	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-03-26	1742947114003	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-04-08	1744147967259	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null
2025-04-08	1744148192390	DarktraceLogSource Message	FNA_Darktrace	null	null	null	null	null	null	null

1.4.20 Fuente Cifado



×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

Writer (1)

Debug

Crossdata table *

Database

FNA_FUENTES

Table

public_events_cifrado

×

Input - Crossdata

Name and description

Configuration

GenAI metadata

Advanced configuration

Execution

1

Writer

Debug

▼

Parquet

Table name

events_cifrado

Discard table name

Save mode *

Overwrite

☐ Enable dynamic overwrite partitioning

Partition By (',' separated)

Number of partitions

List of columns for repartition

×

Output - Parquet

Name and description

Configuration

Execution

Path *

/fna/fuentes/CIFRADO/

Parquet save properties

+

 Add element

Rocket

Projects

Catalog

File Browser

Intelligence

File Browser

Filter file or directory...

Upload file

/ fna / fuentes / CIFRADO / events_cifrado

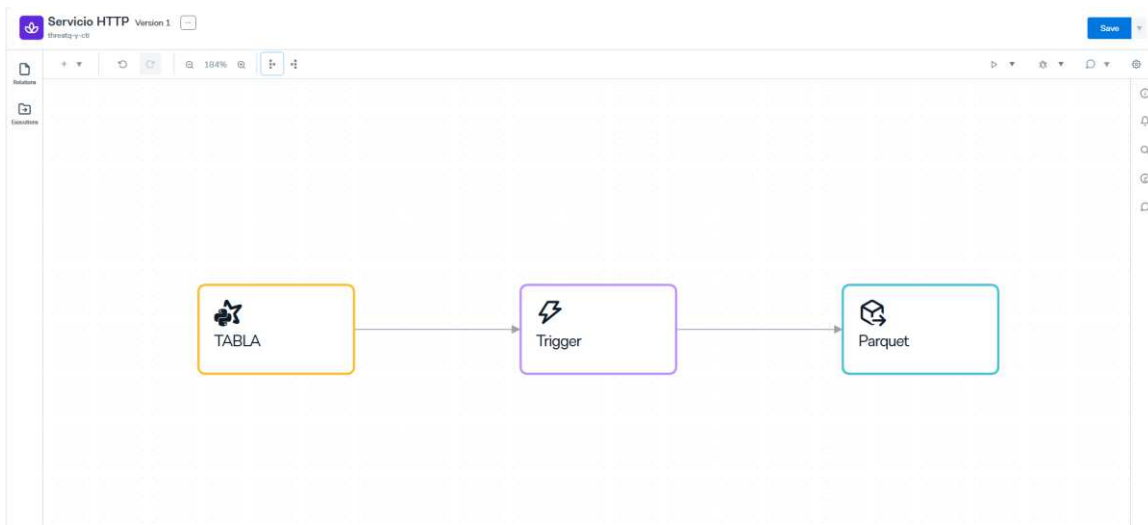
☐	?	Name	Type	Size	Owner	Group	Permissions	Last updated
☐		part-00000-8a98075a-c2a2-4a4d-838a-cc271ac9ce44-c...	parquet	12.21 MB	execution-identity...	supergroup	rw-r--r--	2 May 2025 - 12:16:53
☐		_SUCCESS	file	0 Bytes	execution-identity...	supergroup	rw-r--r--	2 May 2025 - 12:16:53

#	starttime	eventname	logsource	sourceip	destinationip	destinationport	category	username	servicename	ticketfunction	machineidentifier
2025-03-25	1742884164514	Failure Audit: A Kerberos service ticket was rejected	AD - bogpvcwp003.hia.gov.co 172.16.0.72	10.1.151.79	172.16.0.72	0	Kerberos Session Denied	sp_granja	sp_admin	null	BOGPVDCWP003.hia.go
2025-03-25	1742884166553	Failure Audit: A Kerberos service ticket was rejected	AD - bogpvcwp002.hia.gov.co 172.16.0.71	10.1.151.80	172.16.0.71	0	Kerberos Session Denied	sp_granja	sp_admin	null	BOGPVDCWP002.hia.go
2025-03-25	1742884167517	Failure Audit: A Kerberos service ticket was rejected	AD - bogpvcwp002.hia.gov.co 172.16.0.71	172.16.131.100	172.16.0.71	0	Kerberos Session Denied	null	frarodriguez	null	BOGPVDCWP002.hia.go
2025-03-25	1742884184528	Failure Audit: A Kerberos service ticket was rejected	AD - bogpvcwp003.hia.gov.co 172.16.0.72	172.16.131.89	172.16.0.72	0	Kerberos Session Denied	shp_farm_int	shp_search_int	null	BOGPVDCWP003.hia.go
2025-03-25	1742884184530	Success Audit: A Kerberos service ticket	AD - bogpvcwp003.hia.gov.co 172.16.0.72	10.10.28.167	172.16.0.72	0	Information	null	null	null	BOGPVDCWP003.hia.go

1.4.21 Fuente Inteligencia de Amenazas :

1.4.21.1 ETL SERVICIO HTTP

Estructura del flujo:



1. Input – TABLA (PySpark personalizado):

Se conecta a la API

<https://threatq.mnemo.com/api/export/4dac921dae145b74e9b5f48c7a035db1/>
para extraer datos de IPs junto con su nivel de riesgo.

- Se utiliza una función en PySpark que realiza una petición GET con autenticación por token.

- La verificación del certificado fue deshabilitada mediante `verify=False` para permitir la conexión.
- La respuesta se procesa como texto plano con líneas tipo `IP,riesgo`.
- Se crea un RDD y luego un DataFrame con esquema explícito:
 - IP: dirección IP (tipo String)
 - CLASIFICACION_RIESGO: nivel de riesgo (tipo Integer)

2. Transformación – Trigger:

Se utiliza una consulta SQL para enriquecer los datos agregando una columna como marca de tiempo:

```
SELECT *, CURRENT_DATE AS MarcaTiempo FROM TABLA
```

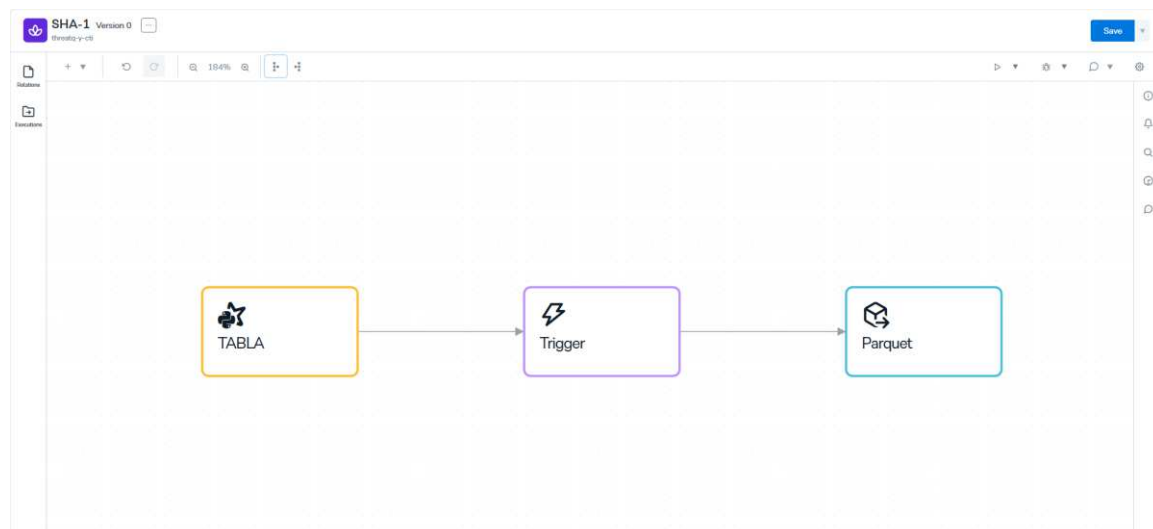
3. Salida – Parquet:

Los datos transformados se almacenan en formato Parquet en la ruta: **fna/fuentes/INTELIGENCIA_DE_AMENZAS**

Esto permite que otras herramientas de Stratio (como Discovery, API Gateway o procesos ETL) puedan consumir los datos estructurados y actualizados.

1.4.21.2 ETL SHA-1

Estructura del flujo:



1. Input – TABLA (PySpark personalizado):

Se conecta a la API `threatq.mnemo.com/api/export/2749eac95d338973cf5966708725f054/` para extraer datos de Hashes SHA-1 junto con su nivel de riesgo.

- Se utiliza una función en PySpark que realiza una petición GET con autenticación por token.

- La verificación del certificado fue deshabilitada mediante `verify=False` para permitir la conexión.
- La respuesta se procesa como texto plano con líneas tipo Hash, riesgo.
- Se crea un RDD y luego un DataFrame con esquema explícito:
 - Hash: (tipo String)
 - CLASIFICACION_RIESGO: nivel de riesgo (tipo Integer)

2. Transformación – Trigger:

Se utiliza una consulta SQL para enriquecer los datos agregando una columna como marca de tiempo:

```
SELECT *, CURRENT_DATE AS MarcaTiempo FROM TABLA
```

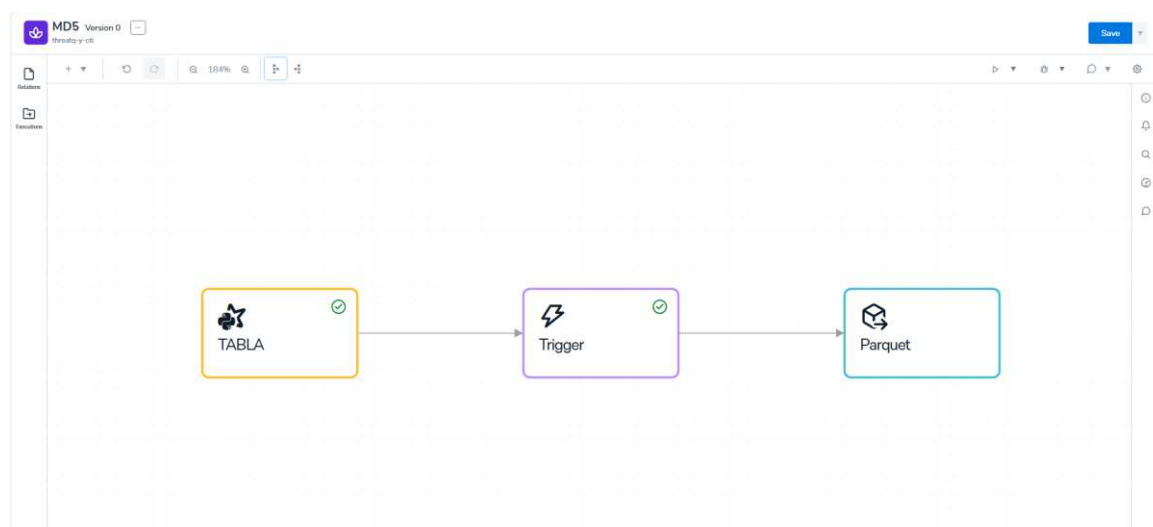
3. Salida – Parquet:

Los datos transformados se almacenan en formato Parquet en la ruta: **fna/fuentes/INTELIGENCIA_DE_AMENZAS**

Esto permite que otras herramientas de Stratio (como Discovery, API Gateway o procesos ETL) puedan consumir los datos estructurados y actualizados.

1.4.21.3 ETL MD5

Estructura del flujo:



1. Input – TABLA (PySpark personalizado):

Se conecta a la API <https://threatq.mnemo.com/api/export/b12b0a0c2f84d255c5a7b4a8f8fe723e/> para extraer datos de Hashes MD5 junto con su nivel de riesgo.

- Se utiliza una función en PySpark que realiza una petición GET con autenticación por token.
- La verificación del certificado fue deshabilitada mediante `verify=False` para permitir la conexión.
- La respuesta se procesa como texto plano con líneas tipo Hash, riesgo.
- Se crea un RDD y luego un DataFrame con esquema explícito:
 - Hash: (tipo String)
 - CLASIFICACION_RIESGO: nivel de riesgo (tipo Integer)

2. Transformación – Trigger:

Se utiliza una consulta SQL para enriquecer los datos agregando una columna como marca de tiempo:

```
SELECT *, CURRENT_DATE AS MarcaTiempo FROM TABLA
```

3. Salida – Parquet:

Los datos transformados se almacenan en formato Parquet en la ruta: **fna/fuentes/INTELIGENCIA_DE_AMENZAS**

Esto permite que otras herramientas de Stratio (como Discovery, API Gateway o procesos ETL) puedan consumir los datos estructurados y actualizados.

1.5 Tablas almacenadas en HDFS:

El FileSystem de Hadoop está integrado con la plataforma y desde Rocket podemos ver la información de carpetas y archivos almacenados. A continuación, un pantallazo de la ruta donde están almacenados los datos:

Rocket

ProjectsCatalogFile BrowserIntelligence

Hermes Puentes

fracyber

File Browser

Filter file or directory...

Upload file

New folder

/ fna / fuentes

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	ANALISIS_DE_CODIGO	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 11:22:52
☐	CIFRADO	directory	-	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 12:15:16
☐	DAM	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:51:08
☐	DNS	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 12:29:49
☐	EVALUACION_DE_SEGURIDAD	directory	-	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:06:41
☐	GOBERNANZA	directory	-	execution-ident...	supergroup	rw-r--r--	1 Apr 2025 - 1:18:36
☐	INTELIGENCIA_DE_AMENAZAS	directory	-	execution-ident...	supergroup	rw-r--r--	30 Apr 2025 - 16:54:04
☐	IPS	directory	-	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:09:15
☐	MALWARE_LAB	directory	-	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:05:50
☐	MULTIFUENTE	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 12:13:30
☐	NDR	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 11:27:16
☐	ORIGEN	directory	-	ji-dot-cuevasm...	supergroup	rw-r--r--	23 Apr 2025 - 16:39:04

Rocket

ProjectsCatalogFile BrowserIntelligence

Hermes Puentes

fracyber

File Browser

Filter file or directory...

Upload file

New folder

/ fna / fuentes

☐	↑ Name	Type	Size	Owner	Group	Permissions	Last updated
☐	PAM	directory	-	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:06:46
☐	SEGURIDAD_CORREO_ELECTRONICO	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 11:33:50
☐	SOAR	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 16:26:50
☐	SOC	directory	-	execution-ident...	supergroup	rw-r--r--	2 May 2025 - 0:05:14
☐	VIGILANCIA	directory	-	rocket.fracyber...	supergroup	rw-r--r--	29 Apr 2025 - 1:04:20
☐	WAF	directory	-	execution-ident...	supergroup	rw-r--r--	29 Apr 2025 - 1:08:34
☐	XDR	directory	-	execution-ident...	supergroup	rw-r--r--	24 Apr 2025 - 12:20:12

MNEMO

NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD



CASOS DE USO

CIBER ANALITICA - STRATIO DATA FABRIC

Contenido

INTRODUCCION.....	4
ALCANCE	4
INTRODUCCIÓN TÉCNICA E INTELIGENCIA OPERATIVA.....	5
INTEGRACIÓN DE CIBER ANALÍTICA EN EL MONITOREO SOC.....	6
CASO DE USO 1 GESTIÓN UNIFICADA DE AMENAZAS	7
1.1. Transformaciones de datos	7
1.2. Tableros de control.....	10
1.2.1. Estadísticas generales	10
1.2.2. Indicadores de compromiso	11
1.2.3. Análisis de vulnerabilidades.....	12
1.2.4. Riesgo de activos.....	13
1.2.5. Riesgo de usuarios	14
CASO DE USO 2 MOVIMIENTOS LATERALES	16
1. Uso sospechoso de protocol Web	16
1.1. Condiciones de activación.....	16
1.2. Detalle de cada componente que debe activarse:.....	16
2. PsExec entrante y descarga de scripts	18
2.1. Condiciones de activación	18
2.2. Detalle de cada componente que debe activarse:	18
2.2.1. Cualquier SMB Todo (5 filtros).....	18
2.2.2. Cualquier conexion externa (6 filtros)	19
3. Movimiento lateral y actividad C2	19
3.1. Condiciones de activación	19
3.2. Detalle de cada componente que debe activarse:	20
3.2.1. Modelo mas de 2 en 24 horas (11 filtros).....	20
3.2.2. Modelo mas de 1 en 1 hora (13 filtros)	20
3.2.3. Cualquier modelo (11 filtros).....	21
3.2.4. Modelo mas de 1 en 24 horas (12 filtros).....	22
CASO DE USO 3 PATRONES DE ATAQUE	23
1. Múltiples indicadores de cadena de ataque.....	23
1.1. Condiciones de activación	23
1.2. Detalle de cada componente que debe activarse:.....	23
1.2.1. Cualquier modelo (5 filtros).....	24
1.2.2. Cualquier modelo (5 filtros).....	24
1.2.3. Cualquier modelo (5 filtros).....	24

1.2.4.	Cualquier modelo (5 filtros)	25
1.2.5.	Cualquier modelo (5 filtros)	25
1.2.6.	Cualquier modelo (5 filtros)	26
1.2.7.	Cualquier modelo (5 filtros)	26
1.2.8.	Cualquier modelo (5 filtros)	26
1.2.9.	Cualquier modelo (5 filtros)	27
1.2.10.	Cualquier modelo (5 filtros)	27
1.2.11.	Cualquier modelo (5 filtros)	28
1.2.12.	Cualquier modelo (5 filtros)	28
1.2.13.	Cualquier modelo (5 filtros)	29
1.2.14.	Cualquier modelo (6 filtros)	29
1.2.15.	Cualquier modelo (5 filtros)	30
1.2.16.	Cualquier modelo (7 filtros)	30
1.2.17.	Cualquier modelo (5 filtros)	31
CASO DE USO 4 EVALUACIÓN INTEGRAL DE RIESGOS		32
1.	Definición conceptual	32
2.	Arquitectura lógica.....	32
3.	Requisitos y fuentes de datos	33
4.	Arquitectura técnica	33
5.	Productos del modelo.....	33
5.1.	EXOS	34
5.2.	THERMOS	35
5.3.	MESOS	36
5.4.	STRATOS	37
5.5.	TROPOS	38
5.6.	DEFCON	40
CASO DE USO 5 CORRELACIÓN AVANZADA.....		45
1.1	Integración de la Correlación Avanzada en el Monitoreo del SOC	45
1.1	Actividad sospechosa seguida de tarea de administración de endpoint	45
1.2	Logica General	45
1.3	Logica Detallada.....	45
1.3.1	Administración habitual de endpoints.....	46
1.1.2	Actividades sospechosas en puntos finales	52

INTRODUCCION

El desarrollo de soluciones tecnológicas basadas en analítica de datos representa un pilar clave para abordar los desafíos en ciberseguridad. Estas soluciones permiten no solo identificar posibles vulnerabilidades, sino también anticipar, detectar y mitigar amenazas de manera proactiva. En este contexto, el presente documento describe el alcance y los resultados de una plataforma de analítica de datos enfocada específicamente en ciberseguridad. Esta solución ha permitido el diseño y la implementación de distintos casos de uso, cada uno construido para abordar áreas estratégicas en la mitigación y gestión de riesgos de ciberseguridad. A través de este documento se presentará el detalle técnico y funcional de cada caso de uso, así como los beneficios operativos que han sido obtenidos como resultado de implementación.

