fna FONDO NACIONAL DEL AHORRO	**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 ESTRATEGIA TI Y 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			NONBRE DE LA SERIE, SUBSERIE O ASUNTOS	NOMBRE DE LA UNIDAD DOCUMENTAL	FECHAS EXTREMAS (dd-mm-aaaa)		SOPORTE O FORMATO		FÍSICO						ELECTRÓNICO			FRECUENCIA DE CONSULTA	OBSERVACIONES
										UNIDAD DE CONSERVACIÓN						Ubicación	Cantidad de documentos	Tamaño de los documentos		
										PAPEL				OTRO						
	CÓDIGO OFICINA	SERIE	SUBSERIE			Inicial	Final	Físico	Electrónico	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 No. 15 factura No. FE15 orden de pago No. 5300437368	20-jun-24	8-jul-24		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	234	15,5 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:	**13-03-2025**	**Fecha:**	**13/03/2025**	**Fecha:**	

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

INFORME No 15 FACTURA No

No. DE ACEPTACIÓN: 1000050288

FECHA		
20	06	24
dd	mm	aaaa

1. GENERALIDADES DEL CONTRATO

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

ORDENADOR DEL GASTO SANDRA MILENA BURGOS BELTRAN (Nombre del ordenador del Gasto) SECRETARIA GENERAL (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 [X] COLEGIADA [ ]

INTERVENTOR Y/O SUPERVISOR Monica Grand Villada (Escriba nombre del supervisor o interventor del contrato) (Escriba nombre del supervisor o interventor del contrato)

APOYO SUPERVISIÓN Andrea Hernandez - Enrique Arrazola (Nombre de la persona delegada para apoyar la supervisión del contrato) Luz Helena Riaño (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 (Día) DE dic (Mes) DE 2023 (Año)

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

REGISTRO PRESUPUESTAL No. 5400001604 - 6200000102

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.

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

PRÓRROGAS	
No.	PLAZO

ADICIONES		
No.	VALOR	RP

SUSPENSIONES		
No	DESDE	HASTA

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	$ 36.499.583.610,00	100,00%
Adiciones	$ -	0,00%
VALOR TOTAL DEL CONTRATO	$ 36.499.583.610,00	100,00%
Valor ejecutado antes del presente pago	$ 20.885.229.464,00	57,22%
Valor del pago aprobado con el presente informe	$ 885.237.430,00	2,43%
VALOR TOTAL EJECUTADO	$ 21.770.466.894,00	59,65%
Porcentaje de ejecución presupuestal programado a la fecha		59,71%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,06%

OBSERVACIONES

Cuenta 15: Instalación, configuración, pruebas, puesta enmarcha y estabilización de plataforma SOAR,Suscripción de licenciamiento.

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 unicamente para Desarrollos o mantenimientos de Aplicaciones Tecnológicas*

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

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

OBSERVACIONES

El contratista cumplió a satisfacción con la instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento.

(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 OCHOCIENTOS OCHENTA Y DOS MILLONES QUINIENTOS QUINCE MIL SETECIENTOS CUARENTA PESOS MCTE ($885,237,430).

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 periodo, 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	X	PDF	**Certificaciones, planilla pago parafiscales, CC y T.P.**
Informes	X	PDF	**Informe de Supervisión** **Informe Gestión Proveedor**
Actas	X	PDF	**Acta Seguimiento Mensual ANS**
OTROS	X	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 (día en letras) **20** (día en números) días del mes de **Junio** (mes en letras) de **2024** (Año)

Monica Grand Villada
Gerente Estrategia TI y aseguramiento informatico
Supervisor CTO173-2023

Revisó y aprobó: Andrea Hernandez - Enrique Arrazola - Luz Helena Riaño - Apoyo a la supervisión

Estadística de datos	Cantidad
Registros transferidos	6

Cl.doc. : RE (Factura bruto) Documento normal

Reg.prelim.por	NTUIRAN	Contab.por	MRINCONZ		
Nº doc.	5100001340	Sociedad	1000	Ejercicio	2024
Fe.docum.	21.06.2024	Fecha contab.	21.06.2024	Período	06
Calc.impuestos	☑				
Referen.	15				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202406253746427				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	830,813,925-
2	86	2511950101	CXP PROVED EM/RF		W0	885,237,430
3	91	5130950401	CENTRO OPER SEG		W0	0
4	50	2519051101	SERVICIO 3.5%			26,036,395-
5	50	2519053801	RTE IVA TARIFA GENER			21,201,065-
6	50	2519054408	SERVICIOS 304 BOGOTA			7,186,045-

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 15

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	21/06/2024, 15:33
Expedición	21/06/2024, 15:33
Vencimiento	21/07/2024

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, Suscripción de licenciamiento. Contrato 173-2023 N° de aceptación 1000050288	1.00	0.00	885,237,430.00

Total items: 1

Valor en Letras:
Ochocientos ochenta y cinco millones doscientos treinta y siete mil cuatrocientos treinta pesos m/cte

Total Bruto	743,897,000.00
IVA 19%	141,340,430.00
Total a Pagar	**885,237,430.00**

Condiciones de Pago:
Crédito - Cuota No. 001 vence el 2024-07-21 por $ 885,237,430.00

Observaciones:
Notas:

1.Instalación realizada en los servidores ya desbloqueados con la salida a producción de la plataforma SIEM

2.PowerEdge Server No. Serial: 4TD4H04, PowerEdge Server No. Serial: 5TD4H04, PowerVault SAN No. Serial: 49L3H04

3.Ver el valor del licenciamiento en la Nota Discriminación _ valores_ licencias V2.docx

Distribución de ingresos:

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

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 18764062145032 aprobado en 20231217 prefijo FE desde el número 1 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

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

CUFE: 091949afe5afb9dbbadd450876040b2ef21973d32996a3361177db1bf1d0d6bbbde443613c4cb6cafe4c2848ddb29b69

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 CIBERSEGUIRIDAD 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 veinticuatro (2024).

Atentamente,

HUMBERTO DE JESUS VELEZ CASTRO
Representante Legal **CONSORCIO SOC-NOC-MINTIC**
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

MNEMO

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 CONPERSONAL 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 2024.

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

CEDULA DE CIUDADANIA

REPÚBLICA DE COLOMBIA

NUIP 8.770.446

Apellidos
VELEZ CASTRO

Nombres
HUMBERTO DE JESUS

Nacionalidad
COL

Estatura
1.70

Sexo
M

Fecha de nacimiento
26 JUL 1970

G.S.
B+

Lugar de nacimiento
BARRANQUILLA (ATLANTICO)

Fecha y lugar de expedición
15 SEPT 1988, SOLEDAD

Fecha de expiración
29 DIC 2030

CO

000016355

REGISTRADOR NACIONAL
Alexander Vega Rocha

ICCOL0000163550030 52<<<<<<<<<<<
7007282M3012291COL8770446<<<<8
VELEZ<CASTRO<<HUMBERTO<DE<JESU

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

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

MNEMO CYBER SEC S.A.S
NIT 901.447.968-1

En mi calidad de revisor fiscal de la compañía **MNEMO CYBER SEC S.A.S.,** identificada con NIT**: 901.447.968-1**, he efectuado los procedimientos de revisión que se detallan a continuación con el propósito de verificar el pago efectuado por la compañía por concepto de **aportes a los sistemas de salud, pensión y riesgos laborales y a las cajas de compensación familiar, instituto colombiano de bienestar familiar (ICBF) y servicio nacional de aprendizaje (SENA)**, por el periodo de **(6)** seis meses comprendidos entre el **1 de noviembre de 2023 y 30 de abril del 2024**. El pago de dichos aportes es responsabilidad de la administración de la compañía como parte de mi gestión.

Los procedimientos de revisión realizados fueron los siguientes:

1. La contratación del personal se realizó el pasado 01 de junio de 2021, antes de esta fecha **MNEMO CYBER SEC S.A.S,** no contaba con personal directo.

2. Indagación con el personal del área responsable, en relación con los procedimientos utilizados para la identificación y pago de los aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

3. Obtención del listado de liquidación de aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA),preparado por la compañía por el periodo de **(6) meses** comprendidos entre el **1 de noviembre de 2023 y 30 de abril del 2024.**

4. El ultimo pago de aportes corresponde a **pensión abril** del año **2024 y salud mayo** del año **2024.**

5. Comparación del listado obtenido según se menciona en el numeral anterior, con los documentos soporte de los respectivos pagos efectuados por la compañía.

Con base en el resultado de los procedimientos enumerados anteriormente, por el **periodo de (6) seis meses** comprendidos entre el **1 de noviembre de 2023 y 30 de abril del 2024**, informo que, a la fecha del presente informe, la compañía se encuentra al día en el pago de los aportes a los Sistemas de Salud, Pensiones y Riesgos Laborales y a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Esta certificación se emite a los once (11) días, del mes de junio del año 2024.

JAIRO DAVID TOVAR LOZANO
C.C. 1.018.408.876
Revisor fiscal de MNEMO CYBER SEC S.A.S.

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**, comprendido entre el 1 de enero de 2024 al 4 de junio de 2024, 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 (4) cuatro días del mes de junio de 2024.

At.

JOSE IGNACIO SALAZAR GOMEZ
Revisor Fiscal T.P. 27.398-T
C.C. 14.239.581 de Ibagué – Cel. 3158889246 joseignaciosago@hotmail.com

Planilla Resumen

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
2024-04	2024-05	646116135	9467214407	E	2024/05/17	2024/05/17	BANCO DAVIVIENDA	0	$28,444,700

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	Días	Codigo	Días	Codigo	Días	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (19 Afiliados)																														
Centro de Trabajo: CENTRO TRABAJO 1 (17 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (17 Afiliados)																														
1	CC	1233493654	BARGAS GARCIA JULIAN ANDRES									X								230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
2	CC	1015417833	BEJARANO DIAZ ANDRES ENRIQUE																	231001	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
3	CC	1070981128	COLLAZOS FONSECA MATEO																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
4	CC	1016043734	GARCIA BUITRAGO JEISSON ALEJANDRO									X								230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
5	CC	91180662	GARRIDO PRADA YEINSON ALBERTO																	230301	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
6	CC	13871620	MARTINEZ CARREÑO HECTOR MANUEL																	230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
7	CC	1026280102	MAYORGA GALINDO ANNYI CATHERINE																	231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
8	CC	1018453849	MERCHAN SANCHEZ LUISA FERNANDA									X								230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
9	CC	1233901826	MOYAN SANTANA CRISTIAN CAMILO									X								230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
10	CC	1053328985	PAEZ CORTES LADY ZOLANYI									X								230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
11	CC	80093909	PICO CARREÑO MAURO JAVIER	X																25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
12	CC	1072431635	RAMIREZ CASTAÑEDA RAMIRO ANDRES									X								230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
13	CC	80091134	SOTELO VIRGUES PABLO EMILIO									X								230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
14	CC	1073515030	TAYLOR CASALLAS BRANDON DAVID																	231001	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
15	CC	79729048	URIBE RUIZ WILSON																	25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
16	CC	1031143384	URREGO BOLIVAR SANDRO JAVIER									X								230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
17	CC	1070307880	ZAMBRANO OSORIO OSCAR ANDRES									X								230201	30	EPS041	30	CCF24	30	14-25	30	0.522%	30	Si
Centro de Trabajo: CENTRO TRABAJO 2 (2 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (2 Afiliados)																														
18	CC	3104161	GARZON ROBAYO GUSTAVO																	230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
19	CC	1070917650	HERNANDEZ PEREZ YENNY FERNANDA																	230201	30	EPS010	30	CCF24	30	14-25	30	1.044%	30	No
Total		**Afiliados(19)**																												

Planilla Resumen

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
2024-04	2024-05	646116135	9467214407	E	2024/05/17	2024/05/17	BANCO DAVIVIENDA	0	$28,444,700

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				19	$16,568,800	$0	$0	$16,568,800
COLFONDOS	231001	800,227,940	6	3	$2,220,000	$0	$0	$2,220,000
COLPENSIONES	25-14	900,336,004	7	3	$3,435,000	$0	$0	$3,435,000
PORVENIR	230301	800,224,808	8	5	$2,729,100	$0	$0	$2,729,100
PROTECCION	230201	800,229,739	0	6	$4,983,500	$0	$0	$4,983,500
SKANDIA	230901	800,253,055	2	2	$3,201,200	$0	$0	$3,201,200
ARL (ADMINISTRADORAS: 1)				19	$648,500	$0	$0	$648,500
COLMENA	14-25	800,226,175	3	19	$648,500	$0	$0	$648,500
CCF (ADMINISTRADORAS: 1)				19	$4,011,900	$0	$0	$4,011,900
COMPENSAR	CCF24	860,066,942	7	19	$4,011,900	$0	$0	$4,011,900
EPS (ADMINISTRADORAS: 7)				19	$6,029,000	$0	$0	$6,029,000
COMPENSAR	EPS008	860,066,942	7	2	$291,200	$0	$0	$291,200
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	2	$1,627,500	$0	$0	$1,627,500
FAMISANAR	EPS017	830,003,564	7	2	$520,000	$0	$0	$520,000
FOSYGA	MIN001	901,037,916	1	2	$480,000	$0	$0	$480,000
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	$130,400	$0	$0	$130,400
SALUD TOTAL	EPS002	800,130,907	4	3	$391,100	$0	$0	$391,100
SANITAS	EPS005	800,251,440	6	7	$2,588,800	$0	$0	$2,588,800
ICBF (ADMINISTRADORAS: 1)				2	$711,900	$0	$0	$711,900
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	2	$711,900	$0	$0	$711,900
SENA (ADMINISTRADORAS: 1)				2	$474,600	$0	$0	$474,600
SENA	PASENA	899,999,034	1	2	$474,600	$0	$0	$474,600
TOTAL				**19**	**$28,444,700**	**$0**	**$0**	**$28,444,700**

Planilla Resumen

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
2024-04	2024-05	653601901	9467410360	E	2024/05/21	2024/05/21	BANCO BBVA COLOMBIA S.A.	0	$147,048,300

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	Días	Codigo	Dias	Codigo	Días	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (98 Afiliados)																															
Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (21 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (21 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		X					25-14	12	EPS001	12	CCF24	5	14-25	12	0.000%	5	No
4	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																		25-14	18	EPS001	18	CCF24	18	14-25	18	1.044%	18	No
5	CC	1122651302	CARO ROA JONATHAN													X					230301	5	EPS005	5	CCF24	5	14-25	5	0.000%	5	Si
6	CC	1122651302	CARO ROA JONATHAN																		230301	25	EPS005	25	CCF24	25	14-25	25	1.044%	25	Si
7	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																		230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
8	CC	1013592039	EMBUS IPIA JULIAN ANDRES											X							230201	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	No
9	CC	1013592039	EMBUS IPIA JULIAN ANDRES																		230201	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	No
10	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
11	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO																		231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	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	52824814	RODRIGUEZ MURCIA NIDIA ESPERANZA																		230301	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
16	CC	80791790	ROJAS ARIAS RICARDO																		230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
17	CC	80066361	ROMERO ARCHILA DANIEL DARIO																		230201	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
18	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI													X					231001	8	EPS005	8	CCF24	8	14-25	8	0.000%	8	Si
19	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																		231001	22	EPS005	22	CCF24	22	14-25	22	1.044%	22	Si
20	CC	24659147	VALDES RAMIREZ ALBA LIBIA																			0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
21	CC	79950164	VARGAS HINCAPIE FERNANDO									X									230301	30	EPS002	30	CCF24	30	14-25	30	1.044%	30	Si
22	CC	1032410736	VARGAS HINCAPIE HENRY																		230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
23	CC	1000349377	VARGAS ALVAREZ MARIA ANTONIA		X															X	230301	1	EPS037	1	CCF24	1	14-25	1	1.044%	1	Si
24	CC	1022411758	VARGAS LEON MARIA CAMILA																		230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
25	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																			0	EPS017	30		0		0	0.000%	0	No

Planilla Resumen

Centro de Trabajo: ADMINISTRACION (73 Afiliados)

Ciudad: BOGOTA Depto: BOGOTA D.E. (73 Afiliados)

26	CC	1014306151	ABRIL MONTES SERGIO LEONARDO									X								230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
27	CC	1019151775	ACOSTA MURILLO JUAN CAMILO									X								25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
28	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO																	25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
29	CC	1031162097	ARISTIZABAL ANGEL LAURA VANESSA									X								230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
30	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER																	231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	1019077197	BELEÑO BUELVAS CHARLES JAVIER									X								230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
32	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER																	230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
33	CC	1012437249	BOCANEGRA MORALES LUIS FELIPE									X								230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
34	CC	1004268659	BONILLA ZUÑIGA ANDERSON																	231001	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
35	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN																	230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
36	CC	1024467791	CARDENAS VARON KEVIN ANDRES		X																0	EPS010	19		0	14-25	19	0.522%	0	No
37	CC	13870244	CARRILLO ALVAREZ OSCAR																	25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
38	CC	1012322665	CASTAÑEDA MESA ANDREA KATHERINE												X					231001	12	EPS008	12	CCF24	12	14-25	12	0.000%	12	Si
39	CC	1012322665	CASTAÑEDA MESA ANDREA KATHERINE																	231001	18	EPS008	18	CCF24	18	14-25	18	0.522%	18	Si
40	CC	1034397473	CASTILLO IDROBO JHON FABER																		0	EPS002	30		0	14-25	30	0.522%	0	No
41	CC	1020809969	CASTILLO MENDOZA JOHN ALEXANDER									X								230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
42	CC	1070590173	CASTRO CALDERON JUAN GUILLERMO																		0	EPS005	30		0	14-25	30	0.522%	0	No
43	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID									X								230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
44	CC	1022418490	DIAZ MONCALEANO JOSE MANUEL									X								230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
45	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER																	25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
46	CC	1023957895	GIL MURILLO JAVIER EDUARDO									X								230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
47	CC	1019009180	GOMEZ ROJAS YENNY PAOLA												X					230301	2	EPS037	2	CCF24	2	14-25	2	0.000%	2	Si
48	CC	1019009180	GOMEZ ROJAS YENNY PAOLA																	230301	28	EPS037	28	CCF24	28	14-25	28	0.522%	28	Si
49	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO												X					230201	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
50	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO																	230201	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
51	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN																		0	EPS005	30		0	14-25	30	0.522%	0	No
52	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL												X					230301	3	EPS017	3	CCF24	3	14-25	3	0.000%	3	Si
53	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL									X								230301	27	EPS017	27	CCF24	27	14-25	27	0.522%	27	Si
54	CC	1000689679	GUARIN PINZON MATEO									X								230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
55	CC	1076663845	GUAYAZAN CORTES JONATHAN STIVEN									X								230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
56	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES																	230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
57	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																	230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si

58	CC	1099374748	LEAL GOMEZ DANIELA												X					230201	5	EPS037	5	CCF24	5	14-25	5	0.000%	5	Si
59	CC	1099374748	LEAL GOMEZ DANIELA																	230201	25	EPS037	25	CCF24	25	14-25	25	0.522%	25	Si
60	CC	52953219	LEON CERON MARIA ALEXANDRA												X					231001	4	EPS005	4	CCF24	4	14-25	4	0.000%	4	Si
61	CC	52953219	LEON CERON MARIA ALEXANDRA																	231001	26	EPS005	26	CCF24	26	14-25	26	0.522%	26	Si
62	CC	1069769484	LOPEZ ZAMORA JUAN DAVID																	230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	1193088387	LUENGAS CORTES DAVID STIWEN	X																230301	26	EPS037	26	CCF24	26	14-25	26	0.522%	26	Si
64	CC	79992827	MARROQUIN GUTIERREZ DIDIER																	230201	30	MIN002	30	CCF24	30	14-25	30	0.522%	30	Si
65	CC	1000032122	MARTIN GARCES JUAN DAVID								X									230301	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
66	CC	1023885573	MARTINEZ CASAS EDWARD ALEJANDRO	X																25-14	12	EPS008	12	CCF24	12	14-25	12	0.522%	12	Si
67	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																	230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
68	CC	1000719172	MARTINEZ BECERRA MARIA JOSE								X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
69	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
70	CC	1000717997	MELO MOSQUERA DANIEL RENE								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
71	CC	98632570	MESA MENDEZ CARLOS MANUEL																	230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
72	CC	1022947945	MOLANO JIMENEZ JESUS RICARDO								X									230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
73	CC	1110173553	MORA TABARES MIGUEL ANGEL								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
74	CC	1033711407	MURCIA TORRES JHON FREDY										X							230301	1	EPS005	1	CCF24	0	14-25	1	0.000%	0	Si
75	CC	1033711407	MURCIA TORRES JHON FREDY																	230301	29	EPS005	29	CCF24	29	14-25	29	0.522%	29	Si
76	CC	1023907046	OCHOA ROJAS ROGER JULIAN								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
77	CC	1032479763	ORJUELA CALDERON PAULA NATALIA												X					231001	12	EPS005	12	CCF24	12	14-25	12	0.000%	12	Si
78	CC	1032479763	ORJUELA CALDERON PAULA NATALIA								X									231001	18	EPS005	18	CCF24	18	14-25	18	0.522%	18	Si
79	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
80	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN																	230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
81	CC	1023886752	PATARROYO JIMENEZ JHON JAIRO								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
82	CC	1019127504	PERDOMO GUZMAN JESSICA LILIANA								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
83	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO																	230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
84	CC	1030618626	PINZON ROJAS ANDRES CAMILO																	230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
85	CC	1023972445	PRIETO SILVA NICOL												X					230301	9	EPS002	9	CCF24	9	14-25	9	0.000%	9	Si
86	CC	1023972445	PRIETO SILVA NICOL																	230301	21	EPS002	21	CCF24	21	14-25	21	0.522%	21	Si
87	CC	1014201989	QUIROGA PERALTA EDWIN FERNANDO																	230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
88	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN								X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
89	CC	1032486411	RINCON HILARION EDWARD MAURICIO		X														X	231001	17	EPS010	17	CCF24	17	14-25	17	0.522%	17	Si
90	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES																	25-14	14	EPS010	14	CCF24	14	14-25	14	0.522%	14	Si
91	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES										X							25-14	16	EPS010	16	CCF24	0	14-25	16	0.000%	0	Si
92	CC	1003712217	RODRIGUEZ PENAGOS JOAN SEBASTIAN																	230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si

93	CC	52505417	ROJAS PEÑA NILSA YAMILE																			25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
94	CC	1030697447	ROJAS PEREZ VALENTINA									X										230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
95	CC	1010180437	SANCHEZ ROMERO CARLOS ANDRES		X							X									X	230201	19	EPS005	19	CCF24	19	14-25	19	0.522%	19	Si
96	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO													X						230201	1	EPS008	1	CCF24	1	14-25	1	0.000%	1	Si
97	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO																			230201	29	EPS008	29	CCF24	29	14-25	29	0.522%	29	Si
98	CC	1030539604	TAMAYO RIVERA FABIO ANDRES											X								231001	15	EPS005	15	CCF24	0	14-25	15	0.000%	0	Si
99	CC	1030539604	TAMAYO RIVERA FABIO ANDRES																			231001	15	EPS005	15	CCF24	15	14-25	15	0.522%	15	Si
100	CC	1020808701	TIBADUIZA CALDERON SEBASTIAN																			231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
101	CC	1032394709	TOLEDO SALAMANCA WALTER OSWALDO																			230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
102	CC	1018408876	TOVAR LOZANO JAIRO DAVID																			230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
103	CC	1031172873	TRUJILLO ALVAREZ VALENTINA																			231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
104	CC	1014279176	URBANO ARDILA SEBASTIAN									X										25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
105	CC	1019136138	VANEGAS CAMARGO DIEGO ALEJANDRO											X								230301	6	EPS005	6	CCF24	0	14-25	6	0.000%	0	Si
106	CC	1019136138	VANEGAS CAMARGO DIEGO ALEJANDRO									X										230301	24	EPS005	24	CCF24	24	14-25	24	0.522%	24	Si
107	CC	80247522	VARGAS HINCAPIE CARLOS																			25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
108	CC	1075280531	VARGAS POLANIA JAIRO ALEXANDER																			230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
109	CC	1014197302	VELASQUEZ RAMOS JOHAN SEBASTIAN																			25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
110	CC	8770446	VELEZ CASTRO HUMBERTO DE JESUS																			230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	No
111	CE	667352	VICENT FERNANDEZ CARLOS																				0	EPS005	30	CCF24	30	14-25	30	0.522%	30	No
Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																																
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																																
112	CC	1019024746	MUÑOZ OROZCO BERTHA JUDITH																			25-14	30	EPS017	30	CCF24	30	14-25	30	1.044%	30	Si
Centro de Trabajo: MENSAJERIA (3 Afiliados)																																
Ciudad: BOGOTA Depto: BOGOTA D.E. (3 Afiliados)																																
113	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS													X						230201	1	EPS008	1	CCF24	1	14-25	1	0.000%	1	Si
114	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS																			230201	29	EPS008	29	CCF24	29	14-25	29	4.350%	29	Si
115	CC	79840394	RODRIGUEZ ANGARITA ELKIN													X						230301	5	EPS008	5	CCF24	5	14-25	5	0.000%	5	Si
116	CC	79840394	RODRIGUEZ ANGARITA ELKIN																		X	230301	25	EPS008	25	CCF24	25	14-25	25	4.350%	25	Si
117	CC	91462884	SERRANO BONILLA JILMER																			230301	30	MIN001	30	CCF24	30	14-25	30	4.350%	30	Si

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: FAMISANAR (1 Afiliados)																														
Centro de Trabajo: FAMISANAR - ADMINISTRATIVO (1 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																														
118	CC	80155666	CHAVES MARTINEZ JORGE ANDRES									X								230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
Total		**Afiliados(99)**																												

Planilla Resumen

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
2024-04	2024-05	653601901	9467410360	E	2024/05/21	2024/05/21	BANCO BBVA COLOMBIA S.A.	0	$147,048,300

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				92	$80,974,800	$0	$0	$80,974,800
COLFONDOS	231001	800,227,940	6	11	$12,505,500	$0	$0	$12,505,500
COLPENSIONES	25-14	900,336,004	7	14	$13,683,900	$0	$0	$13,683,900
PORVENIR	230301	800,224,808	8	38	$25,148,800	$0	$0	$25,148,800
PROTECCION	230201	800,229,739	0	28	$27,494,600	$0	$0	$27,494,600
SKANDIA	230901	800,253,055	2	1	$2,142,000	$0	$0	$2,142,000
ARL (ADMINISTRADORAS: 1)				98	$3,987,300	$0	$0	$3,987,300
COLMENA	14-25	800,226,175	3	98	$3,987,300	$0	$0	$3,987,300
CCF (ADMINISTRADORAS: 1)				94	$21,195,000	$0	$0	$21,195,000
COMPENSAR	CCF24	860,066,942	7	94	$21,195,000	$0	$0	$21,195,000
EPS (ADMINISTRADORAS: 10)				99	$34,071,500	$0	$0	$34,071,500
ALIANSALUD EPS (ANTES COLMEDICA)	EPS001	830,113,831	0	2	$1,795,000	$0	$0	$1,795,000
CAPITAL SALUD	EPSC34	900,298,372	9	1	$129,400	$0	$0	$129,400
COMPENSAR	EPS008	860,066,942	7	20	$5,158,600	$0	$0	$5,158,600
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	4	$506,400	$0	$0	$506,400
FAMISANAR	EPS017	830,003,564	7	13	$2,087,100	$0	$0	$2,087,100
FOSYGA	MIN001	901,037,916	1	7	$3,280,500	$0	$0	$3,280,500
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	$878,700	$0	$0	$878,700
SALUD TOTAL	EPS002	800,130,907	4	9	$1,275,100	$0	$0	$1,275,100
SANITAS	EPS005	800,251,440	6	35	$18,760,700	$0	$0	$18,760,700
ICBF (ADMINISTRADORAS: 1)				9	$4,091,800	$0	$0	$4,091,800
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	9	$4,091,800	$0	$0	$4,091,800
SENA (ADMINISTRADORAS: 1)				9	$2,727,900	$0	$0	$2,727,900
SENA	PASENA	899,999,034	1	9	$2,727,900	$0	$0	$2,727,900
TOTAL				**99**	**$147,048,300**	**$0**	**$0**	**$147,048,300**

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

Acta N°	13	**Tema:**	Reunión de revisión de ANS, contrato 173 de 2023
Fecha:	13/06/2024	**Ubicación:**	Videoconferencia
Hora inicio:	09:00 am	**Hora fin:**	10:00 am

Objetivo	Reunión de revisión de ANS, contrato 173-2023, Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, suscripción de licenciamiento.

PARTICIPANTES CONVOCADOS A LA REUNIÓN

Nombre completo	Dependencia	Cargo	¿Asistió?
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 03	Si
Plinio Esteban Palomino López	Mnemo	Gerente de Proyecto Mnemo	Si

TEMAS TRATADOS (Describir los puntos tratados en la reunión)

Revisión cumplimiento de ANS, contrato 173-2023, Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, suscripción de licenciamiento.

1. **Documentación de soporte**
   - PR-Herramienta - SIEM.pdf
   - Anexo Tecnico de Operación - SIEM.pdf

2. **Informe de ejecución presupuestal**

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor inicial del contrato	$ 36.499.583.610	100%
Adiciones	$ 0	0%
VALOR TOTAL DEL CONTRATO	**$ 36.499.583.610**	**100%**
Valor Ejecutado antes del presente pago	$ 21.277.959.214	58,30%
Valor del pago aprobado con el presente informe	$ 885.237.430	2,43%
VALOR TOTAL EJECUTADO	**$ 22.163.196.644**	**60,72%**
Descuento por ANS	$ 0,00	
DIFERENCIA EN LA EJECUCIÓN PRESUPUESTAL DEL CONTRATO	**0**	

3. Determinación del valor a facturar

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, Suscripción de licenciamiento.	$ 743.897.000	$ -	$ 743.897.000	$ 141.340.430	$ 885.237.430
Valor Total	**$ 743.897.000**	**$ -**	**$ 743.897.000**	**$ 141.340.430**	**$ 885.237.430**

Nota:

Instalación realizada en los servidores ya desbloqueados con la salida a producción de la plataforma SIEM

PowerEdge Server No. Serial: 4TD4H04, PowerEdge Server No. Serial: 5TD4H04, PowerVault SAN No. Serial: 49L3H04
Ver el valor del licenciamiento en la
Nota_Discriminación_valores_licencias V2.docx

COMPROMISOS PACTADOS	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO	FECHA DE CUMPLIMIENTO DEL COMPROMISO
N/A	N/A	N/A	N/A

APROBÓ	APROBÓ
Plinio Esteban Palomino Gerente de Proyecto Mnemo Colombia S.A.S.	**Enrique Arrázola** Apoyo a la supervisión 173-2023 Gerencia de Estrategia de TI y Aseguramiento Informático

SUPERVISIÓN AL CONTRATO No. 173 de 2023
FONDO NACIONAL DEL AHORRO
Informe No. 15

Instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento.

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

Bogotá, D.C. junio de 2024

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 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 del hito referente a la Instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento.

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

El componente EdgeGateway esta soportado e implementado sobre la infraestructura compuesta por 2 appliance Dell Power Edge modelo R660 y una SAN Dell EMC Power Vault modelo ME5012 que albergara múltiples servicios contemplados para el contrato 173-2023. Para este informe se hace referencia al servicio SOAR a través de la solución Cloud Pak (deploymenttesmn9.console.cloudpak.security.ibm.com) más puntualmente del componente conocido como EdgeGateway dentro del servicio mencionado.

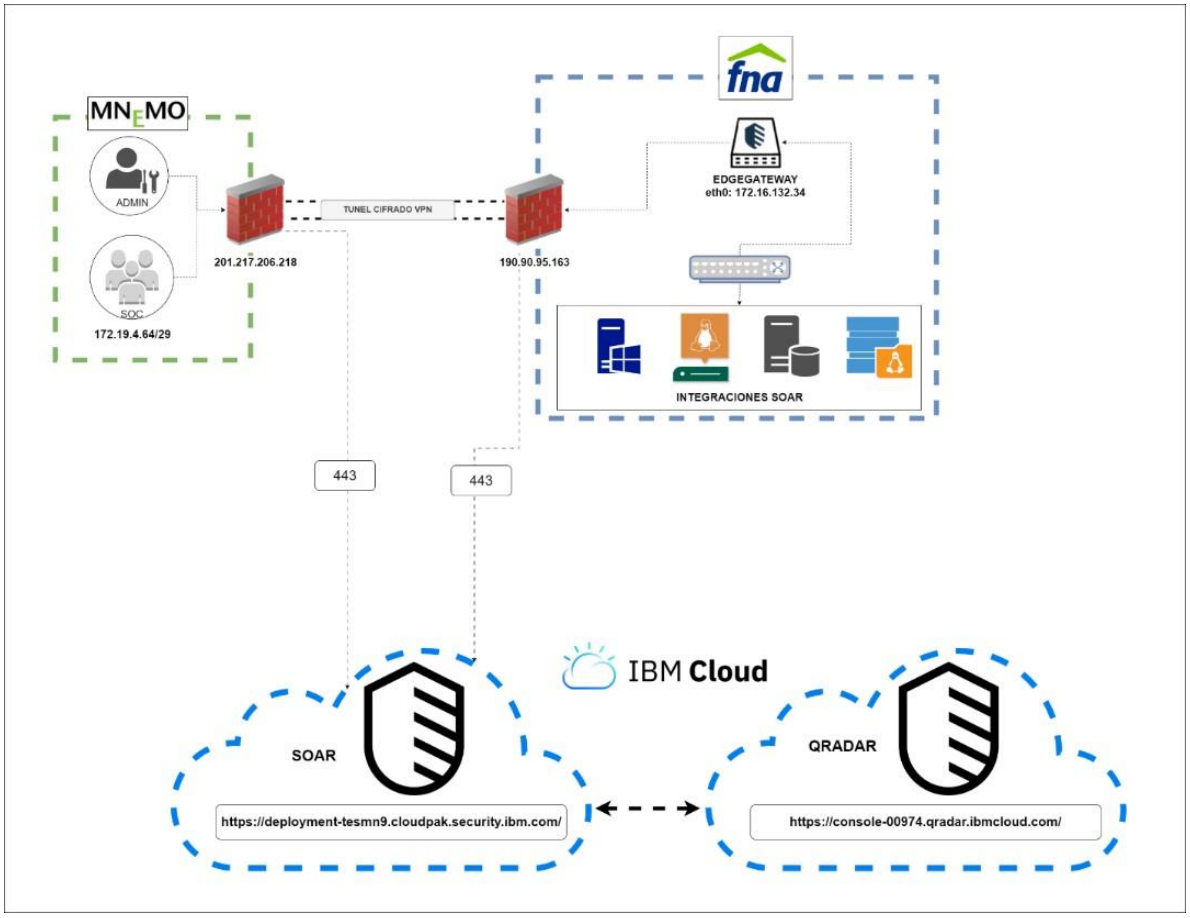
Teniendo en cuenta las especificaciones técnicas definidas, para este caso el EdgeGateway se acondiciono la siguiente máquina virtual con los siguientes recursos:

Configuración de hardware	
CPU	2 vCPUs
Memoria	4 GB
Disco duro 1	100 GB
Adaptador de red 1	VM_Network_VLAN_132 (Conectado)
Tarjeta de vídeo	8 MB
Unidad de CD/DVD 1	ATAPI CD/DVD drive 0.
Otros	Hardware adicional

Así las cosas y de acuerdo con lo establecido en el CTO 173 de 2023, se realiza el seguimiento, control y verificación de las actividades concernientes a la Instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento. Para lo cual se adjuntan con el siguiente informe, las memorias técnicas, Diagramas de arquitectura, informes de instalación, integración, configuración, pruebas e implementación, suscripción de licenciamiento y acta de entrada en producción del componente SOAR, a saber:

1. *Acta de Entrada en producción de la plataforma SOAR.*

2. *Diagrama de arquitectura, que incluye las Características técnicas de Hardware y software de este nuevo componente.*



3. *informes de instalación, configuración, pruebas, puesta en marcha y estabilización de la solución SOAR.*

4. *Suscripción de licenciamiento del nuevo componente.*

5.1 INFORMACIÓN DE AVANCE PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	$ 36.499.583.610,00	**100,00%**
Adiciones	$ -	**0,00%**
VALOR TOTAL DEL CONTRATO	**$ 36.499.583.610,00**	**100,00%**
Valor ejecutado antes del presente pago	$ 21.720.653.494,00	**59,51%**
Valor del pago aprobado con el presente informe	$ 885.237.430,00	**2,43%**
VALOR TOTAL EJECUTADO	**$ 22.605.890.924,00**	**61,93%**
Porcentaje de ejecución presupuestal programado a la fecha		**62,00%**
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		**-0,06%**

Se define que el avance presupuestal del contrato va de acuerdo con las actividades a la fecha incluyendo ANS penalizados.

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 la Instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento.

A continuación, se detalla el porcentaje de avance realizado de la actividad:

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 dé lugar a ninguna penalización.

VALOR A FACTURAR

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, Suscripción de licenciamiento.	$ 743.897.000	$ -	$ 743.897.000	$ 141.340.430	$ 885.237.430
Valor Total	$ 743.897.000	$ -	$ 743.897.000	$ 141.340.430	$ 885.237.430

7. VERIFICACIÓN DE ENTREGABLES

Por el desarrollo de las actividades ejecutadas en cuanto a la Instalación, configuración, pruebas, puesta en marcha y estabilización de la plataforma SOAR y suscripción de licenciamiento, 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**	**Observ aciones**
1	Anexo Técnico de Operación - SIEM.*pdf*	Bueno	27/04/2024	Ninguna
2	*Inf_Gestion Memoria Técnica SOAR Implementación FNA.pdf*	Bueno	27/04/2024	Ninguna
3	*PR-Herramienta - SIEM.pdf*	Bueno	16/05/2024	Ninguna
4	*MNCO-SIG-24-0019_FNA 173-2023_SOAR.pdf*	Bueno	16/05/2024	Ninguna
5	*MNCO-SOC-IG-01 Memoria Técnica SOAR Implementación FNA.pdf*	Bueno	16/05/2024	Ninguna

Se define que, para la facturación del pago del periodo reportado, el contratista debe entregar junto a la prefactura 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 **OCHOCIENTOS OCHENTA Y DOS MILLONES QUINIENTOS QUINCE MIL SETECIENTOS CUARENTA PESOS MCTE ($885,237,430).**

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

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

Se firma a los 24 días del mes de junio de 2024.

MONICA GRAND VILLADA
Gerente Estrategia TI y Aseguramiento Informático
Supervisor CTO 173 de 2023

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

0. OBJETIVO

Documentar los aspectos técnicos de la Solución de Firewall de Aplicación Web (WAF) de la Unidad de Ciberseguridad, sus componentes, sus integraciones, y sus medidas de contingencia.

1. ASPECTOS TÉCNICOS DE LA SOLUCION

1.1. Descripción De la Solución En Operación Normal

1.1.1. Diagrama De Componentes

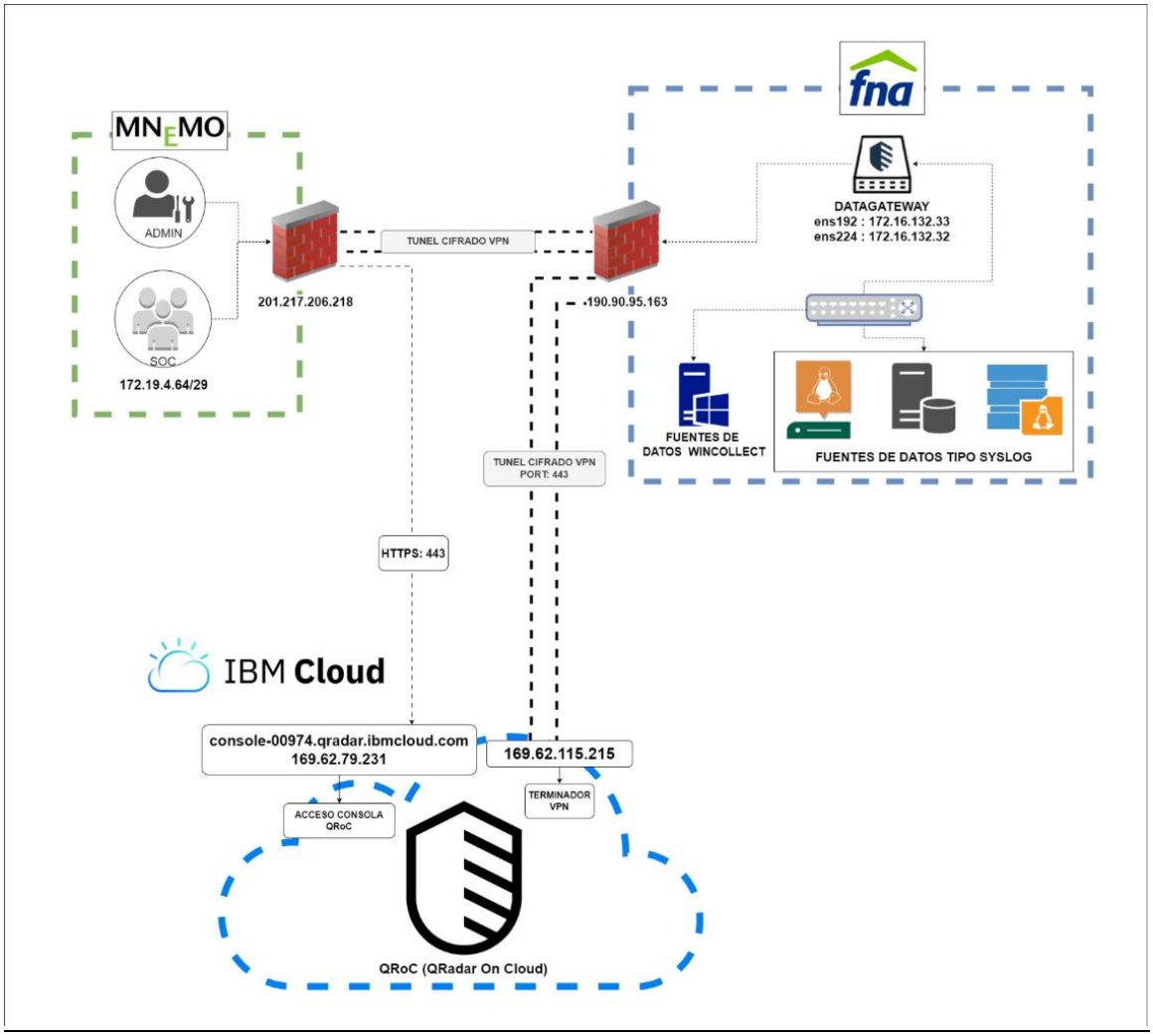


Ilustración 1. Diagrama de Componentes

1.1.2. Integración con Servicios De TI del FNA

La Solución de Administración de Eventos e Información de Seguridad (SIEM) tiene la capacidad de integrarse con cualquier dispositivo de red, servidores, sistemas de informacion o aplicaciones, que se deseen monitorear. Actualmente se encuentra monitoreando alrededor de 68 fuentes criticas para el Fondo Nacional del Ahorro.

1.1.3. Integración con Servicio de Terceros

Integración	IP / URL
TthreatQ	https://threatq.mnemo.com/
Trend Micro XDR	api.xdr.trendmicro.com
CloudPack (SOAR)	https://deployment-tesmn9.console.cloudpak.security.ibm.com/
201.2017.206.218 (FNA)	VPN
172.19.4.64 (MNEMO)	Segmento de VPN con el FNA para los administradores

1.1.4. Recursos Necesarios

1.1.4.1. Personal responsable:

Nombre de la persona	Rol	Datos de contacto
Sergio Sanclemente	Gerente de Ciberseguridad	s.sanclemente@mnemo.com
Oscar Ivan Acevedo Vargas - Analista L2	Administrador de IBM QRADAR	oi.acevedovargas@mnemo.com
Analistas SOC 7x24	Analista SOC	soc.col@mnemo.com

1.1.4.2. Información:

Nombre carpeta	Información que contiene	Ruta
Carpeta compartida	Documentación relacionado con la operación de las soluciones de seguridad informática administradas por la Unidad de Ciberseguridad	/CTO-173-2023/3.EJECUCION CONTRACTUAL/3.Ejecución/Entregables/Implementación unidad de Ciberseguridad/Ejecución/Protocolos de Actuación/3. Gestión de la operación

1.1.4.3. Aplicaciones para hacer la administración:

- **Explorador web (Firefox, Chrome)**
- **MobaXterm**: Conexión por ssh a los servidores

1.1.4.4. Inventario de componentes:

NOMBRE DEL COMPONENTE	DIRECCIÓN IP	ROL DEL COMPONENTE
DATAGATEWAY	172.16.132.33 172.16.132.32	Colector de eventos
IBM QROC (Qradar On Cloud)	Console-00974.qradar.ibmcloud.com	Manager GUI QRADR
WINCOLLECT (fuente de datos)		Agentes del correlacionador para sistemas operativos WINDOWS
SISYLOG (fuente de datos)		Dispositivos a los que no se les puede instalar agentes WINCOLLECT

Inventario de servicios del servidor DATAGATEWAY:

Puerto	Descripción del servicio
443	Conexión HTTPS
22	Conexión SSH

Agente de Monitoreo	Puerto de servicio
Agente de Amazon EC2	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)
Agente de Amazon ELB	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)
Agente de Azure Compute	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)
Agente de Cassandra	• 7199 (para servidor JMX, local y remoto)
Agente de Cisco UCS	• Puerto TCP 80 (para HTTP) • Puerto TCP 443 (para HTTPS)
Agente de Citrix VDI	• Para llamadas PowerShell: • 5985 (para HTTP) • 5986 (para HTTPS)
Agente de Db2	• 50000 (puerto predeterminado de servidor de Db2) • Supervisión remota soportada: utiliza el número de puerto indicado por el usuario al catalogar la instancia de servidor remoto.
Agente de DataPower	• 5550 (para conectarse a un dispositivo DataPower remoto)
Agente de Hadoop	• Supervisión local: valor de la variable de entorno CP_PORT • Supervisión remota: • 50070 (Namenode en espera) • 50090 (Namenode secundario) • 8088 (ResourceManager) • 19888 (JobHistory Server) • 8080 (Ambari)
Agente de HMC Base	• 12443 (para descargar el SDK de HMC)

Agente de Monitoreo	Puerto de servicio
Agente de HTTP Server	• El servidor HTTP se puede configurar en un puerto distinto, pero el agente en sí no tiene ningún puerto predeterminado.
Agente de IBM® Cloud	• Conexión de salida a api.softlayer.com puerto 443.
Agente de IBM Integration Bus	• N/A
Internet Service Monitoring	• Para databridge: • 9510 • 9520
Agente de DataStage	• 9443 (puerto HTTPS de WAS) • 50000 (puerto JDBC de base de datos) • 1433 (Microsoft SQL) • 1521 (Oracle)
Recopilador de datos de J2SE	• N/A
Agente de JBoss	• Varía según la versión del servidor JBoss: • 9990 • 9994 • 9999
Recopilador de datos de Liberty	• N/A
Agente de Linux KVM	• 8080 (para HTTP) • 8443 (para HTTPS)
Agente de sistema operativo Linux	• 22 (para la supervisión de registro remoto con SSH)
Agente de MariaDB	• 3306
Agente de Microsoft Active Directory	• El número de puerto depende del valor de escucha para el uso de supervisión.
Agente de Microsoft Cluster Server	• N/A
Agente de Microsoft Exchange Server	• N/A
Agente de Microsoft Hyper-V Server	• N/A
Agente de Microsoft IIS	• N/D
Agente de Microsoft .NET	• Para enviar datos de rastreo de transacciones, se utiliza el puerto 5456 de forma predeterminada.
Agente de Microsoft Office 365	• 7799 (para la transacción sintética Skype)
Agente de Microsoft SharePoint Server	• 1433 (para servidor SQL)
Agente de Microsoft SQL Server	• 1433 (predeterminado del servidor SQL)
Agente de MQ Appliance	• 162 (para recibir sucesos de SNMP) • 5554 (para conectar a MQ Appliances)
Agente de MongoDB	• 27017 (para instancia única) • 27019 (para clúster)
Agente de MySQL	• 3306 (para conexión JDBC)
Agente de NetApp Storage	• Para la supervisión remota: • 8088 • 8488 • 443 • 8443
Agente de Node.js	• 63336
Recopilador de datos de Node.js	• N/D

Agente de Monitoreo	Puerto de servicio
Agente de OpenStack	• 5000 (para conectar el servicio de identidad de OpenStack)
Agente de Oracle Database	• 1521 (para conexión SQL)
Agente de PHP	• Conexión de Apache • El número de puerto se basa en la configuración de Apache
Agente de PostgreSQL	• 5432 (para conexión JDBC)
Recopilador de datos de Python	• N/D
Agente de RabbitMQ	• Número de puerto en el que el plug-in de gestión de RabbitMQ está habilitado (local y remoto): 15672
Agente de Supervisión de tiempo de respuesta	• El modelo de analizador de paquetes supervisa transacciones HTTP en el puerto 80. • El modelo de servidor HTTP supervisa todos los puertos.
Agente de Ruby	• Se genera dinámicamente
Recopilador de datos de Ruby	• N/D
Agente de SAP	• 33nn (donde nn es el número de instancia de SAP)
Agente de SAP HANA Database	• Valor predeterminado: 30013. Rango: 30013-39913.
Agente de SAP NetWeaver Java™ Stack	• Valor predeterminado: 50004. Rango: 50004-59904.
Agente de Siebel	• N/D
Agente de Skype for Business Server (anteriormente conocido como agente de Microsoft Lync Server)	• Puerto predeterminado de Business server 5061 • Puerto de servidor SQL 1433 (local o remoto en función del entorno).
Agente de Sterling Connect Direct	• 1363
Agente de Sterling File Gateway	• 50000 • El número de puerto de la API REST de IBM B2B Integrator y el número de puerto de base de datos son necesarios y se pueden configurar.
Agente de Sybase	• 5000
Agente de Synthetic Playback	• 4444 (para la conexión de servidor selenium interno) • Los puertos remotos se especifican en el URL http de los sitios web supervisados, generalmente HTTP 80 y HTTPS 443
Agente de Tomcat	• 8686 (para el servidor MBean de Tomcat)
Agente de sistema operativo UNIX	• 22 (para la supervisión de registro remoto con SSH)
Agente de VMware VI	• 443 (para la supervisión remota) • 80 (para la supervisión local)
Agente de WebLogic	• 7003 (Tráfico HTTP de gestión de JMX)
Agente de WebSphere Applications	• 63335 (para agente de supervisión V8) • 63336 (para agente de supervisión V6) • 63355 (para supervisión de recursos) • 5457 (para Transaction Framework Extension)
Agente de WebSphere Infrastructure Manager	• N/D

Agente de Monitoreo	Puerto de servicio
Agente de WebSphere MQ	• El número de puerto depende del valor de escucha para el uso de supervisión.
Agente de sistema operativo Windows	• 22 (para la supervisión de registro remoto con SSH)

1.2. Descripción General Del Servicio En Contingencia

NOMBRE DEL COMPONENTE	DESCRIPCIÓN
DATAGATEWAY	Se cuenta con un servidor virtualizado on premise en el FNA con dos interfaces de red: ens192: 172.16.132.33 ens224: 172.16.132.32
IBM QROC (Qradar On Cloud)	Es un servicio en nube que cuenta con todas las garantías de disponibilidad del proveedor IBM Disponen de Zonas de disponibilidad

Copias de respaldo

El servicio principal es un servicio en nube que cuenta con zonas de disponibilidad que garantizan la continuidad del servicio, asi mismo mantiene una copia de los eventos reportados por el DATAGATEWAY.

Memoria Técnica

Implementación SOAR FNA

GUIA MNEMO

MAYO 2024

CREADO POR:

MNEMO

CONTENIDO

CONTROL DE CAMBIOS 3
1. CONTENIDO DE ESTA GUIA 4
2. INTRODUCCIÓN 5
3. QRADAR SOAR VISIÓN GENERAL 6
4. REQUISITOS GENERALES DEL SISTEMA DEL DISPOSITIVO DATAGATEWAY 8
5. ARQUITECTURA GENERAL QRoC (QRadar On Cloud) 9
6. ARQUITECTURA DE RED SOAR FNA 10
7. INSTALACION DATAGATEWAY 11
8. INTEGRACION DEL EDGE GATEWAY 12
9. INTEGRACION DE APP 16
10. PRUEBA DE PLAYBOOK 20
11. REPORTE PANELES Y METRICAS 24
12. GESTION DE RED EDGE GATEWAY 25
13. COPIA DE SEGURIDAD Y RECUPERACIÓN 26
14. TOLERANCIA A FALLOS 28
15. INTEGRACION CON INTELIGENCIA DE AMENAZAS 28
16. INTEGRACION CON TERCEROS 29
17. NOTIFICACIONES 30
18. GESTION USUARIOS 32
CONCLUSION 35

CONTROL DE CAMBIOS

FECHA	DESCRIPCIÓN	CREADO/MODIFICADO POR
27 Mayo 2024	Memoria Técnica Implementación SOAR FNA	Oscar Ivan Acevedo Vargas

Nota: Se permite controlar los cambios en el control de versiones del repositorio

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados. ***NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL.*** *No está permitida su reproducción, distribución o comunicación fuera del destinatario.*

1. CONTENIDO DE ESTA GUIA

Esta guía está diseñada con el fin de presentar y explicar de la forma más sencilla posible la implementación del componente **EdgeGateway** con la instalación y configuración de la solución SOAR QRadar en la infraestructura de FNA, brindando información técnica acerca de la instalación y de la conectividad tanto física como lógica de la solución.

De igual manera se exponen los escenarios de instalación en las diferentes plataformas que se configuraron para la comunicación y conexión con orígenes de datos.

2. INTRODUCCIÓN

El componente **EdgeGateway** esta soportado e implementado sobre la infraestructura compuesta por 2 appliance **Dell Power Edge** modelo **R660** y una **SAN Dell EMC Power Vault** modelo **ME5012** que albergara múltiples servicios contemplado para el contrato **173-2023** para el presente documento se hace referencia al servicio **SOAR** a través de la solución Cloud Pak (deployment-tesmn9.console.cloudpak.security.ibm.com) más puntualmente del componente conocido como **EdgeGateway** dentro del servicio mencionado.

Esta guía está diseñada con el fin de presentar implementación de la solución **SOAR** y el funcionamiento de la solución implementada para el **FNA**, brindando información técnica acerca de la instalación y de la conectividad tanto física como lógica de la solución.

De igual manera se exponen los escenarios de instalación en las diferentes plataformas que se configuraron para la comunicación y toma de acciones en las integraciones.

AUDIENCIA Y SUGERENCIAS DE LECTURA

Para el entendimiento del actual documento se asume que el lector posee un conocimiento básico sobre los productos y terminología de las *plataformas*, un conocimiento medio en teoría y mejores prácticas en gestión de Logs y un conocimiento básico en seguridad informática y sistemas operativos. Igualmente se espera que el lector disponga de conocimientos sobre el repositorio de logs en las aplicaciones y la característica de cada uno de ellos.

3. QRADAR SOAR VISIÓN GENERAL

Las primeras decisiones que toma al responder a un posible incidente de seguridad o ciberataque a menudo marcan la diferencia entre contenerlo o que ocurra una crisis. Desafortunadamente, la mayoría de las organizaciones utilizan procesos de seguridad manuales que consumen mucho tiempo o código personalizado sin la funcionalidad completa de orquestación, automatización y respuesta de seguridad (SOAR).

La plataforma **IBM Security QRadar SOAR** está diseñada para optimizar los procesos de toma de decisiones, mejorar la eficiencia del **SOC** y garantizar que el proceso de respuesta a incidentes se cumpla con una solución inteligente de automatización y orquestación, ayudando a la organización a:

1. Reducir el tiempo de respuesta con playbooks dinámicos, flujos de trabajo personalizables y automatizados, y respuestas recomendadas

2. Optimizar los procesos de respuesta a incidentes al marcar el tiempo de las acciones clave y ayudar en la inteligencia y la respuesta a las amenazas

3.1. Edge Gateway

IBM Security Edge Gateway habilita IBM Security QRadar Suite Software para conectarse con orígenes de datos alojados en la nube privada, o para instalar y ejecutar aplicaciones IBM Security QRadar SOAR.

Edge Gateway es un componente basado en Kubernetes que puede utilizar para conectar orígenes de datos de su entorno a IBM Security QRadar Suite Software o para instalar y ejecutar apps de IBM Security QRadar SOAR.

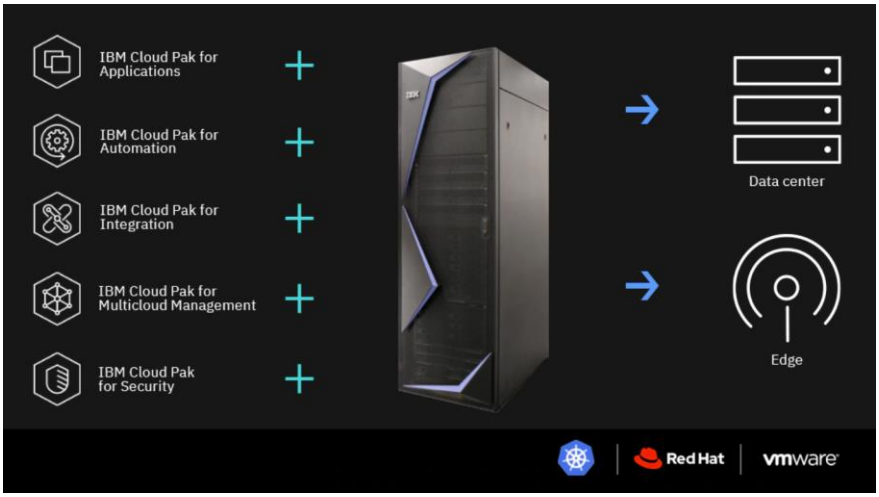
Entre otras funciones IBM Security Edge Gateway sera utilizado en el Fondo Nacional del Ahorro con la siguiente funcionalidad o propósito:

Desplegar apps de IBM Security QRadar SOAR

Puede utilizar la característica de aplicación IBM Security QRadar SOAR para instalar y configurar una aplicación basada en Python, que es un paquete de software que amplía la capacidad de la aplicación IBM Security QRadar SOAR. Puede contener uno o más componentes de playbook, un componente de código externo o ambos. Los componentes de playbook incluyen scripts Python, reglas, flujos de trabajo, funciones, destinos de mensajes, campos y tablas de datos. Un componente de código externo puede acceder y devolver datos externos, interactuar o integrarse con otros sistemas de seguridad, o ser un programa de utilidad que complete una acción específica.

