

	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			NOMBRE DE LA SERIE, SUBSERIE O ASUNTOS	NOMBRE DE LA UNIDAD DOCUMENTAL	FECHAS EXTREMAS		SOPORTE O FORMATO		FÍSICO						ELECTRÓNICO			FRECUENCIA DE CONSULTA	OBSERVACIONES
	CÓDIGO OFICINA	SERIE	SUBSERIE			(dd-mm-aaaa)		Físico	Electrónico	UNIDAD DE CONSERVACIÓN						Ubicación	Cantidad de documentos	Tamaño de los documentos		
						Inicial	Final			PAPEL			OTRO							
										Caja	Carpeta	Tomo	Número de folios	Tipo	Cantidad					
1	1501	13	3	Contrato prestación de servicios	Contrato No. 173-2023 CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA - Soportes Informe Seguimiento para pago Nro.22 factura Nro. FE29 orden de pago No. 5300631158	21-oct-24	12-nov-24		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	212	18,7 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				
	PROCESO CONTRATACION		Versión: 1				
INFORME No 22		FACTURA No		FECHA			
No. DE ACEPTACIÓN: 1000052316 / 1000052317 / 1000052318 / 1000052319				21	10	24	
				dd	mm	aaaa	
1. GENERALIDADES DEL CONTRATO							
CONTRATO No 173		DE 2023		TIPO DE CONTRA1 Prestación de servicios			
(Número de Contrato)		(Año de suscripción)		(Prestación de servicios, interventoría, consultoría, Convenio)			
ORDENADOR DEL GASTO SANDRA MILENA BURGOS BELTRAN		SECRETARIA GENERAL					
(Nombre del ordenador del Gasto)		(Cargo del ordenador del Gasto)					
CONTRATISTA CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA		(Escriba el nombre o razón social del contratista)					
TIPO DE INTERVENTORIA Y/O SUPERVISIÓN: INDIVIDUAL ☒		COLEGIADA ☐					
INTERVENTOR Y/O SUPERVISOR Monica Grand Villada		(Escriba nombre del supervisor o interventor del contrato)					
APOYO SUPERVISIÓN Enrique Arrazola		Luz Helena Riaño - Leonardo Rivera					
(Nombre de la persona delegada para apoyar la supervisión del contrato)		(Nombre de la persona delegada para apoyar la supervisión del contrato)					
OBJETO DEL CONTRATO							
CONTRATAR UNIDAD DE CIBERSEGURIDAD QUE PROPORCIONE SERVICIOS DE SEGURIDAD INTEGRADOS AL FONDO NACIONAL DEL AHORRO							
DEPENDENCIA EJECUCIÓN CONTRATO		VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL (Gerencia de Estrategia TI y aseguramiento informatico)					
		(Indique el nombre de la dependencia responsable del contrato)					
PLAZO DE EJECUCIÓN DEL CONTRATO		24 Meses					
		(Indique en este espacio el número de días o de meses para ejecutar el contrato)					
FECHA DE INICIACIÓN DEL CONTRATO		22	DE	dic	DE	2023	
		(Día)		(Mes)		(Año)	
FECHA DE TERMINACIÓN DEL CONTRATO		21	DE	dic	DE	2025	
		(Día)		(Mes)		(Año)	
REGISTRO PRESUPUESTAL No.		5400001604 - 6200000102					
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		ADICIONES		SUSPENSIONES			
No.	PLAZO	No.	VALOR	RP	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	\$ 25.578.551.384,00	70,08%
Valor del pago aprobado con el presente informe	\$ 237.806.030,00	0,65%
VALOR TOTAL EJECUTADO	\$ 25.816.357.414,00	70,73%
Porcentaje de ejecución presupuestal programado a la fecha		70,79%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,06%

OBSERVACIONES

Cuenta 22: administración y soporte en sitio durante el período del 22 de agosto de 2024 al 21 de septiembre de 2024. items 1 al 9 prefactura C-2-23
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	49%
Porcentaje de ejecución de actividades realizado a la fecha	49%
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☒

*Si corresponde a Software del FNA marque la fase correspondiente

Investigación☐Desarrollo☐

OBSERVACIONES

El contratista cumplió a satisfacción con el servicio de administración y soporte en sitio durante el período del 22 de agosto de 2024 al 21 de septiembre de 2024.

(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 DOCIENTOS TREINTA Y SIETE MILLONES OCHOCIENTOS SEIS MIL TREINTA PESOS MCTE (\$ 237.806.030).

5. EVALUACIÓN CONTRATISTA (Escala de 0 - 5)

EVALUACION PARCIAL	
Cumplimiento del contrato	4
Plazos	4
Aspectos administrativos	4

6. CERTIFICACIÓN PARA PAGO

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

CERTIFICA:

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

ANEXOS PRESENTE INFORME

ANEXO	No FOLIOS	DESCRIPCION
Certificado pago Seguridad Social ☒	PDF	Certificaciones, planilla pago parafiscales, CC y T.P.
Informes ☒	PDF	Informe de Supervisión Informe Gestión Proveedor
Actas ☒	PDF	Acta Seguimiento Mensual ANS
OTROS ☒	PDF	Pre-factura Certificación Cuenta Bancaria Rut's Resolución Facturación Certificación Cumplimiento Circular SFC

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

Veintiuno**21**

días del mes de

octubre

de

2024

(día en letras)

(día en números)

(mes en letras)

(Año)

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

Revisó y aprobó:  Enrique Arrazola - Luz Helena Riaño -  Luz Helena Riaño -  Leonardo Rivera - Apoyo a la supervisión

Estadística de datos	Cantidad
Registros transferidos	12

Cl.doc. : RE (Factura bruto) Documento normal					
Reg.prelim.por		NTUIRAN	Contab.por		MRINCONZ
N° doc.	5100002480	Sociedad	1000	Ejercicio	2024
Fe.docum.	24.10.2024	Fecha contab.	24.10.2024	Período	10
Calc.impuestos	☒				
Referen.	29				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202410284171344				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	223,185,955-
2	86	2511950101	CXP PROVED EM/RF		W0	37,036,370
3	91	5130950408	GESTION Y MON SGSI		W0	0
4	86	2511950101	CXP PROVED EM/RF		W0	155,869,770
5	91	5130950401	CENTRO OPER SEG		W0	0
6	86	2511950101	CXP PROVED EM/RF		W0	16,993,200
7	91	5130950408	GESTION Y MON SGSI		W0	0
8	86	2511950101	CXP PROVED EM/RF		W0	27,906,690
9	91	5130950408	GESTION Y MON SGSI		W0	0
10	50	2519051101	SERVICIO 3.5%			6,994,295-
11	50	2519053801	RTE IVA TARIFA GENER			5,695,355-
12	50	2519054408	SERVICIOS 304 BOGOTA			1,930,425-



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 29

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

Fecha y hora Factura	
Generación	24/10/2024, 15:34
Expedición	24/10/2024, 15:50
Vencimiento	23/11/2024

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Administración y soporte de la plataforma XDR contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	3,957,940.00
2	Administración y soporte de la plataforma SOAR contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	17,406,130.00
3	Administración y soporte de la plataforma THREAT INTELLIGENCE contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	33,078,430.00
4	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING. contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	66,632,860.00
5	Administración y soporte Servicio de MONITOREO DE DNS contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	61,978,770.00
6	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT. contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	9,852,010.00
7	Administración y soporte de la plataforma CIBERDEFENSA contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	6,990,060.00
8	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD. contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	10,003,140.00
9	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM). contrato 173-2023 / No de Autorización: 1000052316 / 1000052317 / 1000052318 / 1000052319	1.00	0.00	27,906,690.00

Total items: 9

Valor en Letras:

Doscientos treinta y siete millones ochocientos seis mil treinta pesos m/cte

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2024-11-23 por \$ 237,806,030.00

Observaciones:

bservaciones:
Distribución de ingresos:

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

Total Bruto	199,837,000.00
IVA 19%	37,969,030.00
Total a Pagar	237,806,030.00

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. Número Autorización Electrónica 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: Sigo SAS - Nit 830.048.145-8, Nombre Software: Sigo Nube, Firma electrónica: ver en el XML

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA
NIT 901.781.625-1

CERTIFICA QUE:

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

Para constancia de lo anterior se firma en Bogotá a los Once (11) días del mes de Octubre 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



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

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

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002. Dada en Bogotá D.C., a los Once (11) días del mes de Octubre de 2024.

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

HUMBERTO DE JESUS VELEZ CASTRO

C.C. 8.770.446 de Soledad – Atlántico

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

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

61061-T

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

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

251625 69149



Identificación Plástica C.A. 180017/0118

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

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

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



FIRMA

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 marzo de 2024 y 31 de agosto 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 marzo de 2024 y 31 de agosto del 2024**.
4. El ultimo pago de aportes corresponde a **pensión agosto** del año **2024 y salud septiembre** 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 marzo de 2024 y 31 de agosto 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 cuatro (4) días, del mes de octubre del año 2024.



JAIRO DAVID TOVAR LOZANO

C.C. 1.018.408.876

Revisor fiscal de MNEMO CYBER SEC S.A.S.

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		Valor
2024-08	2024-09	917704172	9473373526	E	2024/09/16	2024/09/16	BANCO BBVA COLOMBIA S.A.		\$28,967,800

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS		PARAFISCALES		
No.	Identificación	Nombre	ing	ret	de	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (29 Afiliados)																														
Centro de Trabajo: CENTRO TRABAJO 1 (28 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (28 Afiliados)																														
1	CC	80180206	AMAZO WALTER	X																230301	11	EPS008	11	CCF24	11	14-25	11	0.522%	11	Si
2	CC	1000985154	ARIAS ANDRES	X																230301	23	EPS010	23	CCF24	23	14-25	23	0.522%	23	Si
3	CC	1233493654	BARGAS JULIAN								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
4	CC	1070981128	COLLAZOS MATEO																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
5	CC	79619776	ENCISO JOHN	X																230301	19	MIN001	19	CCF24	19	14-25	19	0.522%	19	Si
6	CC	1016043734	GARCIA JEISSON								X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
7	CC	91180662	GARRIDO YEINSON																	230301	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
8	CC	1022394508	GUARIN JOHN	X																230301	23	EPS037	23	CCF24	23	14-25	23	0.522%	23	Si
9	CC	1024460422	JIMENEZ BRAYAN	X																25-14	23	EPSC34	23	CCF24	23	14-25	23	0.522%	23	Si
10	CC	1019138524	MALLAMA JOHNNY	X																230301	23	EPS037	23	CCF24	23	14-25	23	0.522%	23	Si
11	CC	13871620	MARTINEZ HECTOR																	230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
12	CC	1023951729	MARTINEZ MAIKOL	X																230201	25	EPS002	25	CCF24	25	14-25	25	0.522%	25	Si
13	CC	1018453849	MERCHAN LUISA								X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
14	CC	1012373695	MONTERO SINDY								X									230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
15	CC	1019024612	MORA MAGDA	X																230301	5	EPS005	5	CCF24	5	14-25	5	0.522%	5	No
16	CC	1023937645	MORENO WENDY								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
17	CC	1233901826	MOYAN CRISTIAN								X									230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
18	CC	1019079260	PABON PEDRO	X																230301	23	EPS037	23	CCF24	23	14-25	23	0.522%	23	Si
19	CC	80093909	PICO MAURO																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
20	CC	1072431635	RAMIREZ RAMIRO								X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
21	CC	1110459814	SANABRIA LUIS	X																25-14	4	EPS005	4	CCF24	4	14-25	4	0.522%	4	Si
22	CC	1073515030	TAYLOR BRANDON																	231001	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
23	CC	79729048	URIBE WILSON																	25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
24	CC	1031143384	URREGO SANDRO								X									230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
25	CC	79992504	VANEGAS YAIR	X																231001	5	MIN001	5	CCF24	5	14-25	5	0.522%	5	Si
26	CC	1015404947	VARGAS JOSE	X																231001	15	EPS010	15	CCF24	15	14-25	15	0.522%	15	Si
27	CC	1070307880	ZAMBRANO OSCAR								X									230201	30	EPS041	30	CCF24	30	14-25	30	0.522%	30	Si
28	CC	1022438994	ZARAMA JUAN	X																230201	23	EPS005	23	CCF24	23	14-25	23	0.522%	23	Si

Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

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		Limite		Pago		Banco		Dias Mora	Valor
2024-08	2024-09	917704172	9473373526	E		2024/09/16	2024/09/16	BANCO BBVA COLOMBIA S.A.				0	\$28,967,800

RESUMEN DE PAGO									
RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR	
AFP (ADMINISTRADORAS: 5)				29	\$17,756,200	\$0	\$0	\$17,756,200	
COLFONDOS	231001	800,227,940	6	3	\$1,173,400	\$0	\$0	\$1,173,400	
COLPENSIONES	25-14	900,336,004	7	5	\$3,936,700	\$0	\$0	\$3,936,700	
PORVENIR	230301	800,224,808	8	13	\$6,166,800	\$0	\$0	\$6,166,800	
PROTECCION	230201	800,229,739	0	7	\$5,289,300	\$0	\$0	\$5,289,300	
SKANDIA	230901	800,253,055	2	1	\$1,190,000	\$0	\$0	\$1,190,000	
ARL (ADMINISTRADORAS: 1)				29	\$631,600	\$0	\$0	\$631,600	
COLMENA	14-25	800,226,175	3	29	\$631,600	\$0	\$0	\$631,600	
CCF (ADMINISTRADORAS: 1)				29	\$4,353,600	\$0	\$0	\$4,353,600	
COMPENSAR	CCF24	860,066,942	7	29	\$4,353,600	\$0	\$0	\$4,353,600	
EPS (ADMINISTRADORAS: 9)				29	\$5,532,700	\$0	\$0	\$5,532,700	
CAPITAL SALUD	EPSC34	900,298,372	9	1	\$72,100	\$0	\$0	\$72,100	
COMPENSAR	EPS008	860,066,942	7	4	\$503,400	\$0	\$0	\$503,400	
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	2	\$172,000	\$0	\$0	\$172,000	
FAMISANAR	EPS017	830,003,564	7	3	\$633,100	\$0	\$0	\$633,100	
FOSYGA	MIN001	901,037,916	1	4	\$736,100	\$0	\$0	\$736,100	
NUEVA E.P.S.	EPS037	900,156,264	2	3	\$239,700	\$0	\$0	\$239,700	
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	\$134,300	\$0	\$0	\$134,300	
SALUD TOTAL	EPS002	800,130,907	4	4	\$634,900	\$0	\$0	\$634,900	
SANITAS	EPS005	800,251,440	6	7	\$2,407,100	\$0	\$0	\$2,407,100	
ICBF (ADMINISTRADORAS: 1)				2	\$416,200	\$0	\$0	\$416,200	
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	2	\$416,200	\$0	\$0	\$416,200	
SENA (ADMINISTRADORAS: 1)				2	\$277,500	\$0	\$0	\$277,500	
SENA	PASENA	899,999,034	1	2	\$277,500	\$0	\$0	\$277,500	
TOTAL				29	\$28,967,800	\$0	\$0	\$28,967,800	

DATOS GENERALES DEL APORTANTE									
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal		Direccion	
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
2024-08	2024-09	920182352	9473415730	E	2024/09/18	2024/09/17	BANCO BBVA COLOMBIA S.A.	0	\$158,592,300

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES															PENSION		SALUD		CCF		RIESGOS		PARAFISCALES				
No.	Identificación	Nombre	ing	ret	ide	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (94 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							25-14	4	EPS001	4	CCF24	0	14-25	4	0.000%	0	No
4	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																	25-14	26	EPS001	26	CCF24	26	14-25	26	1.044%	26	No
5	CC	1122651302	CARO ROA JONATHAN																	230301	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
6	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																	230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
7	CC	1013592039	EMBUSE IPIA JULIAN ANDRES																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
8	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																	25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
9	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO												X					231001	5	EPS005	5	CCF24	5	14-25	5	0.000%	5	Si
10	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO																	231001	25	EPS005	25	CCF24	25	14-25	25	1.044%	25	Si
11	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
12	CC	79865487	PUENTES CASTRO DAVID EDUARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
13	CC	1018429259	RODRIGUEZ MATEUS JEAMY PAMELA																	230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
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			X						X							X	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																	231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
19	CC	24659147	VALDES RAMIREZ ALBA LIBIA																	0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No	
20	CC	79950164	VARGAS HINCAPIE FERNANDO									X								230301	30	EPS002	30	CCF24	30	14-25	30	1.044%	30	Si
21	CC	1032410736	VARGAS HINCAPIE HENRY																	230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
22	CC	1022411758	VARGAS LEON MARIA CAMILA											X						230301	30	EPS008	30	CCF24	0	14-25	30	0.000%	0	Si
23	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																	0	EPS017	30		0	0	0.000%	0		No	
Centro de Trabajo: ADMINISTRACION (69 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (69 Afiliados)																														

24	CC	1014306151	ABRIL MONTES SERGIO LEONARDO							X									23020 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
25	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO								X								25-14	10	EPS005	10	CCF24	0	14-25	10	0.000%	0		Si
26	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO																25-14	20	EPS005	20	CCF24	20	14-25	20	0.522%	20		Si
27	CC	1023953140	ARIAS NATALIA MELIZA							X									23020 1	30	EPS010	30	CCF24	30	14-25	30	0.522%	30		Si
28	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER																23100 1	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
29	CC	1026295259	BEJARANO QUIROGA ANDRES FELIPE							X									25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
30	CC	1019077197	BELEÑO BUELVAS CHARLES JAVIER									X							23020 1	15	EPS005	15	CCF24	15	14-25	15	0.000%	15		Si
31	CC	1019077197	BELEÑO BUELVAS CHARLES JAVIER							X									23020 1	15	EPS005	15	CCF24	15	14-25	15	0.522%	15		Si
32	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER																23020 1	30	MIN001	30	CCF24	30	14-25	30	0.522%	30		Si
33	CC	1004268659	BONILLA ZUÑIGA ANDERSON	X														X	23100 1	19	EPS037	19	CCF24	19	14-25	19	0.522%	19		Si
34	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN									X							23030 1	5	EPS002	5	CCF24	5	14-25	5	0.000%	5		Si
35	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN																23030 1	25	EPS002	25	CCF24	25	14-25	25	0.522%	25		Si
36	CC	13870244	CARRILLO ALVAREZ OSCAR	X														X	25-14	2	EPS002	2	CCF24	2	14-25	2	0.522%	2		Si
37	CC	1034397473	CASTILLO IDROBO JHON FABER							X									23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
38	CC	1020809969	CASTILLO MENDOZA JOHN ALEXANDER							X									23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
39	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID							X									23030 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
40	CC	6319789	ESPAÑA MOSQUERA JESUS ARBEY																23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		No
41	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER																25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
42	CC	1023957895	GIL MURILLO JAVIER EDUARDO							X									23030 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
43	CC	1019009180	GOMEZ ROJAS YENNY PAOLA																23030 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
44	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO																23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
45	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN																23030 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
46	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL							X									23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
47	CC	1076663845	GUAYAZAN CORTES JONATHAN STIVEN	X														X	23030 1	15	EPS005	15	CCF24	15	14-25	15	0.522%	15		Si
48	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES									X							23020 1	13	EPS005	13	CCF24	13	14-25	13	0.000%	13		No
49	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES							X									23020 1	17	EPS005	17	CCF24	17	14-25	17	0.522%	17		No
50	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
51	CC	1099374748	LEAL GOMEZ DANIELA																23020 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
52	CC	52953219	LEON CERON MARIA ALEXANDRA								X								23100 1	7	EPS005	7	CCF24	0	14-25	7	0.000%	0		Si
53	CC	52953219	LEON CERON MARIA ALEXANDRA																23100 1	23	EPS005	23	CCF24	23	14-25	23	0.522%	23		Si
54	CC	1069769484	LOPEZ ZAMORA JUAN DAVID																23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
55	CC	1000149678	LOZANO GUTIERREZ MARIA CAMILA							X									23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
56	CC	1193088387	LUENGAS CORTES DAVID STIVEN							X									23030 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
57	CC	79992827	MARROQUIN GUTIERREZ DIDIER																23020 1	30	MIN002	30	CCF24	30	14-25	30	0.522%	30		Si

58	CC	1000032122	MARTIN GARCES JUAN DAVID								X							230301	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
59	CC	1023885573	MARTINEZ CASAS EDWARD ALEJANDRO								X							25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
60	CC	1000719172	MARTINEZ BECERRA MARIA JOSE								X							230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
61	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE								X							230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
62	CC	1000717997	MELO MOSQUERA DANIEL RENE								X							230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	98632570	MESA MENDEZ CARLOS MANUEL									X						230201	12	MIN001	12	CCF24	12	14-25	12	0.000%	12	Si
64	CC	98632570	MESA MENDEZ CARLOS MANUEL										X					230201	18	MIN001	18	CCF24	18	14-25	18	0.522%	18	Si
65	CC	1022947945	MOLANO JIMENEZ JESUS RICARDO								X							230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
66	CC	1033711407	MURCIA TORRES JHON FREDY									X						230301	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	Si
67	CC	1033711407	MURCIA TORRES JHON FREDY										X					230301	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
68	CC	1034660019	MURCIA CARVAJAL KAROL DANIELA																0	EPS005	30		0		0	0.000%	0	No
69	CC	1011087203	MURCIA GUERRERO SAMUEL																0	EPS037	30		0		0	0.000%	0	No
70	CC	1023907046	OCHOA ROJAS ROGER JULIAN								X							230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
71	CC	1032479763	ORJUELA CALDERON PAULA NATALIA										X					231001	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
72	CC	1032479763	ORJUELA CALDERON PAULA NATALIA								X							231001	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
73	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER								X							230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
74	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN															230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
75	CC	1019127504	PERDOMO GUZMAN JESSICA LILIANA								X							230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
76	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO															230901	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
77	CC	1030618626	PINZON ROJAS ANDRES CAMILO															230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
78	CC	1023972445	PRIETO SILVA NICOL															230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
79	CC	1014201989	QUIROGA PERALTA EDWIN FERNANDO									X						230201	3	EPS010	3	CCF24	0	14-25	3	0.000%	0	Si
80	CC	1014201989	QUIROGA PERALTA EDWIN FERNANDO				X										X	230201	17	EPS010	17	CCF24	17	14-25	17	0.522%	17	Si
81	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN								X							230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
82	TI	1011096205	RIOS MONTAÑEZ DIEGO ALEXANDER																0	EPS037	30		0		0	0.000%	0	No
83	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES								X							25-14	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
84	CC	1003712217	RODRIGUEZ PENAGOS JOAN SEBASTIAN															230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
85	CC	52505417	ROJAS PEÑA NILSA YAMILE															25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
86	CC	1030697447	ROJAS PEREZ VALENTINA								X							230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
87	CC	80734644	SAGANOME MORA OSCAR JAVIER															25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
88	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO															230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
89	CC	1030539604	TAMAYO RIVERA FABIO ANDRES															231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
90	CC	1020808701	TIBADUIZA CALDERON SEBASTIAN															231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
91	CC	1032394709	TOLEDO SALAMANCA WALTER OSWALDO															230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
92	CC	1018408876	TOVAR LOZANO JAIRO DAVID															230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si

Página 4 de 5

DATOS GENERALES DEL APORTANTE										
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS		B - MENOS DE 200 COTIZANTES		PRINCIPAL	CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION										
Periodo		Clave		Tipo	Fecha		Pago			
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Días Mora	Valor	
2024-08	2024-09	920182352	9473415730	E	2024/09/18	2024/09/17	BANCO BBVA COLOMBIA S.A.	0	\$158,592,300	
RESUMEN DE PAGO										
RIESGO		CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES		VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)					88	\$83,959,600	\$0	\$0		\$83,959,600
COLFONDOS		231001	800,227,940	6	9	\$11,094,900	\$0	\$0		\$11,094,900
COLPENSIONES		25-14	900,336,004	7	15	\$14,246,400	\$0	\$0		\$14,246,400
PORVENIR		230301	800,224,808	8	34	\$24,341,400	\$0	\$0		\$24,341,400
PROTECCION		230201	800,229,739	0	27	\$28,933,700	\$0	\$0		\$28,933,700
SKANDIA		230901	800,253,055	2	3	\$5,343,200	\$0	\$0		\$5,343,200
ARL (ADMINISTRADORAS: 1)					90	\$4,155,000	\$0	\$0		\$4,155,000
COLMENA		14-25	800,226,175	3	90	\$4,155,000	\$0	\$0		\$4,155,000
CCF (ADMINISTRADORAS: 1)					90	\$22,349,800	\$0	\$0		\$22,349,800
COMPENSAR		CCF24	860,066,942	7	90	\$22,349,800	\$0	\$0		\$22,349,800
EPS (ADMINISTRADORAS: 10)					95	\$38,642,200	\$0	\$0		\$38,642,200
ALIANSAUD 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	\$192,600	\$0	\$0		\$192,600
COMPENSAR		EPS008	860,066,942	7	15	\$4,394,000	\$0	\$0		\$4,394,000
EPS SURA (ANTES SUSALUD)		EPS010	800,088,702	2	4	\$560,800	\$0	\$0		\$560,800
FAMISANAR		EPS017	830,003,564	7	14	\$2,230,000	\$0	\$0		\$2,230,000
FOSYGA		MIN001	901,037,916	1	7	\$3,390,500	\$0	\$0		\$3,390,500
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	8	\$1,237,600	\$0	\$0		\$1,237,600
SALUD TOTAL		EPS002	800,130,907	4	8	\$954,300	\$0	\$0		\$954,300
SANITAS		EPS005	800,251,440	6	35	\$23,687,400	\$0	\$0		\$23,687,400
ICBF (ADMINISTRADORAS: 1)					12	\$5,691,400	\$0	\$0		\$5,691,400
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR		PAICBF	899,999,239	2	12	\$5,691,400	\$0	\$0		\$5,691,400
SENA (ADMINISTRADORAS: 1)					12	\$3,794,300	\$0	\$0		\$3,794,300
SENA		PASENA	899,999,034	1	12	\$3,794,300	\$0	\$0		\$3,794,300
TOTAL					95	\$158,592,300	\$0	\$0		\$158,592,300

EL SUSCRITO REVISOR FISCAL

C E R T I F I C A

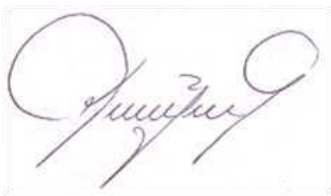
Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO COLOMBIA S.A.S., con NIT 900.396.176-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, 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 abril de 2024 al 04 de octubre 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 (04) cuatro días del mes de octubre 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

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

Acta N°	14	Tema:	Reunión de revisión de ANS, contrato 173 de 2023
Fecha:	11/10/2024	Ubicación:	Virtual.
Hora inicio:	10:00 am	Hora fin:	11:00 am

Objetivo	Reunión de revisión de ANS, contrato 173-2023 para el periodo comprendido entre el 22/08/2024 a 21/09/2024		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	Depende ncia	Cargo	¿Asistió?
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguram iento Informátic o	<u>Profesional 03</u>	Si
Plinio Esteban Palomino López	Mnemo	Gerente de Proyecto Mnemo	Si

TEMAS TRATADOS (Describir los puntos tratados en la reunión)

Revisión cumplimiento de ANS del período del 22 de julio de 2024 al 21 de agosto de 2024.

 1. Acuerdos de niveles de servicio generales	De manera conjunta, el FNA y Mnemo verificaron cada uno de los siguientes niveles de servicio para la actividad desarrollada.	Código GE-GP-FO-001
	GESTIÓN DE PROCESOS Y CALIDAD	Versión: 0

1.1. Documentación

Durante el periodo evaluado se entregaron los siguientes documentos:

- Informe mensual de gestión del 22 de agosto de 2024 al 21 de septiembre de 2024.
- Informes técnicos por solución o servicio

Los anteriores documentos fueron enviados al apoyo a la supervisión de contrato designado por el FNA y cargados en la carpeta respectiva de Transfer.

1.2. Cumplimiento del sistema de gestión de calidad

En materia de cumplimiento de procedimientos, políticas, normas y directrices establecidas por el FNA, no se evidenció incumplimiento alguno por parte del Consorcio Mnemo SOC, por lo que se considera que no hay penalización.

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

1.3. Atención de casos de soporte

Para el tiempo cubierto por la presente revisión, se generaron 15 peticiones de soporte.

PETICIONES

Número	Estado	Título
--------	--------	--------

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

RF405506	Closed	INGRESO DE CORREOS A BUZÓN
RF405514	Closed	URGENTE DESBLOQUEO CORREO RV: CORREO RETENIDO // PROCESO RADICADO 2021-00293 CITA AUDIENCIA ART 77 D
RF405645	Closed	CORREO RETENIDO // ***** ADMISIÓN DE DENUNCIA FISCAL *****
RF405681	Closed	SOLICITUD REVISION CORREO SOSPECHOSO
RF405859	Closed	CORREO SOSPECHOSO
RF405882	Closed	TRASLADO CORREO SOSPECHOSO
RF405883	Closed	CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF405884	Closed	CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF405886	Closed	CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF405890	Closed	CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF406043	Closed	CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF406187	Closed	MESA DE SERVICIO
RF406469	Closed	RV: CORREO RETENIDO // COMO SANCIONAR LA IMPRODUCTIVIDAD DE UN TRABAJADOR
RF406748	Closed	Correo Retenido // Como sancionar la improductividad de un trabajador 2024
RF407214	Closed	[SOC-CERT] ALERTA DE SEGURIDAD FNA_ DARKTRACE 128248
RF407250	Closed	RV: URGENTE CORREO RETENIDO // EXTRAJUDICIAL COMUNICADO –
RF407251	Closed	URGENTE CORREO RETENIDO // EXTRAJUDICIAL COMUNICADO – NOTIFICACIÓN DIAN IMPUESTOS EN MORA EVITE SANC

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

RF407281	Closed	RV: CORREO RETENIDO // FWD: DOCUMENTOS RETIRO PARCIAL DE CESANTÍ COIGO 5DD53C39-FCAA-40F1-9D29-C7746
RF407515	Closed	Urgente desbloqueo RV: Correo Retenido // NORA SANDRA GOMEZ: CONVOCA AUDIENCIA DE REANUDACIÓ
RF407922	Closed	CORREO RETENIDO // CONTRIBUCIó
RF407967	Closed	NOTIFICACION ACTO ADMINISTRATIVO PARA SU RESPECTIVA GESTION
RF408018	Closed	RV: CORREO RETENIDO // NOTIFICACIÓN DE FALLO DE TUTELA PROFERIDO DENTRO DEL RADICADO 2024-78100.
RF408245	Closed	CORREO RETENIDO // CONTRIBUCIó
RF408360	Closed	Solicitud auditoria
RF408473	Closed	CORREO RETENIDO // NOTIFICACIÓ
RF408481	Closed	PRECAUCIÓN CON LOS CORREOS ELECTRÓNICOS SOSPECHOSOS
RF408550	Closed	RV: CORREO RETENIDO // LATAM BANKERS (BANCOS EN LATAM): YOUR INSIGHTS ARE REQUIRED!
RF408573	Closed	CORREO BLOQUEADO INVITACIÓN WEBINAR GRC
RF408740	Closed	RV: CORREO RETENIDO // TRá

CAMBIOS

No se generaron cambios en el periodo

1.4. Cumplimiento del cronograma

El avance en el cronograma del contrato 173-2023 para el periodo en cuestión, a corte de 21-09-24, corresponde al 49% esperado vs 49% completado, sin que se presente desviación general.