ALCANCE

El presente documento busca dar alcance a través de la documentación presente al hito de facturación número 4 que tiene la siguiente descripción

“Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados con base en el Gobierno del dato previamente establecido, en el entorno aprovisionado para la entidad”

El alcance de esta iniciativa incluye diseñar, desarrollar e implementar una solución integral de analítica avanzada de ciberseguridad, utilizando plataformas de datos robustas y flexibles como Datafabric Rocket y Datafabric Discovery. Los casos de uso descritos en este documento ilustran aplicaciones específicas destinadas a gestionar amenazas, identificar patrones de ataque, analizar movimientos laterales, evaluar riesgos y mejorar la capacidad de correlación avanzada del SOC (Centro de Operaciones de Seguridad).

La solución cubre los siguientes aspectos principales:

1. **Gestión Unificada de Amenazas:** Centraliza, integra y transforma fuentes de datos clave (p. ej., logs SIEM, análisis de vulnerabilidades, riesgos de usuarios) para visibilizar amenazas críticas mediante tableros de control interactivos.
2. **Identificación de Movimientos Laterales:** Detecta actividades sospechosas que podrían ser indicadoras de brechas en la seguridad interna, como conexiones HTTP inusuales, comportamiento de redes internas o descargas de scripts sospechosos asociadas a uso de herramientas como PsExec.
3. **Patrones de Ataque:** Señala indicadores relacionados con potenciales cadenas de ataque o comportamiento malicioso repetitivo, asegurando que la detección abarque incluso los escenarios más complejos, como pruebas de penetración o ataques en tiempo real.
4. **Evaluación Integral de Riesgos:** Proporciona una visión centralizada y jerárquica (Nodos, Segmentos, Capas y DEFCON) del nivel de riesgo, apoyándose en fuentes homogéneas y fórmulas de ponderación adaptativas.

5. **Correlación Avanzada:** Fortalece el monitoreo proporcionado por el SOC al relacionar eventos aislados, transformando información aparentemente inofensiva en una visión holística de potenciales amenazas operativas.

El alcance se extiende no solo a organizaciones que priorizan la seguridad, sino también a aquellas que buscan implementar sistemas inteligentes y personalizados que ofrezcan resultados objetivos y precisos en sus operaciones cotidianas.

INTRODUCCIÓN TÉCNICA E INTELIGENCIA OPERATIVA

Las implementaciones desarrolladas están basadas en la capacidad de integración de datos provenientes de fuentes heterogéneas—desde logs de dispositivos perimetrales hasta modelos adaptativos basados en indicadores de compromiso. La transformación y correlación de datos se lleva a cabo a través de procesos ETL diseñados en plataformas avanzadas como Datafabric Rocket, mientras que los resultados son materializados en tableros de control ofrecidos mediante Datafabric Discovery.

La naturaleza modular de esta solución permite que los usuarios visualicen datos críticos en tiempo real, logren anticiparse a incidentes de seguridad y faciliten la colaboración entre los equipos de operaciones de seguridad y líderes del negocio, optimizando la toma de decisiones con información más clara y confiable. Esto, sumado a un enfoque proactivo respaldado por algoritmos avanzados de monitorización y correlación, asegura que los riesgos no solo sean vistos como problemas, sino como oportunidades para fortalecer la resiliencia tecnológica de la organización.

El desarrollo de esta solución se fundamenta en la continua evolución de necesidades y retos en ciberseguridad, asegurando innovación, adaptabilidad y efectividad en su implementación práctica.

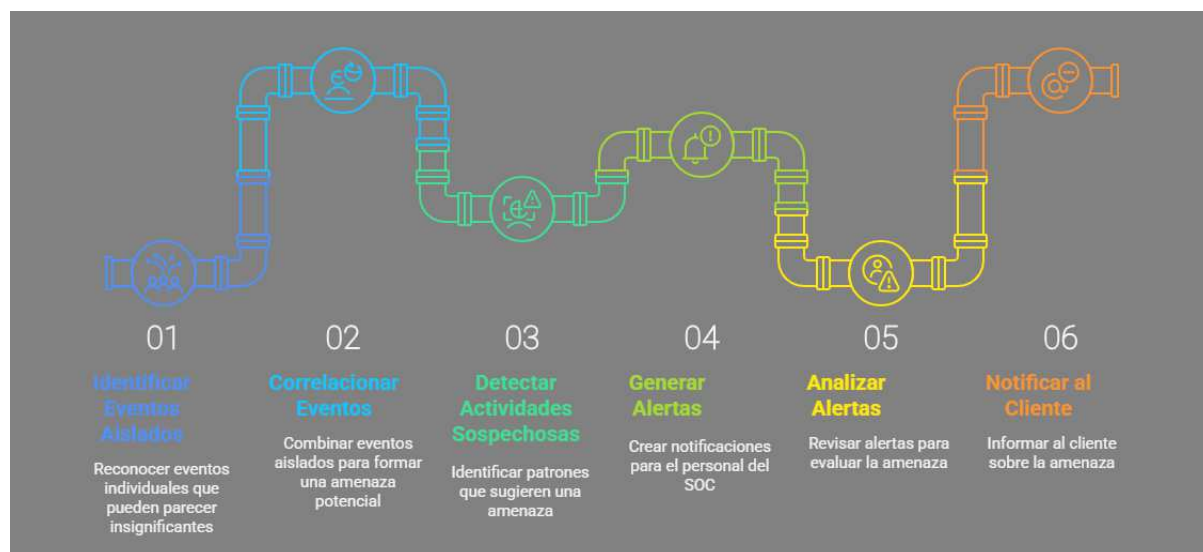
INTEGRACIÓN DE CIBER ANALÍTICA EN EL MONITOREO SOC

La avanzada capacidad de correlación ofrecida por nuestra plataforma de ciber analítica no solo fortalece el monitoreo el cual es llevado a cabo por el Centro de Operaciones de Seguridad (SOC), sino que también ofrece un enfoque proactivo en la identificación de amenazas. Esta integración es clave para optimizar la eficiencia de nuestras operaciones de seguridad.

El proceso de correlación avanzada se inicia con la identificación de eventos aislados, a menudo insignificantes por sí mismos, pero que en conjunto pueden representar una amenaza significativa. Esta capacidad permite a nuestro sistema de ciber analítica detectar actividades sospechosas seguidas de tareas administrativas en endpoints, generando alertas que el personal del SOC, operativo 24/7, puede analizar rápidamente.

Este procedimiento minucioso de análisis no solo permite una detección temprana de posibles amenazas, sino que también asegura una respuesta rápida y bien informada, que se traduce en alertas oportunas al cliente final si se considera necesario. Al desplegar esta capacidad de análisis profundo en tiempo real, el SOC se mantiene a la vanguardia en la protección contra incidentes de seguridad cibernética, asegurando la continuidad de las operaciones de negocio y la confianza del cliente en nuestros servicios.

Por lo tanto, la interoperabilidad entre la inteligencia ofrecida por la correlación avanzada y el monitoreo continuo del SOC establece un sistema robusto que responde a la excelencia operativa y a la seguridad de nuestros clientes.



CASO DE USO 1 GESTIÓN UNIFICADA DE AMENAZAS

El presente documento describe los detalles técnicos más relevantes que se tuvieron en cuenta para el desarrollo del caso de uso 1, incluyendo las fuentes de datos, los procesos de integración/transformación de datos, desarrollados en Datafabric Rocket, y el producto resultante en forma de tableros de control, disponibilizados mediante Datafabric Discovery.

Dentro de las fuentes de datos consideradas para el desarrollo del caso de uso 1 se incluyen:

- **Logs SIEM:** Eventos que representan las actividades de diferentes dispositivos en el tiempo. Esta actividad puede ser interna o externa, es decir, tráfico de algún tipo que se produce enteramente dentro de la red del FNA y que compromete a más de un activo crítico (servidor, terminal, etc.) o, más importante aún en el contexto del actual caso de uso, que viaja desde o hacia internet. Los tipos de logs que se tienen en cuenta provienen de los dispositivos firewalls de borde, WAF y DNS.
- **Indicadores de compromiso:** Conjunto de IPs, principalmente, entregadas por la herramienta TreatQ la cual las ha detectado como fuentes o destinos potencialmente peligrosos, asociándoles una calificación (score). Estos indicadores pueden cambiar a través del tiempo y son el mecanismo principal para la detección de una potencial amenaza.
- **Análisis de vulnerabilidades:** Análisis sobre activos críticos que el equipo de seguridad lleva a cabo periódicamente para identificar y mitigar oportunidades mediante las cuales un potencial atacante puede acceder y/o afectar los datos y servicios ofrecidos por el FNA.
- **Riesgo de usuarios:** Subconjunto de logs SIEM provenientes del directorio activo, los cuales ya han sido analizados por una plataforma intermedia la cual los ha filtrado y les ha asignado un nivel de relevancia y credibilidad en términos de actividad sospechosa de un usuario (conocido o desconocido).
- **Activos críticos:** Lista de activos críticos dentro de la infraestructura del FNA identificados mediante IP.

Mientras que la fuente de logs SIEM y riesgo de usuarios se actualizan de forma diaria, la fuente de análisis de vulnerabilidades se espera que se actualice de forma mensual. Por otro lado, los indicadores de compromiso serán consumidos bajo demanda y la lista de activos críticos permanecerá constante.

1.1. Transformaciones de datos

Los siguientes diagramas lógicos muestran 4 ETLs cuya ejecución periódica (diaria o mensual) es requisito para poblar de forma incremental la bodega de datos que posteriormente será consumida por los tableros de control.

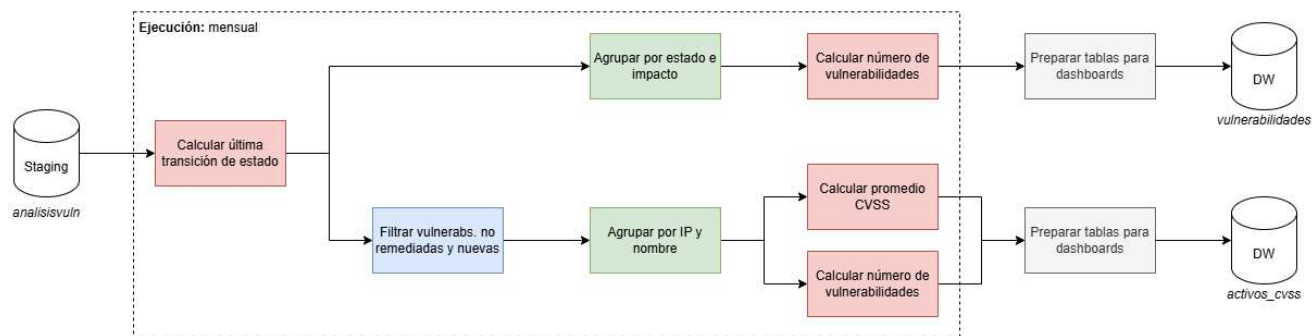
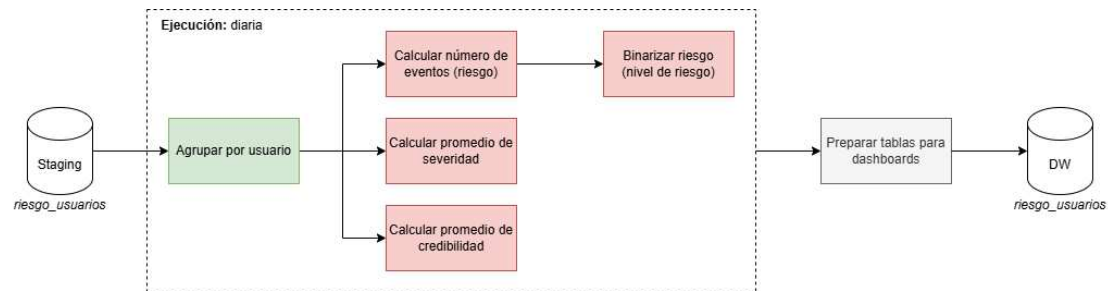
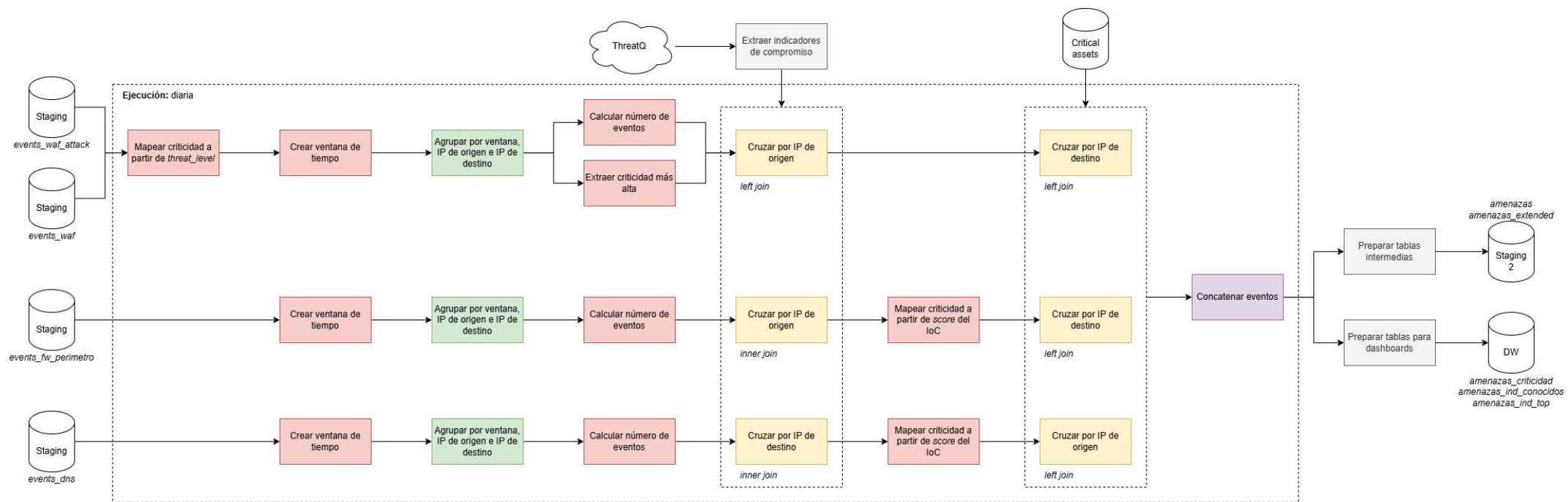
El primer ETL es considerado el principal en términos de volumen de datos y funcionalidad, ya que es el encargado de extraer los logs del SIEM, cruzarlos con los indicadores de compromiso y activos críticos para, como resultado, entregar estadísticas generales de las potenciales amenazas identificadas, incluyendo su grado de criticidad. Adicionalmente, es el que más tablas de la bodega de datos modifica, habilitando la construcción principalmente de los dos primeros tableros de control.