3.2. IBM CloudPak

El sistema IBM Cloud Pak es una solución de nube privada llave en mano que facilita la implementación y el mantenimiento de nubes privadas de nivel empresarial para VM y aplicaciones basadas en contenedores. Evite los gastos y la complejidad de las soluciones tradicionales de nube privada. Viene con entornos VMware y Red Hat OpenShift listos para implementar aplicaciones y middleware.



3.2.1. BENEFICIOS

Conecta aplicaciones con facilidad:

Permite la creación de flujos fácilmente con herramientas de integración sin código, plantillas y conectores prediseñados para las aplicaciones.

Reaccionar en tiempo real

Al remplazar los flujos de trabajo manuales con una serie de acciones automáticas que abordan las necesidades del cliente en tiempo real, activadas por eventos internos o externos.

4. REQUISITOS GENERALES DEL SISTEMA DEL DISPOSITIVO DATAGATEWAY

Esta sección lista los requisitos previos si está instalando **Edge Gateway**, estos requisitos se aplican a los formatos de aplicación autónoma y virtual del software de Edge Gateway:

- Los requisitos previos para el sistema que aloja Edge Gateway son los siguientes:
    - Sistema operativo: Red Hat Enterprise Linux v8.4 a v8.10.
    - Si está instalando el dispositivo virtual de Edge Gateway, se ejecuta en vSphere Hypervisor (ESXi) 6.7 U2 o posterior.
    - Un mínimo de 5 GB de espacio de disco libre.
    - Mínimo de 2 GB de RAM.
    - Un mínimo de dos CPU.
    - Cuenta de sistema operativo dedicada para orígenes de datos.
    - Si está instalando el formato autónomo, se necesita una cuenta de usuario en el sistema con privilegios de sudo.
    - Acceda a la aplicación IBM Security QRadar Suite Software.
    - Acceso a aplicaciones de terceros necesario para los orígenes de datos.
    - Si está instalando la aplicación virtual Edge Gateway, asegúrese también de que el número de puerto TCP 22 sea accesible para su gestión local.

4.1 Configuración de la VM Edge Gateway

Teniendo en cuenta las especificaciones técnicas, para este caso el EdgeGateway se acondiciono la siguiente máquina virtual con los siguientes recursos.

Configuración de hardware	
CPU	2 vCPUs
Memoria	4 GB
Disco duro 1	100 GB
Adaptador de red 1	VM_Network_VLAN_132 (Conectado)
Tarjeta de vídeo	8 MB
Unidad de CD/DVD 1	ATAPI CD/DVD drive 0.
Otros	Hardware adicional

5. ARQUITECTURA GENERAL QRoC (QRadar On Cloud)

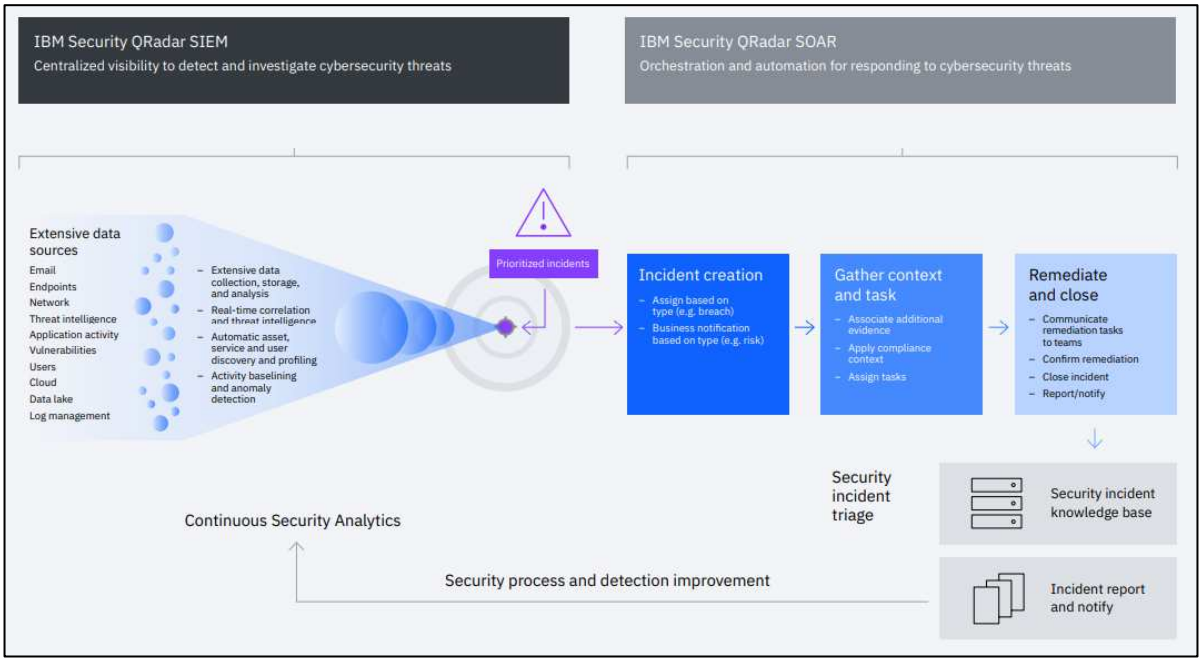


Ilustración 1 Arquitectura IBM SOAR

6. ARQUITECTURA DE RED SOAR FNA

En la gráfica continuación se presenta la arquitectura de red del componente SOAR, en la integración con sus respectivos componentes SIEM y Edge Gateway, así como con la operativa SOC.

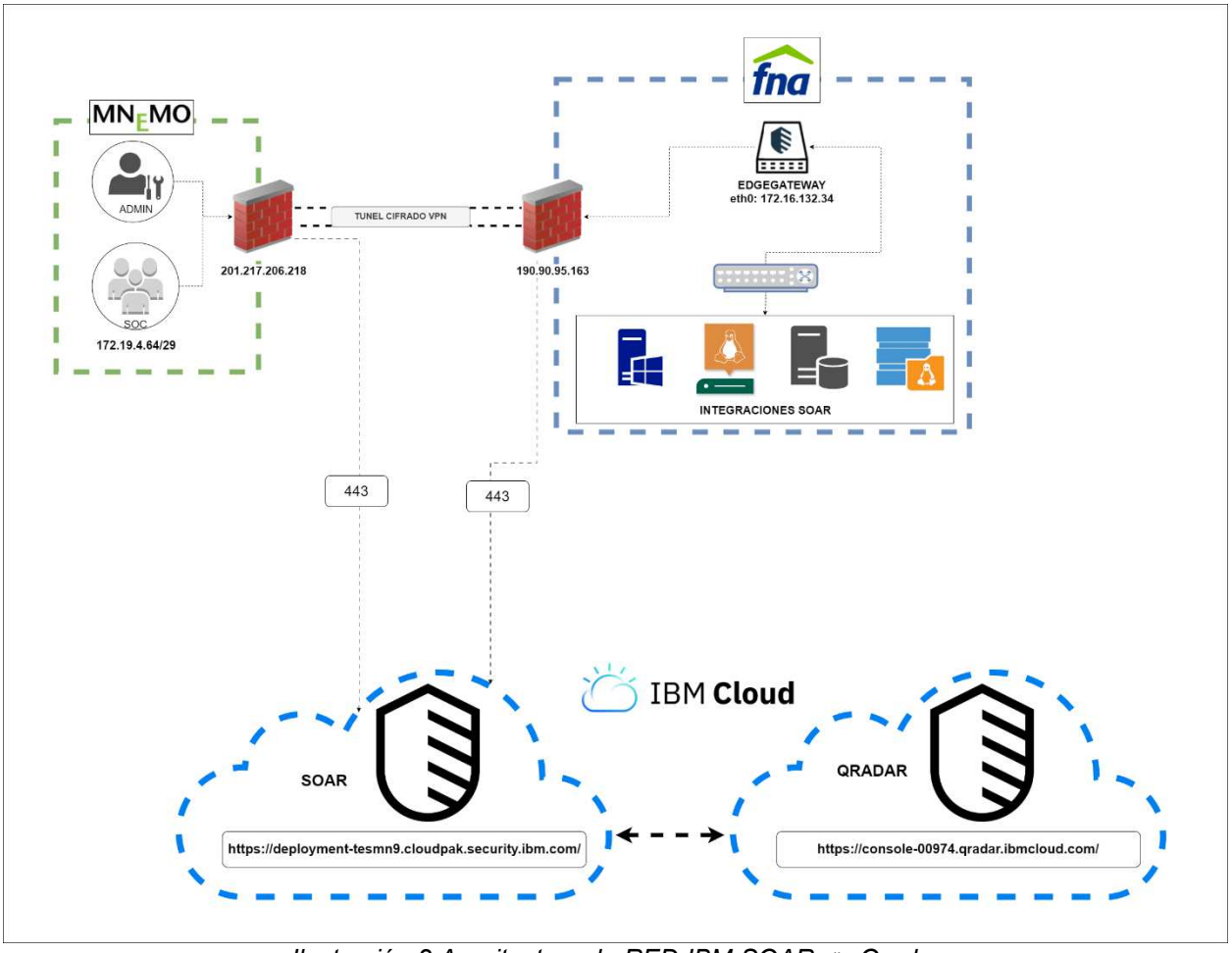


Ilustración 2 Arquitectura de RED IBM SOAR <> Qradar

7. INSTALACION DATAGATEWAY

A continuación, se detalla a la descripción de la instalación del subcomponente SOAR Edge Gateway, con la finalidad de que este pueda ser ejecutado en futuras instalaciones.

1. Abra el cliente VMware vSphere.
2. Seleccione Archivo > Desplegar plantilla OVF.
3. Vaya a la ubicación del archivo .ova que ha descargado y seleccione el archivo apphost_redhat8_1.15.1.1.ova.
4. Cuando se le solicite, escriba un nombre para la plantilla descargada.
5. Cuando se le solicite en la pantalla Formato de disco, seleccione la opción provisiones gruesas, Edge Gateway utiliza inicialmente 100 gigabytes de almacenamiento. Si elige Suministro ligero, el Edge Gateway inicialmente empieza a utilizar una pequeña cantidad de gigabytes y crece con el tiempo.
6. En la pantalla Listo para completarse , seleccione la opción Encender después del despliegue y pulse Finalizar. Aparece una barra de estado durante el despliegue. VMware le notifica cuando la imagen de Edge Gateway se despliega correctamente.
7. Pulse Cerrar en el recuadro de diálogo Despliegue completado correctamente .
8. Después del rearranque, el primer script de arranque se inicia automáticamente e instala la imagen de Edge Gateway . Esto puede tardar unos minutos.
9. Cuando se le solicite, revise los valores de red. Puede aceptar la configuración predeterminada o modificarla.

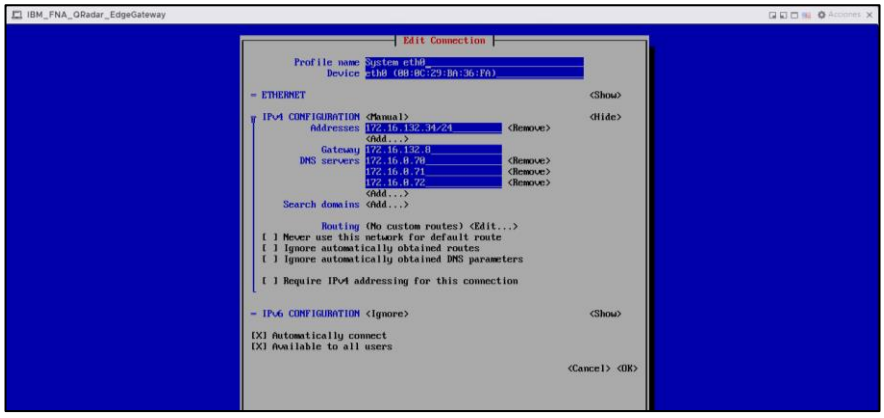


Ilustración 3 configuración de RED EgeGateway

10. Los valores de clúster se listan como Cluster CIDR y Service CIDR, cuyos valores predeterminados son 10.42.0.0/24 y 10.43.0.0/16 respectivamente. Puede cambiarlos por valores CIDR válidos, como 10.50.0.0/16 y 10.60.0.0/16.

8. INTEGRACION DEL EDGE GATEWAY

11. Una vez realizado el proceso de instalación del EdgeGateway, se procede a ingresar a la consola CloudPak (**https://deployment-tesmn9.cloudpak.security.ibm.com**), en la sección EdgeGateway

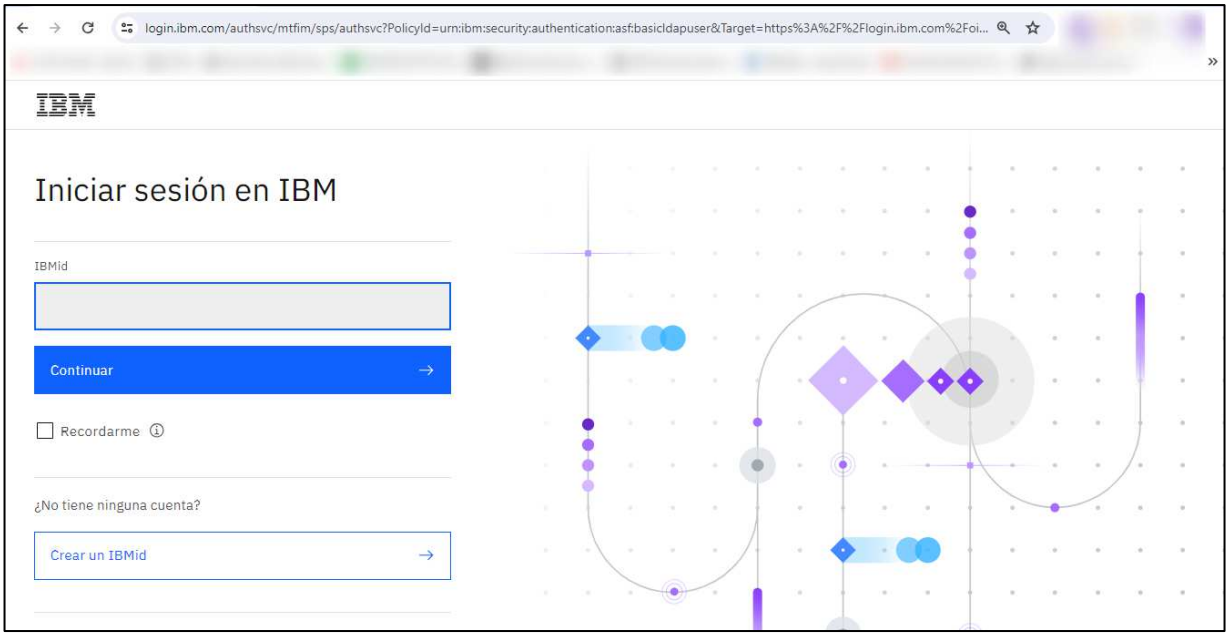


Ilustración 4 ingreso a CloudPak

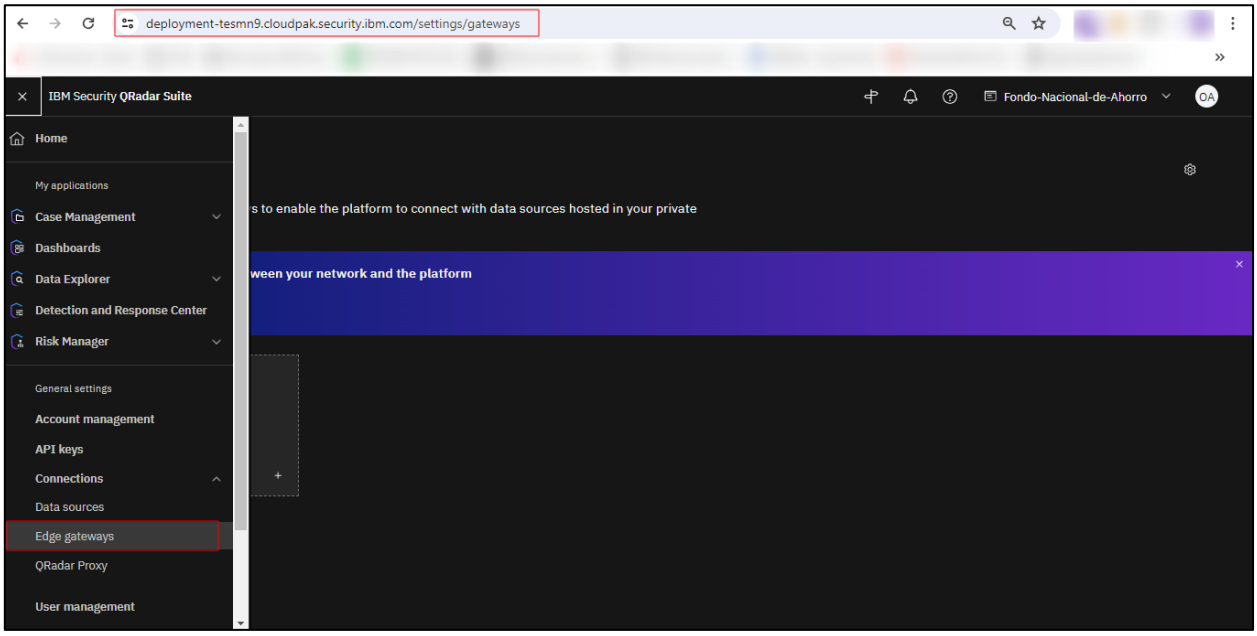


Ilustración 5 selección EdgeGateway

12. En la siguiente imagen se evidencia como se realiza la creación del código de emparejamiento para posteriormente generar la petición en el EdgeGateway y crear la conexión.

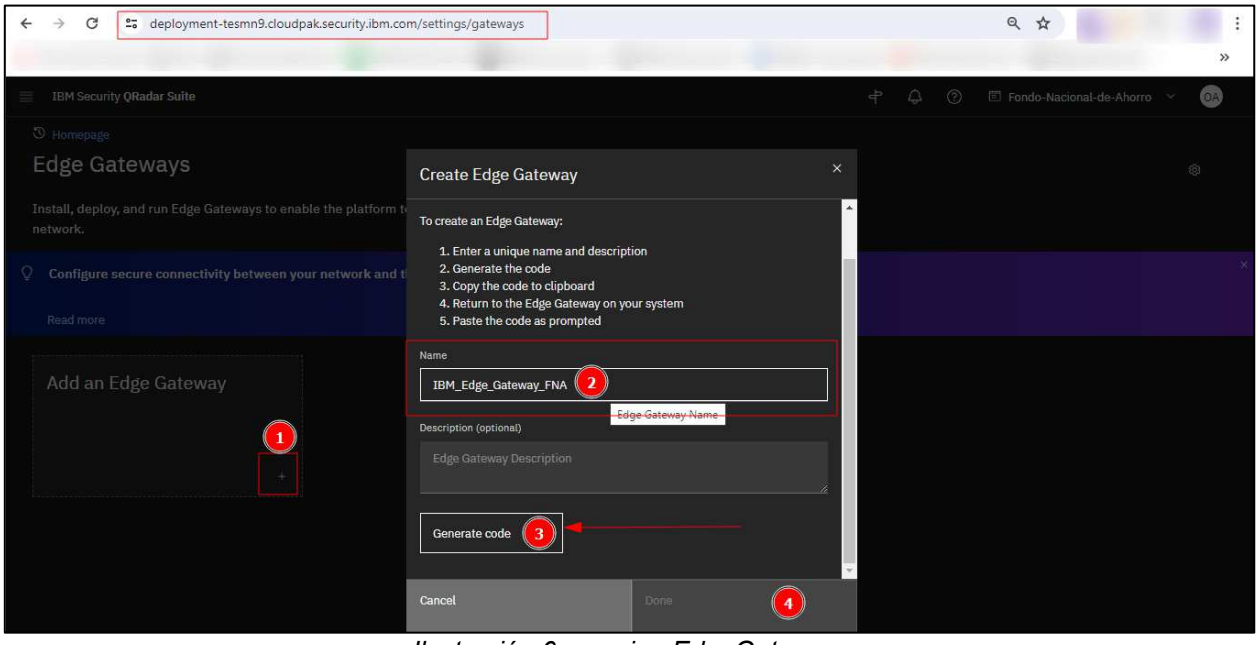


Ilustración 6 creacion EdgeGateway

13. Una vez obtenido dicho código como se evidencia en la pantalla siguiente, se procede a ingresar al EdgeGateway y realizar el proceso de emparejamiento

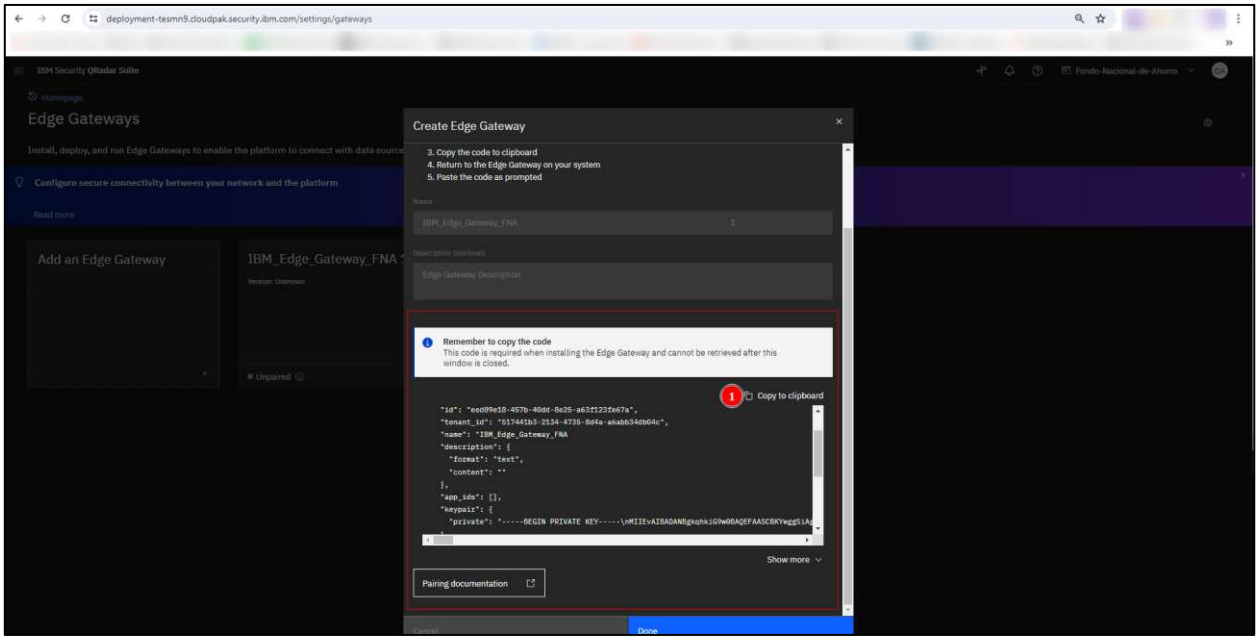


Ilustración 7 generación código emparejamiento

14. Con la ejecución del comando (**sudo manageAppHost install)**, se inicia el proceso de emparejamiento con la consola CloudPak, adicionalmente se ingresa

Ilustración 8 emparejamiento edgeGateway

15. Una vez realizado este proceso en la consola CloudPak, se observa el proceso de emparejamiento

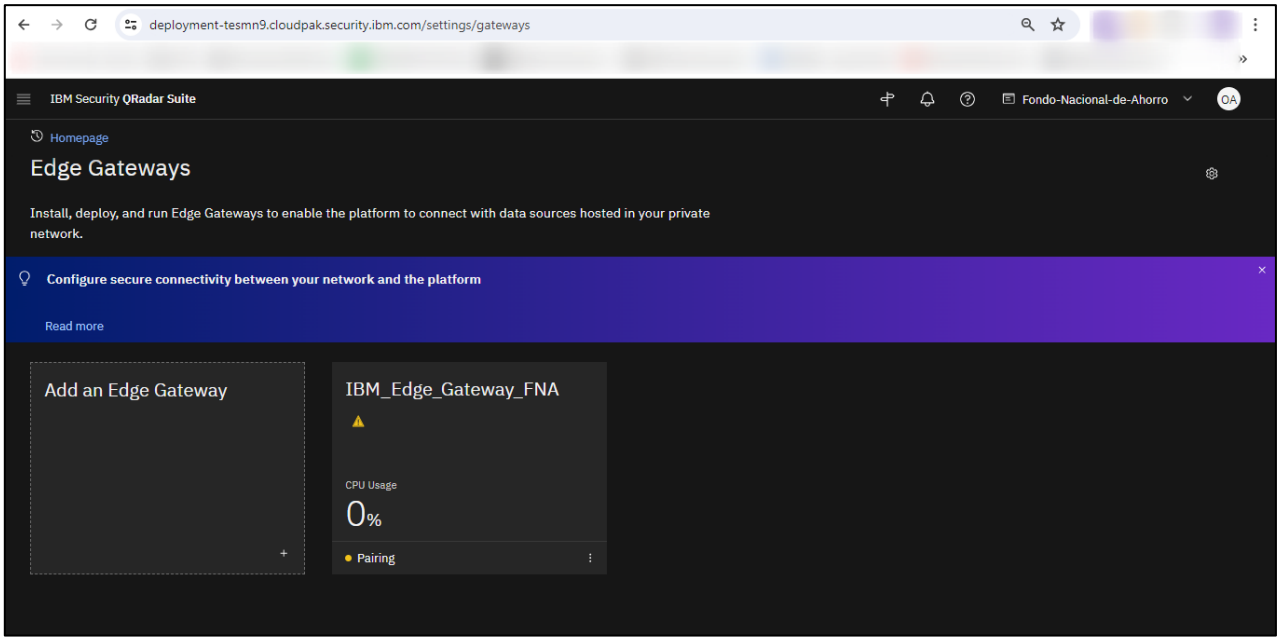


Ilustración 9 emparejamiento consola CloudPak

16. Posteriormente una vez finalice el proceso de emparejamiento se observa en la plataforma que el servicio se encuentra en ejecución.

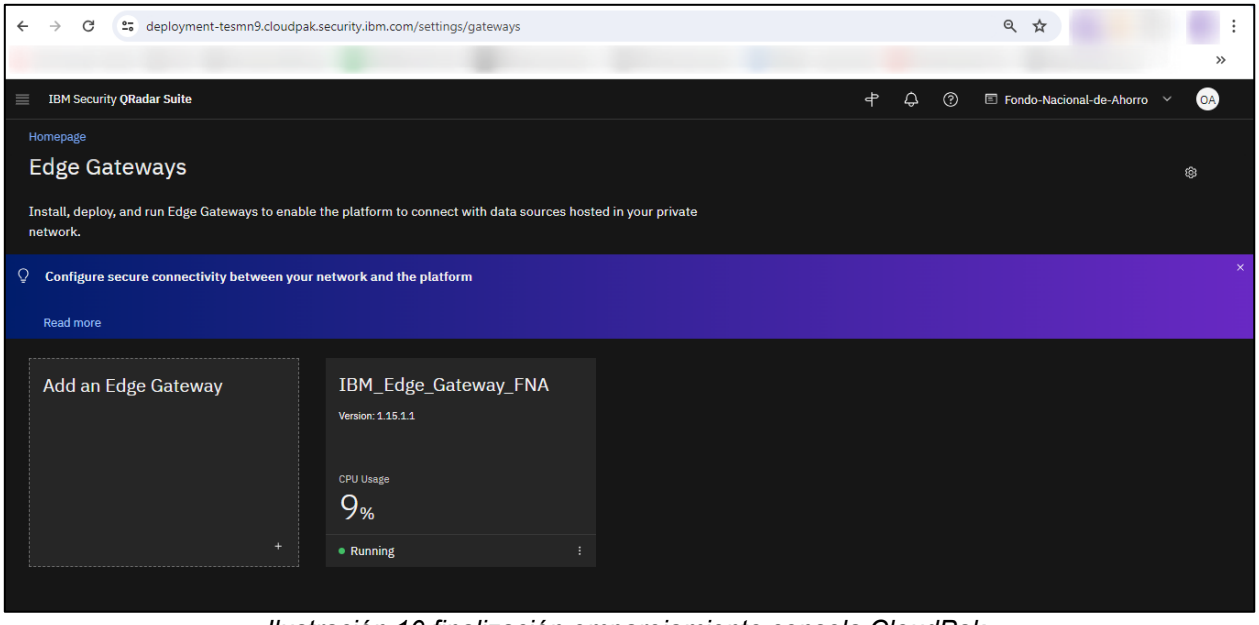


Ilustración 10 finalización emparejamiento consola CloudPak

9. INTEGRACION DE APP

17. Finalizado el proceso de instalación y despliegue se procede a realizar la integración de los diferentes APP las cuales permiten, las ejecuciones de acciones remotas sobre los diferentes productos disponibles para integración de **SOAR.**

Ingresando a la configuración de administración y despliegue de aplicaciones.

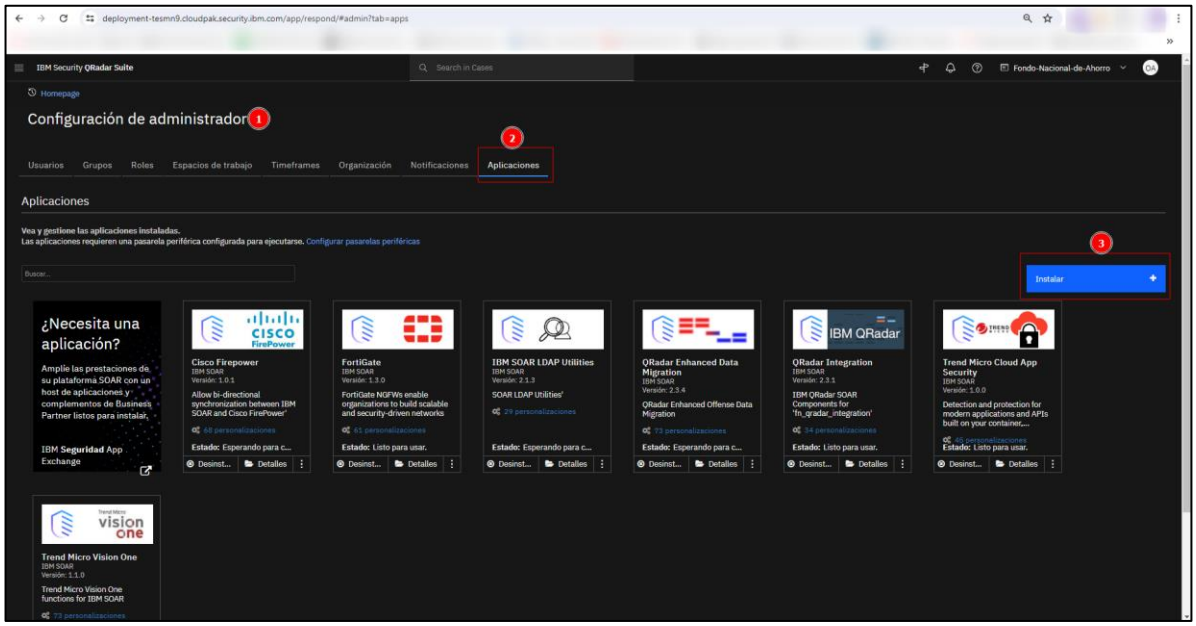


Ilustración 11 selección integración APP

18. Se procede a seleccionar la siguiente herramienta con el fin de establecer la comunicación entre el **SOAR** y esta herramienta de seguridad, para este caso **Trend Micro Vision One**

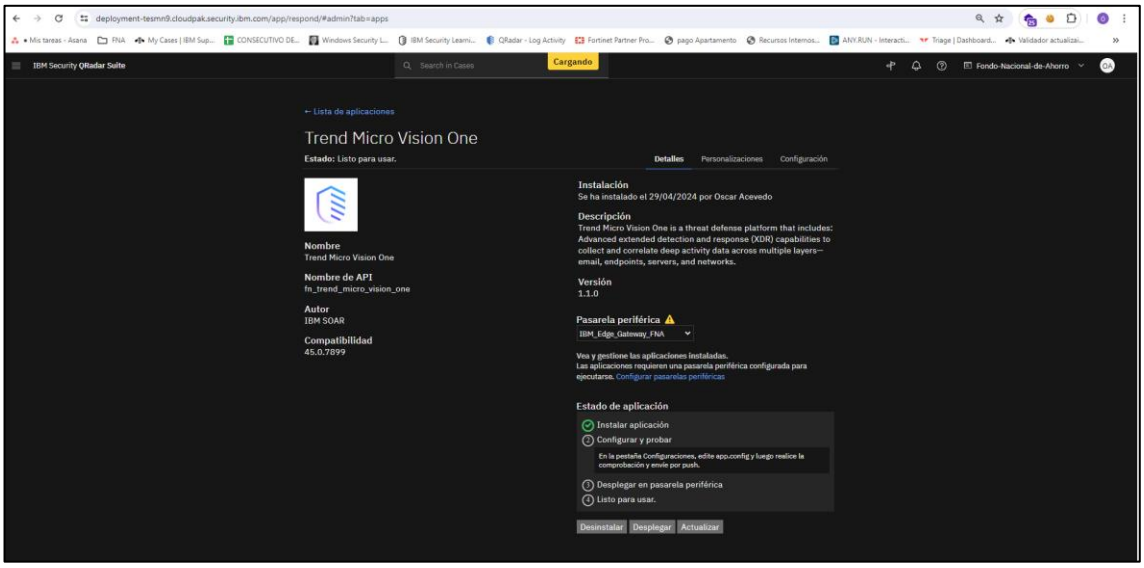


Ilustración 12 validación conexión tren micro

19. Seleccionamos la opción de configuración y se despliega el archivo de configuración (app.config) el cual proporciona los valores para comunicarse con la plataforma SOAR.

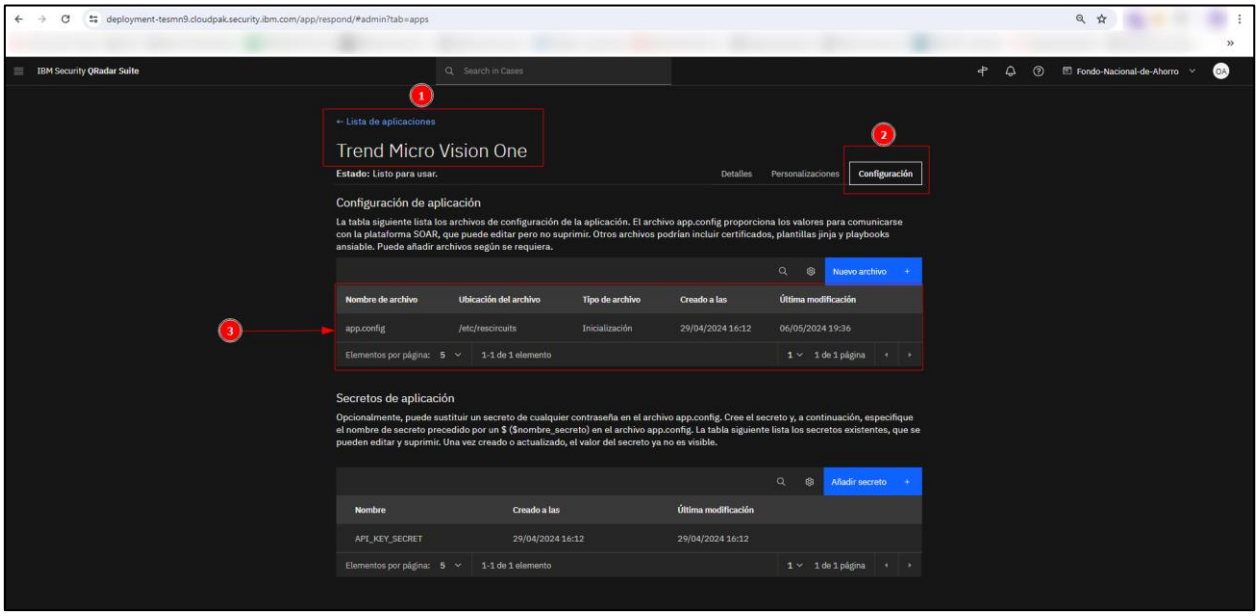


Ilustración 13 configuración archivo app.conf

20. En este apartado se debe con anterioridad obtener el API Key correspondiente, para este caso desde la plataforma Trend Micro Vision One, y la dirección URL de la API, con estos datos se procede a reemplazar los campos 2y3 del archivo de configuración.

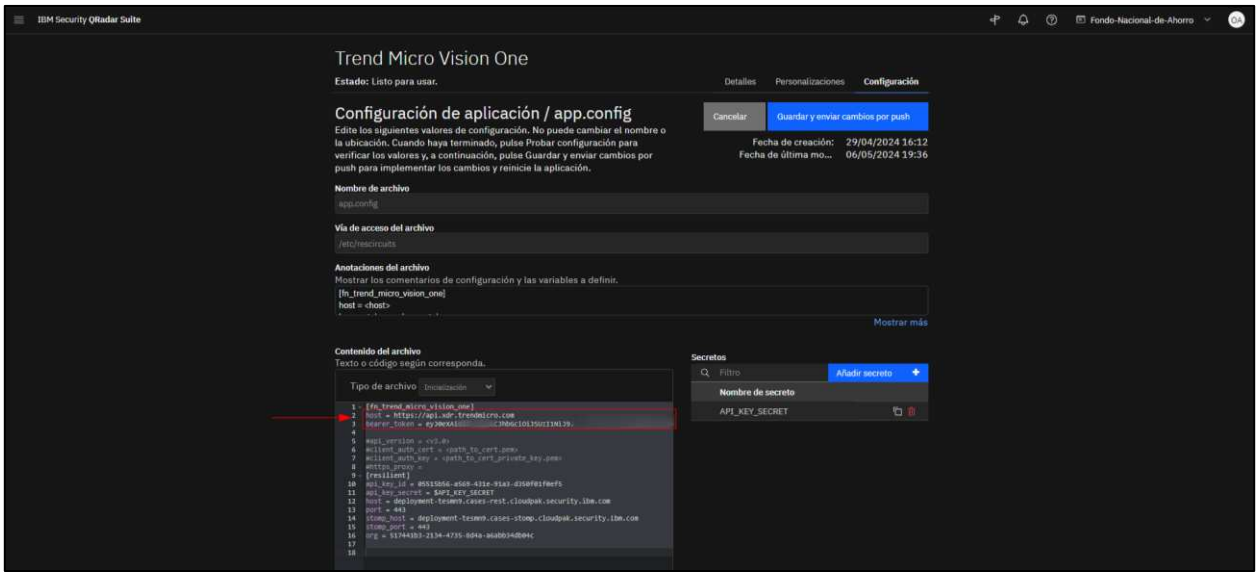


Ilustración 14 configuración conexión API

21. Ahora procedemos a realizar la prueba de conexión, como se puede observar en la imagen a continuación.

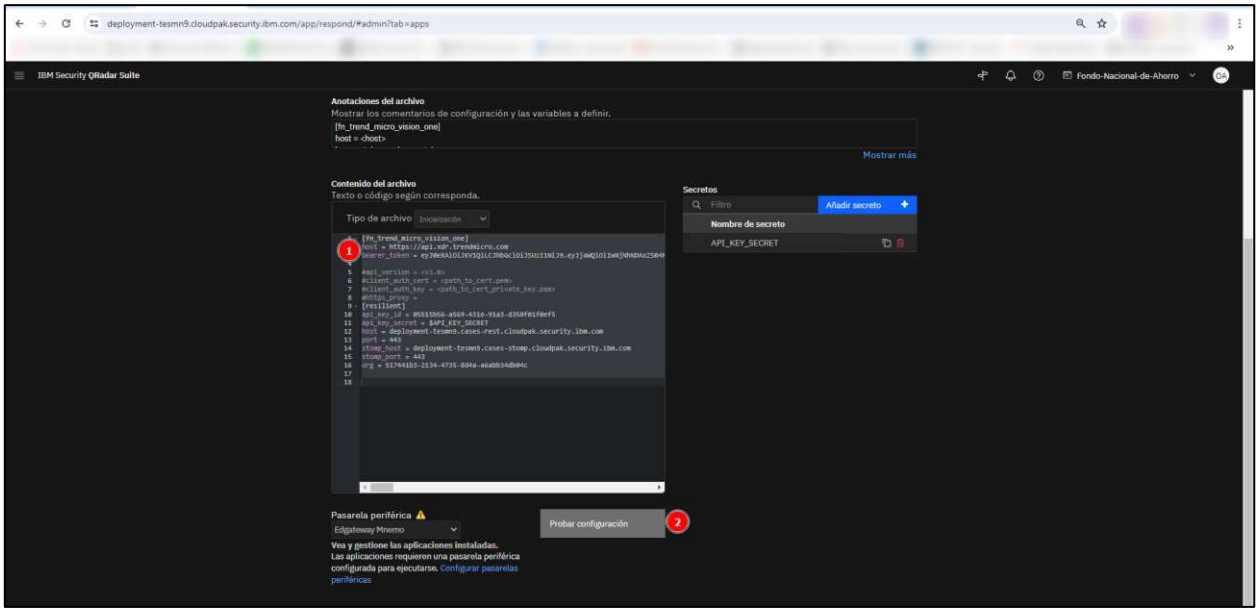


Ilustración 15 prueba de conexión con API

22. En esta imagen se evidencia que la prueba es exitosa

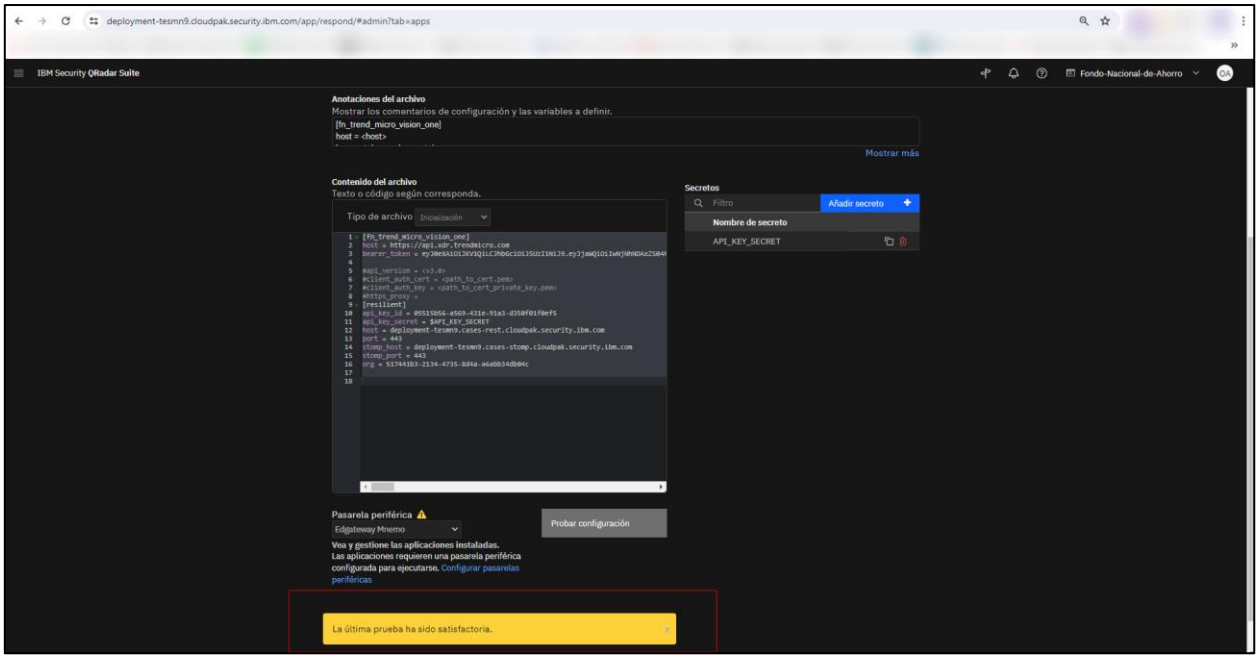


Ilustración 16 prueba correcta

23. Una vez realizado el proceso de integración con las herramientas terceras, se procede a crear los playbook los cuales permiten la generación de respuestas y acciones en dichas herramientas

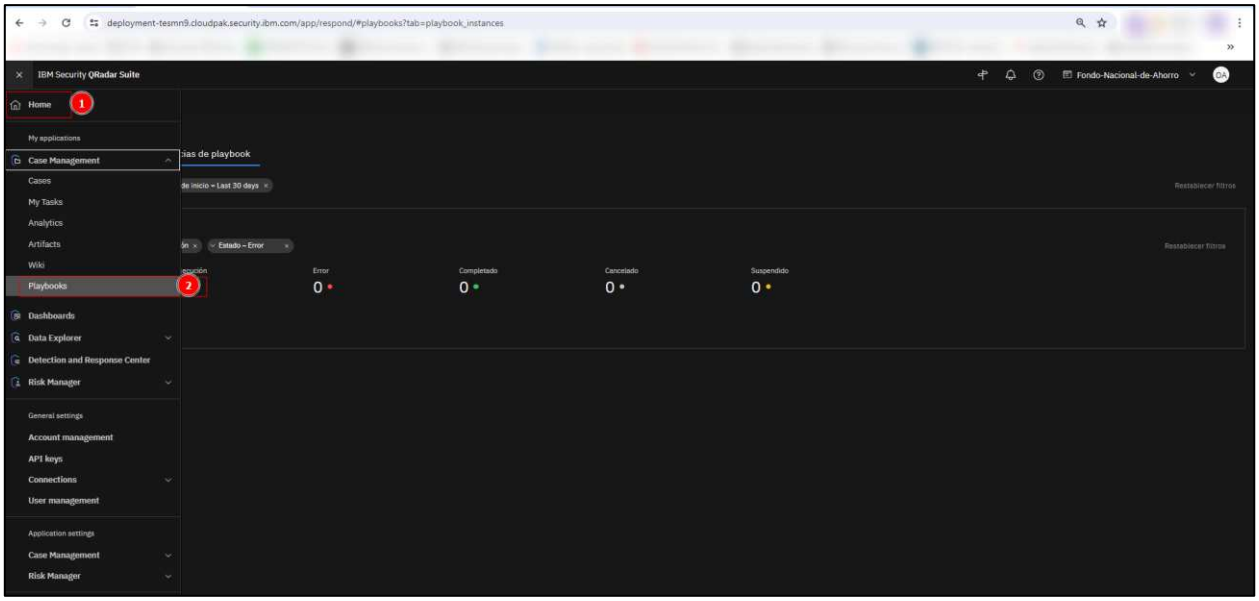


Ilustración 17 menú playbooks

24. En esta pantalla se presenta los playbook disponibles para uso, de acuerdo a lo que se defina por el cliente, estos playbooks pueden ser modificados para que s ajusten a las necesidades del cliente

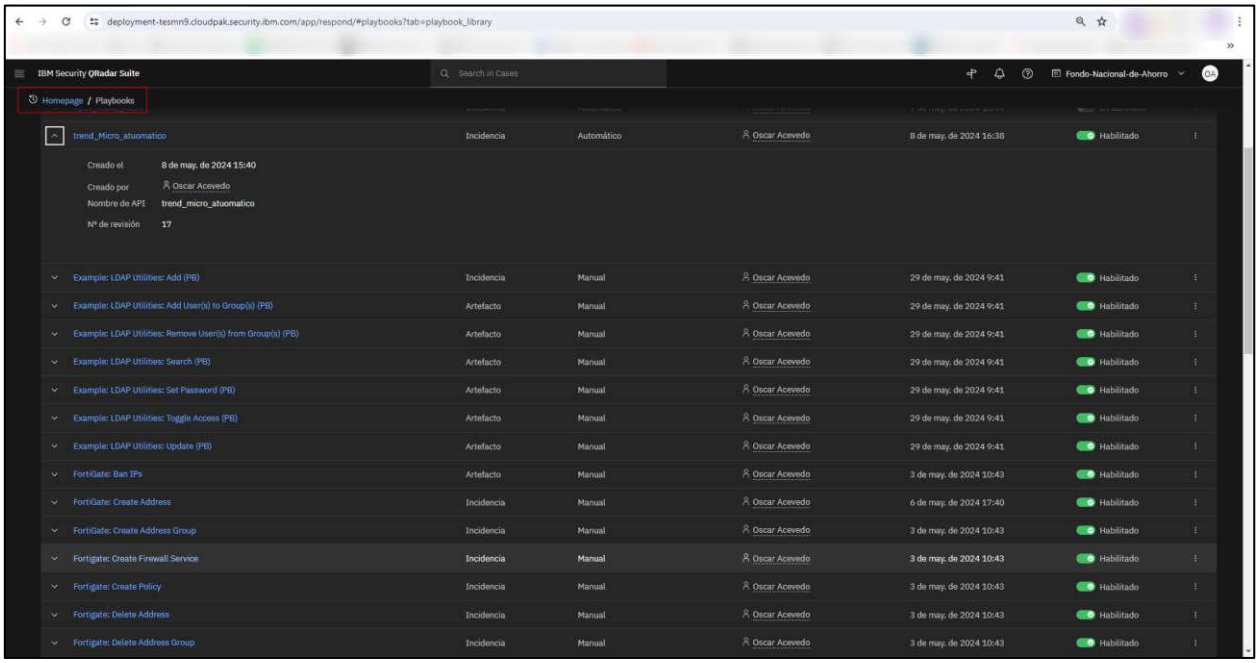


Ilustración 18 playbook disponibles

10. PRUEBA DE PLAYBOOK

25. El siguiente playboook que utilizaremos corresponde a la adición automática de una **iP** catalogada como maliciosa en QRadar, en la lista de **(Suspicious Object List) del tren micro visión one,** como se observa en esta imagen la respuesta a la incidencia se activa en el momento que identifique una regla proveniente de QRadar con el nombre **WAF_Ataque_Detectado**

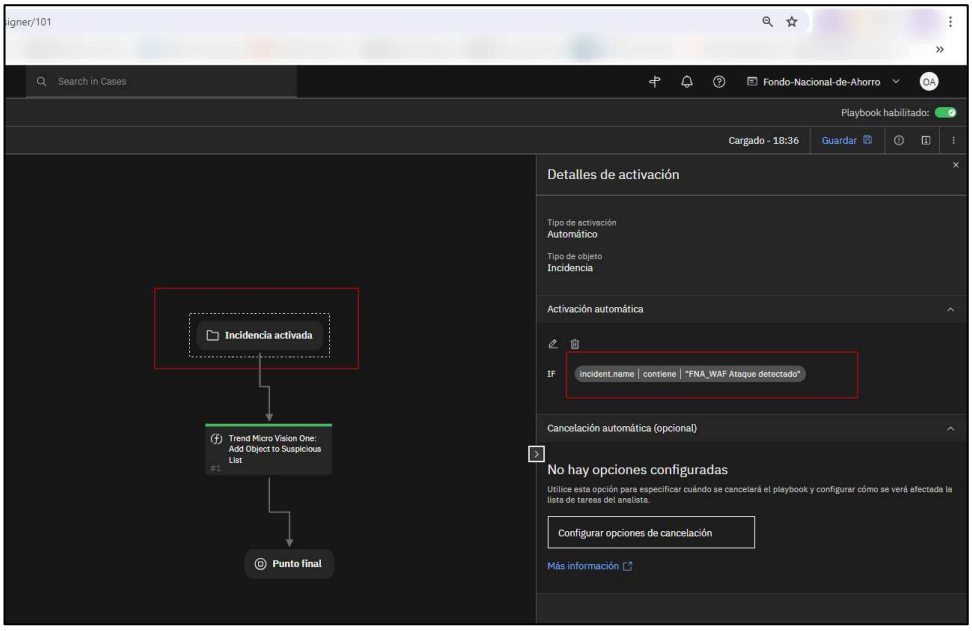


Ilustración 19 acciones playbook

26. En esta ilustración se identifica la acción a tomar por parte del playbook, la cual es adicionar de forma automática la iP de origen tomada del campo proveniente de la incidencia generada en Qradar.