A continuación, captura de pantalla del cronograma actualizado:

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

% completado	% completado	Nombre de tarea	Duración	Comienzo	Fin	F
49%	49%	➤ FNA 173 2023	556 días	vie 22/12/23	jue 29/01/26	
100%	100%	➤ Fase de Inicio	6 días	vie 22/12/23	lun 1/01/24	
100%	100%	➤ Fase de planeación	45 días	lun 1/01/24	vie 1/03/24	
48%	48%	➤ Fase de ejecución	556 días	vie 22/12/23	jue 29/01/26	
99%	100%	➤ Implementación de la unidad de ciberseguridad	80 días	jue 8/02/24	mar 28/05/24	
31%	31%	➤ Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25	
30%	30%	➤ Ejecución de actividades de apoyo al plan de sensibilización	486 días	vie 1/03/24	mié 31/12/25	
100%	100%	➤ Ejecución de análisis GAP de herramientas y servicios de ciberseguridad existentes	41 días	lun 15/01/24	lun 11/03/24	
100%	100%	➤ Ejecución de actividades de evaluación de nivel de madurez actual	79 días	mié 27/12/23	lun 15/04/24	
17%	17%	➤ Medición periodica del nivel de madurez (monitoreo y mejora continua)	366 días	lun 22/07/24	mar 9/12/25	
100%	100%	➤ Adquisición de herramientas tecnológicas	6 días	vie 22/12/23	lun 1/01/24	
100%	100%	➤ Despliegue de herramientas tecnológicas	162 días	vie 22/12/23	jue 1/08/24	
76%	100%	➤ Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24	
37%	37%	➤ Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26	
33%	33%	➤ Fase de monitoreo y control	509 días	dom 28/01/24	mar 30/12/25	
33%	33%	➤ Reunión de seguimiento	497,25 días	mar 13/02/24	mar 30/12/25	
33%	33%	➤ Reunión de ANS	507,25 días	dom 28/01/24	lun 29/12/25	
0%	0%	➤ Fase de cierre	75 días	mié 1/10/25	mar 13/01/26	

2. Disponibilidad de Plataformas

2.1. Disponibilidad solución Darktrace

1. Disponibilidad de la plataforma DARKTRACE					
Garantizar la disponibilidad y acceso a los servicios ofrecidos por la plataforma Darktrace					
Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
99,80% de disponibilidad.	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna

Darktrace- dt-21834-01 - 172.17.81.61



2.2. Disponibilidad solución DAM

2. Disponibilidad de la plataforma DATABASE MONITORING					
Garantizar la disponibilidad y acceso a los servicios ofrecidos por las plataformas de DAM					
Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación

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

99,80% disponibilidad.	de	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna
------------------------	----	--	---	---	---	---------

Aggregation/Archive Log						
Start Date: 2024-07-22 00:00:00 End Date: 2024-08-21 00:00:00						
						
Activity Type	Start Time	End Time	Guardian Host Name	Status	Comment	Run Log Id
Import	2024-08-20 07:00:02	2024-08-20 07:02:11	BOGPVPLP00C.fna.gov.co	Succeeded		07302585515dc0a90f45310c109 69a0a505f1a
Clean Static Orphans	2024-08-20 05:30:13	2024-08-20 05:30:13	BOGPVPLP00F.fna.gov.co	Succeeded	Orphans cleanup had already run today	422660883b44c030c41a8bd399 418a8e1aa7b
Purge	2024-08-20 05:30:02	2024-08-20 05:30:12	BOGPVPLP00F.fna.gov.co	Succeeded		7673c670c3395d5f8acaa1b0509 e441b4fa322f
Archive	2024-08-20 05:30:01	2024-08-20 05:30:13	BOGPVPLP00F.fna.gov.co	Succeeded		fc4fac70c33117578abb75425a0e c005d1542f
Clean Static Orphans	2024-08-20 05:16:06	2024-08-20 05:16:06	BOGPVPLP00E.fna.gov.co	Succeeded	Orphans cleanup had already run today	0f711dcaad49bda7d56c500efa70f b1681c0b359f
Purge	2024-08-20 05:15:02	2024-08-20 05:15:13	BOGPVPLP00E.fna.gov.co	Succeeded		93f75a1a5530ca3e5da09185477 4b43c9e9cab0
Archive	2024-08-20 05:15:02	2024-08-20 05:16:06	BOGPVPLP00E.fna.gov.co	Succeeded		d1812481dc0a9800c0c51b0d6b0 0ed05683c0575c
Clean Static Orphans	2024-08-20 05:00:19	2024-08-20 05:00:19	BOGPVPLP00D.fna.gov.co	Succeeded	Orphans cleanup had already run today	ff4f00a8811908fca37d07a15a9 4c051057dab
Purge	2024-08-20 05:00:02	2024-08-20 05:00:14	BOGPVPLP00D.fna.gov.co	Succeeded		56d1acdf9a3059f73f7805470c8aa a8c057a70a
Archive	2024-08-20 05:00:01	2024-08-20 05:00:19	BOGPVPLP00D.fna.gov.co	Succeeded		4ab377aef9158923140a08a0ba 4c630c085a4
Clean Static Orphans	2024-08-20 03:01:48	2024-08-20 03:01:53	BOGPVPLP00F.fna.gov.co	Succeeded		eb990020c37ba5a5513e0d70 08a0a50c12f1e
Purge	2024-08-20 03:00:37	2024-08-20 03:01:23	BOGPVPLP00F.fna.gov.co	Succeeded		44aa237d27b0fc7c0baa5a5804d0e 48ba0b01b0b1
Export	2024-08-20 03:00:02	2024-08-20 03:01:48	BOGPVPLP00F.fna.gov.co	Succeeded		ee951f57b0c055ed7434908bd73 2a44a2520a0c
Clean Static Orphans	2024-08-20 02:03:54	2024-08-20 02:04:06	BOGPVPLP00E.fna.gov.co	Succeeded		dd0b013a5a0a5fadc31329fa23b cd7fa1a59f40
Purge	2024-08-20 02:00:43	2024-08-20 02:03:43	BOGPVPLP00E.fna.gov.co	Succeeded		483ba05a5bc743a8b70e6899d285 34a472330c00c4
Export	2024-08-20 02:00:04	2024-08-20 02:03:54	BOGPVPLP00E.fna.gov.co	Succeeded		49f0a443508f114855d19701c0a 645a2a2f8aa
Clean Static Orphans	2024-08-20 01:12:30	2024-08-20 01:12:30	BOGPVPLP00D.fna.gov.co	Succeeded		78b0c7f00a0a53ca0c1a5534aa 082ba05c0712af
Purge	2024-08-20 01:01:09	2024-08-20 01:03:28	BOGPVPLP00D.fna.gov.co	Succeeded		4c7434ef1710390cb99a232b2106 52738a3f2687
Export	2024-08-20 01:00:03	2024-08-20 01:03:36	BOGPVPLP00D.fna.gov.co	Succeeded		90a75904411ba8a3088a9fa1fa 34a920000a
Import	2024-08-19 07:00:02	2024-08-19 07:02:09	BOGPVPLP00C.fna.gov.co	Succeeded		3a921ff5a0c020b0a9a920c0c34 270a13519918
Clean Static Orphans	2024-08-19 05:30:14	2024-08-19 05:30:14	BOGPVPLP00F.fna.gov.co	Succeeded	Orphans cleanup had already run today	24a7d6d22b377aeb42c37b5a0b3a 8632b172609c

1. Imagen Disponibilidad Plataforma durante el periodo Servidor Agregador

Aggregation/Archive Log						
Start Date: 2024-08-22 00:00:00 End Date: 2024-09-21 00:00:00						
						
Activity Type	Start Time	End Time	Guardian Host Name	Status	Comment	
Import	2024-09-20 07:00:02	2024-09-20 07:08:12	BOGPVPLP00C.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 05:30:41	2024-09-20 05:30:41	BOGPVPLP00F.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-20 05:30:33	2024-09-20 05:30:33	BOGPVPLP00F.fna.gov.co	Succeeded		
Archive	2024-09-20 05:30:02	2024-09-20 05:30:41	BOGPVPLP00F.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 05:16:05	2024-09-20 05:16:05	BOGPVPLP00E.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-20 05:15:02	2024-09-20 05:15:13	BOGPVPLP00E.fna.gov.co	Succeeded		
Archive	2024-09-20 05:15:02	2024-09-20 05:16:06	BOGPVPLP00E.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 05:00:18	2024-09-20 05:00:18	BOGPVPLP00D.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-20 05:00:31	2024-09-20 05:00:14	BOGPVPLP00D.fna.gov.co	Succeeded		
Archive	2024-09-20 05:00:01	2024-09-20 05:00:19	BOGPVPLP00D.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 03:03:59	2024-09-20 03:03:12	BOGPVPLP00F.fna.gov.co	Succeeded		
Purge	2024-09-20 03:00:44	2024-09-20 03:03:02	BOGPVPLP00F.fna.gov.co	Succeeded		
Export	2024-09-20 03:00:04	2024-09-20 03:03:08	BOGPVPLP00F.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 02:06:10	2024-09-20 02:06:29	BOGPVPLP00E.fna.gov.co	Succeeded		
Purge	2024-09-20 02:00:46	2024-09-20 02:04:87	BOGPVPLP00E.fna.gov.co	Succeeded		
Export	2024-09-20 02:00:06	2024-09-20 02:06:10	BOGPVPLP00E.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-20 01:04:53	2024-09-20 01:13:17	BOGPVPLP00D.fna.gov.co	Succeeded		
Purge	2024-09-20 01:01:46	2024-09-20 01:04:46	BOGPVPLP00D.fna.gov.co	Succeeded		
Export	2024-09-20 01:00:04	2024-09-20 01:04:53	BOGPVPLP00D.fna.gov.co	Succeeded		
Import	2024-09-19 07:00:02	2024-09-19 07:08:19	BOGPVPLP00C.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-19 05:31:07	2024-09-19 05:31:07	BOGPVPLP00F.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-19 05:30:33	2024-09-19 05:30:13	BOGPVPLP00F.fna.gov.co	Succeeded		
Archive	2024-09-19 05:30:03	2024-09-19 05:31:08	BOGPVPLP00F.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-19 05:16:06	2024-09-19 05:16:06	BOGPVPLP00E.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-19 05:15:02	2024-09-19 05:15:13	BOGPVPLP00E.fna.gov.co	Succeeded		
Archive	2024-09-19 05:15:02	2024-09-19 05:16:06	BOGPVPLP00E.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-19 05:00:19	2024-09-19 05:00:19	BOGPVPLP00D.fna.gov.co	Succeeded	Orphans cleanup had already run today	
Purge	2024-09-19 05:00:02	2024-09-19 05:00:16	BOGPVPLP00D.fna.gov.co	Succeeded		
Archive	2024-09-19 05:00:02	2024-09-19 05:00:19	BOGPVPLP00D.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-19 03:03:03	2024-09-19 03:03:09	BOGPVPLP00F.fna.gov.co	Succeeded		
Purge	2024-09-19 03:00:44	2024-09-19 03:02:09	BOGPVPLP00F.fna.gov.co	Succeeded		
Export	2024-09-19 03:00:04	2024-09-19 03:03:03	BOGPVPLP00F.fna.gov.co	Succeeded		
Clean Static Orphans	2024-09-19 02:06:28	2024-09-19 02:06:46	BOGPVPLP00E.fna.gov.co	Succeeded		
Purge	2024-09-19 02:01:01	2024-09-19 02:06:16	BOGPVPLP00E.fna.gov.co	Succeeded		
Export	2024-09-19 02:00:05	2024-09-19 02:06:27	BOGPVPLP00E.fna.gov.co	Succeeded		

2. Imagen Disponibilidad Plataforma en el periodo Servidor Colector 1

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

Aggregation/Archive Log					
Start Date: 2024-08-22 00:00:00 End Date: 2024-09-21 00:00:00					
					
Activity Type	Start Time	End Time	Guardium Host Name	Status	Comment
Clean Static Orphans	2024-09-20 05:00:18	2024-09-20 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	Orphans cleanup had already run today
Purge	2024-09-20 05:00:01	2024-09-20 05:00:14	BOGPVPLP000.fna.gov.co	Succeeded	
Archive	2024-09-20 05:00:01	2024-09-20 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-20 01:04:53	2024-09-20 01:13:17	BOGPVPLP000.fna.gov.co	Succeeded	
Purge	2024-09-20 01:01:48	2024-09-20 01:04:46	BOGPVPLP000.fna.gov.co	Succeeded	
Export	2024-09-20 01:00:04	2024-09-20 01:04:53	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-19 05:00:19	2024-09-19 05:00:19	BOGPVPLP000.fna.gov.co	Succeeded	Orphans cleanup had already run today
Purge	2024-09-19 05:00:02	2024-09-19 05:00:15	BOGPVPLP000.fna.gov.co	Succeeded	
Archive	2024-09-19 05:00:02	2024-09-19 05:00:19	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-19 01:03:52	2024-09-19 01:11:45	BOGPVPLP000.fna.gov.co	Succeeded	
Purge	2024-09-19 01:01:45	2024-09-19 01:03:44	BOGPVPLP000.fna.gov.co	Succeeded	
Export	2024-09-19 01:00:04	2024-09-19 01:03:52	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-18 05:00:18	2024-09-18 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	Orphans cleanup had already run today
Purge	2024-09-18 05:00:02	2024-09-18 05:00:14	BOGPVPLP000.fna.gov.co	Succeeded	
Archive	2024-09-18 05:00:02	2024-09-18 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-18 01:03:53	2024-09-18 01:11:43	BOGPVPLP000.fna.gov.co	Succeeded	
Purge	2024-09-18 01:01:45	2024-09-18 01:03:45	BOGPVPLP000.fna.gov.co	Succeeded	
Export	2024-09-18 01:00:04	2024-09-18 01:03:53	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-17 05:00:21	2024-09-17 05:00:21	BOGPVPLP000.fna.gov.co	Succeeded	Orphans cleanup had already run today
Purge	2024-09-17 05:00:02	2024-09-17 05:00:15	BOGPVPLP000.fna.gov.co	Succeeded	
Archive	2024-09-17 05:00:02	2024-09-17 05:00:21	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-17 01:05:04	2024-09-17 01:12:25	BOGPVPLP000.fna.gov.co	Succeeded	
Purge	2024-09-17 01:01:58	2024-09-17 01:04:58	BOGPVPLP000.fna.gov.co	Succeeded	
Export	2024-09-17 01:00:04	2024-09-17 01:05:04	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-16 05:00:18	2024-09-16 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	Orphans cleanup had already run today
Purge	2024-09-16 05:00:02	2024-09-16 05:00:14	BOGPVPLP000.fna.gov.co	Succeeded	
Archive	2024-09-16 05:00:02	2024-09-16 05:00:18	BOGPVPLP000.fna.gov.co	Succeeded	
Clean Static Orphans	2024-09-16 01:03:41	2024-09-16 01:10:53	BOGPVPLP000.fna.gov.co	Succeeded	
Purge	2024-09-16 01:01:34	2024-09-16 01:03:33	BOGPVPLP000.fna.gov.co	Succeeded	

3. *Imagen Disponibilidad Plataforma en el periodo Servidor Colector 2*

Aggregation/Archive Log				
Start Date: 2024-08-22 00:00:00 End Date: 2024-09-21 00:00:00				
				
Activity Type	Start Time	End Time	Guardium Host Name	Status
Clean Static Orphans	2024-09-20 05:16:05	2024-09-20 05:16:05	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-20 05:16:02	2024-09-20 05:16:13	BOGPVPLP000.fna.gov.co	Succeeded
Archive	2024-09-20 05:16:02	2024-09-20 05:16:05	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-20 02:05:10	2024-09-20 02:05:29	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-20 02:00:49	2024-09-20 02:04:57	BOGPVPLP000.fna.gov.co	Succeeded
Export	2024-09-20 02:00:05	2024-09-20 02:05:10	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-19 05:16:05	2024-09-19 05:16:05	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-19 05:16:02	2024-09-19 05:16:13	BOGPVPLP000.fna.gov.co	Succeeded
Archive	2024-09-19 05:16:02	2024-09-19 05:16:05	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-19 02:05:28	2024-09-19 02:05:46	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-19 02:01:01	2024-09-19 02:05:15	BOGPVPLP000.fna.gov.co	Succeeded
Export	2024-09-19 02:00:05	2024-09-19 02:05:27	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-18 05:16:16	2024-09-18 05:16:16	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-18 05:16:03	2024-09-18 05:16:14	BOGPVPLP000.fna.gov.co	Succeeded
Archive	2024-09-18 05:16:02	2024-09-18 05:16:16	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-18 02:05:40	2024-09-18 02:05:58	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-18 02:00:58	2024-09-18 02:05:26	BOGPVPLP000.fna.gov.co	Succeeded
Export	2024-09-18 02:00:05	2024-09-18 02:05:40	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-17 05:16:13	2024-09-17 05:16:13	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-17 05:16:03	2024-09-17 05:16:15	BOGPVPLP000.fna.gov.co	Succeeded
Archive	2024-09-17 05:16:02	2024-09-17 05:16:13	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-17 02:05:37	2024-09-17 02:05:37	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-17 02:00:49	2024-09-17 02:05:05	BOGPVPLP000.fna.gov.co	Succeeded
Export	2024-09-17 02:00:05	2024-09-17 02:05:19	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-16 05:16:11	2024-09-16 05:16:11	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-16 05:16:03	2024-09-16 05:16:14	BOGPVPLP000.fna.gov.co	Succeeded
Archive	2024-09-16 05:16:03	2024-09-16 05:16:11	BOGPVPLP000.fna.gov.co	Succeeded
Clean Static Orphans	2024-09-16 02:05:45	2024-09-16 02:05:01	BOGPVPLP000.fna.gov.co	Succeeded
Purge	2024-09-16 02:00:50	2024-09-16 02:05:29	BOGPVPLP000.fna.gov.co	Succeeded
Export	2024-09-16 02:00:05	2024-09-16 02:05:45	BOGPVPLP000.fna.gov.co	Succeeded

4. *Imagen Disponibilidad Plataforma en el periodo Servidor Colector 3*

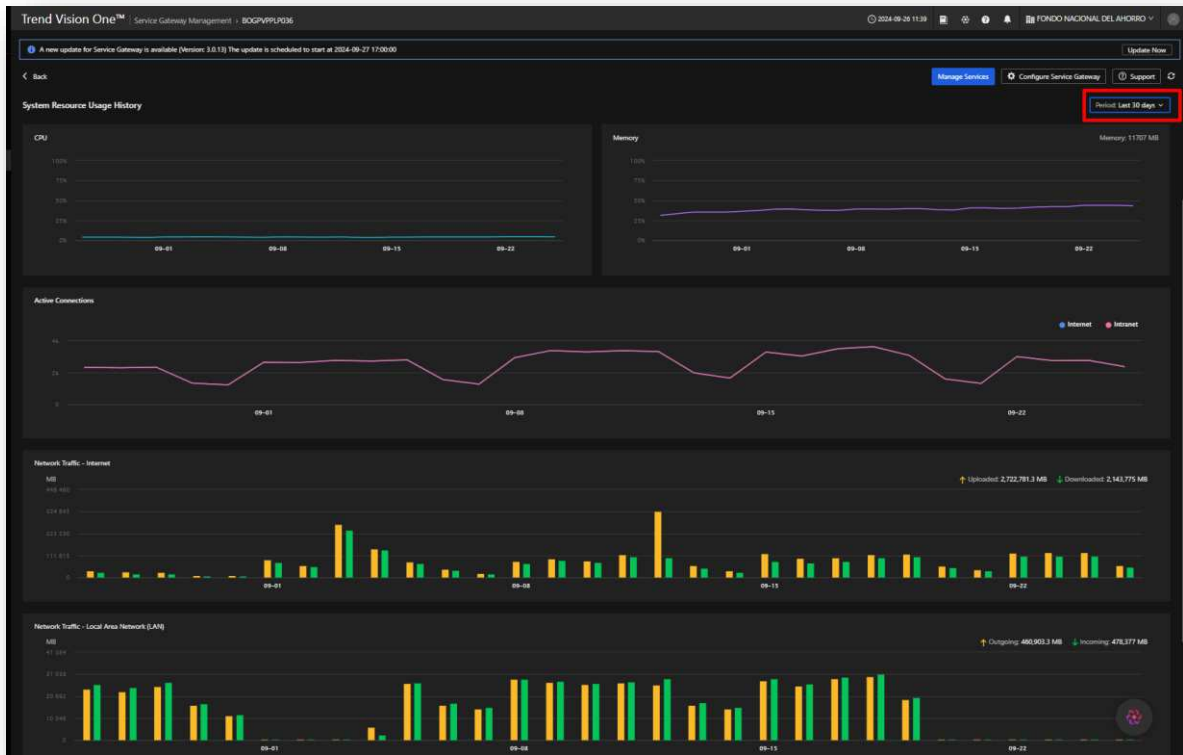
2.3. Disponibilidad solución Antimalware

3. Disponibilidad de la plataforma ANTIMALWARE

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

Garantizar la disponibilidad y acceso a los servicios ofrecidos por las plataformas Antimalware					
Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
99,80% de disponibilidad.	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna

Vision One – Service Gateway 172.16.125.250



BOGPVPPLP037- 172.16.125.214

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

TippingPoint SMS - MNEMOFNA@BOGPVPLP037 - Admin (General)

File Edit View Tools Help

Back
Forward
Events
Reports
Profiles
Responder
Devices
Admin

General
Authentication and Authorization
Certificate Management
Database
Server Properties
High Availability

SMS Server
System Time: 26/09/24 11:45:23 AM CDT
System Uptime: 0 years, 10 weeks, 6 days, 0 hrs, 26 mins, 22 secs

FNABOGWAM - 172.16.125.108

TippingPoint SMS - MNEMOFNA@BOGPVPLP037 - Devices (All Devices - BOGPVPLP00B - Events - System Health)

File Edit View Tools Help

Back
Forward
Events
Reports
Profiles
Responder
Devices
Admin

All Devices
Member Summary
Network Summary
Events
System Health
Performance
Device Users
Traffic Capture
BOGPVPLP00B
Device Configuration
Network Configuration
Authentication
Events

Health Stats
Device: BOGPVPLP00B
Uptime: 0 years, 21 weeks, 5 days, 12 hours, 57 minutes, 57 seconds

Name	State	Current Value	Details
CPU: Data cores	Normal	8%	8 of 100%
CPU: Management cores	Normal	7%	7 of 100%
Disk /user	Normal	1%	166 of 29.924 MB
Disk /var/config	Normal	6%	217 of 3.412 MB
Disk /var/records	Normal	0%	40 of 11.523 MB
Fan: FAN1	Normal	8160 RPM	Thresholds: Major < 2220, Critical < 1980 RPM

11:44:32 a. m.
jueves, 26 de septiembre de 2024

BOGPVPLP00B - 172.16.125.152

TippingPoint SMS - MNEMOFNA@BOGPVPLP037 - Devices (All Devices - BOGPVPLP00B (unlicensed throughput) - Events - System Health)

File Edit View Tools Help

Back
Forward
Events
Reports
Profiles
Responder
Devices
Admin

All Devices
Member Summary
BOGPVPLP00B (unlicensed throughput)
Device Configuration
Network Configuration
Authentication
Events
System Health
Performance
Port Health
Traffic
System Log
Audit Log

Health Stats
Device: BOGPVPLP00B
Uptime: 0 year, 1 week, 1 day, 6 hours, 28 minutes, 27 seconds

Name	State	Current Value	Details
CPU: Data cores	Normal	0%	0 of 100%
CPU: Management cores	Normal	7%	7 of 100%
Disk /user	Normal	0%	44 of 29.924 MB
Disk /var/config	Normal	3%	111 of 3.412 MB
Disk /var/records	Normal	0%	35 of 11.523 MB
Fan: TACH_FAN1	Normal	8100 RPM	Thresholds: Major < 2220, Critical < 1980 RPM

2.4. Disponibilidad Plataformas de Correlación SIEM

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

4. Disponibilidad de la plataforma SOC

Garantizar la disponibilidad y acceso a los servicios ofrecidos por las plataformas de del servicio SOC

Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
99,80% de disponibilidad.	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna

fnabogapp100 - 172.16.132.33

```

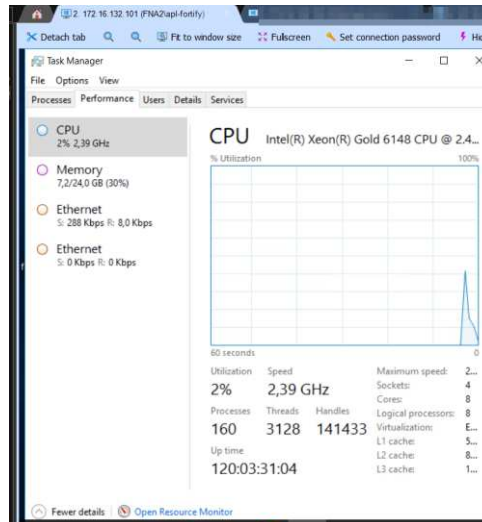
root@fnabogapp100:/root
[root@fnabogapp100 ~]# la
[root@fnabogapp100 ~]# last | grep root
root pts/0 172.19.4.66 Tue Sep 24 09:14 still logged in
root pts/0 172.19.4.66 Wed Sep 18 08:51 - 09:20 (00:28)
root pts/0 10.87.61.56 Fri Sep 13 07:14 - 07:14 (00:00)
root pts/0 172.19.4.66 Wed Sep 11 15:24 - 15:43 (00:18)
root pts/0 172.19.4.66 Tue Sep 10 09:22 - 18:54 (09:31)
root pts/0 10.87.61.56 Tue Sep 10 05:45 - 05:46 (00:00)
root pts/0 172.19.4.66 Mon Sep 9 11:48 - 15:15 (03:26)
root pts/1 172.19.4.66 Fri Sep 6 10:50 - 10:17 (2+23:27)
root pts/0 172.19.4.66 Wed Sep 4 10:59 - 10:17 (4+23:18)
root pts/0 172.19.4.66 Wed Sep 4 10:56 - 10:58 (00:01)
root pts/0 172.19.4.66 Mon Sep 2 16:05 - 18:42 (1+02:36)
root pts/0 172.19.4.66 Fri Aug 30 10:41 - 10:42 (00:01)
root pts/0 172.19.4.66 Mon Aug 26 18:10 - 13:09 (18:58)
root pts/0 172.19.4.66 Wed Aug 14 18:16 - 01:36 (1+07:19)
root pts/0 172.19.4.66 Wed Aug 14 11:12 - 14:09 (02:56)
root pts/0 10.87.61.56 Fri Aug 9 07:20 - 07:20 (00:00)
root pts/0 172.19.4.66 Fri Jul 26 19:13 - 11:19 (2+16:05)
root pts/0 172.19.4.66 Fri Jul 26 19:12 - 19:13 (00:01)
root pts/0 172.19.4.66 Fri Jul 26 09:42 - 09:53 (00:11)
root pts/0 172.19.4.66 Wed Jul 24 10:18 - 11:35 (01:17)
root pts/0 172.19.4.66 Tue Jul 23 17:25 - 17:26 (00:00)
root pts/0 172.19.4.66 Fri Jul 12 16:06 - 08:56 (16:49)
root pts/0 172.19.4.66 Fri Jul 12 11:05 - 14:14 (03:09)
root pts/0 172.19.4.66 Fri Jul 5 15:06 - 00:32 (2+09:25)
root pts/0 172.19.4.66 Fri Jun 28 14:01 - 18:03 (04:02)
root pts/1 10.87.61.56 Mon Jun 24 02:48 - 03:04 (00:16)
root pts/0 172.19.4.66 Fri Jun 21 10:25 - 10:35 (4+00:10)
root pts/1 10.87.61.56 Wed Jun 19 02:43 - 03:31 (00:48)
root pts/2 10.87.61.56 Tue Jun 18 22:27 - 22:43 (00:16)
root pts/1 10.87.61.56 Tue Jun 18 22:09 - 22:54 (00:44)
root pts/0 172.19.4.66 Tue Jun 18 09:35 - 11:11 (1+01:36)
root pts/0 172.19.4.66 Mon Jun 17 17:56 - 09:34 (15:38)
root pts/0 172.19.4.66 Mon Jun 17 09:14 - 10:24 (01:09)
root pts/1 10.87.61.56 Fri Jun 14 18:00 - 18:21 (00:20)
root pts/0 172.19.4.66 Fri Jun 14 17:41 - 00:58 (1+07:17)
root pts/0 172.19.4.66 Fri Jun 14 12:10 - 17:38 (05:27)
root pts/1 10.87.61.56 Fri Jun 14 11:22 - 11:25 (00:03)
root pts/1 10.87.61.56 Fri Jun 14 10:04 - 10:10 (00:06)
root pts/1 10.87.61.56 Fri Jun 14 09:54 - 09:57 (00:03)
root pts/1 10.87.61.56 Fri Jun 14 09:38 - 09:46 (00:07)

```

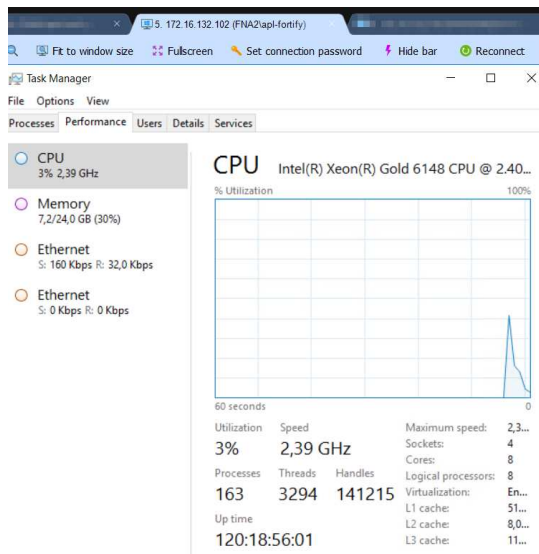
	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTIÓN DE PROCESOS Y CALIDAD	Versión: 0

2.5. Disponibilidad Secure Development Assesment (Fortify)

Fortify – 172.16.132.101

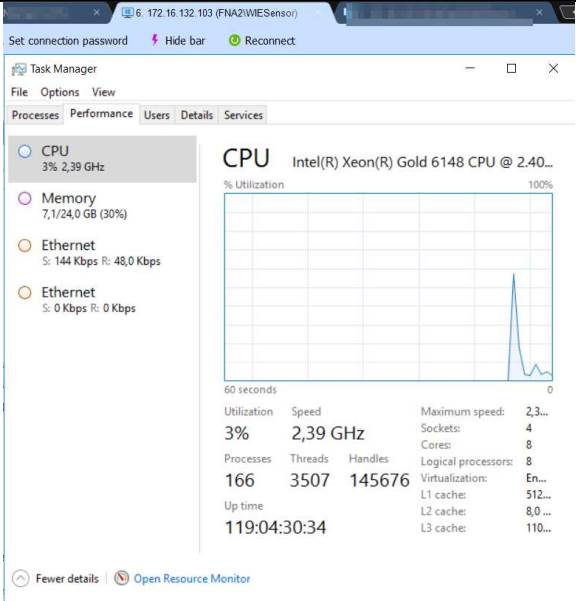


Fortify – 172.16.132.102

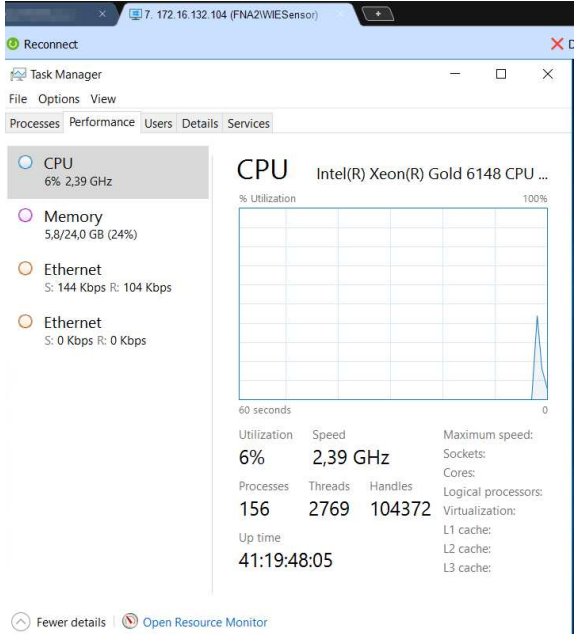


Fortify – 172.16.132.103

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



Fortify – 172.16.132.104



2.6. Disponibilidad monitoreo especiales DNS

Unit	Status	HA Role	Up Time	CPU Usage	Memory Usage	Log Disk Usage	HTTP Connections	HTTP Throughput
FV-1KET119900223	%	PRIMARY	137 days 17 hours 5 minutes				Total Connections: 1158 Total Connections/Sec: 10	Throughput: 59.581 Mbps
FV-1KET119900233	%	SECONDARY	137 days 17 hours 3 minutes				Total Connections: 0 Total Connections/Sec: 0	Throughput: 0.000 Kbps

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

2.7. Disponibilidad monitoreo especiales Portales Web

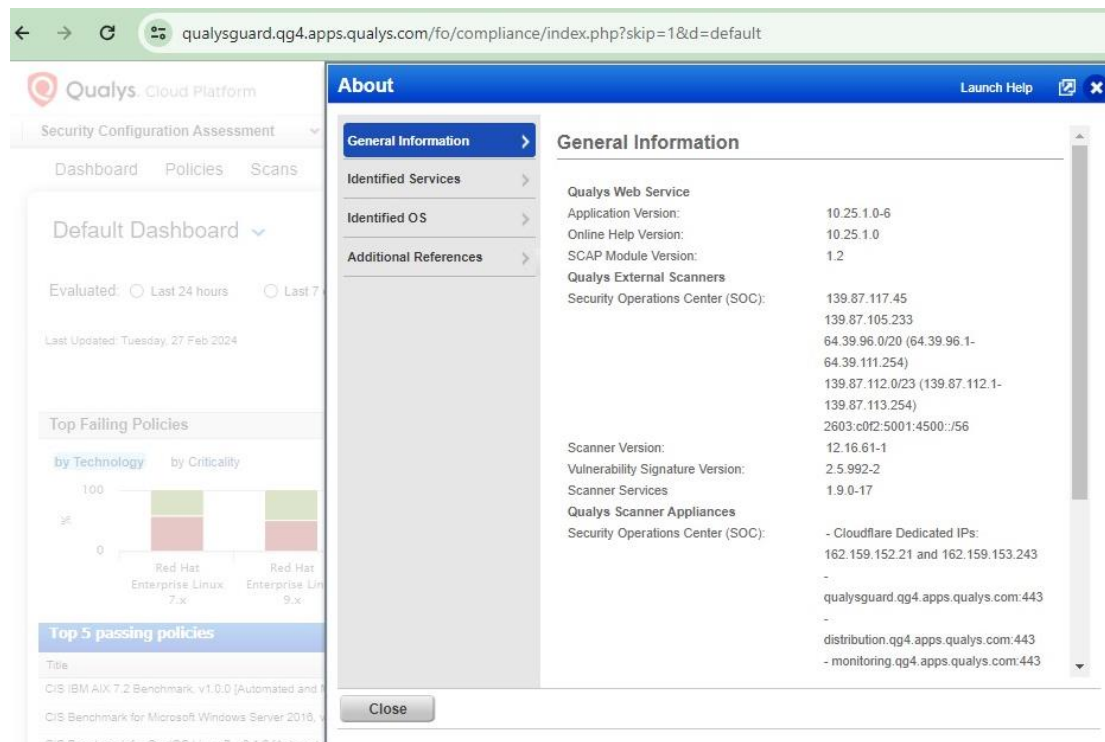


2.8. Disponibilidad Plataforma Qualys

5. Disponibilidad de la plataforma QUALYS

Garantizar la disponibilidad y acceso a los servicios ofrecidos por la plataforma de Líneas Base

Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
99,80% de disponibilidad.	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna



The screenshot shows the Qualys Cloud Platform interface. The main content area displays the 'About' section, which includes a sidebar with 'General Information' and a main panel with 'General Information'. The 'General Information' panel lists various services and their versions, including Qualys Web Service, Application Version, Online Help Version, SCAP Module Version, Qualys External Scanners, Security Operations Center (SOC), Scanner Version, Vulnerability Signature Version, Scanner Services, Qualys Scanner Appliances, and Security Operations Center (SOC). The 'Close' button is visible at the bottom of the sidebar.