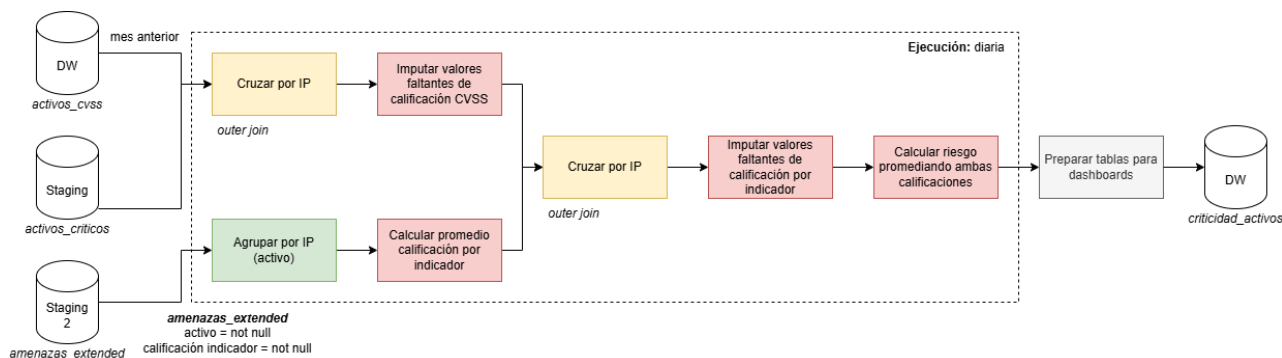
El segundo ETL está enfocado en procesar la información de riesgo de usuarios y, de esta forma, dar soporte al tablero de control con el mismo nombre. Al igual que el primer ETL se ejecuta de forma diaria, con la diferencia de que es más autónomo en términos de las fuentes de datos que intervienen y las tablas en la bodega de datos que modifica.

El análisis de vulnerabilidades, actualizado de forma mensual, cuenta con su ETL dedicado el cual debe ser ejecutado con la misma periodicidad. Similar el ETL de riesgo de usuarios, se puede considerar autónomo en términos de la cantidad de fuentes de datos que intervienen, pero, a diferencia del anterior, se encarga de modificar tablas en la bodega de datos que no solo afectan los tableros de control sino también otros ETLs, como el de criticidad de activos.

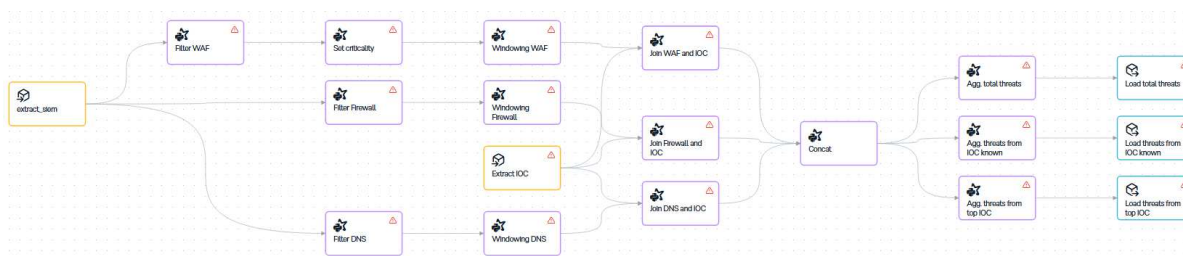
El cuarto ETL, de criticidad de activos, depende de la información generada por los ETLs 1 y 3. A pesar de que se ejecutan con diferentes temporalidades, diaria y mensual, respectivamente, la criticidad de un activo depende de las potenciales amenazas provenientes de indicadores de compromiso detectadas y del análisis de vulnerabilidades. Este ETL se ejecuta de forma diaria buscan asignar una calificación lo más actualizada posible a cada activo crítico.

En los diferentes ETLs, los bloques en rojo representan cálculos realizados a nivel de registro. Los bloques en verde representan agrupaciones por una o varias columnas, y los bloques amarillos representan cruces (*joins*) de diferentes tablas intermedias que se estén construyendo durante la ejecución del ETL. Por otra parte, los bloques azules representan filtros por un valor de columna específico y los morados concatenación de dos o mas tablas que cuentan con una estructura igual o similar en términos de columnas. Los bloques grises representan procesos complementarios para el acceso a fuentes externas de datos (indicadores de compromiso) o preparación final de las tablas que se persistirán, principalmente, en la bodega de datos.





Estos procesos ETL se encuentran en desarrollo dentro de la plataforma Rocket la cual permite, de forma mayoritariamente homologa, desarrollar los diferentes procesos de extracción, transformación y carga de datos previamente descritos. A continuación, se muestra el estado actual del primer ETL dentro de Rocket:



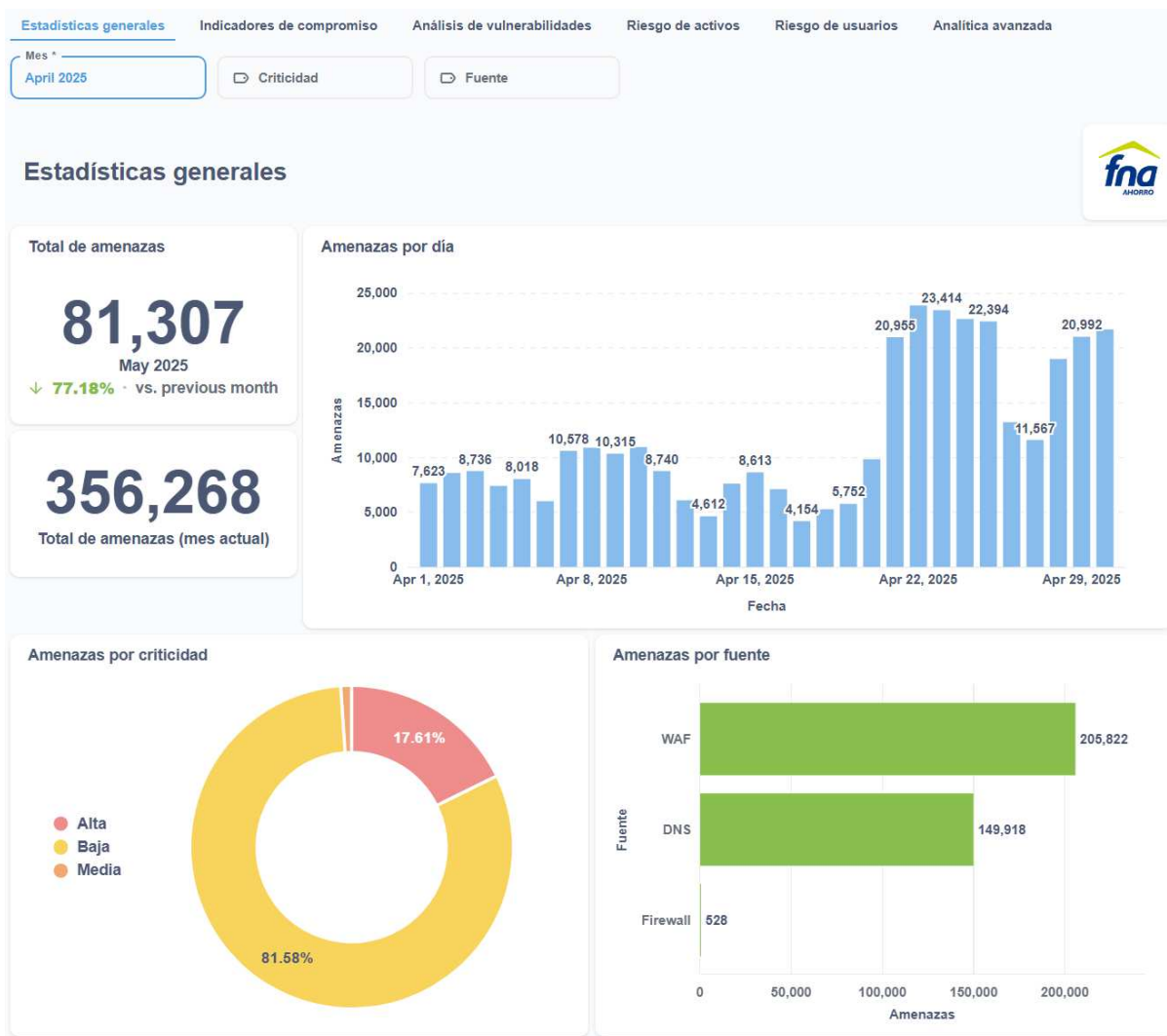
1.2. Tableros de control

Como resultado de los procesos de integración/transformación de datos descritos previamente, se construyen un conjunto de tableros de control en la plataforma Datafabric Discovery los cuales tienen como propósito mostrar el estado actual de los procesos de análisis de amenazas y vulnerabilidades sirviendo a diferentes propósitos. Cada una de las siguientes secciones se enfoca en describir un tablero de control en términos de los indicadores (KPIs), visualizaciones y filtros que integra.

1.2.1. Estadísticas generales

Tras procesar principalmente las fuentes del SIEM, este tablero de control se enfoca en dar una visión general de las potenciales amenazas provenientes de diferentes tipos de dispositivos expuestos a internet (fuente) como firewalls, WAF y DNS. En una ventana de tiempo establecida, el usuario puede obtener información agregada sobre el total de amenazas detectadas respecto al mes anterior, incluyendo su cambio a nivel porcentual.

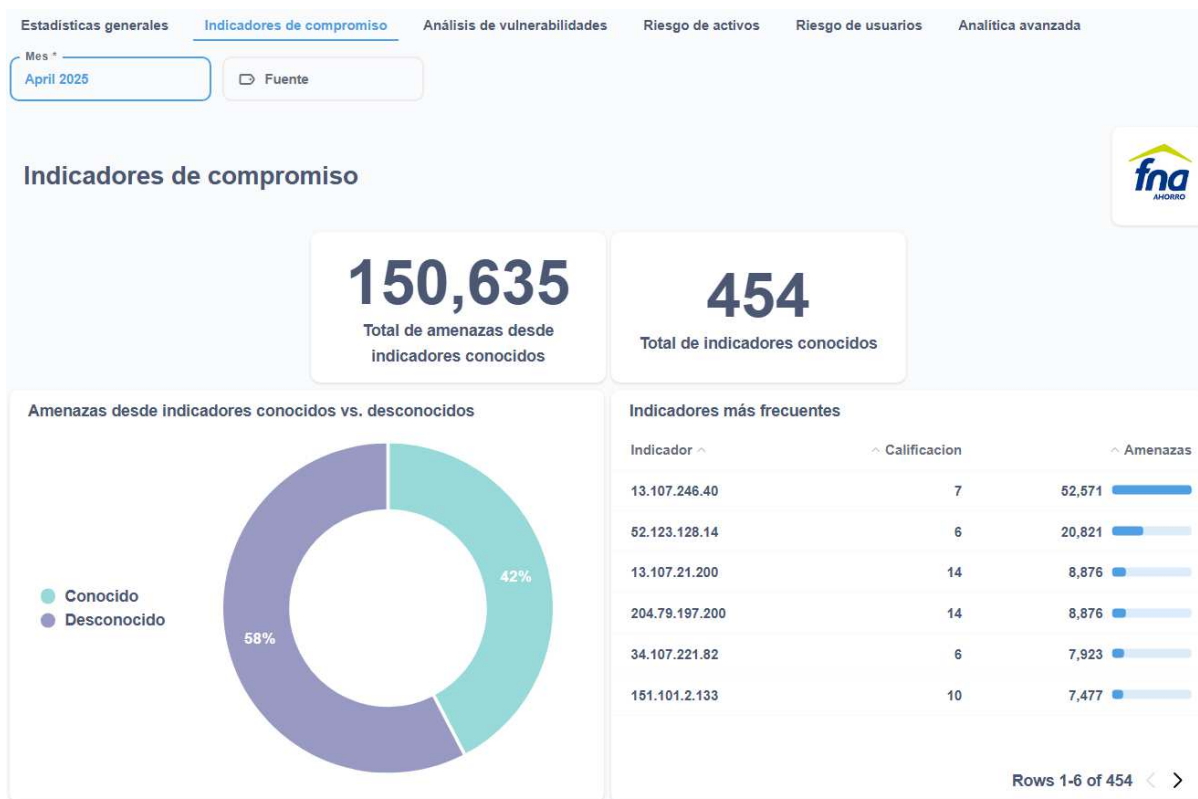
Adicionalmente, el usuario puede visualizar como se han venido comportando cuantitativamente dichas amenazas a través del tiempo, desde cual fuente y la criticidad (baja, media, alta) atribuida a dichas amenazas. De requerirse, el usuario está en la capacidad de enfocar su análisis en un subgrupo de fuentes o criticidades mediante filtros.



1.2.2. Indicadores de compromiso

El segundo tablero de control se propondrá como un caso especial del anterior en donde el foco es ahora cuáles potenciales amenazas pueden ser atribuidas a indicadores de compromiso. En este sentido, el tablero de control permite desarrollar dos tipos de análisis: (i) Del total de amenazas, cuántas provienen de indicadores de compromiso conocidos y desconocidos, y (2) cuántos y cuáles son los indicadores de compromiso más frecuentes. Los análisis dependen de una ventana de tiempo escogida por el usuario y también se pueden enfocar a una fuente particular.

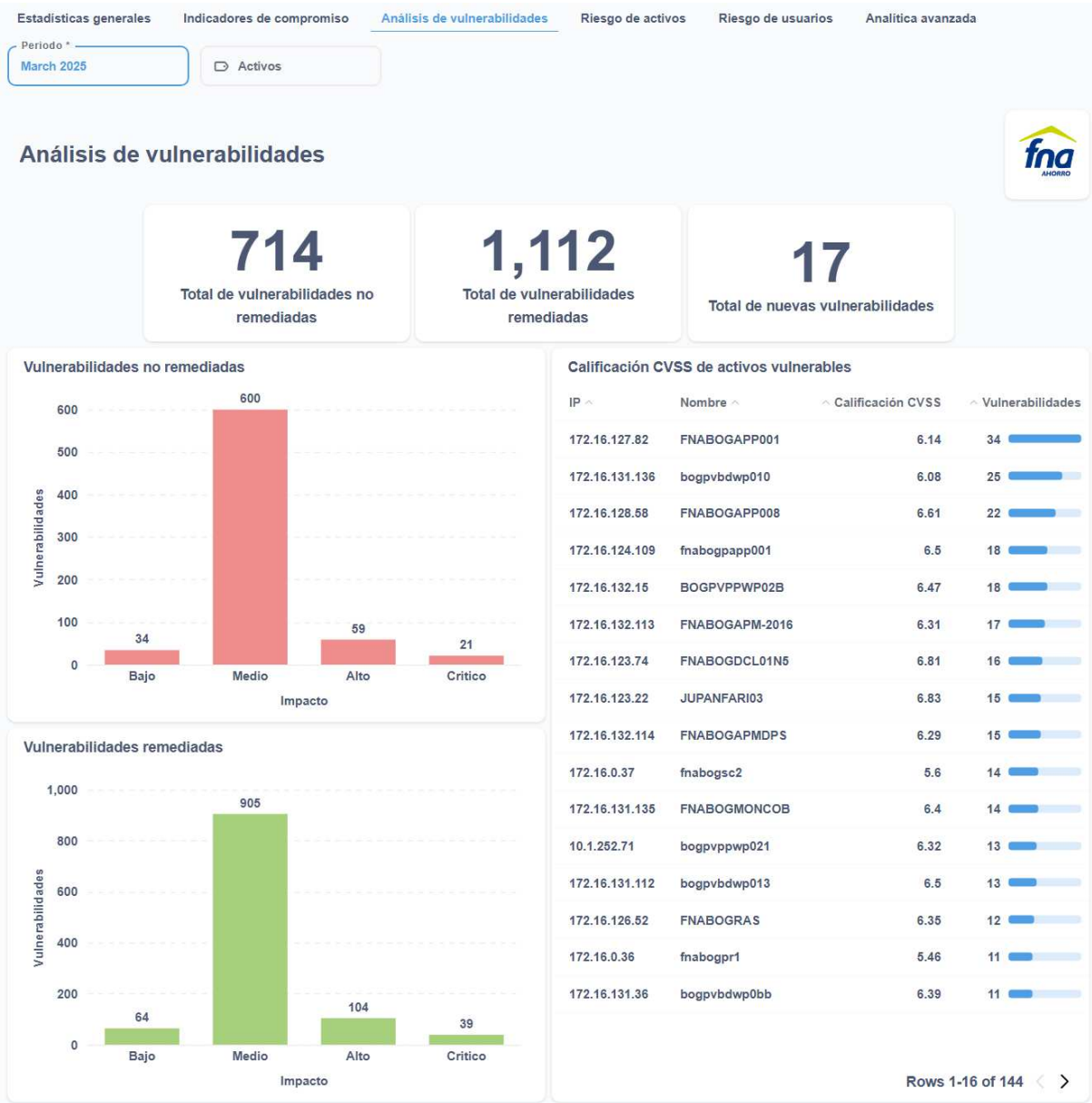
Un detalle adicional incluido en este tablero de control corresponde la calificación de riesgo otorgada a cada indicador de compromiso, la cual es tomada directamente desde ThreatQ.