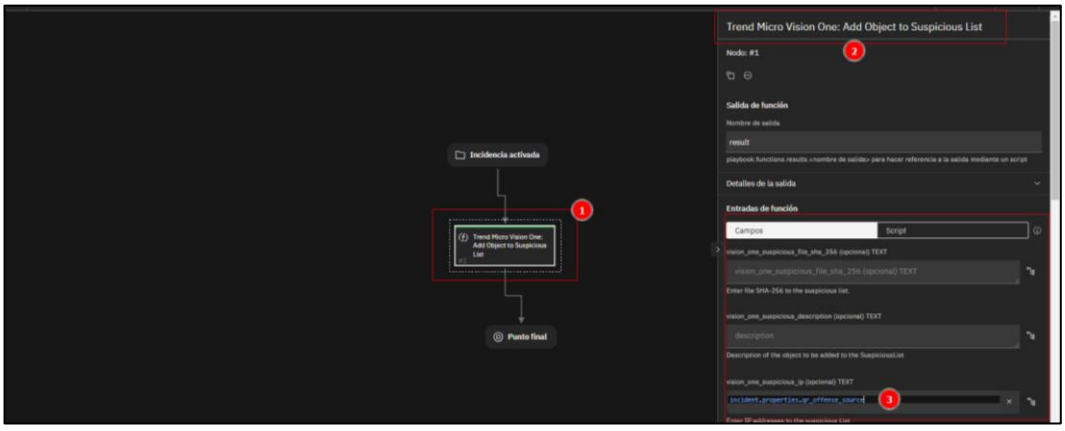


Ilustración 20 acciones playbook

27. En esta sección se evidencia como el Qradar identifica una iP la cual presenta cierto riesgo, esto basado en la validación de la herramienta de theta hunting (IBM X-force), y se levanta la alerta **FNA_WAF Ataque detectado**

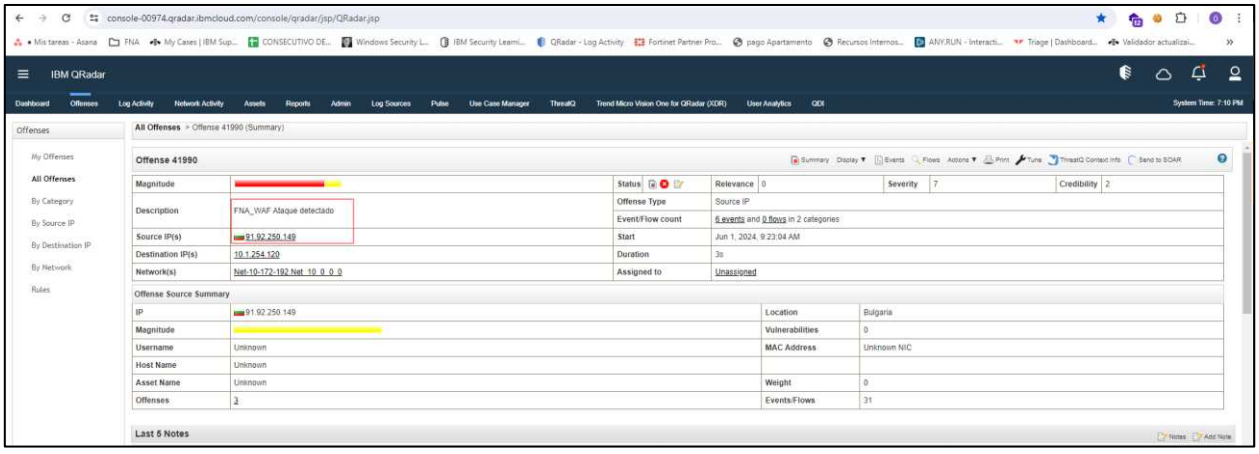


Ilustración 21alerta QRadar

28. Se observa que la iP presenta un riesgo y a partir de esto se levanto la alerta

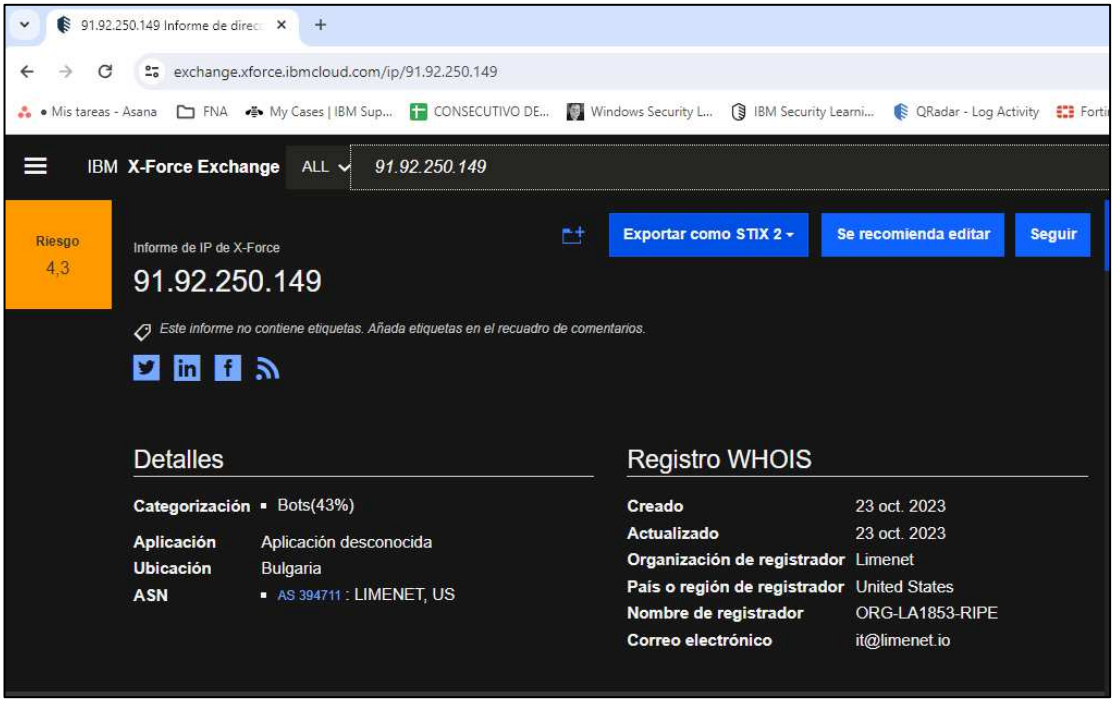


Ilustración 22 validación de IOC

29. Ahora procedemos a enviar esta alerta al SOAR

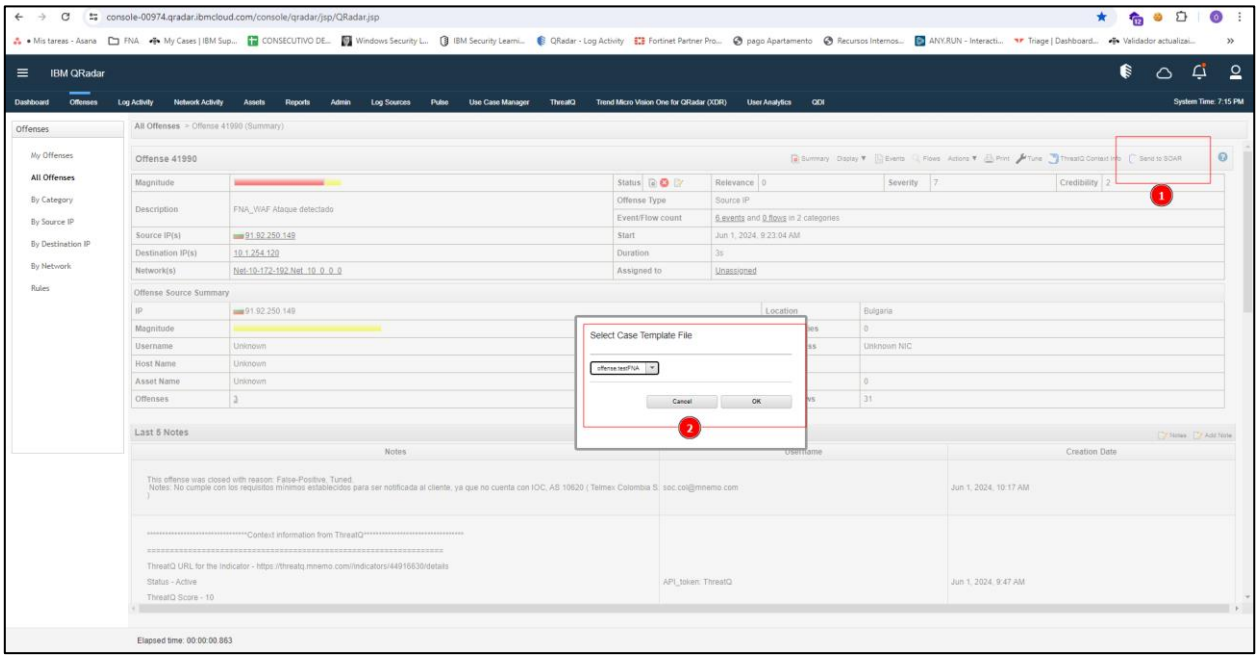


Ilustración 23 envió alerta a SOAR desde Qradar

30. Ahora podemos evidenciar que en la plataforma SOAR de CloudPak aparece la alerta enviada anteriormente, se observa el capo con la iP de origen **91.92.250.149.**

Una vez la alerta en este espacio de casos se activa automáticamente el playbook configurado anteriormente

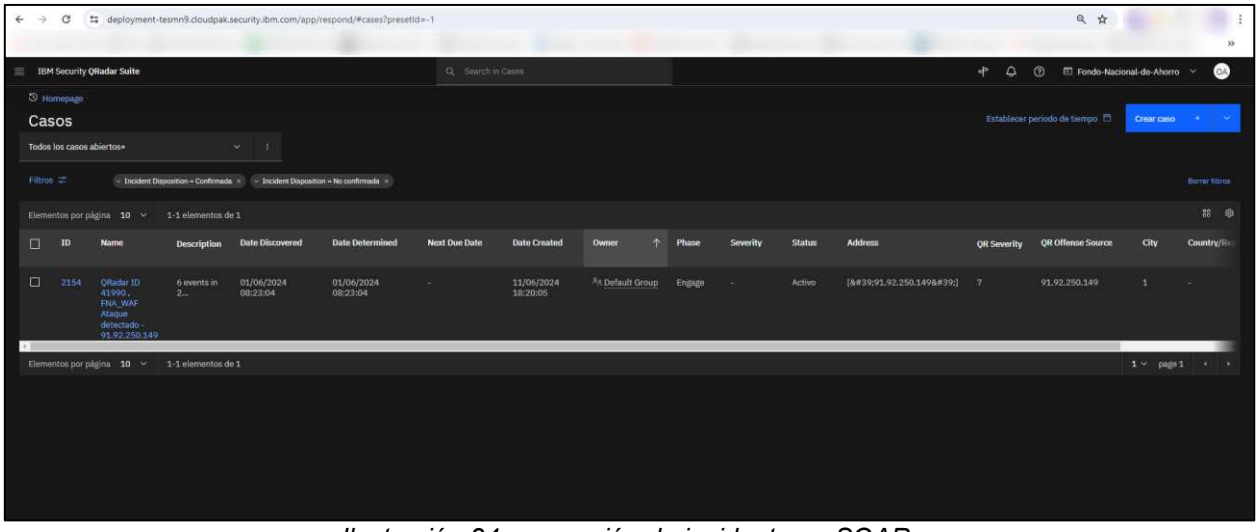


Ilustración 24 generación de incidente en SOAR

31. Como se evidencian en el campo estado del playbook, se encuentra en completado

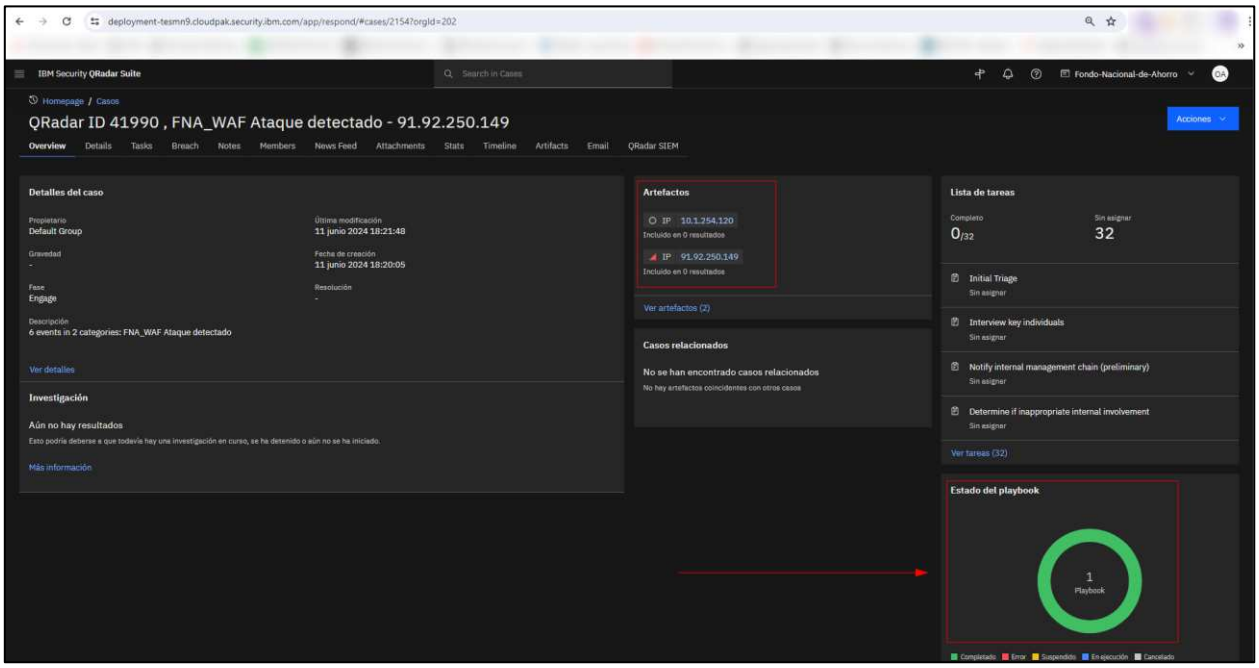


Ilustración 25 validación de ejecución de Playbook

32. Por ultimo se observa que la iP maliciosa se carga exitosamente por medio dela conexión API de forma automatica.

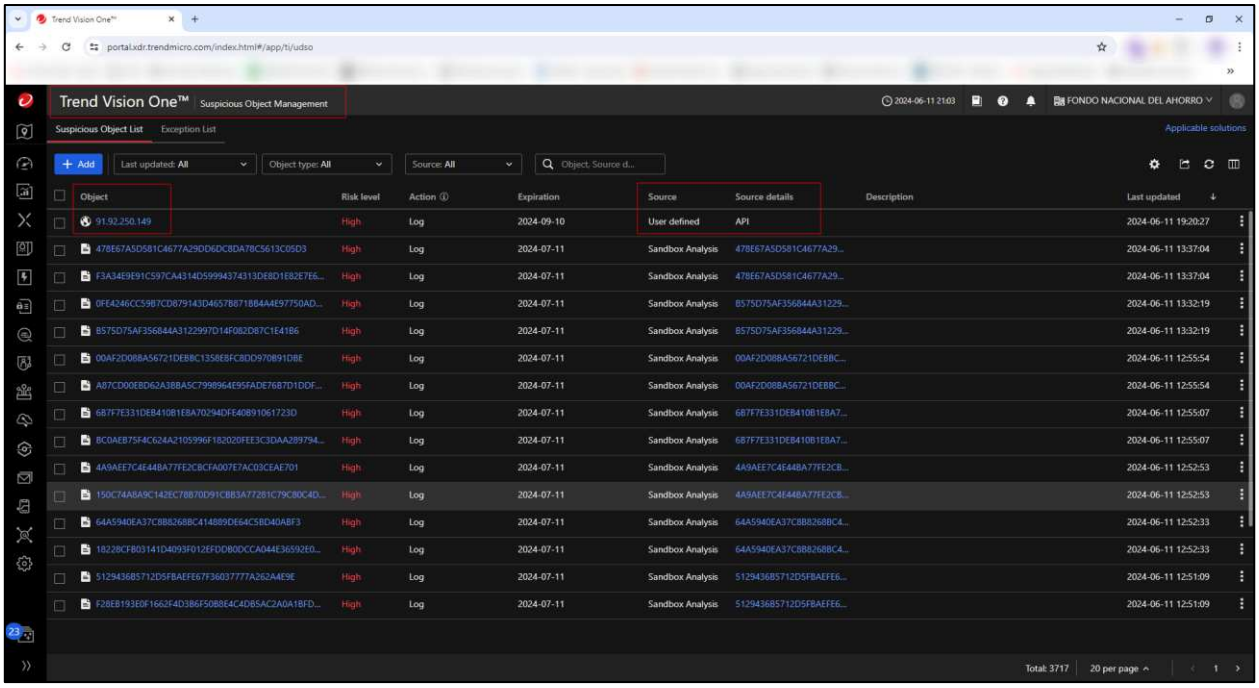


Ilustración 26 acción automática en tren micro visione one

11. REPORTE PANELES Y METRICAS

En este panel WEB generalmente muestra reportes Muestra el número total de incidentes, categorizados por estado (abiertos, en progreso, cerrados).

Gráficos de Tendencias, visualización de las tendencias de incidentes a lo largo del tiempo, permitiendo identificar picos y patrones.

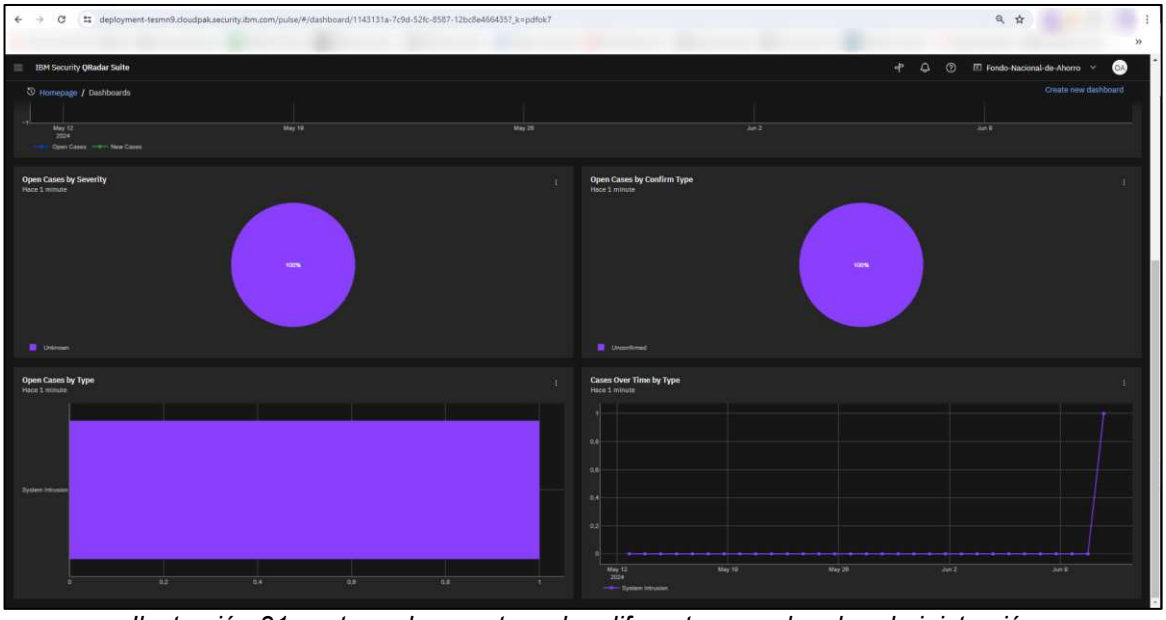


Ilustración 31 ventana de reportes y los diferentes paneles de administración

En esta imagen presentada a continuación se evidencia diferentes dashboard y reportes

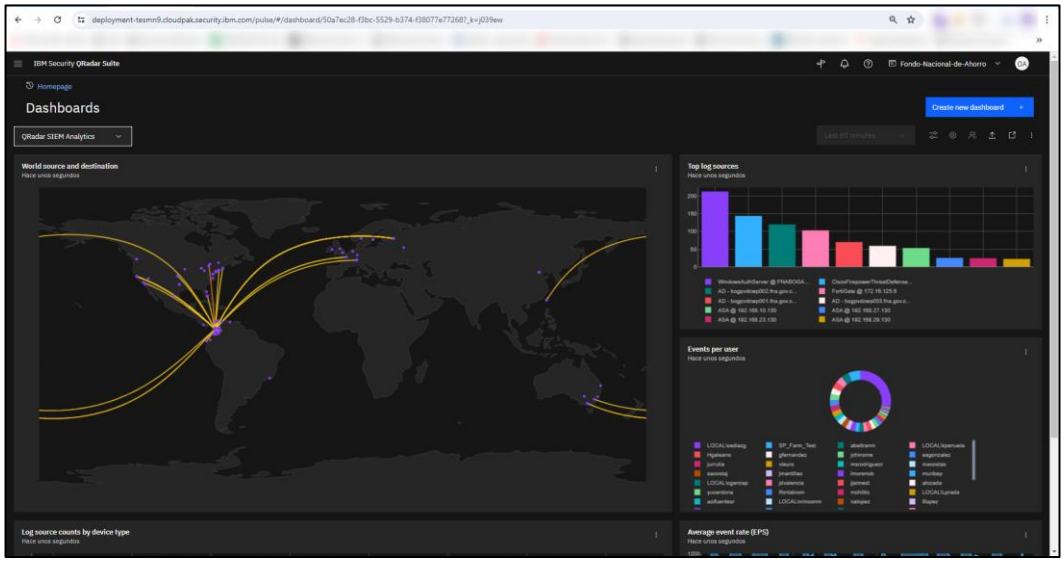


Ilustración 32 evidencia de reportes generados por SOAR

12. GESTION DE RED EDGE GATEWAY

El **EdgeGateway** es una máquina virtual, instalada en la **SONDA** por medio del hipervisor **VMWARE**, el hardware que compone la infraestructura referenciada como sonda es propiedad de **FNA** y administrada por parte del **CONSORCIO DE CIBERSEGURIDAD FNA** bajo el contrato **173-2023**, a continuación, se presentan las configuraciones de red del host virtual:

QRADAR EDGEGATEWAY

IP: **eth0** 172.16.132.34

Gateway: 172.16.132.8

Netmask: 255.255.255.0

DNS: 172.17.0.70 - 172.17.0.70

Hostname: apphost.localdomain

EVIDENCIA CONFIGURCION DE RED

```
appadmin@apphost:~
[appadmin@apphost ~]$
[appadmin@apphost ~]$
[appadmin@apphost ~]$ ifconfig
cni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.42.0.1  netmask 255.255.255.0  broadcast 10.42.0.255
        inet6 fe80::4c7:b4ff:feaa:3744  prefixlen 64  scopeid 0x20<link>
        ether 06:c7:b4:aa:37:44  txqueuelen 1000  (Ethernet)
        RX packets 25858583  bytes 5546033033 (5.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27891664  bytes 17879512640 (16.6 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.132.34  netmask 255.255.255.0  broadcast 172.16.132.255
        inet6 fe80::20c:29ff:feba:36fa  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ba:36:fa  txqueuelen 1000  (Ethernet)
        RX packets 9384950  bytes 1493472171 (1.3 GiB)
        RX errors 0  dropped 2440  overruns 0  frame 0
        TX packets 3855924  bytes 1597752903 (1.4 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ilustración 27 configuración de red

EVIDENCIA CONFIGURCION DNS

```
[appadmin@apphost ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 172.16.0.70
nameserver 172.16.0.71
nameserver 172.16.0.72
[appadmin@apphost ~]$
```

Ilustración 28 configuración DNS

EVIDENCIA CONFIGURCION HOSTNAME

```
[appadmin@apphost ~]$ hostname
apphost.localdomain
```

Ilustración 29 validación hostname

EVIDENCIA CONFIGURCION GATEWAY

```
[appadmin@apphost ~]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.132.8    0.0.0.0         UG    100    0        0 eth0
10.42.0.0       0.0.0.0         255.255.255.0   U     0      0        0 cni0
172.16.132.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
[appadmin@apphost ~]$
```

Ilustración 30 validación Gateway

13. COPIA DE SEGURIDAD Y RECUPERACIÓN

En un despliegue de IBM Cloud Pak for Security, específicamente IBM SOAR (Security Orchestration, Automation, and Response) en la nube de IBM, las copias de seguridad y la recuperación se garantizan mediante una serie de políticas y mecanismos implementados por IBM.

Respaldos Automatizados

IBM Cloud incluye servicios de respaldo automatizados para los datos almacenados en la nube. Estos respaldos se realizan periódicamente y se almacenan en ubicaciones seguras para asegurar que los datos puedan ser recuperados en caso de pérdida o corrupción.

Planes de Recuperación ante Desastres

IBM implementa planes de recuperación ante desastres (DRP, por sus siglas en inglés) que incluyen estrategias para la recuperación rápida y eficiente de servicios críticos. Estos planes están diseñados para minimizar el tiempo de inactividad y la pérdida de datos en caso de incidentes graves.

Redundancia y Replicación de Datos

Los datos en la nube de IBM se almacenan con redundancia, utilizando técnicas de replicación para asegurar que haya múltiples copias de los datos en diferentes ubicaciones geográficas. Esto protege los datos contra fallos de hardware y desastres locales.

Seguridad de los Datos en Reposo y en Tránsito

Los datos en la nube de IBM están protegidos mediante cifrado tanto en reposo como en tránsito. Esto asegura que los datos sean inaccesibles para personas no autorizadas durante el almacenamiento y la transmisión.

Monitoreo y Gestión Proactiva

IBM proporciona servicios de monitoreo y gestión proactiva para detectar y responder rápidamente a posibles problemas que puedan afectar la disponibilidad y la integridad de los datos. Esto incluye la supervisión de los sistemas de respaldo y la integridad de los datos respaldados.

Acceso Controlado y Auditado

El acceso a los sistemas de respaldo y recuperación está estrictamente controlado y auditado. Solo el personal autorizado tiene acceso a estos sistemas, y todas las acciones son registradas para asegurar la trazabilidad y el cumplimiento con las políticas de seguridad.

Pruebas Regulares de Recuperación

IBM realiza pruebas regulares de los procesos de recuperación de datos para asegurar que los planes de recuperación ante desastres sean efectivos y que los datos puedan ser restaurados de manera confiable y en tiempo hábil.

Implementación Específica para IBM SOAR

Para IBM SOAR en particular, estos mecanismos se integran en la infraestructura subyacente del IBM Cloud Pak for Security. Específicamente, se puede esperar:

Respaldo de Configuraciones y Datos de Incidentes: Los datos relacionados con incidentes, playbooks, configuraciones y otros activos críticos de SOAR son respaldados periódicamente.

Restauración de Servicios: En caso de fallo del sistema o pérdida de datos, los servicios de IBM SOAR pueden ser restaurados rápidamente para asegurar la continuidad de las operaciones de seguridad.

Soporte y Asistencia: IBM proporciona soporte técnico y asistencia para ayudar a los clientes a realizar recuperaciones de datos y resolver problemas relacionados con respaldos y restauraciones.

14. TOLERANCIA A FALLOS

EDGE GATEWAY:

En la infraestructura antes mencionada para desplieque de los VMware adicionalmente contamos con la tecnología vMotion es una tecnología desarrollada por VMware que permite la migración en tiempo real de máquinas virtuales (VMs) entre servidores físicos sin interrupciones perceptibles para los usuarios finales. Esta tecnología es parte fundamental de la estrategia de continuidad de errores en entornos virtualizados. A continuación, te proporciono información sobre cómo vMotion contribuye a la continuidad de errores en entornos virtualizados:

Migración en Tiempo Real: vMotion permite mover una VM de un servidor físico a otro mientras la VM sigue en ejecución y atendiendo las solicitudes de los usuarios, esto significa que si uno de los servidores físicos experimenta un fallo, las VMs que estaban en ese servidor pueden migrarse rápidamente a otro servidor operativo sin interrupciones perceptibles para los usuarios.

Resiliencia ante Fallos de Hardware: La migración instantánea de VMs a través de vMotion ayuda a garantizar la resiliencia ante fallos de hardware, si un servidor físico experimenta un problema de hardware, como un fallo en la CPU, la memoria o un componente de almacenamiento, las VMs que estaban alojadas en ese servidor pueden trasladarse automáticamente a otro servidor disponible.

15. INTEGRACION CON INTELIGENCIA DE AMENAZAS

Integrar IBM SOAR con IBM X-Force Red Vulnerability Management Services (VMS) permite a las organizaciones mejorar su capacidad de respuesta a las vulnerabilidades y amenazas de seguridad mediante la automatización y orquestación de procesos:

1. **Automatización del Ciclo de Vida de Vulnerabilidades:**
    - Identificación y priorización automática de vulnerabilidades.

- Creación automática de incidentes en SOAR cuando se descubren nuevas vulnerabilidades.

2. **Respuesta Eficiente:**
   - Uso de playbooks automatizados para responder a vulnerabilidades conocidas.
   - Coordinación de equipos de seguridad y TI para remediar vulnerabilidades.
3. **Visibilidad y Gestión Centralizada:**
   - Consolida datos de vulnerabilidades y respuestas en un único panel de control.
   - Monitoreo en tiempo real de las actividades de remediación.

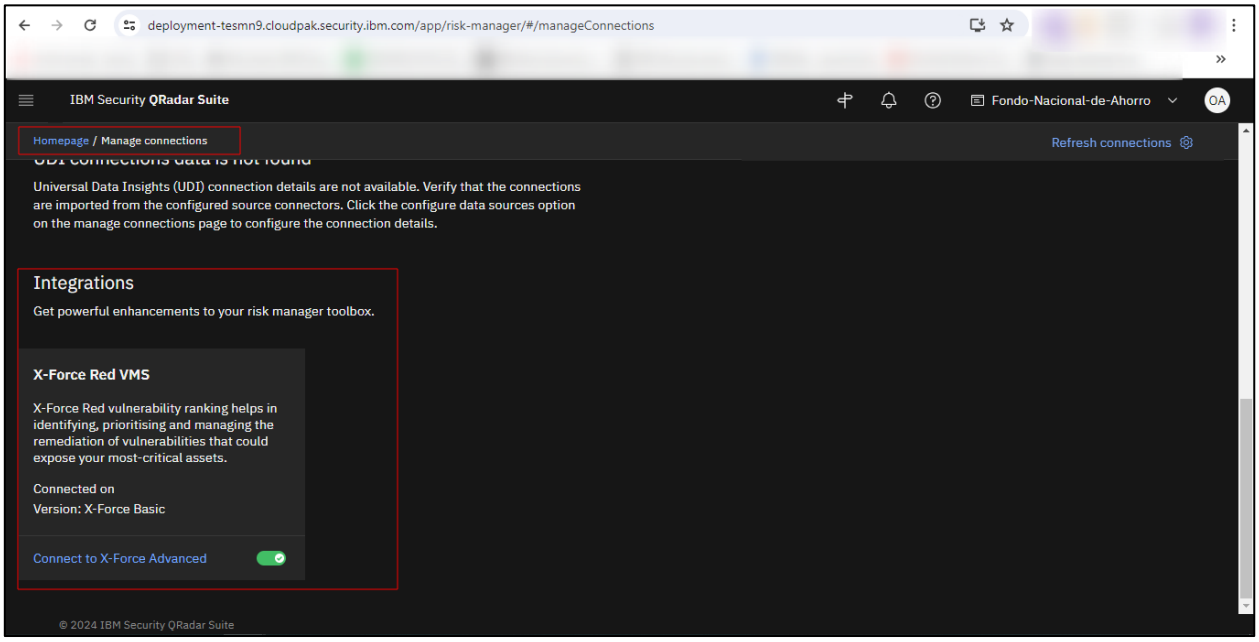


Ilustración 33 integración X-Force Red VMS

16. INTEGRACION CON TERCEROS

La integración de IBM SOAR (Security Orchestration, Automation, and Response) con fuentes de datos externas es esencial para mejorar la visibilidad, automatización y respuesta a incidentes de seguridad.

Visibilidad Ampliada:

- Obtener datos enriquecidos y contextuales desde diversas fuentes para una mejor comprensión de los incidentes.
- Mejorar la detección y análisis de amenazas mediante la correlación de datos.
- Respuesta Automatizada:

Activar respuestas automatizadas basadas en información en tiempo real de fuentes externas.
Reducir el tiempo de respuesta y aumentar la eficiencia operativa.

Análisis y Correlación:

Utilizar datos externos para correlacionar eventos y detectar patrones sospechosos.
Generar alertas más precisas y reducir los falsos positivos.

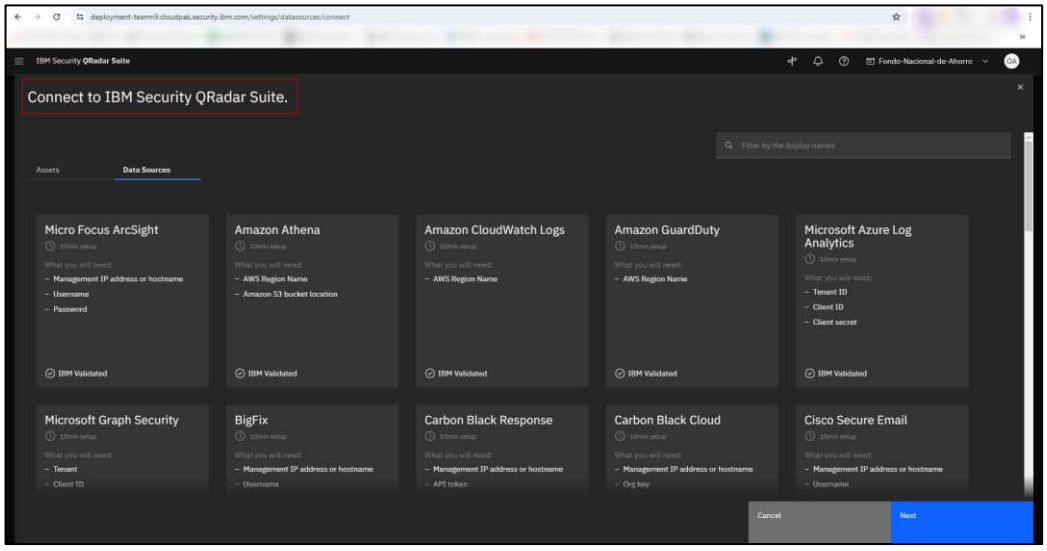


Ilustración 34 integración con terceros

17. NOTIFICACIONES

Integrar notificaciones por correo electrónico en IBM SOAR (Security Orchestration, Automation, and Response) permite a los equipos de seguridad mantenerse informados sobre los incidentes y eventos críticos en tiempo real. A continuación, se evidencia cómo configurar notificaciones por correo electrónico en IBM SOAR.

Beneficios de las Notificaciones por Correo Electrónico

1. **Alertas en Tiempo Real:**

- Recibir notificaciones inmediatas sobre nuevos incidentes, cambios en el estado de los incidentes, y acciones completadas.

2. **Mejora de la Comunicación:**
   - Mantener a todos los miembros del equipo informados y coordinados, mejorando la colaboración y la respuesta.

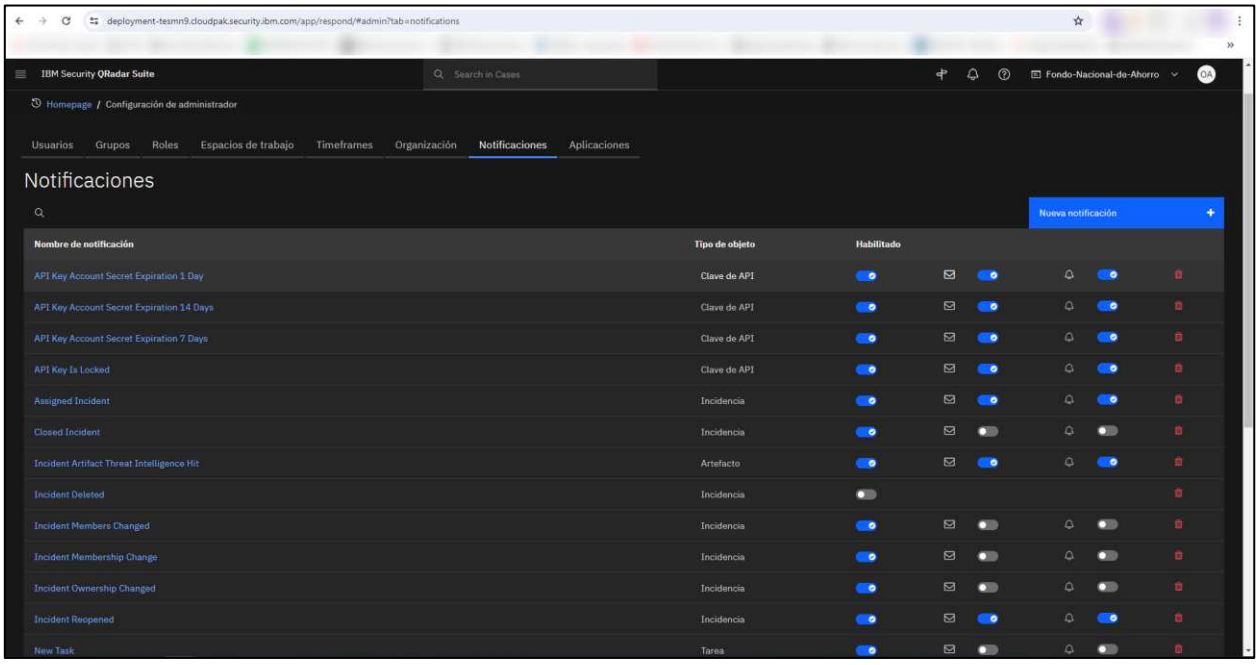


Ilustración 35 verificación de envió de E-mail

3. **Configuración Personalizada:**
   - Personalizar las notificaciones para diferentes tipos de incidentes y destinatarios según las necesidades específicas de la organización.

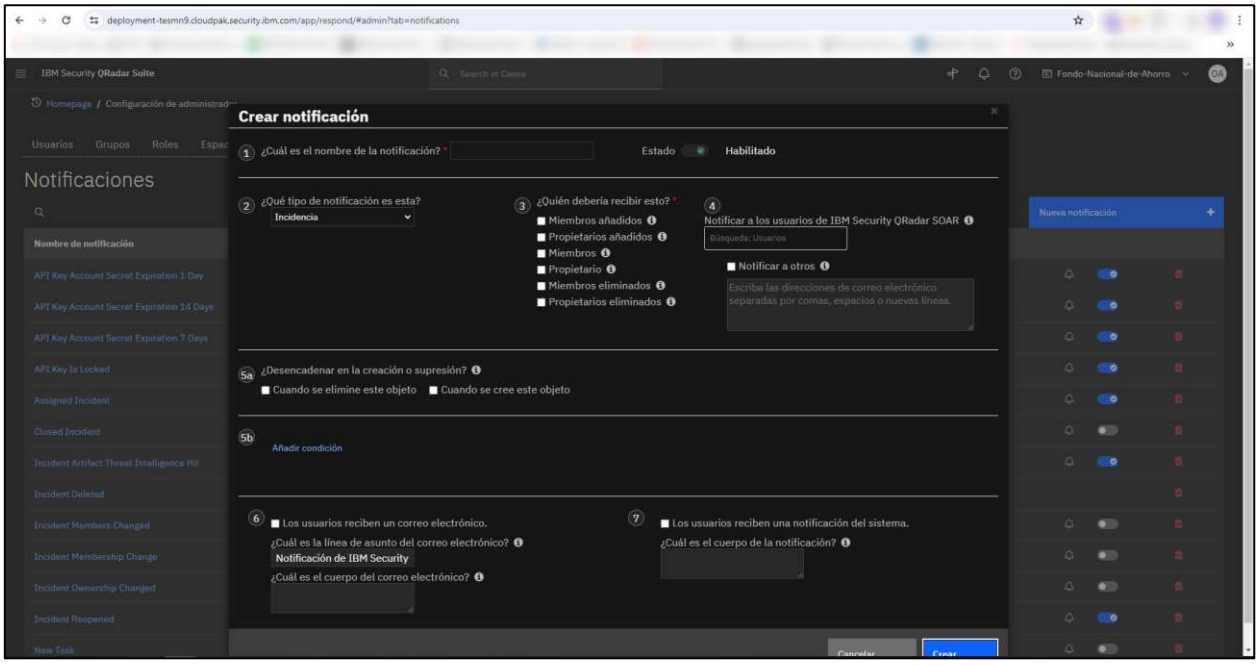


Ilustración 36 configuración notificaciones

18. GESTION USUARIOS

Creación de Usuarios

Para crear usuarios en IBM SOAR, se sigue un proceso estructurado que incluye la definición de los detalles del usuario y la asignación de roles adecuados. A continuación, se describe el proceso paso a paso:

Acceso a la Consola de Administración:

Inicie sesión en la consola de administración de IBM SOAR con una cuenta que tenga privilegios administrativos.

Navegación a la Sección de Usuarios:

Vaya a "Administración" y seleccione "Usuarios" o "Gestión de Usuarios" en el menú.

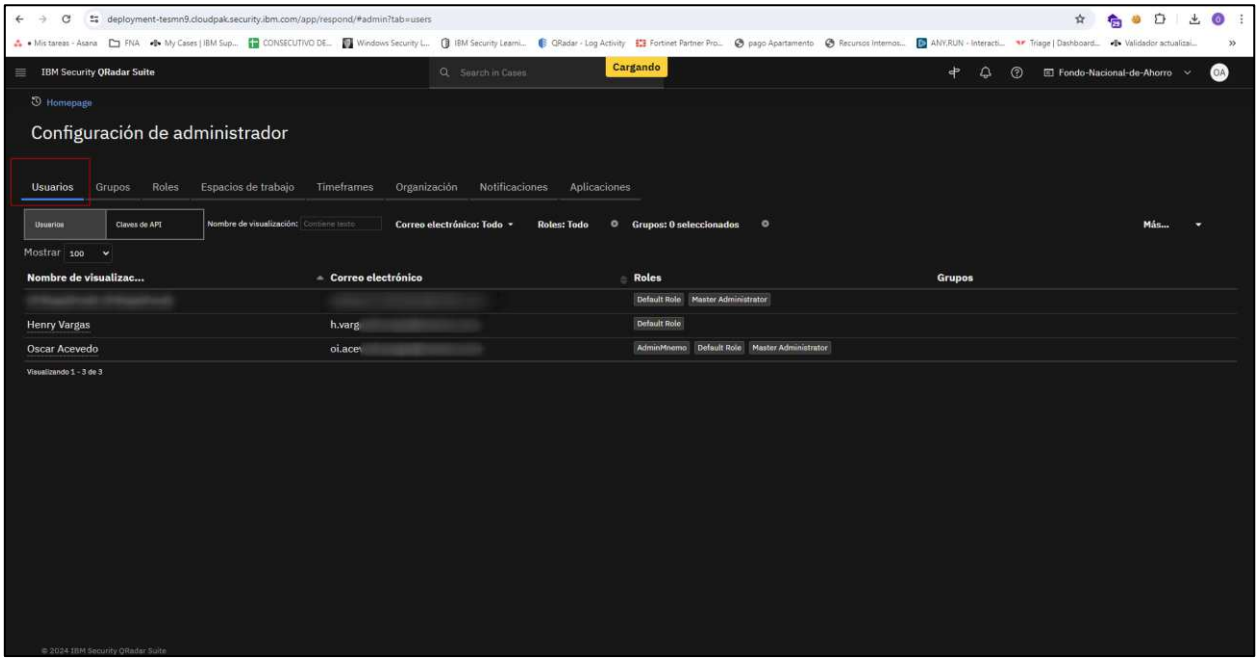


Ilustración 37 creación de usuarios

Asignación de Roles y Permisos

La asignación de roles y permisos es crucial para asegurar que los usuarios tengan acceso adecuado según sus responsabilidades. IBM SOAR utiliza roles predefinidos y permite la creación de roles personalizados.

Roles Predefinidos:

Administrador: Tiene acceso completo a todas las funciones y configuraciones del sistema.

Analista: Puede gestionar y responder a incidentes, pero con acceso limitado a configuraciones de administración.

Visor: Puede ver incidentes e informes, pero no realizar acciones sobre ellos.

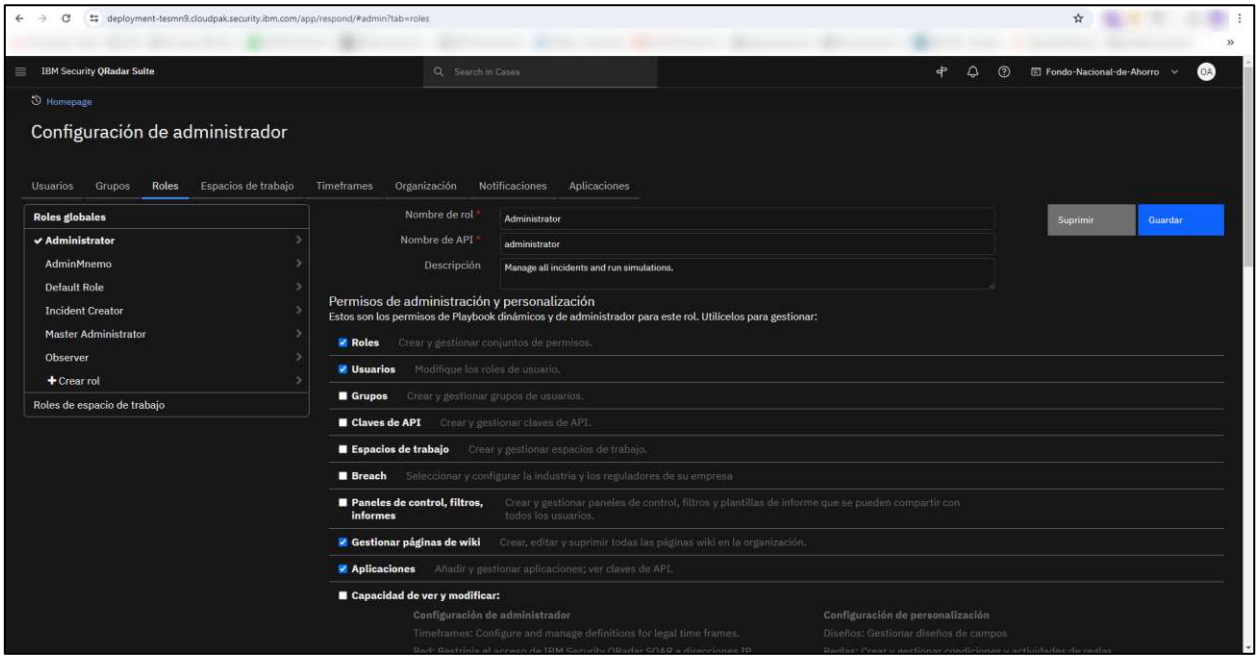


Ilustración 38 asignación de roles

CONCLUSION

Gestión de Usuarios:

- Crear usuarios y asignar roles específicos basados en sus responsabilidades.
- Implementar políticas de contraseñas robustas y autenticación multifactor para mejorar la seguridad.
- Realizar revisiones periódicas de accesos y permisos para asegurar que sigan siendo apropiados.

Integración con Fuentes de Datos Externas:

- Ampliar la visibilidad y mejorar la correlación de incidentes mediante la integración con sistemas de inteligencia de amenazas, SIEM, EDR, y otros.
- Automatizar la respuesta a incidentes con playbooks que utilizan datos en tiempo real de fuentes externas.

Notificaciones por Correo Electrónico:

- Configurar notificaciones para mantener a los equipos informados sobre incidentes y eventos críticos.
- Personalizar las plantillas de correo y las reglas de notificación para adaptarse a las necesidades específicas de la organización.

Mejores Prácticas:

- Aplicar el principio de menor privilegio al asignar roles y permisos.
- Proveer capacitación continua a los usuarios sobre políticas de seguridad y uso de IBM SOAR.
- Monitorear y auditar regularmente las actividades de los usuarios para detectar y mitigar posibles amenazas.

Índice

1. SOC
2. CTI
3. Threat Hunting
4. Laboratorio avanzado de malware
5. Infoblox
6. WAF - Fortiweb
7. Darktrace
8. Guardium
9. Verify
10. Monitoreo de marca
11. Seguridad ofensiva
12. Qualys
13. Fortify
14. Antimalware
15. Consultoría

Fuentes

42

Activas

Informe SOC

2024

Objetivo

En el presente informe están estipulados los parámetros más importantes asociados al servicio de monitoreo y servicio de correlación, así como las configuraciones realizadas sobre la plataforma de correlación por parte del equipo de SOC-CERT de Mnemo Colombia S.A.S., para el Fondo Nacional del ahorro

Objetivos específicos

- Resumen de eventos gestionados en el periodo correspondiente
- Mostrar los indicadores de reglas y carga operativa sobre la solución SIEM
- Estatus de desarrollos implementados para integración de fuentes no soportadas.
- Validación de oportunidades de mejora de acuerdo a los indicadores expuestos en el documento.
- Presentar conclusiones relevantes.

Alcance

Exponer los eventos identificados en el servicio de monitorización ejecutado por SOC-CERT de Mnemo Colombia durante el periodo comprendido entre el 22 de Abril y el 21 de Mayo de 2024 comprendiendo los siguientes temas

Los temas a tratar sobre este informe son:

•Descripción de fuentes de información

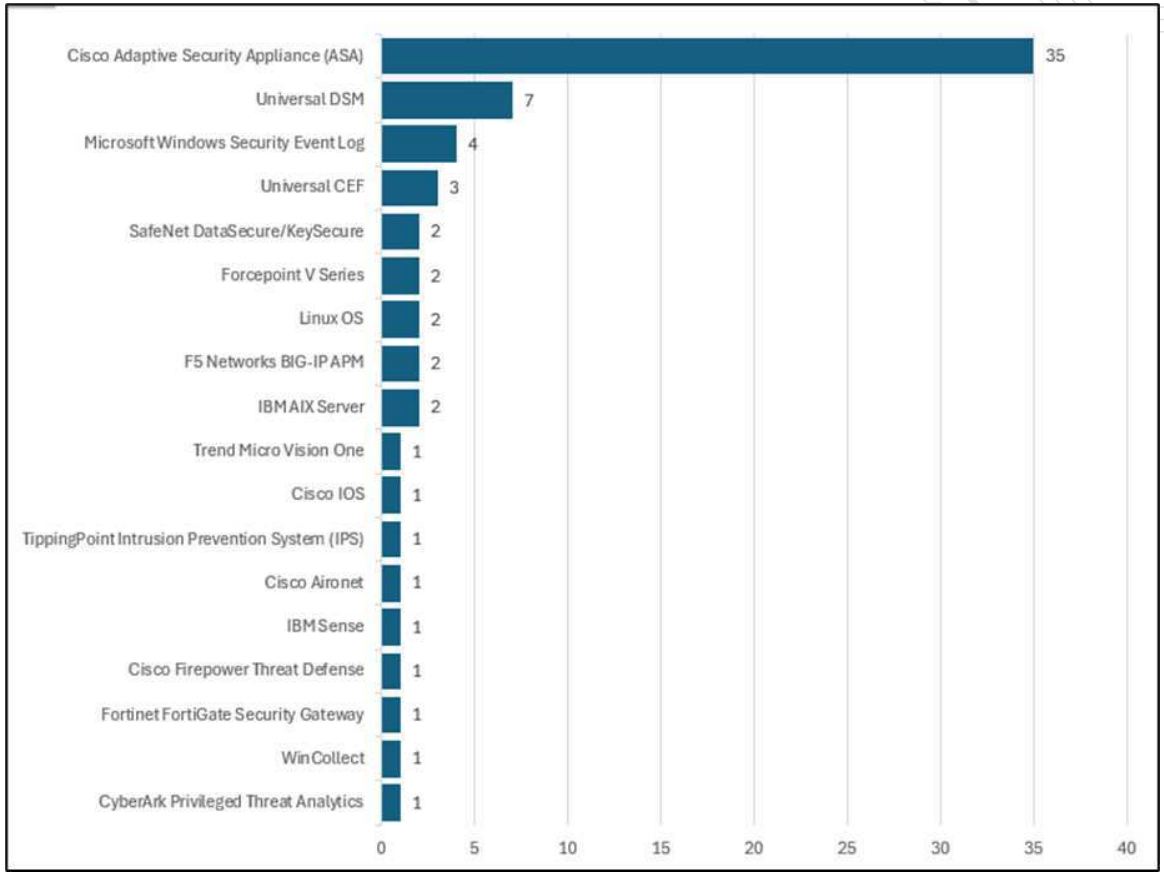
•Taxonomía definida y detalle de los eventos identificados.

•Recomendaciones y conclusiones

TIPOS DE FUENTES ESTÁNDAR

Fuentes de información

Durante el periodo se identificaron 68 fuentes las cuales se desglosan a continuación.



DESGLOSE FUENTES UNIVERSAL CEF Y DSM

En IBM Security QRadar, "Universal CEF" y "Universal DSM" son componentes que permiten la integración de fuentes de datos externas al sistema mediante el formato de registro común de eventos

Etiquetas de fila	Cuenta de Log Source Type	
Universal CEF	**3**	DESARROOLLOS
FNA_ DarkTrace	1	
Forcepoint DLP - 172.16.127.84	1	
InfoBlox 172.16.132.157	1	
Universal DSM	**7**	
FMC-AUDIT - 172.31.1.100	1	
FNA_Adminfo_DESARROLLO_172.16.132.105	1	
FNA_BO_DESARROLLO_172.16.132.105	1	
FNA_GOANYWHERE_APLICACION_172.16.132.105	1	
FNA_GOANYWHERE_HTTPS_172.16.132.105	1	
FNA_GOANYWHERE_SFT_172.16.132.105	1	
FNA_LOG_SAP_DESARROLLO_172.16.132.105	1	
Total general	**10**	

VALIDACIÓN DE FUENTES

A continuación se presentan una serie de fuentes las cuales en el momento NO se encuentran enviando eventos, estas fueron reportada y estamos pendientes de realizar la validación con los equipos respectivos

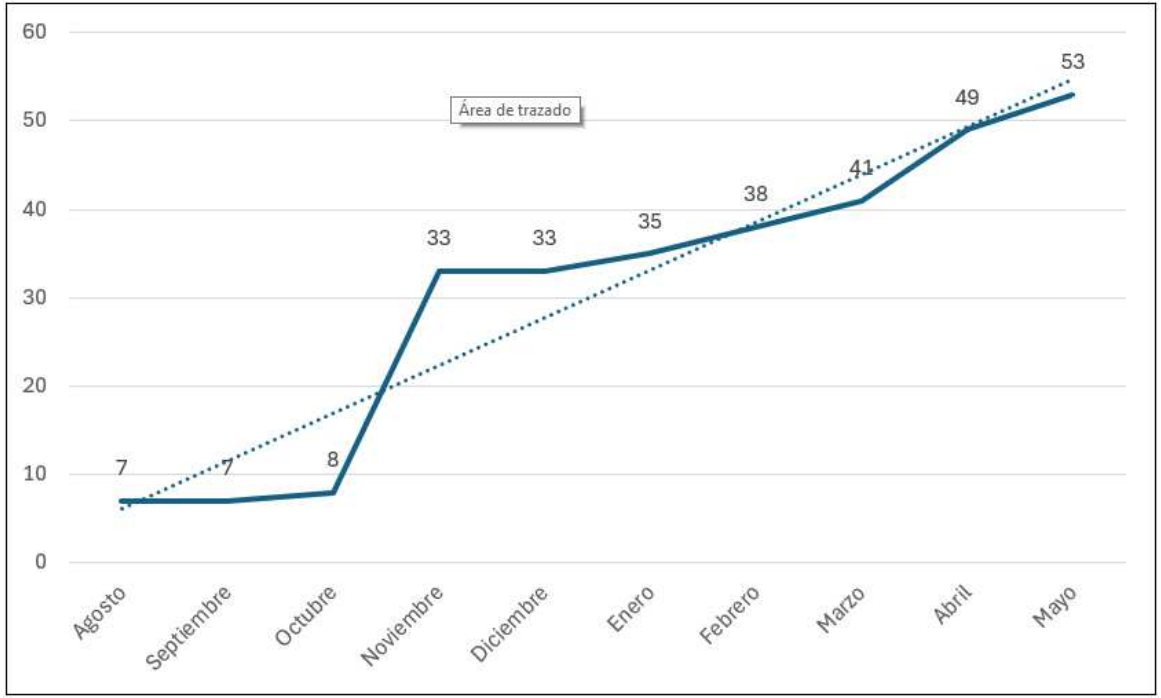
LogSource No envio de eventos		
ASA @ 192.168.13.130	Cisco Adaptive Security Appliance (ASA)	192.168.13.130
ASA @ 192.168.38.130	Cisco Adaptive Security Appliance (ASA)	192.168.38.130
ASA @ 192.168.31.130	Cisco Adaptive Security Appliance (ASA)	192.168.31.130
ASA @ 192.168.41.130	Cisco Adaptive Security Appliance (ASA)	192.168.41.130

CASOS DE USO

A continuación, se muestran un histórico de las actividades relevantes del servicio:

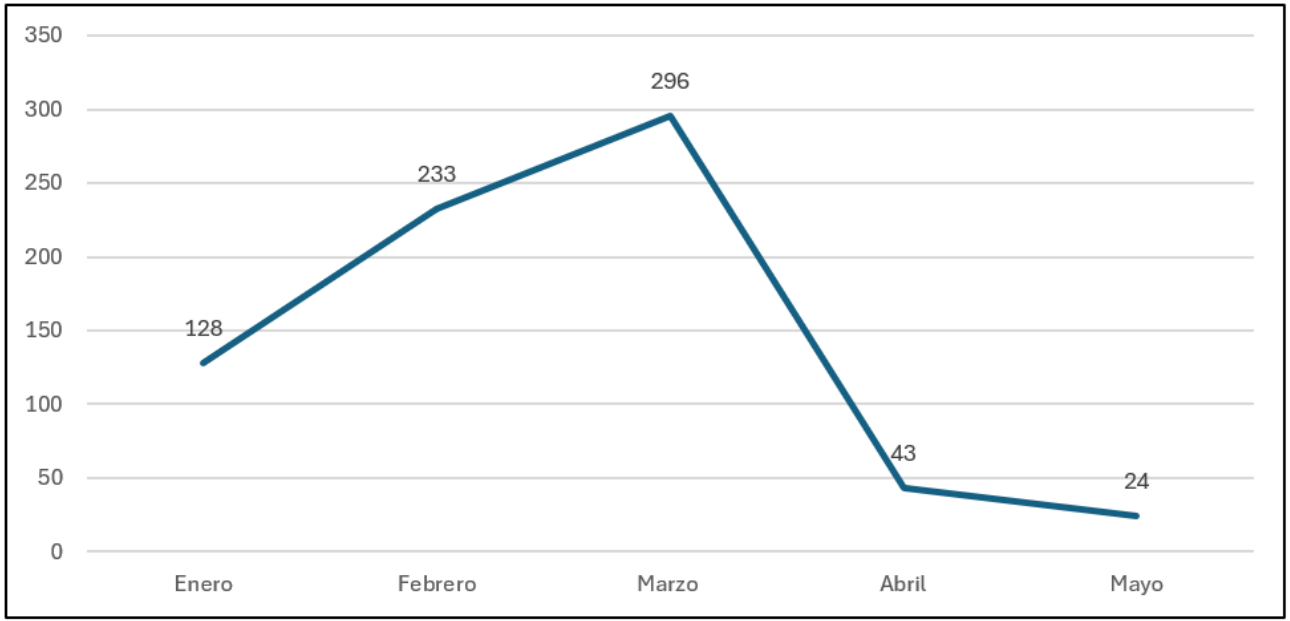
Para este periodo se realizó un incremento de 4 casos de uso

- FNA_Local L2L LDAP Server Scanner
- FNA_Suspicious Svchost Process
- FNA_Excessive Login Failures via RDP Connection
- FNA_Credential Dumping Activities Discovered



ALERTAMIENTO SOC

Para este periodo se identificó una disminución en el alertamiento con respecto al periodo anterior, debido a que se está realizando un proceso de hunting para descartar falsos positivos y así realizar el respectivo afinamiento de las herramientas de monitoreo.



Tareas de Gestión Plataforma SIEM

1 de Mayo de 2024

Integración de IPS: Se llevó a cabo la integración del sistema de prevención de intrusiones (IPS) en la plataforma Gradar para mejorar la capacidad de detección y respuesta ante posibles amenazas de seguridad en la red.

Creación de Casos de Uso:

FNA_Local L2L LDAP Server Scanner: Se diseñó un caso de uso para identificar y alertar sobre actividades sospechosas relacionadas con escaneos de servidores LDAP a nivel local.

FNA_Suspicious Svchost Process: Se creó un caso de uso específico para detectar procesos sospechosos de Svchost, que podrían indicar actividades maliciosas.

2 de Mayo de 2024

Creación de Casos de Uso:

FNA_Excessive Login Failures via RDP Connection: Se desarrolló un caso de uso para monitorizar e identificar fallos excesivos en intentos de inicio de sesión a través de conexiones RDP, lo cual podría ser indicativo de intentos de acceso no autorizados.

FNA_Credential Dumping Activities Discovered: Se estableció un caso de uso para detectar actividades relacionadas con el volcado de credenciales, una técnica comúnmente utilizada por atacantes para escalar privilegios dentro de una red.

9 de Mayo de 2024

Adición de Usuarios a Listas Blancas de DA: Se realizó la actualización de listas blancas en Directorio Activo (DA) para asegurar que usuarios legítimos no sean incorrectamente marcados como amenazas.

10 de Mayo de 2024

Seguimiento de Validación CyberArk: Se hizo un seguimiento para validar las integraciones y funcionalidades de CyberArk dentro de la infraestructura de seguridad.

Investigación Masiva de Bloqueo de Eventos: Se llevó a cabo una investigación exhaustiva para identificar y resolver problemas relacionados con el bloqueo masivo de eventos.

Validación de Fuentes de Log:

172.16.126.32 y 172.16.126.33 Se validaron las fuentes de log provenientes de estas direcciones IP para asegurar la correcta recolección y análisis de datos en QRadar.

Envío de Reporte: Se envió un reporte detallado sobre el bloqueo y la validación de bloqueo masivo de usuarios, asegurando que las medidas implementadas estén funcionando adecuadamente.

17 de Mayo de 2024

Seguimiento de Validación de Niveles de Auditoría en Dispositivos ASA: Se realizó un seguimiento para validar que los niveles de auditoría en dispositivos ASA cumplan con los niveles de auditoria requeridos para la monitorizacion.

Tareas de Gestión Plataforma SIEM

Sesión de Seguimiento de Integración de Firewalls: Se llevó a cabo una sesión para seguir el progreso de la integración de varios firewalls (BOGPFFWCP003, BOGPFFWCP004, BOGPFFWCP001, BOGPFFWCP002, BOGPFVPCP001, BOGPFVPCP002) en la infraestructura de seguridad.

21 de Mayo de 2024

Seguimiento de Permisos en AD: Se realizó un seguimiento de los permisos en Directorio Activo para garantizar que estén configurados adecuadamente y que no haya permisos excesivos o mal configurados que pudieran comprometer la seguridad de la red.

Monitoreo Continuo:

1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.
3. **Gestión de Reglas y Correlaciones:**
4. Revisar y actualizar regularmente las reglas de detección de amenazas y las correlaciones para adaptarse a las nuevas amenazas y vulnerabilidades.
5. Ajustar la sensibilidad de las reglas y correlaciones para reducir falsos positivos y mejorar la eficacia de la detección de amenazas.

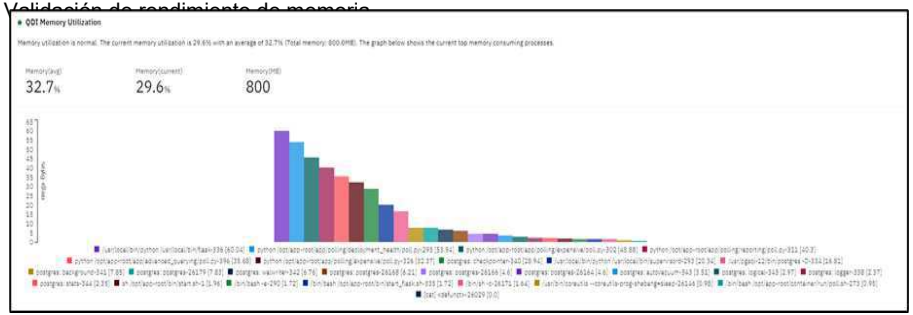
Seguimiento Healt metrics

Esta métrica evalúa la salud general del sistema QRadar, incluyendo la disponibilidad de hardware, la integridad del software y la capacidad de procesamiento. Se pueden monitorear indicadores como el uso de la CPU, la memoria, el almacenamiento y la conectividad de red para garantizar un funcionamiento óptimo del sistema.

Tareas de Gestión Plataforma SIEM

Consumo de rendimiento:

Validación de rendimiento de memoria



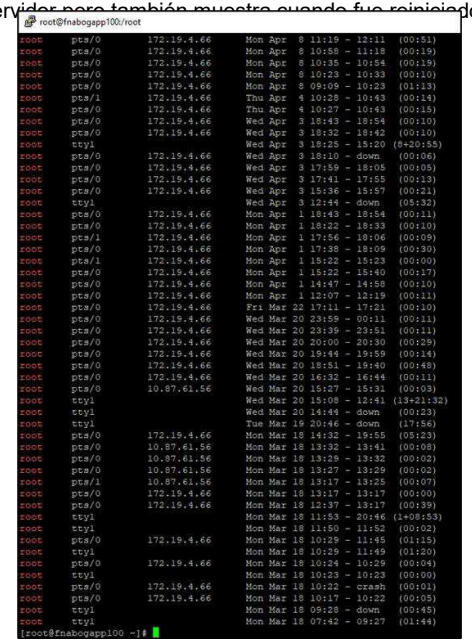
Seguimiento y estados de los diferentes servicios

Process Monitor - Last 7 days

Component	Total Outage(min)	Current Status
reporting_executor	2.02	Available
ecs-ec	1.00	Available
ecs-ec-ingress	2.99	Available
vis	1.99	Available
hostcontext	1.00	Available
assetprofiler	0.98	Available
tomcat	0.00	Available
ariel_proxy_server	0.00	Available
ecs-ep	0.00	Available
accumulator	0.00	Available
historical_correlation_server	0.00	Available
offline_forwarder	0.00	Available

Disponibilidad:

En esta vista se despliega una lista de los últimos usuarios que se han logueado al servidor pero también muestra cuando fue reiniciado el sistema:



```
root@fnabogapp100:/root
root     pts/0        172.19.4.66      Mon Apr  8 11:19 - 12:11  (00:51)
root     pts/0        172.19.4.66      Mon Apr  8 10:58 - 11:18  (00:19)
root     pts/0        172.19.4.66      Mon Apr  8 10:35 - 10:54  (00:19)
root     pts/0        172.19.4.66      Mon Apr  8 10:23 - 10:33  (00:10)
root     pts/0        172.19.4.66      Mon Apr  8 09:09 - 10:23  (01:13)
root     pts/1        172.19.4.66      Thu Apr  4 10:29 - 10:43  (00:14)
root     pts/0        172.19.4.66      Thu Apr  4 10:27 - 10:43  (00:15)
root     pts/0        172.19.4.66      Wed Apr  3 18:43 - 18:54  (00:10)
root     pts/0        172.19.4.66      Wed Apr  3 18:32 - 18:42  (00:10)
root     tty1                          Wed Apr  3 18:25 - 15:20  (8+20:55)
root     pts/0        172.19.4.66      Wed Apr  3 18:10 - down   (00:06)
root     pts/0        172.19.4.66      Wed Apr  3 17:59 - 18:05  (00:05)
root     pts/0        172.19.4.66      Wed Apr  3 17:41 - 17:55  (00:13)
root     pts/0        172.19.4.66      Wed Apr  3 15:36 - 15:57  (00:21)
root     tty1                          Wed Apr  3 12:44 - down   (05:32)
root     pts/0        172.19.4.66      Mon Apr  1 18:43 - 18:54  (00:11)
root     pts/0        172.19.4.66      Mon Apr  1 18:22 - 18:33  (00:10)
root     pts/1        172.19.4.66      Mon Apr  1 17:56 - 18:06  (00:09)
root     pts/0        172.19.4.66      Mon Apr  1 17:38 - 18:09  (00:30)
root     pts/1        172.19.4.66      Mon Apr  1 15:22 - 15:23  (00:00)
root     pts/0        172.19.4.66      Mon Apr  1 15:22 - 15:40  (00:17)
root     pts/0        172.19.4.66      Mon Apr  1 14:47 - 14:58  (00:10)
root     pts/0        172.19.4.66      Mon Apr  1 12:07 - 12:19  (00:11)
root     pts/0        172.19.4.66      Fri Mar 22 17:11 - 17:21  (00:10)
root     pts/0        172.19.4.66      Wed Mar 20 23:59 - 00:11  (00:11)
root     pts/0        172.19.4.66      Wed Mar 20 23:39 - 23:51  (00:11)
root     pts/0        172.19.4.66      Wed Mar 20 20:00 - 20:30  (00:29)
root     pts/0        172.19.4.66      Wed Mar 20 19:44 - 19:59  (00:14)
root     pts/0        172.19.4.66      Wed Mar 20 18:51 - 19:40  (00:48)
root     pts/0        172.19.4.66      Wed Mar 20 16:32 - 16:44  (00:11)
root     pts/0        10.87.61.56      Wed Mar 20 15:27 - 15:31  (00:03)
root     tty1                          Wed Mar 20 15:08 - 12:41  (13+21:32)
root     tty1                          Wed Mar 20 14:44 - down   (00:23)
root     tty1                          Tue Mar 19 20:46 - down   (17:56)
root     pts/0        172.19.4.66      Mon Mar 18 14:32 - 19:55  (05:23)
root     pts/0        10.87.61.56      Mon Mar 18 13:32 - 13:41  (00:08)
root     pts/0        10.87.61.56      Mon Mar 18 13:29 - 13:32  (00:02)
root     pts/0        10.87.61.56      Mon Mar 18 13:27 - 13:29  (00:02)
root     pts/1        10.87.61.56      Mon Mar 18 13:17 - 13:25  (00:07)
root     pts/0        172.19.4.66      Mon Mar 18 13:17 - 13:17  (00:00)
root     pts/0        172.19.4.66      Mon Mar 18 12:37 - 13:17  (00:39)
root     tty1                          Mon Mar 18 11:53 - 20:46  (1+08:53)
root     tty1                          Mon Mar 18 11:50 - 11:52  (00:02)
root     pts/0        172.19.4.66      Mon Mar 18 10:29 - 11:45  (01:15)
root     tty1                          Mon Mar 18 10:29 - 11:49  (01:20)
root     pts/0        172.19.4.66      Mon Mar 18 10:24 - 10:29  (00:04)
root     tty1                          Mon Mar 18 10:23 - 10:23  (00:00)
root     pts/0        172.19.4.66      Mon Mar 18 10:22 - crash  (00:01)
root     pts/0        172.19.4.66      Mon Mar 18 10:17 - 10:22  (00:05)
root     tty1                          Mon Mar 18 09:28 - down   (00:45)
root     tty1                          Mon Mar 18 07:42 - 09:27  (01:44)
[root@fnabogapp100 ~]#
```

54
Alertas Preventivas

44
Alertas Tempranas

25.613
IoC reportados

1994
Amenazas identificadas

14
Actores de amenazas identificados

Informe CTI

2024

Objetivo

Describir las tareas ejecutadas por el equipo de Cyber Threat Intelligence de Mnemo con relación al Fondo Nacional del Ahorro.

Objetivos específicos

- Resumen de investigaciones realizadas.
- Resumen de actividades.

Alcance

Los temas a tratar sobre este informe son:

- Resumen de investigaciones.
- Actividades realizadas.
- Recomendaciones y conclusiones.

Resumen de investigaciones

En el periodo evaluado se realizaron un total de 34 investigaciones, cada una de ellas se convirtió en una **alerta preventiva** que fue compartida vía correo electrónico y eventos en MISP.

Número de alertas

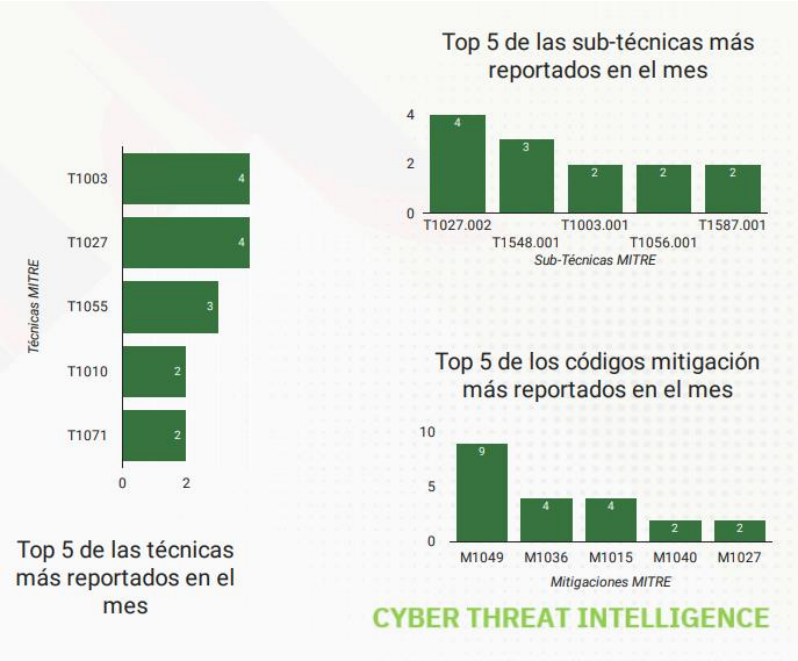
34

Alertas y eventos MISP reportados

ALERTAS REPORTADAS 14

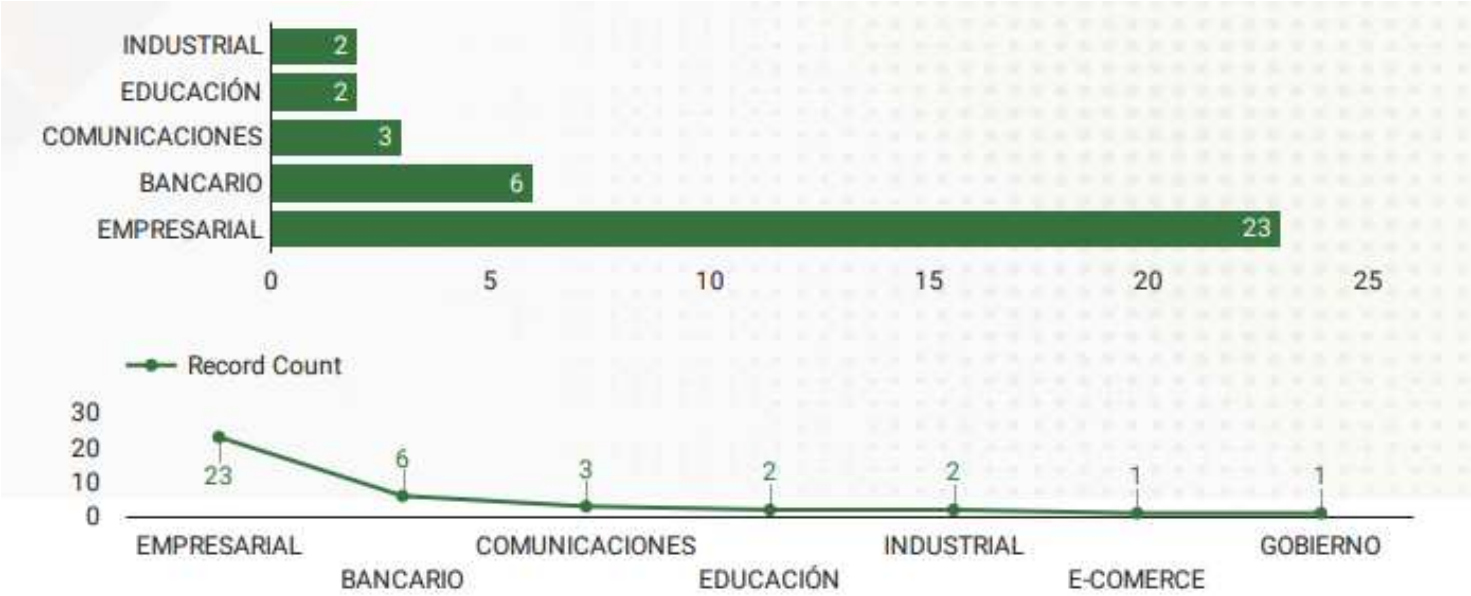
En el periodo evaluado se generaron 14 **alertas tempranas,** cada una de ellas fue compartida vía correo electrónico.

Mitre Att&CK en la investigación de CTI



En los gráficos a la izquierda se pueden observar las técnicas y subtécnicas (framework de referencia: MITRE ATT&CK) más identificadas durante el periodo analizado, además, también se pueden observar las mitigaciones relacionadas con dichas técnicas.

Industria objetivo de cibercriminales



En este gráfico se pueden observar los sectores de la industria que fueron afectados por las amenazas investigadas durante el periodo informado.

Actividades realizadas

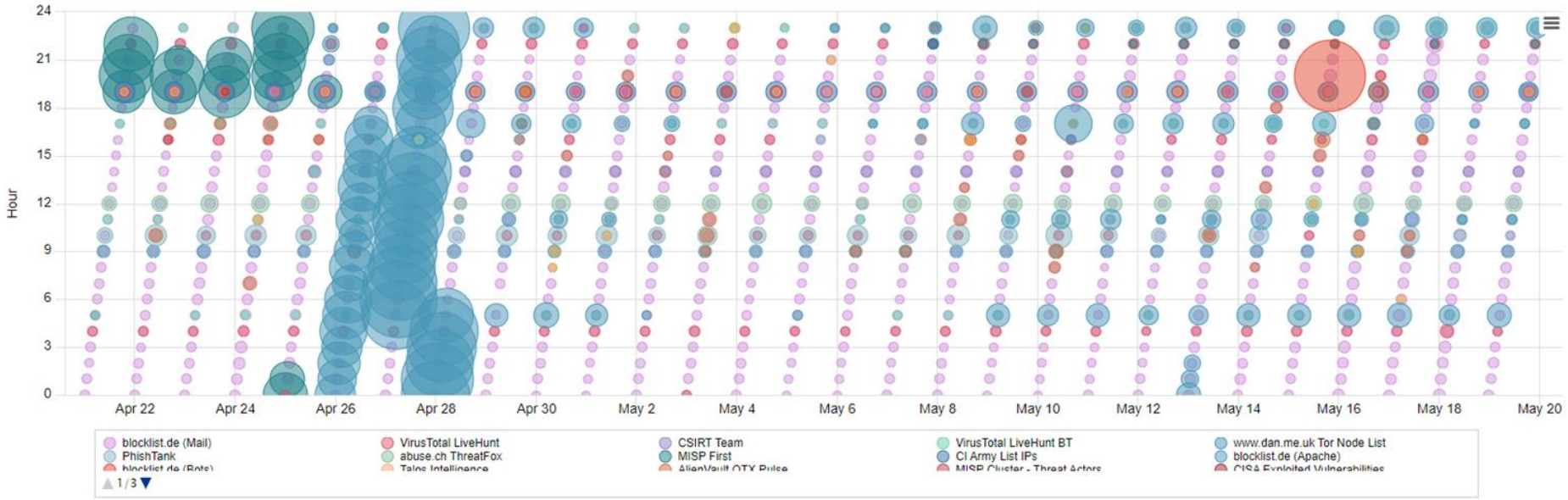
- Todas las investigaciones realizadas por el equipo de CTI se han compartido con el cliente vía correo electrónico.
- Se llevó a cabo un monitoreo constante de las actividades de diversos grupos y amenazas con el objetivo de investigar y profundizar en aquellas que pudieran tener un mayor impacto en los clientes de Mnemo.
- Se han compartido los indicadores de compromiso correspondientes a las investigaciones realizadas sobre alertas preventivas de amenazas que afectan la región y los sectores empresariales de interés.

Recomendaciones y conclusiones

- Durante el periodo reportado, el servicio de Cyber Threat Intelligence realizó un análisis exhaustivo de las tendencias y patrones de amenazas emergentes en el panorama cibernético global. Esto incluyó la identificación de nuevas variantes de malware, técnicas de ataque en evolución y vectores de amenazas más comunes.
- Es recomendado ajustar todas las herramientas de seguridad para permitir la ingesta de indicadores de compromiso de manera automatizada con los indicadores compartidos por Mnemo durante las investigaciones realizadas a las distintas amenazas que afectan tanto al sector como a la región.

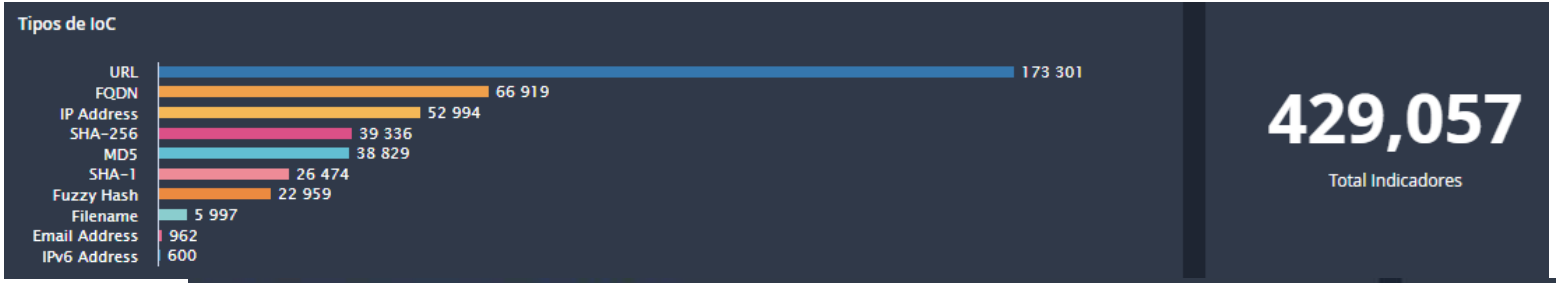
Resumen de objetos obtenidos - TIP

En la siguiente imagen se relacionan las fuentes de información y un resumen de los indicadores de compromiso y eventos obtenidos en las fechas reportadas.



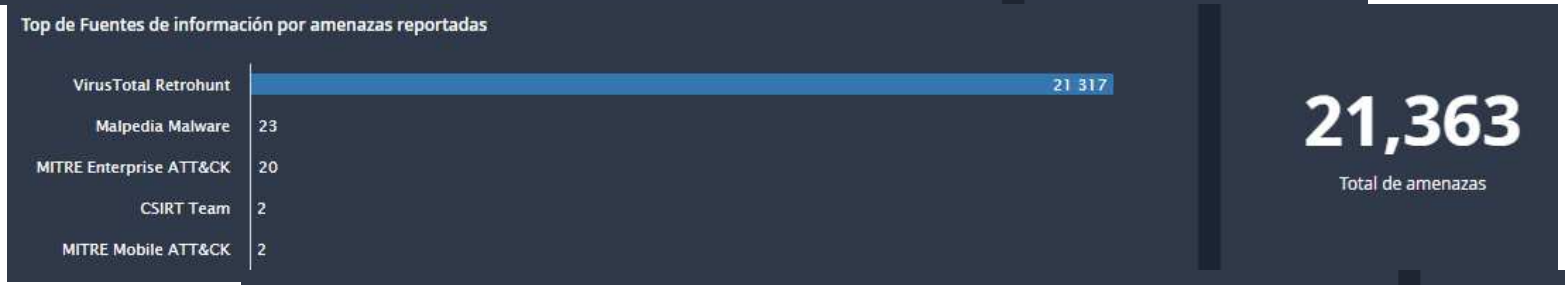
Resumen de objetos obtenidos – TIP

A continuación, se observa un resumen de los objetos obtenidos en la herramienta TIP de la organización.



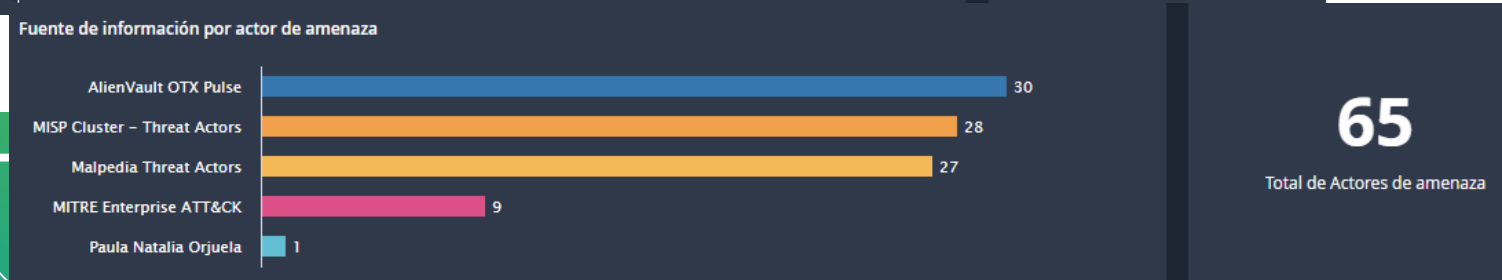
429,057

Total Indicadores



21,363

Total de amenazas



65

Total de Actores de amenaza

Actividades realizadas

- Se realizaron ajustes en las fuentes de datos de Threat Intelligence que funcionan como ingestores de indicadores de compromiso en la plataforma TIP, con el fin de mejorar tanto la confiabilidad y utilidad de la información recopilada como la actualización de los indicadores obtenidos.
- Se solucionan problemas con integraciones de fuentes de datos que no se entregan con el formato correcto generando inconvenientes de sincronización.

Indicators (429,057)

Manage Columns

QUICK FILTERS Type Status Score Expiration

VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	EXPIRATION DATE	TAGS	SOURCES
d507974c89556eadcd184aef49eda38cfa88e66e	SHA-1	20/05/2024 05:38pm UTC	20/05/2024 05:38pm UTC	Active			VirusTotal LiveHunt BT
d03f1525c6d1f9c0e74d38a2f55f189b50530ea0	SHA-1	20/05/2024 05:38pm UTC	20/05/2024 05:38pm UTC	Active			VirusTotal LiveHunt BT
701df48171ac3a3ecadf1f54baafd6abe05d506f	SHA-1	20/05/2024 05:38pm UTC	20/05/2024 05:38pm UTC	Active			VirusTotal LiveHunt BT
3e98c98bf7d697b054e93b7c8321257b798ebbd6	SHA-1	20/05/2024 05:38pm UTC	20/05/2024 05:38pm UTC	Active			VirusTotal LiveHunt BT
170ea226a1a2ad163b9061c2896213901f039d41	SHA-1	20/05/2024 05:38pm UTC	20/05/2024 05:38pm UTC	Active			VirusTotal LiveHunt BT
78.47.33.18	IP Address	20/05/2024 05:36pm UTC	20/05/2024 05:36pm UTC	Active	20/06/2024 12:00am UTC		blocklist.de (Mail)
66.220.155.147	IP Address	20/05/2024 05:36pm UTC	20/05/2024 05:36pm UTC	Active	20/06/2024 12:00am UTC		blocklist.de (Mail)
60.174.30.232	IP Address	20/05/2024 05:36pm UTC	20/05/2024 05:36pm UTC	Active	20/06/2024 12:00am UTC		blocklist.de (Mail)

Recomendaciones y conclusiones

- Han sido incorporadas nuevas fuentes de información a la plataforma de inteligencia de amenazas, suministrando indicadores de compromiso actualizados para asegurar que las herramientas de defensa estén al corriente frente a los nuevos artefactos de amenazas que surgen.

- Durante el período observado, se ha notado un aumento considerable en la cantidad de URLs maliciosas provenientes de la ingestión de indicadores de compromiso de diversas fuentes de información. Basándonos en esta información, se recomienda implementar políticas de control de navegación rigurosas para salvaguardar la infraestructura de la compañía contra visitas, ya sean intencionadas o no, a este tipo de sitios web.

Informe Threat Hunting

2024

02

Reglas a nivel de comportamiento

01

Análisis de amenazas en profundidad y focalizado

Objetivo

Indicar las actividades realizadas por el equipo de Cyber Threat Intelligence de Mnemo para el Fondo Nacional del Ahorro en el servicio de Threat Hunting.

Objetivos específicos

- Generar un resumen de las reglas SIGMA compartidas por el equipo de CTI para el Fondo Nacional del Ahorro
- Resumen de actividades realizadas durante el periodo reportado.

Alcance

Los temas a tratar sobre este informe son:

- Resumen de investigaciones.
- Actividades realizadas.
- Recomendaciones y conclusiones.

Resumen de reglas compartidas

File_Decoded_From_Base64/Hex_Via_Certutil

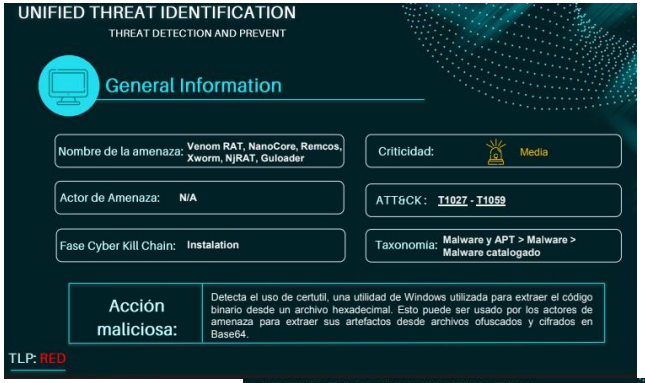
- El equipo de CTI de Mnemo ha identificado un comportamiento utilizado por los actores de amenaza en el que utilizan el software legítimo de Windows CertUtil.exe para decodificar binarios desde un string en Base64 para posteriormente extraer el código hexadecimal y por último un binario ejecutable y malicioso. La regla sigma mencionada detecta este comportamiento.

Suspicious_Extrac32_Copy_Powershell_File

- Durante la investigación realizada a una amenaza que distribuye familias de RAT a través de archivos cifrados con ScrubCrypt, se detectó un comportamiento de abuso de PowerShell, copiando su ejecutable original a una ruta usada por los actores de amenaza con el software legítimo de Windows “Extract32.exe”. Este comportamiento es detectado a través de la aplicación de la regla Sigma.

Actividades realizadas

- Durante el periodo reportado, se generó un producto Threat Focus Report sobre la técnica T1037.001 usada por los actores de amenaza para generar persistencia en los equipos infectados a través de scripts de inicio de sesión.
- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se crearon 2 reglas Sigma en la que se identifican los comportamientos de persistencia y ejecución.
- Para la primera regla sigma compartida, se detectó que RisePro agrega entradas a la carpeta de inicio de Windows, permitiendo que la amenaza se ejecute cada que un usuario inicia sesión.
- Para la segunda regla sigma, se identificó que el troyano bancario Zusy abusa de los intérpretes de comandos y scripts para llevar a cabo sus acciones maliciosas.



Recomendaciones y conclusiones

```yaml
title: File Decoded From Base64/Hex Via Certutil.EXE
id: cc9cbe82-7bc0-4ef5-bc23-bbfb83947be7
status: experimental
description: Detects the execution of certutil with either the "decode" or "decodehex" flags to decode ba
references:
    - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
    - https://learn.microsoft.com/en-us/archive/blogs/pki/basic-crl-checking-with-certutil
    - https://www.fortinet.com/blog/threat-research/scrubcrypt-deploys-venomrat-with-arsenal-of-plugins

author: Cyber Threat Intelligence MNEMO
date: 2024/04/30
Add Tag
tags:
    - attack.defense_evasion
    - attack.t1027
    - attack.execution
    - attack.t1059
logsource:
    category: process_creation
    product: windows
Look Up
detection:
    selection_i
      - Image|e
      - Origina
    selection_c
      CommandLi
        # Dec
        - '-d
```

```yaml
title: File Decoded From Base64/Hex Via Certutil.EXE
id: cc9cbe82-7bc0-4ef5-bc23-bbfb83947be7
status: experimental
description: Detects the execution of certutil with either the "decode" or "decodehex" flags to decode ba
references:
    - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
    - https://learn.microsoft.com/en-us/archive/blogs/pki/basic-crl-checking-with-certutil
    - https://www.fortinet.com/blog/threat-research/scrubcrypt-deploys-venomrat-with-arsenal-of-plugins