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

3. Anexo 2.1 – Otros ANS adicionales

De acuerdo con la revisión realizada, para los ANS adicionales contemplados en el Anexo 2.1, no se evidenciaron penalidades aplicables al periodo en cuestión. A continuación, se relacionan los ANS del Anexo 2.1:

3.1. Recurso Humano

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

3.2. Facturación

- Se realiza la entrega y radicación de documentación soporte requerida junto con la Prefactura y factura en los tiempos establecidos, por tal motivo no se genera penalidad.

3.3. Modelo de Gestión de Incidentes de Seguridad.

- Durante el periodo revisado no se generaron casos de incidentes de seguridad en la infraestructura de FNA, por lo que se considera que no existe penalización por este ítem.

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

3.4. Modelo de Gestión de Requerimientos.

- Se realizó la actualización y entrega de matriz de comunicación, escalamiento jerárquico y funcional y para realizar la gestión de incidentes, de acuerdo con el horario del servicio y horario de soporte contratado, sin embargo, durante el periodo revisado no se generaron requerimientos por parte de FNA o incumplimientos asociados a los requerimientos, por lo que se considera que no existe penalización por este ítem.

3.5. Modelo de Gestión de Problemas.

- Durante el periodo revisado no se generaron requerimientos problemas y tareas de problemas por parte de FNA, por lo que se considera que no existe penalización por este ítem.

3.6. Modelo de Gestión de Cambios.

- Durante el periodo revisado no se generaron requerimientos de los cuales cumplieron con los lineamientos del procedimiento de cambios, por lo que se considera que no existe penalización por este ítem.

3.7. Modelo de Gestión Aseguramiento.

- Con el fin de dar cumplimiento a los procedimientos que garantizan el aseguramiento de la infraestructura del FNA se da cumplimiento a los procedimientos definidos que cuentan con monitoreo permanente, sin embargo, no se tienen vulnerabilidades identificadas que requieren remediación, por lo que se considera que no existe penalización por este ítem.

3.8. Monitoreo de marca.

- Durante el periodo en mención se ejecutó el servicio de monitoreo de marca del FNA con las herramientas y recurso humano especializado para realizar el monitoreo del servicio en Dark web, Deep web, redes sociales, buscadores, entre otros, por lo que se considera que no existe penalización por este ítem.

3.9. Análisis comportamiento usuarios.

- Durante el periodo en mención se realizaron las validaciones relacionadas con este tipo de tendencias, a través de estas, no se han presentado incidentes asociados al parámetro de análisis de comportamiento de usuarios, por lo que se considera que no existe penalización por este ítem.

4. Riesgos del proyecto

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

5. Informe de ejecución presupuestal

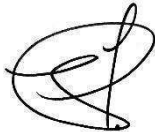
DESCRIPCIÓN	VALOR	PORCENTAJE
Valor inicial del contrato	\$ 36.499.583.610	100,00%
Adiciones	\$ -	0,00%
VALOR TOTAL DEL CONTRATO	\$ 36.499.583.610	100,00%
Valor Ejecutado antes del presente pago	\$ 25.971.281.134	71,16%
Valor del pago aprobado con el presente informe	\$ 237.806.030	0,65%
VALOR TOTAL EJECUTADO	\$ 26.209.087.164	71,81%
Descuento por ANS	\$ -	
DIFERENCIA EN LA EJECUCIÓN PRESUPUESTAL DEL CONTRATO	\$ -	

6. Determinación del valor a facturar

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	\$ 3.326.000	\$ -	\$ 3.326.000	\$ 631.940	\$ 3.957.940
Administración y soporte de la plataforma SOAR	\$ 14.627.000	\$ -	\$ 14.627.000	\$ 2.779.130	\$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	\$ 27.797.000	\$ -	\$ 27.797.000	\$ 5.281.430	\$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	\$ 55.994.000	\$ -	\$ 55.994.000	\$ 10.638.860	\$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	\$ 52.083.000	\$ -	\$ 52.083.000	\$ 9.895.770	\$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	\$ 8.279.000	\$ -	\$ 8.279.000	\$ 1.573.010	\$ 9.852.010
Administración y soporte de la plataforma CIBERDEFENSA	\$ 5.874.000	\$ -	\$ 5.874.000	\$ 1.116.060	\$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	\$ 8.406.000	\$ -	\$ 8.406.000	\$ 1.597.140	\$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	\$ 23.451.000	\$ -	\$ 23.451.000	\$ 4.455.690	\$ 27.906.690
Valor Total	\$ 199.837.000	\$ -	\$ 199.837.000	\$ 37.969.030	\$ 237.806.030

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

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

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. 22

Recurrente mensual (administración y soporte en sitio) plataformas XDR, Threat Intelligence Platform (TIP), BRAND CIBERSECURITY MONITORING (Monitoreo Marca), servicio de Monitoreo DNS, Secure Development Assessment (Fortify), Ciberdefensa (DarkTrace), Lineas Base (QUALYS), monitoreo Bases de datos (DAM) y SOAR del periodo comprendido del 22 de agosto de 2024 al 21 de septiembre de 2024.

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

Bogotá, D.C. octubre 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 de los servicios de administración y soporte en sitio prestados por el contratista durante el período del **22 de agosto de 2024 al 21 de septiembre de 2024** referente al **9no** mes de recurrente mensual de las plataformas que hacen parte de los servicios de la Unidad de ciberseguridad, a saber:

1. XDR
2. Threat Intelligence Platform (TIP)
3. BRAND CIBERSECURITY MONITORING (Monitoreo Marca)
4. Servicio de Monitoreo DNS
5. Secure Development Assessment (Fortify)
6. Ciberdefensa (DarkTrace)
7. Líneas Base (QUALYS)
8. Monitoreo Bases de Datos (DAM)
9. SOAR

3. OBJETIVO DEL INFORME

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

4. OBJETIVOS ESPECÍFICOS DEL INFORME

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

5. INFORME DE AVANCE

De acuerdo con lo establecido en el CTO 173 de 2023, se realiza el seguimiento, control y verificación del servicio de administración y soporte en sitio prestados por el contratista durante el período del **22 de agosto de 2024 al 21 de septiembre de 2024**, donde se detalla lo siguiente:

Las actividades más relevantes realizadas de administración y soporte por plataformas se indican a continuación:

1. XDR

- En XDR los eventos con mayor cantidad de registros están relacionados con la herramienta de CCleaner
- El ips registra un total de 116134 eventos para el periodo del informe.
- se recomienda validar la lista de aplicaciones no permitidas, para alimentar la base de aplicaciones restringidas.
- se continua con la validación de reglas de las diferentes soluciones de Trend Micro, con el fin de optimizar las políticas, activando las reglas recomendadas de acuerdo a las mejores prácticas.
- Se realiza depuración de los dispositivos sin comunicación en los últimos meses, versiones de productos se encuentran en su mayoría cerca al 100 %
- Se realizaron análisis de sandbox, sobre los archivos mediante peticiones por correo, sin IOC activas para ninguna de las muestras
- Se agregaron las exclusiones para la solución de Device Control.
- 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 1987 hasta el momento del informe.
 - Se mitigaron los 864 eventos presentados en los equipos final y 21 eventos de bloqueo en servidores.
 - El IPS analizó 116134 eventos de los cuales 39% fueron categorizados con severidad menor.
 - 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.
 - Se recomienda realizar la mitigación de la vulnerabilidad Apache Struts2 Remote Code Execution Vulnerability (CVE-2017-5638) realizando la actualización de apache en los servidores BOGPVPPLP001,BOGPVPPLP002 y BOGPVPPLP003
 - El módulo de Attack Surface Discovery detectó los equipos bogvpplp015 y bogvpplp019 con clasificación alta por tener más de 35 vulnerabilidades.
 - No se identifican dominios ni ips con clasificación alta por parte Attack Surface Discovery
 - Las cuentas Admin 365 y Backup son las cuentas con clasificación de riesgo alto debido a los permisos asignados y la desactivación del vencimiento de la contraseña.
 - En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 81 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.
 - Análisis de muestra aportada por el equipo de monitoreo de herramientas de FNA.
 - 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.

2. THREAT INTELLIGENCE

Actividades de Gestión de la plataforma

- Se generaron 48 alertas y eventos en MISP.
- De las 48 alertas se han extraído un total de 22.734 indicadores de compromiso.
- Los indicadores de compromiso se han compartido con la herramienta de inteligencia de amenazas TIP para la integración con otras herramientas de seguridad.
- Las amenazas encontradas fueron perpetradas por 12 actores de amenazas identificados.
- Fueron generadas 11 alertas que contienen información sobre vulnerabilidades que pueden afectar la infraestructura de la compañía.
- Las alertas tempranas se han compartido junto a la solución o mitigación brindada por el fabricante responsable de publicar las actualizaciones de los productos afectados.
- 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 continúa el seguimiento con respecto a la integración entre TIP y XDR Vision One con el fin de entregar indicadores de compromiso que mejoren la detección temprana de amenazas en sus fases iniciales y de conexión a servidores de Comando y Control C2.
- Se ajusta la priorización y enriquecimiento de los indicadores de compromiso que son ingestados por la plataforma de inteligencia de amenazas.
- Se crean investigaciones realizadas a determinadas amenazas, asociando indicadores de compromiso, actores de amenazas y campañas utilizadas.

Threat Hunting

- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se crearon 2 reglas Sigma en la que se identifican comportamientos de ofuscación y ejecución.
- La primera regla SIGMA detecta la descarga de artefactos maliciosos a través de comandos ofuscados.
- Para la segunda regla sigma, se identificó un proceso que utiliza el ejecutable "fsutil" para sobre escribir el contenido de un archivo legítimo.

-
- Se realizó un análisis focalizado sobre la amenaza conocida como ELPACO Ransomware, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.

3. BRAND CYBERSECURITY MONITORING

Actividades de Gestión de la plataforma de monitoreo de marca

- 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

4. SECURE DEVELOPMENT ASSESSMENT

Actividades de Gestión de la plataforma Fortify

- Se realiza una verificación periódica del estado de cada servidor y los componentes que aloja la suite de Fortify. Hasta el 21 de septiembre, los servidores y la aplicación no han presentado ninguna falla que haya afectado la disponibilidad del servicio.
 - **Fortify Source Code Analyzer (SCA):** Actualización de las últimas reglas de análisis y parches de seguridad.
 - **Software Security Center (SSC):** Validar funcionamiento y actualizaciones de las políticas de seguridad personalizadas para la ejecución de informes de las aplicaciones auditadas.
 - **Fortify WebInspect Enterprise (WIE):** Se valida la integración con el módulo SSC para asegurarse de que no se estén generando errores, y se realiza un monitoreo constante del estado de los escaneos ejecutados.
 - **Fortify WebInspect Sensor (WIS):** Se valida el estado del sensor para asegurar la disponibilidad del módulo WebInspect.
- Por medio de la mesa de ayuda se restablecen credenciales usuarios de dominio suite fortify.
- En la suite, están configurados los usuarios correspondientes para la administración y ejecución de la suite de Fortify
- Actualización de Rulpacks del módulo SSC.
- Actualización de Rulpacks del módulo Audith WorkBench.

5. MONITOREO DNS

Actividades de Gestión de la plataforma INFOBLOX

- Monitoreo de plataforma Infoblox para la verificación de conexiones sospechosas y maliciosas.
- Actualización de la plataforma Infoblox.
- 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.
- Para el periodo en mención se evidencia un aumento 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 disminuyó en la resolución de DNS.

6. MONITOREO DE LINEAS BASE DE SEGURIDAD

Actividades de Gestión de la plataforma QUALYS

- 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
- Solicitud información dispositivos de red faltantes, progreso con 192.168.35.130, 192.168.39.130 y 192.168.43.130, pendiente 192.168.64.249
- Solicitud de instalación Cloud Agent en Windows (C62893)
- Solicitud de instalación Cloud Agent en Linux (C62010)
- Solicitud de información sobre servidores AIX sin reportar en más de un mes
- Solicitud de información sobre servidores Windows sin reportar en más de un mes
- identificación de causa de duplicidad de activos, en su mayoría se trató de reinstalaciones o migraciones de OS, estos duplicados fueron eliminados manualmente. En su mayoría AIX y RedHat

7. CIBERDEFENSA

Actividades de Gestión de la plataforma DARKTRACE

- 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 genera exclusión de los modelos Suspicious SMB Scanning Activity, SMB Enumeration, Unusual Internal EXE File Transfer. De acuerdo alerta reportada 46580.
- Se realiza revisión de correo retenido por LINK del usuario vgomez@fna.gov.co, el cual por tiempo de retención no se puede liberar, solicitud desde seguridad de la información.
- Se realiza solicitud al área de redes, para suministrar archivo con información de las Subredes de FNA, SD1114412
- Se realiza revisión de los correos las cuentas de correo gerenciadejuzgamiento@fna.gov.co y zespinoza@fna.gov.co, de las cuales no se evidencian registros de correos retenidos, Solicitud por correo electrónico
- Se genera informe detallado de la alerta reportada 46992 del equipo DESKTOP-BDRKOTP
- 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.

8. DAM

- Pruebas de ofuscamiento.
- Tarjeta red appliance.
- Monitoreo roles 60 y 222 COBIS.
- Monitoreo transacciones SAP Hana.
- Definición reglas COBIS producción.
- Adición reglas en políticas generales.

9. SOAR

- Para este periodo se realizó un incremento de 5 casos de uso.
- Para este periodo se identificó un aumento en el alertamiento con respecto al periodo anterior, debido a que se está realizando un proceso de para descartar falsos positivos y así realizar el respectivo afinamiento de las herramientas de monitoreo.
- Se identifican fuentes y estados para las integraciones dispuestas para SOAR, a saber:

APP DESPLEGADAS	
Cisco Firepower	En Pruebas
Trend Micro Vision One	OPERATIVA
FortiWeb	INTEGRADA

- Actualmente se tienen disponible para Fortiweb 20 playbook los cuales permiten la interacción y ejecución de tareas automatizadas.
- En el periodo evaluado se realizaron un total de 64 investigaciones, cada una de ellas se convirtió en una alerta preventiva que fue compartida vía correo electrónico y eventos en MISP.
- En el periodo evaluado se generaron 16 alertas tempranas, cada una de ellas fue compartida vía correo electrónico.

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	\$ 25.578.551.384,00	70,08%
Valor del pago aprobado con el presente informe	\$ 237.806.030,00	0,65%
VALOR TOTAL EJECUTADO	\$ 25.816.357.414,00	70,73%
Porcentaje de ejecución presupuestal programado a la fecha		70,79%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,06%

Se define que el avance presupuestal del contrato a la fecha va de acuerdo con lo planeado 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 el servicio de administración y soporte en sitio durante el período del **22 de agosto de 2024 al 21 de septiembre de 2024**.

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

Porcentaje de ejecución proyectado	49%
Porcentaje de ejecución realizado	49%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	0%

% completado	% completado	Nombre de tarea	Duración	Comenzó	Fin
49%	49%	FNA 173 2023	556 días	vie 22/12/23	jue 29/01/26
100%	100%	↳ Fase de Inicio	6 días	vie 22/12/23	lun 1/01/24
100%	100%	↳ Fase de planeación	45 días	lun 1/01/24	vie 1/03/24
48%	48%	↳ Fase de ejecución	556 días	vie 22/12/23	jue 29/01/26
99%	100%	↳ Implementación de la unidad de ciberseguridad	80 días	jue 8/02/24	mar 28/05/24
31%	31%	↳ Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25
30%	30%	↳ Ejecución de actividades de apoyo al plan de sensibilización	486 días	vie 1/03/24	mié 31/12/25
100%	100%	↳ Ejecución de análisis GAP de herramientas y servicios de ciberseguridad existentes	41 días	lun 15/01/24	lun 11/03/24
100%	100%	↳ Ejecución de actividades de evaluación de nivel de madurez actual	79 días	mié 27/12/23	lun 15/04/24
17%	17%	↳ Medición periódica del nivel de madurez (monitoreo y mejora continua)	366 días	lun 22/07/24	mar 9/12/25
100%	100%	↳ Adquisición de herramientas tecnológicas	6 días	vie 22/12/23	lun 1/01/24
100%	100%	↳ Despliegue de herramientas tecnológicas	162 días	vie 22/12/23	jue 1/08/24
76%	100%	↳ Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24
37%	37%	↳ Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26
33%	33%	↳ Fase de monitoreo y control	509 días	dom 28/01/24	mar 30/12/25
33%	33%	↳ Reunión de seguimiento	497,25 días	mar 13/02/24	mar 30/12/25
33%	33%	↳ Reunión de ANS	507,25 días	dom 28/01/24	lun 29/12/25
0%	0%	↳ Fase de cierre	75 días	mié 1/10/25	mar 13/01/26

6. NIVELES DE SERVICIO

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

VALOR A FACTURAR

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	\$ 3.326.000	\$ -	\$ 3.326.000	\$ 631.940	\$ 3.957.940
Administración y soporte de la plataforma SOAR	\$ 14.627.000	\$ -	\$ 14.627.000	\$ 2.779.130	\$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	\$ 27.797.000	\$ -	\$ 27.797.000	\$ 5.281.430	\$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	\$ 55.994.000	\$ -	\$ 55.994.000	\$ 10.638.860	\$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	\$ 52.083.000	\$ -	\$ 52.083.000	\$ 9.895.770	\$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	\$ 8.279.000	\$ -	\$ 8.279.000	\$ 1.573.010	\$ 9.852.010
Administración y soporte de la plataforma CIBERDEFENSA	\$ 5.874.000	\$ -	\$ 5.874.000	\$ 1.116.060	\$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	\$ 8.406.000	\$ -	\$ 8.406.000	\$ 1.597.140	\$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	\$ 23.451.000	\$ -	\$ 23.451.000	\$ 4.455.690	\$ 27.906.690
Valor Total	\$ 199.837.000	\$ -	\$ 199.837.000	\$ 37.969.030	\$ 237.806.030

7. VERIFICACIÓN DE ENTREGABLES

Por el desarrollo de las actividades ejecutadas en cuanto a los servicios de soporte y administración en sitio de las plataformas descritas en el presente documento, el contratista ha facilitado los siguientes entregables producto de las actividades gestionadas y acordadas en el cronograma de trabajo:

Seguimiento a Entregables del Periodo				
Nº.	Nombre del entregable	Criterio de aceptación	Fecha de entrega	Observaciones
1	Informe-FNA-173-septiembre-2024.pdf	Bueno	28/09/2024	Ninguna

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

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

8. CONCLUSIÓN

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de **DOCIENTOS TREINTA Y SIETE MILLONES OCHOCIENTOS SEIS MIL TREINTA PESOS MCTE (\$ 237.806.030).**



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

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 18 días del mes de octubre 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

LEONARDO RIVERA PEREZ
Profesional 04
Apoyo supervisión CTO 173 de 2023

LUZ H. RIAÑO MORENO
Profesional 04
Apoyo supervisión CTO 173 de 2023



Fuentes

78

Activas

Informe SOC / SIEM /SOAR

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 agosto y el 21 de septiembre de 2024 comprendiendo los siguientes temas

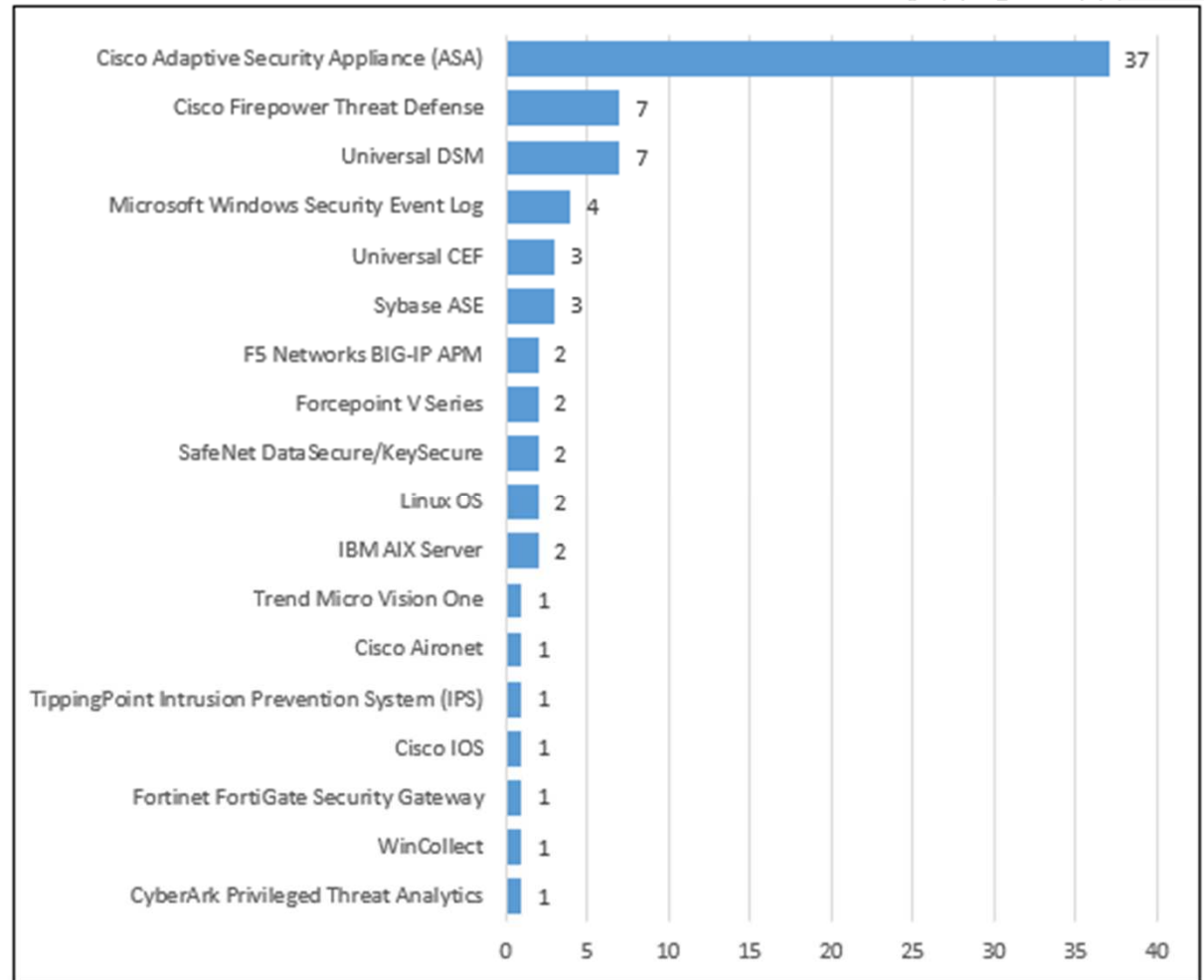
Los temas a tratar sobre este informe son:

- 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 78 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	DESARROOLLOS
[-] Universal CEF	3	
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_Admininfo_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

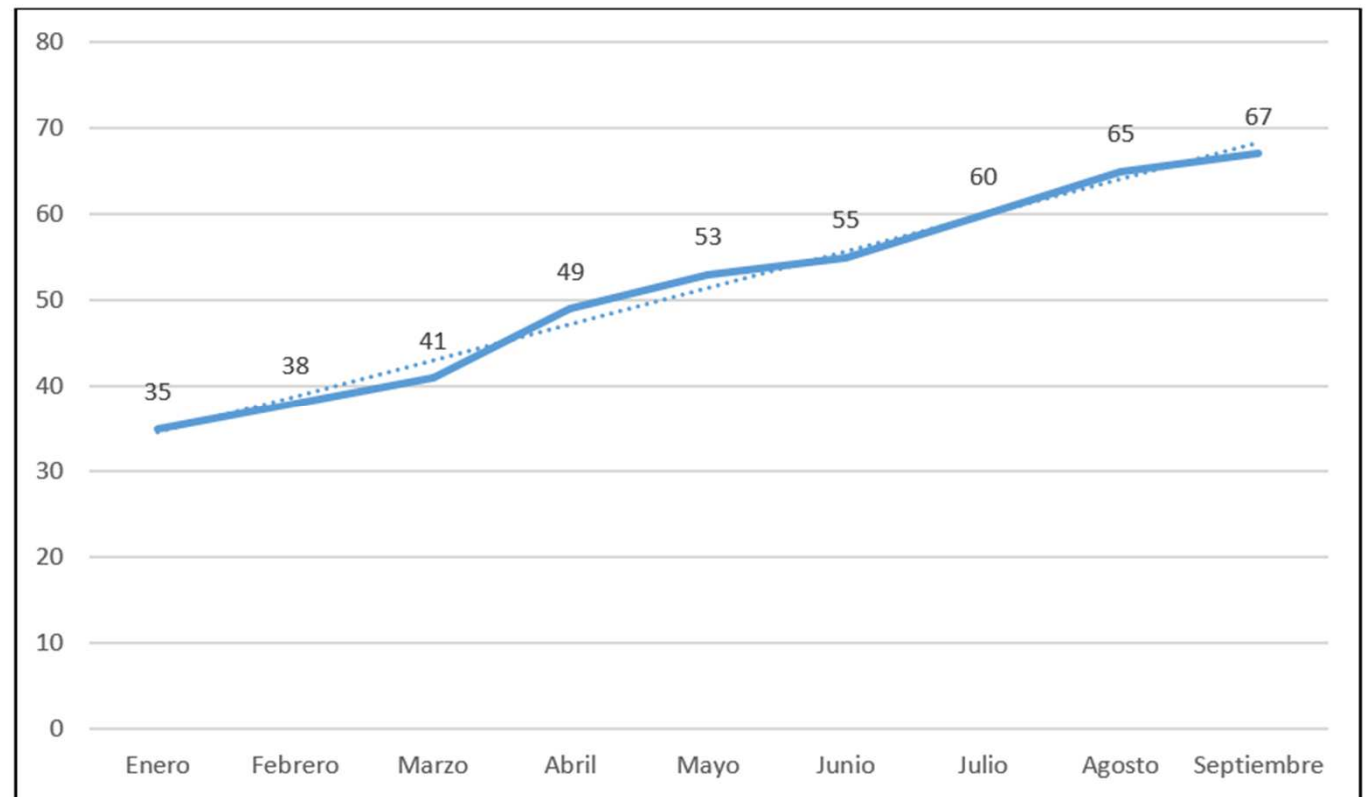
Name	Log Source Type	Log Source Identifier
571	CiscoFirepowerThreatDefense @ 172.17.1.250	Cisco Firepower Threat Defense
526	ASA @ 192.168.31.130	Cisco Adaptive Security Appliance (ASA)
524	ASA @ 192.168.13.130	Cisco Adaptive Security Appliance (ASA)
265	ASA @ 192.168.20.130	Cisco Adaptive Security Appliance (ASA)
260	ASA @ 192.168.38.130	Cisco Adaptive Security Appliance (ASA)
241	ASA @ 192.168.29.130	Cisco Adaptive Security Appliance (ASA)

CASOS DE USO

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

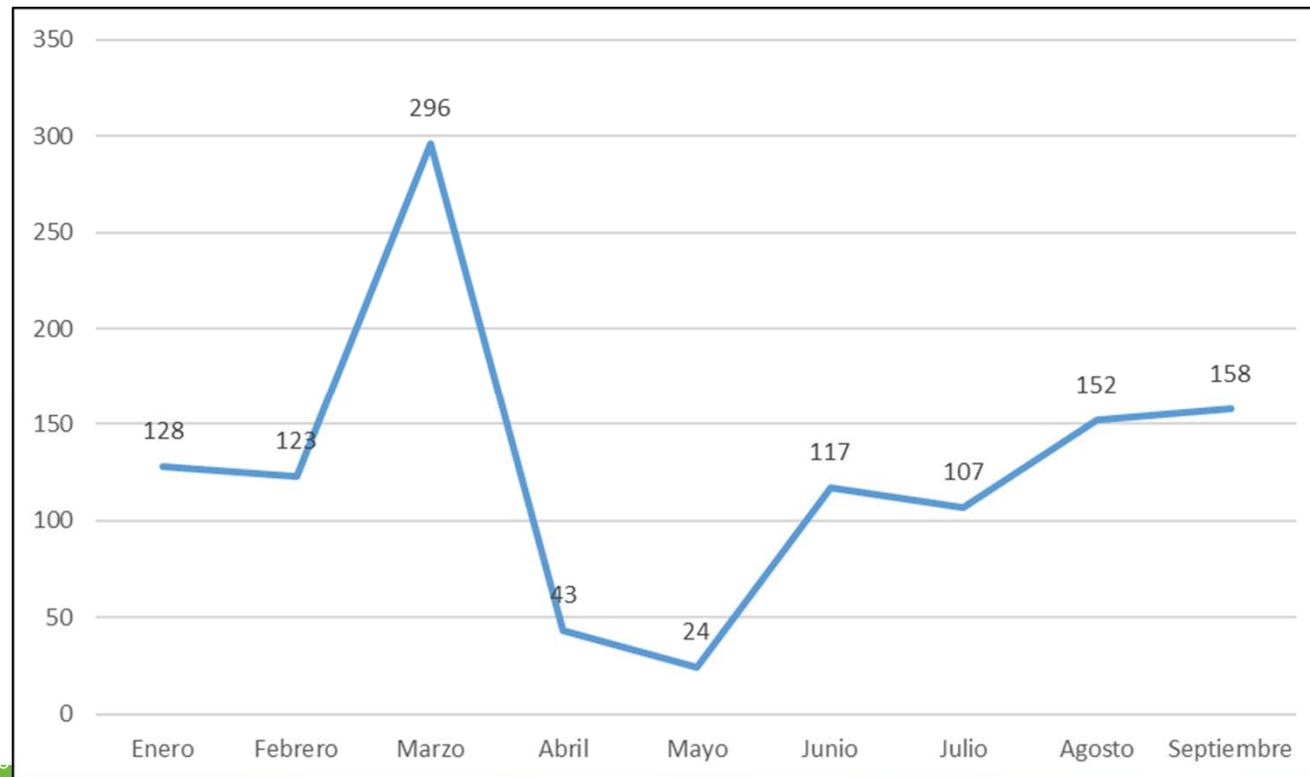
Para este periodo se realizó un incremento de 5 casos de uso

- FNA_Formulario 60 Cesantías
- FNA_SIGMA_Creation of executables for persistence.



ALERTAMIENTO SOC

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



Tareas de Gestión Plataforma SIEM

26 de agosto:

- **10:00 AM - 11:00 AM:** Revisión de alerta CiscoFirepowerThreatDefense @ 172.31.1.101 | IPS TippingPoint con el ingeniero Cristian. Revisamos las detecciones recientes y se analizan posibles falsos positivos, además de documentar los resultados para una posterior evaluación del equipo SOC.
- **2:00 PM - 4:00 PM:** Creación de caso de uso FNA_SIGMA_Creation of executables for persistence. Este caso se enfocará en identificar comportamientos de persistencia en sistemas, particularmente en la creación de ejecutables maliciosos que puedan evadir medidas de seguridad comunes.

28 de agosto:

- **9:00 AM - 11:00 AM:** Sesión de validación [SOC-CERT] ALERTA DE SEGURIDAD | ASA @ 192.168.28.130 | BOGPFFWCP001_172.31.1.96_FW_BORDE-1 | BOGPFVPCP002_172.31.1.102_FW_VPN. Revisión de alertas generadas por los firewalls de borde y VPN, incluyendo posibles ataques externos y validación de eventos críticos.

30 de agosto:

- **11:00 AM - 12:30 PM:** Sesión de validación de Integración E-Finac - QRadar. Revisión de la integración entre el sistema de E-Finac y QRadar, validando los requerimientos técnicos para su implementación

4 y 5 de septiembre:

- **Todo el día:** Parseo de campo correspondiente a los logs de formulario 60 cesantías. Revisión de los campos capturados por los logs, asegurando que los datos estén siendo procesados adecuadamente para análisis de y generación de casos de uso.

5 de septiembre:

- **3:00 PM - 5:00 PM:** Sesión de validación de casos de uso de Directorio Activo. Verificación de los casos de uso asociados con la seguridad del Directorio Activo, como la detección de accesos no autorizados, cambios de configuración críticos y actividades sospechosas de usuarios privilegiados.

6 de septiembre:

- **10:00 AM - 12:00 PM:** Sesión de validación de Integración aplicación Vigía. validando los requerimientos técnicos para su implementación, enfocándonos en la correlación de eventos y generación de alertas.

9 de septiembre:

- **11:00 AM - 12:30 PM:** Sesión de validación de Integración aplicación Vigía. Continuación de la sesión de validación previa, con foco en los eventos críticos y la creación de reportes para auditoría.

11 de septiembre:

- **2:00 PM - 4:00 PM:** Creación de caso de uso FNA_formulario 60 Cesantías en conjunto con el ingeniero Mauro Pico. Definición de reglas de correlación y alertas basadas en los campos del formulario 60 para prevenir fraudes o accesos indebidos a las cesantías.

18 de septiembre:

- **10:00 AM - 11:30 AM:** Validación de origen de bloqueo para el usuario cnx_iam. Investigación sobre bloqueos de acceso al usuario cnx_iam, incluyendo análisis de logs de autenticación, posibles errores de configuración o intentos de acceso no autorizados.

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.

Gestión de Reglas y Correlaciones:

1. Revisar y actualizar regularmente las reglas de detección de amenazas y las correlaciones para adaptarse a las nuevas amenazas y vulnerabilidades.
2. Ajustar la sensibilidad de las reglas y correlaciones para reducir falsos positivos y mejorar la eficacia de la detección de amenazas.

SOAR FUENTES INTEGRADAS

A continuación se presenta en la siguiente tabla se identifican las fuentes y estados de las Integraciones dispuestas para **SOAR**

APP DESPLEGADAS	
Cisco Firepower	En Pruebas
Trend Micro Vision One	OPERATIVA
FortiWeb	INTEGRADA

PLAYBOOKS NUEVO IMPLEMENTADO

FORTIWEB

Actualmente se tienen disponible para Fortiweb 20 playbook los cuales permiten la interacción y ejecución de tareas automatizadas.

PLAYBOOK	TIPO
fortiweb_app_name	Entrada de función
fortiweb_application_filter	Entrada de función
fortiweb_backend_ip	Entrada de función
fortiweb_backend_port	Entrada de función
fortiweb_backend_type	Entrada de función
fortiweb_block_mode	Entrada de función
fortiweb_cdn_status	Entrada de función
fortiweb_continent	Entrada de función
fortiweb_domain	Entrada de función

PLAYBOOKS NUEVO IMPLEMENTADO

FORTIWEB

Actualmente se tienen disponible para Fortiweb 20 playbook los cuales permiten la interacción y ejecución de tareas automatizadas.