1.2.3. Análisis de vulnerabilidades

Paralelamente al análisis de amenazas se realiza el análisis de vulnerabilidades. A diferencia de los datos del SIEM, la información del análisis de vulnerabilidades es carga de forma mensual, cuantificando el cambio de estado de las diferentes vulnerabilidades en activos críticos detectadas a través del tiempo. Estos estados incluyen principalmente: vulnerabilidad nueva, vulnerabilidad no remediada y vulnerabilidad remediada. Una vez que una vulnerabilidad cambia de estado no remediada a remediada, dejará de tenerse en cuenta en el análisis del próximo mes. Cada vulnerabilidad cuenta con un impacto asociado, el cual se muestra de forma agregada tanto para las vulnerabilidades remediadas como no remediadas en el mes de análisis.

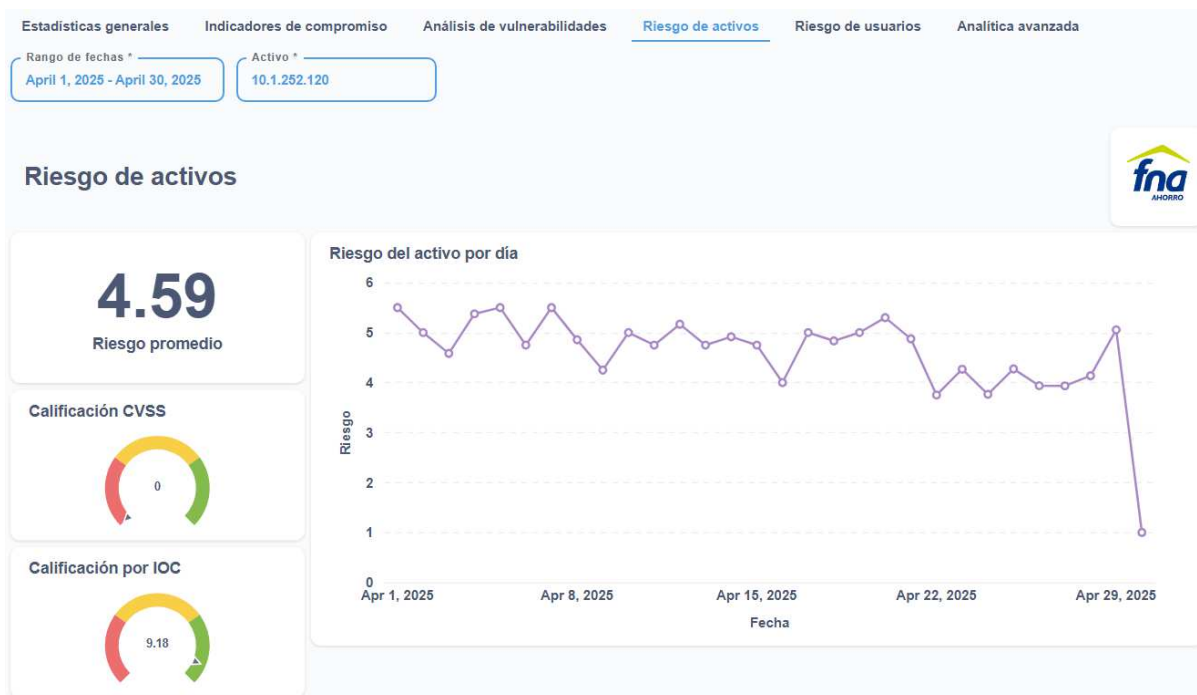
Además, se muestra la lista de activos críticos con vulnerabilidades abiertas (nuevas o no remediadas), el promedio de la calificación CVSS otorgada a cada vulnerabilidad y el total de vulnerabilidades abiertas para el mes actual. A partir de esta lista, el usuario está en capacidad de localizar un activo por su IP y ver su detalle de calificación CVSS y total de vulnerabilidades.



1.2.4. Riesgo de activos

A partir de los análisis de vulnerabilidades y potenciales amenazas, se realiza una estimación del riesgo asociado a cada activo crítico el cual es variable a través del tiempo. Para su calculo se tiene en cuenta la calificación CVSS (vulnerabilidades) otorgada al activo para el mes inmediatamente anterior, y el promedio de las calificaciones de los indicadores de compromiso relacionados al activo durante el análisis de amenazas para la ventana de tiempo seleccionada. El riesgo del activo corresponde al promedio de las dos calificaciones, por lo que, para mayor interpretabilidad por parte del usuario, también se muestran ambos valores de calificación.

El riesgo de activos se centra en un activo particular el cual puede ser localizado mediante su IP. En otros términos, no se entregan indicadores agregados como se realiza en los tableros de control previos, a excepción del riesgo promedio en el tiempo del mismo activo seleccionado.



1.2.5. Riesgo de usuarios

De forma muy similar al tablero de riesgo de activos, se presenta un nuevo tablero de control que corresponde al riesgo de usuarios a través del tiempo, cuya fuente información original son los eventos de DNS tomados del SIEM, pero que, a diferencia del riesgo de activos, el riesgo asociado a cada usuario se calcula a partir de los eventos pre-analizados por una plataforma intermedia.

El riesgo del usuario para un día particular se encuentra dado en un rango de 0 a 5, valor que es calculado a partir de la frecuencia de eventos entregados por la plataforma intermedia. Esta plataforma también entrega una severidad y una credibilidad asociada a cada evento, las cuales son promediadas y mostradas al usuario junto con el riesgo promedio en la ventana de tiempo seleccionada.

El riesgo de usuarios se centra en un usuario particular el cual puede ser localizado mediante su nombre único. En otros términos, no se entregan indicadores agregados como se realiza en los tableros de control iniciales.



CASO DE USO 2 MOVIMIENTOS LATERALES

1. Uso sospechoso de protocolo Web

Un dispositivo ha establecido conexiones HTTP nuevas o inusuales y conexiones SSL/TLS no válidas a una máquina interna, junto con un volumen inesperado de conexiones internas. Este patrón de actividad se ha observado en ataques drive-by internos donde se configura un receptor C2 en un puerto HTTP no estándar, o durante intentos de explotación contra aplicaciones web alojadas internamente. Acción: Investigue la actividad de los dispositivos de origen y destino y compruebe si esta actividad es la esperada por el dispositivo.

1.1. Condiciones de activación

Este modelo se activará si: todos los componentes son verdaderos

Componentes que activaran este modelo:

1. Cualquier conexión interna (8 filtros)
2. Cualquier conexión interna (11 filtros)
3. Cualquier evento de actividad inusual (3 filtros)

Todos los componentes deben activarse dentro de esta cantidad de segundos 10800

Todos los componentes deben compartir puntos finales (endpoints)

1.2. Detalle de cada componente que debe activarse:

1.2.1. Cualquier conexión interna (8 filtros)

Conexiones internas en 60 minutos

FILTROS:

- A. Dirección solo saliente
- B. Puerto de destino = 443
- C. Protocolo de aplicación no es SSL
- D. Protocolo de aplicación no es Desconocido
- E. Conexión mediante proxy no es verdadero
- F. Protocolo es TCP
- G. Protocolo de aplicación no es HTTPS
- H. Puerto de origen != 18000

CONDICIONES DE ACTIVACIÓN: Este componente se activará si

A, B, C, D, E, F, G y H son verdaderas

1.2.2. *Cualquier conexión interna (11 filtros)*

Conexiones internas en 60 minutos

FILTROS:

- A. Dirección solo saliente
- B. Protocolo de aplicación es HTTP
- C. Nueva conexión
- D. Conectividad Inusual > 80
- E. Tamaño individual de bajada > 0
- F. Tamaño individual de subida > 0
- G. Agente de usuario no coincide con la expresión regular `.*(Cb Response|LANDesk|McAfee Agent|Windows-Update-Agent|Skype for Business|QualysGuard|SMS CCM|Avast).*`
- H. Destino interno etiquetado no tiene etiqueta Dispositivo de seguridad
- I. fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- J. URL no coincide con la expresión regular `/^\\(ldlogon|ScanInstructions|landesk|WSVulnerabilityCore|kiali)\\.*.*(qualys).*/i`
- K. Puerto de origen != 18000

CONDICIONES DE ACTIVACIÓN: Este componente se activará si

A, B, C, E, F, G, H, I, J y K son verdaderas

A, B, D, E, F, G, H, I, J y K son verdaderas

1.2.3. *Cualquier evento de actividad inusual (3 filtros)*

Eventos de actividades inusuales >0 en 60 minutos

FILTROS:

- A. Métricas coincidentes es Conexiones internas
- B. Fortaleza (strenght) >= 20
- C. Lista de métricas coincidentes no contiene SMB

CONDICIONES DE ACTIVACIÓN: Este componente se activará si

A, B y C son verdaderas

2. PsExec entrante y descarga de scripts

Un dispositivo descargó un archivo de script sospechoso mientras se controlaba remotamente mediante PSEXEC, la herramienta de administración de SMB. Esta actividad podría indicar un movimiento lateral malicioso. Acción: Revise la legitimidad de la actividad de administración remota, así como la naturaleza del archivo descargado.

2.1. Condiciones de activación

Este modelo se activará si: todos los componentes son verdaderos

Componentes que activarán este modelo:

1. Cualquier SMB Todo (5 filtros)
2. Cualquier conexión externa (6 filtros)

Ambos componentes deben activarse en el orden indicado anteriormente.

Ambos componentes deben activarse dentro de esta cantidad de segundos 3600

2.2. Detalle de cada componente que debe activarse:

2.2.1. Cualquier SMB Todo (5 filtros)

SMB Todo > 0 en 5 minutos

FILTROS

Mensaje contiene psexesvc

Nuevo uso de PYMES

Dirección solo entrantes

Mensaje coincide con la expresión regular `/.\"paexec(outlerrlin) .* /i`

Uso inusual de SMB > 50

CONDICIONES DE ACTIVACIÓN

Este componente se activará si

A, B y C son verdaderas

B, C y D son verdaderas

A, C y E son verdaderas

C, D y E son verdaderas

2.2.2. Cualquier conexión externa (6 filtros)

Conexiones externas > en 5 minutos

FILTROS

Punto final externo raro > 95

URL coincide con la expresión regular `/.\". (apklapp(?:
lication)?lbatlbinlcmdlcpdlldlllexelgadgetlhtaljarljsemlsclmsh(?:
1|2)?(`

Dirección solo saliente

Puerto de destino != 25

Edad del destino < 345600

Nombre de host de confianza es FALSO

CONDICIONES DE ACTIVACION

Este componente se activará si:

A, B, C, D, E y F son verdaderas

3. Movimiento lateral y actividad C2

Detectar un dispositivo realizando una secuencia movimiento lateral y actividad C2. Esto podría indicar una vulnerabilidad activa en el dispositivo. Acción: Revise las alertas del modelo relacionado y si se esperan del dispositivo. Revise también el endpoint externo poco común para detectar señales sospechosas.

3.1. Condiciones de activación

Este modelo se activará si: Se alcanza una puntuación objetivo

Componentes que contribuyen a la puntuación objetivo:

1. Modelo mas de 2 en 24 horas (11 filtros)
2. Modelo mas de 1 en 1 hora (13 filtros)
3. Cualquier modelo (11 filtros)
4. Modelo mas de 1 en 24 horas (12 filtros)

Puntuación objetivo 5

La puntuación objetivo debe alcanzarse dentro de este tiempo (segundos) 129600

3.2. Detalle de cada componente que debe activarse:

3.2.1. Modelo mas de 2 en 24 horas (11 filtros)

- A. Mensaje coincide con la expresión regular (Anomalous Connection \|Anomalous Server Activity \|Compliance \|Compromise \|).*
- B. Mensaje contiene Rare external
- C. Mensaje contiene New Endpoint
- D. Mensaje contiene Increase
- E. Mensaje contiene Beacon
- F. Mensaje contiene Repeat
- G. Incidencia nueva o poco comun de incumplimiento del modelo >= 90
- H. Fuente interna etiquetada no tiene etiqueta Agentes de usuario en conflicto
- I. Edad de la fuente > 172800
- J. Mensaje contiene External Windows
- K. Mensaje contiene to Rare Endpoint

Este componente se activara si:

A, B, G, H y I es verdadero

A, C, G, H y I es verdadero

A, D, G, H y I es verdadero

A, E, G, H y I es verdadero

A, F, G, H y I es verdadero

A, G, H, I y J es verdadero

A, G, H, I y K es verdadero

3.2.2. Modelo mas de 1 en 1 hora (13 filtros)

- A. Mensaje coincide con la expresión regular (Unusual Activity VIDevice VCompliance VAnomalous Connection VIUser V) .*
- B. Mensaje no contiene Activity Identifier
- C. Mensaje no contiene Anomaly Indicator
- D. Mensaje contiene SMB
- E. Mensaje contiene RPC
- F. Mensaje coincide con la expresión regular /."Brute[\s-]?Force .* /i

- G. Mensaje contiene Compromise / Ransomware
- H. Mensaje contiene Anomalous File / Internal
- I. Mensaje coincide con la expresión regular *(High Priority Compliance ModelNew or Uncommon WMIService ControlWinF
- J. Incidencia nueva o poco comun de incumplimiento del modelo >= 90
- K. Fuente interna etiquetada no tiene etiqueta Agentes de usuario en conflicto
- L. Edad de la fuente > 172800
- M. Fuente interna etiquetada no tiene etiqueta Dispositivo

Este componente se activara si:

- A, B, C, D, J, K, L y M son verdaderas
- A, B, C, E, J, K, L y M son verdaderas
- A, B, C, F, J, K, L y M son verdaderas
- G, J, K, L y M son verdaderas
- H, J, K, L y M son verdaderas
- B, C, I, J, K, L y M son verdaderas

3.2.3. Cualquier modelo (11 filtros)

- A. Mensaje no contiene Activity Identifier
- B. Mensaje no contiene Anomaly Indicator
- C. Mensaje coincide con la expresión regular /Anomalous File V Internal V .* (EXEISMBIDownload) .* /i
- D. Mensaje coincide con la expresión regular Compliance V SMB Drive Write
- E. Mensaje contiene Compromise / Ransomware
- F. Mensaje coincide con la expresión regular /Device V (EXE fileISuspicious File) .* /i
- G. Mensaje coincide con la expresión regular /Unusual Activity V ."Write .* /i
- H. Incidencia nueva o poco comun de incumplimiento del modelo >= 90
- I. Fuente interna etiquetada no tiene etiqueta Agentes de usuario en conflicto
- J. Fuente interna etiquetada no tiene etiqueta Dispositivo
- K. Edad de la fuente > 172800

Este componente se activara si:

- A, B, C, H, I, J y K son verdaderas
- A, B, D, H, I, J y K son verdaderas

E, H, I, J y K son verdaderas

A, B, F, H, I, J y K son verdaderas

A, B, G, H, I, J y K son verdaderas

3.2.4. Modelo mas de 1 en 24 horas (12 filtros)

- A. Mensaje coincide con la expresión regular (Anomalous Connection ∨|Anomalous Server Activity ∨|Compliance ∨|Compromise ∨).*
- B. Mensaje contiene Rare external
- C. Mensaje contiene New Endpoint
- D. Mensaje contiene Increase
- E. Mensaje contiene Beacon
- F. Mensaje contiene Repeat
- G. Incidencia nueva o poco comun de incumplimiento del modelo ≥ 90
- H. Fuente interna etiquetada no tiene etiqueta Agentes de usuario en conflicto
- I. Edad de la fuente > 172800
- J. Mensaje contiene External Windows
- K. Mensaje contiene to Rare Endpoint
- L. Campos de mensajes únicos

Este componente se activara si:

A, B, G, H, I y L son verdaderas

A, C, G, H, I y L son verdaderas

A, D, G, H, I y L son verdaderas

A, E, G, H, I y L son verdaderas

A, F, G, H, I y L son verdaderas

A, G, H, I, J y L son verdaderas

A, G, H, I, K y L son verdaderas

CASO DE USO 3 PATRONES DE ATAQUE

1. Múltiples indicadores de cadena de ataque

Un dispositivo ha exhibido comportamientos que indicadores de cadena de muerte múltiple Han emitido una alerta. Esto se observa a menudo en una prueba de penetración, pero también ocurre durante ataques en vivo. Acción: Identifique los dispositivos de origen y su participación en la actividad para determinar si esta representa una amenaza para la red. Etiquete el dispositivo como dispositivo de seguridad si los ataques están autorizados para inhibir futuras alertas de este dispositivo.