author: Cyber Threat Intelligence MNEMO
date: 2024/04/30
Add Tag
tags:
    - attack.defense_evasion
    - attack.t1027
    - attack.execution
    - attack.t1059
logsource:
    category: process_creation
    product: windows
Look Up
detection:
    selection_img:
      - Image|endswith: '\.exe'
      - OriginalFileName: '.exe'
    selection_cli:
      CommandLine|contains:
        # Decode Base64
        - '-decode '
```

- El equipo de Threat Intelligence realiza un análisis continuo de diversas amenazas con el objetivo de identificar patrones de comportamiento significativos. Esta información se utiliza para crear reglas SIGMA, las cuales simplifican tanto la detección de amenazas como el análisis preventivo de eventos de seguridad. Estas reglas permiten identificar eficazmente estos patrones de comportamiento, lo que facilita la identificación temprana de posibles amenazas.
- Se recomienda agregar las reglas SIGMA generadas a las plataformas de (SIEM) de la empresa. Esto permitirá detectar activamente las posibles amenazas que puedan estar ocultas en la infraestructura tecnológica, proporcionando una capa adicional de seguridad y permitiendo una respuesta rápida y eficiente ante posibles incidentes de seguridad.

Informe Laboratorio avanzado de malware

2024

38

Muestras sospechosas analizadas

35

Muestras confirmadas con algún tipo de malware

Objetivo

Demostrar las capacidades de uso del **Laboratorio Avanzado de Malware** y su uso durante el periodo informado.

Objetivos específicos

- Indicar las capacidades de análisis del que dispone el laboratorio avanzado de malware.
- Brindar un panorama de las tácticas y técnicas más utilizadas por los cibercriminales.
- Detectar las categorías de malware más comunes, con el fin de mejorar la defensa contra estas en las herramientas de seguridad.

Alcance

Los temas a tratar en este informe son:

• Capacidades del laboratorio de malware.

• Dar una visión de las muestras que continuamente se analizan durante el ejercicio de Threat Hunting.

Resumen de análisis de muestras sospechosas

Durante el período informado, el laboratorio de malware ha analizado 38 muestras, de las cuales 35 fueron encontradas con algún tipo de malware activo. La información obtenida de las muestras identificadas se utiliza para desarrollar reglas Yara que permiten detectar los artefactos de manera efectiva.

Además, permite mantener una estadística de las amenazas más prevalentes, lo que ayuda a desarrollar un panorama de los posibles ataques prevalentes en la región y en la industria.

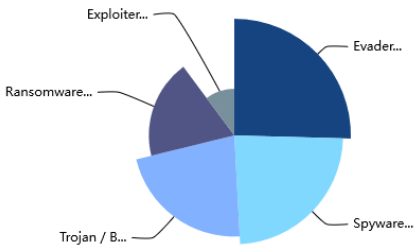
Malware

35 | 2125

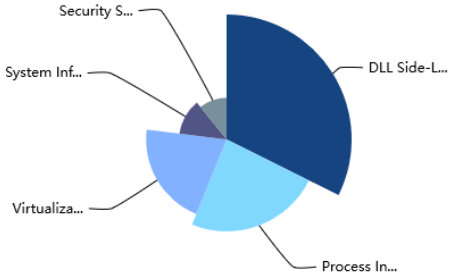
Muestras analizadas

38 | 2377

Top 5 Categorías

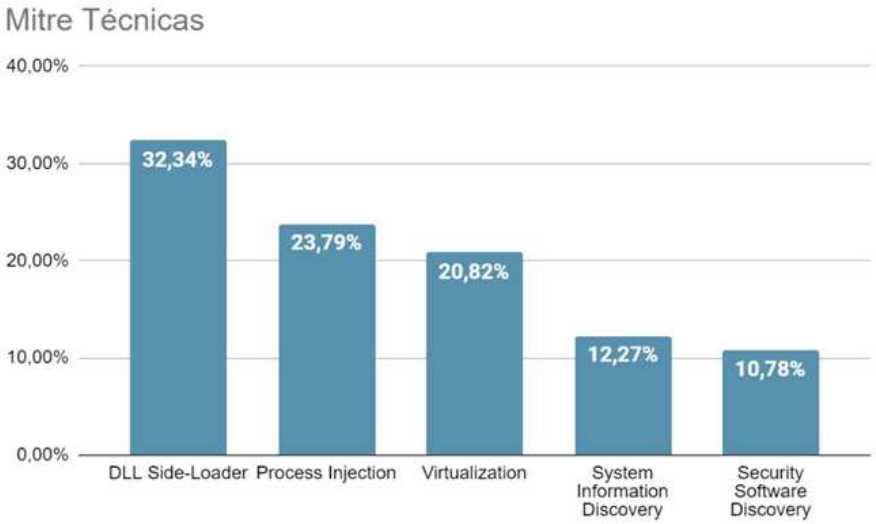


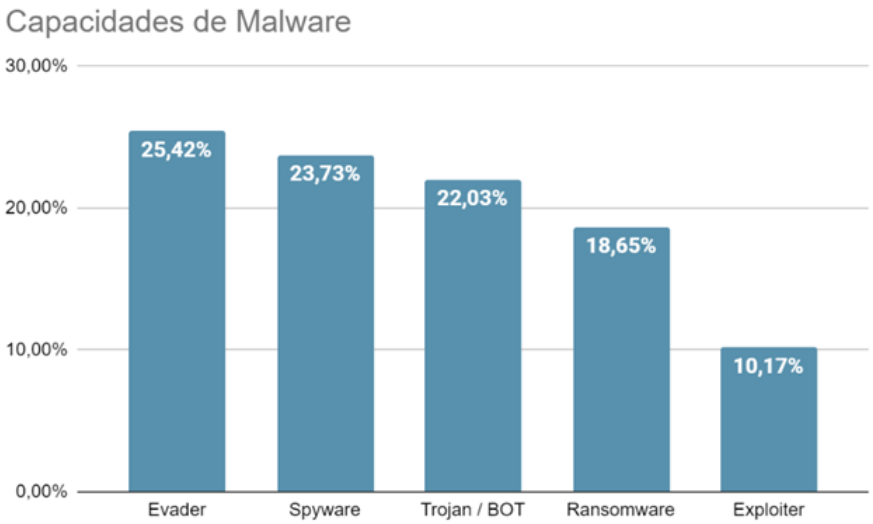
Top 5 MITRE Técnicas



Técnicas más utilizadas y categorías de malware más detectadas

Se muestran a continuación el top 5 de técnicas Mitre descubiertas en las muestras analizadas, así como el top 5 de las capacidades de malware descubiertas durante los análisis del periodo informado.





Tácticas y técnicas utilizadas

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact	Resource Development	Reconnaissance
Valid Accounts	Execution through API	DLL Side-Loading	[redacted]	[redacted]	Input Capture	[redacted]		Archive Collected Data		[redacted]			System Shutdown/ Reboot	Scripting	
	Windows Management Instrumentation	Scripting	DLL Side-Loading	DLL Side-Loading	Credential Dumping	Security Software Discovery		Clipboard Data		Standard Application Layer Protocol			Defacement		
	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Obfuscated Files or Information	Credentials in Registry	Virtualization/ Sandbox Evasion		Input Capture		Standard Non-Application Layer Protocol					
	PowerShell	Valid Accounts	Registry Run Keys / Startup Folder	Virtualization/ Sandbox Evasion	Credentials in Files	File and Directory Discovery		Email Collection		Remote File Copy					
	Exploitation for Client Execution	Windows Service	Valid Accounts	Masquerading		Process Discovery		Data from Local System		Non-Standard Port					
	Service Execution	Scheduled Task	Exploitation for Privilege Escalation	Deobfuscate/ Decode Files or Information		Application Window Discovery				Remote Access Tools					
	Scheduled Task		Abuse Elevation Control Mechanism	Access Token Manipulation		System Network Configuration Discovery				Web Service					
			Extra Window Memory Injection	Software Packing		System Time Discovery									
			Scheduled Task	Disable or Modify Tools		System Owner/ User Discovery									

Actividades realizadas

- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 38 análisis de muestras sospechosas.
- Utilizando herramientas de Threat Hunting, el equipo ha recopilado muestras de diversas fuentes, teniendo en cuenta las tendencias de ataques en la región.
- La validación de las características de los malware detectados es crucial para clasificar cada uno en función de las capacidades demostradas durante el análisis avanzado.
- Identificación de las tácticas, técnicas y procedimientos utilizados por los actores de amenazas a través de cada una de las muestras recolectadas, obteniendo así las tendencias de ataque perpetrado por los cibercriminales.
- Los indicadores de compromiso se tienen en cuenta para ser agregados a eventos en la herramienta de MISP así como a la herramienta de Threat Intelligence Platform TIP donde se enriquecen los indicadores con información como actores de amenaza, familias de malware, tácticas y técnicas de la matriz de Mitre Att&ck. Por consiguiente, los indicadores son agregados a las herramientas de seguridad del cliente.

Recomendaciones y conclusiones

- A través del Laboratorio Avanzado de Malware, el equipo de Cyber Threat Intelligence automatiza y mejora los procesos de detección y análisis de muestras sospechosas de contener malware y que puedan afectar la infraestructura corporativa.
- Se recomienda reportar cualquier tipo de archivo sospechoso que sea detectado al interior de la infraestructura de la empresa provenientes de correos electrónicos sospechosos, descargas de software no autorizadas, dispositivos de almacenamiento no autorizados, etc.

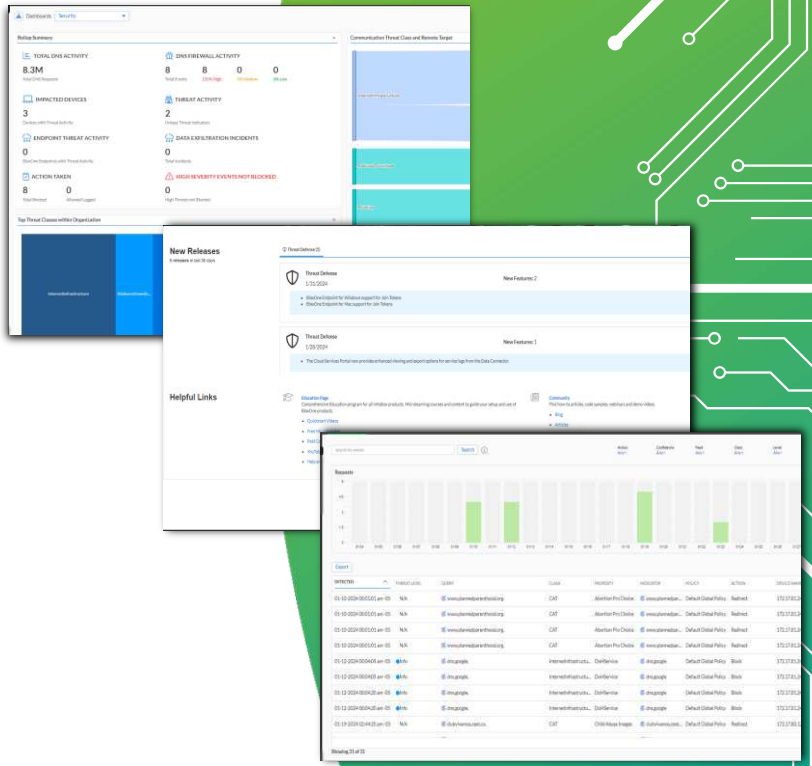
Infoblox

DEFINICIONES

Protección DNS: Brinda seguridad contra ataques de malware, phishing y ransomware a través de la inspección y el filtrado de DNS.

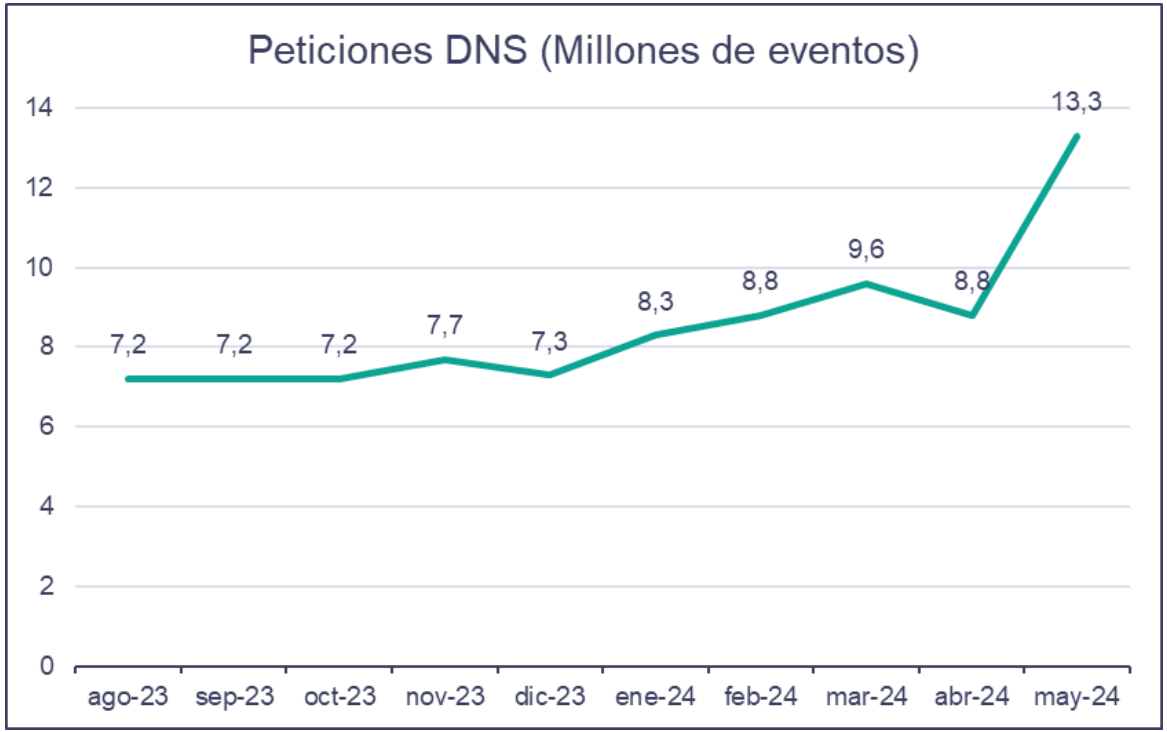
Política: cuenta con una serie de políticas que rigen cómo opera la empresa. Estas políticas se establecen para proteger a los empleados, clientes y socios de Infoblox, así como para garantizar que la empresa cumpla con todas las leyes y regulaciones aplicables.

Reportes: Herramienta integral que recopila, analiza y presenta datos de todas las soluciones de Infoblox.

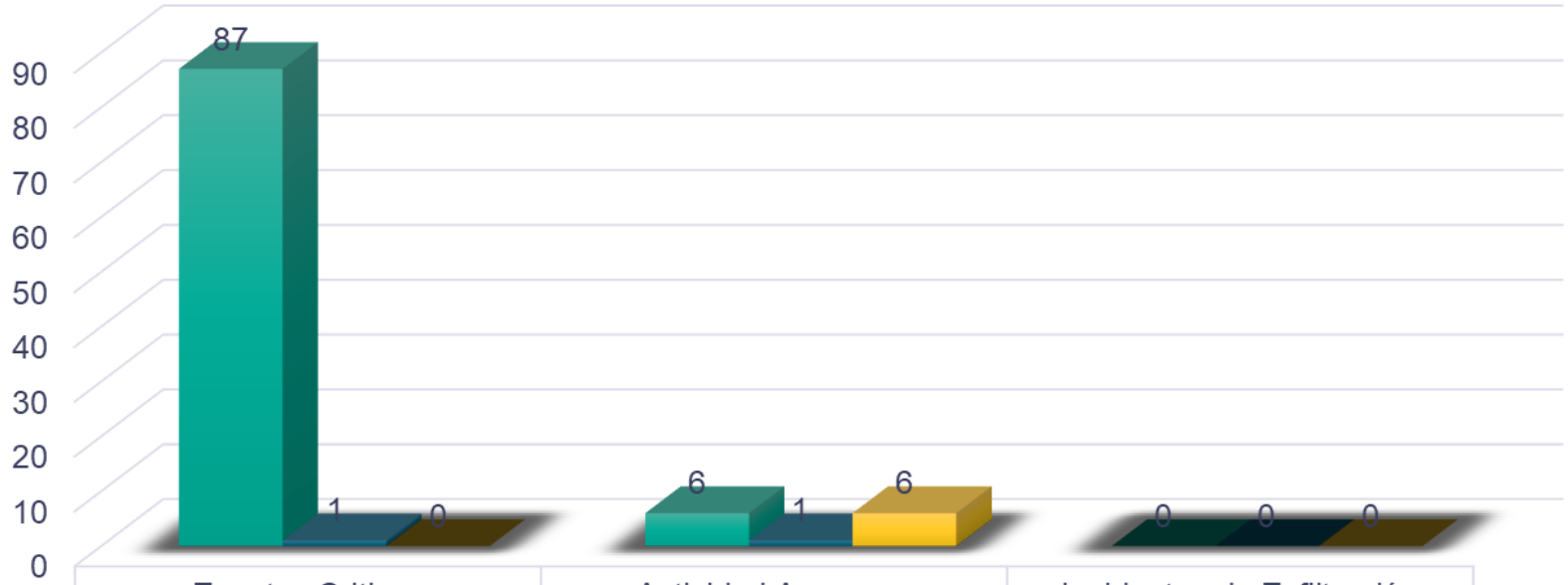


DNS SECURITY – INFOBLOX (Millones de eventos)

Se evidencia que para el periodo en mención hubo un aumento en el promedio de peticiones DNS que fueron resueltas por Infoblox. Por otra parte, se evidencia una disminución en la actividad de amenaza a nivel de actividades detectadas y contenidas por el FW DNS.



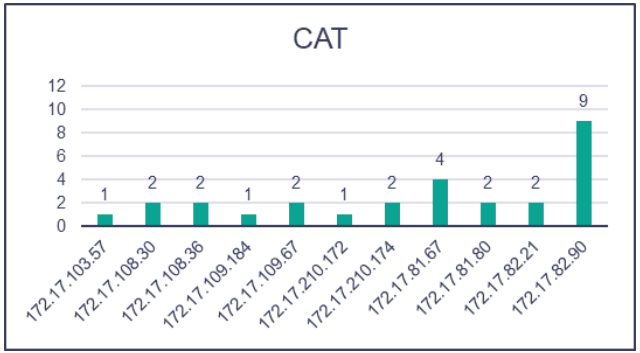
INDICADOR AMENAZAS

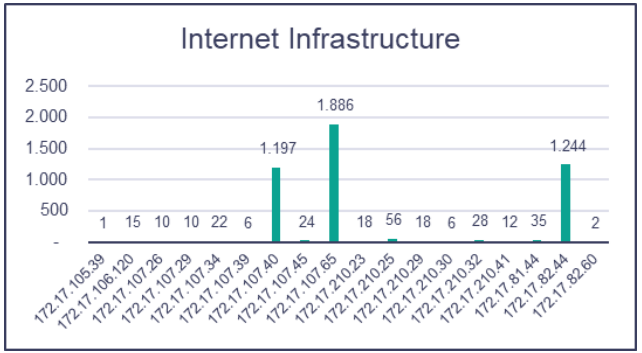


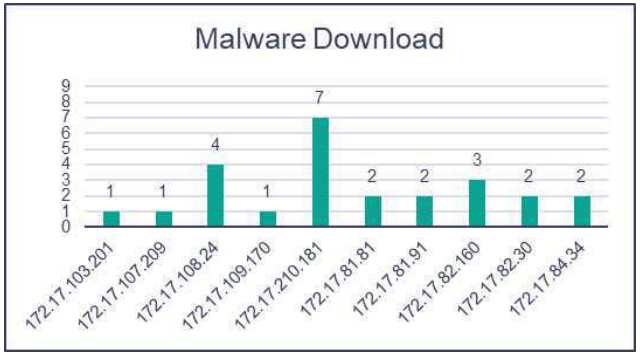
	Eventos Criticos	Actividad Amenaza	Incidentes de Exfiltración
mar-24	87	6	0
abr-24	1	1	0
may-24	0	6	0

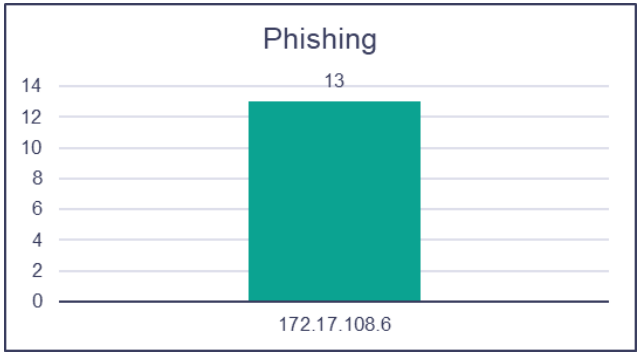
DNS SECURITY – INFOBLOX

Top de las clases de amenazas por host que más impactan al FNA

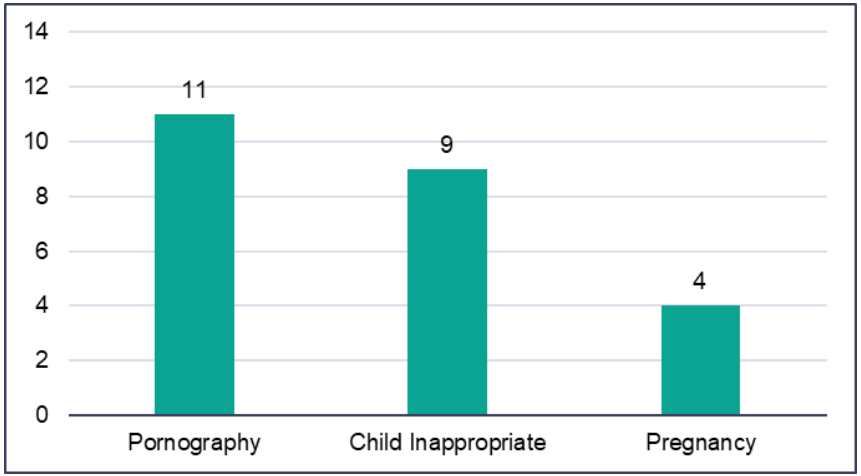








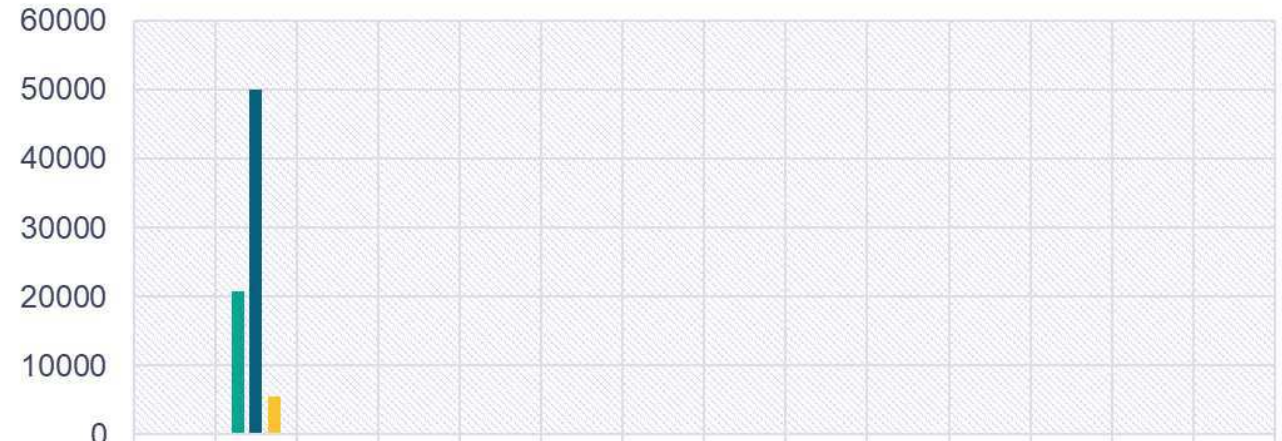
Top de los destinos malintencionados consultados a nivel interno del FNA, los cuales fueron bloqueados por la herramienta Infoblox.



Para el periodo en mención se evidencia una disminución con relación al mes anterior en cuanto al índice de amenazas detectadas, de igual forma se identifica que el volumen de consultas a portales de pornografía aumento en la resolución de DNS.

GENERAL DNS – INFOBLOX

Para el periodo en mención se evidenció una disminución considerable en la categoría de DoHservice en las consultas DNS.



	Abortion Pro Choice	Do Hservice	Generic	Malvertising	Pornography	R-Rated	Sex Education	SexualMaterial	Child Abuse Images	Child Inappropriate	Pregnancy	Nudity	Sex & Erotic	Look alike
mar-24	0	20790	10	26	16	0	0	0	75	0	2	0	324	0
abr-24	0	49909	0	0	24	4	0	0	0	0	5	0	0	1
may-24	0	5490	23	15	13	0	0	0	0	9	6	0	0	0

Actividades realizadas

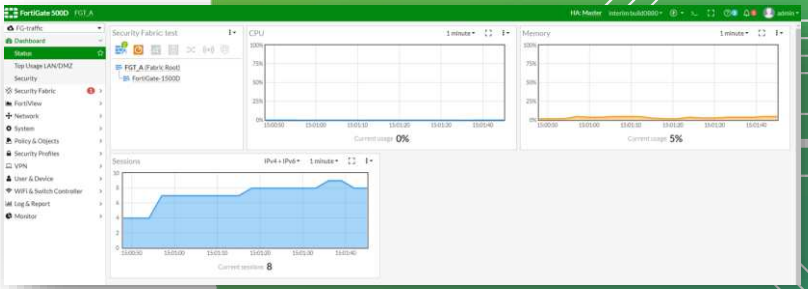
- Se relacionan las actividades realizadas durante el periodo en mención.
- Monitoreo de plataforma Infoblox para la verificación de conexiones sospechosas y maliciosas.
- Actualización de la plataforma Infoblox.
- EL día 29 de abril se realizó la migración de la VM al servidor físico ZTP_bogpvpplp028.fna.gov.co_3020112524152165659.
- El día 15 de mayo se realizó la migración del servidor principal ZTP_BOGPVPPLP027.fna.gov.co_3050650800160578 43.

FORTINET

FortiWeb™

GENERAL WAF – FORTIWEB

FortiWeb es un firewall de aplicaciones web (WAF) que protege aplicaciones web y API de ataques dirigidos a usuarios conocidos y exploits desconocidos y ayuda a mantener el cumplimiento de regulaciones. Usando el aprendizaje automático para modelar cada aplicación, FortiWeb defiende las aplicaciones de vulnerabilidades conocidas y de las amenazas de día cero. Alto rendimiento físico, dispositivos virtuales y contenedores se implementan en el sitio o en el nube pública para dar servicio a organizaciones de cualquier tamaño, desde pequeñas empresas hasta proveedores de servicios, operadores y grandes empresas.



Protección de aplicaciones web

Protección multicapa contra los 10 principales ataques a aplicaciones de OWASP, incluido el aprendizaje automático para defenderse de ataques conocidos y desconocidos.

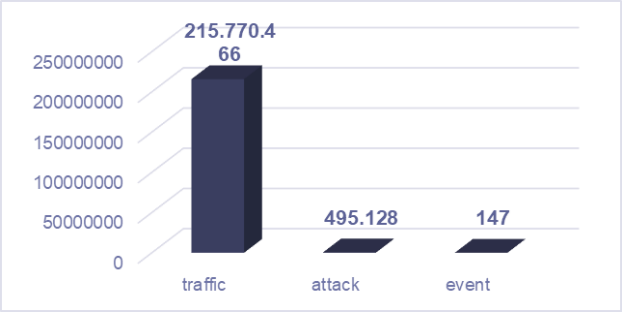
Protección API

Protege los API de actores maliciosos aplicando automáticamente lo positivo y lo negativo. políticas de seguridad. Integra la seguridad API en su proceso de CI/CD.

Mitigación de Bots

Protege sitios web, aplicaciones móviles y API de ataques automatizados con un bot avanzado mitigación que diferencia con precisión entre el tráfico de bots buenos y los bots maliciosos. FortiWeb Bot Mitigation proporciona la visibilidad y el control que necesita sin ralentizar a los usuarios con captchas o desafíos innecesarios.

GENERAL WAF – FORTIWEB

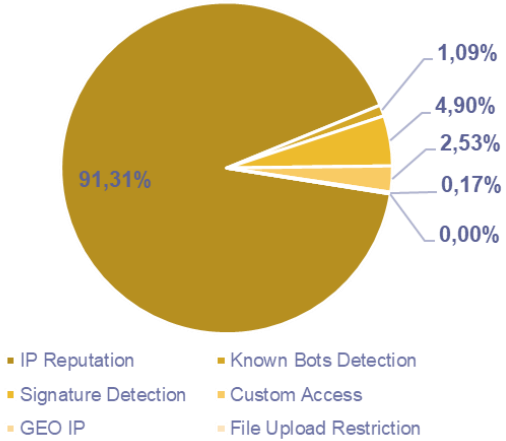


+216 M

Eventos verificados por el WAF

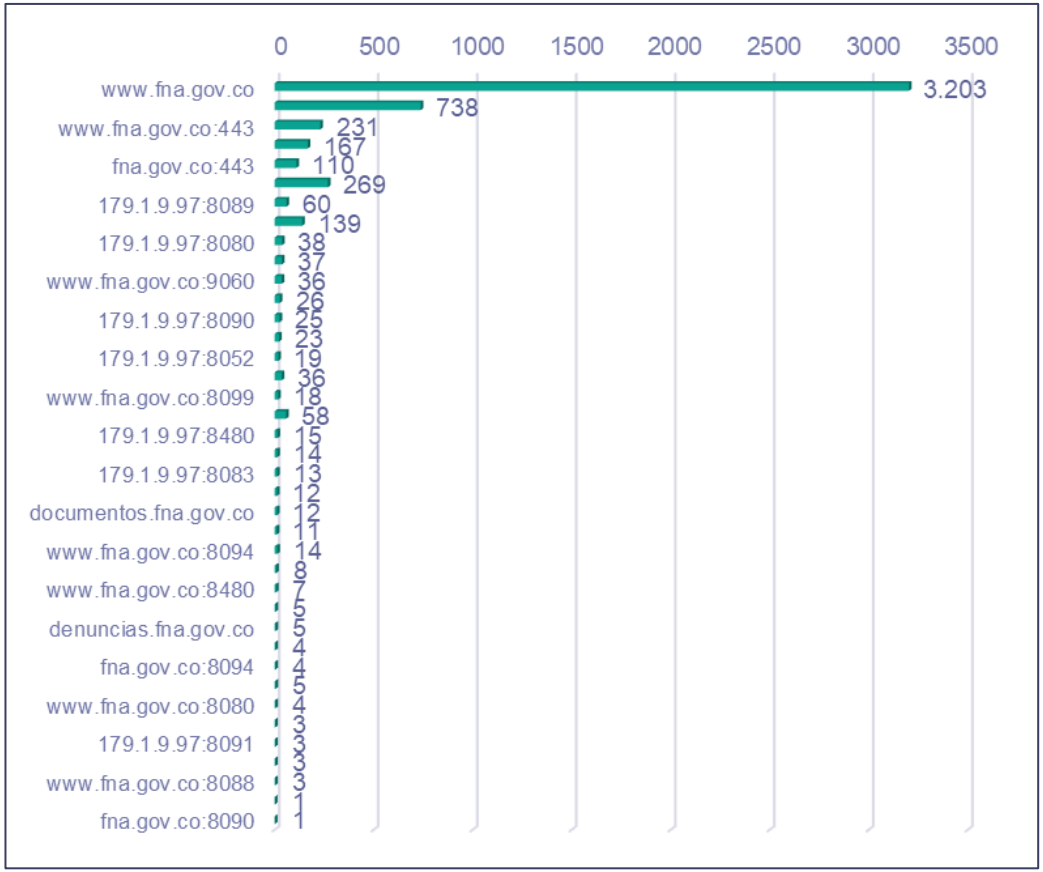
-0,23%

Del tráfico total es categorizado como amenaza



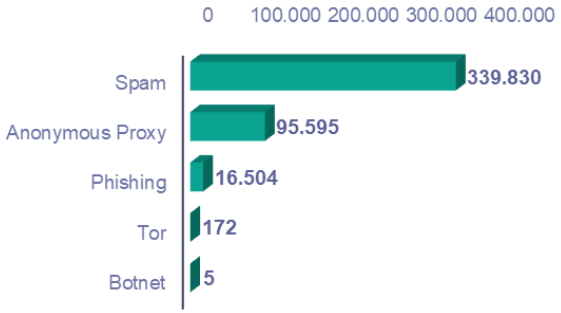
De lo anterior: En el periodo del 22 de abril al 21 de mayo se visualizó tráfico a través del WAF de aproximadamente 216 Millones de eventos de los cuales menos del 0,23% están dentro de la categoría Amenaza.

GENERAL WAF – FORTIWEB



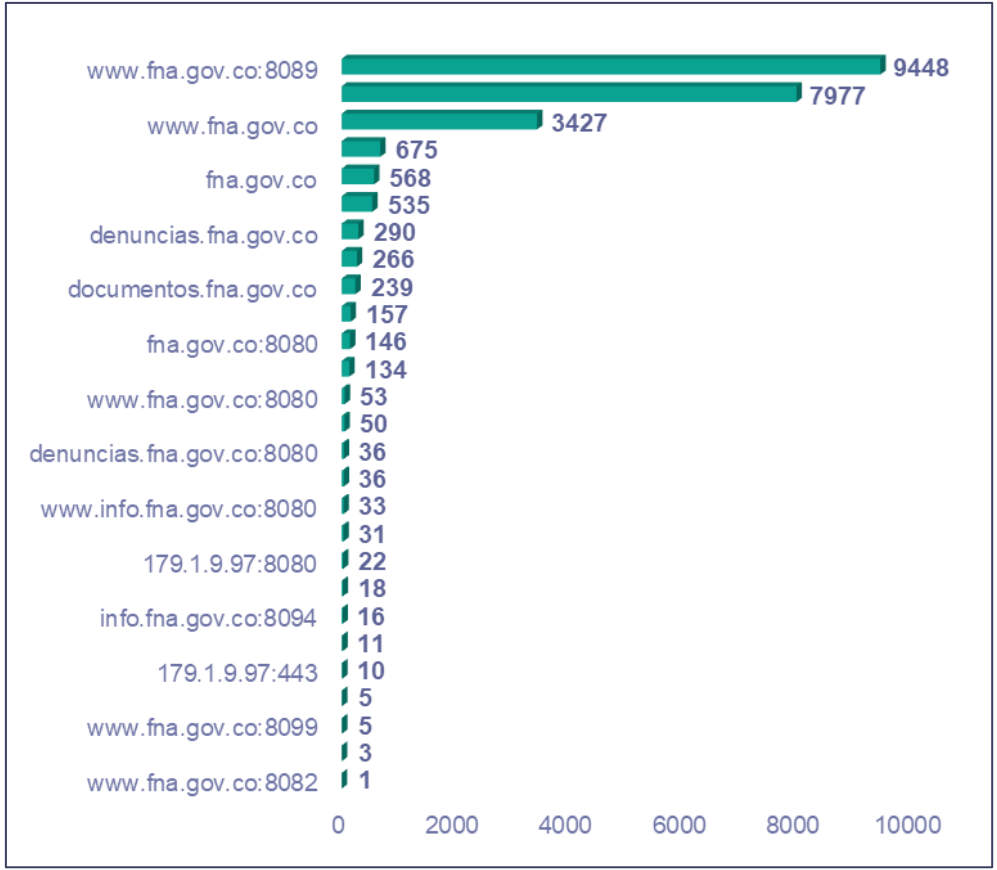
+452 M

IP Reputation



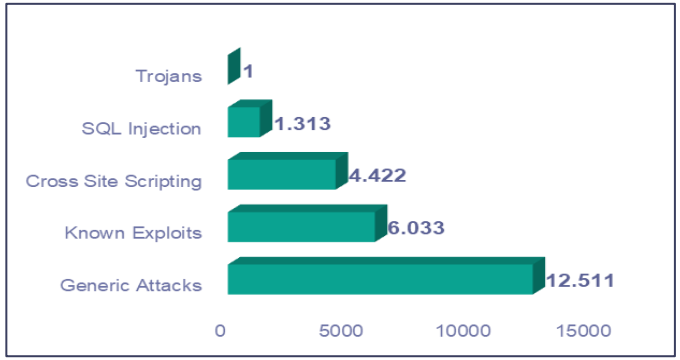
Se detectaron un total 452.106 eventos de amenazas de tráfico proveniente de direcciones IP maliciosas

GENERAL WAF – FORTIWEB



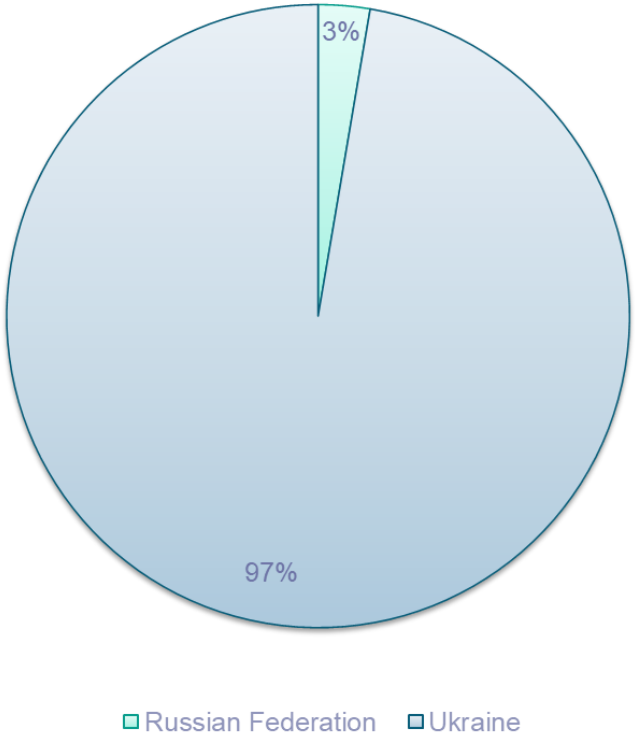
+24 M

Signature Detection



Se detectaron un total 24.280 eventos de ataques conocidos.

GENERAL WAF – FORTIWEB



822

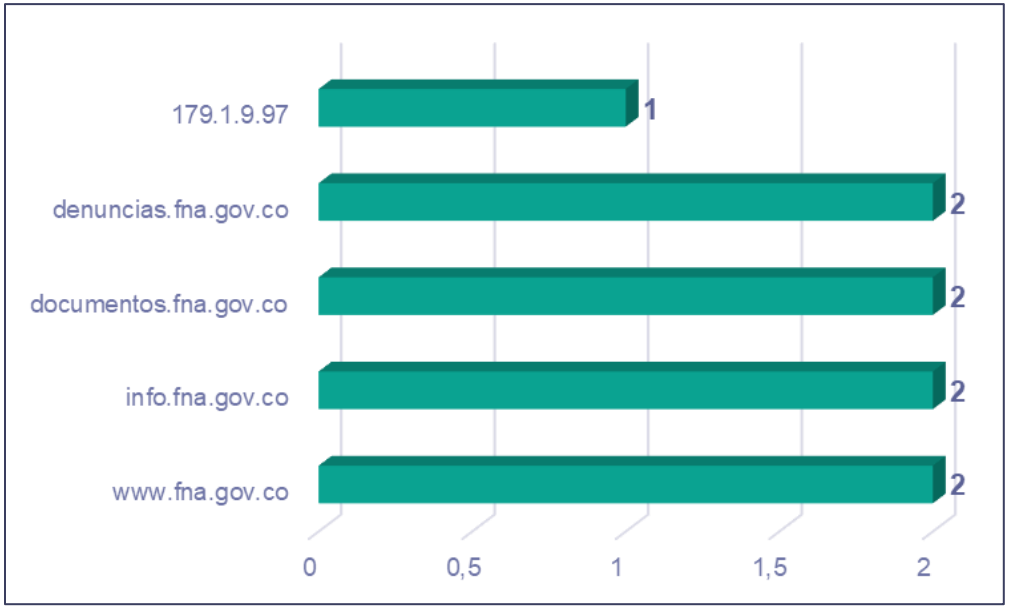
GEO IP

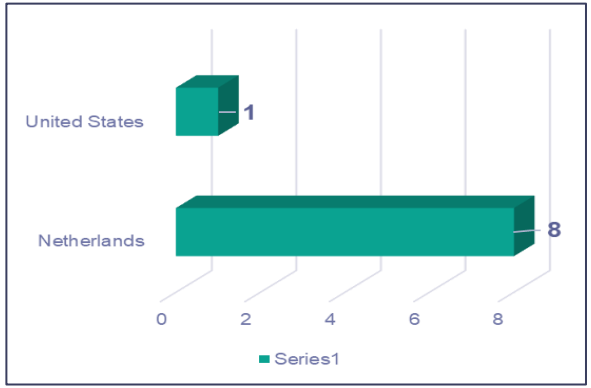
En FNA se ha dispuesto bloquear el tráfico desde Rusia y Ucrania.

GENERAL WAF – FORTIWEB

9

File Upload Restriction

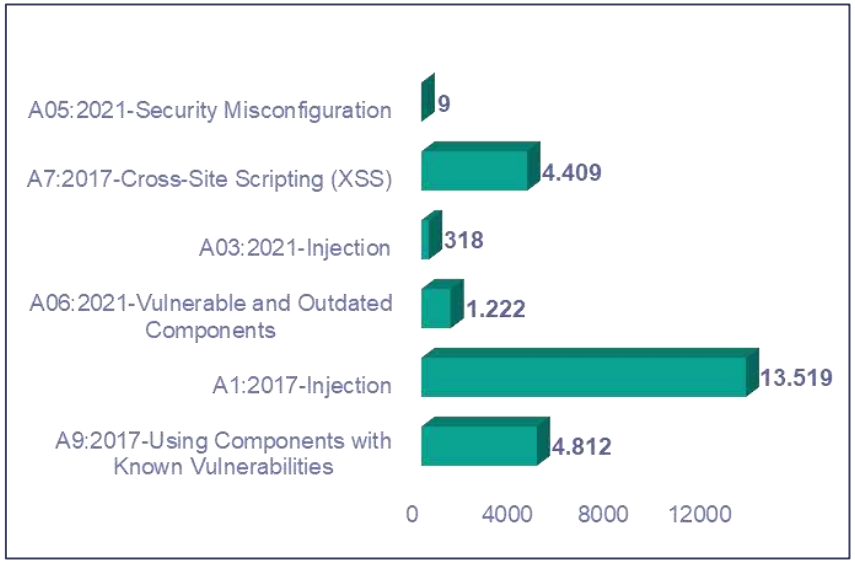




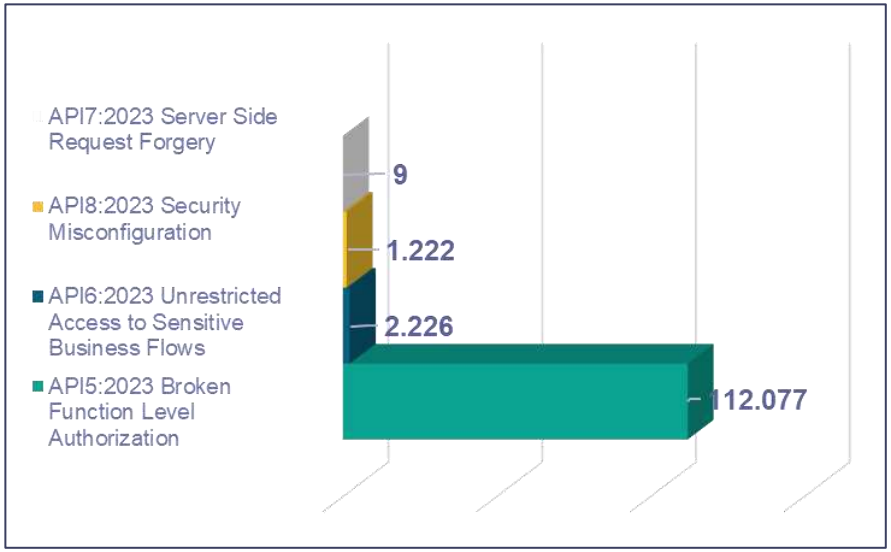
Se detectaron un total 9 eventos de ataques de archivos que se pueden cargar o modificar en una aplicación web.

GENERAL WAF – FORTIWEB

OWASP TOP 10



OWASP API TOP 10



Actividades realizadas

A continuación, se relacionan las actividades realizadas durante el periodo en mención.

Actividades diarias:

- Análisis y revisión de alertas
- Revisión de registros
- Revisión de las firmas de virus

Actividades semanales:

- Limpieza de registros
- Revisión del firmware
- Realizar una verificación de integridad del sistema
- Verificación y actualización de los IOC compartidos desde CTI

Actividades realizadas

- **Verificación del correcto funcionamiento del HA backup**

Según el control de Cambios C53837, el día 02 de mayo se realizó la prueba de HA, esta prueba constó del reinicio de los dispositivos y verificar el correcto funcionamiento del dispositivo secundario además de verificar que las comunicaciones funcionaran según lo planeado y que los servicios del fondo se mantuvieran activos.

En la prueba hubo una indisponibilidad de 40 segundos en el reinicio del dispositivo primario y de 30 segundos en el reinicio del dispositivo secundario, las pruebas ocurrieron según lo planeado y todas las aplicaciones web funcionaron correctamente.

Según esta prueba se procedió con la actualización del firmware de los dispositivos.

Actualización del Firmware de Fortiweb

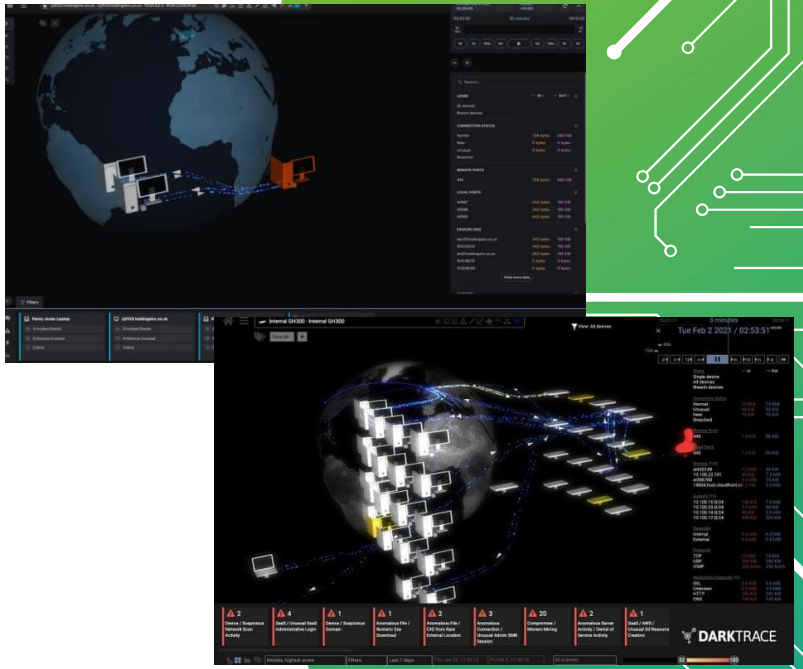
Según el control de Cambios C53837, el día 09 de mayo se realizó la actualización del firmware de los dispositivos desde la versión FV-1KE-7.0.0-build0057-220119 a la versión FV-1KE-7.4.3-build0638-240405.

El procedimiento se realizó a las 10:00 p.m. sin ninguna novedad con una indisponibilidad de 30 segundos según lo planeado**.**

DARKTRACE

DEFINICIONES

La tecnología de Darktrace se basa en un tipo de machine learning conocido como no supervisado, lo cual implica que el software está programado para aprender desde cero acerca del estado normal del sistema o la red. Así, puede detectar todo tipo de amenazas, incluyendo las que explotan vulnerabilidades desconocidas.



Informe solución Darktrace/Respond

2024

6880
Dispositivos modelados

233
Subredes

536
Dispositivos en brechas

812
Brechas

129
Modelos

Objetivo

Presentar los resultados del servicio de soporte de la solución de Ciberdefensa Darktrace, realizados por el Ingeniero especialista en Ciberdefensa de Mnemo Colombia S.A.S., permitiendo contar con la visibilidad del estado actual de las amenazas presentadas y del soporte dado sobre la solución del Fondo Nacional de Ahorro.

Alcance

Los hallazgos presentados en el presente informe fueron detectados durante el periodo comprendido entre el 22 de Abril y el 21 de Mayo de 2024, comprendiendo los siguientes temas.

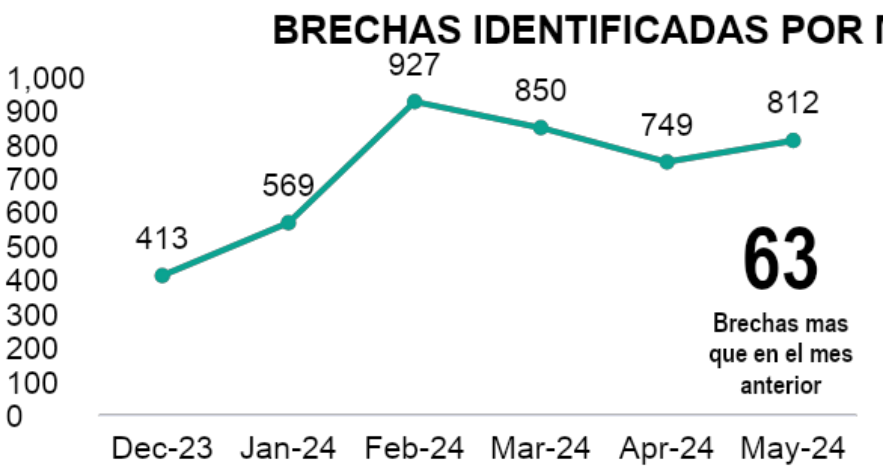
- Dar a conocer las estadísticas generales de la solución de Ciberdefensa.
- Presentar los modelos que se alertaron durante el periodo.
- Dar a conocer los sistemas identificados en los modelos presentados.
- Recomendaciones.

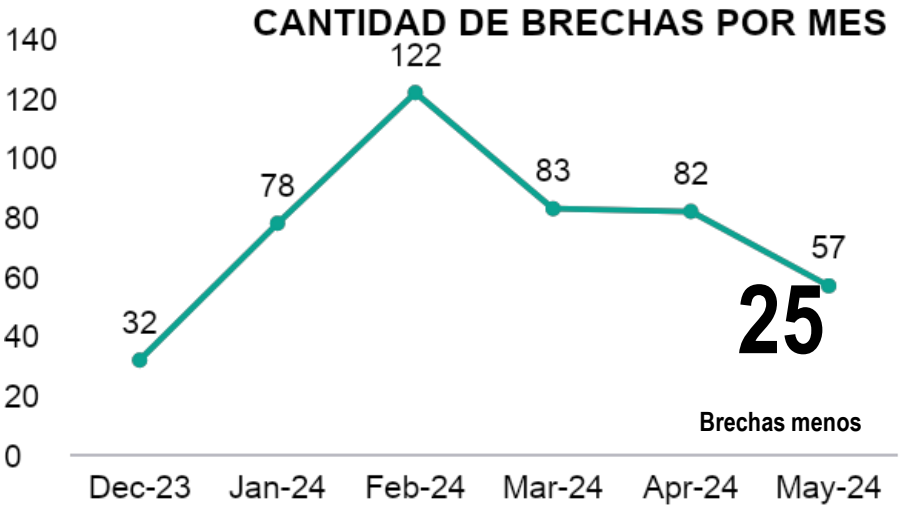
Distribución de Brechas

Brechas Darktrace/Detected

Modelos Darktrace/Respond

En las gráficas a continuación se dan a conocer las brechas totales registradas hasta la fecha junto con el equivalente en porcentaje respecto al periodo anterior.



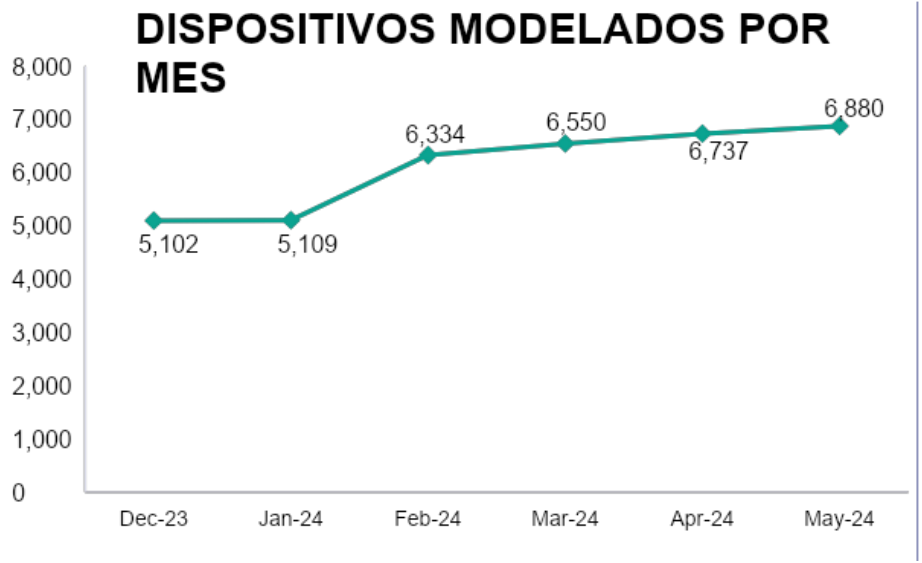


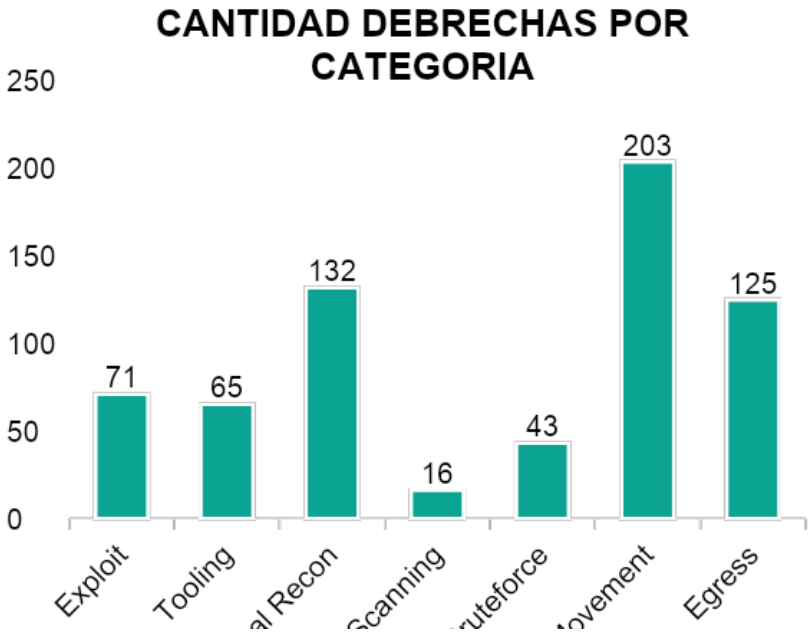
Brechas identificadas por categoría

Licenciamiento

Distribución de Brechas

Los modelos de ciberdefensa se pueden organizar de acuerdo con la fase de ataque que es más probable que detecten. Los modelos de monitoreo de acuerdo con estas categorías pueden permitir que el patrón de comportamiento característico de un ataque en curso sea observado.





Informe solución Darktrace/Email

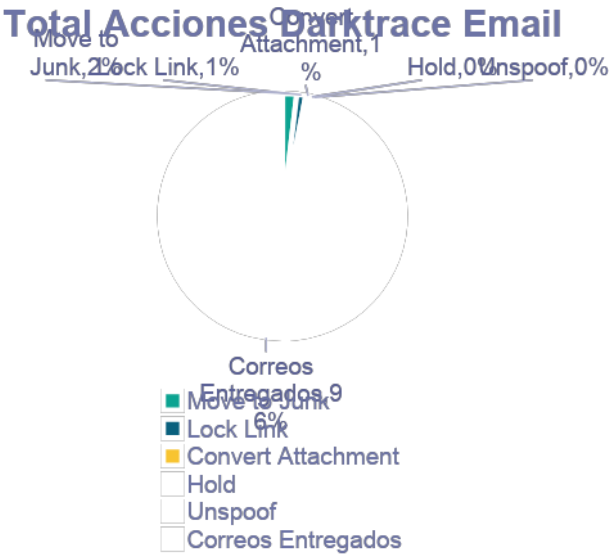
2024

287.481
Correos Entrantes

12.261
Correos con accion

275.220
Correos Entregados

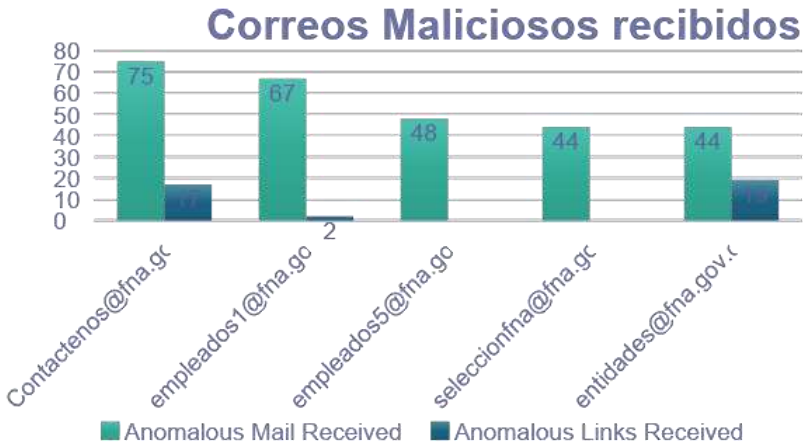
501.270
Correos Salientes



Top Acciones	Total, Acciones	% total de correos
Move to Junk	5.348	2%
Lock Link	3.425	1%
Convert Attachment	1.706	0,6%
Hold	1.202	0,4%
Unspoof	590	0,2%

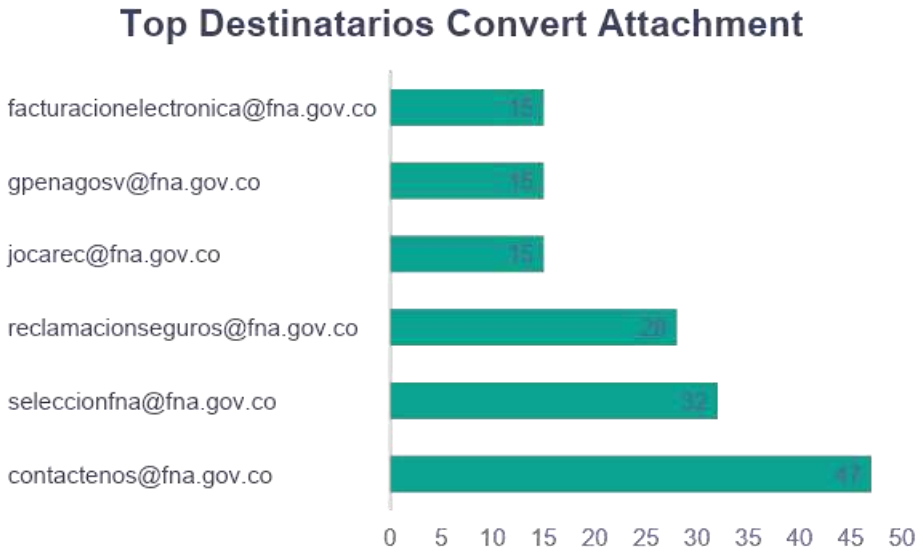
Administración Email

Los siguientes usuarios recibieron la mayor parte del correo de este tipo en el periodo correspondiente al presente informe. Todo el correo incluido en este recuento habría alcanzado el umbral básico para la acción Mover a correo no deseado de Darktrace/Email.

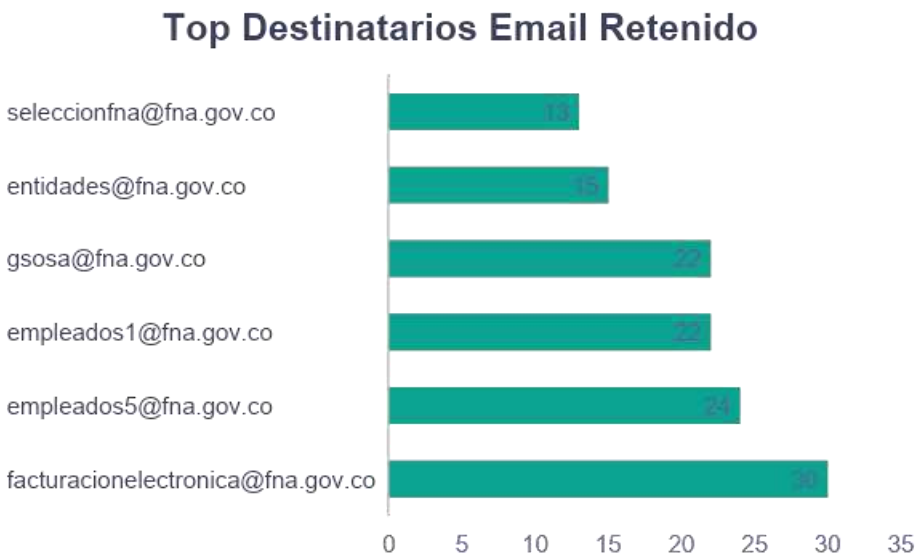


Administración Email

Múltiples anomalías han elevado la puntuación de este correo electrónico por encima del umbral (threshold) de retención.



Destaca archivos adjuntos inesperados de corresponsales conocido que pueden indicar que la cuenta de usuario del corresponsal extern ha sido comprometida



Actividades realizadas

De acuerdo con los eventos generados en las diferentes herramientas y la gestión diaria dentro del FNA se dan las siguientes recomendaciones y conclusiones.

- Nombramiento de Subredes, de acuerdo con información suministrada por Redes.
- Se realiza Back up Semanal, el cual se conserva copia en el dispositivo de Darktrace y equipo administrador de la plataforma.
- Se realiza análisis de los correos enviados por el remitente inversiones.lamarula@outlook.com
- Se realiza análisis de correos del remitente marthasaenz@solusoftcorp.com como destinatario facturacionelectronica@fna.gov.co
- Se realiza análisis de los correos enviados por el remitente radicación.facturacion@sdtinngenieria.com
- Por solicitud del Área de seguridad de la información se extiende las acciones de Respond del incidente 43477 - miguel2024.kozow.com
- Por solicitud del Área de seguridad de la información se extiende las acciones de Respond del incidente 43480 - 74.112.186.144 - api.box.com
- Revisión eventos Darktrace incidente bloqueo de usuarios de red
- Se genera solicitud con mesa de ayuda para realizar el análisis de los correos del remitente posgradoseconomiauis@gmail.com
- Generación de Informe solicitud de Enrique Arrazola, indicadores mensuales.
- Se realizan los correspondientes alertamientos de los modelos activos durante la administración en sitio.
- Se recomienda continuar con las labores de revisión y validación de los modelos reportados con el área de Seguridad de la Información para poder ajustar las reacciones del Darktrace con las políticas de Seguridad de la Información.

Guardium es una plataforma de protección de datos que permite a los equipos de seguridad analizar automáticamente lo que sucede en entornos de datos confidenciales. Ayuda a garantizar la integridad de la información en los centros de datos y a automatizar los controles de cumplimiento.

Estado plataforma

En el periodo comprendido entre el 22 de abril al 21 de mayo de 2024, la plataforma presentó estabilidad y normalidad en su operación.

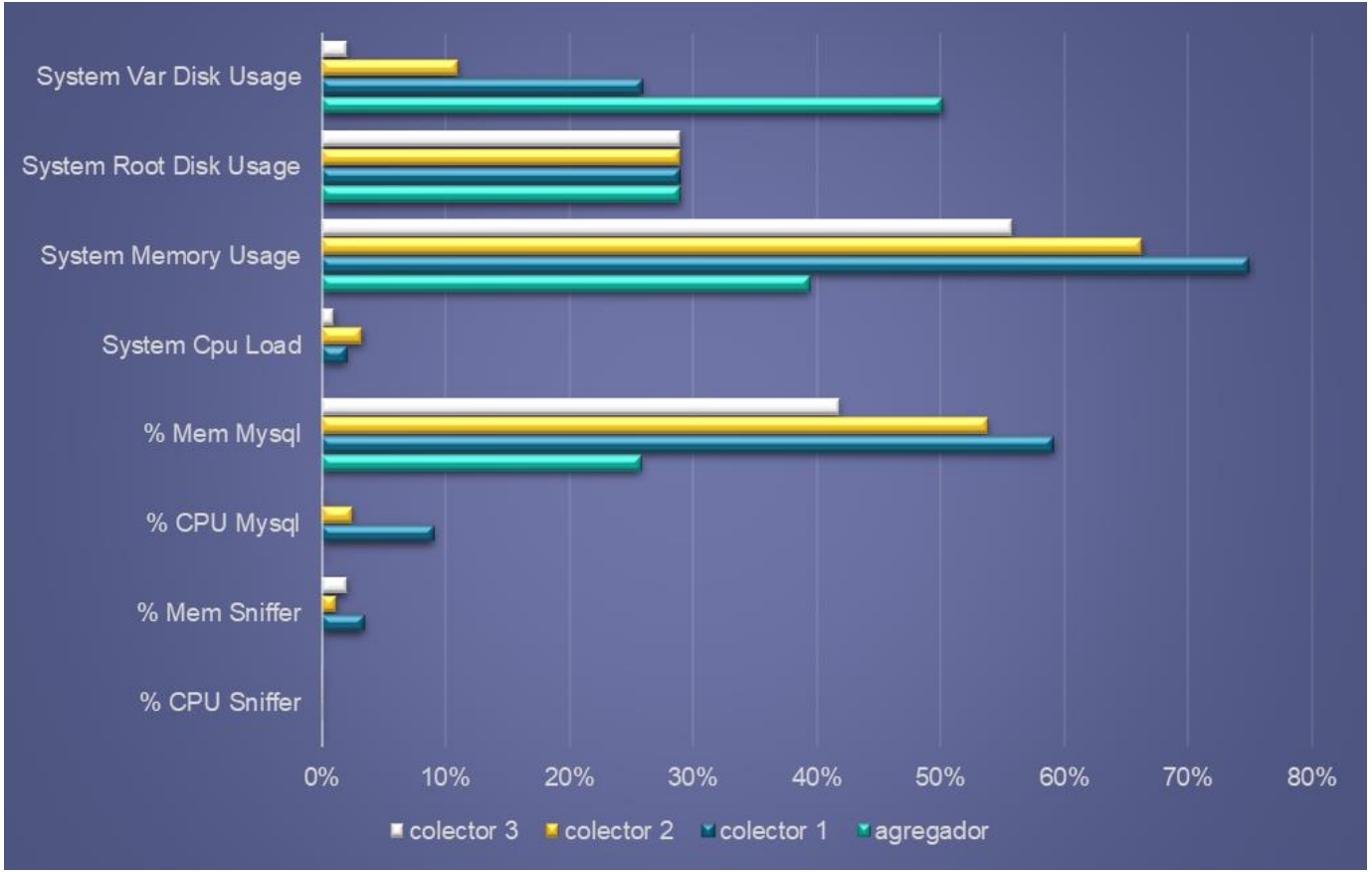
Actividades macro ejecutadas	Actividades a ejecutar
• Actualización de parches 1042, 1266, 9997. • Sesiones base de datos COBIS, solicitud desarrollo monitoreo campos consumidor financiero. • Validación de monitoreo de tráfico, insumo base políticas. • Creación políticas base COBIS.	• Despliegue guardium sobre servidores pre productivos. • Configuración de regla del consumidor financiero de acuerdo con el desarrollo solicitado.

Eventos reglas COBIS

A continuación, se relacionan los eventos que se generaron de acuerdo con el registro de tráfico y reglas configuradas para la base de datos de COBIS producción. Esto quiere decir que los eventos corresponden al tráfico que hace match en los criterios de las reglas, y que es motivo de validación y revisión para afinamiento:

- **FNA_COBIS_nuevas_conexiones:** APLBKPINC, CNX_COBISNS, CNX_ORECIPROCAS, GGONZALEZ, HPAPM, INTRANET, LALVEAR, OPCRUZ
- **FNA_COBIS_usuarios_app_ipdesconocida:** ETLSYB
- **FNA_COBIS_usuarios_cnx_ipdesconocida:** CNX_MON_ASEPROD, CNXCONTROLGARANTIAS
- **FNA_COBIS_usuarios_cnx_srcapp_desconocida:** CNX_COBISNS, CNX_MON_ASEPROD, CNXCONTROLGARANTIAS
- **FNA_COBIS_usuarios_nombrados_ipdesconocida:** CPPALACIOSR, GGONZALEZ, JEMORENOR, LJOPEREZQ, OPORTIZ, SRODRIGUEZ
- **FNA_COBIS_usuarios_nombrados_srcapp_desconocida:** LJOPEREZQ

Comportamiento plataforma, 22 de abril al 21 de mayo de 2024



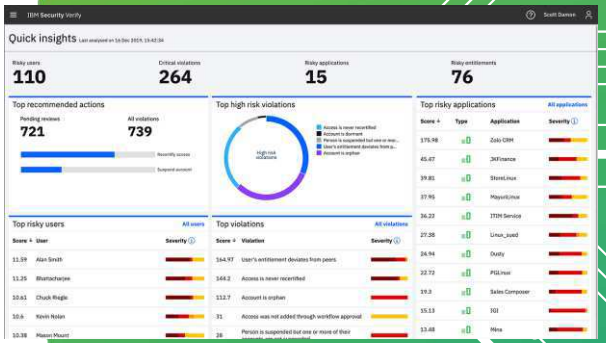
Servidores de bases de datos monitoreados

Servidor	Ultima respuesta de STAP
10.10.12.74	2024-05-24 15:36:15
172.16.126.68	2024-05-24 15:36:18
172.16.128.20	2024-05-24 15:36:19
172.16.131.100	2024-05-24 15:36:18
172.16.131.101	2024-05-24 15:36:16
172.16.131.109	2024-05-24 15:36:16
172.16.131.110	2024-05-24 15:36:19
172.16.131.128	2024-05-24 15:36:15
172.16.131.129	2024-05-24 15:36:18
172.16.131.57	2024-05-24 15:36:19
192.168.180.153	2024-05-24 15:36:18

IBM **Security**

Verify

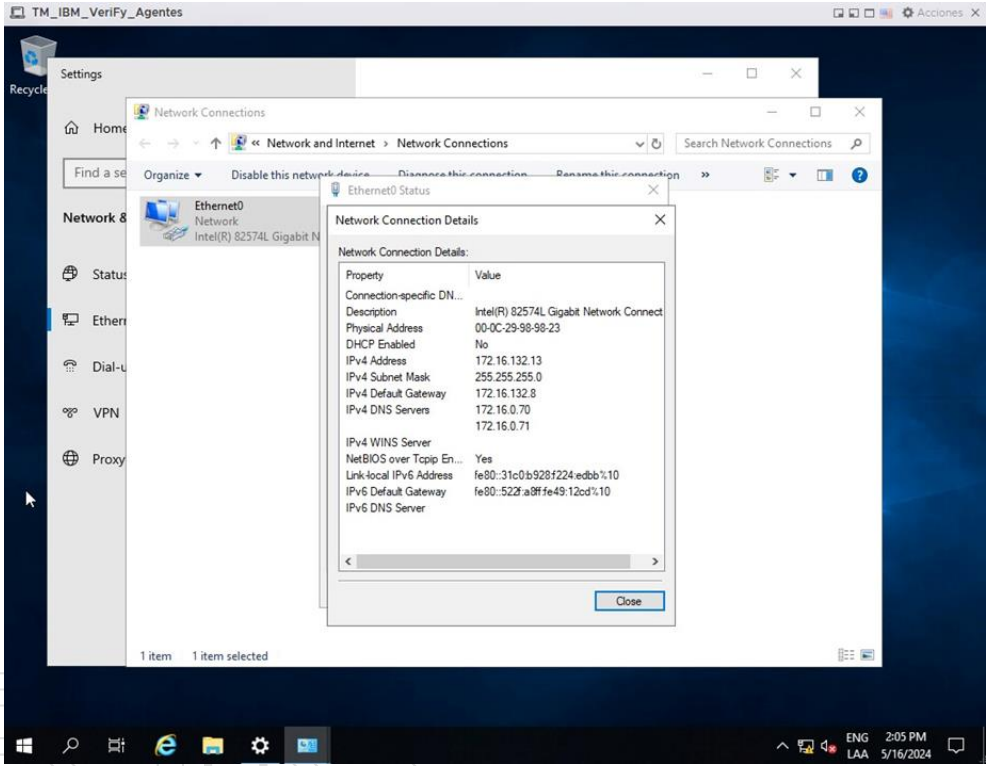
La solución IBM Security Verify, modernizada y modular, proporciona un contexto profundo impulsado por IA para la gestión de identidades y accesos (IAM) tanto de los consumidores como del personal. Proteja a sus usuarios y aplicaciones, dentro y fuera de la empresa, con un enfoque de software como servicio (SaaS) nativo de la nube de baja fricción que saca partido de la nube. Para las aplicaciones locales heredadas, la versión Verify access proporciona una ruta fluida a la nube, para que pueda realizar la transición a su propio ritmo.



Autenticación avanzada, incluida la autenticación sin contraseña

Añada una capa de seguridad, como la autenticación de múltiples factores (MFA), o prescinda por completo de contraseñas para acceder más rápidamente a los datos y las aplicaciones.

Instalación máquina de pruebas wmware



AD

Se realizó la instalación de una máquina de prueba en el vmware par la conectividad y realización de las pruebas correspondientes a la creación, modificación y eliminación de usuarios en el AD QA

Parametrización cuentas Cobis

Request 1

https://172.16.123.130:8099/WSAdmin/CreacionFuncionario