PLAYBOOK	TIPO
vision_one_submit_sandbox_url	Entrada de función
vision_one_suspicious_days_to_expiration	Entrada de función
vision_one_suspicious_description	Entrada de función
vision_one_suspicious_domain	Entrada de función
vision_one_suspicious_file_sha_256	Entrada de función
vision_one_suspicious_file_sha1	Entrada de función
vision_one_suspicious_filter	Entrada de función
vision_one_suspicious_ip	Entrada de función
vision_one_suspicious_risklevel	Entrada de función

vision_one_suspicious_scanaction	Entrada de función
vision_one_suspicious_sender_address	Entrada de función
vision_one_suspicious_url	Entrada de función
vision_one_task_date_time_target	Entrada de función
vision_one_task_end_date_time	Entrada de función
vision_one_task_filter	Entrada de función
vision_one_task_id	Entrada de función
vision_one_task_limit	Entrada de función
vision_one_task_start_date_time	Entrada de función

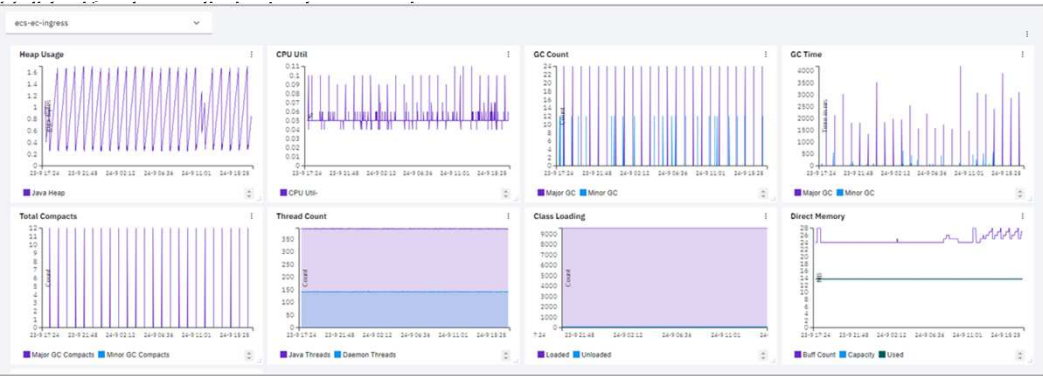
PLAYBOOK GENERADOS EN SOAR PARA TREND MICRO

RESPUESTAS

☐	ID	Name	Description	Date Discovered	Date Determined	Next Due Date	Date Created	Owner	↑	Phase	Severity	Status	Address
☐	2159	QRadar ID 71152 , FNA_X-Force Risky IP Malware_Conexiones Salientes - 185.191.126.213	2 events in 2 categories: FNA_X-Force Risky IP ...	03/09/2024 01:12:06	03/09/2024 01:12:06	-	18/09/2024 16:04:49	Default Group		Engage	-	Activo	['185.191.126.213']
☐	2158	QRadar ID 70775 , FNA_X-Force Risky IP Malware_Conexiones Salientes - 185.191.126.213	2 events in 2 categories: FNA_X-Force Risky IP ...	01/09/2024 10:48:37	01/09/2024 10:48:37	-	18/09/2024 15:28:14	Default Group		Engage	-	Activo	['185.191.126.213']
☐	2157	QRadar ID 74013 , FNA_X-Force Risky IP Malware_Conexiones Salientes - 185.191.126.213	6 events in 2 categories: FNA_X-Force Risky IP ...	18/09/2024 12:24:52	18/09/2024 12:24:52	-	18/09/2024 15:11:33	Default Group		Engage	High	Activo	-
☐	2156	QRadar ID 70745 , FNA_X-Force Risky IP Malware_Conexiones Salientes - 185.191.126.213	4 events in 2 categories: FNA_X-Force Risky IP ...	01/09/2024 00:50:16	01/09/2024 00:50:16	-	18/09/2024 15:10:29	Default Group		Engage	-	Activo	['185.191.126.213']
☐	2155	QRadar ID 68309 , FNA_X-Force Risky IP Dynamic - 192.168.28.75	14 events in 2 categories: FNA_X-Force Risky IP ...	26/08/2024 10:16:07	26/08/2024 10:16:07	-	26/08/2024 10:20:17	Default Group		Engage	-	Activo	['192.168.28.75']

Tareas de Gestión Plataforma SIEM

Consumo de rendimiento:



Seguimiento y estados de los diferentes servicios

Process Monitor - Last 7 days			
Enter value to filter			
Component	Total Outage(min)	Current Status	Last Outage Starttime
ecs-ep	1.00	Available	24 Sep 2024 5:49 PM
accumulator	3.00	Available	24 Sep 2024 12:51 PM
tomcat	2.00	Available	24 Sep 2024 9:29 AM
ecs-ec	2.00	Available	23 Sep 2024 8:02 AM
assetprofiler	2.01	Available	19 Sep 2024 4:59 PM
ariel_proxy_server	2.01	Available	19 Sep 2024 4:59 PM