1.1. Condiciones de activación

Este modelo se activará si: Se alcanza una puntuación objetivo

Componentes que contribuyen a la puntuación objetivo:

1. Cualquier modelo (5 filtros)
2. Cualquier modelo (5 filtros)
3. Cualquier modelo (5 filtros)
4. Cualquier modelo (5 filtros)
5. Cualquier modelo (5 filtros)
6. Cualquier modelo (5 filtros)
7. Cualquier modelo (5 filtros)
8. Cualquier modelo (5 filtros)
9. Cualquier modelo (5 filtros)
10. Cualquier modelo (5 filtros)
11. Cualquier modelo (5 filtros)
12. Cualquier modelo (5 filtros)
13. Cualquier modelo (5 filtros)
14. Cualquier modelo (6 filtros)
15. Cualquier modelo (5 filtros)
16. Cualquier modelo (7 filtros)
17. Cualquier modelo (5 filtros)

Puntuación objetivo 6

La puntuación objetivo debe alcanzarse dentro de este tiempo (segundos) 6000

1.2. Detalle de cada componente que debe activarse:

1.2.1. Cualquier modelo (5 filtros)

Modelo > 0 en 45 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Attack and Recon Tools
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.2. Cualquier modelo (5 filtros)

Modelo > 0 en 30 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Unusual Activity from New Device
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.3. Cualquier modelo (5 filtros)

Modelo > 0 en 20 minutos

FILTROS

- A. Dirección solo saliente

- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene AT Service
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.4. Cualquier modelo (5 filtros)

Modelo > 0 en 10 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene New or Unusual Remote Command Execution
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.5. Cualquier modelo (5 filtros)

Modelo > 0 en 30 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene WinRM
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.6. Cualquier modelo (5 filtros)

Modelo > 0 en 30 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Scan
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.7. Cualquier modelo (5 filtros)

Modelo > 0 en 10 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene `/. *Brute[\s-]?Force.* /i`
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.8. Cualquier modelo (5 filtros)

Modelo > 0 en 5 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene New or Uncommon Service Control
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.9. Cualquier modelo (5 filtros)

Modelo > 0 en 10 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Kerberos Failures
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.10. Cualquier modelo (5 filtros)

Modelo > 0 en 30 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Unusual Internal Connections
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.11. Cualquier modelo (5 filtros)

Modelo > 0 en 60 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Tunnel
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.12. Cualquier modelo (5 filtros)

Modelo > 0 en 10 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Mensaje contiene Reverse DNS Sweep
- E. Fuente interna etiquetada no tiene etiqueta Apoderado

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.13. Cualquier modelo (5 filtros)

Modelo > 0 en 15 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Fuente interna etiquetada no tiene etiqueta Apoderado
- E. Mensaje contiene New Admin Credentials on Client

Este componente se activara si:

A, B, C, D y E son verdaderas

A, B, C, D y F son verdaderas

1.2.14. Cualquier modelo (6 filtros)

Modelo > 0 en 15 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Fuente interna etiquetada no tiene etiqueta Apoderado
- E. Mensaje contiene Unusual Internal Remote Desktop
- F. Mensaje contiene Active Remote Desktop Tunnel

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.15. Cualquier modelo (5 filtros)

Modelo > 0 en 15 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Fuente interna etiquetada no tiene etiqueta Apoderado
- E. Mensaje contiene New Admin Credential Ticket Request

Este componente se activara si:

A, B, C, D y E son verdaderas

1.2.16. Cualquier modelo (7 filtros)

Modelo > 0 en 60 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Fuente interna etiquetada no tiene etiqueta Apoderado
- E. Mensaje contiene Possible RPC Lateral Movement
- F. Mensaje contiene Possible RPC Recon Activity
- G. Mensaje contiene Anomaly Indicator

Este componente se activara si:

A, B, C, D, E y G son verdaderas

A, B, C, D, F y G son verdaderas

1.2.17. Cualquier modelo (5 filtros)

Modelo > 0 en 15 minutos

FILTROS

- A. Dirección solo saliente
- B. Fuente interna etiquetada no tiene etiqueta Dispositivo de seguridad
- C. Fuente interna etiquetada no tiene etiqueta Puerta
- D. Fuente interna etiquetada no tiene etiqueta Apoderado
- E. Mensaje contiene Suspicious New User Agents

Este componente se activara si:

A, B, C, D y E son verdaderas

CASO DE USO 4 EVALUACIÓN INTEGRAL DE RIESGOS

El caso de uso "Evaluación Integral de Riesgos" está diseñado para proporcionar una visión completa y centralizada del nivel de riesgo al que está expuesta una organización, permitiendo identificar, gestionar y mitigar amenazas potenciales en tiempo real. Este modelo se organiza en distintos niveles jerárquicos y utiliza una arquitectura lógica y técnica avanzada para un monitoreo y análisis eficiente. A continuación se explican los aspectos clave del funcionamiento:

1. Definición conceptual

El modelo está estructurado en 4 niveles jerárquicos que permiten evaluar y clasificar las diferentes fuentes de riesgo:

- **Nodo:** Representa cada servicio individual que se encuentra monitoreado, generando un valor de riesgo específico.
- **Segmento:** Agrupa nodos con objetivos o funciones similares, consolidando resultados para un análisis más amplio.
- **Capa:** Integra varios segmentos según su proximidad con la infraestructura y su funcionalidad, clasificándose en 5 capas específicas (EXOS, THERMOS, MESOS, STRATOS y TROPOS).
- **DEFCON:** Es el indicador global agregado generado a partir de las cinco capas, que ofrece una visión consolidada del riesgo, clasificada en 5 niveles (Crítico, Muy Alto, Alto, Medio y Bajo).

Cada fuente de datos genera información de riesgo que pasa por fórmulas específicas, utilizando un sistema de ponderación (pesos) basado en la relevancia de parámetros críticos.

2. Arquitectura lógica

La lógica se basa en un modelo escalonado, donde los cálculos se realizan siguiendo una jerarquía:

- **Nodo:** Integración de riesgos individuales de servicios. Ejemplos incluyen análisis de monitoreo digital, redes sociales, credenciales, aplicaciones externas y mucho más.
- **Segmento:** Los valores de riesgo de los nodos se ponderan para establecer un nivel global segmentado.
- **Capa:** Las capas consolidan los riesgos por segmento utilizando fórmulas específicas. Cada capa establece niveles de criticidad basándose en la suma ponderada de los segmentos.
- **DEFCON:** Agrega y estandariza la criticidad general combinando el estado de todas las capas, cada una con un peso del 20%.

Las fórmulas específicas permiten que el sistema sea adaptable y modular, según las características de los servicios monitoreados.

3. Requisitos y fuentes de datos

El modelo requiere una identificación previa de todos los servicios activos en la organización, además de sus fuentes de información. Estos son monitoreados a través de herramientas específicas que generan indicadores críticos. Por ejemplo:

- **Monitoreo Digital:** Analiza riesgos como sentimiento de marca, aplicaciones externas y redes sociales.
- **Cibercrimen:** Sigue vulnerabilidades relacionadas con credenciales filtradas y ataques a dominios.
- **Inteligencia Preventiva:** Anticipa amenazas basándose en información y alertas preventivas.
- **Infraestructura y Seguridad:** Analiza riesgos relacionados con infraestructuras, identidades y datos en plataformas sensibles.

Los cálculos de riesgo dependen de registros, detecciones y alertas, clasificándolos según niveles de criticidad establecidos. Estos indicadores son individualmente configurados para cada cliente, evaluando umbrales personalizados.

4. Arquitectura técnica

El modelo recopila y centraliza los datos en un sistema adaptado que procesa, pondera y consolida los riesgos en cada nivel. Con una estructura jerárquica, los cálculos garantizan precisión y relevancia:

- Nivel 1: Nodos individuales.
- Nivel 2: Segmentos formados por nodos relacionados.
- Nivel 3: Capas que integran segmentos según la infraestructura.
- Nivel 4: DEFCON como indicador global.

Esta organización lógica permite la agregación escalada y facilita la visualización de riesgos desde lo más granular (nodos) hasta lo más global (DEFCON).

5. Productos del modelo

El caso de uso genera paneles gráficos interactivos (dashboards) que presentan la información procesada en diferentes niveles:

- **Dashboards por niveles:** Riesgos clasificados por nodos, segmentos, capas y DEFCON.

- **Personalización visual:** Los resultados se presentan a través de herramientas externas de BI, como Looker Studio, garantizando claridad y utilidad en la toma de decisiones.
- **Alertas dinámicas:** Los servicios son monitoreados constantemente, con alertas en tiempo real cuando cambios significativos o situaciones críticas surgen.

5.1. EXOS

(Digital Monitoring Risk x 0,40) + (E-crime Monitoring Risk x 0,40) + (Threat Monitoring Risk x 0,20)

- %50 > = 5 (Suma de alertas críticas, altas)
- Entre 40% y 49% = 4 - Muy alto
- Entre 30% y 39% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

Digital Monitoring

(Brand Sentiment Risk x 0,60) + (Social Monitoring Risk x 0,30) + (External application Risk x 0,10)

- %90 > = 5 - Crítico
- Entre %80 y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- %30% < = 1 Bajo

Brand Sentiment

Social Monitoring

External Application Monitor

E-crime Monitoring

(Critical Information Risk x 0,30) + (Domain Attacks Risk x 0,70)

- %40 > = 5 (Suma de alertas críticas, altas)
- Entre 30% y 39% = 4 - Muy alto
- Entre 20% y 29% = 3 - Alto
- Entre 10% y 19% = 2 - Medio
- %9 < = 1 - Bajo

Critical information leaks

Domain attacks

Threats Monitoring

(Intelligence Preventive Risk x 0,30) + (CyberFraud x 0,70)

- %60 > = 5 (Suma de alertas críticas, altas)
- Entre 50% y 59% = 4 - Muy alto
- Entre 40% y 49% = 3 - Alto
- Entre 30% y 39% = 2 - Medio
- %29 < = 1 - Bajo

Cyberfraud

- %80 > = 5 (Suma de alertas críticas, altas)
- Entre 70% y 79% = 4 - Muy alto
- Entre 50% y 69% = 3 - Alto
- Entre 30% y 49% = 2 - Medio
- %29 < = 1 - Bajo

Intelligence Preventive

5.2. THERMOS

(Corporate Intelligence x 0,45) + (Cloud x 0,45) + (Third Parties x 0,10)

- %50 > = 5 (Suma de alertas críticas, altas)
- Entre 40% y 49% = 4 - Muy alto
- Entre 30% y 39% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

Corporate Intelligence

(Risk Scoring Status x 0,80) + (VIP Fingerprint x 0,10) + (Infrastructure Fingerprint x 0,10)

- %70 > = 5 - Crítico
- Entre %60 y 69% = 4 - Muy Alto
- Entre 50% y 59% = 3 - Alto

- Entre 40% y 49% = 2 - Medio
- %39% < = 1 Bajo

Risk Scoring Status

VIP Fingerprint

Infrastructure Fingerprint

Cloud

(Vulnerabilities & Weaknesses Riskx 0,70) + (Attacks and Threat Behavior Risk x 0,30)

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

Third Parties

(Risk Scoring Status x 0,50) + (CyberReputation Risk x 0,30) + (Vulnerabilities & Weaknesses Risk x 0,20)

- %90 > = 5 - Crítico
- Entre %80 y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- %30% < = 1 Bajo

Risk Scoring Status

CyberReputation Risk

Vulnerabilities & Weaknesses Risk

5.3. MESOS

(Exposure monitoring x 0,25) + (Operation Availability x 0,60) + (Vulnerability Intelligence x 0,15)

- %50 > = 5
- Entre 40% y 49% = 4 - Muy alto
- Entre 30% y 39% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

Exposure monitoring

(Applications x 0,50) + (communications x 0,25) + (services x 0,25)

- %90 > = 5 - Crítico
- Entre %80 y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- %30% < = 1 Bajo

Applications

Communications

Services

Operation Availability

(Applications x 0,50) + (communications x 0,25) + (services x 0,25)

Applications

Communications

Services

Vulnerability Intelligence

(Early detection x 0,90 + Risk landscapes x 0,10)

Early detection

Risk Landscape

5.4. STRATOS

(External Application Security x 0,33) + (External Communication Security x 0,33) + (External Services Security x 0,33)

- %50 > = 5
- Entre 40% y 49% = 4 - Muy alto
- Entre 30% y 39% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

External Applications Security

(Vulnerabilities & Weaknesses Riskx 0,25) + (Attacks and Threat Behavior Risk x 0,75)

- %90 > = 5 - Crítico
- Entre %80 y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- %30% < = 1 Bajo

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

External Communication Security

(Vulnerabilities & Weaknesses Risk x 0,25) + (Attacks and Threat Behavior Risk x 0,75)

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

External Services Security

Weaknesses Riskx 0,25) + (Attacks and Threat Behavior Risk x 0,75)

Vulnerabilities & Weaknesses Risk

5.5. TROPOS

(Infrastructure security x 0,33) + (Identity security x 0,33) + (Data security x 0,33)

- %50 > = 5 Crítico
- Entre 40% y 49% = 4 - Muy alto
- Entre 30% y 39% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

Infrastructure Security

(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)

- %90 > = 5 - Crítico

- Entre 80% y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- 30% < = 1 Bajo

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

CounterIntelligence & Deception

External Communication Security

(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)

- 90% > = 5 - Crítico
- Entre 80% y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- 30% < = 1 Bajo

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

CounterIntelligence & Deception

Data Security

(Vulnerabilities & Weaknesses Riskx 0,20) + (Attacks and Threat Behavior Risk x 0,75) + (CounterIntelligence & Deception x 0,05)

- 90% > = 5 - Crítico
- Entre 80% y 89% = 4 - Muy Alto
- Entre 60% y 79% = 3 - Alto
- Entre 30% y 59% = 2 - Medio
- 30% < = 1 Bajo

Vulnerabilities & Weaknesses Risk

Attacks and Threat Behavior Risk

CounterIntelligence & Deception

5.6. DEFCON

(Capa EXOS x 0,2) + (Capa THERMOS x 0,2) + (Capa MESOS x 0,2) + (Capa STRATOS x 0,2) + (Capa TROPOS x 0,2)

- %80 > = 5 Crítico
- Entre 60% y 79% = 4 - Muy alto
- Entre 40% y 69% = 3 - Alto
- Entre 20% y 29% = 2 - Medio
- %19 < = 1 - Bajo

A - DEFCON LEVEL

B - DEFCON RISK SCORING R...