```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:cre="htt
  <soapenv:Header/>
  <soapenv:Body>
    <cre:crearFuncionarioRequest>
      <header>
        <soa:peticionId>20210430094681</soa:peticionId>
        <soa:peticionFecha>2024-05-09T09:22:00</soa:peticionFecha>
        <soa:aplCod>066</soa:aplCod>
        <soa:usuarioId>ws_serv_soa</soa:usuarioId>
        <soa:usuarioOrigenId>cnx_iam</soa:usuarioOrigenId>
        <!--Optional:-->
        <soa:sesionId>?</soa:sesionId>
        <soa:terminalId>?</soa:terminalId>
      </header>
      <body>
        <funcionario>
          <identificacion>
            <numero>11223311</numero>
            <tipo>
              <codigo>CC</codigo>
            </tipo>
          </identificacion>
          <nombre>Diego Torres Prueba</nombre>
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/e
  <soapenv:Body>
    <ns3:crearFuncionarioResponse xmlns:ns3="http://cobiscorp.ec
      <header>
        <ns2:correlacionId>20210430094681</ns2:correlacionId>
        <ns2:errorCod>0</ns2:errorCod>
        <ns2:errorDesc/>
        <ns2:errorSisDesc/>
      </header>
      <body>
        <funcionario>
          <codigo>17653</codigo>
        </funcionario>
      </body>
    </ns3:crearFuncionarioResponse>
  </soapenv:Body>
</soapenv:Envelope>
```


COBIS

Se realizaron pruebas en la creación de usuarios, ya se tiene la conectividad entre verify y Cobis, al momento de realizar la creación hay una falla en la creación se escala al área de cobis.

SAP

Target Client

Login ID

Password

SAP System (DNS hostname or IP)

SAP System Number

SAP

- Se realizo la configuración correspondiente para realizar la integración entre verify y Sap
- Se solicitaron los archivos al cliente el (SAPJCO) para la conectividad entre verify y Sap.

Actividades realizadas

- Se realizo por parte del implementador la creación y actualización del escript de la fuente autoritativa para el cargue de usuarios del cliente en verify
- Se realizo la gestión de poner en producción una máquina virtual (wmware) para QA a cual es para realizar el proceso de creación, modificación y eliminación de usuarios y creación de OU en QA AD.
- Se gestiono con Windows la solicitud de creación de un AD QA para la realización de las pruebas de creación, modificación y eliminación de los usuarios empleados
- Se gestiono la solicitud para los permisos de conectividad entre srv QA y AD QA por parte del área de Windows.
- Se realizo por parte de implementador la instalación de verify en el servidor de QA
- Se realizaron sesiones con el área de Service Manager para la creación de usuarios en la aplicación, se evidencio que faltaron permisos a una tabla (ACTIVO).
- Se realizo la gestión y diligenciamiento del formato para solicitar los permisos correspondientes a la tabla mencionada para la creación de los usuarios en SM del FNA.

Actividades realizadas

- Se realizaron sesiones con el área encargada de la solución (COBIS), se gestiona el usuario de conexión para la integración de verify y COBIS.
- Se realizaron configuraciones del Webservice, no se están creando los usuarios al momento de la ejecución del mismo.
- Por cambio de proveedor se realizó una sesión en la cual se cambió esta implementación para SAP
- Se realizo la primera sesión se acercamiento con las áreas involucradas indicando la necesidad de la integración.
- Se solicito mediante correo electrónico los archivos de conexión (SAPJCO) hacia sap y el usuario para la conexión del verify hacia SAP, se enviaron al implementador

Recomendaciones y conclusiones

- Para el periodo no se evidenciarían eventos de retrasos al momento de solicitar la información necesaria para avanzar en el proyecto
- Se está realizando la gestión correspondiente con las áreas involucradas para el proceso de integración hacia verify.

Informe Monitoreo de marca

2024

58
Eventos reportados

47
Identity Fraud

8
Data protection

3
Brand protection

Objetivo

Presentar de forma clara y detallada las alertas generadas por el equipo de Monitoreo de marca basadas en los análisis descubiertos en fuentes abiertas (Surface web, Deep web, Dark web), asociados al Fondo Nacional del Ahorro y sus productos durante el mes de abril de 2024.

Objetivos específicos.

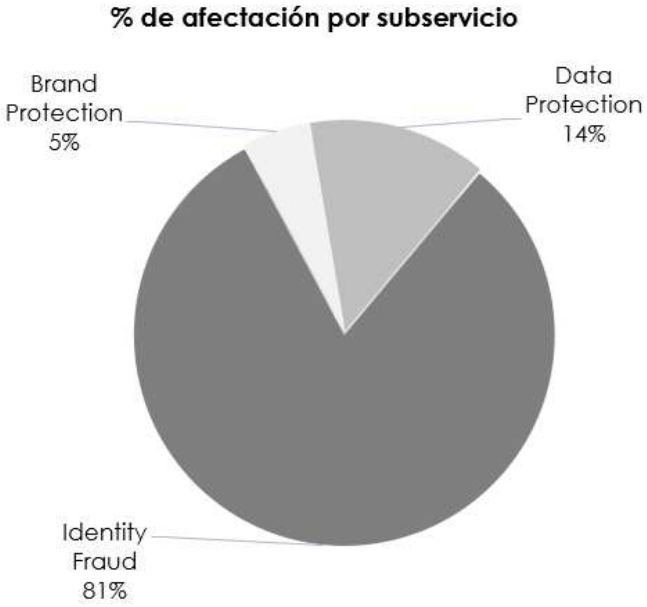
- Presentar los eventos identificados de acuerdo a las categorías y subcategorías definidas.
- Presentar los eventos que generen riesgo de manera inmediata a través de alertas en tiempo real.
- Identificar recomendaciones de mejora de acuerdo con los datos analizados.
- Presentar conclusiones relevantes.

Alcance

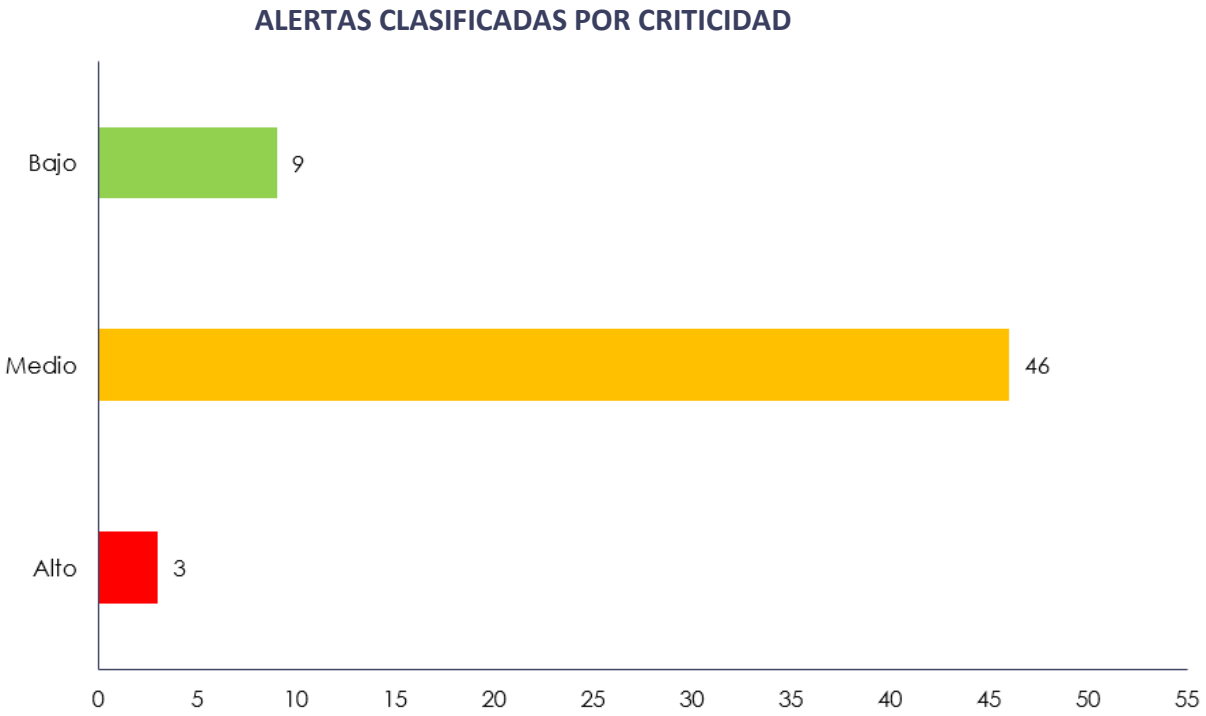
En el monitoreo de marca se busca realizar una captación de la información durante el periodo en mención, en la cual podemos identificar la presencia que tiene la entidad en la Clear, Deep y Dark Web, empleando distintas técnicas digitales que nos permita acceder. En un servicio 7x24 para la identificación de cualquier amenaza y desprestigio de la imagen corporativa.

Resultados Monitoreo de Marca

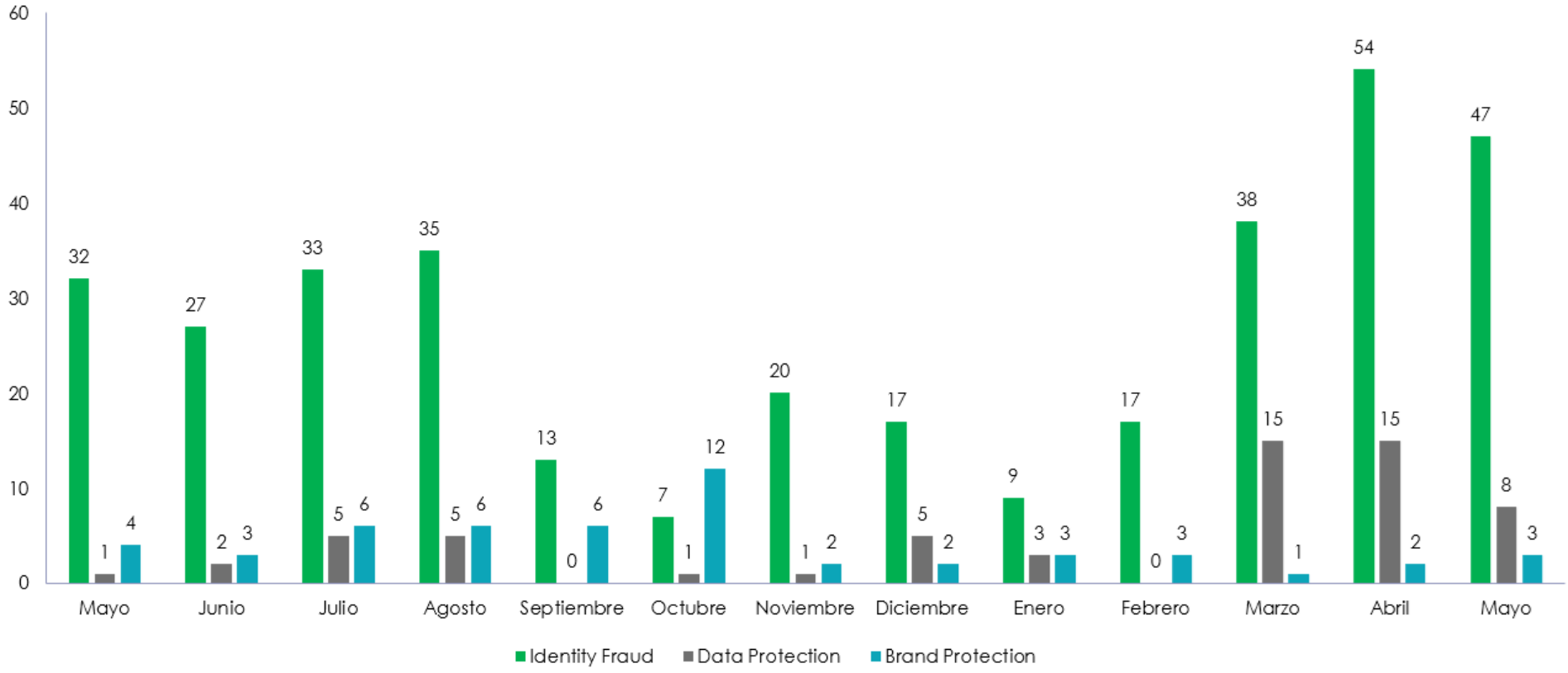
1. Comportamiento del servicio global Vigilancia



KPIs > Comportamiento del servicio global

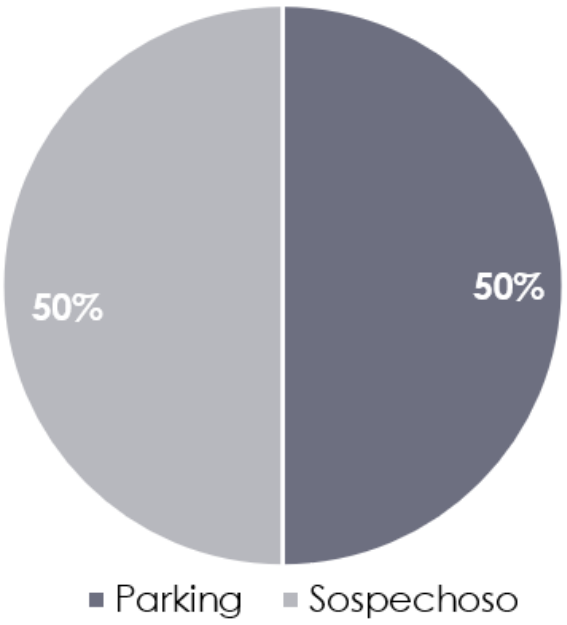


Evolución del servicio a nivel mensual



Resultados Monitoreo de Marca

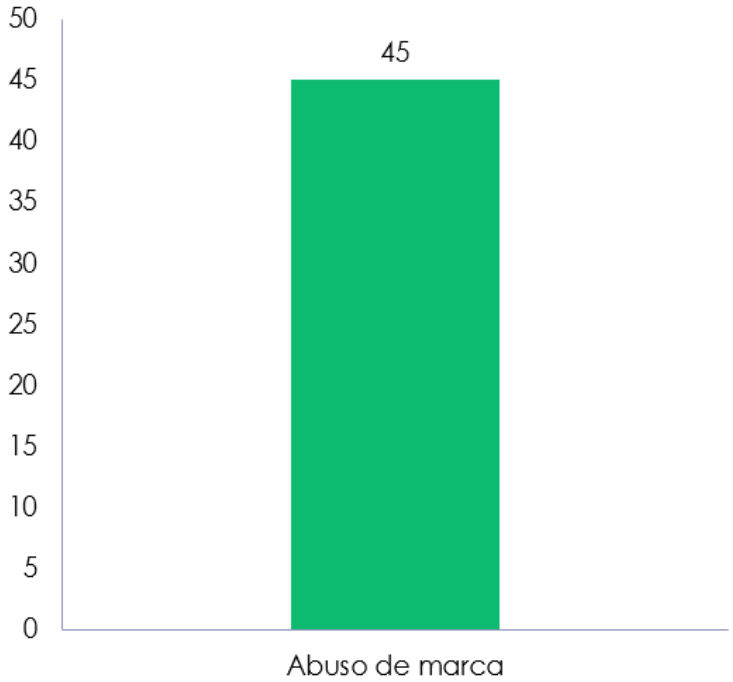
3. Dominios

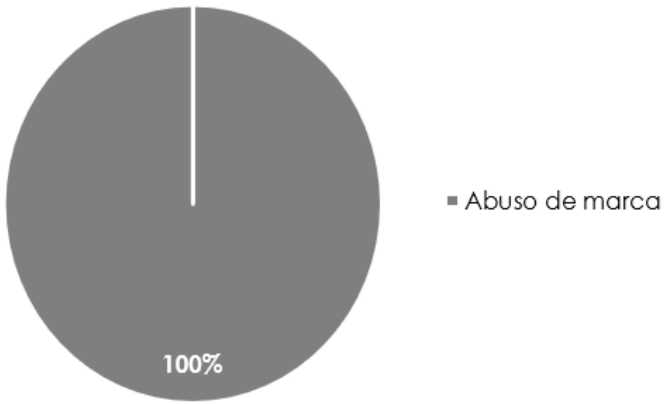


Resultados Monitoreo de Marca

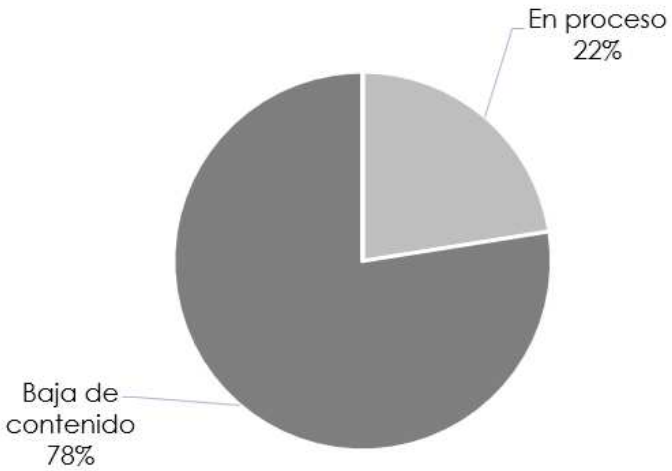
2. REDES SOCIALES

Se identificaron publicaciones en la red social de Facebook, haciendo referencia a ofrecimientos de servicios relacionados con el retiro cesantias y ofrecimientos de créditos en nombre del Fondo Nacional del Ahorro.





Resultados Monitoreo de marca



En Proceso: Continúan las gestiones para el cierre.

Baja de contenido: Cerrado. Amenaza eliminada

Descartado: No se continúan con las acciones de cierre por circunstancias ajenas al servicio.

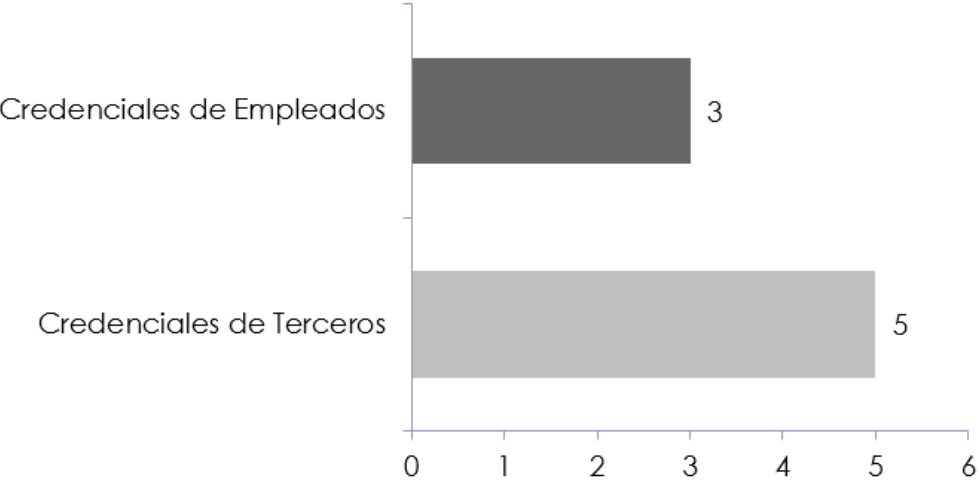
Sin gestión: Eventos sin gestionar. Pendientes de la solicitud del cliente.

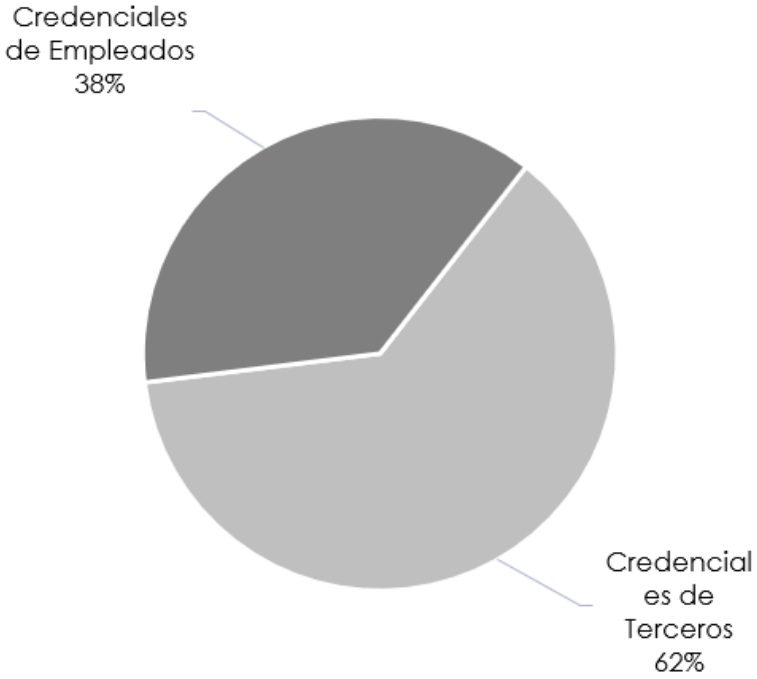
Resultados Monitoreo de marca

3. Información Expuesta – Credenciales filtradas

Volumetría por tipo de fuga

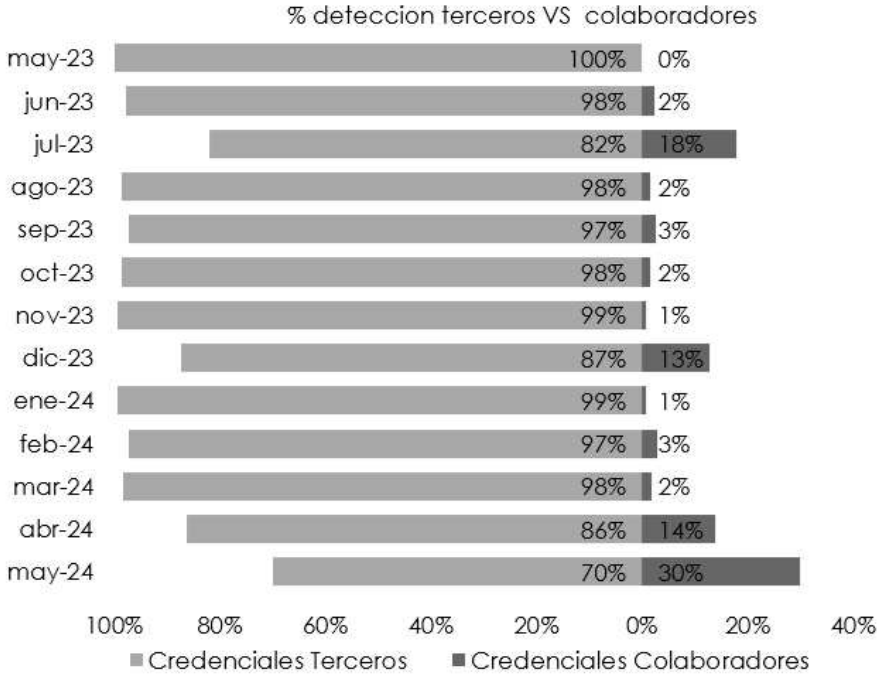
Nº Total de Alertas enviadas: 8

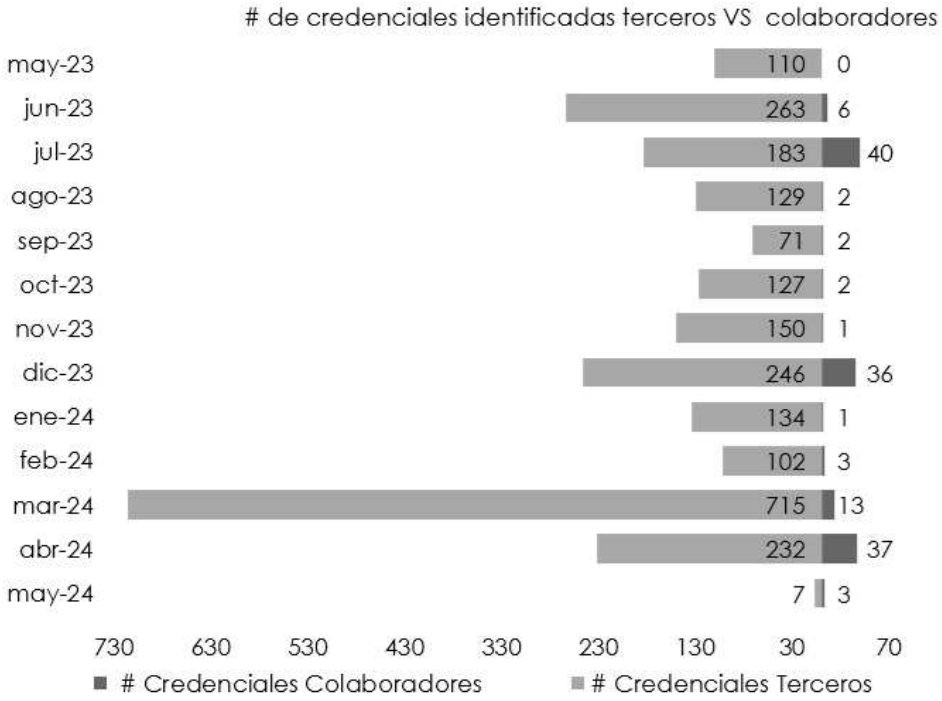




Resultados Monitoreo de marca

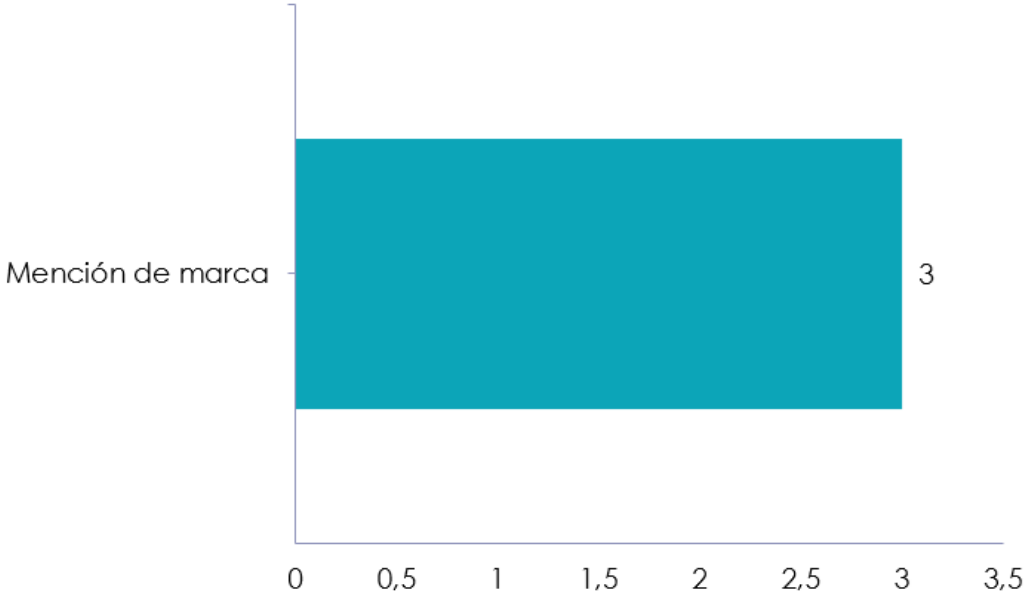
Histórico > Evolución del servicio a nivel mensual

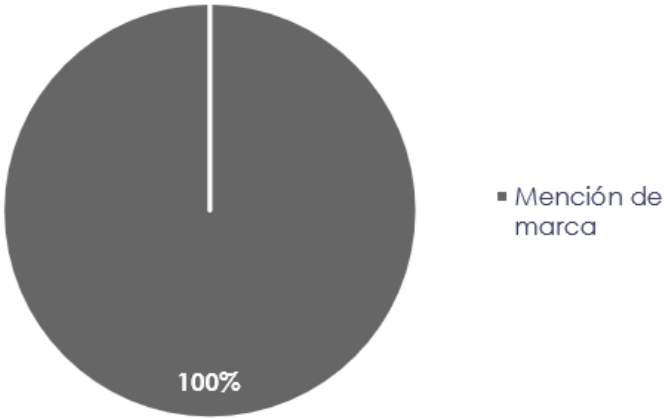




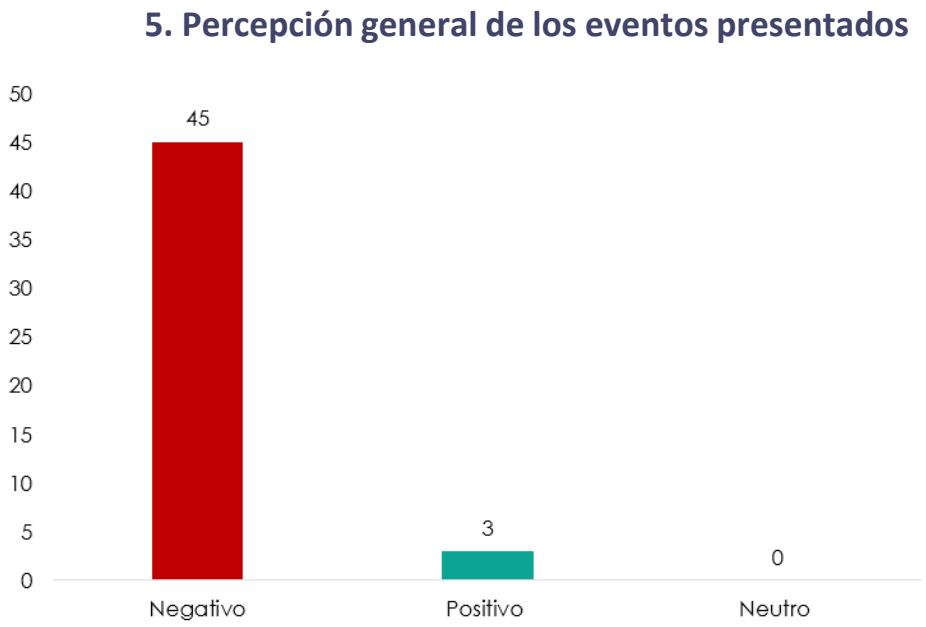
Resultados Monitoreo de marca

4. Menciones de marca





Resultados Monitoreo de marca



Para los eventos presentados durante el periodo en mención se identifica que la percepción **negativa** tuvo la mayor **afectación reputacional**, debido a los hallazgos relacionados **abusos de marca**.

Actividades realizadas

- Identificación y notificación de eventos
- Monitoreo de redes sociales
- Gestión de baja de contenidos fraudulentos o con abuso de marca
- Identificación de credenciales filtradas
- Ejecución de mediciones de marca
- Análisis de percepción de eventos presentados

Observaciones y conclusiones

Observación: se evidencia un aumento en el número de eventos identificados bajo la tipología abuso de marca relacionados con publicaciones ofreciendo servicios financieros a nombre de la entidad.

Recomendación: Hacer campañas de concientización y difusión de los riesgos que representan este tipo de servicios con el fin de reducir la efectividad de este tipo de amenazas.

Observación: Se evidencia que la percepción de la entidad en redes sociales fue principalmente “negativa”, debido a los eventos que representaron un riesgo reputacional a la organización y sus servicios.

Informe Seguridad Ofensiva

2024

0
Ethical Hacking

0
Retest Ethical Hacking

7
Retest Análisis de Vulnerabilidades

5
Análisis de Vulnerabilidades

1
Ingeniería Social

Objetivo

Presentar como parte del proceso de aseguramiento de la plataforma tecnológica los resultados de los escaneos de vulnerabilidades realizados sobre los equipos antes de que estos salgan a producción y realizar la correspondiente revisión una vez sean mitigadas las vulnerabilidades encontradas.

Objetivos específicos

- Presentar las solicitudes recibidas y atendidas durante el periodo.
- Presentar las vulnerabilidades más relevantes.
- Identificar recomendaciones de mejora de acuerdo con los datos analizados.
- Presentar conclusiones relevantes.

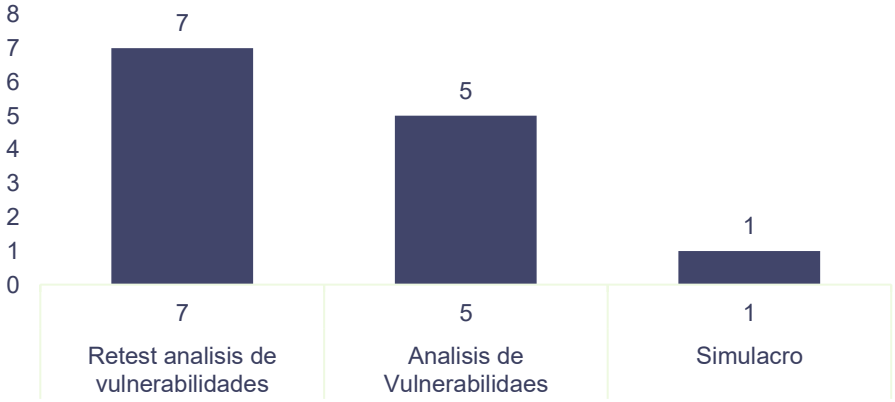
Alcance

Exponer los eventos identificados en el servicio de aseguramiento ejecutado por SOC-CERT de Mnemo Colombia durante el periodo comprendido entre el 22 de marzo hasta el 21 de abril del año 2024.

Resultados de solicitudes (Retest) y Análisis de vulnerabilidades (AV)

Durante el periodo, se documentaron un total de **13** solicitudes y una solicitud de AV. Se evidencia una disminución de **6** solicitudes respecto al periodo anterior, como se ilustra en el gráfico adjunto.

Cantidad de solicitudes, por categorías (análisis de vulnerabilidades, retest) entre otros.

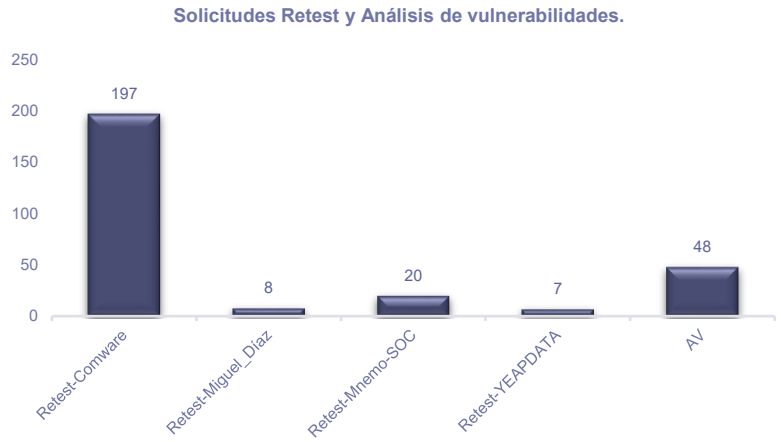


Para el periodo reportado, se ejecutaron 7 solicitudes acerca de Retest referentes a análisis de vulnerabilidades (RAV 5 análisis de vulnerabilidades y 1 simulacro cibernetico.

Resultados de solicitudes (Retest y AV)

Resultados Retest - General

Resultados – De los retest solicitados fueron reportadas **232** vulnerabilidades para su respectivo escaneo y validación. En cuanto a los análisis de vulnerabilidades se identificaron 48 hallazgos. Las actividades se muestran a continuación:



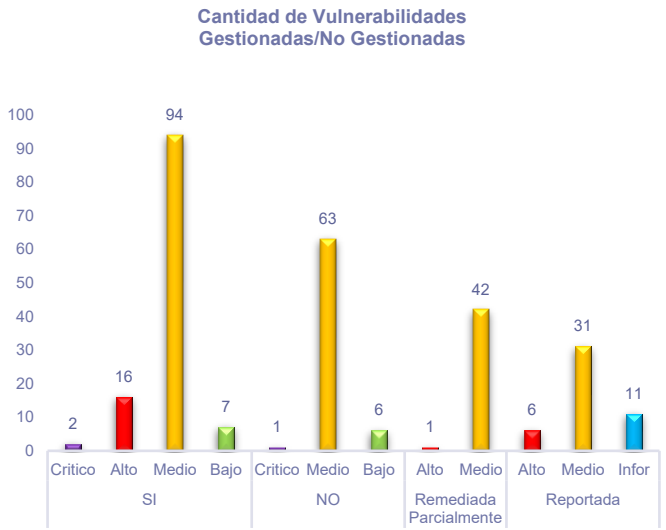
Resultados – A continuación, se muestra el porcentaje por nivel de criticidad de las vulnerabilidades de retest y de los escaneos iniciales reportadas en las actividades, se organizan desde las más críticas llegando a las bajas.

Impacto	Cantidad
Critico	3
Alto	23
Medio	230
Bajo	13
Informativo	11
Total	280

Resultados de solicitudes (Retest y AV)

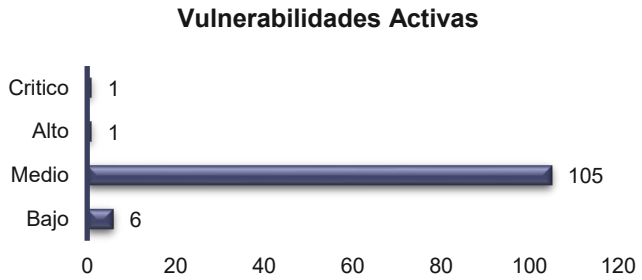
Resultados Retest y Análisis de Vulnerabilidades Remediadas - General

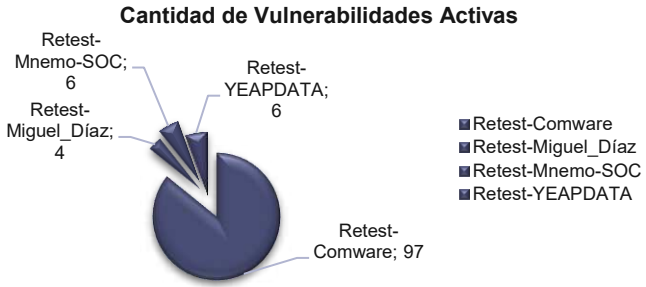
De las **232** vulnerabilidades reportadas en los re-test, **119** fueron remediadas y **70** continúan activas, 43 remediadas parcialmente y 48 vulnerabilidades nuevas reportadas de los AV. Se recalca que dentro de las vulnerabilidades **remediadas** hay unas de impacto **crítico**, alto, medio y bajo.



Estado	Cantidad
SI	119
Critico	2
Alto	16
Medio	94
Bajo	7
NO	70
Critico	1
Medio	63
Bajo	6
Remediada Parcialmente	43
Alto	1
Medio	42
Reportada	48
Alto	6
Medio	31
Informativo	11

Es de resaltar que, en los retest del periodo reportado, **solo se evidencia** una **vulnerabilidad** de nivel **crítico activa**, y una **alta.**

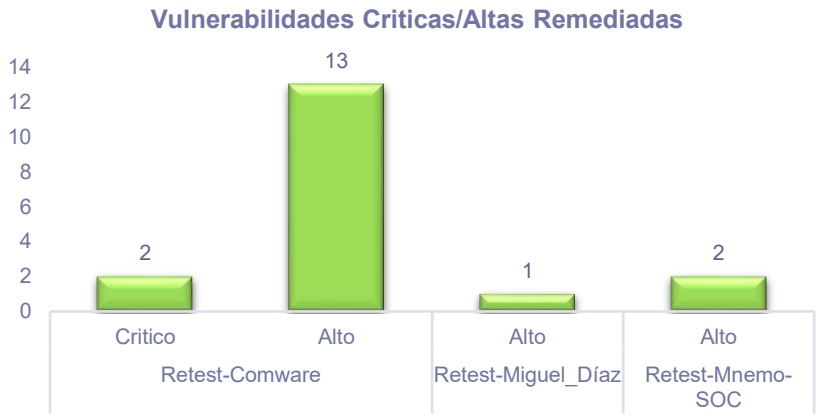




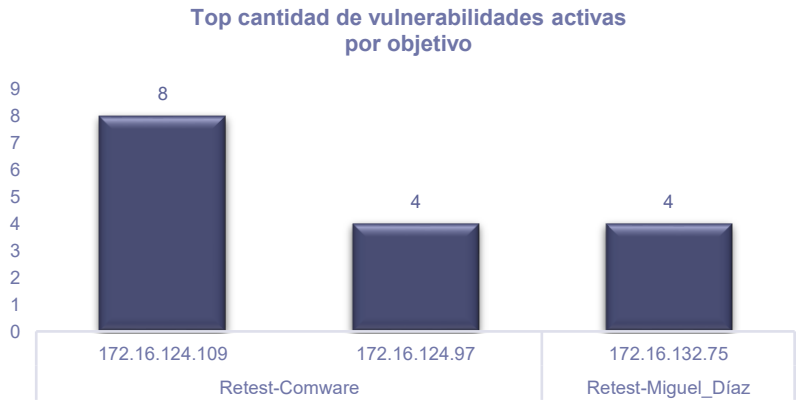
Resultados de solicitudes (Retest y AV)

Resultados Retest AV Remediadas - General

De las 119 vulnerabilidades remediadas se destaca la efectividad de solución de las críticas y altas.



Del total de **vulnerabilidades activas (70)** los activos que se destacan con **más vulnerabilidades** es el **172.16.124.109 (8 vuln), 172.16.132.75 (4 Vuln) y 172.16.124.97 (4) Vuln**, estos activos corresponden al proveedor Comware y Miguel Diaz.



Resultados de solicitudes Análisis de vulnerabilidades (AV)

Resultados Análisis de vulnerabilidades - General

A continuación, se presenta el resultado de los análisis de vulnerabilidades ejecutados en el mes de abril.

Vulnerabilidad	Afectados
SSL Certificate Cannot Be Trusted	5
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	4
SSL Medium Strength Cipher Suites Supported (SWEET32)	4
TLS Version 1.1 Protocol Deprecated	4
SSL Self-Signed Certificate	4
TLS Version 1.0 Protocol Detection	4
SSL Certificate with Wrong Hostname	3
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	3
SSH Server Type and Version Information	1

Actividades realizadas

- Se ejecutó actualización de los plugins de nessus de manera semanal, los cuales sirven para identificar nuevas vulnerabilidades.

- Se ejecutan los siguientes ejercicios de retest de análisis de vulnerabilidades, los activos pertenecen a los siguientes proveedores encargados de la administración:

    - Re-test COMWARE (2)
    - Re-test YEAPDATA (1)
    - Re-test Mnemo (2)
    - Re-test Miguel Angel (2)

- Se ejecutan los siguientes ejercicios de análisis de vulnerabilidades:

    - 172.16.132.165
    - 172.31.1.120
    - 172.16.123.93
    - 172.16.133.9-172.16.123.9-172.16.123.17

Recomendaciones y conclusiones

- Se enviaron un total de 74 hosts para llevar a cabo las validaciones de retest del análisis de vulnerabilidades, identificándose un total de 17 vulnerabilidades únicas en el proceso.
- La vulnerabilidad que afecta al mayor número de activos (4) es "SSL Medium Strength Cipher Suites Supported (SWEET32)", clasificada como de alto impacto, seguida por "SSL Certificate Cannot Be Trusted", la cual afecta a (4) activos y se considera de nivel medio en cuanto a su criticidad.
- Se destaca el enfoque dedicado en abordar las vulnerabilidades. En este período, se realizó una revisión exhaustiva de 232 vulnerabilidades, lo que resultó en la resolución de 162 de ellas. En la actualidad, solo persisten activas 70, lo que implica una reducción significativa del 30% en el número total de vulnerabilidades identificadas.
- Es importante señalar que de las 70 vulnerabilidades restantes, una se clasifica como crítica y ninguna como alta, lo que refleja el firme compromiso con la seguridad de los activos.
- Implementar estrategias para atender las vulnerabilidades de impacto medio y bajo: Elaborar un plan detallado que describa las acciones a seguir para solucionar cada vulnerabilidad detectada. Priorizar estas vulnerabilidades en base a su impacto y gravedad, estableciendo plazos viables para su corrección.

Informe de Actividades Qualys módulo SCA

2024

Resumen Ejecutivo

En este informe se presenta un resumen de las actividades y resultados del módulo SCA (Security Configuration Assessment) de la plataforma Qualys durante el periodo comprendido entre el 22 de marzo y el 21 de abril.

Objetivos

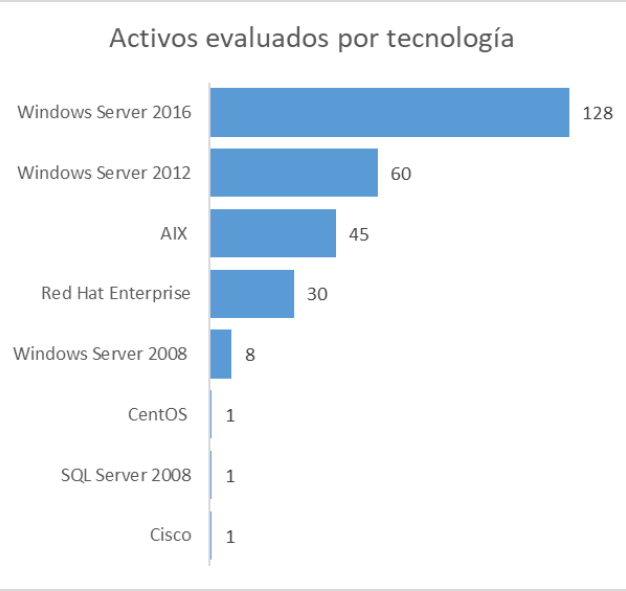
- Evaluar los controles comprendidos en las 13 políticas desplegadas.
- Analizar el nivel de riesgo que representa el incumplimiento de los controles de seguridad planteados por el CIS.
- Presentar un insumo de valor para la toma de decisiones en cuanto a la aplicación de controles de seguridad en los activos tecnológicos.
- Cumplir con estándares y regulaciones de seguridad de la información.

RESUMEN GENERAL

284	25	2	9	13	1.506
Activos evaluados	Activos duplicados	Activos sin controles	Activos sin conexión en un mes	Políticas evaluadas	Controles evaluados

62,47%
Controles superados

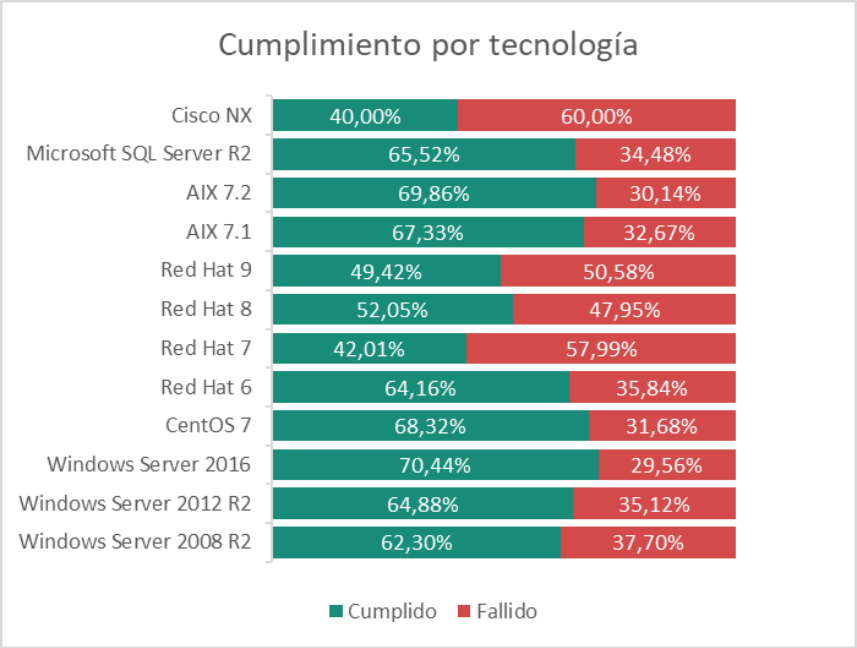
37,53%
Controles fallidos

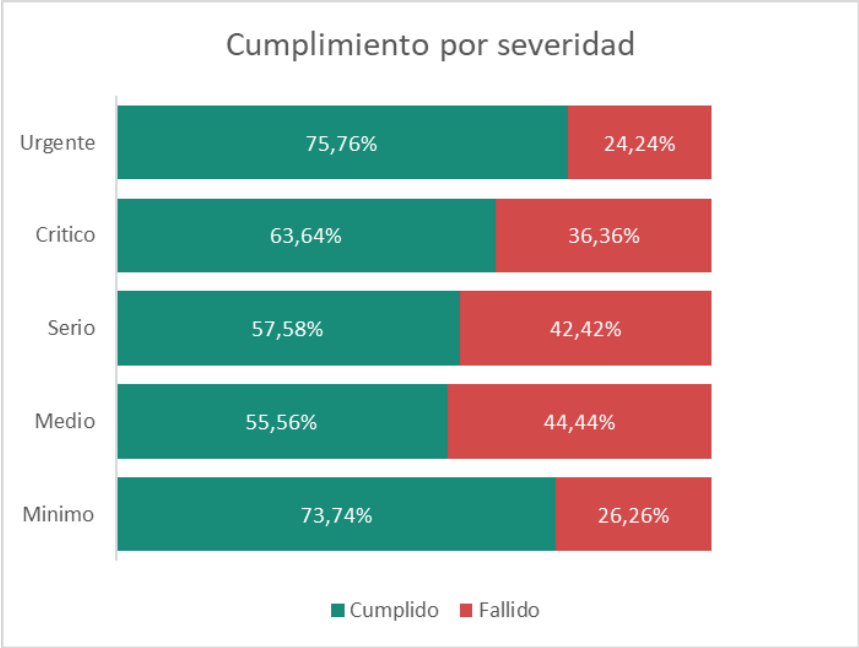


CONTROLES EVALUADOS POR POLÍTICA

CIS Benchmark for CentOS Linux 7	483
CIS Benchmark for Microsoft Windows Server 2008 R2	266
CIS Benchmark for Microsoft Windows Server 2012 R2	348
CIS Benchmark for Microsoft Windows Server 2016	324
CIS Benchmark for Red Hat Enterprise Linux 6	279
CIS Benchmark for Red Hat Enterprise Linux 7	459
CIS Benchmark for Red Hat Enterprise Linux 8	491
CIS Benchmark for Red Hat Enterprise Linux 9	477
CIS IBM AIX 7.1 Benchmark	246
CIS IBM AIX 7.2 Benchmark	218
CIS Microsoft Windows Server 2016	377
CIS Benchmark for Cisco NX	10
CIS Microsoft Windows Server 2016	29

EVALUACIÓN DE LÍNEAS BASE





De acuerdo a las gráficas anteriores, se puede evidenciar que más del 50% de los controles se encuentran en cumplimiento, sin embargo, existe una cantidad importante de controles en estado no superado los cuales deben ser verificados con el fin de validar si el criterio de evaluación es el correcto o por el contrario se debe ajustar la configuración en cada carga de trabajo.

CONCLUSIONES Y RECOMENDACIONES

- Se debe tener en cuenta que al momento de reinstalar un sistema operativo o revertirlo a un estado anterior (snapshot), el sistema origen pierde cualquier parche instalado o configuración realizada, causando así, por ejemplo, la reapertura de vulnerabilidades que se habían dado por cerradas

- De los 255 dispositivos de red listados e incluidos en el control de cambios C55236 solo 3 fueron alcanzados por el Appliance, de estos 3, solo en el dispositivo de pruebas fue exitosa la autenticación con el usuario UserQualys, esto es debido a que el usuario no estaba habilitado en todos y la IP del Scanner Appliance de Qualys no se encuentra en los ACL de los dispositivos de red

- Los dispositivos de red Wireless AP no permiten conexión SSH, son controlados desde 172.168.4.4, 172.17.4.7 y 172.17.4.8

- Las IPs 172.16.132.55, 172.16.123.32, 172.16.123.173, 172.16.127.96, 172.16.123.126, 172.16.123.222, 172.16.132.75, 172.16.128.44, 172.16.128.21 no reportan actividad hace más de un mes, se recomienda indagar en conjunto la causa

GESTIÓN PLATAFORMA – ACTIVIDADES REALIZADAS

- Se realizó revisión semanal para revisar el estado de los agentes en su etiquetado, duplicidad y última conexión
- Se identificaron los agentes que llevan más de un mes sin reportar conexión
- Se llevó a cabo sesión de acompañamiento para definir la causa del no alcance y autenticación fallida en los dispositivos de red
- Creación de caso (SD1068868) para la habilitación de UserQualys en todos los dispositivos de red (plataformas seguridad, seguridad/virtual, wireless y telefonía), este se encuentra cerrado, usuario de solo lectura creado
- Creación de control de cambios para que sea anexada la IP del Scanner Appliance de Qualys (172.16.125.65) a las ACL de los dispositivos de red, (C58046) actualmente en fase de implementación
- Envío de enlace de acceso a tablero de control vía correo electrónico a buzón AGHernandez@fna.gov.co, aún a espera de retroalimentación
- Mejoras en tablero de control para presentar información detallada de cumplimiento

Fortify SCA

Informe de Actividades y Funcionamiento Fortify

2024

Resumen Ejecutivo

En este informe se presenta un resumen de las actividades y el funcionamiento de la plataforma de análisis de código Fortify durante el período comprendido entre el 22 de marzo y el 21 de abril.

Objetivos

- Mejorar la calidad del código.
- Identificar y corregir vulnerabilidades de seguridad.
- Facilitar la colaboración entre equipos de desarrollo.
- Optimizar el proceso de revisión de código.
- Cumplir con estándares y regulaciones de seguridad de la información.

Gestión y actividades

Actividad General:

- Durante este periodo, no se realizó actividad de análisis de códigos en activos ni se llevaron a cabo ejecuciones de análisis ni generación de informes correspondientes.

Integraciones y Automatizaciones (Desarrollos):

- No se realizaron actividades de desarrollo en este periodo.

Rendimiento y Disponibilidad:

- A pesar de la activación de la suite de Fortify, hubo contratiempos en su funcionamiento debido a dificultades al cargar el sensor de la herramienta.
- No se presentó tiempo de inactividad programado o no planificado y el rendimiento del sistema se mantuvo dentro de los parámetros normales durante períodos de carga máxima.

Planes para futuras mejoras o actualizaciones:

- Se están gestionando nuevas licencias, IPs, nombres de hosts y backup para DB como parte de la migración de la solución de Fortify.
- Se tiene la expectativa de progresar en el proceso de migración hacia una nueva infraestructura, incluyendo la implementación de controles de cambio y la gestión de las solicitudes necesarias.

Gestión y actividades

- **Monitoreo del sistema:**
  Se realiza una verificación periódica del estado de cada servidor que alberga la suite de Fortify.
  Fortify Source Code Analyzer (SCA): Se asegura de que el Rulepack de los módulos Audit Workbench y SSC estén actualizados.
  Software Security Center (SSC): Se valida el funcionamiento del módulo SSC, se accede a varios de los módulos del portal.
  Fortify WebInspect Enterprise (WIE): Actualmente, el sensor está experimentando problemas debido a las nuevas políticas de GPO implementadas en el servidor. Se está gestionando un control de cambios para llevar a cabo la migración de la suite a una nueva infraestructura.
  Fortify WebInspect Sensor (WIS): Se verifica el estado de conexión con la base de datos y se confirma que la conexión es satisfactoria.
- **Gestión de usuarios y permisos:**
  Se validan los permisos y roles de los usuarios creados en la plataforma, además se verifica que sean los autorizados.
- **Seguimiento de actualización nuevas versiones de Fortify y sus componentes:**
  Se comprueba el funcionamiento de actualización de los rulepacks de los módulos AudithWorkBech y SSC.
  Actualmente se encuentra la versión 23.2 publicada en la página del fabricante, se están gestionando los controles de cambios y solicitudes necesarias para proceder con la migración y realizar una instalación del producto a su última versión.

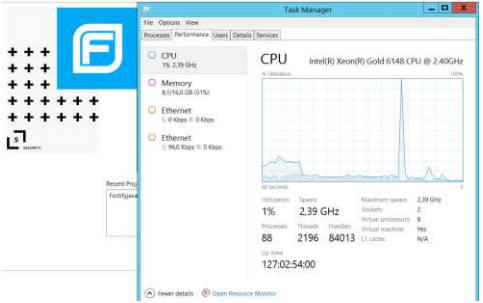
Actividades realizadas

- 02/04/2024: Se crea el caso RF389418 solicitando respaldo completo de los 4 servidores de la suite de Fortify. El día 8 de abril fue confirmada la finalización de la solicitud.
- 11/04/2024: Se crea caso SD1071289 para el reinicio de contraseña del usuario APL-Fortify.
- 18/04/2024: Se crea caso SD1074050 para el traslado del Backup BD Fortify al nuevo servidor de base de datos.
- 18/04/2024: Se crea control de cambios C58263 para iniciar la migración de la suite de Fortify.

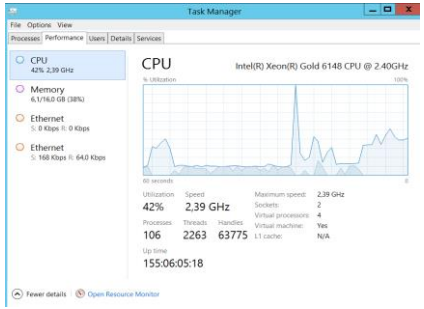
Disponibilidad y rendimiento del sistema.

A continuación, se muestra la disponibilidad de los servidores correspondientes al periodo.

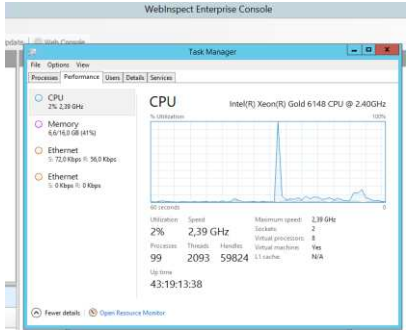
172.16.132.101



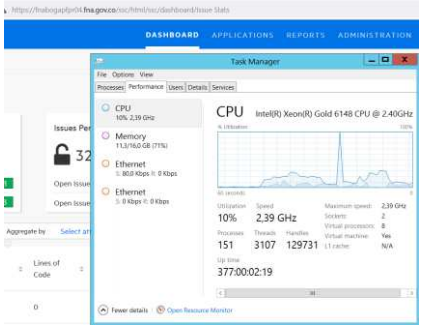
172.16.132.102



172.16.132.103



172.16.132.104



Conclusiones

- Durante el periodo actual, se notó una actividad constante en términos de análisis de códigos en activos y la generación de informes en comparación con el periodo anterior.

- Se llevaron a cabo actividades de solicitud de backup y copias de respaldo para la planificación de la migración de la solución.

- A pesar de los desafíos encontrados con la suite de Fortify al cargar el sensor, el sistema se mantuvo disponible y su rendimiento durante los períodos de carga máxima fue normal. Se están gestionando el control de cambios y los casos necesarios para la migración a la nueva infraestructura.

Recomendaciones

- Continuar monitoreando y evaluando el rendimiento y la disponibilidad de la suite de Fortify, así como abordar proactivamente cualquier dificultad que surja con el sensor o cualquiera de los otros componentes.

- Priorizar la resolución de los temas recurrentes identificados en las consultas de soporte, garantizando una gestión eficiente y satisfactoria para los servidores de la solución fortify.

- Proseguir con las actividades de gestión planificadas, como la migración de la suite de Fortify, asegurando una adecuada planificación y coordinación entre los equipos involucrados.

- Mantener un enfoque en la gestión de copias de respaldo, control de cambios y la realización de pruebas para garantizar la integridad y disponibilidad de los datos en la suite Fortify.

Informe Soluciones Antimalware

2024

Objetivo

Presentar en detalle los eventos de disponibilidad, actividades e incidentes registrados en la operación y administración de Mnemo sobre las plataformas de seguridad Trellix y Trend Micro pertenecientes al Fondo Nacional del Ahorro para el periodo de 22 de abril al 21 de mayo del 2024 .

Las actividades desarrolladas por parte de Mnemo corresponden a la gestión para la administración de las plataformas de seguridad que se encuentra en producción actualmente tanto de Trend Micro como de Trellix.

Alcance

Exponer los eventos identificados y gestión en el servicio de las soluciones antimalware gestionadas por Mnemo Colombia durante el periodo comprendido entre el 22 de abril hasta el 21 de mayo del año 2024.

Estadísticas Generales de detección

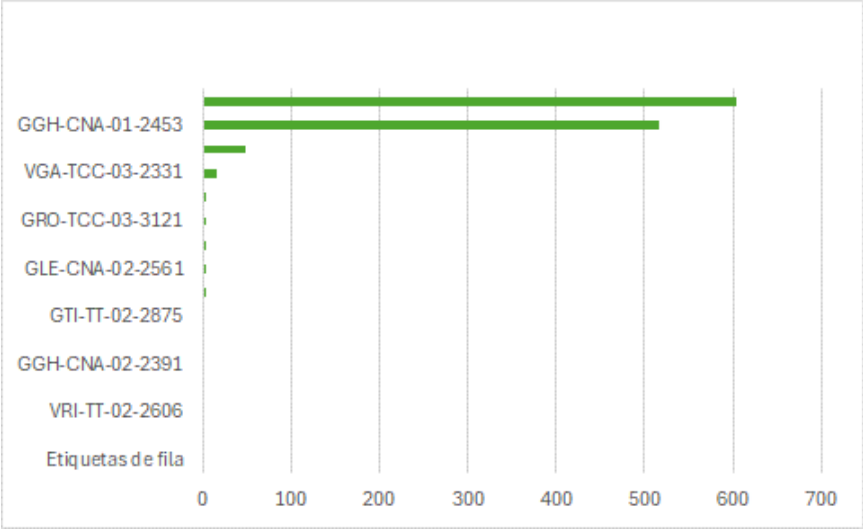
Detecciones en puntos finales Trellix

Se evidencian un total de 604 eventos de amenazas gestionados por Trend Micro, en su mayoría es por la detección por la regla Possible_Hifrm-6 que detecta frames embebidos dentro de archivos que pueden redirigir a posibles URLS Maliciosas, se valida los eventos y se detecta que en su mayoría corresponde al usuario FNA2\mrojasm que genera archivos PDF detectados por la regla.

Eventos por nombre de amenaza	