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:~# last
root@fnabogapp100:~# last | grep root
```

root	pts/0	172.19.4.66	Tue Sep 24 09:14	still	logged in
root	pts/0	172.19.4.66	Wed Sep 18 08:51	- 09:20	(00:28)
root	pts/0	10.87.61.56	Fri Sep 13 07:14	- 07:14	(00:00)
root	pts/0	172.19.4.66	Wed Sep 11 15:24	- 15:43	(00:18)
root	pts/0	172.19.4.66	Tue Sep 10 09:22	- 18:54	(09:31)
root	pts/0	10.87.61.56	Tue Sep 10 05:45	- 05:46	(00:00)
root	pts/0	172.19.4.66	Mon Sep 9 11:48	- 15:15	(03:26)
root	pts/1	172.19.4.66	Fri Sep 6 10:50	- 10:17	(2+23:27)
root	pts/0	172.19.4.66	Wed Sep 4 10:59	- 10:17	(4+23:18)
root	pts/0	172.19.4.66	Wed Sep 4 10:56	- 10:58	(00:01)
root	pts/0	172.19.4.66	Mon Sep 2 16:05	- 18:42	(1+02:36)
root	pts/0	172.19.4.66	Fri Aug 30 10:41	- 10:42	(00:01)
root	pts/0	172.19.4.66	Mon Aug 26 18:10	- 13:09	(18:58)
root	pts/0	172.19.4.66	Wed Aug 14 18:16	- 01:36	(1+07:19)
root	pts/0	172.19.4.66	Wed Aug 14 11:12	- 14:09	(02:56)
root	pts/0	10.87.61.56	Fri Aug 9 07:20	- 07:20	(00:00)
root	pts/0	172.19.4.66	Fri Jul 26 19:13	- 11:19	(2+16:05)
root	pts/0	172.19.4.66	Fri Jul 26 19:12	- 19:13	(00:01)
root	pts/0	172.19.4.66	Fri Jul 26 09:42	- 09:53	(00:11)
root	pts/0	172.19.4.66	Wed Jul 24 10:18	- 11:35	(01:17)
root	pts/0	172.19.4.66	Tue Jul 23 17:25	- 17:26	(00:00)
root	pts/0	172.19.4.66	Fri Jul 12 16:06	- 08:56	(16:49)
root	pts/0	172.19.4.66	Fri Jul 12 11:05	- 14:14	(03:09)
root	pts/0	172.19.4.66	Fri Jul 5 15:06	- 00:32	(2+09:25)
root	pts/0	172.19.4.66	Fri Jun 28 14:01	- 18:03	(04:02)
root	pts/1	10.87.61.56	Mon Jun 24 02:48	- 03:04	(00:16)
root	pts/0	172.19.4.66	Fri Jun 21 10:25	- 10:35	(4+00:10)
root	pts/1	10.87.61.56	Wed Jun 19 02:43	- 03:31	(00:48)
root	pts/2	10.87.61.56	Tue Jun 18 22:27	- 22:43	(00:16)
root	pts/1	10.87.61.56	Tue Jun 18 22:09	- 22:54	(00:44)
root	pts/0	172.19.4.66	Tue Jun 18 09:35	- 11:11	(1+01:36)
root	pts/0	172.19.4.66	Mon Jun 17 17:56	- 09:34	(15:38)
root	pts/0	172.19.4.66	Mon Jun 17 09:14	- 10:24	(01:09)
root	pts/1	10.87.61.56	Fri Jun 14 18:00	- 18:21	(00:20)
root	pts/0	172.19.4.66	Fri Jun 14 17:41	- 00:58	(1+07:17)
root	pts/0	172.19.4.66	Fri Jun 14 12:10	- 17:38	(05:27)
root	pts/1	10.87.61.56	Fri Jun 14 11:22	- 11:25	(00:03)
root	pts/1	10.87.61.56	Fri Jun 14 10:04	- 10:10	(00:06)
root	pts/1	10.87.61.56	Fri Jun 14 09:54	- 09:57	(00:03)
root	pts/1	10.87.61.56	Fri Jun 14 09:38	- 09:46	(00:07)



48

Alertas Preventivas

11

Alertas Tempranas

22.734

IoC reportados

1.677

Amenazas identificadas

12

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 64 investigaciones, cada una de ellas se convirtió en una **alerta preventiva** que fue compartida vía correo electrónico y eventos en MISP.

Número de alertas

48

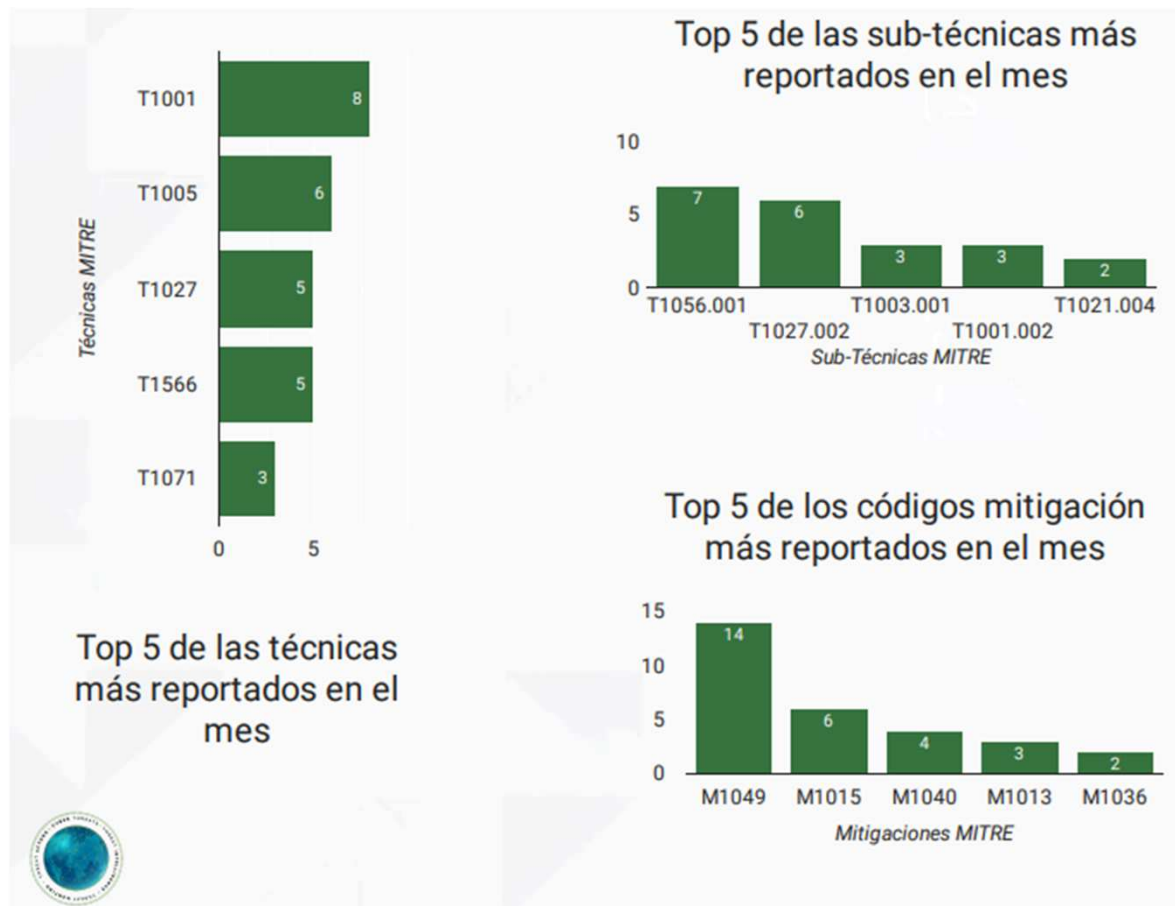
Alertas y eventos
MISP reportados

**ALERTAS
REPORTADAS**

11

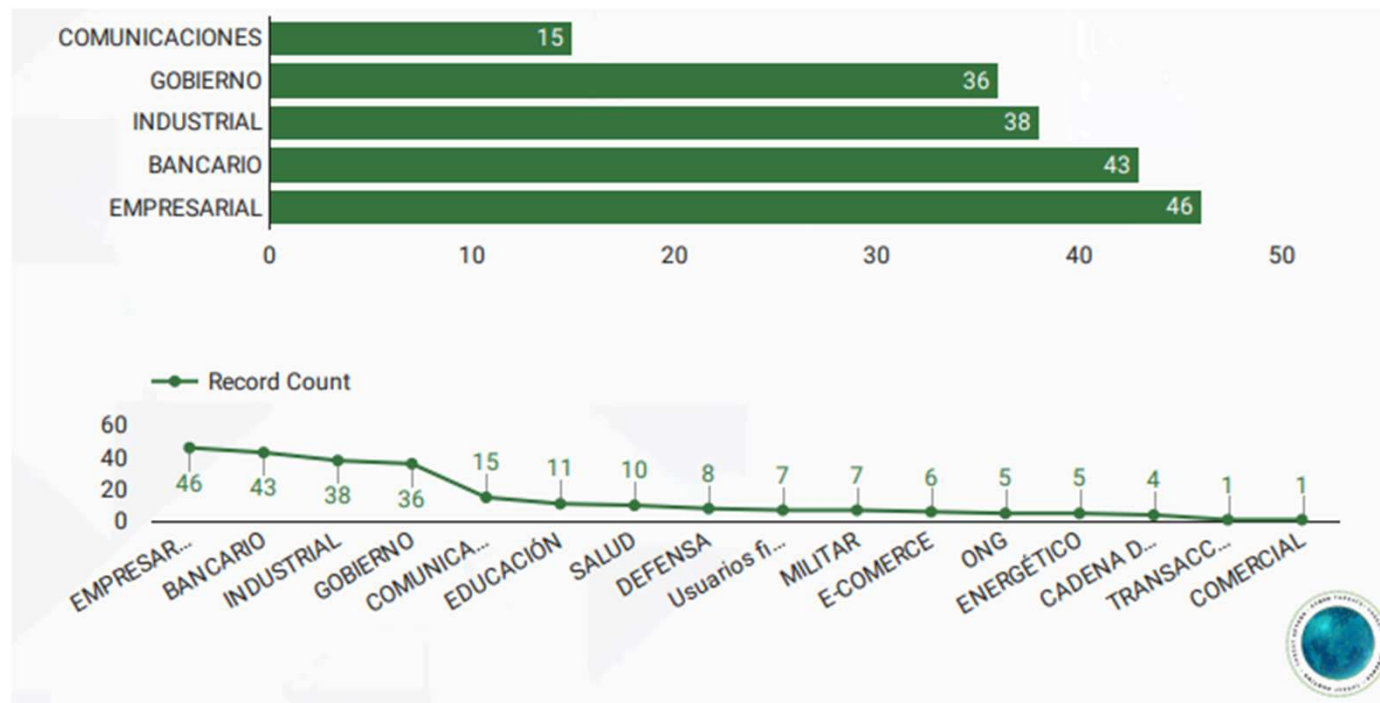
En el periodo evaluado se generaron 16 **alertas tempranas**, cada una de ellas fue compartida vía correo electrónico.

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.

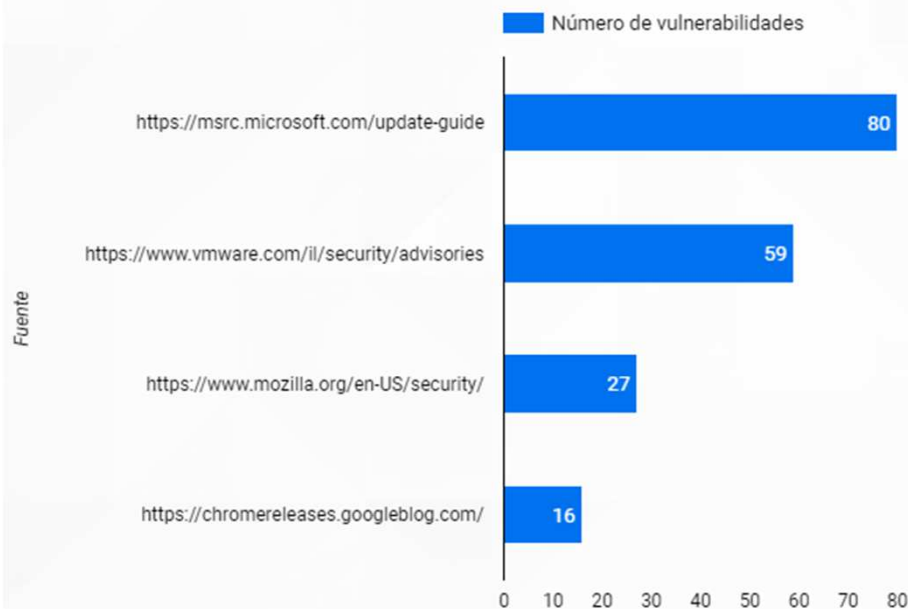
Industria objetivo de cibercriminales



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

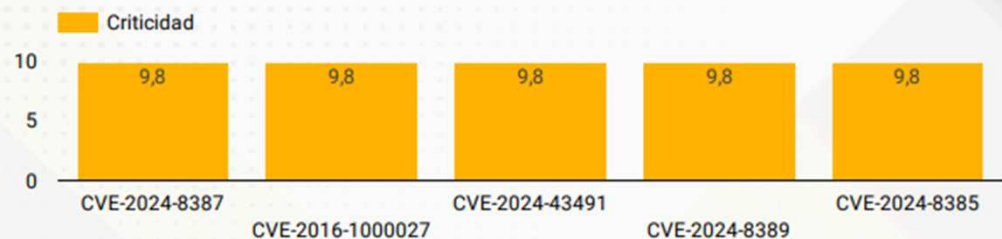
Vulnerabilidades reportadas

Número de CVE reportadas por fuente



Se reportaron 182 vulnerabilidades de 87 productos pertenecientes a 4 fabricantes distintos

Top 5 de los CVE con la mayor criticidad reportada en el transcurso del mes



Se reportaron 22 vulnerabilidades de importancia crítica al tener un puntaje de clasificación superior a 9.0 en CVSS Score. Estas vulnerabilidades pueden ser explotadas con mayor facilidad y significan un riesgo más alto en cuanto al impacto que se tiene sobre la compañía.

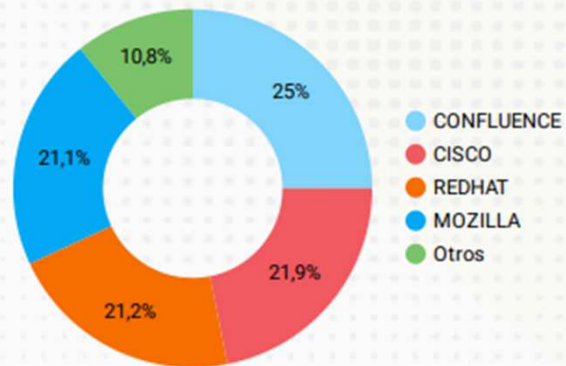
Actividades realizadas

- Se generaron 48 alertas y eventos en MISP.
- De las 48 alertas se han extraído un total de 22.734 indicadores de compromiso.
- Los indicadores de compromiso se han compartido con la herramienta de inteligencia de amenazas TIP para la integración con otras herramientas de seguridad.
- Las amenazas encontradas fueron perpetradas por 12 actores de amenazas identificados.
- Fueron generadas 11 alertas que contienen información sobre vulnerabilidades que pueden afectar la infraestructura de la compañía.
- Las alertas tempranas se han compartido junto a la solución o mitigación brindada por el fabricante responsable de publicar las actualizaciones de los productos afectados.



Recomendaciones y conclusiones

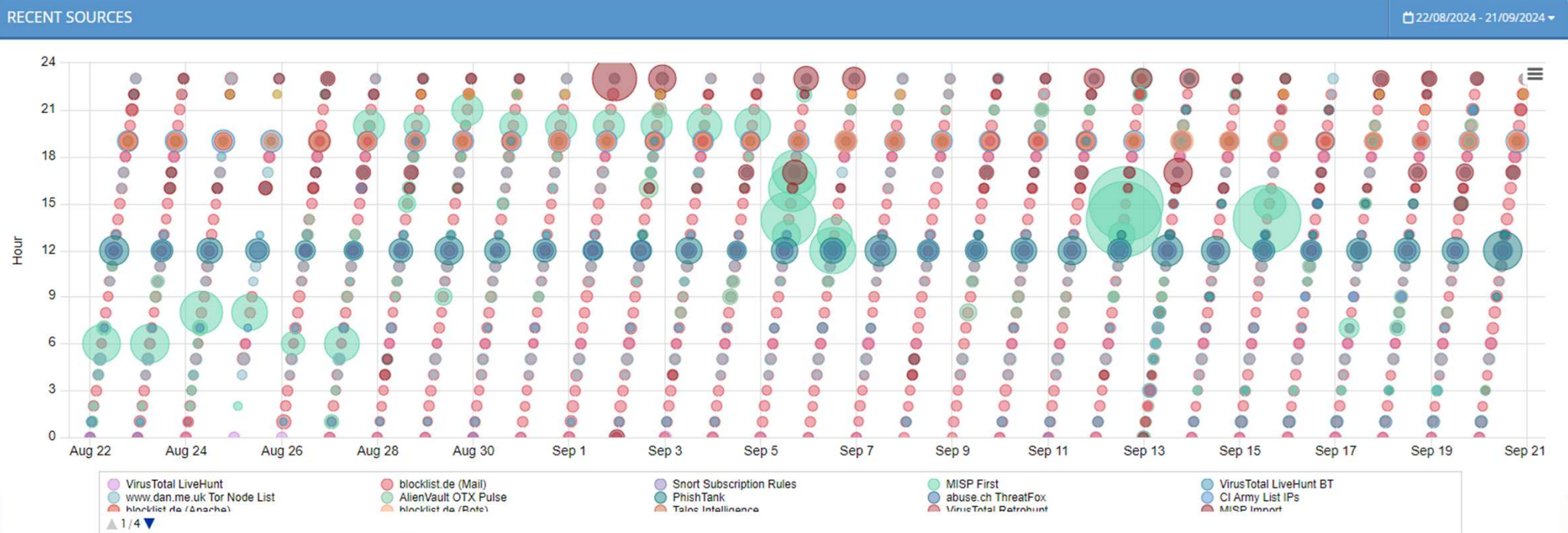
Nivel de criticidad promedio por fabricante, tomando el cvss reportado por cada uno



- 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, además del seguimiento de amenazas compartidas en eventos anteriores.
- Es recomendado ajustar todas las herramientas de seguridad para permitir la ingesta de indicadores de compromiso de manera automatizada con los indicadores compartidos por el equipo de CTI Mnemo durante las investigaciones realizadas a las distintas amenazas que afectan tanto al sector como a la región.
- Se recomienda mantener una política de actualización y parcheo constante del software utilizado por la compañía.

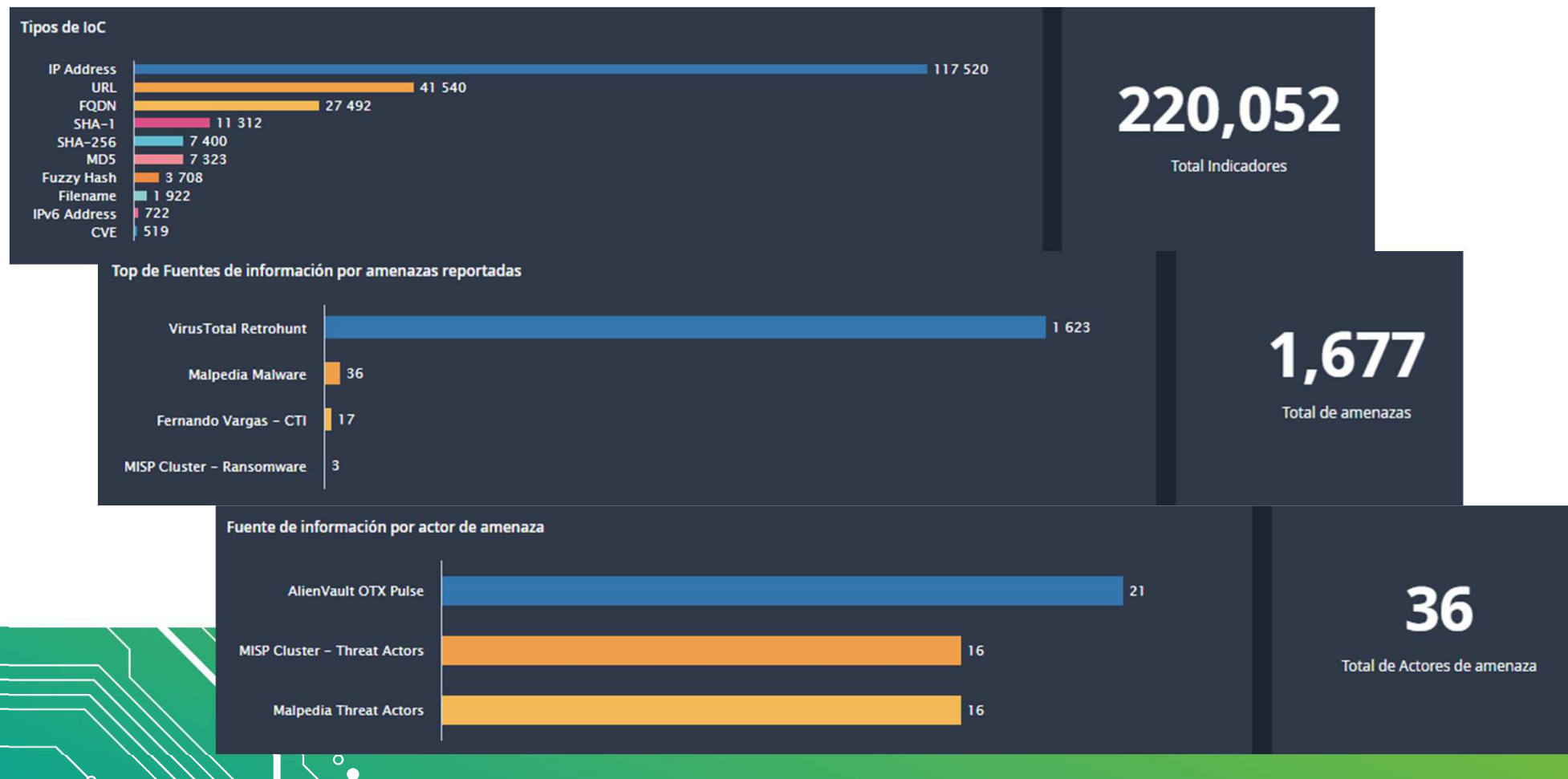
Resumen de objetos obtenidos – TIP

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.



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 continúa el seguimiento con respecto a la integración entre TIP y XDR Vision One con el fin de entregar indicadores de compromiso que mejoren la detección temprana de amenazas en sus fases iniciales y de conexión a servidores de Comando y Control C2.
- Se ajusta la priorización y enriquecimiento de los indicadores de compromiso que son ingestados por la plataforma de inteligencia de amenazas.
- Se crean investigaciones realizadas a determinadas amenazas, asociando indicadores de compromiso, actores de amenazas y campañas utilizadas.



Recomendaciones y conclusiones

- Como resultado de la integración entre la herramienta TIP y el XDR del Fondo Nacional del Ahorro se evidenciaron indicadores de compromiso cargados en la lista de bloqueo de la herramienta, lo que permite una detección y contención más temprana sobre los ataques realizados por los actores de amenazas.
- Durante el período observado, se ha notado un aumento considerable en la cantidad de URL maliciosas provenientes de la ingestión de indicadores de compromiso de diversas fuentes de información. Basándonos en esta información, se recomienda implementar reglas de bloqueo estrictas sobre herramientas de seguridad perimetrales como proxies de navegación o Firewalls, permitiendo únicamente los servicios vitales para el funcionamiento normal de las actividades de los colaboradores.



02

Reglas a nivel de
comportamiento

01

Análisis de amenazas en
profundidad y focalizado

Informe Threat Hunting

2024

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



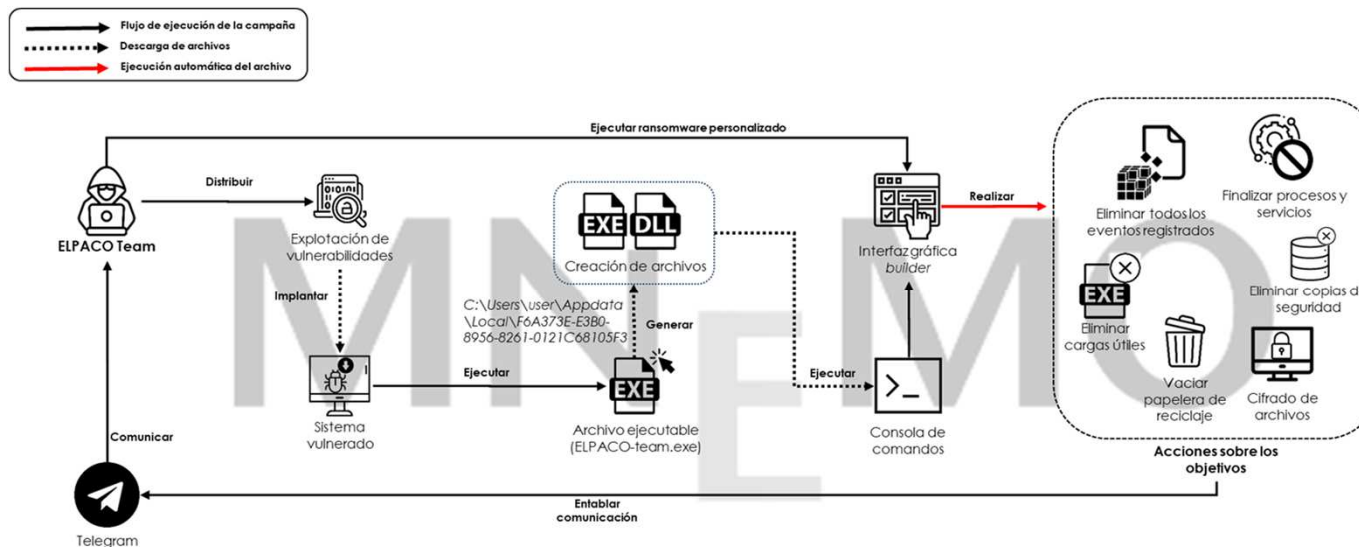
Powershell for Downloading and Hidden Execution of Commands

- Como resultado del análisis de AgentTesla donde se identificó un comando ofuscado para descargar y ejecutar artefactos maliciosos. La regla SIGMA detecta el momento en el que la amenaza ejecuta el comando ofuscado para descargar artefactos maliciosos adicionales.

Malicious overwriting of a file

- Identifica un comando para sobrescribir con ceros los primeros 20 MB de un archivo utilizando la herramienta fsutil. Luego, elimina de manera forzada, silenciosa y sin confirmación, todos los archivos con las extensiones .exe, .ini, .dll, .bat y .db. Este comportamiento fue visualizado durante la ejecución de la amenaza conocida como ELPACO Ransomware.