▼ C - EXOS Detail

EXOS - Digital Monitoring

EXOS - E-Crime Monitoring

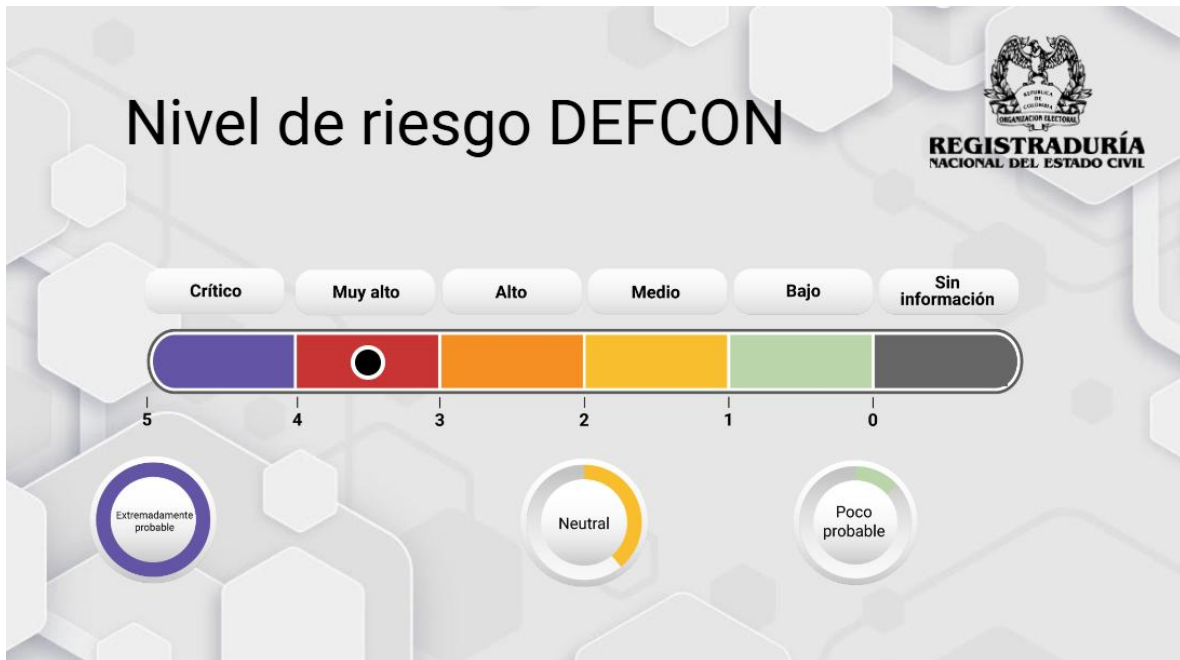
EXOS - Threats Monitoring

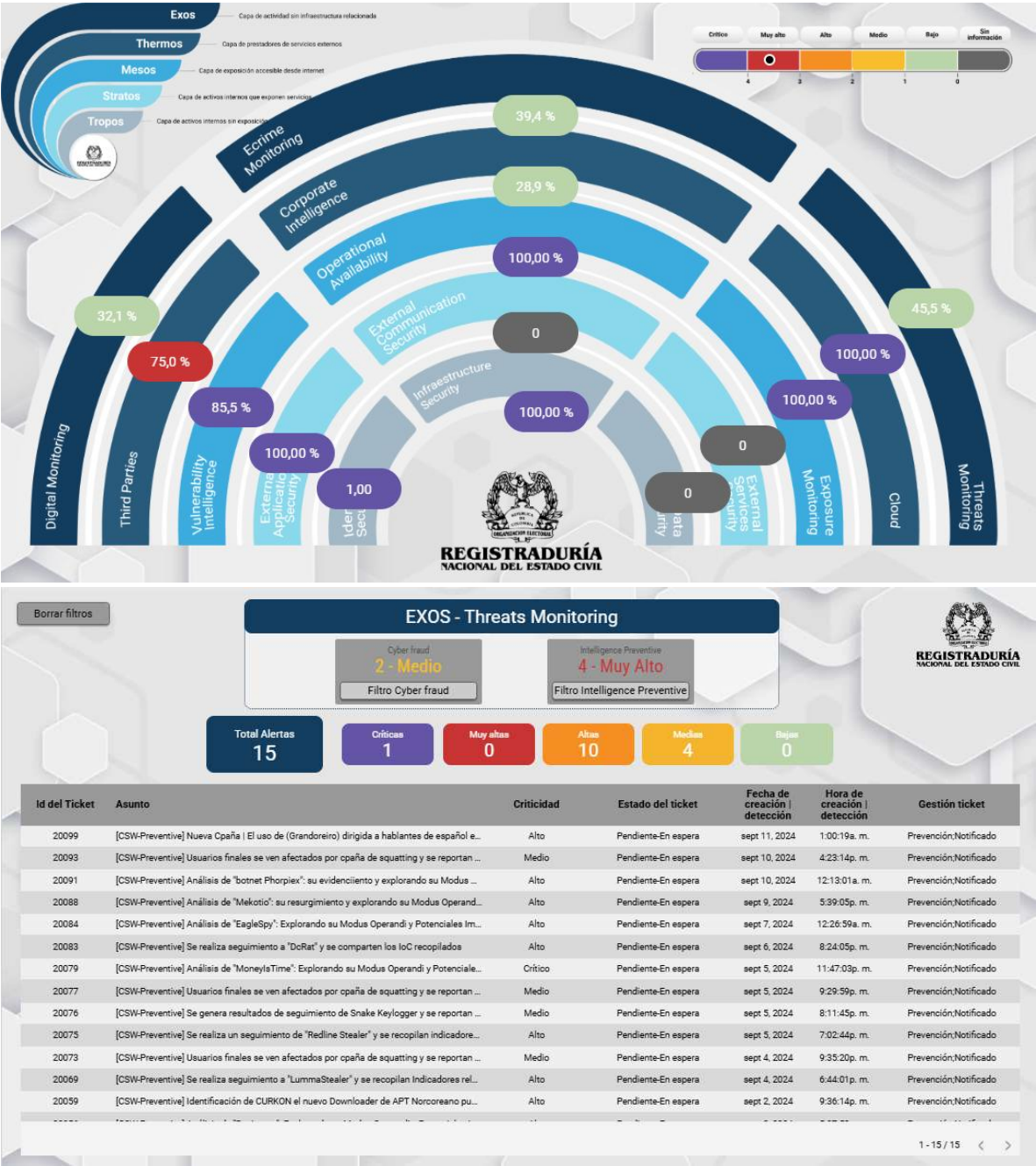
► C - THERMOS Detail

► C - MESOS Detail

► C - STRATOS Detail

► C - TROPOS Detail





Versión Stratio Data Fabric

(BI Interno)

FNA Cybersight

✎ 📧 📄 ⌚ | 📌 ⓘ ...

DEFCON

Risk Scoring Ratio

EXOS Layer Detail

MESOS Layer Detail

STRATOS Layer Detail

TROPOS Layer Detail



Nivel de riesgo DEFCON

Critico	Muy Alto	Alto	Medio	Bajo	Sin Informacion
				1 - Bajo	

MNEMO

FNA Cybersight

✎ 📧 📄 ⌚ | 📌 ⓘ ...

DEFCON

Risk Scoring Ratio

EXOS Layer Detail

MESOS Layer Detail

STRATOS Layer Detail

TROPOS Layer Detail

Risk Scoring Ratio



EXOS			
1 - Bajo	9.6% Digital Monitoring	15% E-Crime Monitoring	20.7% Threats Monitoring
MESOS			
1 - Bajo	0.9% Vulnerability Intellig...		
STRATOS			
1 - Bajo	50.25% External Application...	6% External Communica...	
TROPOS			
2 - Medio	8.5% Infrastructure Secu...	0% Data Security	

MNEMO



EXOS Layer

1 - Bajo
EXOS_NIVEL



Detalle

Segmentos

Nodos

1 - Bajo

Digital
Monitoring

1 - Bajo
Brand Sentiment

1 - Bajo
Social Monitoring

1 - Bajo
External Application ...

2 - Medio

E-Crime
Monitoring

3 - Alto
Critical Information ...

1 - Bajo
Domains Attack

1 - Bajo

Threats
Monitoring

4 - Muy Alto
Intelligence Preventive



CASO DE USO 5 CORRELACIÓN AVANZADA

1.1 Integración de la Correlación Avanzada en el Monitoreo del SOC

La avanzada capacidad de correlación ofrecida por nuestra plataforma de ciber analítica no solo fortalece el monitoreo el cual es llevado a cabo por el Centro de Operaciones de Seguridad (SOC), sino que también ofrece un enfoque proactivo en la identificación de amenazas. Esta integración es clave para optimizar la eficiencia de nuestras operaciones de seguridad.

El proceso de correlación avanzada se inicia con la identificación de eventos aislados, a menudo insignificantes por sí mismos, pero que en conjunto pueden representar una amenaza significativa. Esta capacidad permite a nuestro sistema de ciber analítica detectar actividades sospechosas seguidas de tareas administrativas en endpoints, generando alertas que el personal del SOC, operativo 24/7, puede analizar rápidamente.

Este procedimiento minucioso de análisis no solo permite una detección temprana de posibles amenazas, sino que también asegura una respuesta rápida y bien informada, que se traduce en alertas oportunas al cliente final si se considera necesario. Al desplegar esta capacidad de análisis profundo en tiempo real, el SOC se mantiene a la vanguardia en la protección contra incidentes de seguridad cibernética, asegurando la continuidad de las operaciones de negocio y la confianza del cliente en nuestros servicios.

Por lo tanto, la interoperabilidad entre la inteligencia ofrecida por la correlación avanzada y el monitoreo continuo del SOC establece un sistema robusto que responde a la excelencia operativa y a la seguridad de nuestros clientes.

1.1 Actividad sospechosa seguida de tarea de administración de endpoint

Esta regla se activa cuando se realizan tareas de administración (descargar un archivo, actualizar los derechos de usuario, ejecutar como otro usuario, etc.) después de que se detecta una actividad sospechosa en el mismo sistema.

1.2 Logica General

A continuación se describen los componentes lógicos generales que se deben cumplir para la ejecución de la regla de correlación avanzada, estos componentes generales agrupan una serie de criterios detallados que se explicaran en la sección posterior.

- Actividad sospechosa seguida de tarea de administración de endpoint se ejecuta en coincidencia
- when Administration habitual de endpoints match at least 1 times in 10 minutes after
- any of Actividades sospechosas en puntos finales match with the same Identifier

1.3 Logica Detallada

A continuación, se detalla la composición de cada uno de los componente generales presentados anteriormente, el objetivo es poder visualizar los criterios unitarios que componente la lógica de ejecución de la regla.

1.3.1 Administración habitual de endpoints

Este bloque de construcción define actividades de administración habituales, como la gestión de usuarios, la descarga de archivos en la línea de comandos y la ejecución con privilegios elevados.

Aplicar definición de comportamiento: Administración habitual de endpoints en eventos detectados y cuando un evento coincida con alguno de los siguientes criterios:

- Privilegios de administrador añadidos (Unix)
- Privilegios de administrador añadidos (Windows)
- Privilegios de administrador eliminados (Windows)
- Descargar utilidades en eventos
- Descubrimiento de grupos o cuentas
- Archivo o carpeta ocultos creados
- Descubrimiento de políticas de contraseñas (Unix)
- Descubrimiento de políticas de contraseñas (Windows)
- Ejecutar como superusuario u otro usuario (Unix)
- Ejecutar como superusuario u otro usuario (Windows)
- Cuenta de usuario añadida (Unix)
- Cuenta de usuario añadida (Windows)
- Cuenta de usuario eliminada (Unix) User Account Deleted (Windows)
- File Permission Changed
- PowerShell File Download Activity
- PowerShell File Upload Activity
- Directory Discovery (Windows)
- Repeated Nslookup Usage
- Hostname or Network Discovery
- Multiple File Deletions on Endpoint System
- Directory Discovery (Unix)
- Administrative Share Accessed

1.3.1.1 Privilegios de administrador añadidos (Unix)

Aplicar Privilegios de administrador añadidos (Linux) en eventos detectados

- when an event matches any of the following Operating System is Unix
- and when the event category for the event is one of the following Authentication.Group Member Add Success
- and when the event matches Application (custom) is any of usermod
- and when the event matches Group Name (custom) is any of sudo

1.3.1.2 Privilegios de administrador añadidos (Windows)

Aplicar Privilegios de administrador añadidos (Windows) en eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following Authentication.Group Member Added
- and when the event matches Group Name is any of Administrators, Group Name is any of Administradores

1.3.1.3 *Privilegios de administrador eliminados (Windows)*

Aplicar BB:BehaviorDefinition: Privilegios de administrador eliminados (Windows) en eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following Authentication.Group Member Removed
- and when the event matches Group Name (custom) is any of Administrators

1.3.1.4 *Descargar utilidades en eventos*

Aplicar Descargar utilidades en eventos en eventos detectados

- when an event matches any of the following Operating System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following Audit.General Audit Event, System.Process Creation Success, Audit.Command Execution Success, Audit.Command Execution Attempt
- and when the event matches Process Name (custom) is not N/A
- and when the event matches Process Name (custom) matches any of expressions (?i)(bitsadmin\.exe|c(ertutil\.exe|url)|ftp|nc|wget)

1.3.1.5 *Descubrimiento de grupo o cuenta*

Aplicar Descubrimiento de grupos o cuentas en eventos detectados

- when an event matches any of the following Operating System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following System.Process Creation Success, Audit.Command Execution Attempt
- and when the event matches "Command Arguments" is not NULL or "Command" is not NULL AQL filter query

- and when the event matches LOWER("Command Arguments") MATCHES '.*"(groups|users|w(ho(ami)?)?|ldapsearch|id)".*' OR "Command" MATCHES '.*?net(\.exe\)"?)\s+(localgroup|group.*?\domain).*' AQL filter query

1.3.1.6 Archivo o carpeta ocultos creados

Aplicar la creación de archivos o carpetas ocultos en los eventos detectados

- when an event matches any of the following Operating System System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following System.File Created
- and when the event matches ("Filename" is not NULL and Filename not in ('.viminfo')) OR "Encoded Filename" is not NULL AQL filter query
- and when the event matches "Filename" MATCHES '^(\.*/)*\..*' OR "Encoded Filename" MATCHES '^(.{2})*2F)*2E.*' OR "File Permissions" MATCHES '\d?(12|10|04)0\d00' AQL filter query

1.3.1.7 Descubrimiento de políticas de contraseñas (Unix)

Aplicar el Descubrimiento de políticas de contraseñas (Unix) a los eventos detectados

- when an event matches any of the following Operating System System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following Audit.Command Execution Attempt
- and when the event matches Command Arguments (custom) is not N/A
- and when the event matches LOWER("Command Arguments") MATCHES '.*\Vetc/(pam.d/(common-password|system-auth)|security/pwquality.conf|login.defs).*' AQL filter query

1.3.1.8 Descubrimiento de políticas de contraseñas (Windows)

Aplicar el Descubrimiento de políticas de contraseñas (Windows) a los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following System.Process Creation Success
- and when the event matches Command (custom) is not N/A
- and when the event matches LOWER("Command") MATCHES '.*?net(\.exe\)"?)\s+accounts(\s+\/(domain))?.*' AQL filter query

1.3.1.9 Ejecutar como superusuario u otro usuario (Unix)

Aplicar la función "Ejecutar como superusuario u otro usuario" (Unix) en los eventos detectados.

- when an event matches any of the following Operating System is Unix
- and when the event category for the event is one of the following System.Process Creation Success
- and when Audit ID (custom) not equals Effective User ID (custom)
- and NOT when the event matches User ID (custom) is any of [0 or 100]
- and NOT when the event matches Process Name (custom) is any of [su or sudo or sh or bash]

1.3.1.10 Ejecutar como superusuario u otro usuario (Windows)

Aplicar la función "Ejecutar como superusuario u otro usuario" (Windows) en los eventos detectados.

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following System.Process Creation Attempt, System.Process Creation Success
- and when the event matches Token Elevation Type (custom) is not N/A
- and when the event matches "Token Elevation Type" in ('%%1937', '%%1938') AQL filter query

1.3.1.11 Cuenta de usuario añadida (Unix)

Aplicar la cuenta de usuario añadida (Unix) a los eventos detectados

- when an event matches any of the following BB:DeviceDefinition: Operating System is Unix
- and when the event category for the event is one of the following Authentication.User Account Added
- and when the event matches LOWER("Application") MATCHES 'useradd|adduser' AQL filter query

1.3.1.12 Cuenta de usuario añadida (Windows)

Aplicar la cuenta de usuario añadida (Windows) a los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event QID is one of the following (5000892) Success Audit: A user account was created

1.3.1.13 Cuenta de usuario eliminada (Unix)

Aplicar la función "Cuenta de usuario eliminada" (Unix) a los eventos detectados

- when an event matches any of the following BB:DeviceDefinition: Operating System is Unix
- and when the event category for the event is one of the following Authentication.User Account Removed
- and when the event matches LOWER("Application") MATCHES '.*(userdel|deluser).*' AQL filter query

1.3.1.14 Cuenta de usuario eliminada (Windows)

Aplicar la eliminación de cuenta de usuario (Windows) en los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event QID is one of the following (5000897) Success Audit: A user account was deleted

1.3.1.15 Permiso de archivo modificado

Aplicar BB:CategoryDefinition: Permiso de archivo modificado en los eventos detectados

- when an event matches any of the following Operating System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following System.Process Creation Success
- and when the event matches Audit ID (custom) is not N/A
- and when the event matches Call Type (custom) is 268
- and when the event matches Process Name (custom) is any of chmod

1.1.1.1 Actividad de descarga de archivos de PowerShell

Aplicar la actividad de descarga de archivos de PowerShell en eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following Audit.Command Execution Success
- and when the event matches Command (custom) is not N/A
- and when the event matches LOWER("Command") matches '.*(invoke-webrequest|start-bitstransfer|\\(new-object \\system\\.net\\.webclient\\)\\.download(file|string)\\).*' AQL filter query

1.1.1.2 Actividad de carga de archivos de PowerShell

Aplicar la actividad de carga de archivos de PowerShell en los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following Audit.Command Execution Success
- and when the event matches LOWER("Command") MATCHES '.*?\\.uploadfile\\(.*' AQL filter query

1.1.1.3 Descubrimiento de directorios (Unix)

Aplicar el Descubrimiento de directorios (Unix) en los eventos detectados

- when an event matches any of the following Operating System System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400

- and when the event category for the event is one of the following Audit.Command Execution Attempt
- and when the event matches Command Arguments (custom) is not N/A
- and when the event matches LOWER("Command Arguments") MATCHES '.*?("[ls".*?"]-[^\\s-]{0,3}(d|r)|"find".*?"-type"\\sa[0-9]+="d").*' AQL filter query

1.1.1.4 Descubrimiento de directorios (Windows)

Aplicar el Descubrimiento de directorios (Windows) en los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event category for the event is one of the following Audit.Command Execution Success
- and when the event matches LOWER("Command") MATCHES '(. *?get-childitem.*?-recurse.*|. *?foreach.*?\\{.*?get-childitem.*?\\}.*)' AQL filter query

1.1.1.5 Uso repetido de Nslookup

Aplicar el uso repetido de Nslookup en los eventos detectados

- when an event matches any of the following Operating System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following System.Process Creation Success
- and when the event matches Process Name (custom) matches any of expressions (?i)nslookup(\\.exe)?
- and when at least 5 events are seen with the same Machine Identifier (custom) in 5 minutes

1.1.1.6 Eliminación de varios archivos en el sistema de endpoints

Aplicar la eliminación de varios archivos en el sistema de endpoints en eventos detectados

- when an event matches any of the following Operating System is detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilasoft QJRN/400
- and when the event category for the event is one of the following System.File Deleted
- and when the event matches Filename (custom) is not N/A
- and when the event matches NOT ("File Extension" IN ('swp', 'swpx') OR "Filename" MATCHES '~\\\$.*') AQL filter query
- and when at least 3 events are seen with the same Machine Identifier (custom) in 10 minutes

1.1.1.7 Acceso a recurso compartido administrativo

Aplicar acceso a recurso compartido administrativo en eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log
- and when the event QID is one of the following (5001108) Success Audit: A network share object was accessed
- and when the event matches Share Name (custom) is any of [ADMIN\$ or C\$]

1.1.2 Actividades sospechosas en puntos finales

Este componente define las actividades sospechosas en endpoints.