Etiquetas de fila	**Cuenta de Virus/Malware**
Backdoor.MSIL.REMCOS.SM	1
Trojan.PDF.FRS.VSNW16I23	1
Eicar_test_file	1
Trojan.Win32.MALINEX.SMA	1
WORM_NUWAR.RAR	1
Worm.LNK.DORKBOT.SM23	1
TROJ_GEN.R002C0DDU24	2
TROJ_FRS.VSNTL423	2
TROJ_GEN.R002C0PFB21	2
BKDR_XTRAT.XYC	2
Trojan.HTML.IFRAME.JCFASHF	3
BKDR_NOANCOOE.SMMSC	4
TSC_GENCLEAN	4
Possible_Hifrm-6	579
Total general	604

Top de equipos con mayor cantidad de detecciones

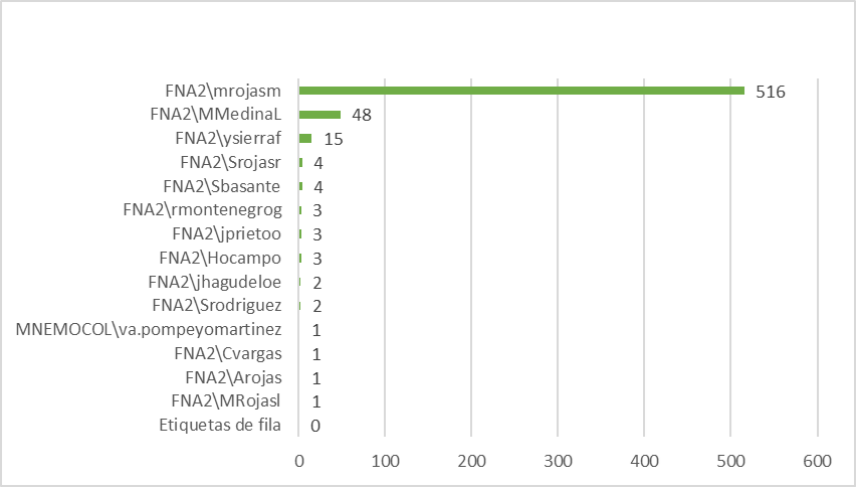
En el top de equipos se encuentra GGH-CNA-01-2453 por la misma detección de Possible_Hifrm-6 e nsegurndo lugar se encuentra también por el mismo tipo de detección, pero el usuario es MMedinaL de la misma área que mrojasm Gre Gestion Humana, por lo que se puede tratar de una aplicación o archivo que este generando el evento.



Estadísticas Generales de detección

Top de usuarios con mas eventos.

En el top de usuarios se encuentra MMedinaL y mrojasm relacionado con las mismas detecciones **Possible_Hifrm-6**



Conexiones sospechosas

Este módulo identifica, archivos o conexiones nuevas, que resultan sospechosas dentro de los equipos. Para este periodo se identificaron 1325 archivos, la mayoría identificados con el archivo mac.exe este fue excluido de las políticas para que no sea bloqueado, ya que pertenece a una herramienta utilizadas por los usuarios del FNA.

Archivos sospechosos	
Path	count
C:\$Recycle.Bin\S-1-5-21-1472853535-1591411291-823966058-14075\$RDKTZ5S\mac.exe	19
C:\$Recycle.Bin\S-1-5-21-1472853535-1591411291-823966058-4016\$RFUV256\mac.exe	20
C:\Users\cparedes\Desktop\mac.exe	23
C:\Users\DDUFFIS\Desktop\mac.exe	24
C:\COBIS\Produccion64\mac.exe	27
C:\Users\amrincon\Desktop\mac.exe	29
C:\Users\ytirado\Desktop\mac.exe	45
C:\mac (1)\mac.exe	164
C:\Soporte\MAC.zip	192
C:\Soporte\mac.exe	255

Estadísticas Generales de detección

URLS Sospechosas

Dentro de las urls sospechosas por el módulo, se encuentran las listadas en la tabla inferior, de estas se validan en virus total, se encuentran “api.startservicefounds[.]com” y start.apistatexperience[.]com calificadas como maliciosas, las otras dos no tienen detecciones

URL Sospechosas	
Etiquetas de fila	Cuenta de Object
http://api.startservicefounds.com:443/service/sort.js	1
http://etcohome.us17.list-manage.com:443/track/click?u=37a782eb0edbdb702a900e028&id=36e9418699&e=41dc1943ac	1
http://start.apistatexperience.com:443/scripts/cdn.js	1
http://www.sero.com.co:443/	1
Total general	4

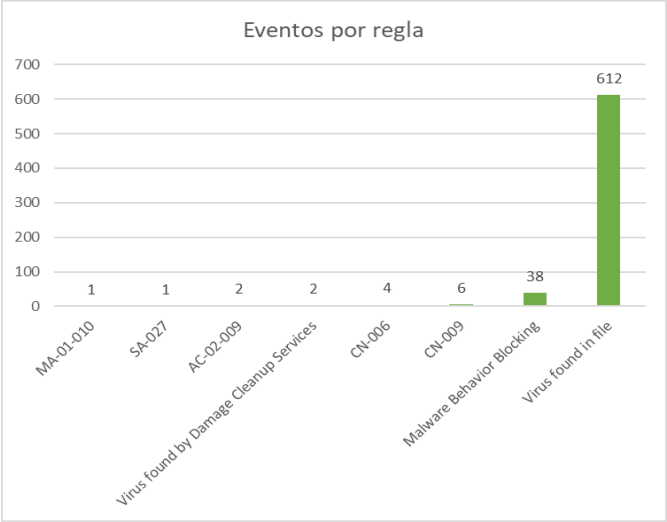
Eventos por grupo organizacional

En la cantidad de eventos por grupo en el árbol de sistemas, se puede ver que el grupo que mayor cantidad de eventos genera es Gre Grestion Humana con 565 eventos, relacionados con la regla Possible_Hifrm-6 que detectó archivos pdf sospechosos

Estadísticas Generales de detección

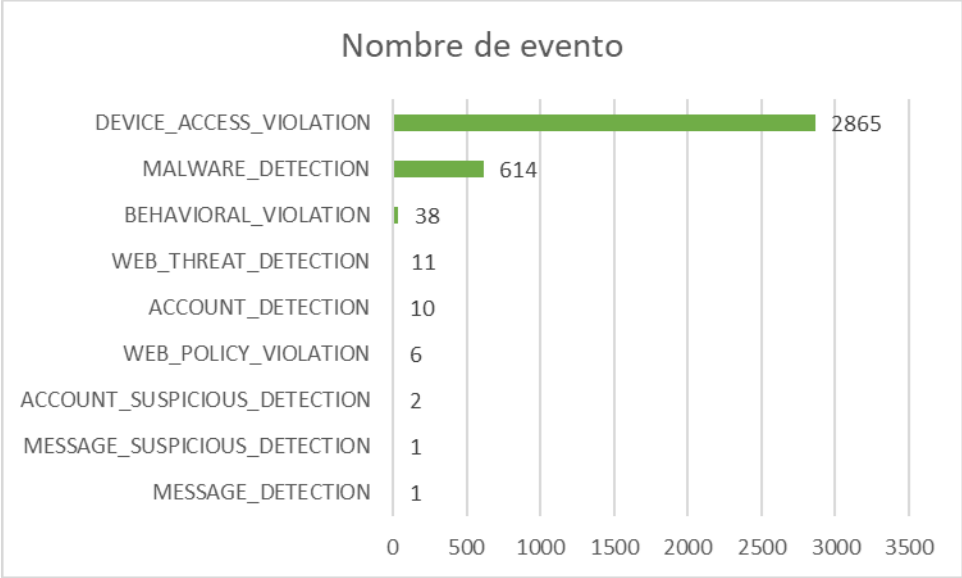
Top de eventos por regla XDR

Dentro del top de eventos de XDR por regla, se identifica la regla de virus en archivo, debido a las reglas de endpoint que detectan archivos con contenido de urls sospechosas. Para la regla de detección de comportamiento se visualizan los eventos relacionados con los ejecutables mis.exe, mac.exe y varios setup.exe que se veían en las detecciones para endpoint.



Eventos por nombre de la detección XDR

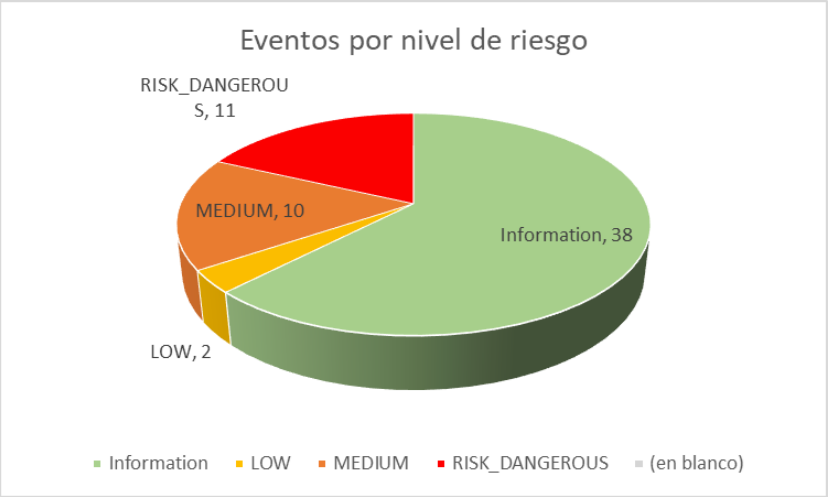
XDR se encuentra relacionado con todos los otros módulos de protección es por esto por lo que en los eventos por nombre la mayor cantidad, corresponde a las reglas de Device control, de usuarios que conectaron dispositivos no autorizados. En los eventos de malware se puede evidenciar bloqueos a sitios detectados como phishing.



Estadísticas Generales de detección

Eventos por nivel de riesgo

En los eventos por nivel de riesgo, identificados por XDR se identificaron 11 eventos con clasificación alta.



Workbench Events

El "Workbench de XDR de Trend Micro" es una aplicación que forma parte de la plataforma XDR (Detección y Respuesta Extendida) de Trend Micro. Esta herramienta permite a los clientes realizar detección y análisis de amenazas en múltiples capas de seguridad.
En lo eventos encontrados se encuentran 4 eventos en nivel medio y dos de nivel bajo

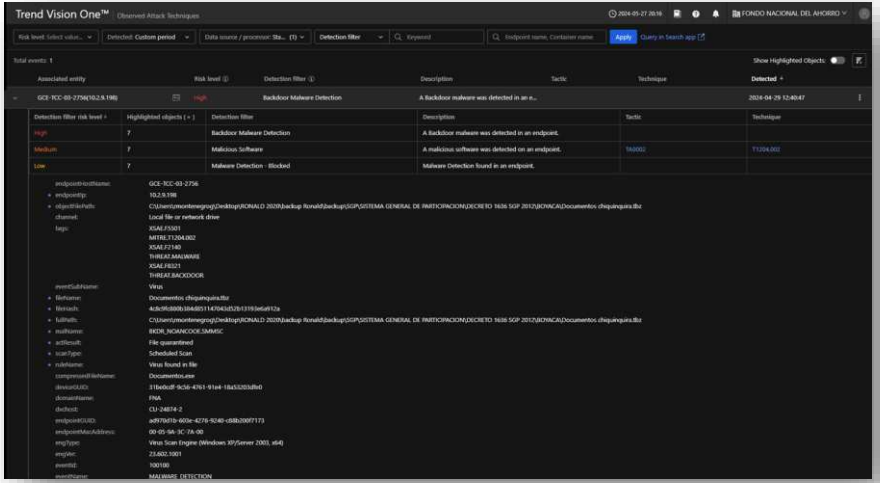
Dispositivo	cantidad de eventos
VRE-PA-BGA-3409	33
GLE-CNA-02-3879	34
GSE-TT-02-3324	34
VTT-TCC-04-2856	34
VRE-PA-BGA-3348	44
GES-TCC-04-3160	46
GTI-TT-02-2598	81
OIN-CNA-01-3495	107
GGH-CNA-01-2453	133
GLE-CNA-02-2423	599

Estadísticas Generales de detección

MALWARE_DETECTION

Dentro de las detecciones se encuentra la detección de malware dentro de archivo tipo .tbz, que fue puesto en cuarentena por las herramientas antimalware.

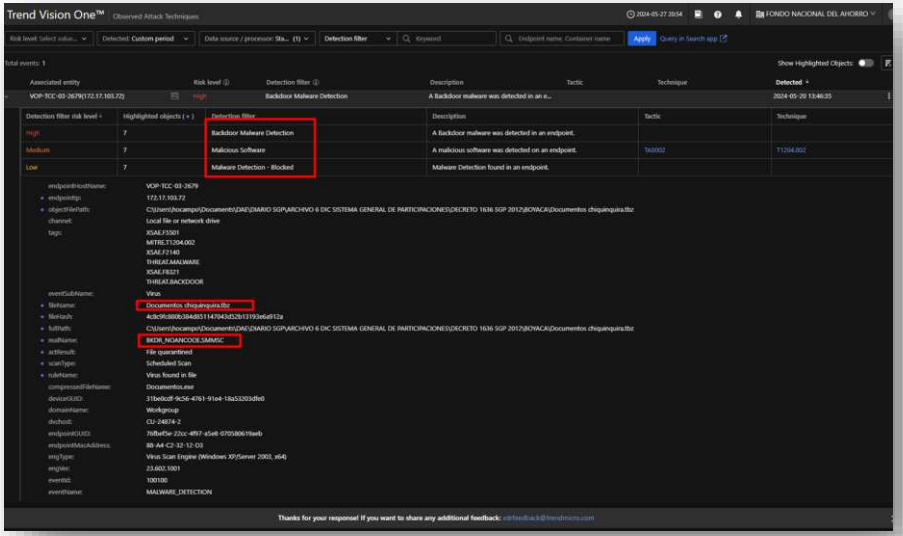
- C:\Users\rmontenegrog\Desktop\RONALD 2020\backup Ronald\backup\SGP\SISTEMA GENERAL DE PARTICIPACION\DECRETO 1636 SGP 2012\BOYACA\Documentos chiquinquira.tbz
- MALWARE_DETECTION
- 4c8c9fc880b384d851147043d52b13193e6a912a
- File quarantined



Estadísticas Generales de detección

MALWARE_DETECTION

Adicional un evento relacionado, con el reporte de una detección por parte del SOC. Esta contenía IOC por lo que fue detectado como posiblemente maliciosa WB-35600-2024042900001. El evento IC-35600-20240423-00000 corresponde al intento de desactivación de antivirus en el servidor FNABOGDLP, el evento WB-35600-20240520-00000 corresponde a un evento de clasificación alta por la ejecución del archivo C:\Users\hocampo\Documents\DAE\DIARIO SGP\ARCHIVO 6 DIC SISTEMA GENERAL DE PARTICIPACIONES\DECRETO 1636 SGP 2012\BOYACA\Documentos chiquinquira.tbz que contenía un Backdoor “BKDR_NOANCOOE.SMMSC” y fue puesto en cuarentena.

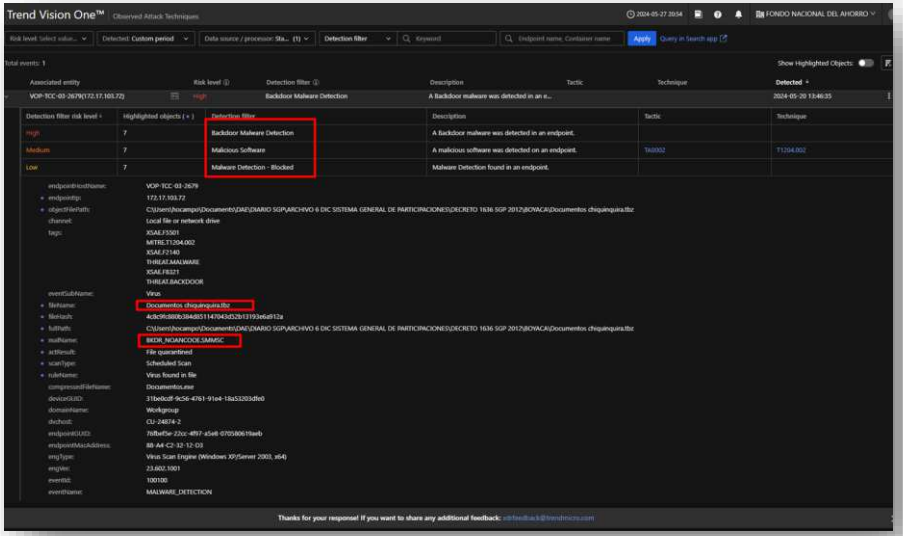


Estadísticas Generales de detección

MALWARE_DETECTION

El evento WB-35600-20240504-00000 se bloque ya que fue detectado como troyano, al detectarse código malicioso

- C:\Users\jprietoo\AppData\Local\Mozilla\Firefox\Profiles\tu9rjugq.default-release\cache2\entries\E2DDFEB0B15B024F1B45FC4014DF98E7F7A415A6
- Trojan.HTML.IFRAME.JCFASHF
- e51699e30d3e3b09f4643402d24691ce3f48c5a2
- Moved



Estadísticas Generales de detección

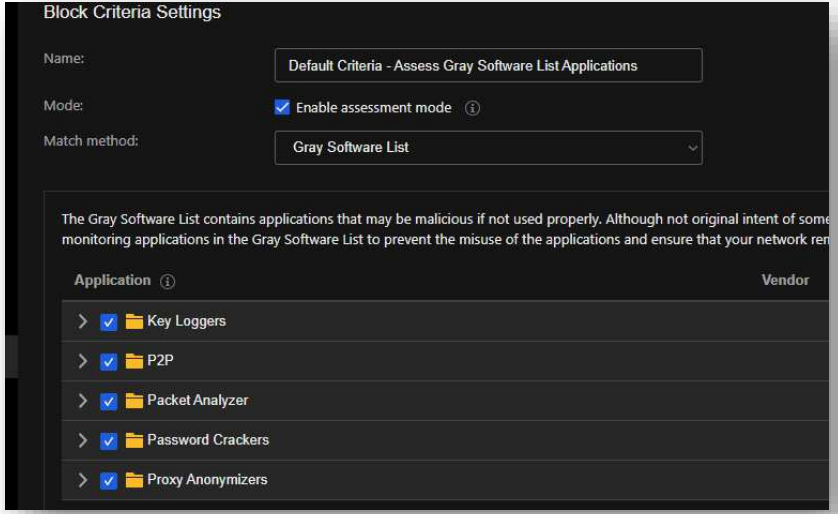
Application Control

Dentro de los eventos generados, se bloqueó la ejecución de la aplicación AnyDesk, que estaba dentro de las aplicaciones a bloquear como prueba de la política, no se detectan aplicaciones dentro la lista de bloqueo.

Aplicaciones Bloqueadas	
Etiquetas de fila	**Cuenta de File**
u.exe	1
AnyDesk (1).exe	2
AnyDesk.exe	21
Total general	24

Application Control Policy

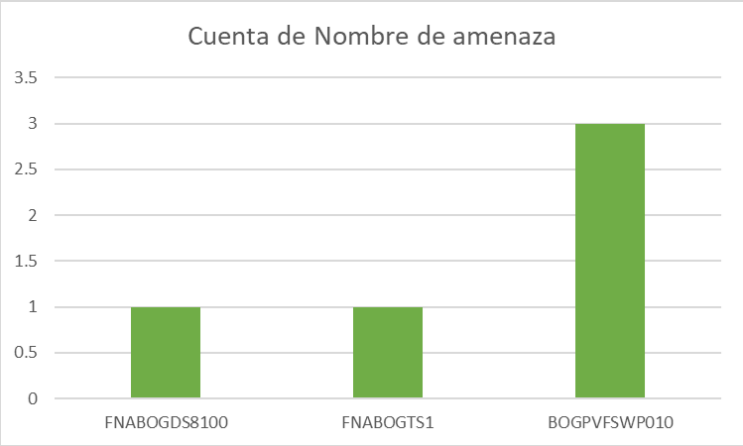
Dentro de la política se tiene configuradas las listas de aplicaciones con usos posiblemente maliciosos, que vienen por defecto en Trend Micro.



Estadísticas Generales de detección

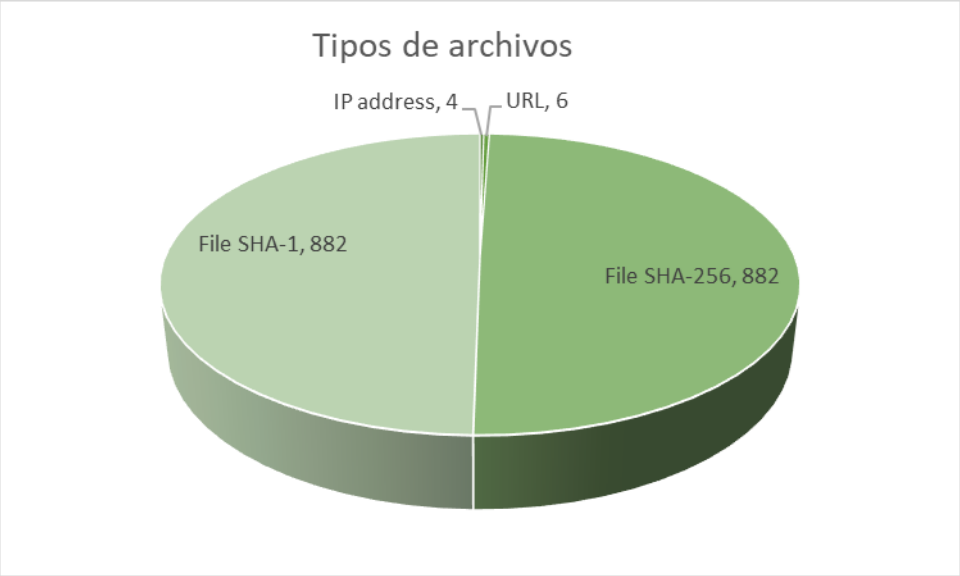
Eventos Servidores

Se generaron 5 eventos , el equipo con más eventos es BOGPVFSWP010 por la ejecución de archivos auto ejecutables “T1562.001 NT AUTHORITY\SYSTEM ran SYSTEM:REMOTE\SYSTEM:REMOTE, which tried to access the file T:\VpT&TransfDigit\2024\GciaSsTi&Infra\DocSrvrs\DOCUMENTACION_INFRAESTRUCTURA\COMPRIMIR\Escritorio\ProjectStd2013\x86\autorun.inf, violating the rule "Remotely creating autorun files", and was blocked. For information on how to respond to this event, see KB85494



Threat Intelligent

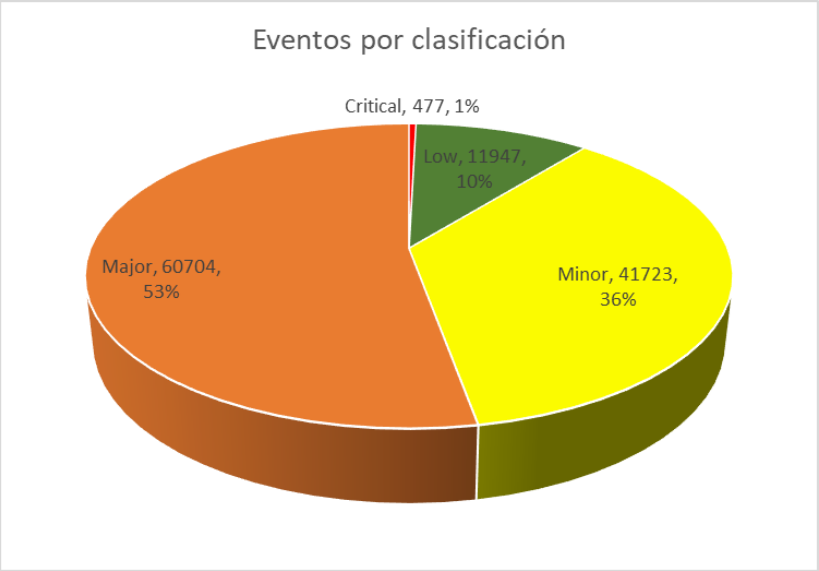
Se actualizo de 1774 archivos dentro de inteligencia de amenazas en su mayoría por Sha1 y SHA256.



Estadísticas Generales de detección

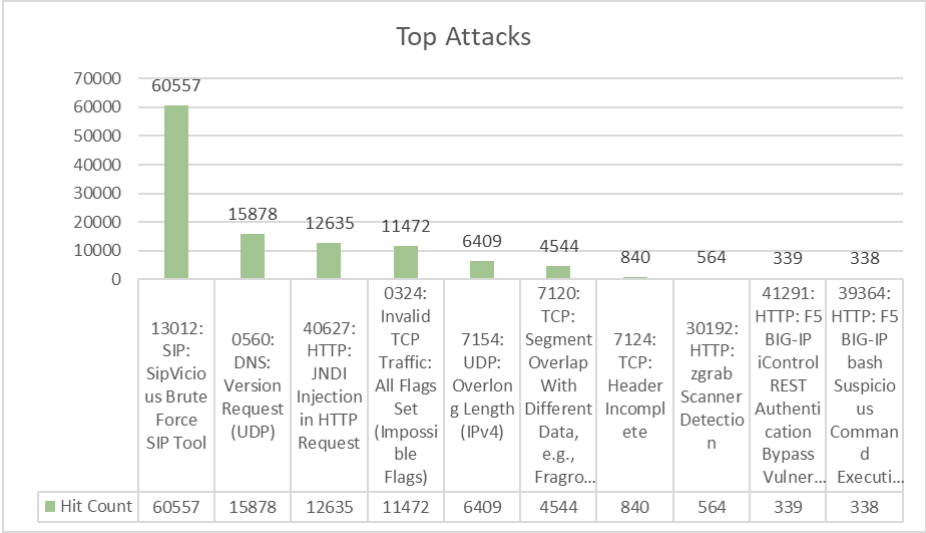
IPS Eventos por clasificación

Durante el periodo analizado del periodo de 22 de abril al 21 de mayo del 2024 , se encuentra el siguiente TOP de Eventos identificados por el IPS. Del total de los 114851 eventos, en su mayoría con clasificación major con el 53 % de los eventos



Top de ataques IPS

En el top de ataques se encuentra la regla 13012: SIP: SipVicious Brute Force SIP Tool, por el uso de herramientas SIPVICIOUS para realizar intentos de ataque por fuerza bruta, este evento registra el 53% del total. En segundo lugar se encuentra la regla 0560: DNS: Version Request (UDP). Este filtro detecta una solicitud para obtener el número de versión del servidor DNS Bind. El atacante utiliza la información de la versión para determinar si el servidor DNS es vulnerable a ciertos ataques de desbordamiento de búfer o de denegación de servicio.



Estadísticas Generales de detección

Top de origen de ataques

Top Source			
No.	Source IP Address	Country Name	Hit Count
1	185.243.5.55	Poland	23425
2	45.143.9.30	Unknown	9572
3	172.16.132.65	Unknown	9088
4	51.15.18.33	Netherlands	7707
5	64.112.75.2	United States	2599
6	159.192.106.207	Thailand	2521
7	46.101.113.210	Germany	2432
8	45.143.9.162	Unknown	2344
9	64.112.73.18	United States	2142
10	172.16.125.65	Unknown	2079

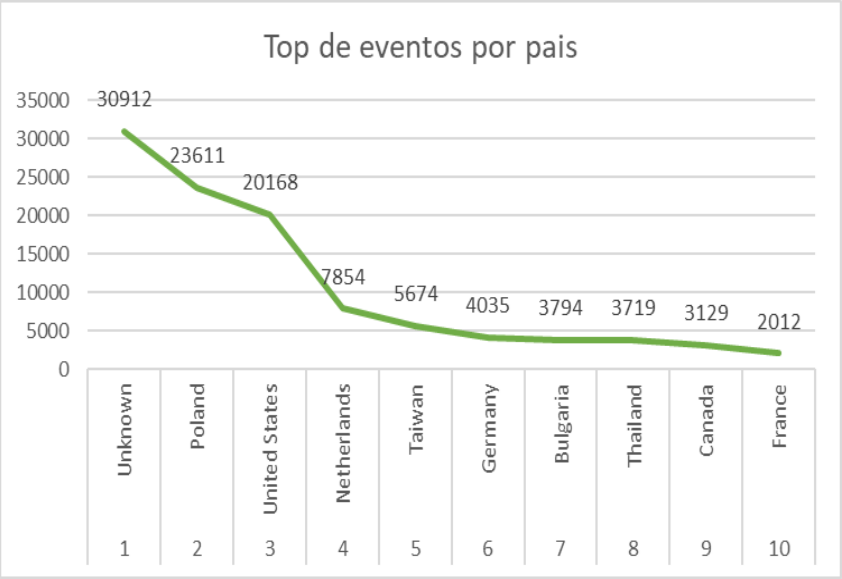
Top de destino de ataques

Top Destination			
No.	Dest IP Address	Country Name	Hit Count
1	179.1.9.97	Colombia	5027
2	179.1.9.100	Colombia	2328
3	179.1.9.99	Colombia	2312
4	190.90.95.170	Colombia	2265
5	179.1.142.165	Colombia	1675
6	179.1.9.104	Colombia	1521
7	179.1.9.102	Colombia	1516
8	179.1.9.103	Colombia	1508
9	179.1.9.107	Colombia	1484
10	179.1.9.108	Colombia	1478

Estadísticas Generales de detección

Top de paises detectados por IPS

En el top de eventos por país, se encuentra Polonia con mayor cantidad de registros, seguido de estados unidos y Holanda



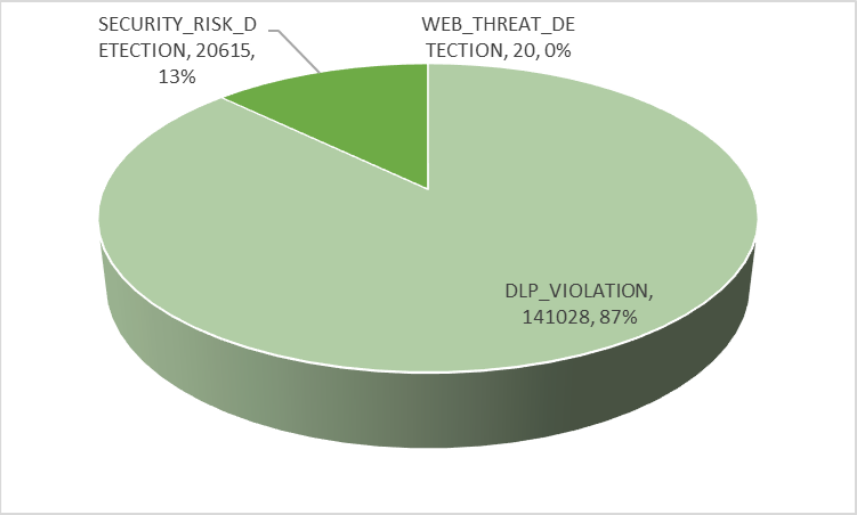
Top de eventos por política CASB

Para el periodo de 22 de abril al 21 de mayo del 2024 se presentaron un total de 141028 eventos registrados por la solución CASB, la política que tiene mayor cantidad de eventos es “Detección de Cedulas” con 61285 eventos.

Estadísticas Generales de detección

Top de eventos por regla CASB

Dentro de los eventos la mayoría corresponden a DLP, seguido de eventos de seguridad y amenaza web.



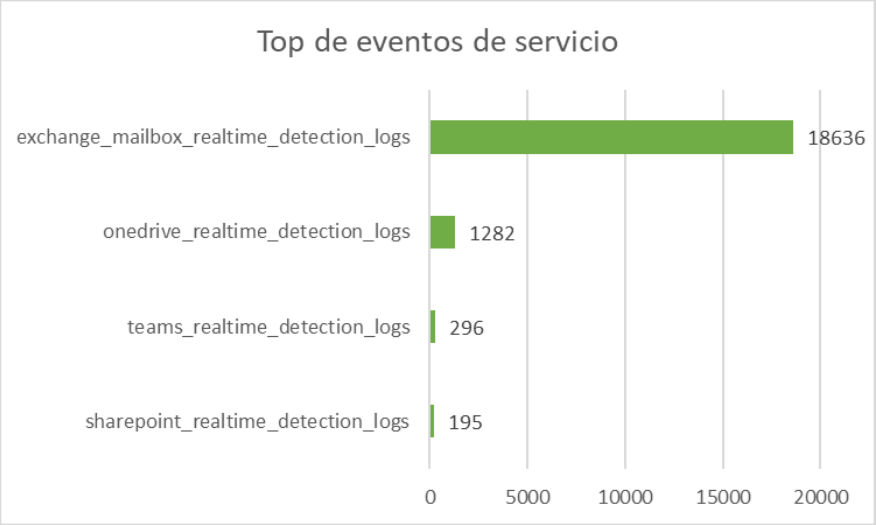
Filtros de detección CASB

En las detecciones los objetos, que mayor cantidad de registros genera por políticas de seguridad son adjuntos, seguido de archivos maliciosos dentro del cuerpo del correo y archivos.

Estadísticas Generales de detección

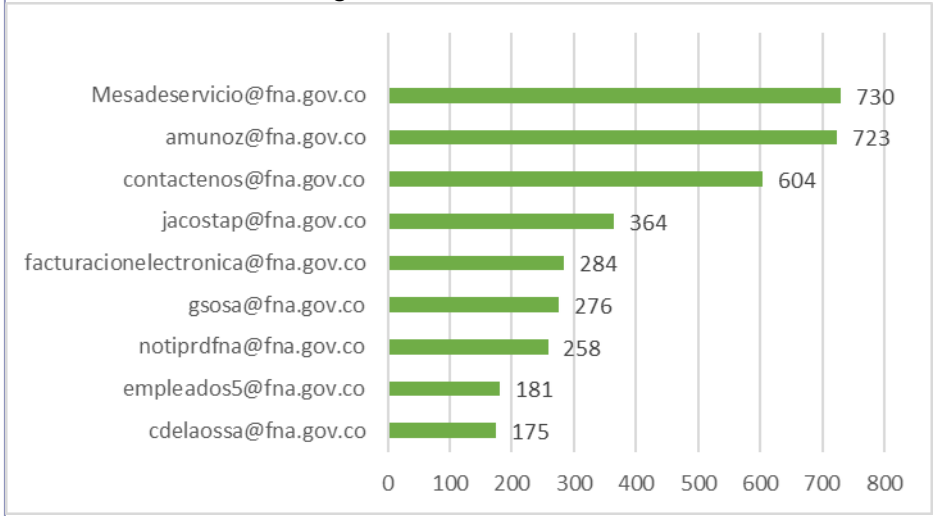
Top de eventos por servicio CASB

Exchange online y OneDrive, son los servicios que mayor cantidad de eventos, relacionados con archivos maliciosos registran.



Top de usuario con eventos de amenaza CASB

En el top de cuentas que mayor cantidad de eventos genera, son las cuentas de servicio Mesadeservicio@fna.gov.co, con 730 eventos, estos en su mayoría por recepción de correo de bloqueos de otros usuarios. El usuario amunoz@fna.gov.co tiene detecciones en su



Resumen y conclusiones.

De acuerdo con los eventos generados en las diferentes herramientas y la gestión diaria dentro del FNA se da el siguiente resumen de actividades y conclusiones.

- durante el periodo del informe se evidenciaron 604 eventos en dispositivos finales
- La mayoría de los eventos corresponden a la regla Possible_Hifrm-6 , se recomienda validar la regla para confirmar que no sean falsos positivos.
- En el dispositivo y el usuario con mayor cantidad de detecciones, se encuentra GGH-CNA-01-2453 y MMedinaL por la misma regla Possible_Hifrm-6
- para el módulo de conexiones sospechosas se encontraron 1325 archivos
- el archivo mac.exe y mis.exe fue detectado como sospechoso, pero se excluyó ya que corresponde a ejecutables del FNA
- Dentro de las URLS sospechosas se encuentra “api.startservicefounds[.]com” y start.apistatexperience[.]com
- el grupo Gre Grestion Humana con 565 eventos, es el grupo organizacional dentro de Vision One con mayor cantidad de eventos. Se recomienda validar, los procesos dentro de este grupo, para ver si es necesario crear exclusiones.
- Para XDR la regla que mayor detecciones género, es Virus encontrado en archivo, relacionado con la ejecución de pdf con conexiones sospechosas para el grupo de gre gestion humana
- Los eventos con mayor cantidad de registros son reglas de control de dispositivos. seguido de las reglas de malware.
- Se bloquearon diferentes urls relacionas con phishing, en total 11 eventos de clasificación alta.
- En los eventos de Workbench de XDR se generarón 6 eventos, tres relacionados con backdoor, uno de malware, uno de prueba con el archivo eicar y uno por la detección de intento de desactivación del antivirus.
- Para App control se evidenciaron 24 eventos, la mayoría de prueba sobre la aplicación AnyDesk.
- Se generaron 5 eventos , el equipo con más eventos es BOGPVFSWP010 por la ejecución de archivos auto ejecutables
- Se actualizo de 1774 archivos dentro de inteligencia de amenazas en su mayoría por Sha1 y SHA256.
- El ips detecto 114851 eventos a través de las reglas de detección, la mayoría con clasificación mayor.
- SipVicious Brute Force SIP Tool ocupo el top de eventos del ips con 53% de los eventos totales, seguido de 0560: DNS: Version Request (UDP)

- En el top de paises se encuentra Polonia con mayor cantidad de registros, se recomienda validar las reglas que se detectan hacia este país
- Caso con fabricante para validar errores con el despliegue en servidores, para lo cual se genera cambio para la salida a Trend por parte de los servidores.
- análisis de archivos recibidos por parte de la herramienta de sandbox
- Adicion permisos service Gateway C58336
- Adicion de permisos para la conexión de DDA Sandbox con servidores de actualización REF C56867
- Cierre de informes CASB
- migración de servidor IPS de Trellix a Trend Micro, se realiza de forma exitosa, se realiza aun validaciones sobre las reglas para mejorar la protección
- Despliegue de antivirus tanto en endpoints como en servidores al momento de generación del informe se cuenta con 1204 endpoints 146 servidores
- Cierre cambio C57964 Permisos de conexión Edge Gateway 172.16.132.34 hacia cloud Park IBM Qradar
- Cierre cambio C58336 Adicion de permisos para service Gateway y Server Workload security REF: C56714
- Creación cambio C58388 permisos IPS hacia TMC para descarga de actualizaciones.
- configuración de integración con SIEM de Tipping Point.
- Configuración Backup automático en SMS.
- Creación tarea T228232 Ejecución Despliegue antivirus Trend Micro servidores Productivos.
- envío informe implementación IPS de acuerdo a los anexos técnicos.
- cierre petición RF393468 bloqueo cobis
- respuesta caso RF393104 correo bloqueado
- Ejecución tarea RFT158282 jogonzaleze
- envío de informe integración SIEM-Darktrace con Tipping Point
- envío informe de implementación Server and Workload y XDR
- Envío informe de implementación endpoint protection y sus módulos Web Control, App Control, Device Control y antimalware

- solicitud instalación antivirus en atriles y kioskos
- Se realiza depuración de los dispositivos sin comunicación en los últimos meses, versiones de productos se encuentran en su mayoría cerca al 100 %
- Depuración de dispositivos grupo recolector.
- Las plataformas y soluciones de Trellix y Trend Micro no presentaron indisponibilidad.
- Se cierra las peticiones pendientes de eliminación de dispositivos que ya no se encuentran en la entidad.
- El uso de licencias de Trellix y Trend Micro en equipos finales es de 2017 hasta el momento del informe.
- Se mitigaron los 604 eventos presentados en los equipos finales, se presentó 5 eventos en servidores del FNA por parte del antivirus.
- El IPS analizó 114851 eventos de los cuales 96601 fueron categorizados con severidad alta y 74516 con severidad media.
- Durante el periodo se gestionaron correctamente los requerimientos y cambios generados hacia y por el equipo de MNEMO.
- Se realiza depuración de dispositivo reportados por mesa de servicio como fuera de servicios o de baja.

Informe de Consultoría

2024

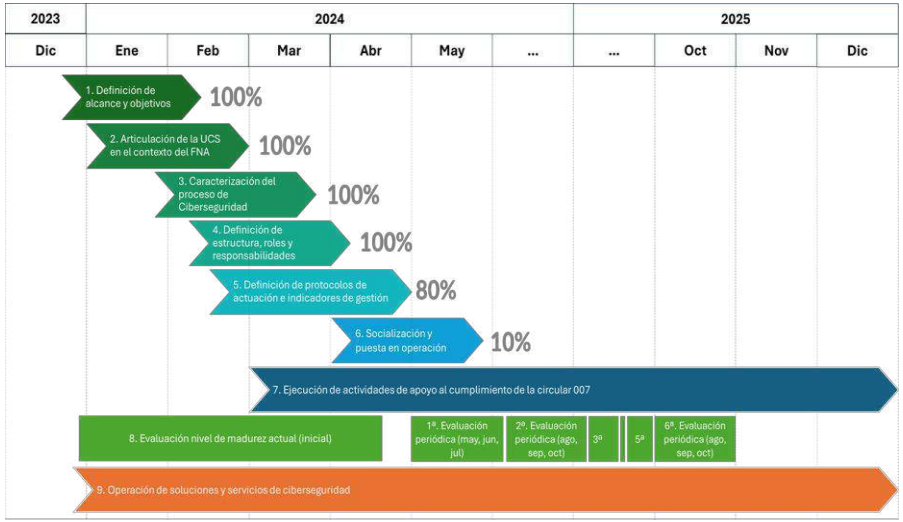
Objetivo

Presentar las principales actividades realizadas para la implementación de la unidad de ciberseguridad en el FNA indicando su estado actual y pasos a seguir.

Alcance

Incluye las actividades de planeación realizadas a la fecha del corte, las actividades ejecutadas en busca de concretar los objetivos planeados, los logros alcanzados y los pasos siguientes.

Plan de implementación unidad de ciberseguridad



Se desarrolla el plan de implementación de la unidad de ciberseguridad contemplando 6 etapas cuyos ejes centrales son la caracterización de proceso de ciberseguridad, la definición de los roles y responsabilidades y los protocolos de actuación.

Se recibe la retroalimentación por parte del equipo de supervisión sobre los documento elaborados y se inicia el proceso de ajuste y adecuación.

Se emprende el desarrollo de los documentos de procedimientos internos de operación.

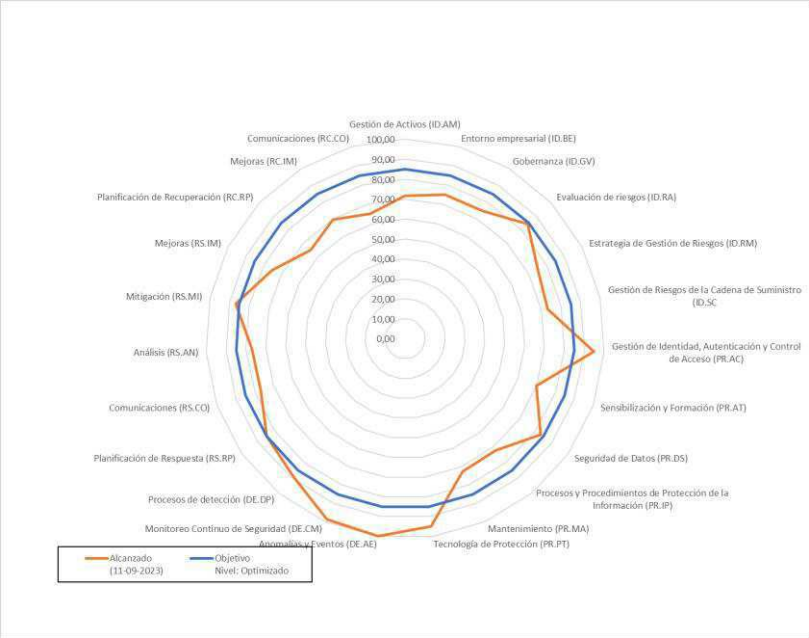
Se realiza el apoyo para la documentación de los catálogos de arquitectura empresarial de seguridad.

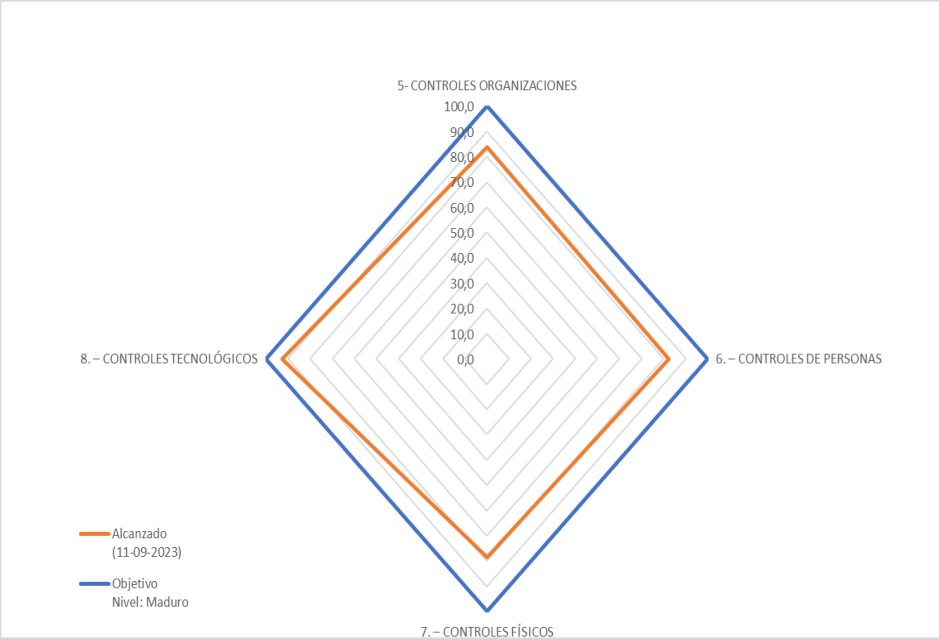
Plan de construcción de protocolos de actuación

Plan de Construcción de Protocolos de Actuación		
Proceso	**Protocolo**	**Guía**
Atención de peticiones	Análisis de Vulnerabilidades y Hacking Ético	
	Evaluaciónes de seguridad de productos	
	Configuración de reglas en servicios de ciberseguridad	
	Pruebas de recorrido	
	Solicitudes de sensibilización y/o capacitación	
Atención de incidentes	Gestión de escalamiento	
	Respuesta ante incidentes	Abuso de contenido
		Código malicioso
		Recopilación de información
		Intrusiones
		Disponibilidad del servicio DoS
		Fraude
		Seguridad del contenido de la información
		Vulnerabilidades
		Otros
Gestión de la operación	Monitoreo de soluciones	
	Gestión y administración de herramientas	
	Generación de informes periódicos y por demanda	
	Instalación, configuración y documentación de nuevas herramientas	
	Administración de tableros de control	
	Ejecución de Análisis de Vulnerabilidades y Hacking Ético	
	Gestión de la continuidad del servicio	
	Seguimiento a KPIs	
	Gestión de la mejora continua	

El plan de construcción de los protocolos de actuación contemplan el diseño de 24 documentos, entre los cuales se incluyen 8 playbooks, alineados con la taxonomía de la superintendencia financiera, para la atención de incidentes de ciberseguridad.

Evaluación inicial del nivel de madurez – GAP



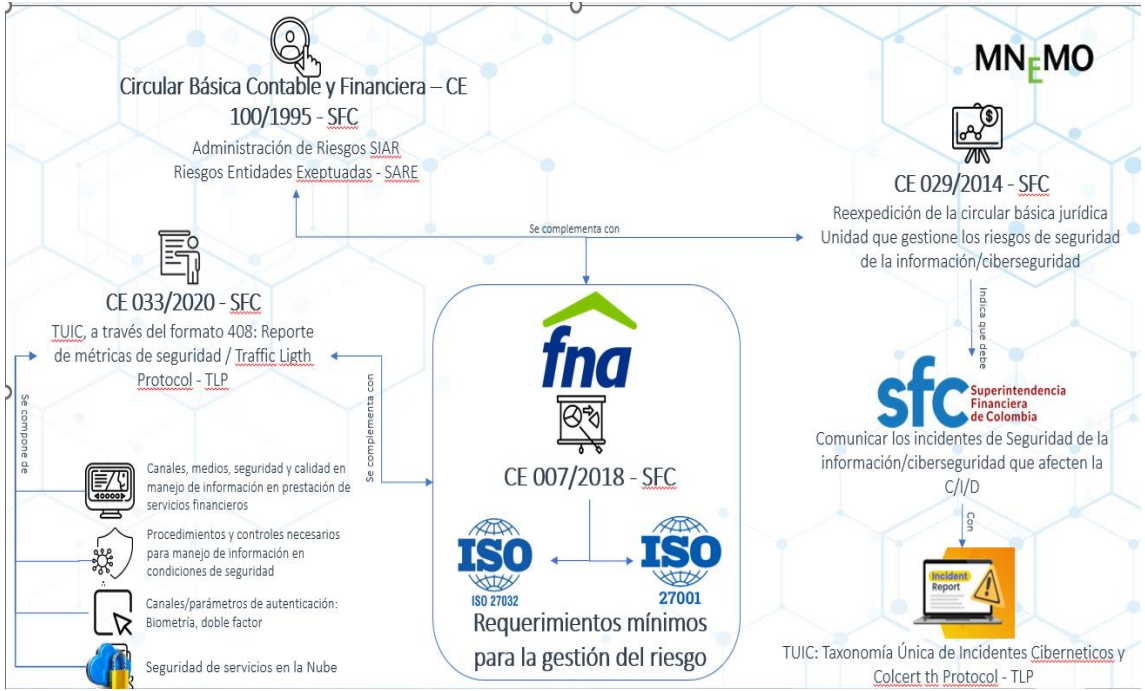


Construcción del modelo de análisis de nivel de madurez con base en marcos de referencia reconocidos como NIST, COBIT e ISO 27001.

Diseño preliminar de tableros de control

Diseño preliminar de tableros de control que se irán evolucionando conforme se obtienen datos y se determinan necesidades de información.

Apoyo al cumplimiento de la circular 007



Desarrollo de estrategia de apoyo y solicitud de información, en curso de recolección:

- Informes de auditorías externas
- Matrices de riesgos asociadas SGSI y SARO
- Proceso Gestión de la estrategia de Gobierno y TI
- Proceso Gestión de la demanda
- Proceso Gestión de soporte e incidentes
- Matriz de riesgo identificados riesgos asociados a la ciberseguridad de la entidad
- Plan de comunicaciones
- Declaración de aplicabilidad
- Plan de implementación/seguimiento de CE 007/2018 del año 2023 y/o 2024

Resumen de actividades

- Desarrollo del plan de implementación de la unidad de ciberseguridad
- Desarrollo del plan de diseño de protocolos de actuación
- Desarrollo de protocolos de actuación
- Desarrollo del instrumento de evaluación de nivel de madurez
- Evaluación preliminar del nivel de madurez
- Desarrollo de tablero de control preliminar
- Plan de apoyo al cumplimineto de la circular 007

0. LISTA DE VERSIONES

Versión	Fecha	Razon de la Actualización
0	24-05-2024	Creación del documento.

1. OBJETIVO

Documentar como se lleva a cabo la administración, monitoreo y generación de informes periódicos y por demanda de la Solución SIEM de la Unidad de Ciberseguridad, asi como la documentación de las contingencias definidas en caso de presentarse una falla prolongada de esta solución.

2. ALCANCE

El procedimiento inicia con la descripción de la solución en operación normal teniendo en cuenta componentes, interfaces, recursos necesarios, y el inventario correspondiente, luego se hace la descripción del servicio operando en contingencia, seguidamente se describe los pasos para llevar a cabo la gestión y administración de la solución, para hacer el monitoreo y finalmente los pasos para la generación de informes periódicos y por demanda.

3. DEFINICIONES

Amenaza
Circunstancia que tiene el potencial de causar daños o pérdidas a la información, puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS), afectando la integridad, confidencialidad y disponibilidad de esta.

Appliance
Sistema informático con una combinación de hardware, software o firmware que está diseñado específicamente para proporcionar un recurso informático particular.

Ataque de denegación de servicio DoS
Ataque de denegación de servicio, llamado también ataque DoS (por sus siglas en inglés, (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Ataque Web
Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta, entre los objetivos de un ataque están los activos web (aplicaciones, paginas, portales).

Copia de seguridad
Backup o copia de seguridad, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Disponibilidad
Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

Evento
Un log del sistema supervisa eventos varios del sistema, como inicio, apagado y eventos como fallas de hardware y controladores.

Firewall
Un firewall es la parte de un sistema o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los firewalls pueden ser implementados en hardware o software, o en una combinación de ambos.

Fuga de información
Se denomina fuga de información "al incidente (tanto interno como externo, y a la vez intencional o no) que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de esta.

Incidente Informático
Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informático.

SOC
SOC o Centros de Operaciones de Seguridad se encargan de realizar un seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad. Un SOC es responsable de garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente.

SIEM
SIEM significa Security Information and Event Management y es una combinación de dos conceptos: SIM (Security Information Management) y SEM (Security Event Management). Esta unión plantea un enfoque basado en software que permite obtener una visión completa de la seguridad informática. Un sistema SIEM considera en todo momento los requisitos específicos de la empresa, siempre que existan definiciones claras e individuales sobre qué procesos y eventos son relevantes para la seguridad, así como de qué manera y con qué prioridad es preciso reaccionar ante ellos.

4. ASPECTOS GENERALES

La Solución de Administración de Eventos e Información de Seguridad (SIEM) le permite al Fondo Nacional del Ahorro detectar con precisión y priorizar las amenazas, además de proporcionar análisis inteligentes que le permiten al FNA responder rápidamente para reducir el impacto de los incidentes.

La Solución de Administración de Eventos e Información de Seguridad (SIEM) del FNA, recopila y agrega datos y eventos de dispositivos de seguridad, infraestructuras de red, servidores, sistemas de informacion y aplicaciones. A continuación, aplica inteligencia a esos datos mediante combinación de información contextual acerca de usuarios, activos, vulnerabilidades y amenazas. Finalmente correlaciona toda esta información y agrega eventos relacionados a alertas únicas que aceleran el análisis y la resolución de incidentes.

Esta Solución se compone de un servicio en Nube que proporciona flexibilidad para llevar a cabo el monitoreo sin invertir en todo el hardware y software necesarios para una implementación local, esto se logra mediante un dispositivo DataGateway, el cual tiene como fin recopilar datos y eventos de todas las fuentes, para luego ser reenviados al servicio en Nube, a través de un túnel VPN seguro, donde se almacenan y gestionan los datos.

4.1. Integración con servicios tecnológicos

La Solución de Administración de Eventos e Información de Seguridad (SIEM) tiene la capacidad de integrarse con cualquier dispositivo de red, servidores, sistemas de informacion o aplicaciones, que se deseen monitorear. Actualmente se encuentra monitoreando alrededor de 68 fuentes criticas para el Fondo Nacional del Ahorro.

4.2. Recursos Necesarios

4.2.1. Personal responsable:

Para llevar a cabo la gestión y administración de la Solución de Administración de Eventos e Información de Seguridad (SIEM) en el Fondo Nacional del Ahorro se cuenta con Administradores Expertos en la solución.