Análisis de amenazas focalizados



- Se realizó el análisis de la amenaza conocida como ELPACO Ransomware, distribuida por el actor de amenazas identificado como ELPACO TEAM.
- Se dan recomendaciones para detectar, mitigar y contener la amenaza evitando el compromiso de la seguridad de la información en la infraestructura corporativa
- Se demuestra el funcionamiento de la amenaza, así como vectores de distribución y reglas de detección con respecto a la amenaza.

Actividades realizadas

- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se crearon 2 reglas Sigma en la que se identifican comportamientos de ofuscación y ejecución.
- La primera regla SIGMA detecta la descarga de artefactos maliciosos a través de comandos ofuscados.
- Para la segunda regla sigma, se identificó un proceso que utiliza el ejecutable “fsutil” para sobre escribir el contenido de un archivo legítimo.
- Se realizó un análisis focalizado sobre la amenaza conocida como ELPACO Ransomware, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.

The image displays two screenshots of the UNIFIED THREAT IDENTIFICATION (TIP) interface, which is used for threat detection and prevention. Both screenshots show the 'General Information' tab for a specific threat.

Top Screenshot (AgentTesla):

- Nombre de la amenaza:** AgentTesla
- Criticidad:** Media (indicated by a yellow bell icon)
- Actor de Amenaza:** N/A
- ATT&CK :** T1559
- Fase Cyber Kill Chain:** Execution
- Taxonomía:** Malware y APT > Malware > Malware catalogado
- Acción maliciosa:** Como resultado del análisis de AgentTesla se identificó un comando ofuscado para descargar y ejecutar artefactos maliciosos.
- TLP:** RED

Bottom Screenshot (ELPACO Ransomware):

- Nombre de la amenaza:** ELPACO Ransomware
- Criticidad:** Alta (indicated by a red flame icon)
- Actor de Amenaza:** ELPACO Team
- ATT&CK :** T1070.004
- Fase Cyber Kill Chain:** Defense Evasion
- Taxonomía:** Malware y APT > Malware > Malware catalogado
- Acción maliciosa:** Como resultado del análisis realizado al ransomware ELPACO se ha identificado un comando para sobrescribir con ceros los primeros 20 MB de un archivo utilizando la herramienta fsutil. Luego, elimina de manera forzada, silenciosa y sin confirmación, todos los archivos con las extensiones .exe, .ini, .dll, .bat y .db.
- TLP:** RED

81

Muestras sospechosas
analizadas

61

Muestras confirmadas con
algún tipo de malware

Informe Laboratorio avanzado de malware 2024

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 81 muestras, de las cuales 61 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.

Muestras analizadas

81 | 2591

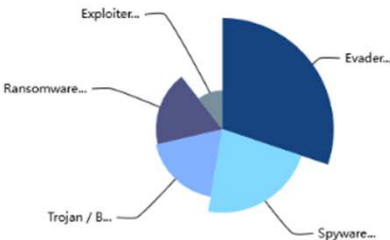


Malware

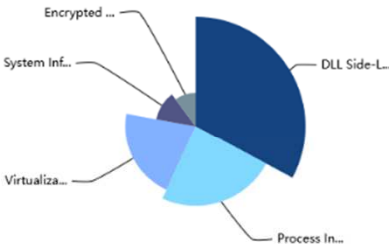
61 | 2298



Top 5 Categorías



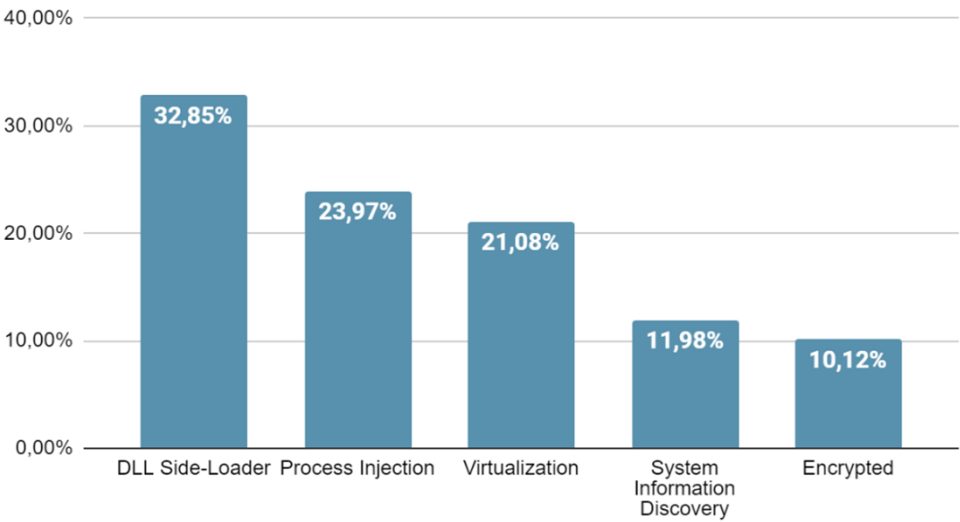
Top 5 MITRE Técnicas



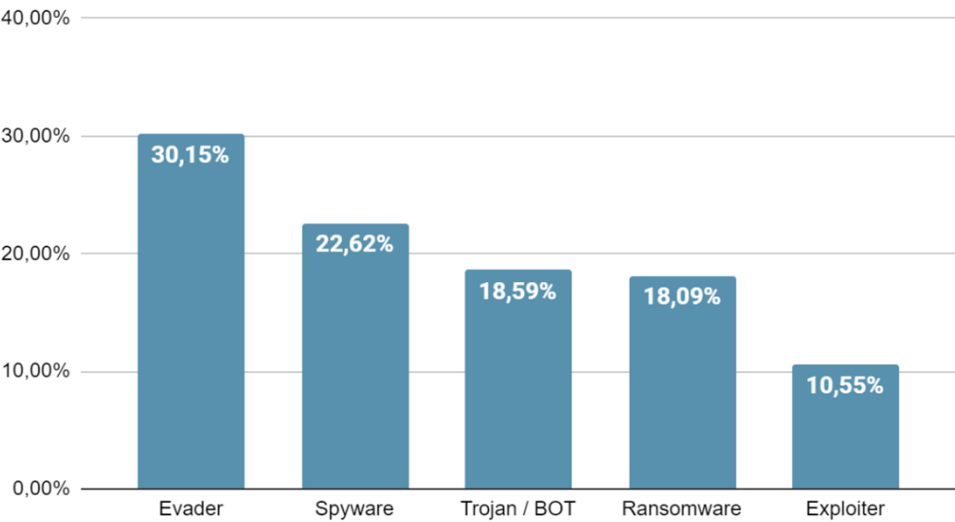
Técnicas más utilizadas y categorías de malware más detectadas

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.

Mitre Técnicas



Capacidades de Malware

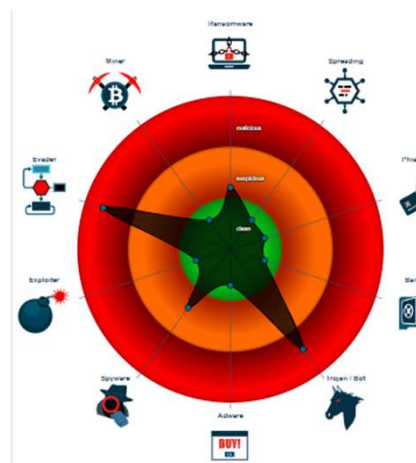


Tácticas y técnicas utilizadas

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
Valid Accounts	Execution through API	DLL Side-Loading	Process Injection	Process Injection	Input Capture	System Information Discovery	Taint Shared Content	Archive Collected Data		Encrypted Channel			System Shutdown/ Reboot	Scripting
Replication Through Removable Media	Command-Line Interface	Scripting	DLL Side-Loading	DLL Side-Loading	Credential Dumping	Virtualization/Sandbox Evasion		Input Capture		Standard Application Layer Protocol			Data Encrypted for Impact	
	Scheduled Task	Scheduled Task	Scheduled Task	Virtualization/Sandbox Evasion	Credentials In Files	Security Software Discovery		Data from Local System		Standard Non-Application Layer Protocol			Defacement	
	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Obfuscated Files or Information	Credentials in Registry	Process Discovery		Clipboard Data		Non-Standard Port			Inhibit System Recovery	
	Exploitation for Client Execution	Valid Accounts	Access Token Manipulation	Masquerading		Application Window Discovery		Email Collection		Remote File Copy				
	PowerShell	Windows Service	Windows Service	Disable or Modify Tools		File and Directory Discovery		Screen Capture		Web Service				
	Service Execution	Bootkit	Valid Accounts	Software Packing		System Time Discovery				Remote Access Tools				
	Execution through Module Load	Obfuscated Files or Information	Exploitation for Privilege Escalation	Deobfuscate/Decode Files or Information		System Owner/User Discovery				Connection Proxy				
		Services File Permissions Weakness	Bypass User Access Control	Access Token Manipulation		Account Discovery								
			Abuse Elevation Control Mechanism	Rundll32		System Network Configuration Discovery								
			Extra Window Memory Injection	Valid Accounts		System Service Discovery								
			Services File Permissions Weakness	Timestamp		Query Registry								
				Modify Registry		Peripheral Device Discovery								

Análisis de muestras propias FNA

- Desde el servicio de Laboratorio avanzado de Malware se recibió una muestra captada en el servicio de monitoreo de correos electrónicos, donde un actor de amenaza desconocido ha entregado un correo tipo phishing con un artefacto adjunto con extensión SVG.
- El análisis arrojó como resultado la amenaza AsyncRAT, sin embargo, en un análisis más específico, se detectó que, además, luego de un tiempo de ejecución, la amenaza descarga dos tipos de malware más, QuasarRAT y RemcosRAT.



Actividades realizadas

- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 81 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.
- Análisis de muestra aportada por el equipo de monitoreo de herramientas de FNA.
- 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.



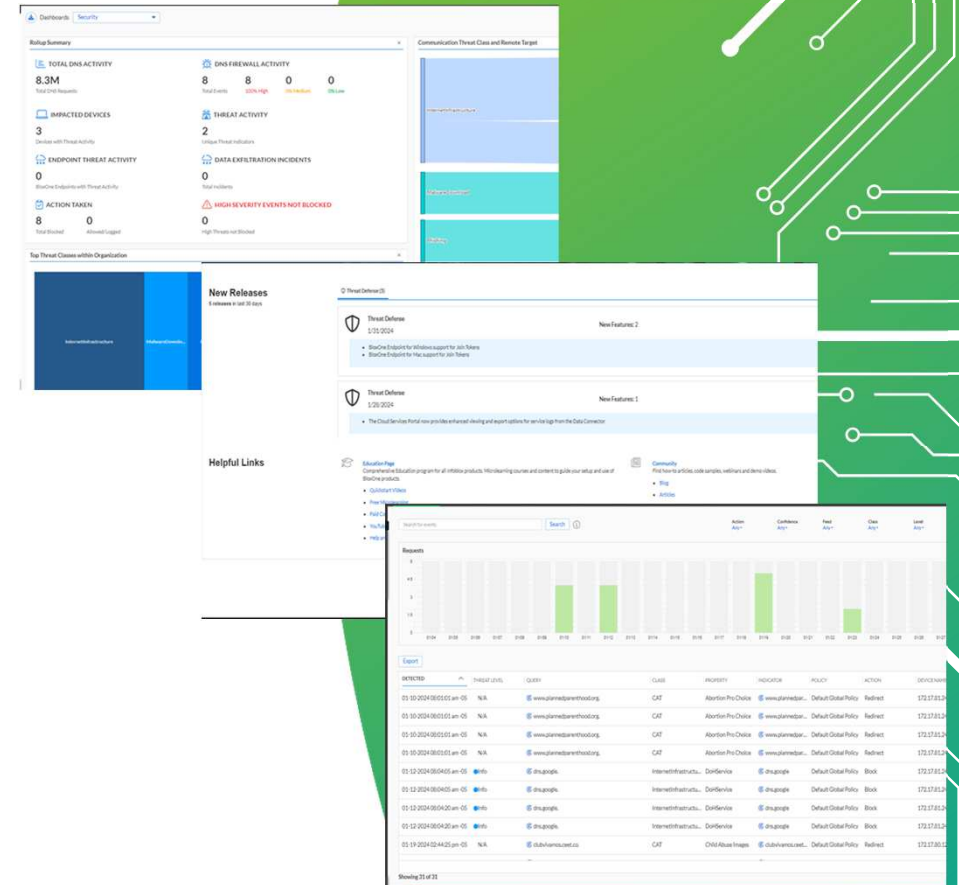


DEFINICIONES

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

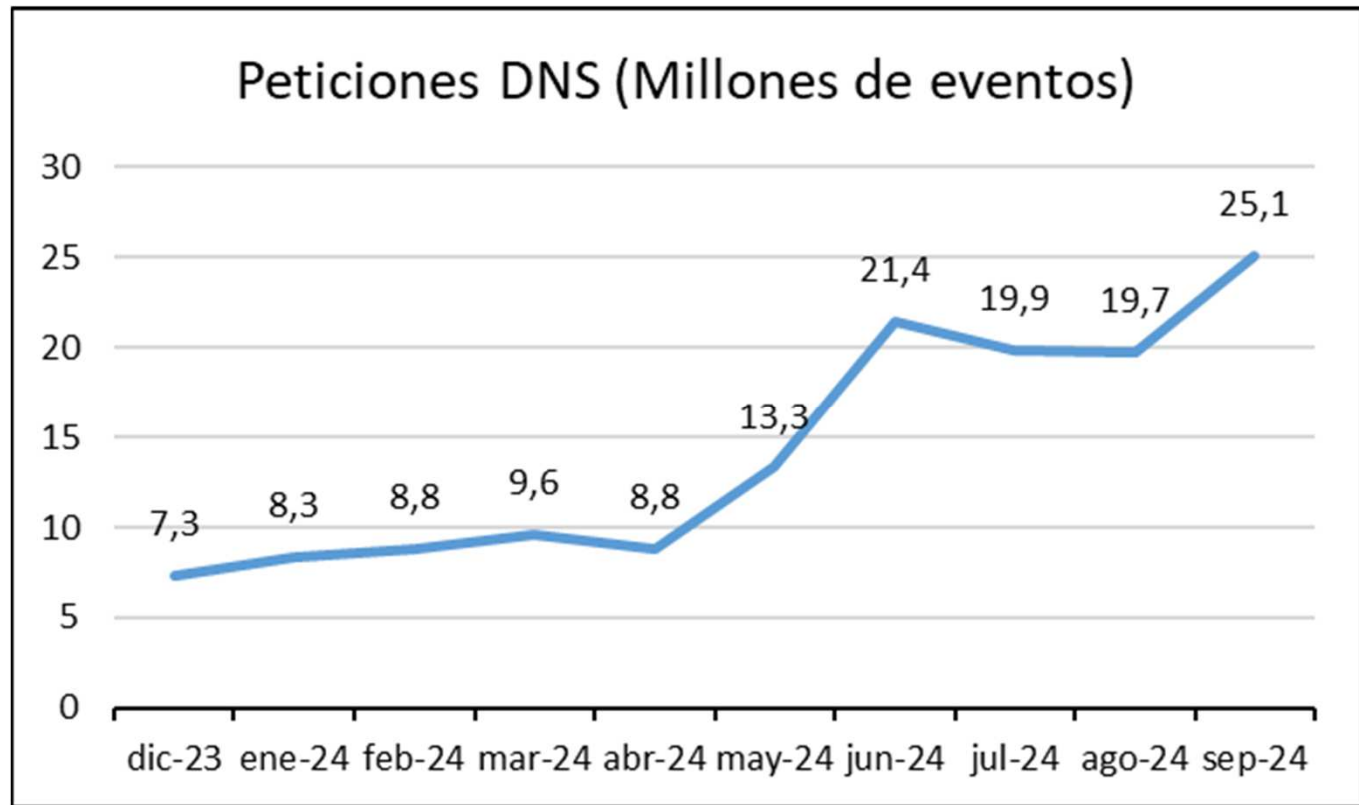
Política: cuenta con una serie de políticas que rigen cómo opera la empresa. Estas políticas se establecen para proteger a los empleados, clientes y socios de Infoblox, así como para garantizar que la empresa cumpla con todas las leyes y regulaciones aplicables.

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

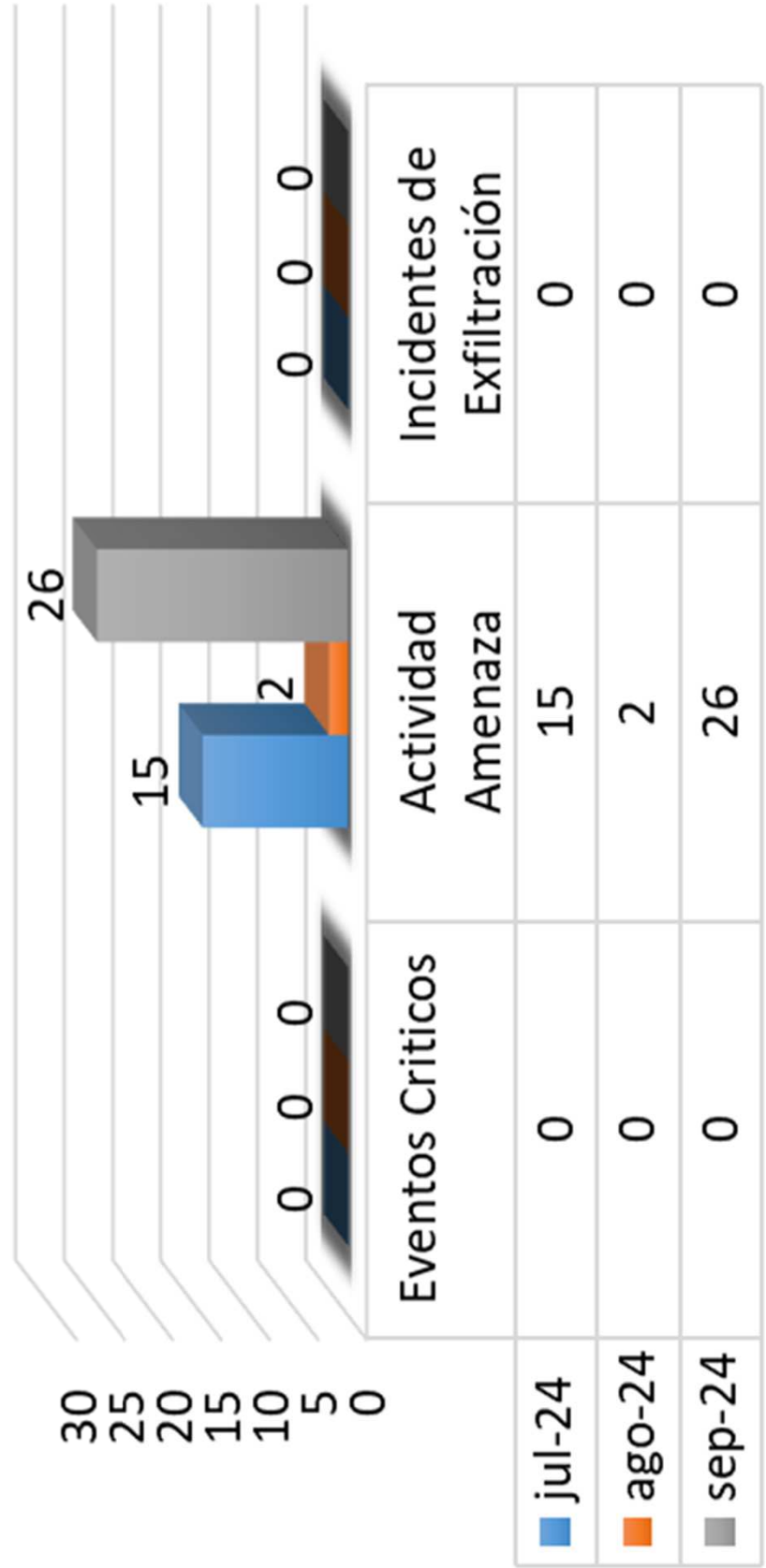


DNS SECURITY – INFOBLOX (Millones de eventos)

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.

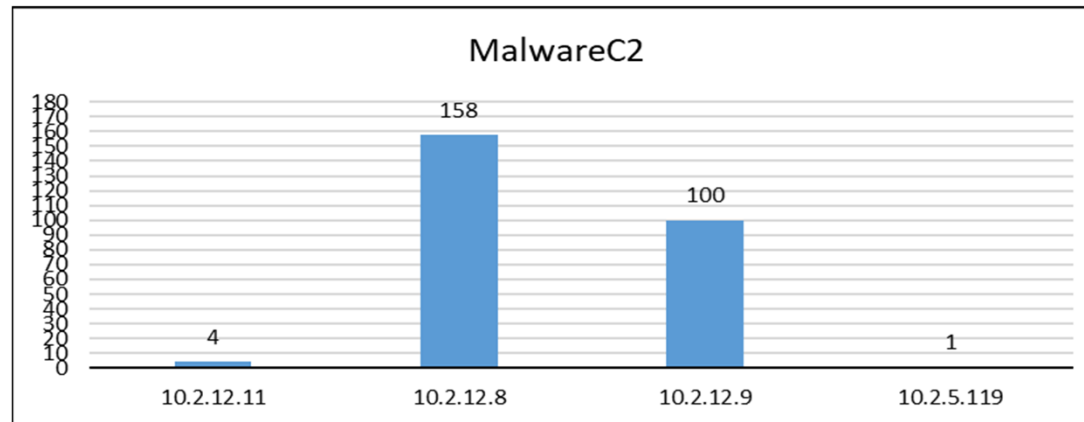
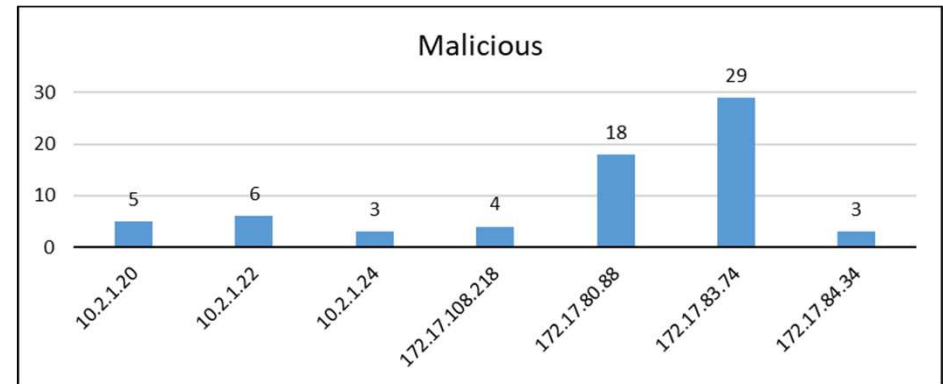
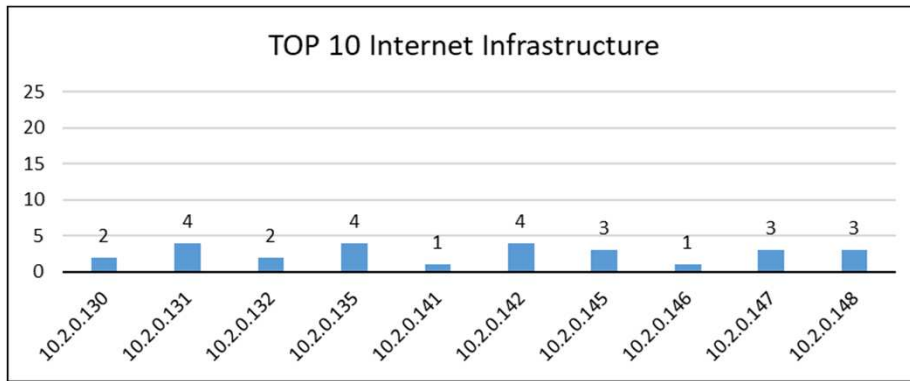


INDICADOR AMENAZAS



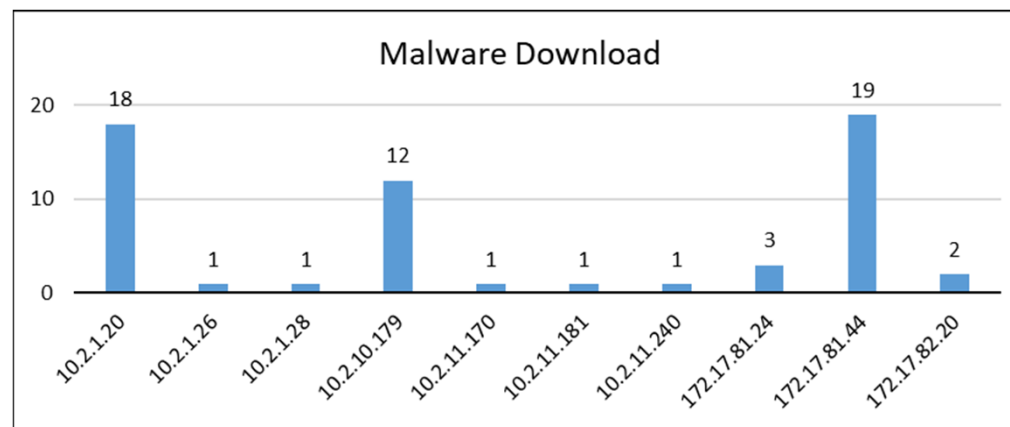
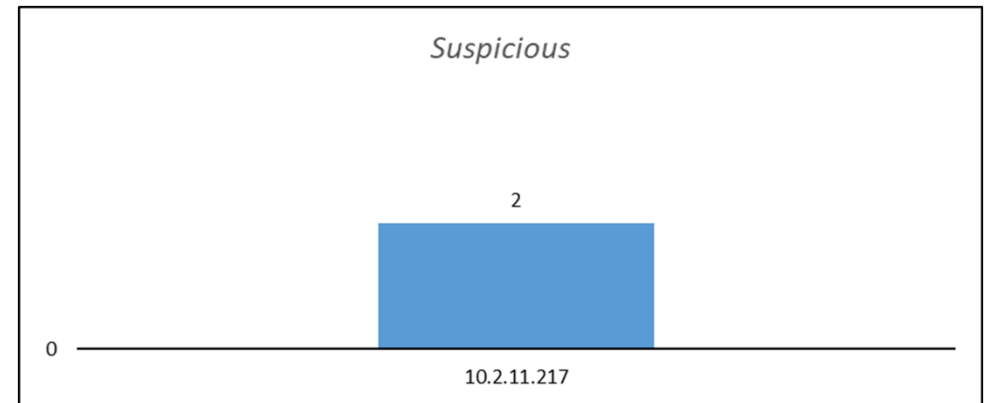
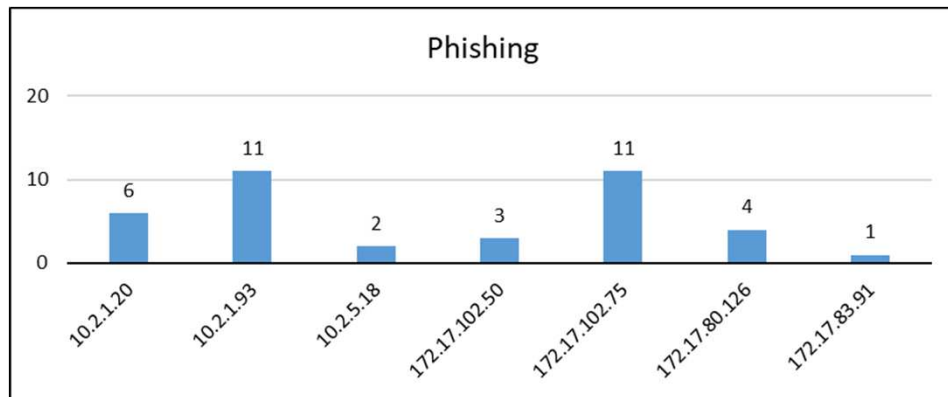
DNS SECURITY – INFOBLOX

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

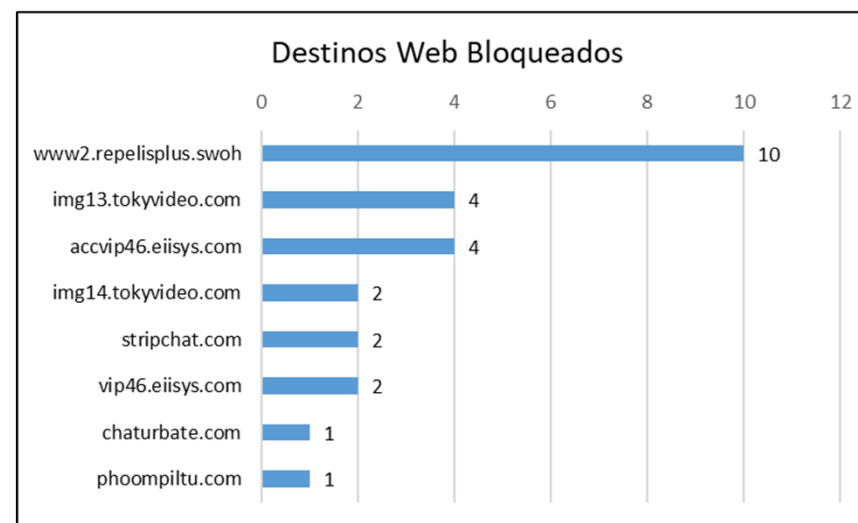
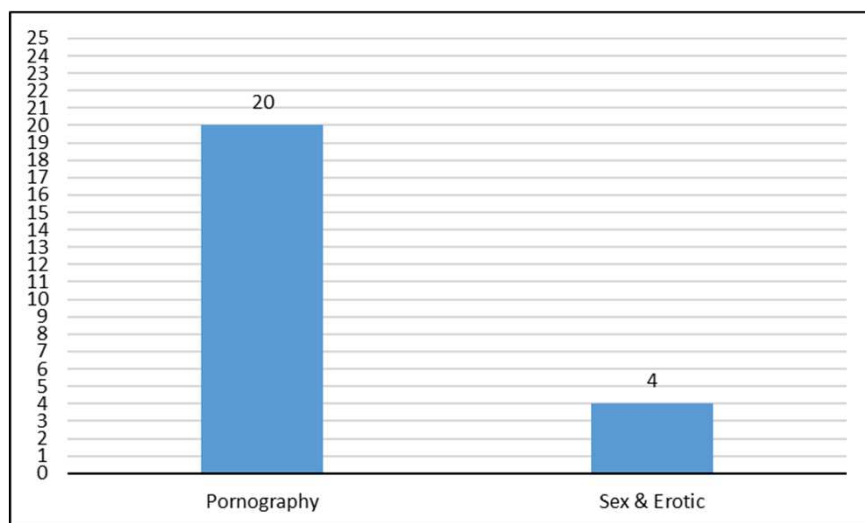


DNS SECURITY – INFOBLOX

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



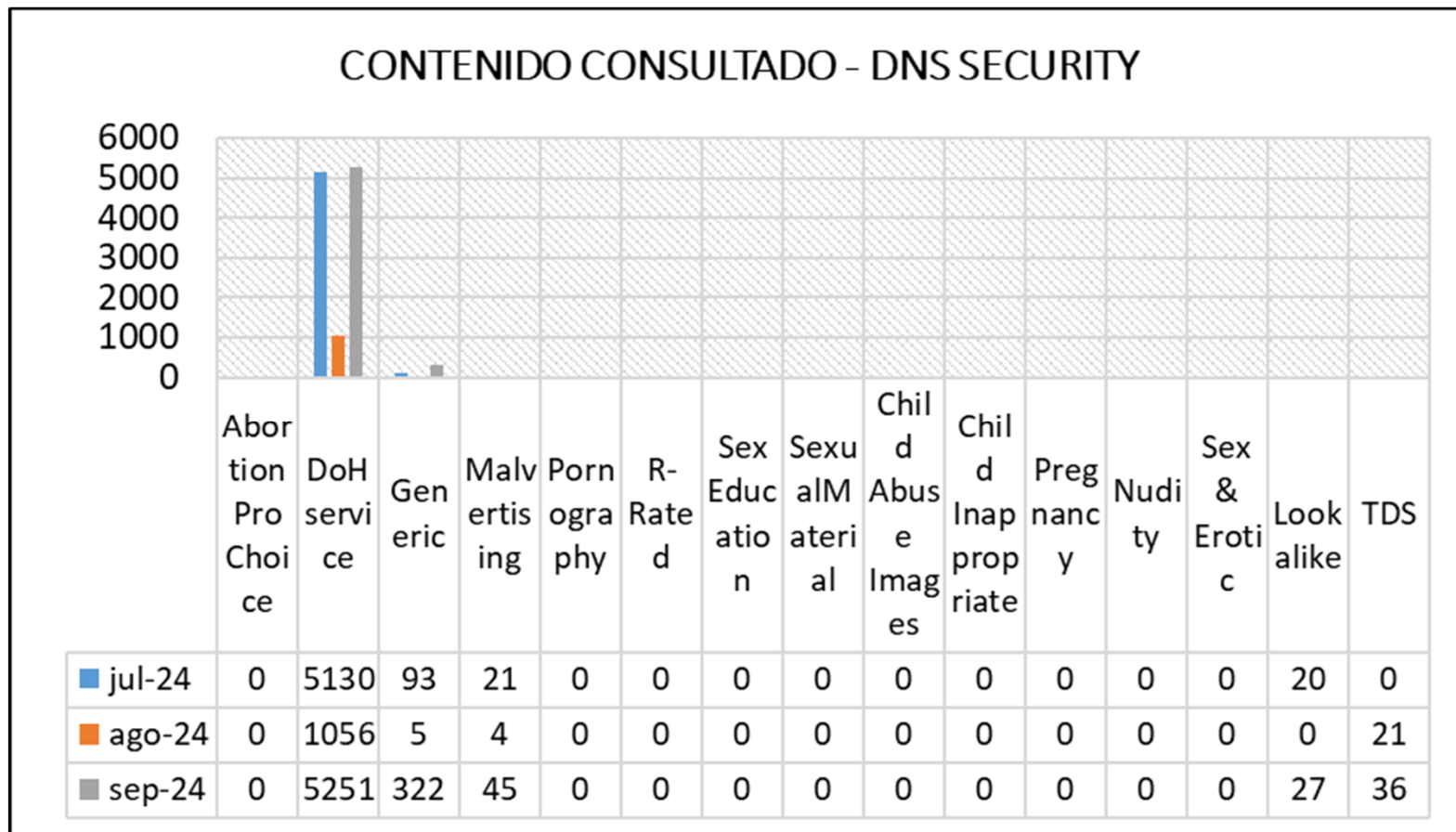
Top de los destinos malintencionados consultados a nivel interno del FNA, los cuales fueron bloqueados por la herramienta Infoblox.



Para el periodo en mención se evidencia un aumento 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 aumentó en la resolución de DNS.

GENERAL DNS - INFOBLOX

Para el periodo en
mención se
evidenció un
aumento en la
categoría de
DoHservice en las
consultas DNS.



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.



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 la 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

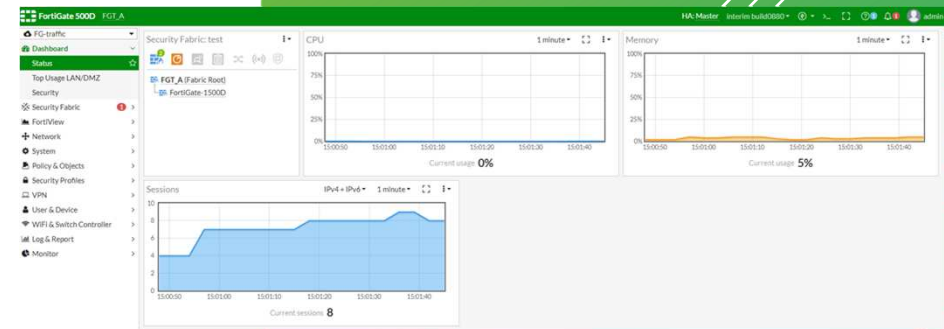