Aplicar Actividades sospechosas de endpoints en eventos detectados y cuando un evento coincida con alguno de los siguientes criterios:

1.1.2.1 Operating System

Aplicar el sistema operativo a los eventos detectados

- when the event(s) were detected by one or more of Microsoft Windows Security Event Log, Linux OS, Hewlett Packard UniX, Solaris Operating System Authentication Messages, IBM AIX Audit, IBM AIX Server, Mac OS X, IBM i, Cilsoft QJRN/400

1.1.2.2 Reglas de correlacion

- Comunicación con un host potencialmente hostil
- Comunicación con una dirección IP potencialmente hostil
- Descubrimiento de actividades de volcado de credenciales FNA
- Permiso de archivo crítico modificado
- Herramienta de seguridad crítica desactivada (Unix)
- Herramienta de seguridad crítica detenida
- Detección de IOC malicioso en eventos
- Archivo creado con anulación de derecha a izquierda
- Archivo creado con espacio después del nombre de archivo
- Posible secuestro del Modelo de objetos componentes (COM)
- Posible secuestro de DLL
- Posible falsificación de aplicaciones maliciosas
- Entorno de programación generado por un proceso sospechoso
- Enmascaramiento de procesos (Unix)
- Enmascaramiento de procesos (Windows)
- Proceso bloqueado recomendado en ejecución
- Creación de cuenta de usuario seguida de eliminación de cuenta (Unix)
- Creación de cuenta de usuario seguida de eliminación de cuenta (Windows)
- Intento de eliminar instantáneas
- Cobalt Strike Comportamiento detectado
- Errores excesivos de acceso a recursos compartidos administrativos desde el mismo host
- Eliminación y creación excesivas de archivos
- Errores excesivos de inicio de sesión a través de la conexión de red

- Errores excesivos de inicio de sesión a través de la conexión de red a varias máquinas
- Uso excesivo de Nslookup
- Instrucciones de descifrado de ransomware creadas
- Extensión de archivo cifrada de ransomware
- Ransomware: Maze IOC en eventos
- Ransomware: REvil IOC en eventos
- Herramienta de secuestro de RDP detectada
- Herramienta de reconocimiento detectada
- Recuperación deshabilitada en los datos de configuración de arranque
- Búsqueda de archivos de contraseña con findstr (Windows)
- Búsqueda de archivos de contraseña con grep o find (Unix)
- Búsqueda de archivos de contraseña con Select-String (Windows)
- Detección de SharpHound PowerShell
- Cantidad sospechosa de archivos eliminados en la misma máquina
- Cantidad sospechosa de archivos renombrados en la misma máquina (Windows)
- Cantidad sospechosa de archivos renombrados/movidos en la misma máquina (Unix)
- Módulo PSEXEC sospechoso Uso detectado
- Posible omisión de UAC
- Posible comportamiento de ransomware Mailto (Windows)
- Acceso directo (lnk) al ejecutar comandos (Windows)
- Posible vulnerabilidad de Windows a través de MSDT



CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA
NIT 901.781.625-1
CALLE 99 10 19
Tel: (601) 5527210
Bogotá - Colombia

PRE FACTURA
No. C-2-37

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2025-06-11

Autorización numeración de facturación electrónica DIAN No 18764085737391 vigencia desde 19-12-2024 hasta el 18-12-2025 desde el FE 33 al 5.000 vigencia 12 meses.

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
1	Integración de las fuentes de seguridad existentes en la Unidad de Ciberseguridad del FONDO NACIONAL DEL AHORRO S.A Contrato 173-2023	1.00	154,318,000.00	183,638,420.00	0.00
2	Entrega de cinco (5) modelos predefinidos adaptados a las fuentes de seguridad del FONDO NACIONAL DE AHORRO S.A., probados, documentados y disponibilizados. Contrato 173-2023	1.00	64,482,000.00	76,733,580.00	0.00

Total Bruto	218,800,000.00
Subtotal	218,800,000.00
IVA 19%	41,572,000.00
Total a Pagar	260,372,000.00

Elaborado por Siigo S.A.S Nit: 830.048.145-8

SUMAS IGUALES: Doscientos sesenta millones trescientos setenta y dos mil pesos mcte.

- Mnemo Colombia S.A.S. 49% NIT 900.396.176-1 Contribuyente
- Mnemo Cyber Sec SAS 50% NIT 901.447.968-1 Contribuyente
- Mnemo Evolution & integration Service SA 1% NIT:901.306.687-2 Contribuyente

DAVID TOVAR LOZANO
contadorjunior@mnemo.com
(3017710213)



BBVA Colombia
NIT 860.003.020-1
Certifica

Que nuestro(a) cliente **CONSORCIO UNIDAD DECIBERSEGURIDAD FNA**, identificado(a) con NIT número **901.781.625-1** se encuentra vinculado(a) a nuestra entidad a través de la CUENTA **CUENTA DE AHORROS EM** No. **0136002901** apertura el **19 de diciembre del 2023**, cuenta **ACTIVA** y que a la fecha ha presentado un manejo conforme a lo establecido contractualmente.

Esta certificación se expide a solicitud del titular con destino a quien interese, el **15 de mayo del 2025**.

Para trámites de nómina, legales, internacionales y otros, también puedes usar las siguientes opciones de números de cuenta:

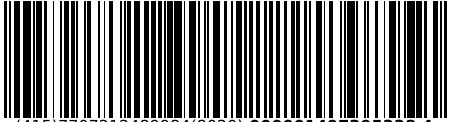
Cuenta de 10 dígitos:**0136002901**

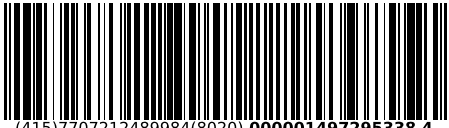
Cuenta de 16 dígitos:**0136000200002901**

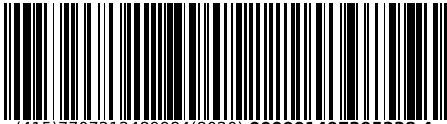
Cuenta de 20 dígitos:**00130136000200002901**

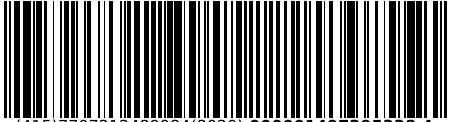
Firma autorizada
BBVA Colombia

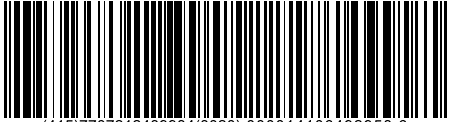
DIAN		Formulario del Registro Único Tributario		001	
2. Concepto 02 Actualización				4. Número de formulario 14972953384	
5. Número de Identificación Tributaria (NIT) 9017816251				6. DV 1	
12. Dirección seccional Impuestos de Bogotá				14. Buzón electrónico 32	
IDENTIFICACIÓN					
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación	
Lugar de expedición		28. País		29. Departamento	
31. Primer apellido		32. Segundo apellido		33. Primer nombre	
34. Otros nombres		35. Razón social CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA		37. Sigla	
UBICACIÓN					
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.	
41. Dirección principal CL 99 # 10 - 19 OF 502 ED TRADE CENTER					
42. Correo electrónico r.rojasarias@mnemo.com					
43. Código postal 011001		44. Teléfono 1 3183835117		45. Teléfono 2 3016327986	
CLASIFICACIÓN					
Actividad económica		Ocupación			
Actividad principal		Actividad secundaria		Otras actividades	
46. Código 6201		47. Fecha inicio actividad 20231214		48. Código	
49. Fecha inicio actividad		50. Código 1		2	
51. Código		52. Número establecimientos			
Responsabilidades, Calidades y Atributos					
53. Código 7144855					
07- Retención en la fuente a título de rent					
14- Informante de exogena					
48 - Impuesto sobre las ventas - IVA					
55 - Informante de Beneficiarios Finales					
Usuarios aduaneros					
Exportadores					
55. Forma 56. Tipo Servicio 1 2 3					
57. Modo					
58. CPC					
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					
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 VELEZ CASTRO HUMBERTO DE JESUS					
985. Cargo Representante legal Certificado					

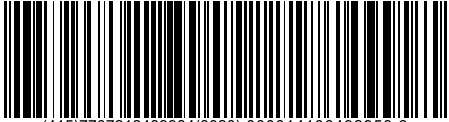
DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 5 Hoja 2		
			4. Número de formulario 14972953384		
 (415)7707212489984(8020) 000001497295338 4					
5. Número de Identificación Tributaria (NIT) 9 0 1 7 8 1 6 2 5 1		6. DV 1		12. Dirección seccional Impuestos de Bogotá	
				14. Buzón electrónico 3 2	
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas		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 3		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma					
Documento		1. Constitución		2. Reforma	
71. Clase 0 2					
72. Número					
73. Fecha 2 0 2 3 1 1 2 3					
74. Número de notaría					
75. Entidad de registro 9 8					
76. Fecha de registro 2 0 2 3 1 2 1 3					
77. No. Matrícula mercantil					
78. Departamento 1 1					
79. Ciudad/Municipio 0 0 1					
Composición del Capital					
Vigencia					
80. Desde 2 0 2 3 1 2 1 3				82. Nacional 1 0 0 %	
81. Hasta 2 0 2 5 1 2 3 1				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					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1				-	
2				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
97. Nombre o razón social de la matriz o controlante				96. DV.	
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					

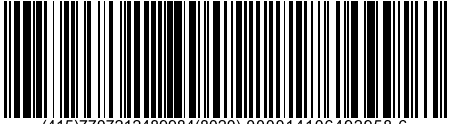
DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 5 Hoja 3			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5		1		Impuestos de Bogotá		3 2	
Representación							
98. Representación REPRS LEGAL PRIN				99. Fecha inicio ejercicio representación 2 0 2 3 1 1 2 3			
100. Tipo de documento Cédula de Ciudadaní		101. Número de identificación 1 3 8 7 7 0 4 4 6		102. DV		103. Número de tarjeta profesional	
104. Primer apellido VELEZ		105. Segundo apellido CASTRO		106. Primer nombre HUMBERTO		107. Otros nombres DE JESUS	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
98. Representación REPRS LEGAL SUPL				99. Fecha inicio ejercicio representación 2 0 2 3 1 1 2 3			
100. Tipo de documento Cédula de Ciudadan		101. Número de identificación 1 3 8 0 8 0 8 4 2 0		102. DV		103. Número de tarjeta profesional	
104. Primer apellido PARRA		105. Segundo apellido GAMBOA		106. Primer nombre JOHN		107. Otros nombres JAIRO	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
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			
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			
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			

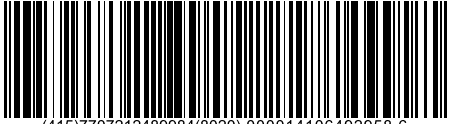
DIAN		Formulario del Registro Único Tributario Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales				001	
Espacio reservado para la DIAN				Página 4 de 5 Hoja 4			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5 1		1		Impuestos de Bogotá		3 2	
Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales							
1	111. Tipo de documento NIT		112. Número de identificación		113. DV 114. Nacionalidad		
	3 1		9 0 1 4 4 7 9 6 8		1 1 COLOMBIA 1 6 9		
	115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres
	119. Razón social MNEMO CYBER SEC S.A.S						
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	
				5 0 2 0 2 3 1 1 2 3			
2	111. Tipo de documento NIT		112. Número de identificación		113. DV 114. Nacionalidad		
	3 1		9 0 0 3 9 6 1 7 6		1 1 COLOMBIA 1 6 9		
	115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres
	119. Razón social MNEMO COLOMBIA SAS						
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	
				4 9 2 0 2 3 1 1 2 3			
3	111. Tipo de documento NIT		112. Número de identificación		113. DV 114. Nacionalidad		
	3 1		9 0 1 3 0 6 6 8 7		2 1 COLOMBIA 1 6 9		
	115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres
	119. Razón social MNEMO EVOLUTION & INTEGRATION SERVICES S.A.						
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	
				1 2 0 2 3 1 1 2 3			
4	111. Tipo de documento		112. Número de identificación		113. DV 114. Nacionalidad		
	115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres
	119. Razón social						
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	
5	111. Tipo de documento		112. Número de identificación		113. DV 114. Nacionalidad		
	115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres
	119. Razón social						
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001	
Espacio reservado para la DIAN				Página 5 de 5 Hoja 5			
				4. Número de formulario 14972953384			
 (415)7707212489984(8020) 000001497295338 4							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5		1		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		
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres
	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada		
	135. Fecha de nombramiento						
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 3 0 6 1 8 6 2 6		4		2 8 1 3 8 9 T
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres
	PINZON		ROJAS		ANDRES		CAMILO
156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada			
159. Fecha de nombramiento							
2 0 2 3 1 1 0 8							

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064929586			
				 (415)7707212489984(8020) 000014106492958 6			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 4 4 7 9 6 8		1		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							
MNEMO CYBER SEC S.A.S							
36. Nombre comercial							
37. Sigla							
UBICACIÓN							
38. País		39. Departamento		40. Ciudad/Municipio			
COLOMBIA		Bogotá D.C.		Bogotá, D.C.		0 0 1	
41. Dirección principal							
CL 99 NO 10 19 OF 502							
42. Correo electrónico j.parra@mnemo.com							
43. Código postal		44. Teléfono 1		45. Teléfono 2			
1 1 0 1 1 1		6 9 1 3 1 3 3					
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código		47. Fecha inicio actividad		48. Código		49. Fecha inicio actividad	
50. Código		1 2		51. Código			
6 2 0 1		2 0 2 0, 1 2, 2 9		6 2 0 2		2 0 2 0, 1 2, 2 9	
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 1 4 4 2 4 8 5 2 5 5							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
52 - Facturador electrónico							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
1 2 3 4 5 6 7 8 9 10				55. Forma 56. Tipo Servicio 1 2 3			
54. Código 11 12 13 14 15 16 17 18 19 20				57. Modo 58. CPC			
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			
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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre VELEZ CASTRO HUMBERTO DE JESUS			
				985. Cargo Representante Legal Suplente Certificado			

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 141064929586		
 (415)7707212489984(8020) 000014106492958 6					
5. Número de Identificación Tributaria (NIT) 9 0 1 4 4 7 9 6 8		6. DV 1	12. Dirección seccional Impuestos de Bogotá		14. Buzón electrónico 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			Composición del Capital		
Documento		1. Constitución		2. Reforma	
71. Clase 0 4					
72. Número					
73. Fecha 2 0 2 0 1 2 2 8					
74. Número de notaría					
75. Entidad de registro 0 3					
76. Fecha de registro 2 0 2 0 1 2 2 9					
77. No. Matrícula mercantil 0 3 3 2 0 4 4 3					
78. Departamento 1 1					
79. Ciudad/Municipio 4					
Vigencia					
80. Desde 2 0 2 0 1 2 2 8					
81. Hasta 2 0 9 9 1 2 3 1					
				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 0	2 0 2 1 0 1 2 5		-	
2				-	
3				-	
4				-	
5				-	
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					

DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 4 Hoja 3			
				4. Número de formulario 141064929586			
 (415)7707212489984(8020) 000014106492958 6							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 4 4 7 9 6 8		1		Impuestos de Bogotá		3 2	
Representación							
98. Representación REPRS LEGAL PRIN				99. Fecha inicio ejercicio representación 2 0 2 0 1 2 2 8			
100. Tipo de documento Cédula de Extranjeri		101. Número de identificación 2 2 6 6 7 3 5 2		102. DV		103. Número de tarjeta profesional	
104. Primer apellido VICENT		105. Segundo apellido FERNANDEZ		106. Primer nombre CARLOS		107. Otros nombres	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
98. Representación REPRS LEGAL SUPL				99. Fecha inicio ejercicio representación 2 0 2 2 0 1 1 2			
100. Tipo de documento Cédula de Ciudadan		101. Número de identificación 1 3 8 7 7 0 4 4 6		102. DV		103. Número de tarjeta profesional 6 1 0 6 1 - T	
104. Primer apellido VELEZ		105. Segundo apellido CASTRO		106. Primer nombre HUMBERTO		107. Otros nombres DE JESUS	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
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			
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			
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			

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001		
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5				
				4. Número de formulario 141064929586				
 (415)7707212489984(8020) 000014106492958 6								
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico		
9 0 1 4 4 7 9 6 8		1		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 1 8 4 0 8 8 7 6				2 3 2 3 2 5 T	
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres	
	TOVAR		LOZANO		JAIRO		DAVID	
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada			
	135. Fecha de nombramiento							
	2 0 2 3 0 3 3 0							
	136. Tipo de documento		137. Número de identificación		138. DV		139. Número de tarjeta profesional	
Revisor fiscal suplente	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 3 0 6 1 8 6 2 6				2 8 1 3 8 9 T	
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres	
	PINZON		ROJAS		ANDRES		CAMILO	
Contador	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada			
	159. Fecha de nombramiento							
	2 0 2 2 0 2 2 3							

DIAN

Formulario del Registro Único Tributario

001

2. Concepto02Actualización

4. Número de formulario141064925838

(415)7707212489984(8020)0000141064925838

5. Número de Identificación Tributaria (NIT)90039617616. DV112. Dirección seccionalImpuestos de Bogotá14. Buzón electrónico32

IDENTIFICACIÓN

24. Tipo de contribuyentePersona jurídica1

25. Tipo de documento

26. Número de Identificación

Lugar de expedición28. País

29. Departamento

30. Ciudad/Municipio

31. Primer apellido

32. Segundo apellido

33. Primer nombre

34. Otros nombres

35. Razón socialMNEMO COLOMBIA SAS

36. Nombre comercial

37. Sigla

UBICACIÓN

38. PaísCOLOMBIA169

39. DepartamentoBogotá D.C.11

40. Ciudad/MunicipioBogotá, D.C.001

41. Dirección principalCL 99 10 19 OF 502

42. Correo electrónicorecepcion.colombia@mnemo.com

43. Código postal11011144. Teléfono 1318383511745. Teléfono 2575527210

CLASIFICACIÓN

Actividad económica

Actividad principal

46. Código6201

47. Fecha inicio actividad20101112

Actividad secundaria

48. Código6202

49. Fecha inicio actividad20101112

Otras actividades

50. Código12

62098551

Ocupación

51. Código

52. Número establecimientos

Responsabilidades, Calidades y Atributos

53. Código57910141819264142485255

05- Impto. renta y compl. régimen ordinario26- Declaración individual precios de tran

07- Retención en la fuente a título de renta41- Declaración anual de activos en el exte

09- Retención en la fuente en el impuesto42- Obligado a llevar contabilidad

10- Obligado aduanero48- Impuesto sobre las ventas - IVA

14- Informante de exogena52- Facturador electrónico

18- Precios de transferencia55- Informante de Beneficiarios Finales

19- Productor de bienes y/o servicios exen

Usuarios aduaneros

54. Código23

Exportadores

55. Forma

56. Tipo

Servicio

1

2

3

57. Modo

58. CPC

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. AnexosSI[]NO[X]

60. No. de Folios:0

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:

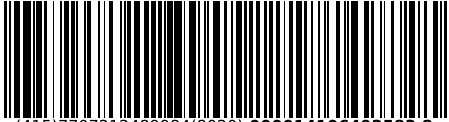
Sin perjuicio de las verificaciones que la DIAN realice.