4.2.2. Herramientas para hacer la administración:

- **Explorador web:** Firefox, Chrome, Microsoft Edge.
- **MobaXterm**: Conexión por SSH a los appliances.

4.2.3. Inventario de componentes:

La Solución de Administración de Eventos e Información de Seguridad (SIEM) se compone de un dispositivo DATAGATEWAY instalado en el DataCenter del FNA, el cual cuenta con dos interfaces de red, para la recepción de eventos que provengan desde los agentes instalados en los servidores Windows (WINCOLLECT) y los eventos tipo SYSLOG que provienen de otros dispositivos en los que no se puede instalar el agente.

La Solución de Administración de Eventos e Información de Seguridad (SIEM) tambien se compone de un servicio en Nube, mediante el cual se realiza el analisis y correlación de los eventos reportados por el dispositivo DATAGATEWAY.

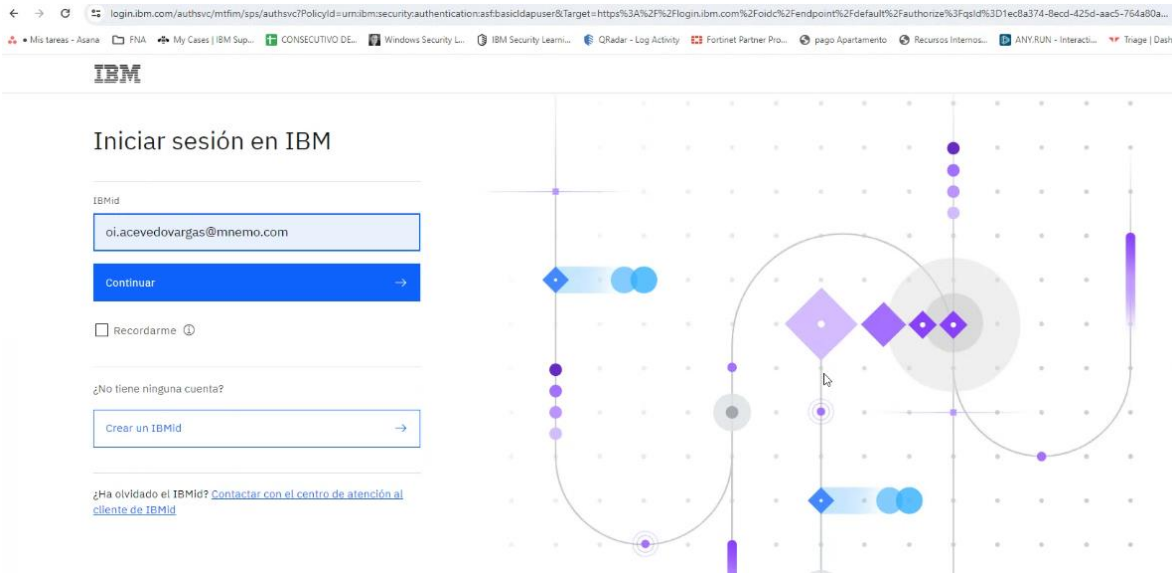
4.2.4. Copias de respaldo:

El servicio principal es un servicio en nube que cuenta con zonas de disponibilidad que garantizan la continuidad del servicio, asi mismo mantiene una copia de los eventos reportados por el DATAGATEWAY.

5. DESARROLLO DE LOS PASOS

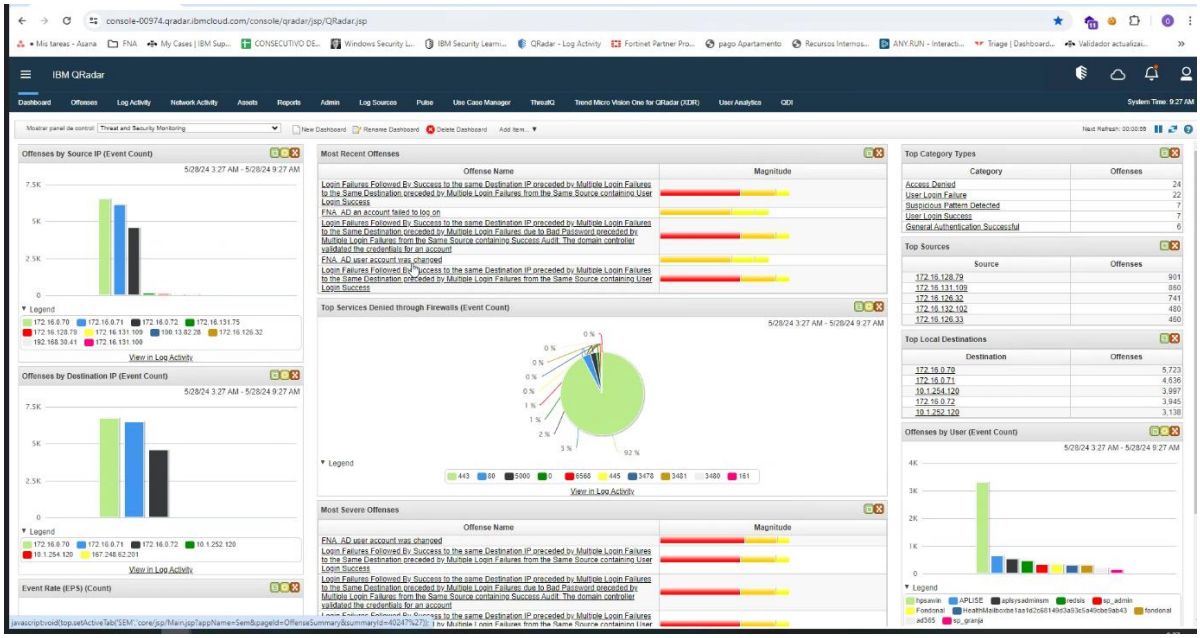
5.1. Gestión y administración de la Solución

1. La administración de la solución SIEM, se realiza mediante la siguiente URL: https://console-00974.qradar.ibmcloud.com/console/qradar/jsp/QRadar.jsp

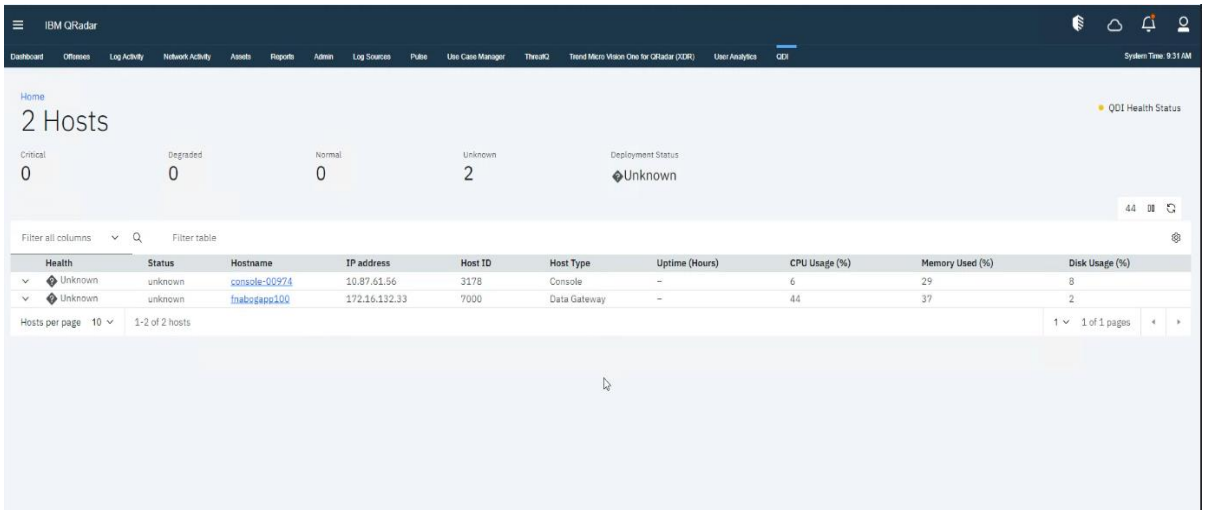


Nota: El usuario y contraseña se almacenan en la herramienta Keepass instalada en el servidor Mnemo.

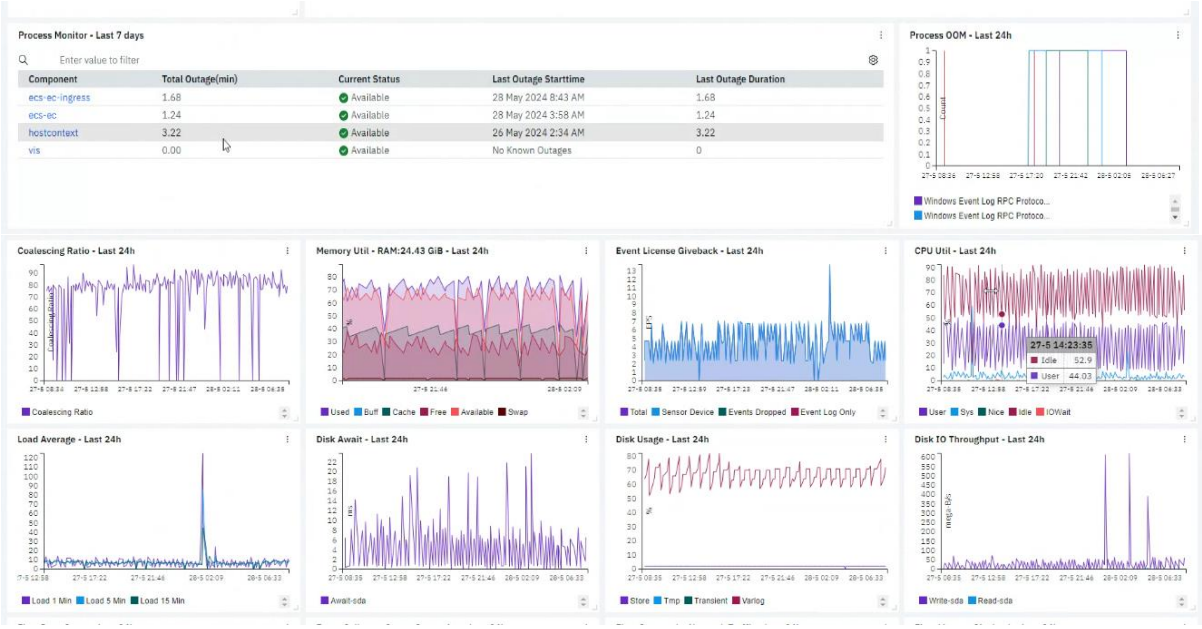
A continuación se observa el acceso exitoso a la solución SIEM



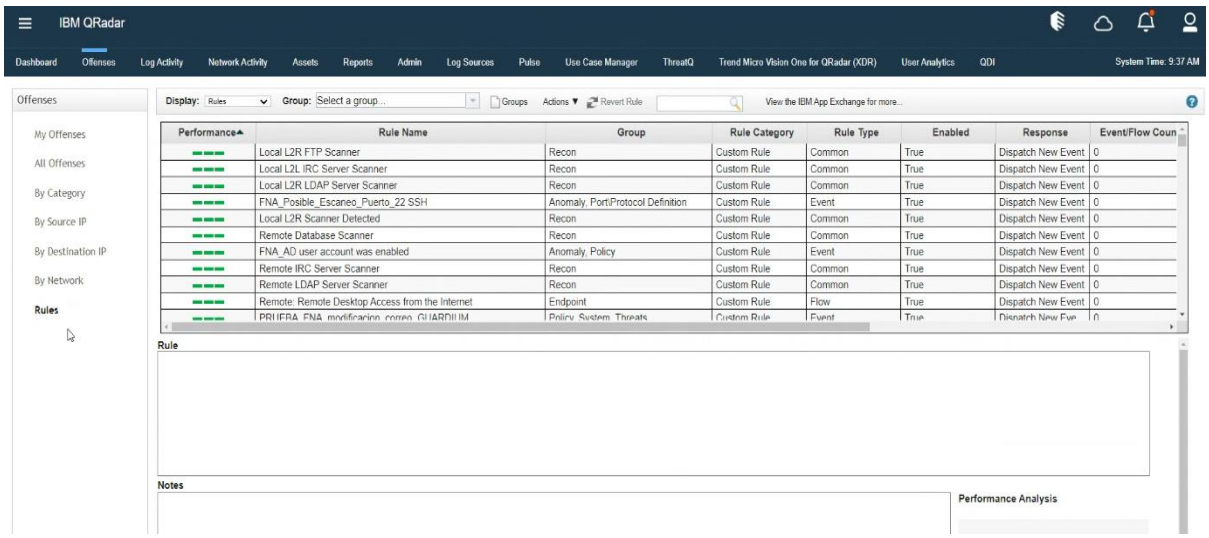
2. Para la verificación del estado del dispositivo DataGateway, se debe ingresar a través de la opción QDI, en el menú superior



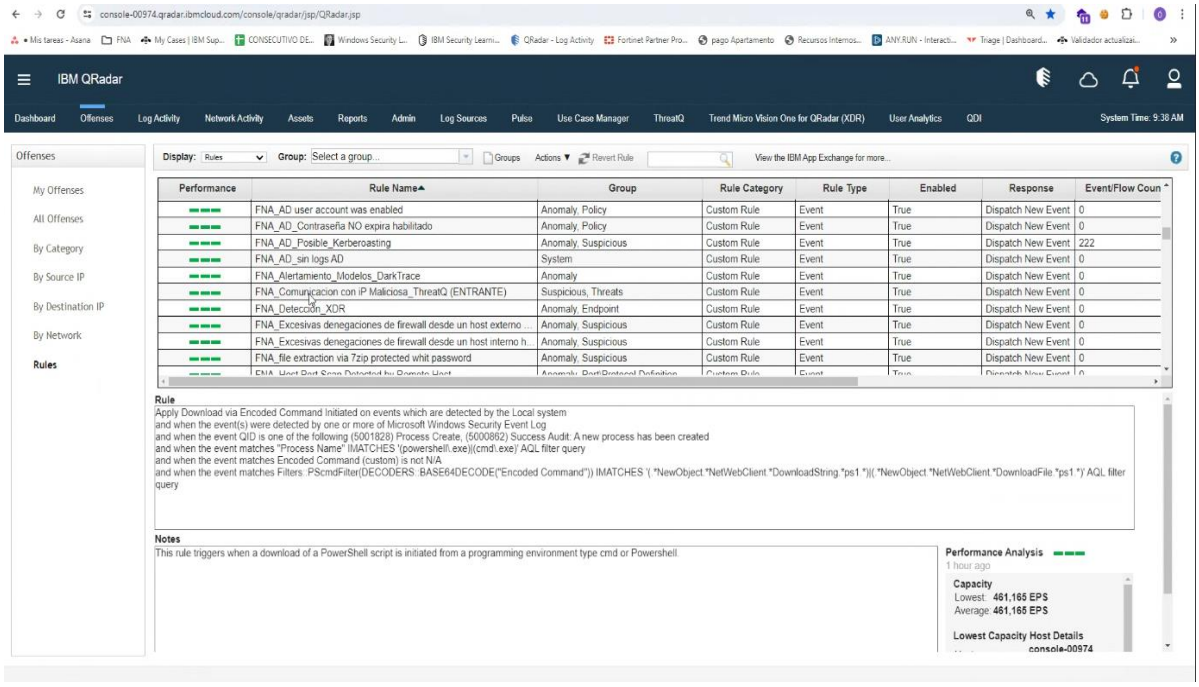
Al hacer click en el link que corresponde al DataGateway, se puede observar el estado de los servicios del dispositivo, asi como estadísticas sobre el uso de memoria y de disco duro entre otros



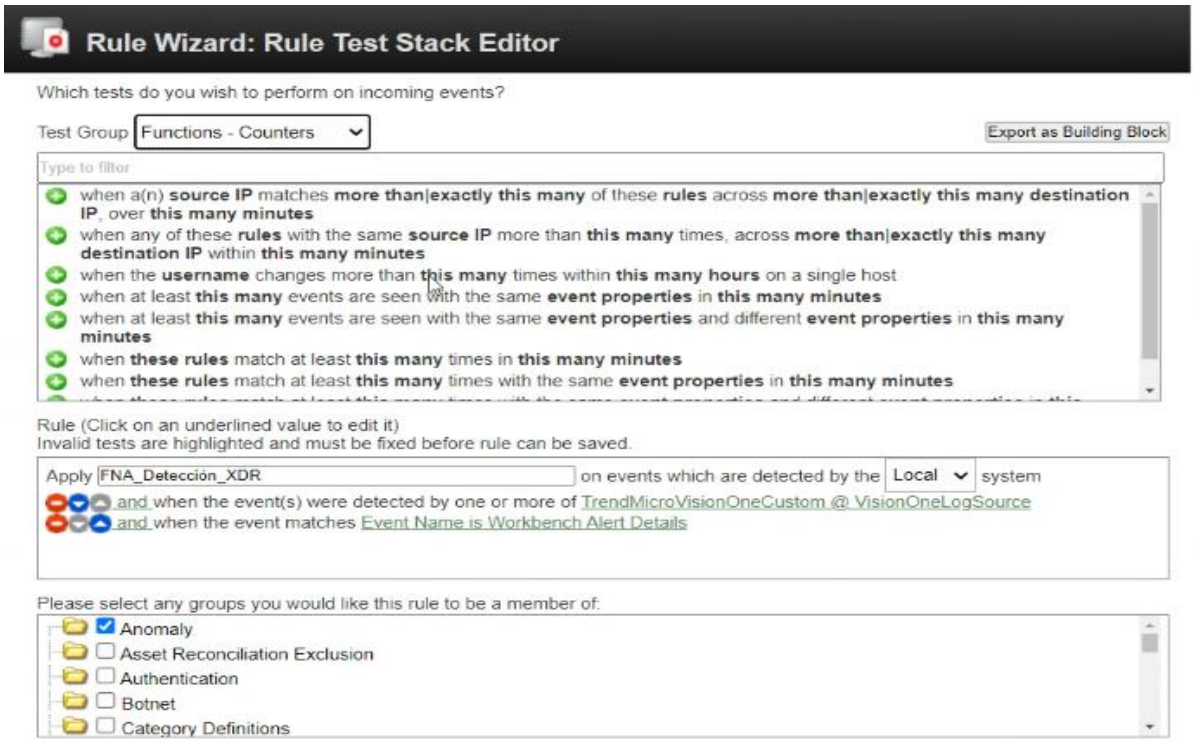
3. Para la creación de reglas en el SIEM, se debe ingresar a través de la opción Offenses, en el menú superior > Rules



A continuación se observan reglas personalizadas para el FNA

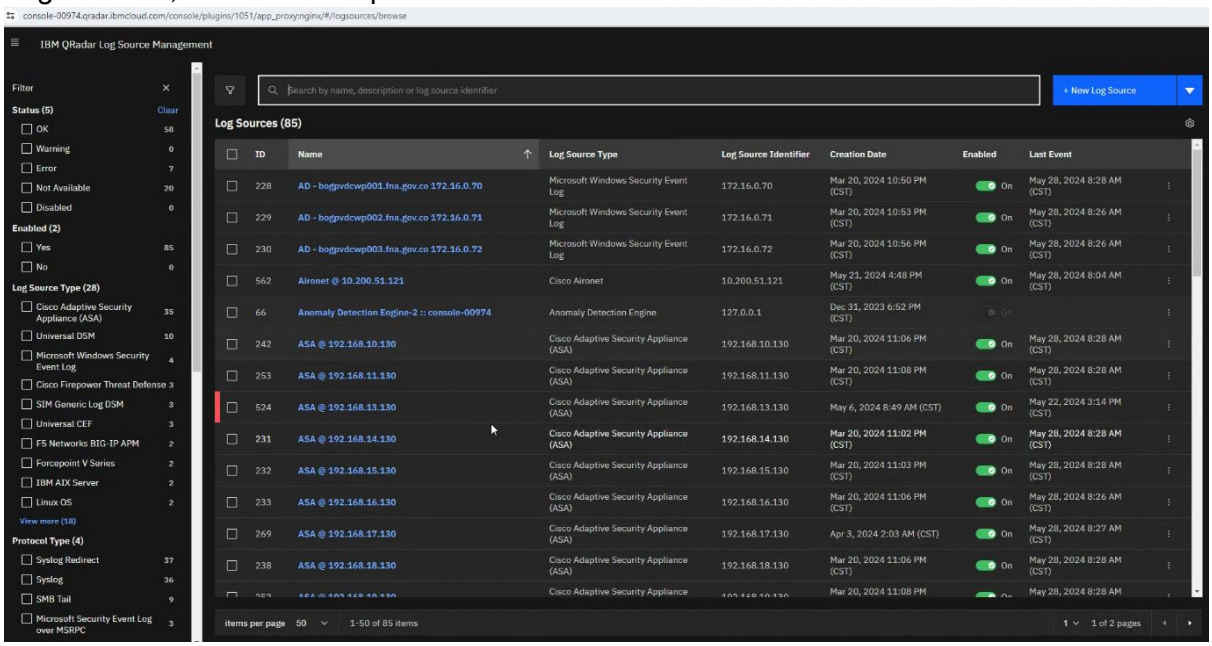


Para ver el detalle de una regla se debe hacer doble click sobre la misma

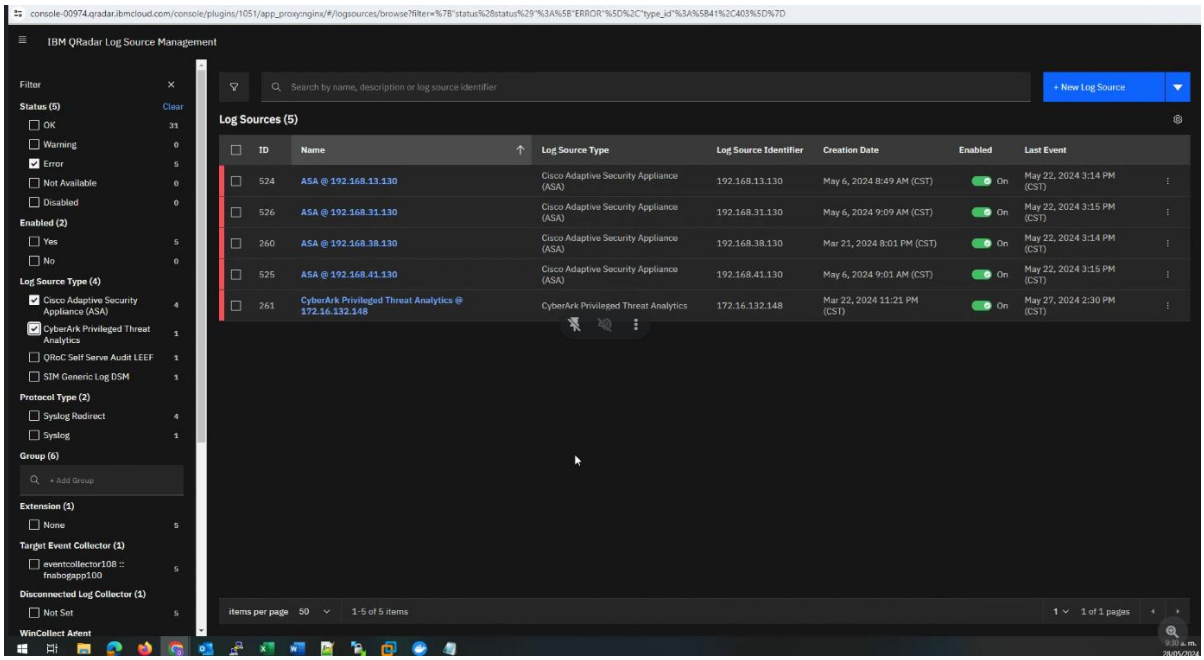


5.2. Monitoreo de la Solución

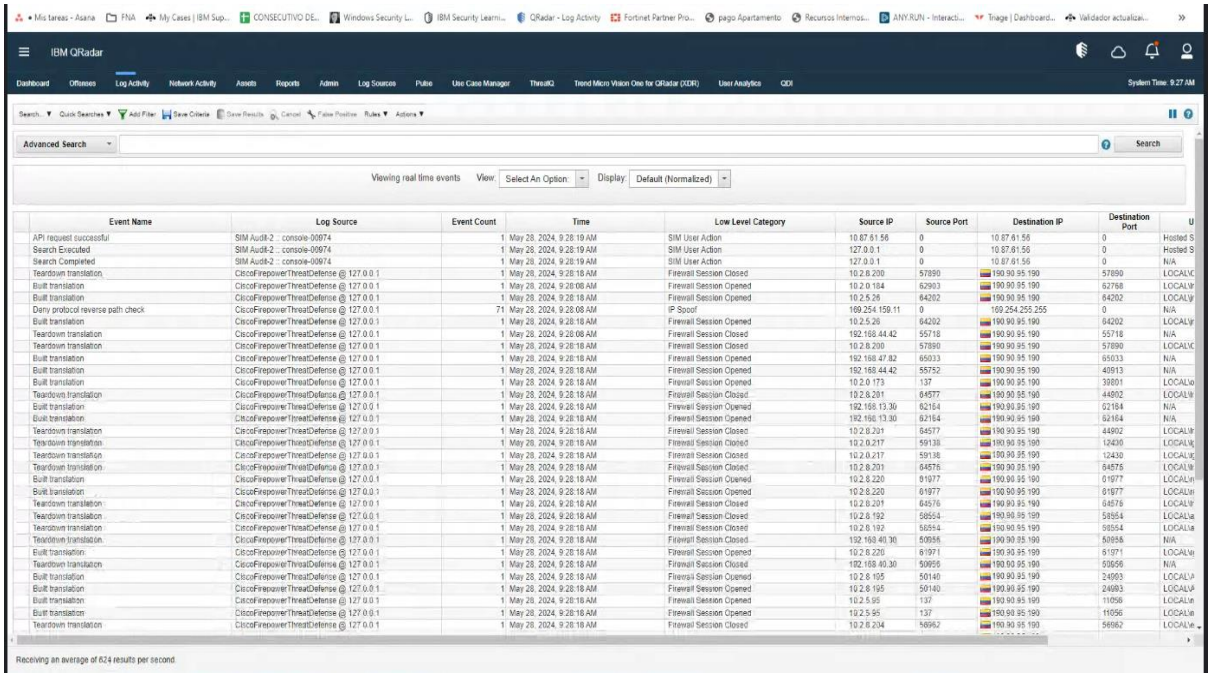
1. Para ver las fuentes de eventos configuradas en la solución, se debe seleccionar la opción Log Sources, en el menú superior



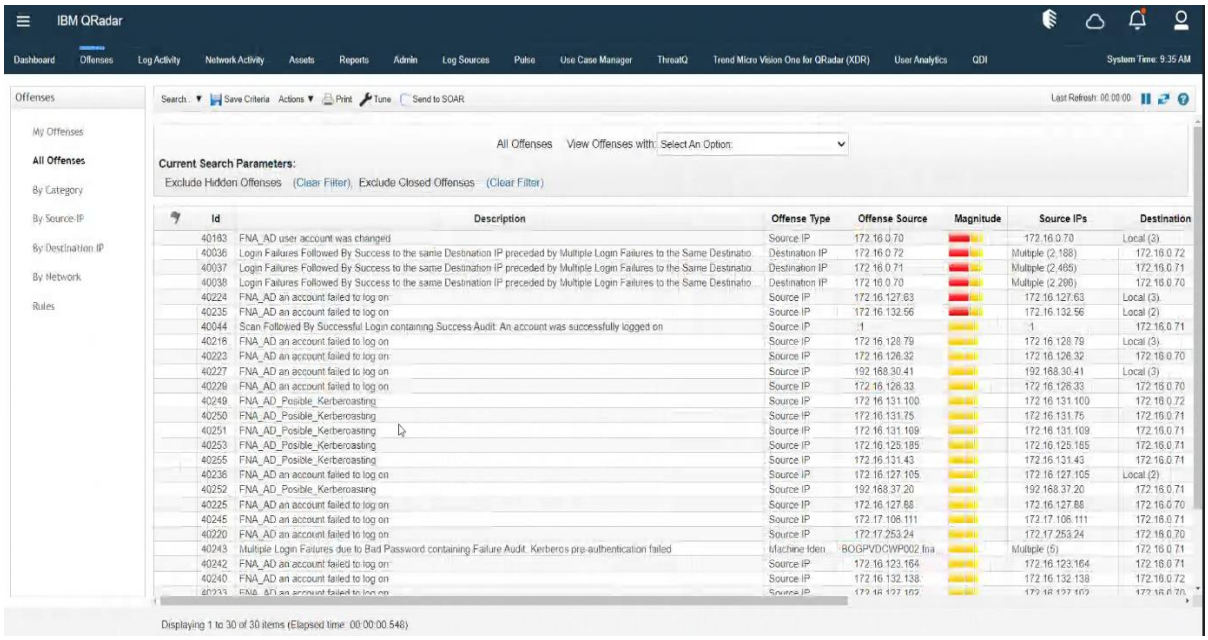
Las fuentes que presentan problemas en la recepción de logs, se pueden filtrar en el menú lateral en Status > Error



2. Para ver la recepción de eventos en tiempo real se debe seleccionar la opción Log Activity, en el menú superior

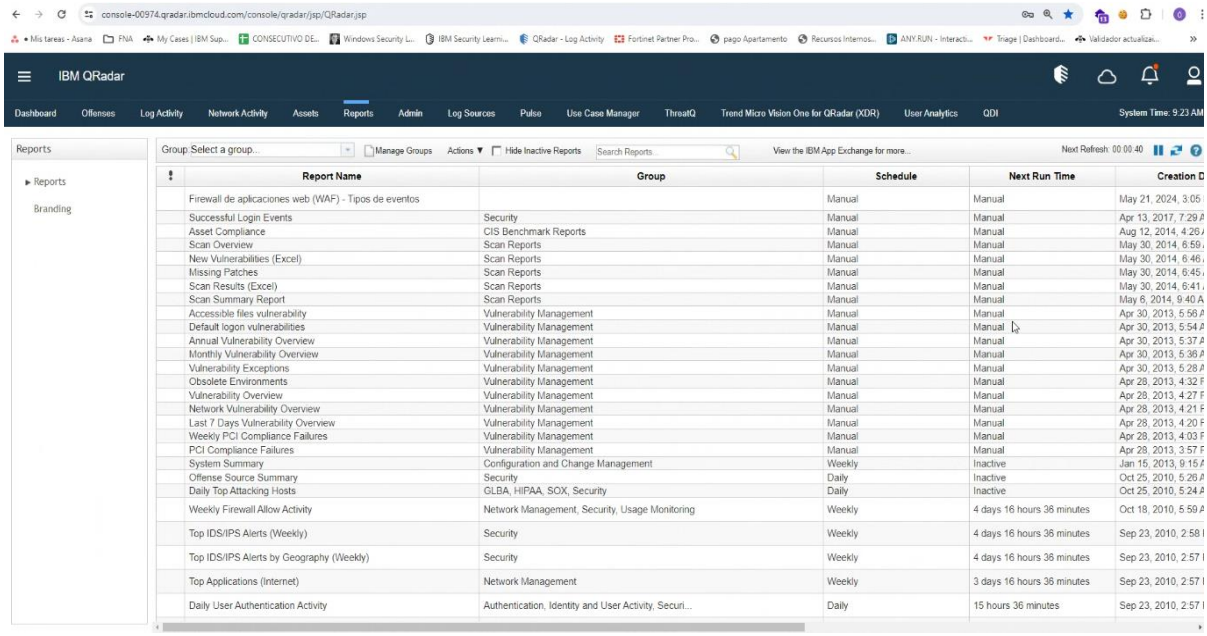


3. Para ver las alertas en tiempo real se debe seleccionar la opción Offenses, en el menú superior

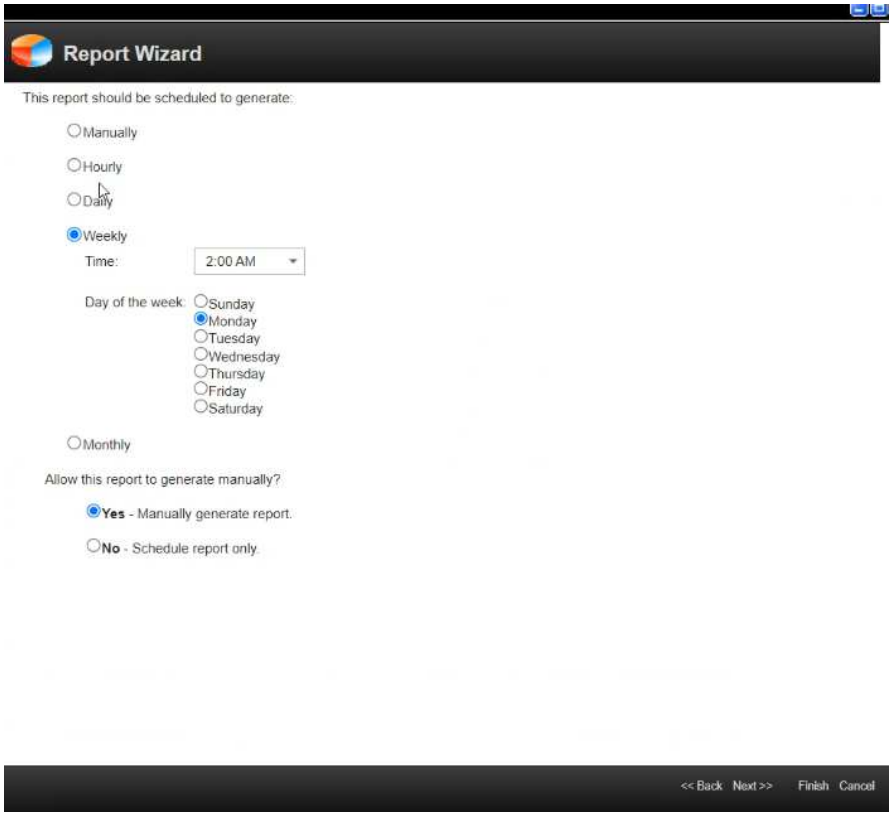


5.3. Generación de Informes Periódicos y por Demanda

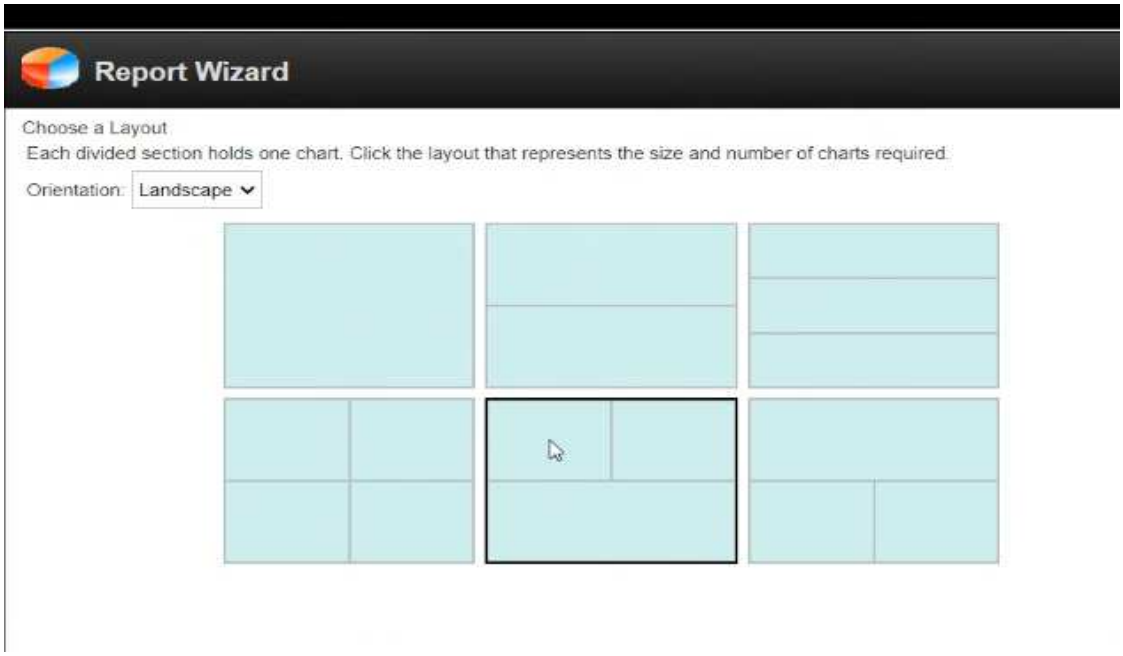
1. Para acceder al módulo de reportes, se debe hacer click en Reports, en el menú superior



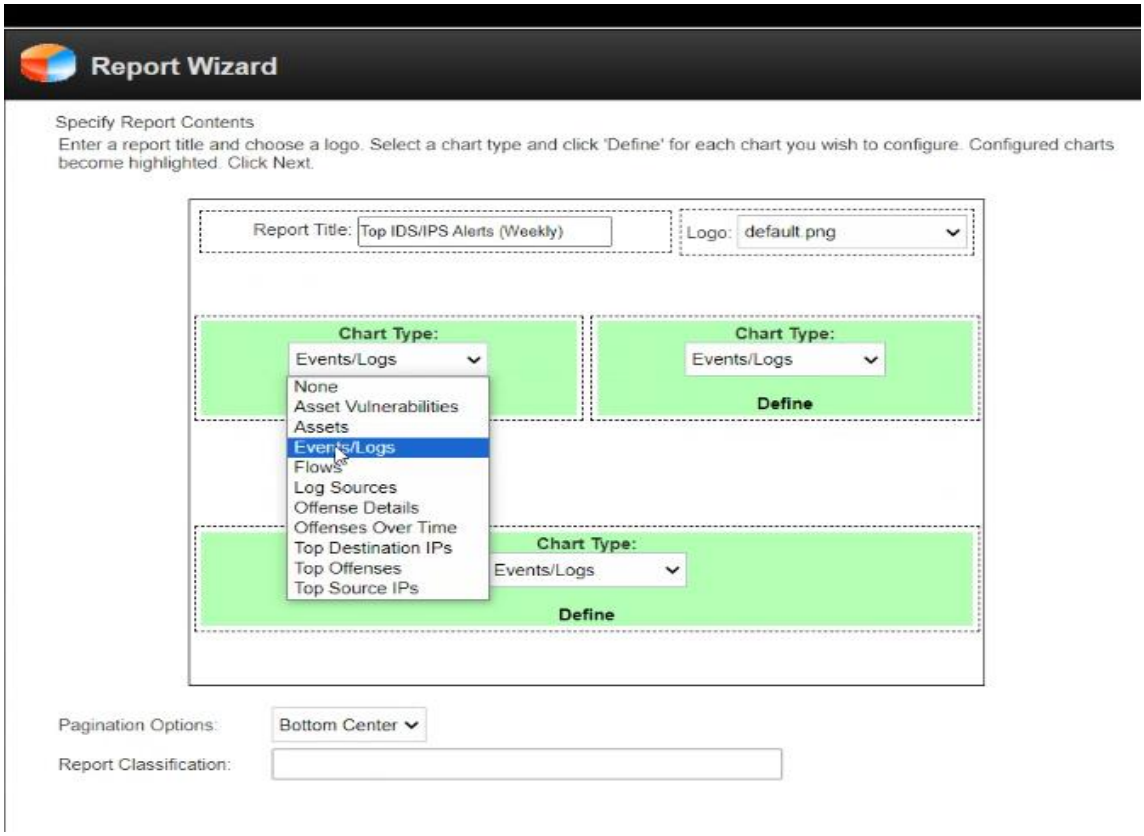
Luego de lo cual se despliega el asistente



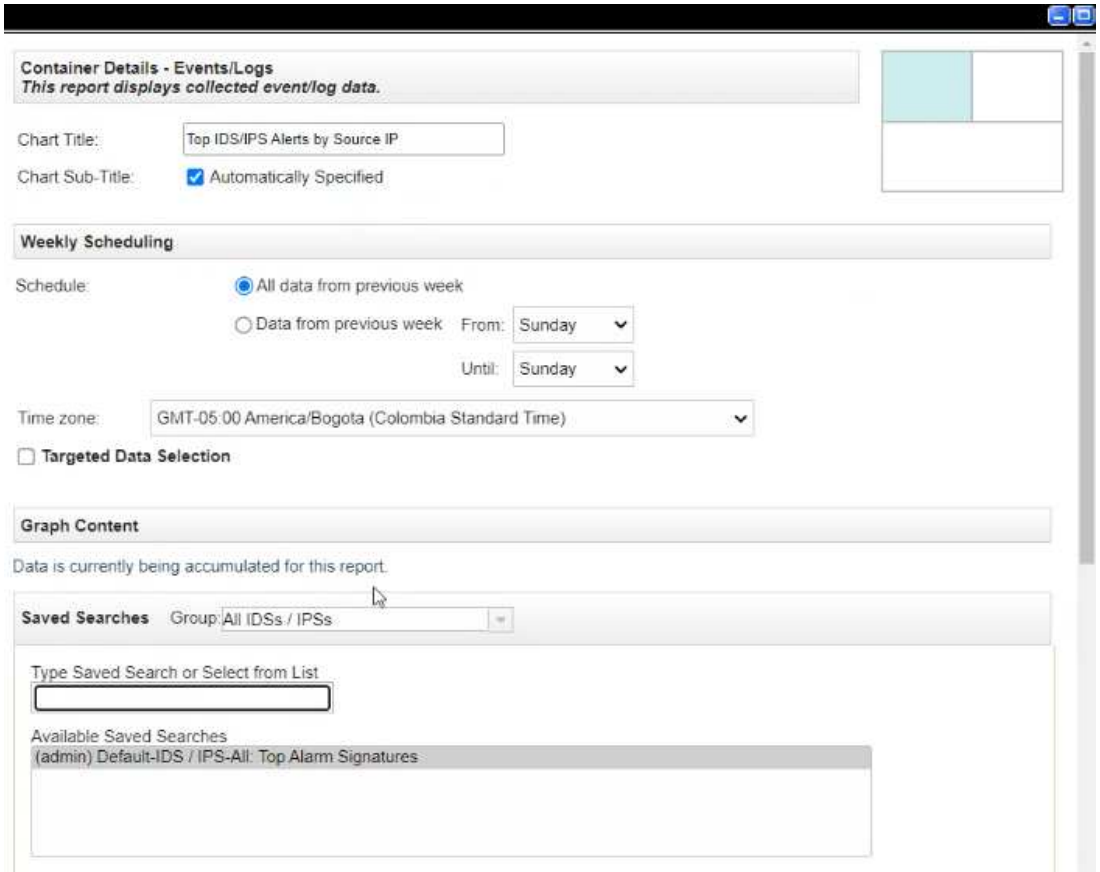
El asistente permite seleccionar la distribución de contenido del reporte que se quiere:



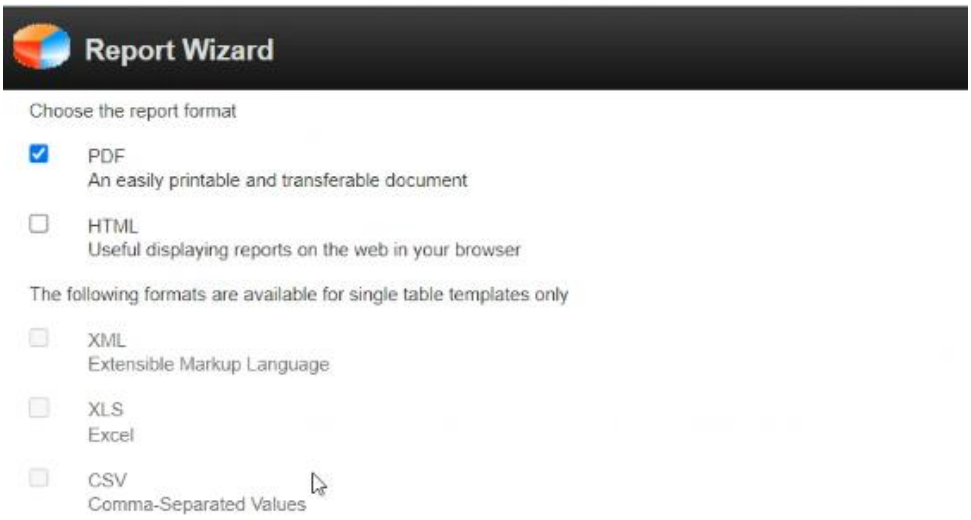
Una vez seleccionado la distribución, se selecciona el contenido de cada sección:



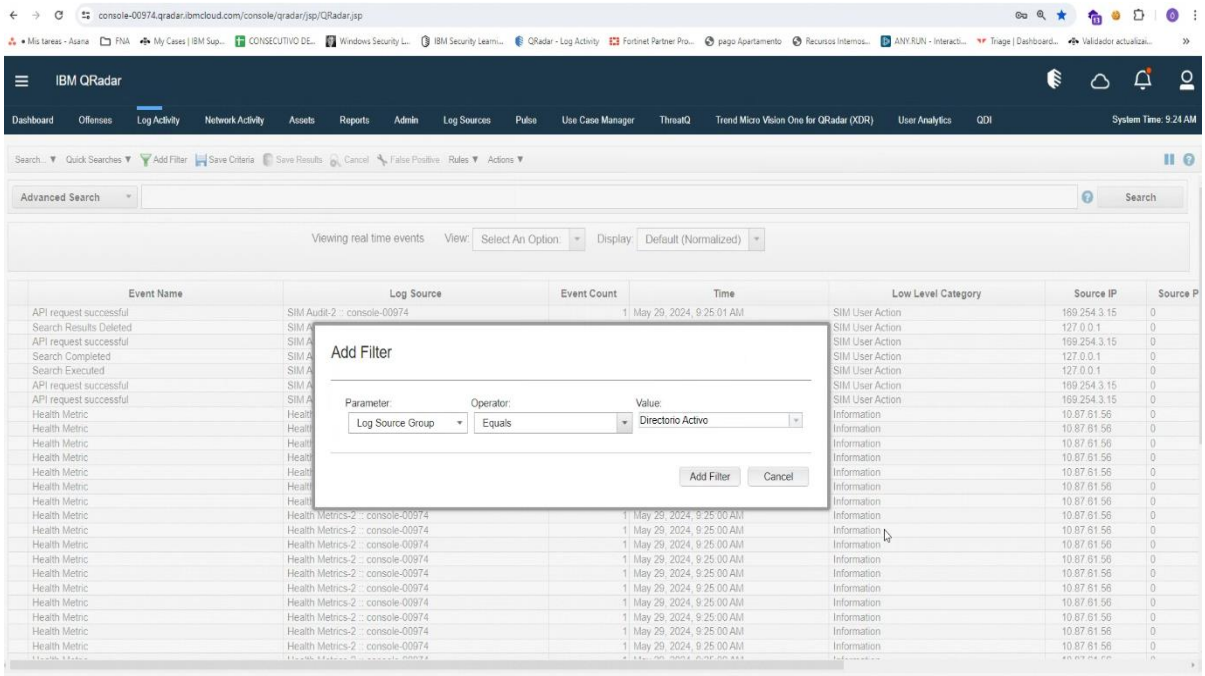
Luego se selecciona el filtro sobre los eventos deseado



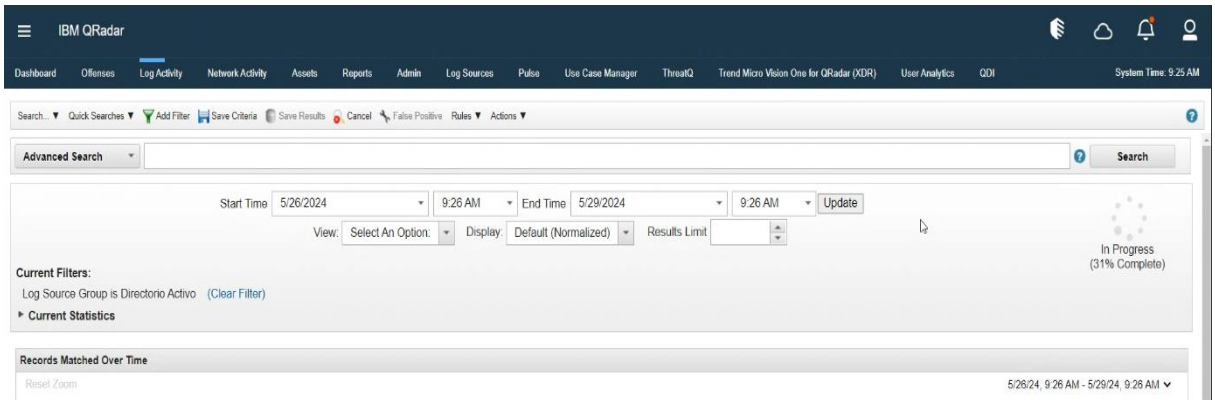
Luego se selecciona el filtro sobre los eventos deseado



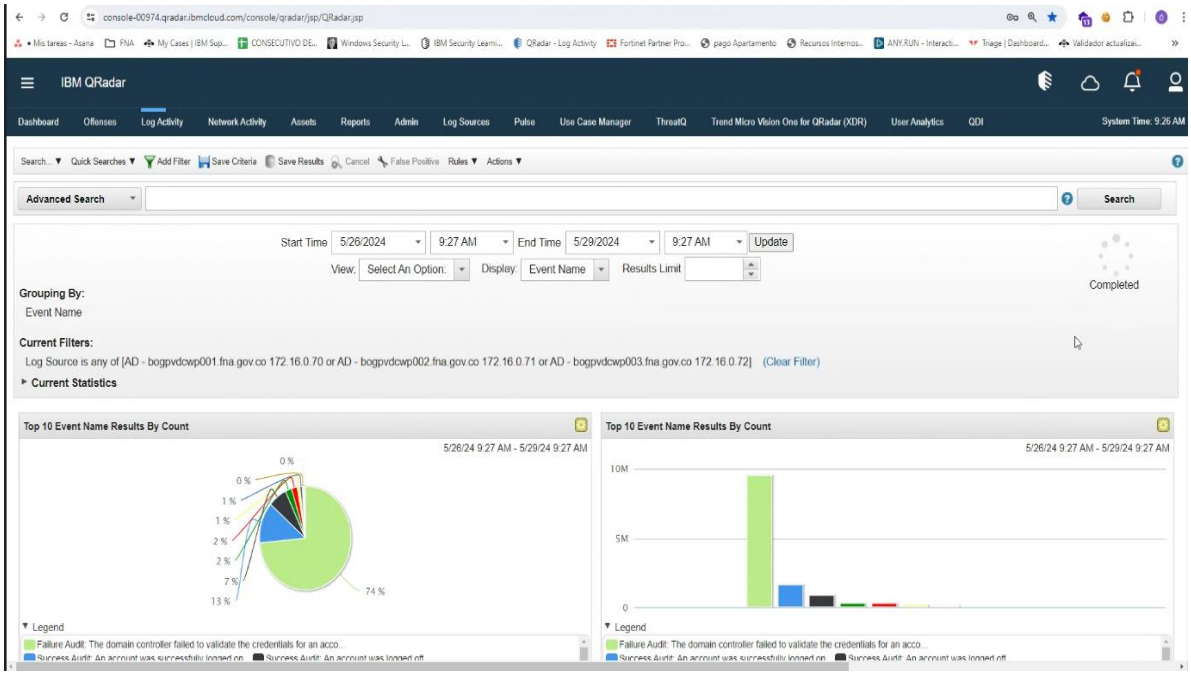
2. Por otra parte en el menú Log Activity, se pueden llevar a cabo filtros por fuente de eventos, para el ejemplo se filtró por Directorio Activo



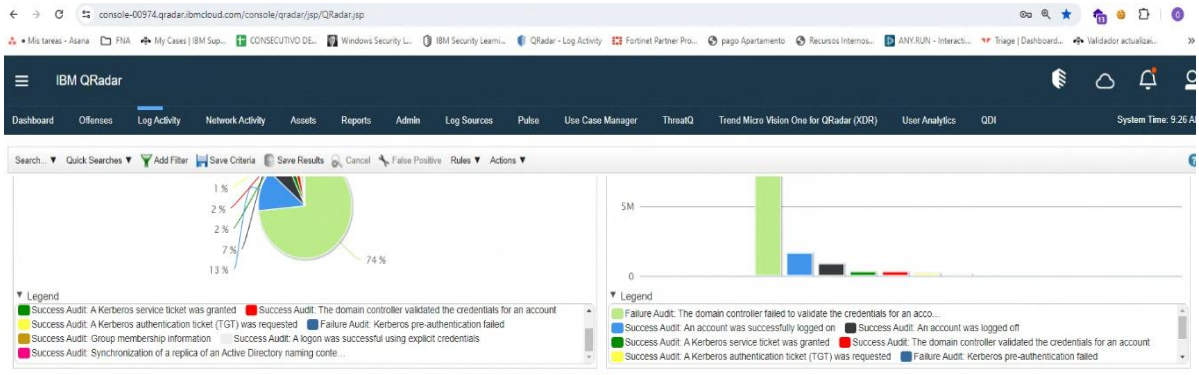
La solución indicara que el filtro se encuentra en proceso



Una vez completado el proceso, podemos observar graficas y el detalle de los eventos como se observa a continuación



Eventos identificados según el filtro



Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Uniq Count)
Failure Audit: The domain controller failed to validate the credentials for an account	Multiple (3)	Multiple (3)	0	Multiple (3)	General Authentication Failed	Other
Success Audit: An account was successfully logged on	Multiple (3,272)	Multiple (3)	0	Multiple (3)	User Login Success	Other
Success Audit: An account was logged off	Multiple (3)	Multiple (3)	0	Multiple (3)	Host Logout	Other
Success Audit: A Kerberos service ticket was granted	Multiple (3,070)	Multiple (3)	0	Multiple (3)	Kerberos Session Opened	Other
Success Audit: The domain controller validated the credentials for an account	Multiple (4)	Multiple (3)	0	Multiple (3)	General Authentication Successful	Other
Success Audit: A Kerberos authentication ticket (TGT) was requested	Multiple (2,941)	Multiple (3)	0	Multiple (3)	Kerberos Session Opened	Other
Failure Audit: Kerberos pre-authentication failed	Multiple (964)	Multiple (3)	0	Multiple (3)	Kerberos Session Denied	Other
Success Audit: Group membership information	Multiple (3)	Multiple (3)	0	Multiple (3)	Information	Other
Success Audit: A logon was successful using explicit credentials	Multiple (40)	Multiple (3)	0	Multiple (3)	User Login Success	Other
Success Audit: Synchronization of a replica of an Active Directory naming context has begun	Multiple (3)	Multiple (3)	0	Multiple (3)	Information	Other
Success Audit: Synchronization of a replica of an Active Directory naming context has ended	Multiple (3)	Multiple (3)	0	Multiple (3)	Information	Other
Failed domain controller login attempt per expired credentials	Multiple (3)	Multiple (3)	0	Multiple (3)	General Authentication Failed	Other
Success Audit: A user right was adjusted	Multiple (3)	Multiple (3)	0	Multiple (3)	User Right Assigned	Other
Success Audit: Successful logon with administrative or special privileges	Multiple (3)	Multiple (3)	0	Multiple (3)	Admin Login Successful	Other
Success Audit: The handle to an object was closed	Multiple (3)	Multiple (3)	0	Multiple (3)	Information	Other
Success Audit: A handle to an object was requested	Multiple (3)	Multiple (3)	0	Multiple (3)	Information	Other

6. ANEXOS

N/A

PRE FACTURA

No. C-2-16

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

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2024-06-12

Autorización numeración de facturación electrónica DIAN No 18764062145032 vigencia desde 18-12-2023 hasta el 17-12-2024 desde el FE 1 al 5.000 vigencia 12 meses.

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
1	Instalación, configuración, pruebas, puesta en marcha y estabilización de plataforma SOAR, Suscripción de licenciamiento. Contrato 173-2023	1.00	743,897,000.00	885,237,430.00	0.00

Total Bruto	743,897,000.00
Subtotal	743,897,000.00
IVA 19%	141,340,430.00
Total a Pagar	885,237,430.00

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

Valor en letras:Ochocientos ochenta y cinco millones doscientos treinta y siete mil cuatrocientos pesos mcte.

Notas:

1.Instalación realizada en los servidores ya desbloqueados con la salida a producción de la plataforma SIEM

2.PowerEdge Server No. Serial: 4TD4H04, PowerEdge Server No. Serial: 5TD4H04, PowerVault SAN No. Serial: 49L3H04

3.Ver el valor del licenciamiento en la Nota Discriminación _ valores_ licencias V2.docx

Distribución de ingresos:

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** aperturada 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 **18 de marzo del 2024.**

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

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14932552929

(415)7707212489984(8020) 000001493255292 9

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	27. Fecha expedición
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 1 6 9	Bogotá D.C. 1 1	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
	6 9 1 3 1 3 3	

CLASIFICACIÓN

Actividad económica						Ocupación	
Actividad principal		Actividad secundaria		Otras actividades			
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código 1	2	51. Código	52. Número establecimientos
6 2 0 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 ordinar
07- Retención en la fuente a título de rent
14- Informante de exogena
42- Obligado a llevar contabilidad
48 - Impuesto sobre las ventas - IVA
52 - Facturador electrónico
55 - Informante de Beneficiarios Finales

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

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 61. Fecha 2023 - 07 - 30 / 23 : 41: 33

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 Suplente Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario 14932552929

(415)7707212489984(8020) 000001493255292 9

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	

Características y formas de las organizaciones

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

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 4	
72. Número		
73. Fecha	2 0 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	

Composición del Capital

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

Entidad de vigilancia y control

88. Entidad de vigilancia y control
Superintendencia de Sociedades 5

Estado y Beneficio

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

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario 14932552929

(415)7707212489984(8020) 000001493255292 9

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

1

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

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Extranjerí 2 2	6 6 7 3 5 2		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
VICENT	FERNANDEZ	CARLOS	

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

2

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

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadan 1 3	8 7 7 0 4 4 6		6 1 0 6 1 - T

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
VELEZ	CASTRO	HUMBERTO	DE JESUS

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario 14932552929

(415)7707212489984(8020) 000001493255292 9

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

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

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		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 2 0 2 2 3

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14933306804

(415)7707212489984(8020) 000001493330680 4

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	27. Fecha expedición
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 1 6 9	Bogotá D.C. 1 1	Bogotá, D.C. 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
	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			
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código 1	2	51. Código	52. Número establecimientos
6 2 0 1	2 0 1 9 0 7 0 2	6 2 0 2	2 0 1 9 0 7 0 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 ordinar
07- Retención en la fuente a título de rent
14- Informante de exogena
42- Obligado a llevar contabilidad
48 - Impuesto sobre las ventas - IVA
55 - Informante de Beneficiarios Finales

Usuarios aduaneros

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

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 61. Fecha 2023 - 07 - 31 / 16 : 56: 19

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 PARRA GAMBOA JOHN JAIRO

985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario 14933306804

(415)7707212489984(8020) 000001493330680 4

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

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 5	
72. Número		
73. Fecha	2 0 1 9 0 7 2 6	
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	
78. Departamento	1 1	
79. Ciudad/Municipio	0 0 1	
Vigencia		
80. Desde	2 0 1 9 0 7 2 6	
81. Hasta	9 9 9 9 1 2 3 1	

Composición del Capital

82. Nacional	0	%
83. Nacional público	0 . 0	%
84. Nacional privado	0 . 0	%
85. Extranjero	1 0 0	%
86. Extranjero público	0 . 0	%
87. Extranjero privado	1 0 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	4 9	2 0 1 9 0 7 2 6		-
2	8 1	2 0 1 9 0 7 2 6		-
3		Año Mes Día		-
4		Año Mes Día		-
5		Año Mes Día		-

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario 14933306804

(415)7707212489984(8020) 000001493330680 4

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

1

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

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadaní 1 3	8 0 8 0 8 4 2 0		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
PARRA	GAMBOA	JOHN	JAIRO

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

2

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario 14933306804

(415)7707212489984(8020) 000001493330680 4

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	125. Número de identificación	126. DV	127. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	8 7 7 0 4 4 6		6 1 0 6 1

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
VELEZ	CASTRO	HUMBERTO	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	149. Número de identificación	150. DV	151. 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

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 1 0 6 0 1

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14908474061

(415)7707212489984(8020) 000001490847406 1

5. Número de Identificación Tributaria (NIT): 9 0 0 3 9 6 1 7 6
6. DV: 1
12. Dirección seccional: Impuestos de Bogotá 3 2
14. Buzón electrónico:

IDENTIFICACIÓN

24. Tipo de contribuyente: Persona jurídica 1
25. Tipo de documento:
26. Número de Identificación:
27. Fecha expedición:

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 COLOMBIA SAS

36. Nombre comercial:
37. Sigla:

UBICACIÓN

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

41. Dirección principal: CL 99 10 19 OF 502

42. Correo electrónico: recepcion.colombia@mnemo.com

43. Código postal:
44. Teléfono 1: 3 1 8 3 8 3 5 1 1 7
45. Teléfono 2: 6 9 1 3 3 3 3

CLASIFICACIÓN

Actividad económica						Ocupación	
Actividad principal		Actividad secundaria		Otras actividades			
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código 1	2	51. Código	52. Número establecimientos
6 2 0 1	2 0 1 0 1 1 1 2	6 2 0 2	2 0 1 0 1 1 1 2	6 2 0 9	8 5 5 1		

Responsabilidades, Calidades y Atributos

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

05- Impto. renta y compl. régimen ordinar
07- Retención en la fuente a título de rent
09- Retención en la fuente en el impuesto
10- Obligado aduanero
14- Informante de exogena
18- Precios de transferencia
19- Productor de bienes y/o servicios exen
26- Declaración individual precios de tran
41- Declaración anual de activos en el exte
42- Obligado a llevar contabilidad
48 - Impuesto sobre las ventas - IVA
52 - Facturador electrónico
55 - Informante de Beneficiarios Finales

Usuarios aduaneros

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

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
61. Fecha: 2023 - 04 - 14 / 10 : 02: 37

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 Suplente Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario 14908474061

(415)7707212489984(8020) 000001490847406 1

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
900396176	1	Impuestos de Bogotá 32	

Características y formas de las organizaciones

62. Naturaleza	2	63. Formas asociativas	12	64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio	1

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	04	04
72. Número		
73. Fecha	20101112	20130418
74. Número de notaría		
75. Entidad de registro	03	03
76. Fecha de registro	20101119	20130709
77. No. Matrícula mercantil	02045162	02045162
78. Departamento	11	11
79. Ciudad/Municipio	4	4
Vigencia		
80. Desde	20101112	
81. Hasta		

Composición del Capital

82. Nacional	0	%
83. Nacional público	0.0	%
84. Nacional privado	0.0	%
85. Extranjero	100	%
86. Extranjero público	0.0	%
87. Extranjero privado	100.0	%

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	80	20160101		-
2		Año Mes Día		-
3		Año Mes Día		-
4		Año Mes Día		-
5		Año Mes Día		-

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario 14908474061

(415)7707212489984(8020) 000001490847406 1

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
900396176	1	Impuestos de Bogotá 32	

Representación

1

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL PRIN 18	20170829

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Extranjerí 22	667352		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
VICENT	FERNANDEZ	CARLOS	

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

2

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL SUPL 19	20220117

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadan 13	87704446		61061-T

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
VELEZ	CASTRO	HUMBERTO	DE JESUS

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario 14908474061

(415)7707212489984(8020) 000001490847406 1

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
900396176	1	Impuestos de Bogotá 32	

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 13	1423958 1		27398T

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
SALAZAR	GOMEZ	JOSE	IGNACIO

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

135. Fecha de nombramiento
2023 03 31

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 13	1018408876		232325T

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
2022 01 17

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

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	

IDENTIFICACIÓN

24. Tipo de contribuyente	25. Tipo de documento	26. Número de Identificación	27. Fecha expedición
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
CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

36. Nombre comercial	37. Sigla

UBICACIÓN

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

41. Dirección principal
CL 99 # 10 - 19 OF 502 ED TRADE CENTER

42. Correo electrónico r.rojasarias@mnemo.com

43. Código postal	44. Teléfono 1	45. Teléfono 2
0 1 1 0 0 1	3 1 8 3 8 3 5 1 1 7	3 0 1 6 3 2 7 9 8 6

CLASIFICACIÓN

Actividad económica						Ocupación	
Actividad principal		Actividad secundaria		Otras actividades			
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código 1	2	51. Código	52. Número establecimientos
6 2 0 1	2 0 2 3 1 2 1 4						

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	7	1	4	4	8	5	5																			

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

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

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 61. Fecha 2024 - 01 - 16 / 17 : 26: 47

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

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	

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	
Vigencia		
80. Desde	2 0 2 3 1 2 1 3	
81. Hasta	2 0 2 5 1 2 3 1	

Composición del Capital

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

Entidad de vigilancia y control

88. Entidad de vigilancia y control

Estado y Beneficio

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

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario 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

1

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL PRIN 1 8	2 0 2 3 1 1 2 3

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadaní 1 3	8 7 7 0 4 4 6		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
VELEZ	CASTRO	HUMBERTO	DE JESUS

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

2

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL SUPL 1 9	2 0 2 3 1 1 2 3

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadan 1 3	8 0 8 0 8 4 2 0		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
PARRA	GAMBOA	JOHN	JAIRO

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales

001

Espacio reservado para la DIAN

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	

Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales

1

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad
NIT 3 1	9 0 1 4 4 7 9 6 8	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	112. Número de identificación	113. DV	114. Nacionalidad
NIT 3 1	9 0 0 3 9 6 1 7 6	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	112. Número de identificación	113. DV	114. Nacionalidad
NIT 3 1	9 0 1 3 0 6 6 8 7	2	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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario 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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN
POR UNA COLOMBIA MÁS HONESTA

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764062145032

(415)7707212489984(8020) 001876406214503 2

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
901781625	1				

11. Razón social
CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

12. Dirección seccional
Impuestos de Bogotá
Cód. 32

24. Dirección
CL 99 # 10 - 19 OF 502 ED TRADE CENTER

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

La U.A.E. Dirección de Impuestos y Aduanas Nacionales, conforme a la facultad discrecional establecida en el artículo 684 - 2 del Estatuto Tributario y en virtud de lo estipulado en la Resolución 0042 del 05/05/2020, por la cual se dictan otras disposiciones en materia de sistemas de facturación; previo estudio y evaluación de la solicitud realizada por el contribuyente, representante legal o apoderado debidamente acreditado; determina autorizar los rangos de numeración de facturación y/o documento equivalente. En los casos, en que se agote dicha numeración antes de culminar su vigencia, el interesado tendrá derecho a solicitar una nueva autorización, de acuerdo con el tramite establecido.

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

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

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

AUTORIZADO

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

Firma del solicitante

Firma del funcionario autorizado

DIAN
2023-12-18 / 03:12:27 PM
Fecha Acuse de Recibo
Firmado

984. Apellidos y nombres
985. Cargo
989. Dependencia SUBDIRECCION DE FACTURA ELECTRONICA Y SOLUCI
990. Lugar administrativo
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 8770446 1004. DV 3
1005. Cod. Representación Representante Legal Principal
1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

997. Fecha formalización 2023-12-18/15:12:27

DIAN
POR UNA COLOMBIA MÁS HONESTA

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764062145032

(415)7707212489984(8020) 001876406214503 2

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

	29. Establecimiento	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.
1	CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA CL 99 # 10 - 19 OF 502 ED TRADE CENTER	FACTURA ELECTRÓNICA DE VENTA	4	FE	1	5,000	12	AUTORIZACIÓN	1
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

AUTORIZADO

Bogotá, 11 de Junio 2024

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

División de Presupuesto
Documento de Pago

N° ORDEN DE PAGO	5300437368	**FECHA DE CONTABILIZACIÓN**	21.06.2024
N° DE REFERENCIA	15	**FECHA DE PAGO**	08.07.2024

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°**	CTO 173-20
N° FACTURA PROVEEDOR	FE15 RAD 02-2303-202406253746427		

OBSERVACIONES:

INFORMACIÓN PRESUPUESTAL

SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
20001186	6200000102	00010	CTO 173 DE 2023 .	1000048947	5105627820	885.237.430
					AFECTACIÓN PEDIDO	885.237.430

DETALLE DE LA ORDEN DE PAGO

VALOR TOTAL FAC.	885.237.430,00
DESCUENTOS	54.423.505,00
NOTAS CRÉDITOS	0,00
VALOR A PAGAR	830.813.925,00

Usuario: Jessebell Mejias
Fecha de impresión: 01.08.2024

División de Tesorería
Documento de Pago

No. ORDEN DE PAGO	15	**FECHA DE CONTABILIZACION**	08-jul-24
No. DOCUMENTO DE PAGO	5300437368	**FECHA DE DOCUMENTO**	08-jul-24
		FECHA DE COMPENSACION	08-jul-24
PROPUESTA	44486	**FECHA DE LA PROPUESTA**	08-jul-24

RESPONSABLE DEL PAGO

NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO		
No. IDENTIFICACIÓN	8999992844	**TIPO DE IDENTIFICACÓN**	NIT
CONCEPTO	GIRO DE CESANTIAS PARCIALES SEC		

DATOS GENERALES

NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSE		
No. INDENTIFICACION	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:	FE15 RAD 02-2303-202406253746427		
NÚMERO DE CUENTA	2501050101	**TIPO DE CUENTA**	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	830.813.925		

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	5300437368	15	830.813.925	FE15 RAD 02-2303-202406253746427	6200000102	CTO 173 DE 2023