Protección multicapa contra los 10 principales ataques a aplicaciones de OWASP, incluido el aprendizaje automático para defenderse de ataques conocidos y desconocidos.

Protección API

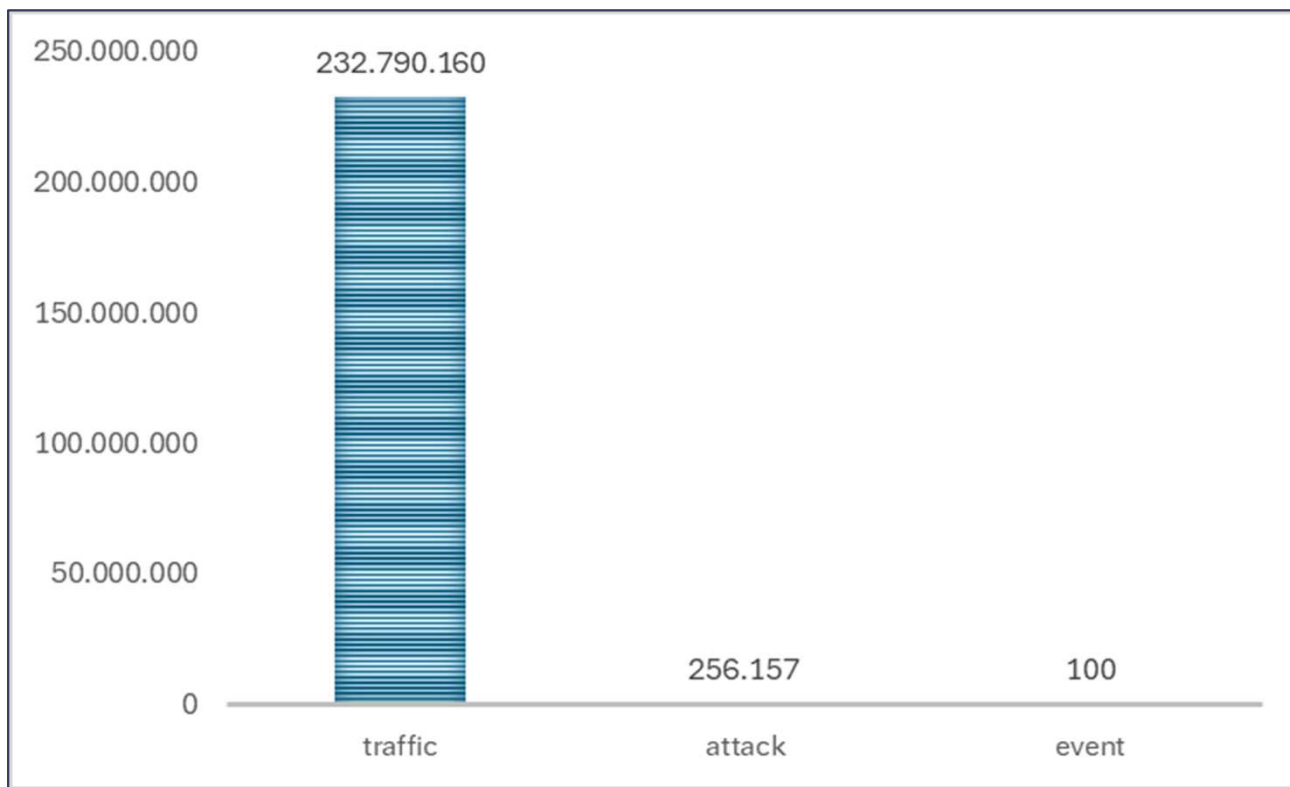
Protege los API de actores maliciosos aplicando automáticamente lo positivo y lo negativo. políticas de seguridad. Integra la seguridad API en su proceso de CI/CD.

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



+233 M

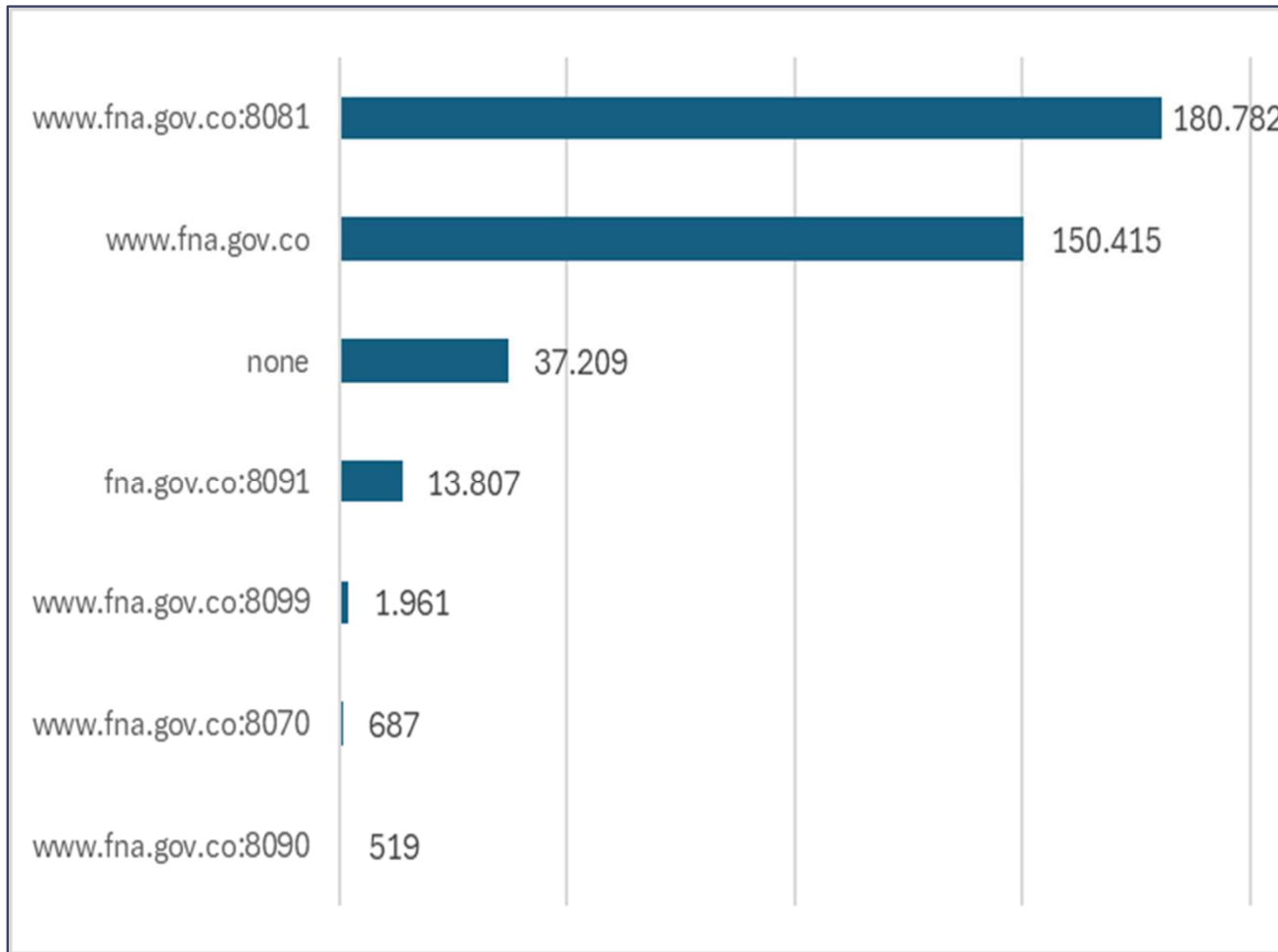
Eventos verificados por el WAF

-0,11%

Del tráfico total es
categorizado como
amenaza

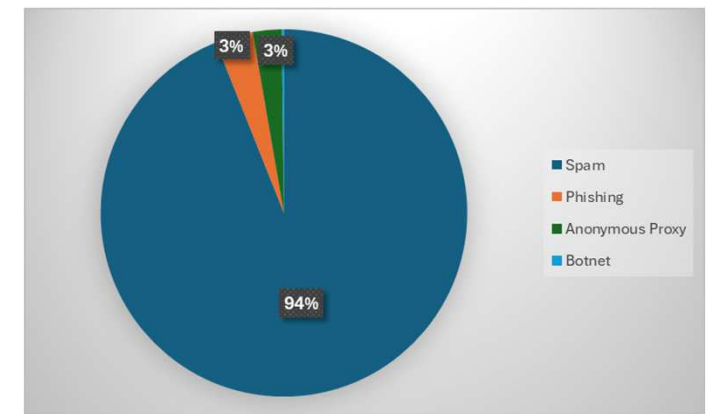
De lo anterior: En el periodo del 22 de agosto al 21 de septiembre se visualizó tráfico a través del WAF de aproximadamente 233 Millones de eventos de los cuales menos del 0,11% están dentro de la categoría Amenaza.

GENERAL WAF – IP REPUTATION



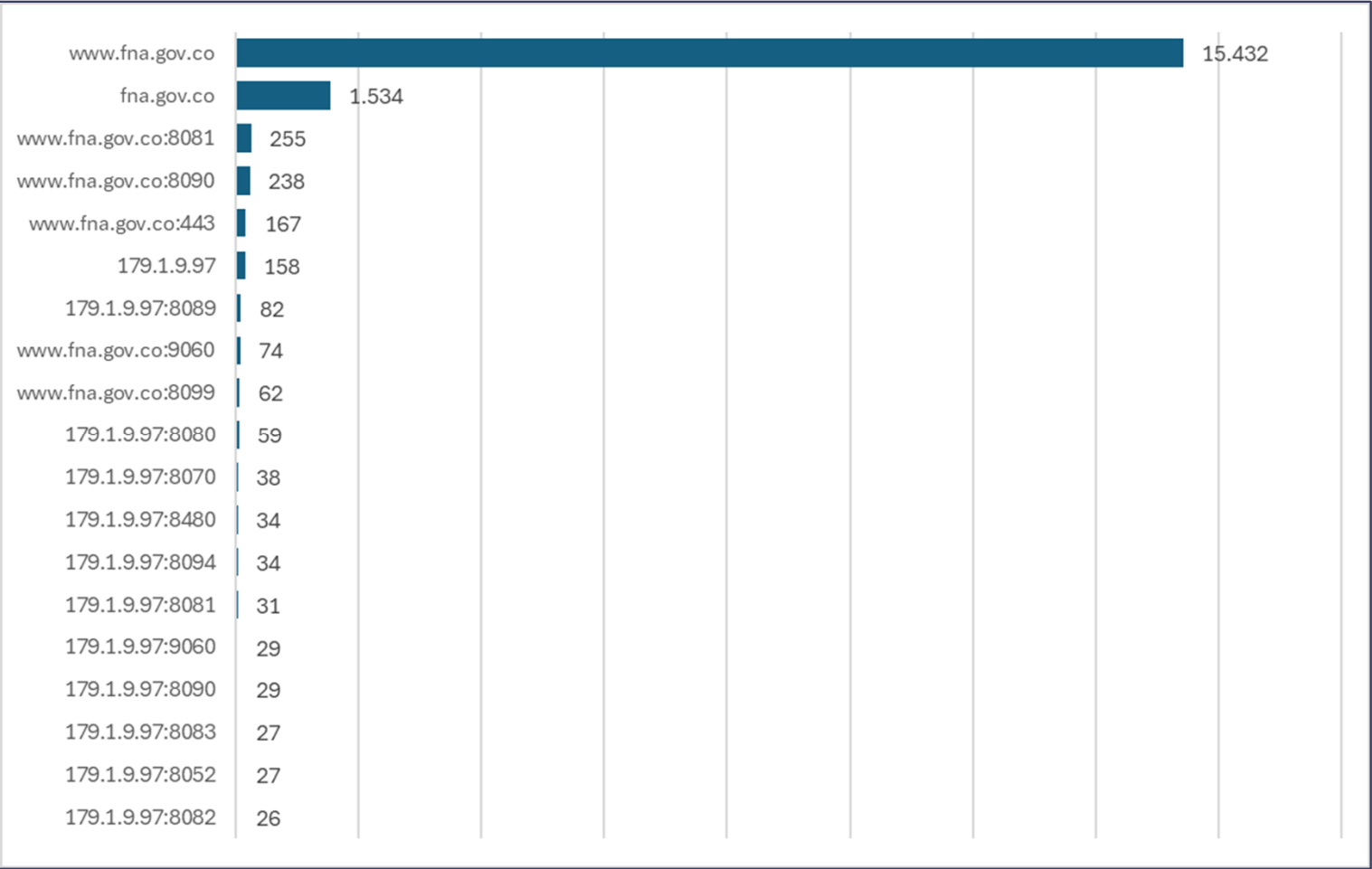
+222 m

IP Reputation



Se detectaron un total 222.691 eventos de amenazas de tráfico proveniente de direcciones IP maliciosas

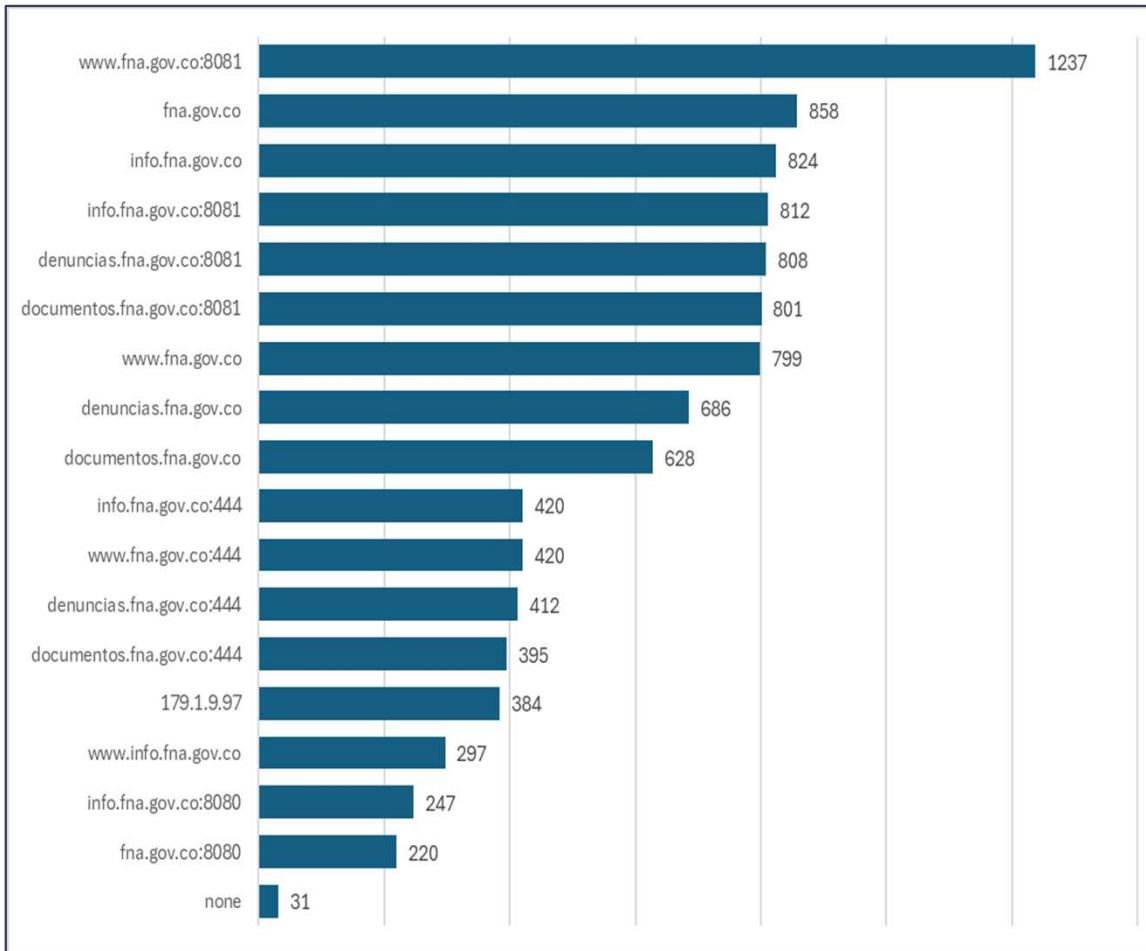
GENERAL WAF – KNOWN BOTS



18.336
KNOWN BOTS

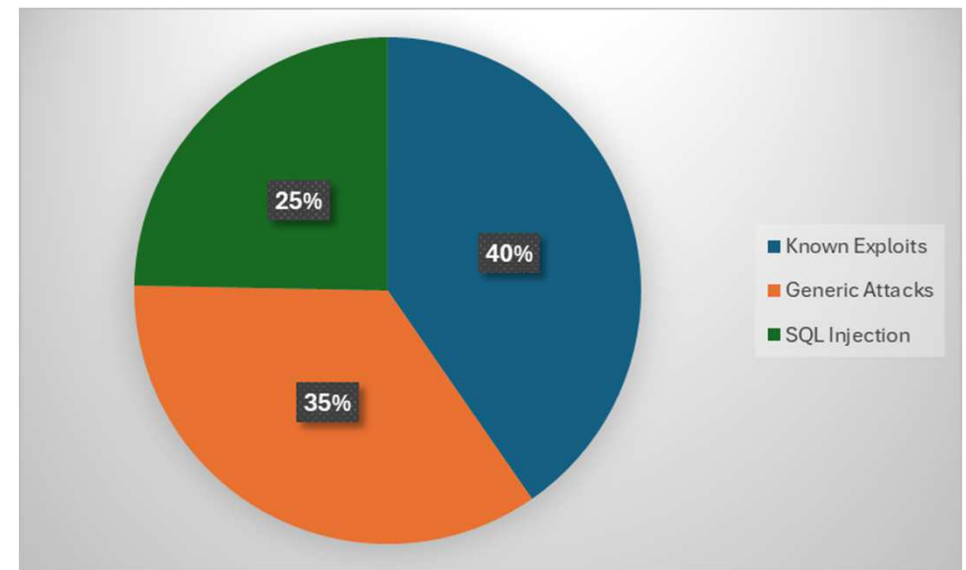


GENERAL WAF – SIGNATURE DETECTION



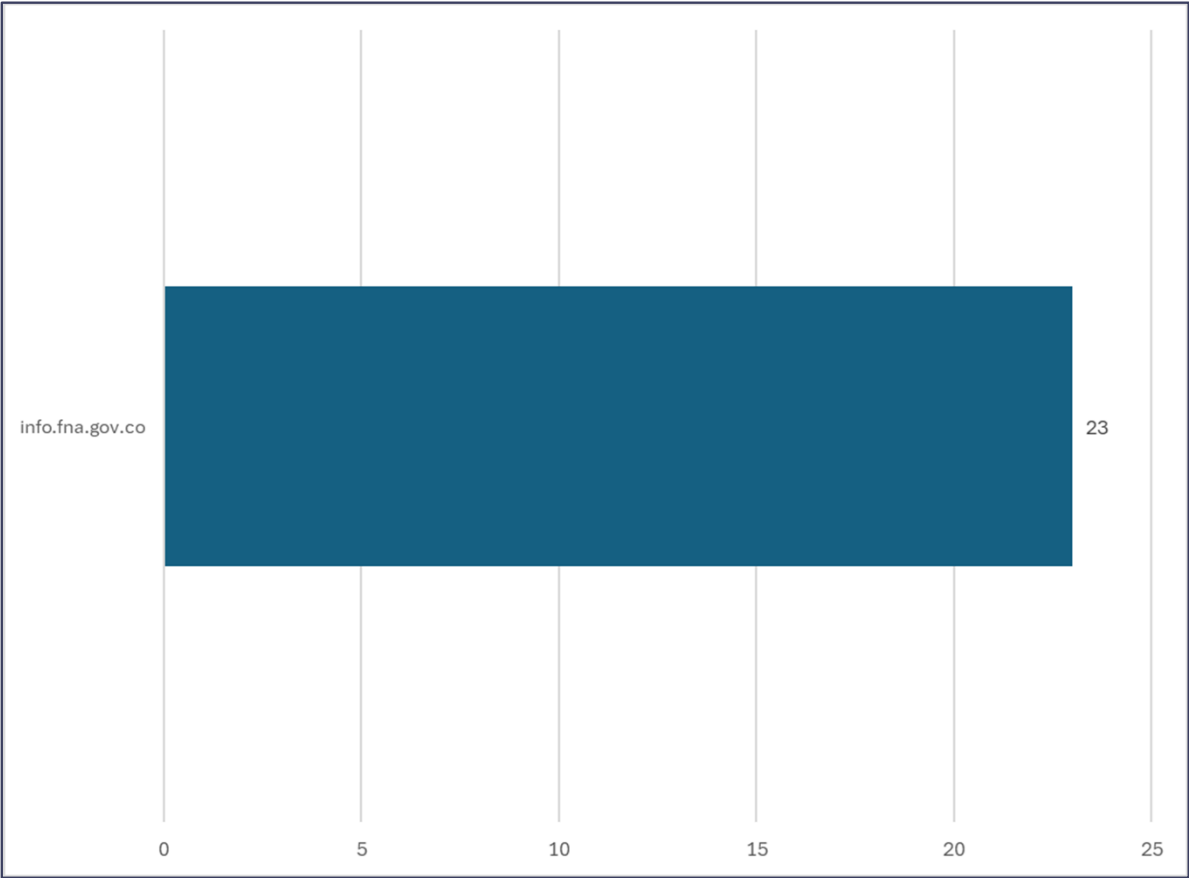
10,279

Signature Detection

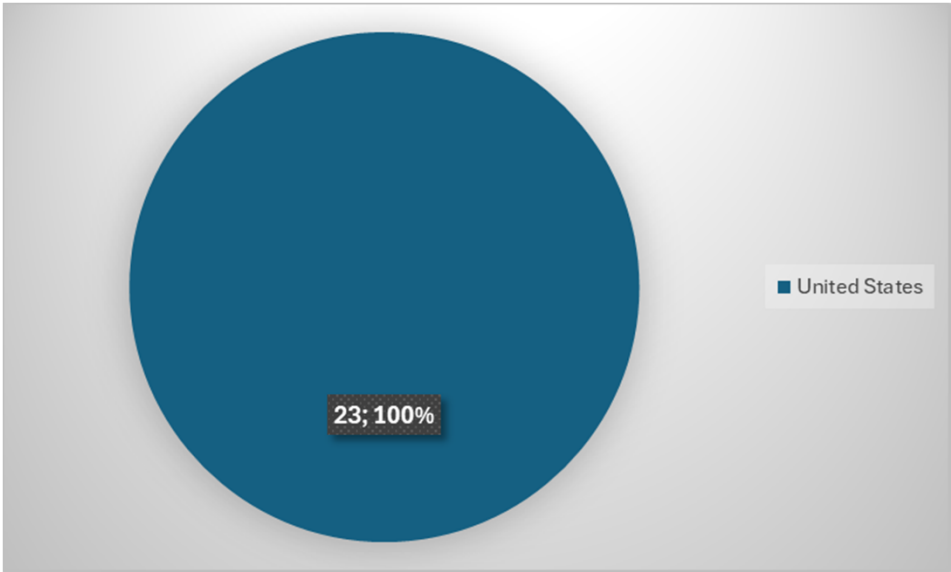


Se detectaron un total 10.273 eventos de ataques conocidos.

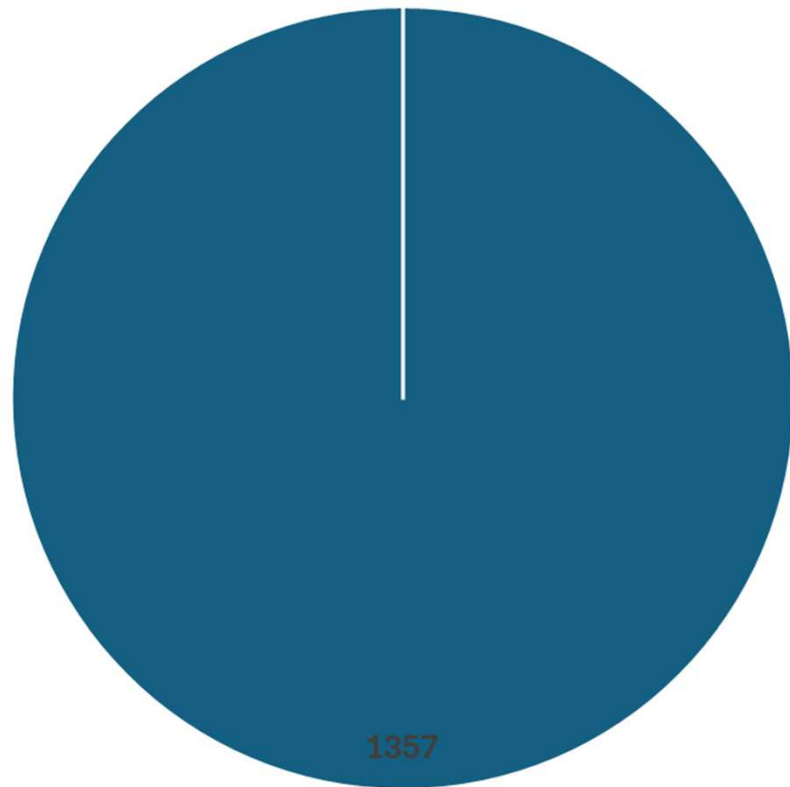
GENERAL WAF - CUSTOM ACCESS



23
Custom Access



GENERAL WAF - GEO IP

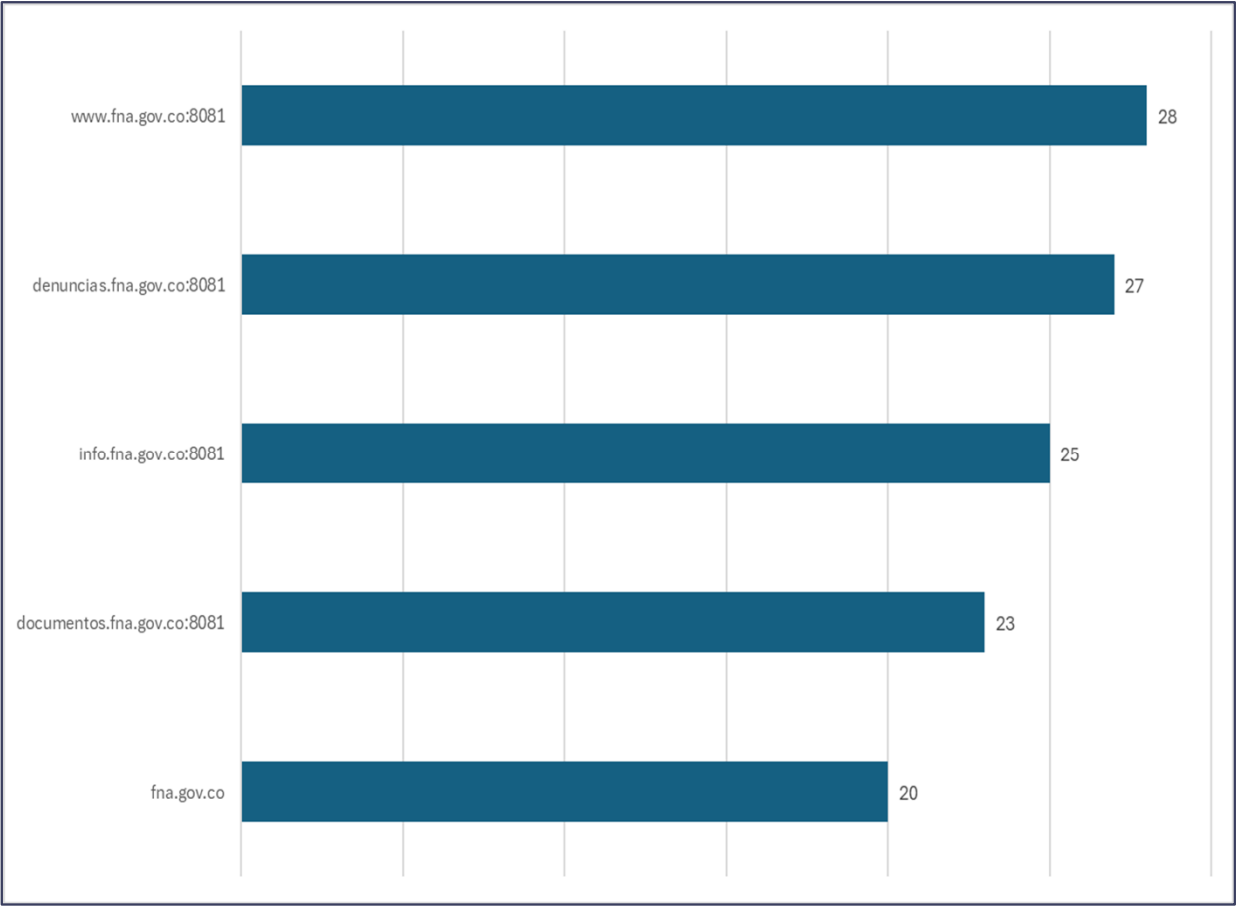


1.357

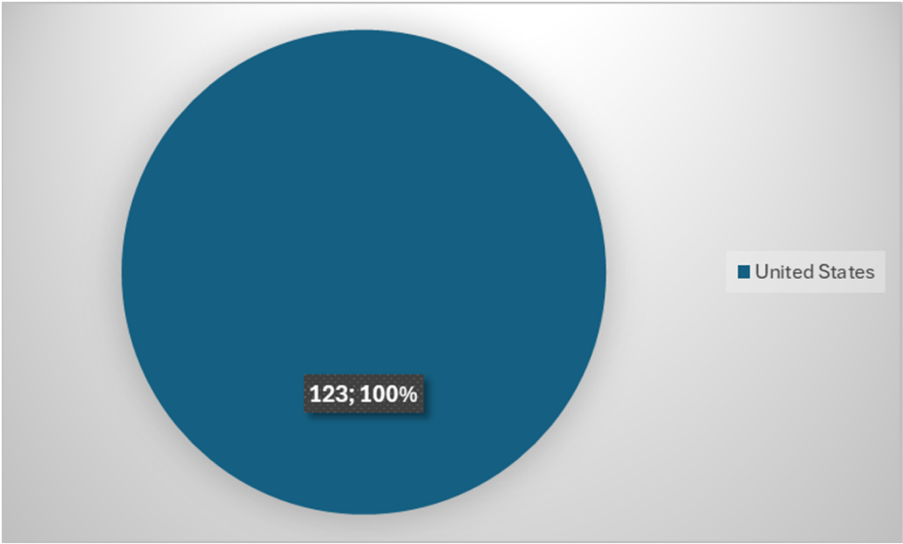
GEO IP

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

GENERAL WAF – FILE UPLOAD RESTRICTION

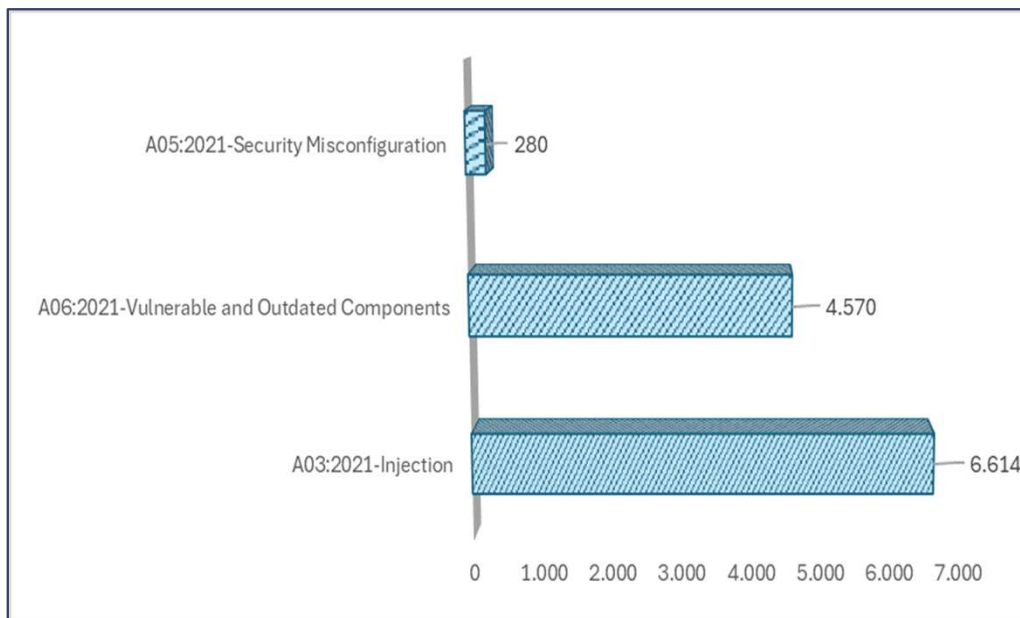


123
Custom Access

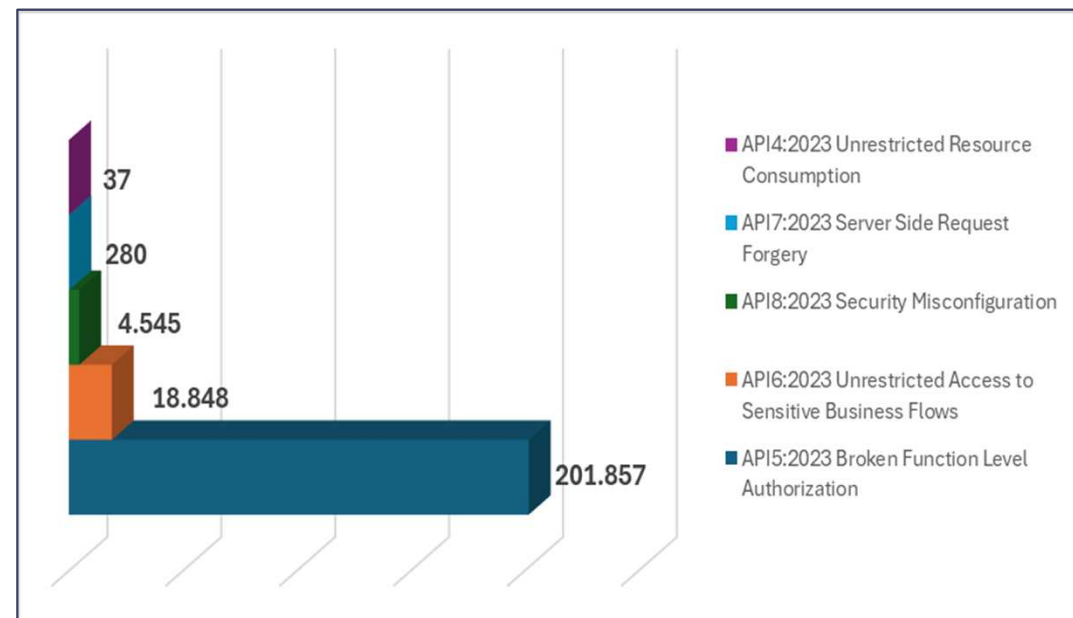


GENERAL WAF – FORTIWEB

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

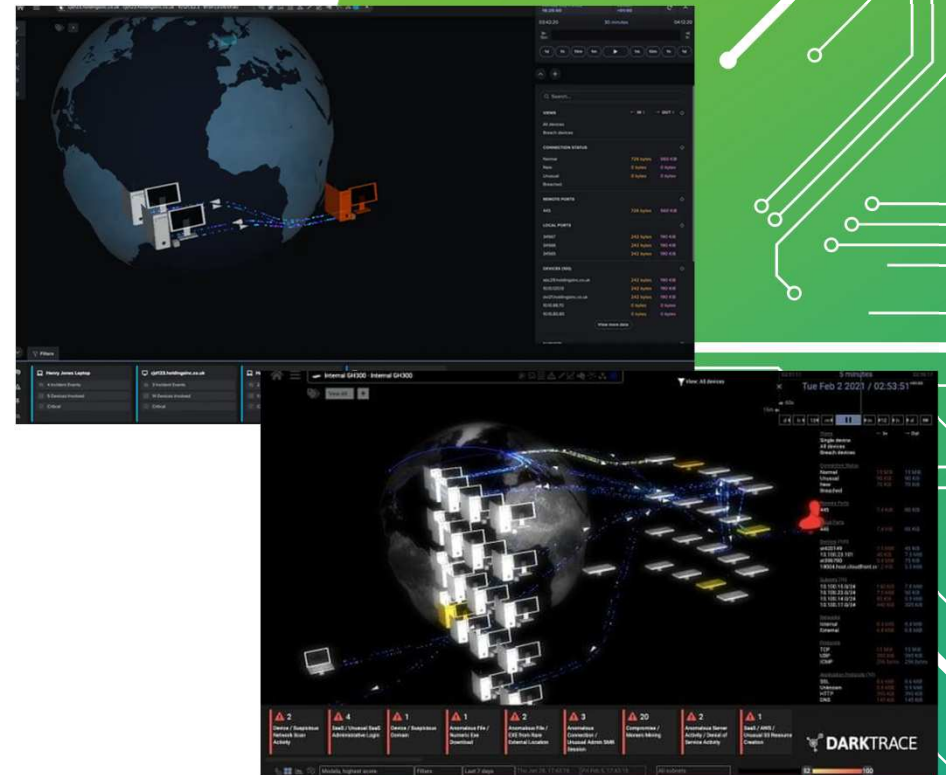
Actividades en proceso: Se realizó el control de cambios **C62792**, para empezar con la actividad de protección de las aplicaciones restantes.



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.





7.515

Dispositivos
modelados

222

Subredes

671

Dispositivos en
brechas

1.077

Brechas

151

Modelos

Informe solución Darktrace/Respond

2024

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 Agosto y el 21 de Septiembre de 2024, comprendiendo los siguientes temas.

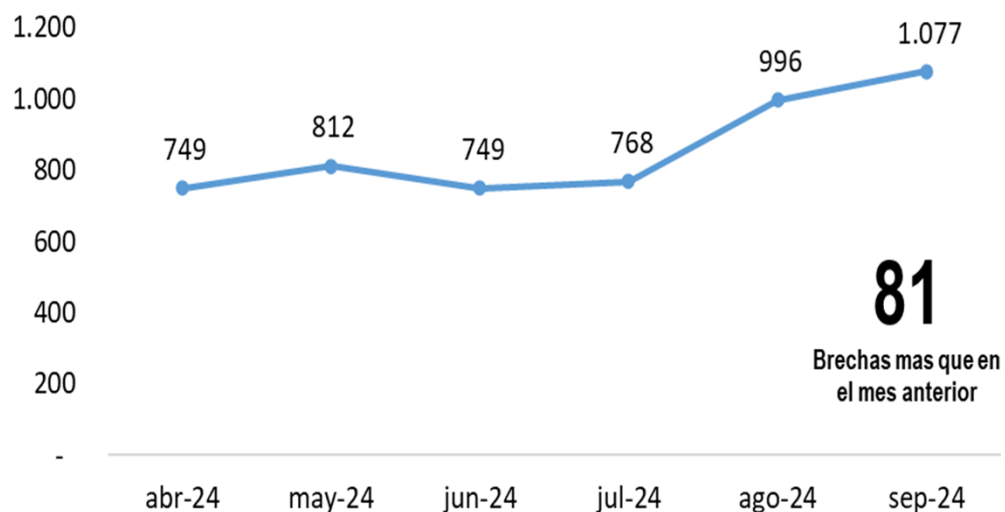
- Dar a conocer las estadísticas generales de la solución de Ciberdefensa.
- Presentar los modelos que se alertaron durante el periodo.
- Dar a conocer los sistemas identificados en los modelos presentados.
- Recomendaciones.

Distribución de Brechas

Brechas Darktrace/Detected

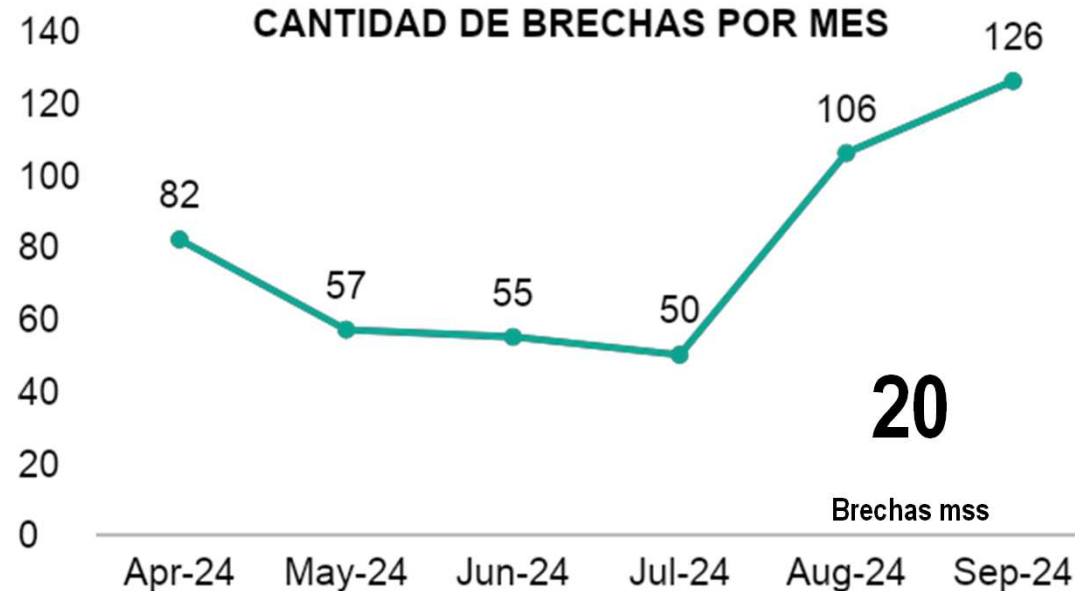
En las gráficas a continuación se dan a conocer las brechas totales registradas hasta la fecha junto con el equivalente en porcentaje respecto al periodo anterior.

BRECHAS IDENTIFICADAS POR MES



Modelos Darktrace/Respond

CANTIDAD DE BRECHAS POR MES

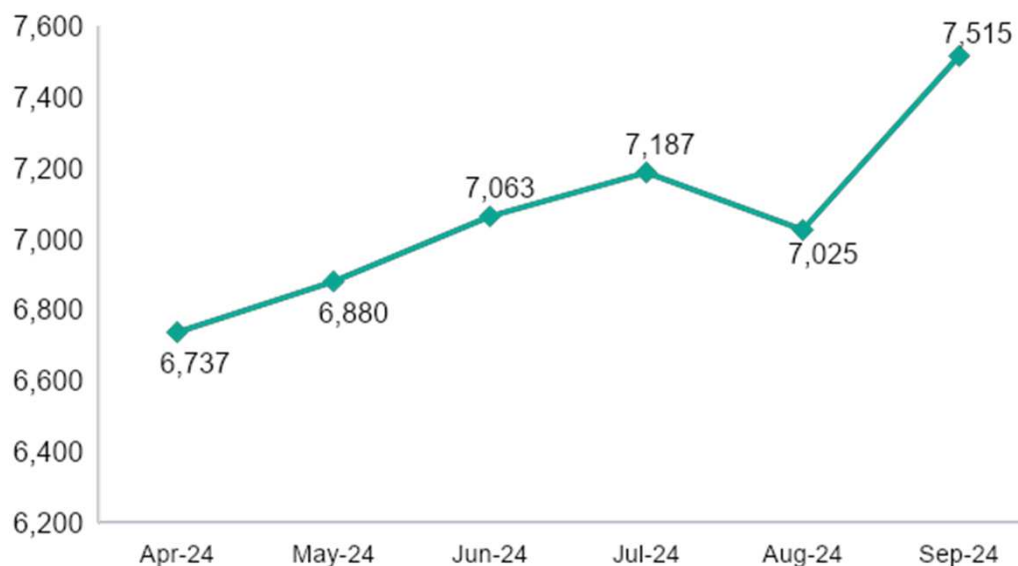


Brechas identificadas por categoría

Licenciamiento

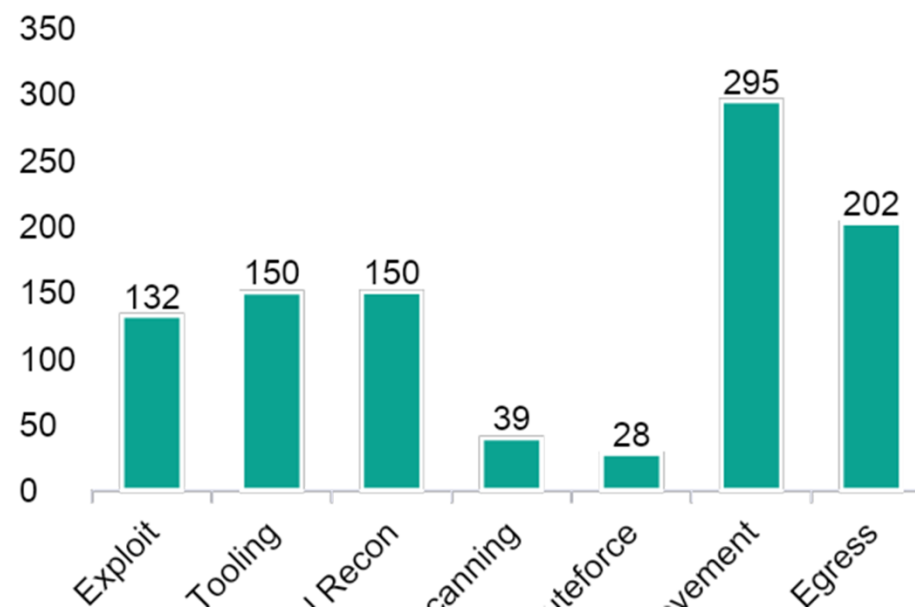
Los modelos de ciberdefensa se pueden organizar de acuerdo con la fase de ataque que es más probable que detecten. Los modelos de monitoreo de acuerdo con estas categorías pueden permitir que el patrón de comportamiento característico de un ataque en curso sea observado.

DISPOSITIVOS MODELADOS POR MES



Distribución de Brechas

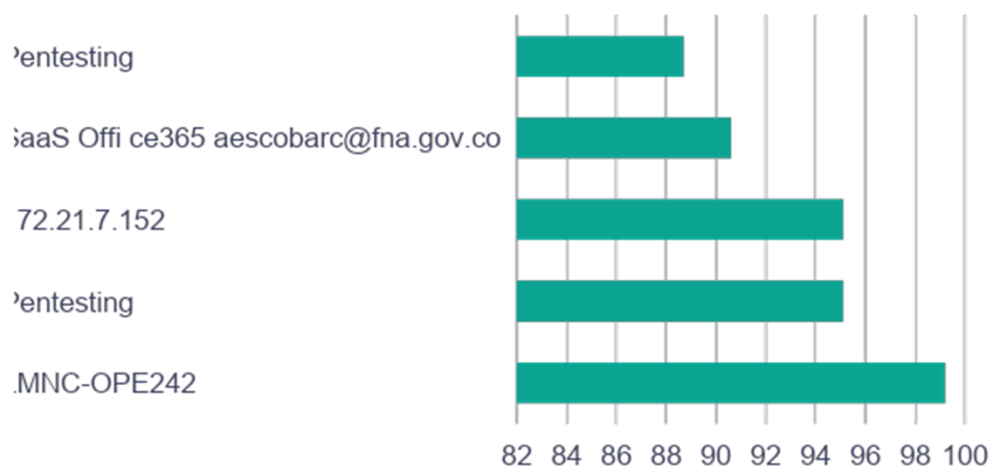
CANTIDAD DE BRECHAS POR CATEGORIA



TOP Dispositivos con Modelos de Alta Prioridad

Los dispositivos destacados aquí han violado modelos evaluados para representar comportamientos considerados de alta prioridad para la organización

TOP Dispositivos Modelos Alta Prioridad



Equipo /Modelo

LMNC-OPE242

- Suspicious Network Scan Activity
- Large DNS Volume for Suspicious Domain

Pentesting

- Suspicious SMB Scanning Activity
- Suspicious Network Scan Activity
- Attack and Recon Tools

172.21.7.152

- Suspicious HTTP and Anomalous Activity

SaaS Offi ce365 aescobarc@fna.gov.co

- Unusual Login and New Email Rule

Pentesting

- Possible SMB/NTLM Brute Force
- Suspicious SMB Scanning Activity
- Kerberos Username Brute Force

Distribución de Dispositivos Modelados

Equipos Modelados Darktrace

Tipo Dispositivo	Total
desktop	4.761
server	1.002
mobile	892
iphone	139
unknown	137
laptop	109
dnsserver	49
proxyserver	4
fileserver	3
printer	2
Total	7.098

Distribucion Nuevos Equipos

Mes	xDia	Total
Enero	5	150
Febrero	61	1.830
Marzo	6	180
Abril	15	450
Mayo	18	540
Junio	17	510
Julio	42	1.260
Agosto	37	1.110
Septiembre	15	450

Los días que más se presentaron equipos nuevos fueron:

- 6 de Febrero con 462
- 7 de Febrero con 281
- 2 de Julio con 102
- 25 de Julio con 132

Equipos con Nombres Duplicado 1.320, estos porque se conectan por Cable y Wifi.

304.933
Correos Entrantes

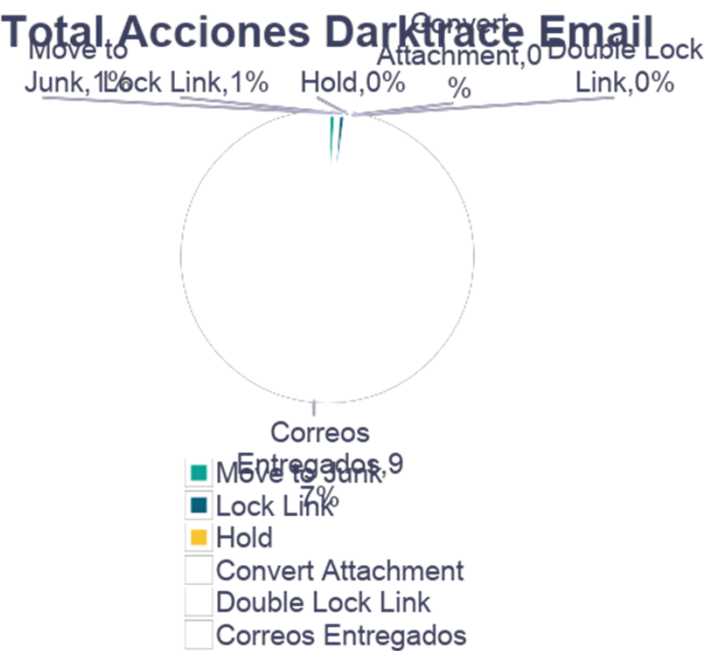
9.408
Correos con accion

300.797
Correos Entregados

911.779
Correos Salientes

Informe solución Darktrace/Email

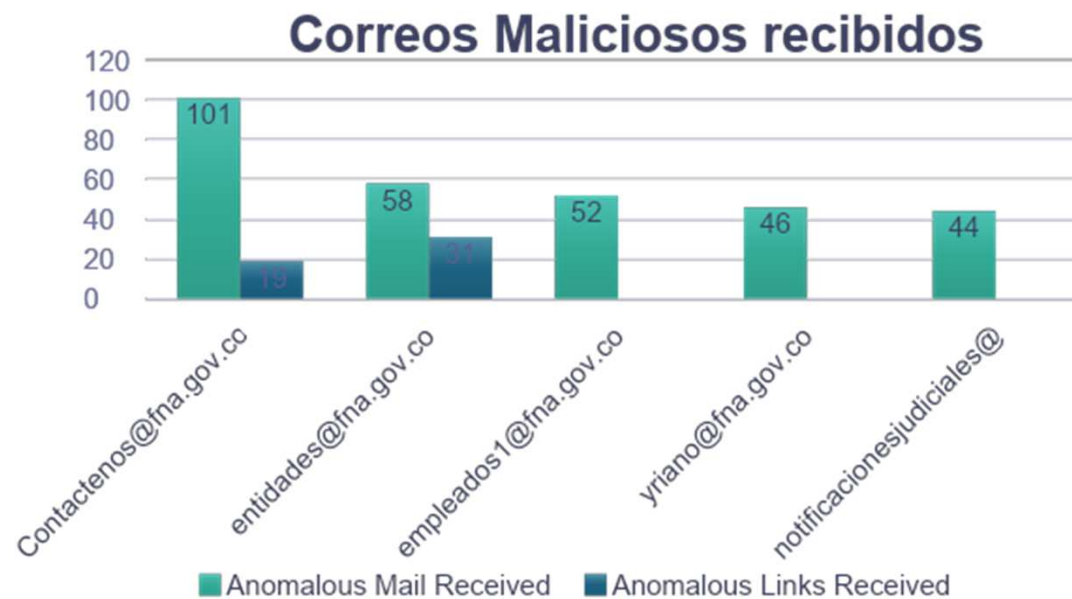
2024



Top Acciones	Total, Acciones	% total de correos
Move to Junk	4.565	1%
Lock Link	2.779	1%
Hold	1.001	0,3%
Convert Attachment	617	0,2%
Double Lock Link	446	0,1%

Administración Email

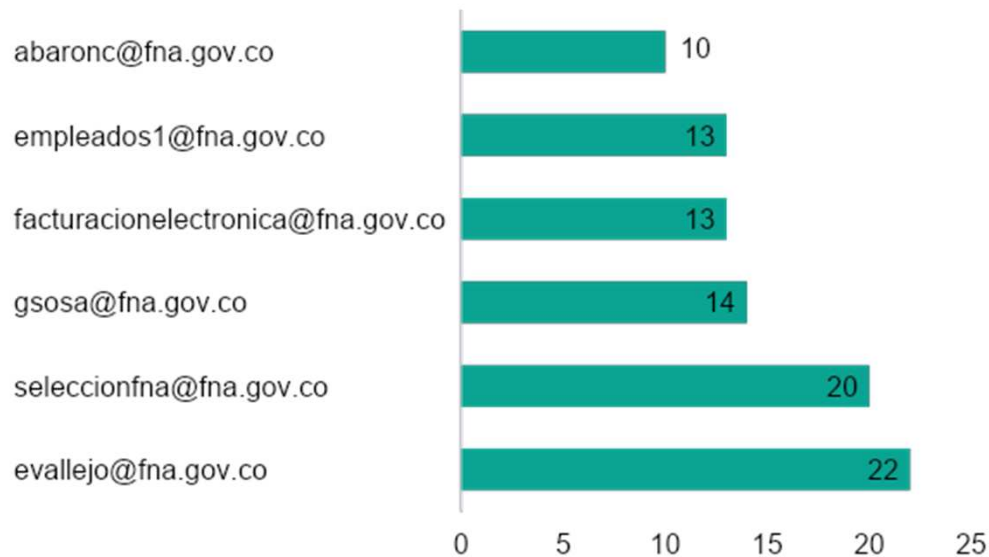
Los siguientes usuarios recibieron la mayor parte del correo de este tipo en el periodo correspondiente al presente informe. Todo el correo incluido en este recuento habría alcanzado el umbral básico para la acción Mover a correo no deseado de Darktrace/Email.



Administración Email

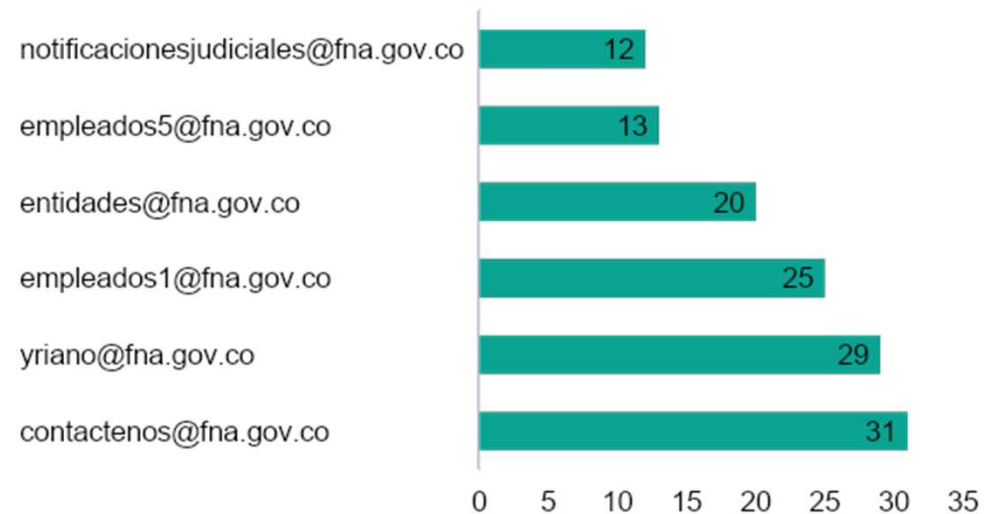
Múltiples anomalías han elevado la puntuación de este correo electrónico por encima del umbral (threshold) de retención.

Top Destinatarios Convert Attachment



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

Top Destinatarios Email Retenido



Actividades realizadas

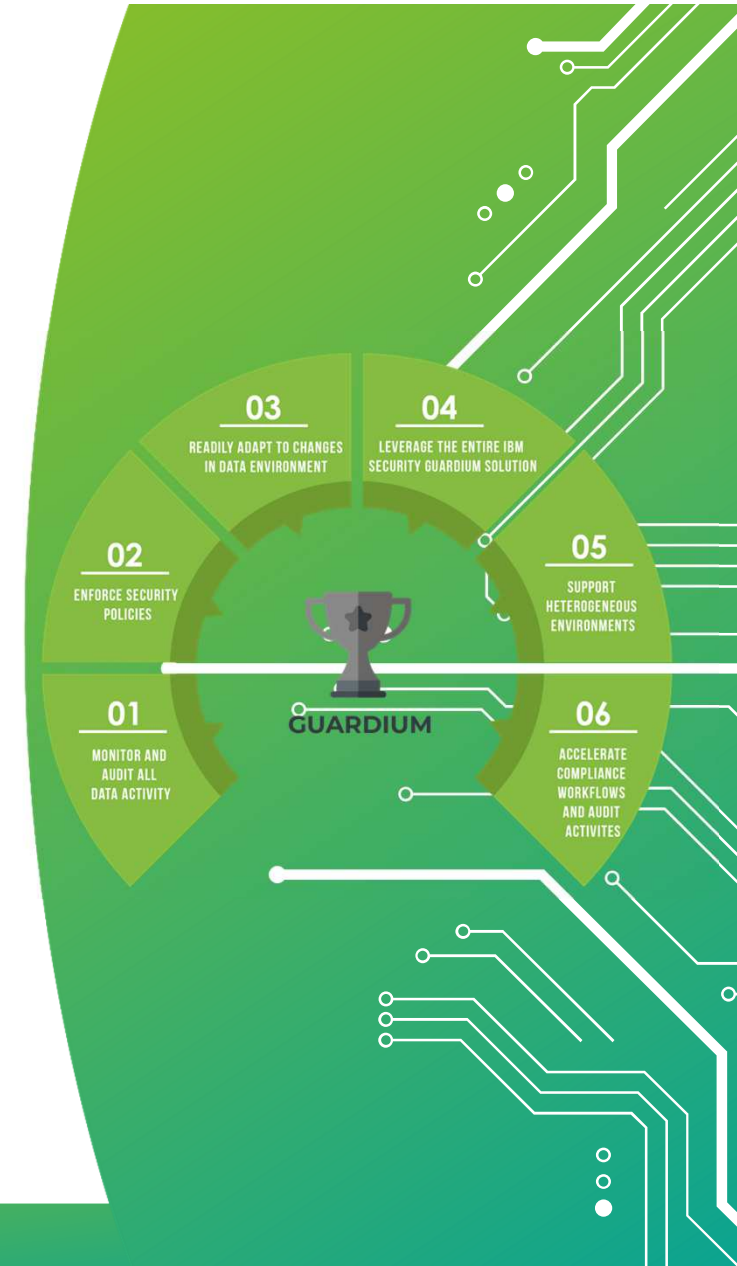
De acuerdo con los eventos generados en las diferentes herramientas y la gestión diaria dentro del FNA se dan las siguientes recomendaciones y conclusiones.

- 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 genera exclusión de los modelos Suspicious SMB Scanning Activity, SMB Enumeration, Unusual Internal EXE File Transfer. De acuerdo alerta reportada 46580.
- Se realiza revisión de correo retenido por LINK del usuario vgomez@fna.gov.co, el cual por tiempo de retención no se puede liberar, solicitud desde seguridad de la información.
- Se realiza solicitud al área de redes, para suministrar archivo con información de las Subredes de FNA, SD1114412
- Se realiza revisión de los correos las cuentas de correo gerenciadejuzgamiento@fna.gov.co y zespinoza@fna.gov.co, de las cuales no se evidencian registros de correos retenidos, Solicitud por correo electrónico
- Se genera informe detallado de la alerta reportada 46992 del equipo DESKTOP-BDRKOTP
- 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 agosto y el 21 de septiembre de 2024, la plataforma presentó estabilidad y normalidad en su operación.

Actividades macro ejecutadas	Actividades a ejecutar
● Pruebas de ofuscamiento. ● Tarjeta red appliance. ● Monitoreo roles 60 y 222 COBIS. ● Monitoreo transacciones SAPHana. ● Definición reglas COBIS producción. ● Adición reglas en políticas generales.	Continuación de actividades: ● Monitoreo roles 60 y 222 COBIS. ● Monitoreo transacciones SAPHana. ● Definición reglas COBIS producción. ● Pruebas de ofuscamiento.



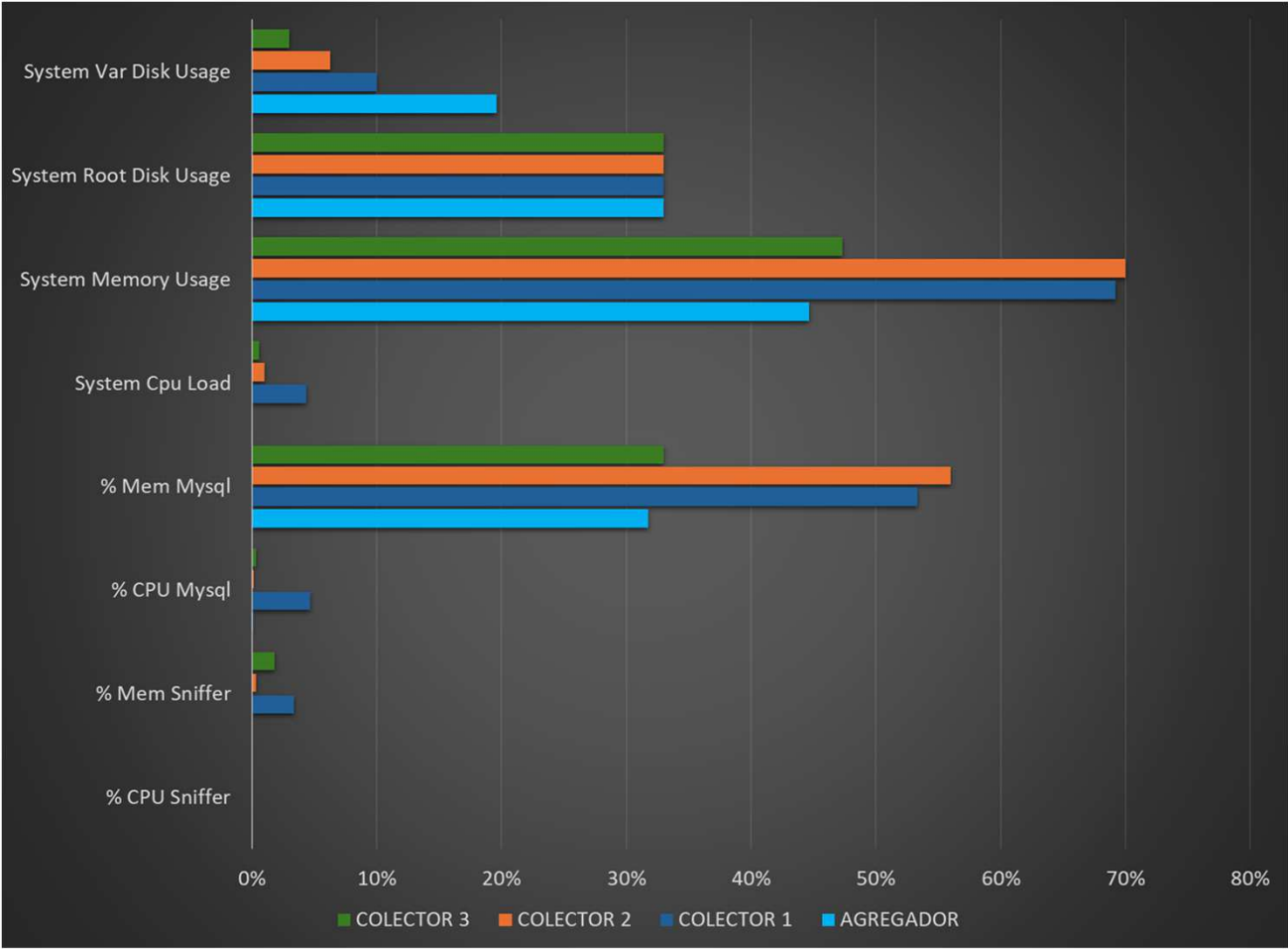
Top errores base datos