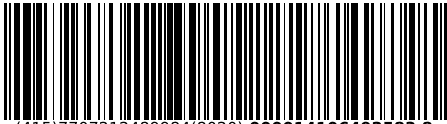
Firma autorizada:

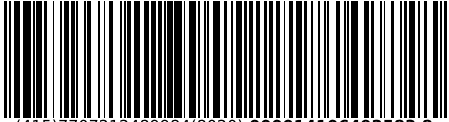
984. NombreVELEZ CASTRO HUMBERTO DE JESUS

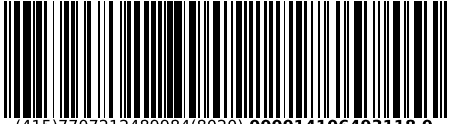
985. CargoRepresentante Legal Suplente Certificado

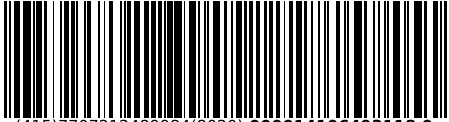
Fecha generación documento PDF: 05-02-2025 05:39:39PM

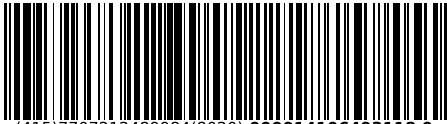
DIAN		Formulario del Registro Único Tributario				001	
Espacio reservado para la DIAN				Página 2 de 4 Hoja 2			
				4. Número de formulario 141064925838			
 (415)7707212489984(8020) 000014106492583 8							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 0 3 9 6 1 7 6		1		Impuestos de Bogotá		3 2	
Características y formas de las organizaciones							
62. Naturaleza		2		63. Formas asociativas		1 2	
65. Fondos				66. Cooperativas			
68. Sin personería jurídica				69. Otras organizaciones no clasificadas			
				64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados			
				67. Sociedades y organismos extranjeros			
				70. Beneficio		1	
Constitución, Registro y Última Reforma							
Documento		1. Constitución		2. Reforma		Composición del Capital	
71. Clase		0 4		0 4		82. Nacional	
72. Número						0 %	
73. Fecha		2 0 1 0 1 1 1 2		2 0 1 3 0 4 1 8		83. Nacional público	
74. Número de notaría						0 . 0 %	
75. Entidad de registro		0 3		0 3		84. Nacional privado	
76. Fecha de registro		2 0 1 0 1 1 1 9		2 0 1 3 0 7 0 9		0 . 0 %	
77. No. Matrícula mercantil		0 2 0 4 5 1 6 2		0 2 0 4 5 1 6 2		85. Extranjero	
78. Departamento		1 1		1 1		1 0 0 %	
79. Ciudad/Municipio		4		4		86. Extranjero público	
						0 . 0 %	
Vigencia						87. Extranjero privado	
80. Desde		2 0 1 0 1 1 1 2				1 0 0 . 0 %	
81. Hasta							
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 0		2 0 1 6 0 1 0 1		-	
2						-	
3						-	
4						-	
5						-	
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							

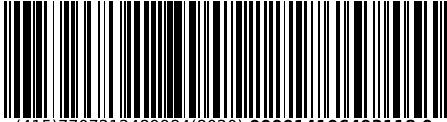
DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 4 Hoja 3			
				4. Número de formulario 141064925838			
				 (415)7707212489984(8020) 000014106492583 8			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 0 3 9 6 1 7 6		1		Impuestos de Bogotá		3 2	
Representación							
98. Representación REPRS LEGAL PRIN				99. Fecha inicio ejercicio representación 2 0 1 7 0 8 2 9			
100. Tipo de documento Cédula de Extranjeri		101. Número de identificación 2 2 6 6 7 3 5 2		102. DV		103. Número de tarjeta profesional	
104. Primer apellido VICENT		105. Segundo apellido FERNANDEZ		106. Primer nombre CARLOS		107. Otros nombres	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
98. Representación REPRS LEGAL SUPL				99. Fecha inicio ejercicio representación 2 0 2 2 0 1 1 7			
100. Tipo de documento Cédula de Ciudadan		101. Número de identificación 1 3 8 7 7 0 4 4 6		102. DV		103. Número de tarjeta profesional 6 1 0 6 1 - T	
104. Primer apellido VELEZ		105. Segundo apellido CASTRO		106. Primer nombre HUMBERTO		107. Otros nombres DE JESUS	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
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			
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			
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			

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001	
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5			
				4. Número de formulario 141064925838			
 (415)7707212489984(8020) 000014106492583 8							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 0 3 9 6 1 7 6		1		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 4 2 3 9 5 8 1		2 7 3 9 8 T		
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres
	SALAZAR		GOMEZ		JOSE		IGNACIO
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada		
	135. Fecha de nombramiento						
	2 0 2 3 0 3 3 1						
	136. Tipo de documento		137. Número de identificación		138. DV 139. Número de tarjeta profesional		
Contador	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						
	148. Tipo de documento		149. Número de identificación		150. DV 151. Número de tarjeta profesional		
Contador	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6		2 3 2 3 2 5 T		
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres
	TOVAR		LOZANO		JAIRO		DAVID
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada		
159. Fecha de nombramiento							
2 0 2 2 0 1 1 7							

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064931180			
				 (415)7707212489984(8020) 000014106493118 0			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		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 MNEMO EVOLUTION & INTEGRATION SERVICES S.A.							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País		39. Departamento		40. Ciudad/Municipio			
COLOMBIA		Bogotá D.C.		Bogotá, D.C.			
1 6 9		1 1		0 0 1			
41. Dirección principal CL 99 10 19 OF 502							
42. Correo electrónico Jc.aponte@mnemo.com							
43. Código postal		44. Teléfono 1		45. Teléfono 2			
1 1 0 1 1 1		6 9 1 3 1 3 3		3 1 0 3 2 4 3 4 7 5			
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código		47. Fecha inicio actividad		48. Código		49. Fecha inicio actividad	
6 2 0 1		2 0 1 9 0 7 0 2		6 2 0 2		2 0 1 9 0 7 0 2	
				50. Código		51. Código	
				1 2			
				6 2 0 9			
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 1 4 4 2 4 8 5 5							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
1 2 3 4 5 6 7 8 9 10				55. Forma 56. Tipo Servicio 1 2 3			
54. Código				57. Modo			
11 12 13 14 15 16 17 18 19 20				58. CPC			
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			
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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre PARRA GAMBOA JOHN JAIRO			
				985. Cargo Representante legal Certificado			

DIAN		Formulario del Registro Único Tributario				001	
Espacio reservado para la DIAN				Página 2 de 4 Hoja 2			
				4. Número de formulario 141064931180			
				 (415)7707212489984(8020) 000014106493118 0			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2	
Características y formas de las organizaciones							
62. Naturaleza		2		63. Formas asociativas		9 9	
65. Fondos				66. Cooperativas			
68. Sin personería jurídica				69. Otras organizaciones no clasificadas			
				64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados			
				67. Sociedades y organismos extranjeros			
				70. Beneficio		1	
Constitución, Registro y Última Reforma							
Documento		1. Constitución		2. Reforma		Composición del Capital	
71. Clase		0 5				82. Nacional 0 %	
72. Número						83. Nacional público 0 . 0 %	
73. Fecha		2 0 1 9 0 7 2 6				84. Nacional privado 0 . 0 %	
74. Número de notaría		6 5					
75. Entidad de registro		0 3					
76. Fecha de registro		2 0 1 9 0 7 2 6					
77. No. Matrícula mercantil		0 0 0 3 1 4 4 6 0 3				85. Extranjero 1 0 0 %	
78. Departamento		1 1				86. Extranjero público 0 . 0 %	
79. Ciudad/Municipio		0 0 1				87. Extranjero privado 1 0 0 . 0 %	
Vigencia							
80. Desde		2 0 1 9 0 7 2 6					
81. Hasta		9 9 9 9 1 2 3 1					
Entidad de vigilancia y control							
88. Entidad de vigilancia y control							
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 9 0 7 2 6		-			
2	8 1	2 0 1 9 0 7 2 6		-			
3				-			
4				-			
5				-			
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							

DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 4 Hoja 3			
				4. Número de formulario 141064931180			
				 (415)7707212489984(8020) 000014106493118 0			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2	
Representación							
98. Representación REPRS LEGAL PRIN 1 8				99. Fecha inicio ejercicio representación 2 0 2 2 0 4 0 8			
100. Tipo de documento Cédula de Ciudadaní 1 3		101. Número de identificación 8 0 8 0 8 4 2 0		102. DV		103. Número de tarjeta profesional	
104. Primer apellido PARRA		105. Segundo apellido GAMBOA		106. Primer nombre JOHN		107. Otros nombres JAIRO	
108. Número de Identificación Tributaria (NIT)		109. DV		110. Razón social representante legal			
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			
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			
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			
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			
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			

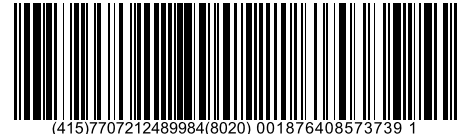
DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001	
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5			
				4. Número de formulario 141064931180			
 (415)7707212489984(8020) 000014106493118 0							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2	
Revisor Fiscal y Contador							
Revisor fiscal principal	124. Tipo de documento Cédula de Ciudadanía		125. Número de identificación 1 3 8 7 7 0 4 4 6		126. DV 127. Número de tarjeta profesional 6 1 0 6 1		
	128. Primer apellido VELEZ		129. Segundo apellido CASTRO		130. Primer nombre HUMBERTO		131. Otros nombres DE JESUS
	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada		
	135. Fecha de nombramiento 2 0 2 1 0 2 1 5						
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 Cédula de Ciudadanía		149. Número de identificación 1 3 1 0 1 8 4 0 8 8 7 6		150. DV 151. Número de tarjeta profesional 2 3 2 3 2 5		
	152. Primer apellido TOVAR		153. Segundo apellido LOZANO		154. Primer nombre JAIRO		155. Otros nombres DAVID
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada		
	159. Fecha de nombramiento 2 0 2 1 0 6 0 1						

Espacio reservado para la DIAN



4. Número de formulario

18764085737391



(415)7707212489984(8020) 001876408573739 1

5. Número de Identificación Tributaria - NIT

6. DV

7. Primer apellido

8. Segundo apellido

9. Primer nombre

10. Otros nombres

9 0 1 7 8 1 6 2 5

1

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

12. Dirección seccional

Impuestos de Bogotá

Cód.

3 2

24. Dirección

CL 99 # 10 - 19 OF 502 ED TRADE CENTER

25. País

Colombia

26. Departamento

Bogotá D.C.

27. Municipio

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 trámite 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 funcionario autorizado

Firma del solicitante



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 VELEZ CASTRO HUMBERTO DE JESUS

1002. Tipo documento Cédula de Ciudadanía

1003. No. Identificación 8 7 7 0 4 4 6

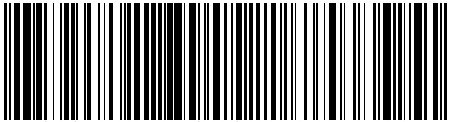
1004. DV 3

1005. Cod. Representación Representante Legal Principal

1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

997. Fecha formalización

2 0 2 4 - 1 2 - 1 9 / 1 5 : 4 8 : 1 0

DIAN		Autorización Numeración de Facturación						1876		
Espacio reservado para la DIAN 						Página 2 de 2 Hoja No. 2				
						4. Número de formulario 18764085737391  (415)7707212489984(8020) 001876408573739 1				
5. Número de Identificación Tributaria - NIT		6. DV	7. Primer apellido		8. Segundo apellido		9. Primer nombre		10. Otros nombres	
9 0 1 7 8 1 6 2 5		1								
11. Razón social CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA										
Rangos de numeración para autorizar, habilitar o inhabilitar										
1	29. Establecimiento CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA CL 99 # 10 - 19 OF 502 ED TRADE CENTER									
	30. Modalidad FACTURA ELECTRÓNICA DE VENTA	Cód. 4	31. Prefijo FE	32. Desde el número 33	33. Hasta el número 5,000	38. Vigencia 12	34. Tipo solicitud HABILITACIÓN	Cód. 2		
2	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
3	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
4	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
5	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
6	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
7	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
8	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
9	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
10	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		
11	29. Establecimiento									
	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.		



Bogotá, 13 de Junio de 2025

Señores

FONDO NACIONAL DEL AHORRO SA

Ciudad.

REF: CIRCULAR 042 DE 2012

Respetados señores:

Con la presente certificamos que para la empresa **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA SA**, identificada con **NIT.901.781.625-1**, no aplica la circular en referencia, debido a que no nos encontramos vigilados por la Superintendencia de Sociedades.

Agradecemos la atención a la presente,

Cordialmente,

HUMBERTO DE JESUS VELEZ CASTRO
Representante legal
MNENO COLOMBIA SAS

Gerencia Tesorería

Documento de Pago

No. ORDEN DE PAGO	43	FECHA DE CONTABILIZACION	07-jul-25
No. DOCUMENTO DE PAGO	5300437522	FECHA DE DOCUMENTO	07-jul-25
		FECHA DE COMPENSACION	07-jul-25
PROPUESTA	52058	FECHA DE LA PROPUESTA	07-jul-25

RESPONSABLE DEL PAGO			
NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO		
No. IDENTIFICACIÓN	8999992844	TIPO DE IDENTIFICACIÓN	NIT
CONCEPTO	GIRO DE CESANTIAS DEFINITIVAS SE		

DATOS GENERALES			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSE		
No. IDENTIFICACION	9017816251	TIPO DE IDENTIFICACION	NIT
FORMA DE ENTREGA	PAGO ELECTRÓNICO		
CIUDAD DE ENTREGA	BOGOTÁ		
NUMERO DE CUENTA	0136002901	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BANCO BBVA		
GRAV MOVIMIENTOS FINANCIEROS	0		

BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSEGURIDAD		
No. IDENTIFICACIÓN	9017816251	TIPO DE IDENTIFICACIÓN	25
NOMBRE:	CONSORCIO UNIDAD DE		
OBSERVACIONES:	FE43 RAD 02-2303-202506260793743		
NÚMERO DE CUENTA	2511050101	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	244.364.592		

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
1003700788	5300437522	43	244.364.592	FE43 RAD 02-2303-202506260793743	6200000115	CTO 173 DE 2023

División de Presupuesto

Documento de Pago

N° ORDEN DE PAGO	5300437522	FECHA DE CONTABILIZACIÓN	24.06.2025
N° DE REFERENCIA	43	FECHA DE PAGO	07.07.2025

RESPONSABLE DEL PAGO			
NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO		
N° IDENTIFICACIÓN	NIT	8999992844	

PROVEEDOR	CONSORCIO UNIDAD DE CIBERSEGURIDAD	N° IDENTIFICACION	9017816251
BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE		
N° IDENTIFICACION	9017816251	TIPO DE IDENTIFICACION	NIT
FORMA DE PAGO	PAGO ELECTRÓNICO	CIUDAD	BOGOTÁ
N° DE CUENTA	0136002901	BANCO	BANCO BBVA
TIPO DE CUENTA	CUENTA DE AHORROS	INFORME N°	
N° FACTURA PROVEEDOR	FE43 RAD 02-2303-202506260793743		

OBSERVACIONES:

INFORMACIÓN PRESUPUESTAL						
SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
	6200000115	00030	CTO 173 DE 2023		5105630934	76.733.580
					AFECCIÓN PEDIDO	76.733.580
DETALLE DE LA ORDEN DE PAGO						
VALOR TOTAL FAC.		76.733.580,00				
DESCUENTOS		-167.631.012,00				
NOTAS CRÉDITOS		0,00				
VALOR A PAGAR		244.364.592,00				