Client IP	Server IP	Server Type	DB User Name	Database Error Text	Count
172.16.126.33	172.16.128.20	SYBASE	INTRANETPOOL	Arithmetic overflow during %S_MSG conversion of %s value '%s' to a %s field .	397974
172.16.126.32	172.16.128.20	SYBASE	INTRANETPOOL	Incorrect syntax near '%.*s'.	395181
172.16.128.20	172.16.128.20	SYBASE	OPBATCH	"Cannot drop the %S_MSG '%.*s'"	49930
192.168.180.135	192.168.180.143	SAP HANA	SAPABAP1	ERR_SQL_UNIQUE_VIOLATED :unique constraint violated	43356
172.16.126.33	172.16.128.20	SYBASE	COBISCTS3	Unable to connect to server '%.*s'.	13071

Top login failed

DB User Name	Source Address	Destination Address	Database Protocol	Count
WM_USER	172.16.124.109	172.16.123.250	MS SQL SERVER	188550
WM_USER	172.16.124.174	172.16.123.252	MS SQL SERVER	84922
MONITOR	192.168.180.135	192.168.180.143	SAP HANA	45310
WM_USER	172.16.124.113	172.16.123.252	MS SQL SERVER	40892
BIZAGICERT	172.16.124.157	172.16.123.190	MS SQL SERVER	27411
COBROJUR	172.16.123.112	172.16.123.75	SYBASE	11517
COBROJUR	172.16.123.100	172.16.123.75	SYBASE	11512
FNACALLCENTER	172.16.123.100	172.16.123.190	MS SQL SERVER	2935

Comportamiento plataforma, 22 de agosto al 21 de septiembre de 2024



Servidores de bases de datos monitoreados

Servidor	Servidor
10.10.12.74	172.16.131.57
172.16.123.141	192.168.180.143
172.16.123.175	192.168.180.153
172.16.126.68	172.16.123.75
172.16.128.20	172.16.123.128
172.16.131.100	172.16.123.132
172.16.131.101	172.16.123.133
172.16.131.109	172.16.123.171
172.16.131.110	172.16.123.172
172.16.131.128	172.16.123.76
172.16.131.129	172.16.123.77

Producción	11
db2	2
HANA	1
MSSQL	7
sybase	1
Pruebas	11
db2	1
HANA	1
MSSQL	7
ORACLE	1
sybase	1

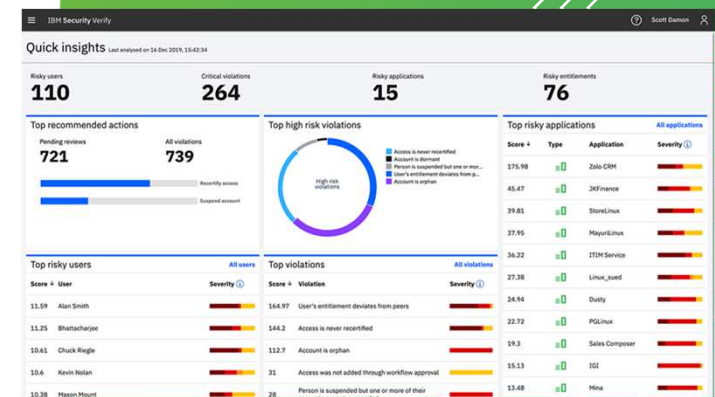


Verify

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.

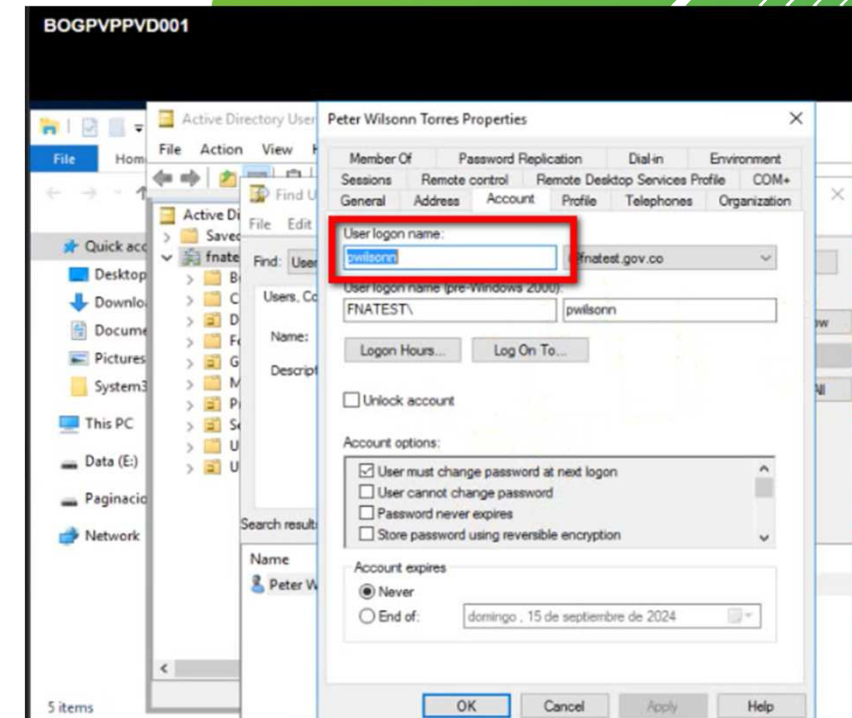
Autenticación avanzada, incluida la autenticación sin contraseña

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.



Directorio Activo

- Para el periodo de Agosto 22 a Septiembre 21 se continúa con las pruebas Funcionales para paso a producción desde Verify contra el Directorio activo con resultados satisfactorios en la creación, modificación y retiro de los usuarios.
- Se realiza el paso a producción el lunes 16 de septiembre con resultados satisfactorios, queda en monitoreo para ajustes del día a día.



SERVICE MANAGER

- Para el periodo de Agosto 22 a Septiembre 21 se realizaron los ajustes solicitados para Service Manager por lo tanto las pruebas integrales desde la plataforma de Verify que cubre todos los aspectos funcionales, de creación, modificación y cese de un usuario se realizaron con resultados positivos; se inicia la solicitud de cambios para paso a producción.
- Se realiza el paso a producción el lunes 16 de septiembre con resultados satisfactorios, quedando en monitoreo ya que el usuario CNX_IAM se bloquea y realizar ajustes que se presenten en el día a día.

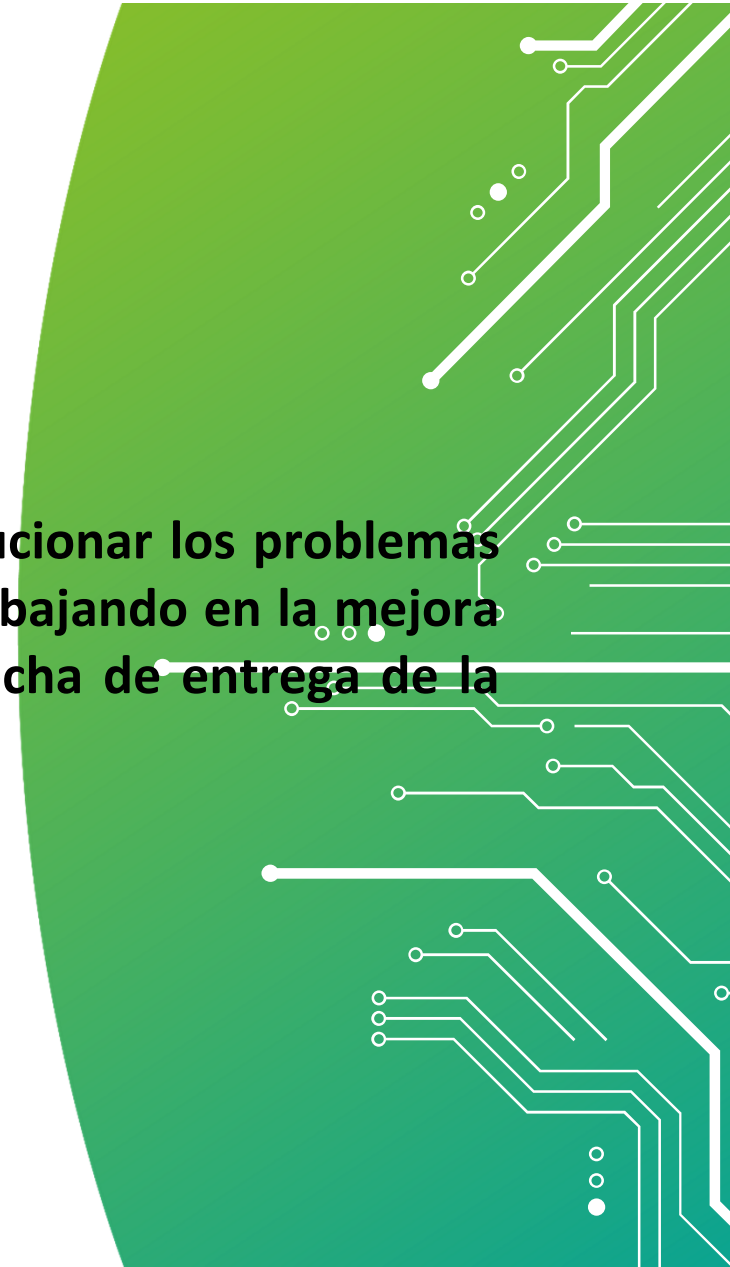


SAP

- Para el periodo de Agosto 22 a Septiembre 21 se realizaron los ajustes solicitados para SAP por lo tanto las pruebas integrales desde la plataforma de Verify que cubre todos los aspectos funcionales, de creación, modificación y suspensión de un usuario se realizaron con resultados positivos; se inicia la solicitud de cambios para paso a producción.
- Se realiza el paso a producción el lunes 16 de septiembre con resultados satisfactorios, queda en monitoreo para ajustes del día a día.

Cobis

Por parte de fábrica se debe hacer un desarrollo para solucionar los problemas de creación de los usuarios, nos informan que ya están trabajando en la mejora y hasta el 21 de Septiembre de 2024 no nos han dado fecha de entrega de la solución.



QRADAR

Se realiza el paso a producción de Verify el lunes 16 de septiembre con resultados satisfactorios, se están verificando nuevos eventos y queda en monitoreo para posibles ajustes del día a día.



ADMINISTRACIÓN DE USUARIOS

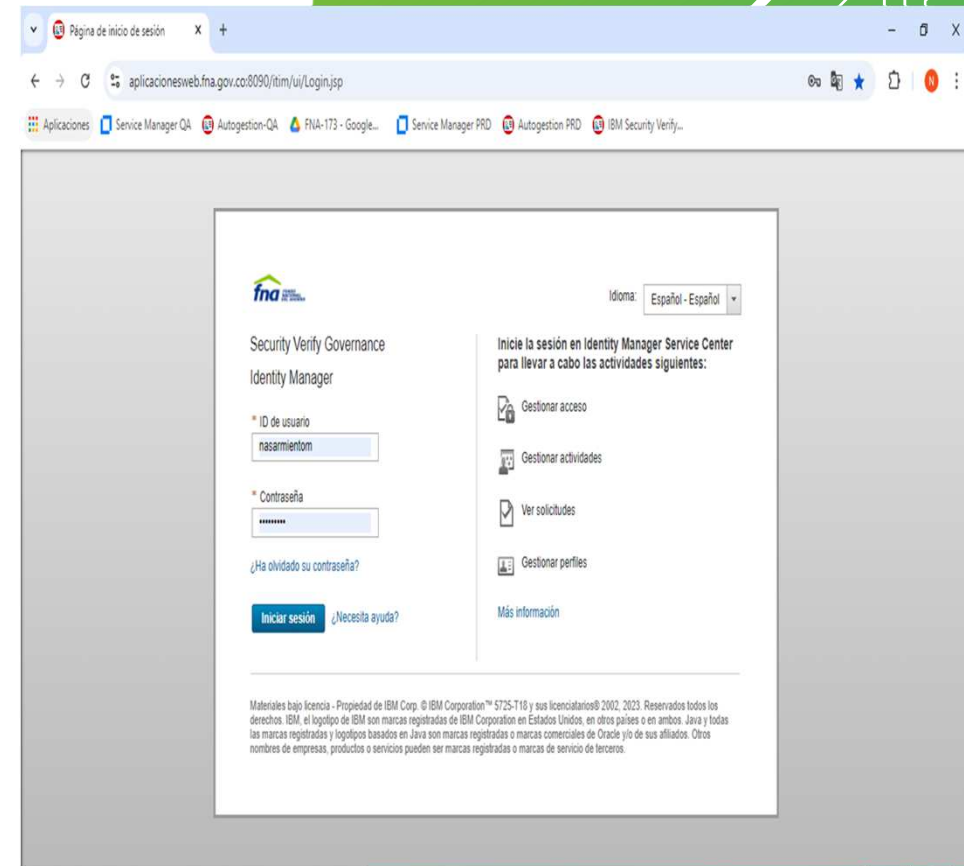
El lunes 29 de Julio se hace la solicitud al ingeniero Wilson Morales de la siguiente información:

- **solicitamos nos entreguen los archivos WSDL de pruebas para poder consumir los webs Services**
- **Solicitamos la asignación de un usuario de servicio para administración de usuarios**
- **solicitamos la información del servidor de pruebas de administración de usuarios para la integración con Verify (IP, puerto), para solicitar los permisos y poder consumir los webs Services.**

El martes 13 de agosto se reenvió el correo recordándole la entrega de la información, hasta el 21 de Septiembre no hemos revisado la información solicitada.

AUTOGESTIÓN

- Se realizan las pruebas el miércoles 28 de agosto con resultados satisfactorio y se inicia la solicitud de cambios para paso a producción.
- Se dictan las capacitaciones a los analistas de mesa de servicio y se genera el documento del paso a paso para los funcionarios del FNA
- Se realiza el paso a producción el lunes 16 de septiembre con resultados satisfactorios, queda en monitoreo para los ajustes del día a día.



Recomendaciones y conclusiones

Para este periodo se realizan las pruebas integrales para paso a producción en la integración con SAP, Directorio activo, Service Manager y la activación de Autogestión.

Se hace el paso a producción de la solución de Verify con las integraciones de SAP, Directorio Activo, Service Manager y Autogestión.

Para este periodo se sigue evidenciando el siguiente evento que nos lleva a retrasos:

- Por parte del equipo de Cobis deben hacer un desarrollo y aun no nos han dado fecha de entrega para que nosotros podamos seguir con la integración.
- No nos han entregado la documentación solicitada para Administración de Usuarios.

Se siguen realizando las gestiones correspondientes con las áreas involucradas para el proceso de integración hacia Verify con las demás aplicaciones.





52

Eventos reportados

40

Identity Fraud

8

Data protection

4

Brand protection

Informe Monitoreo de marca

2024

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 septiembre 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

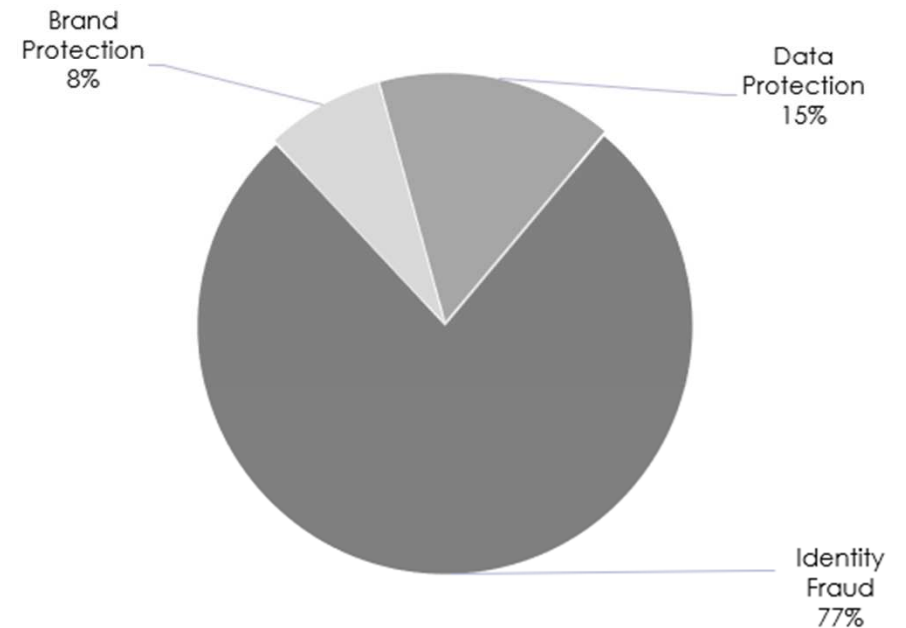
En el monitoreo de marca se busca realizar una captación de la información durante el periodo en mención, en la cual podemos identificar la presencia que tiene la entidad en la Clear, Deep y Dark Web, empleando distintas técnicas digitales que nos permita acceder. En un servicio 7x24 para la identificación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

Resultados Monitoreo de Marca



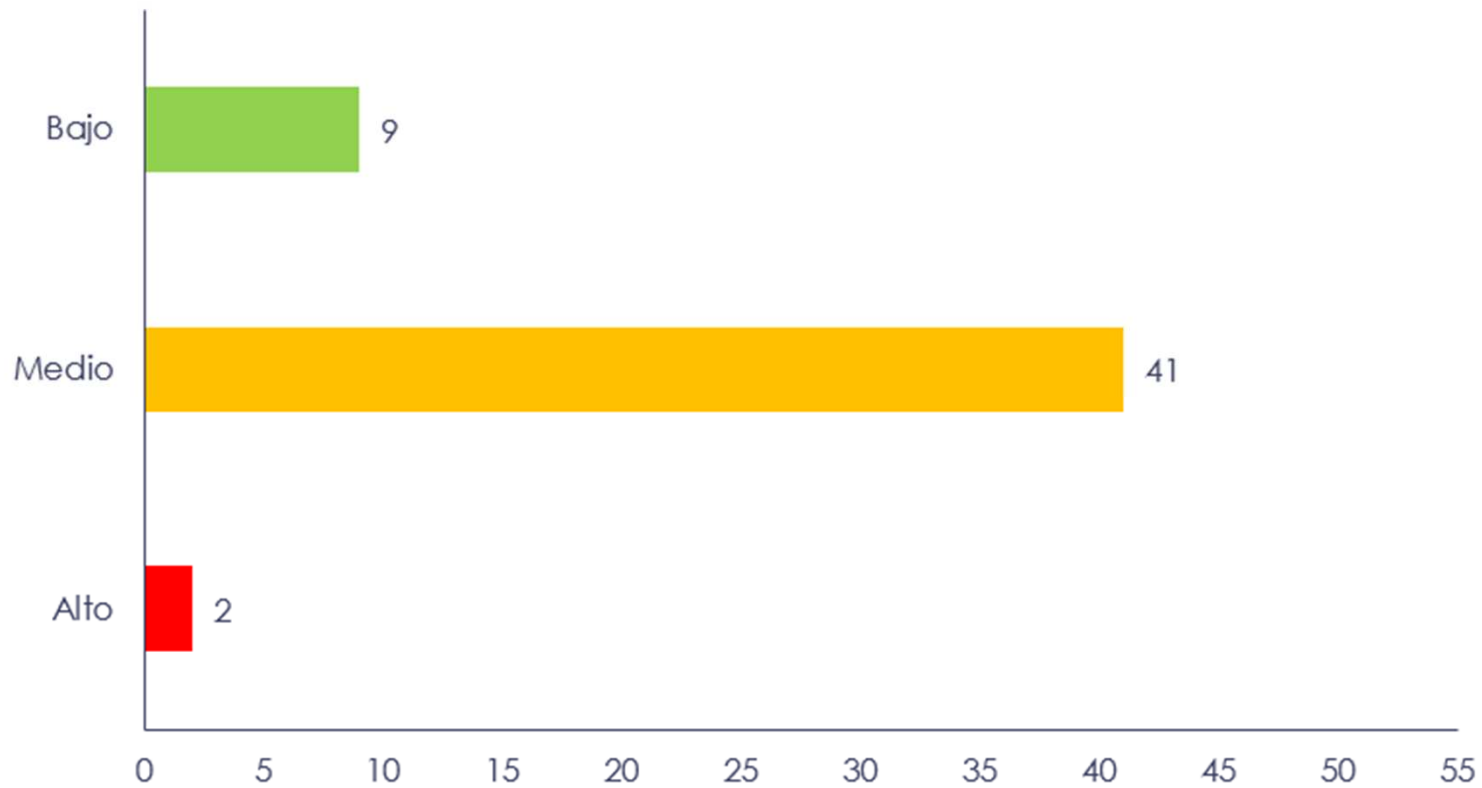
1. Comportamiento del servicio global Vigilancia

% de afectación por subservicio

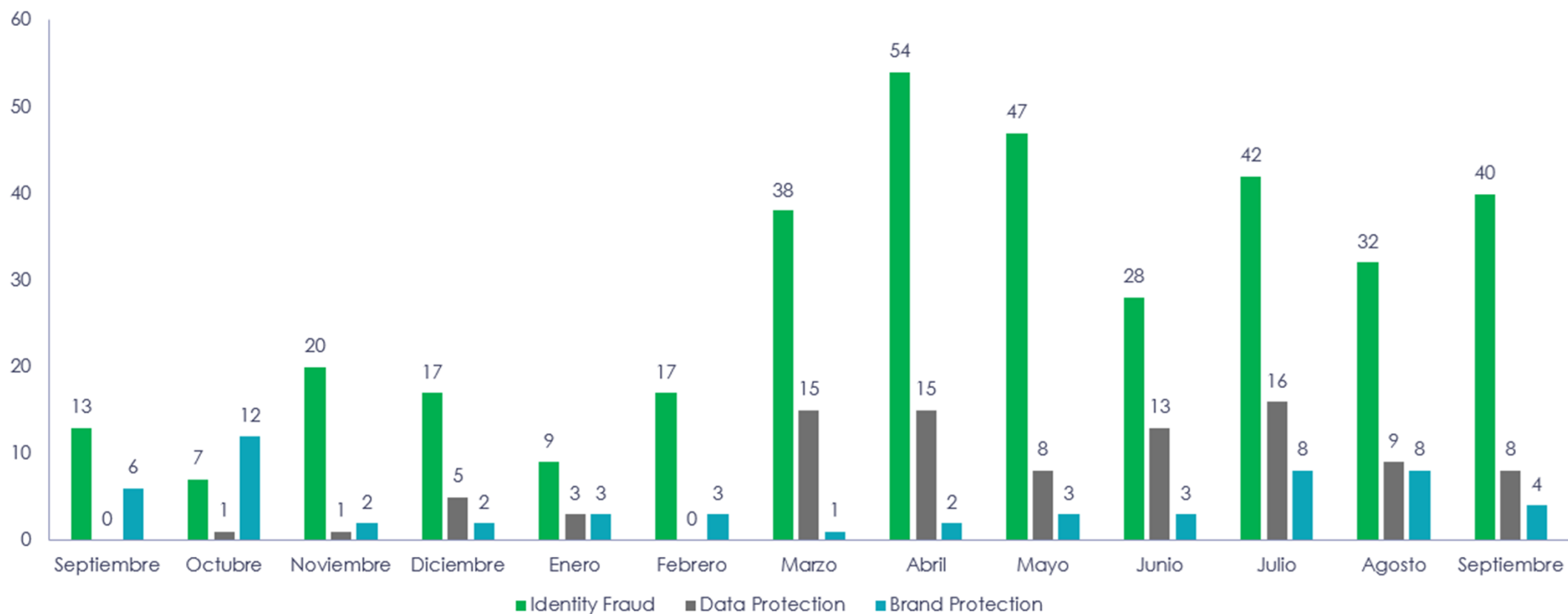


KPIs › Comportamiento del servicio global

ALERTAS CLASIFICADAS POR CRITICIDAD

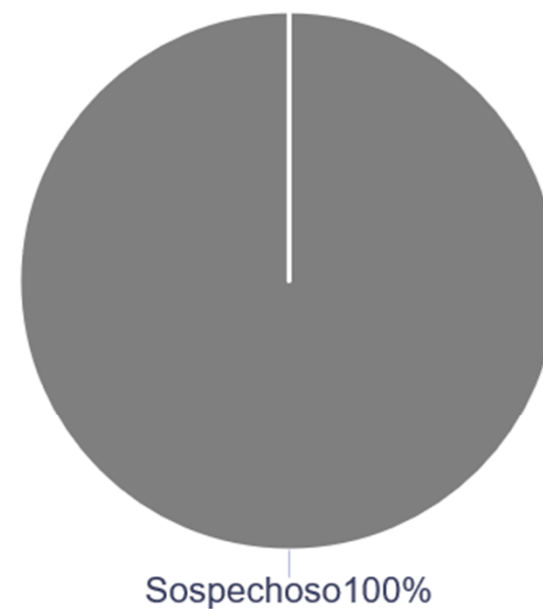


Evolución del servicio a nivel mensual



Resultados Monitoreo de Marca

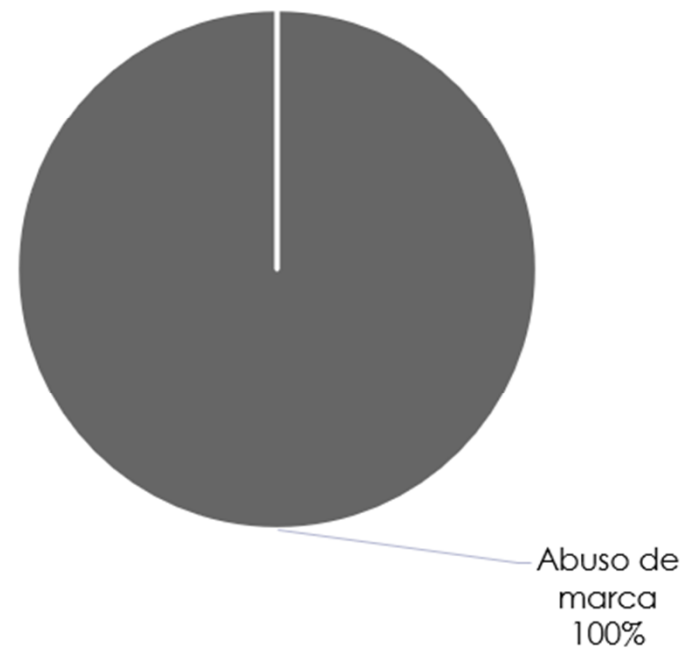
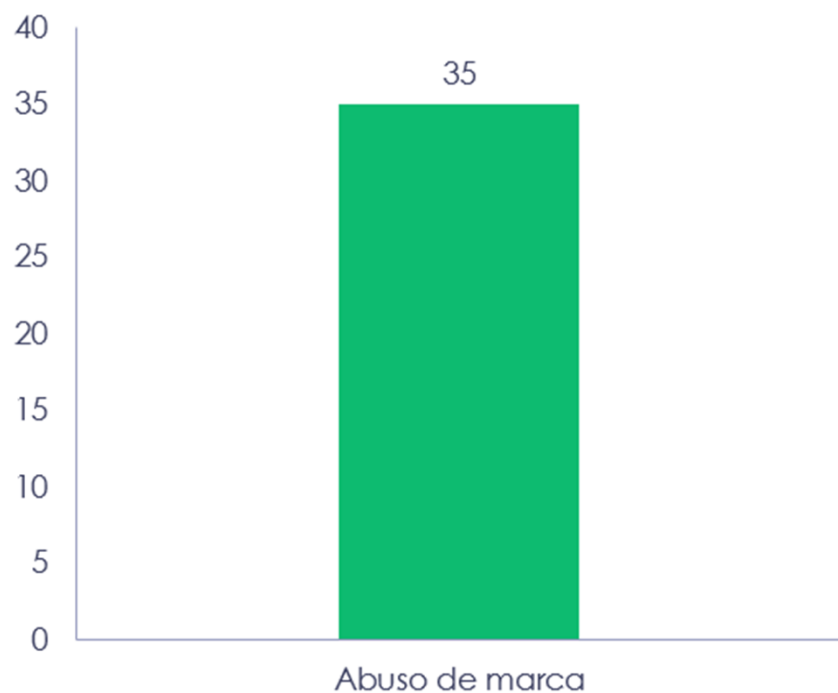
1. DOMINIOS



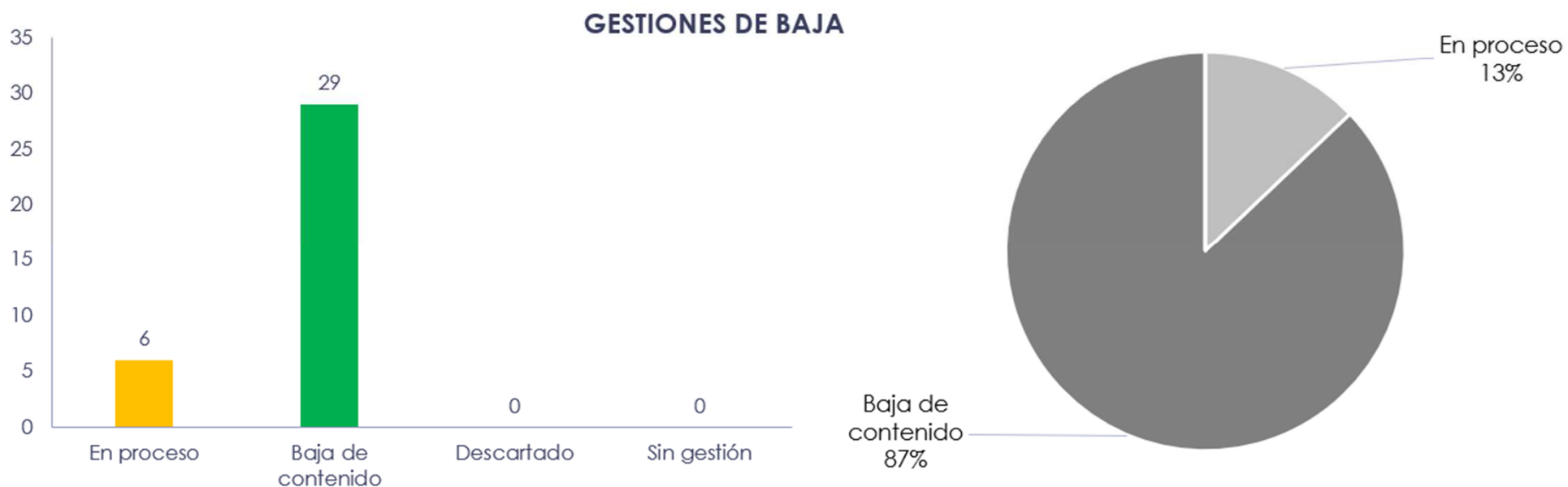
Resultados Monitoreo de Marca

2. REDES SOCIALES

Se identificaron publicaciones en la red social de Facebook, haciendo referencia a ofrecimientos de servicios relacionados con el retiro cesantías 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.

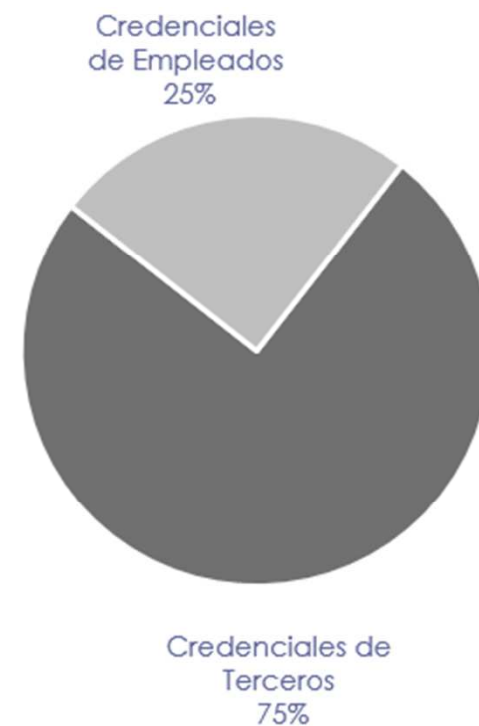
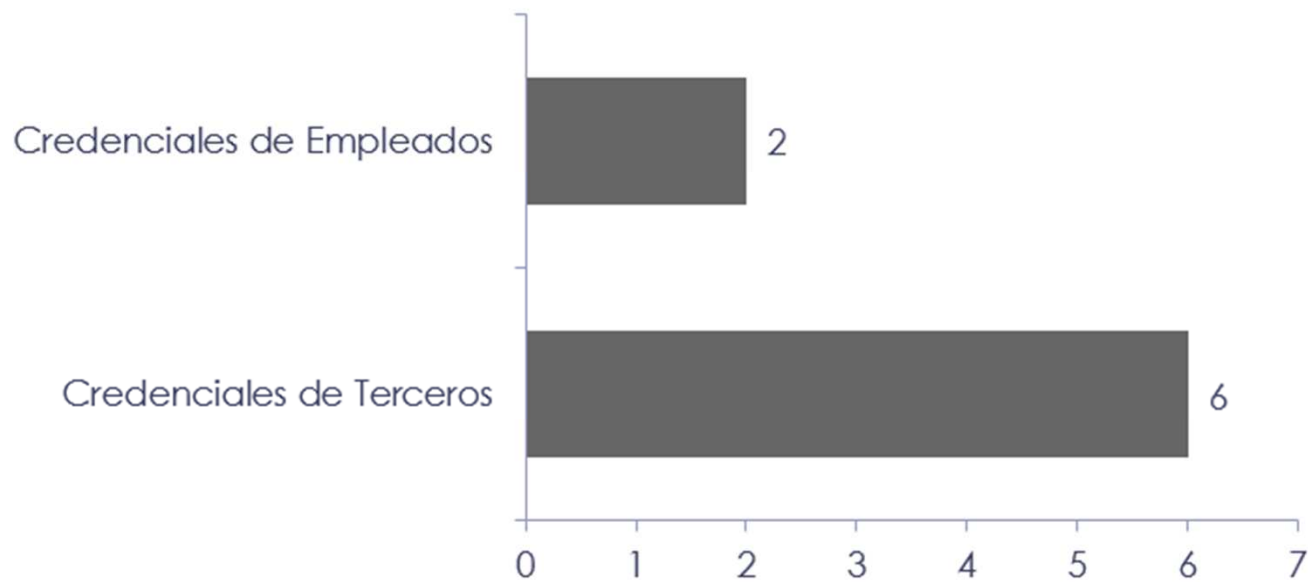
Sin gestión: Eventos sin gestionar. Pendientes de la solicitud del cliente.

Resultados Monitoreo de marca

3. Información Expuesta – Credenciales filtradas

Volumetría por tipo de fuga

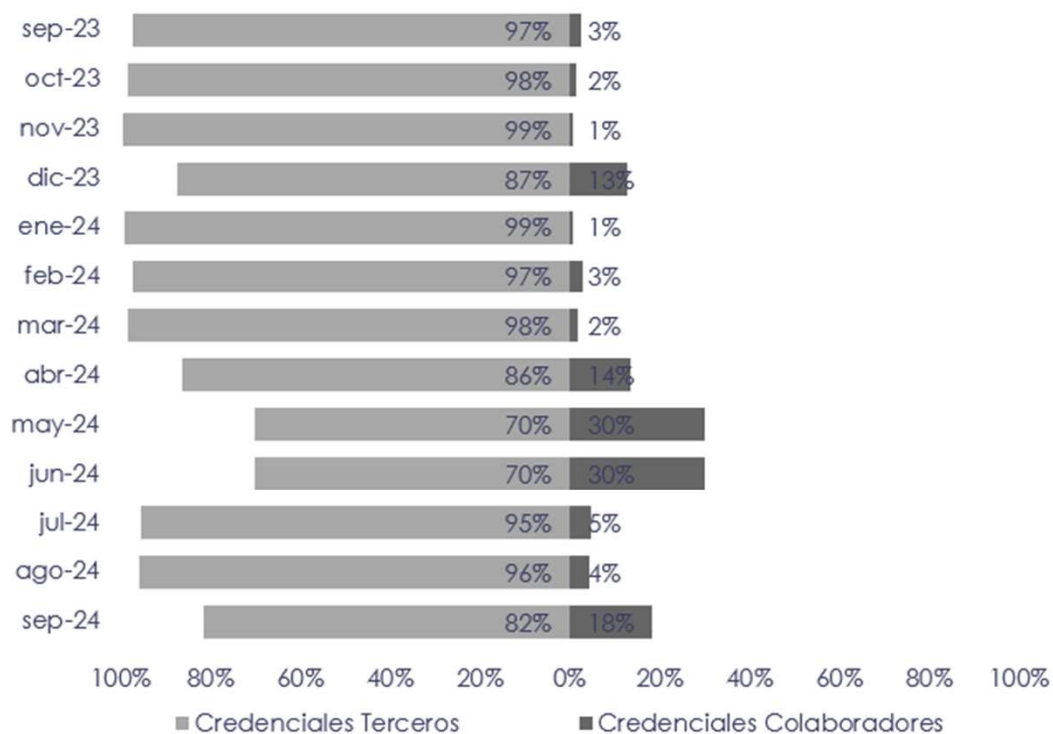
Nº Total de Alertas enviadas: 8



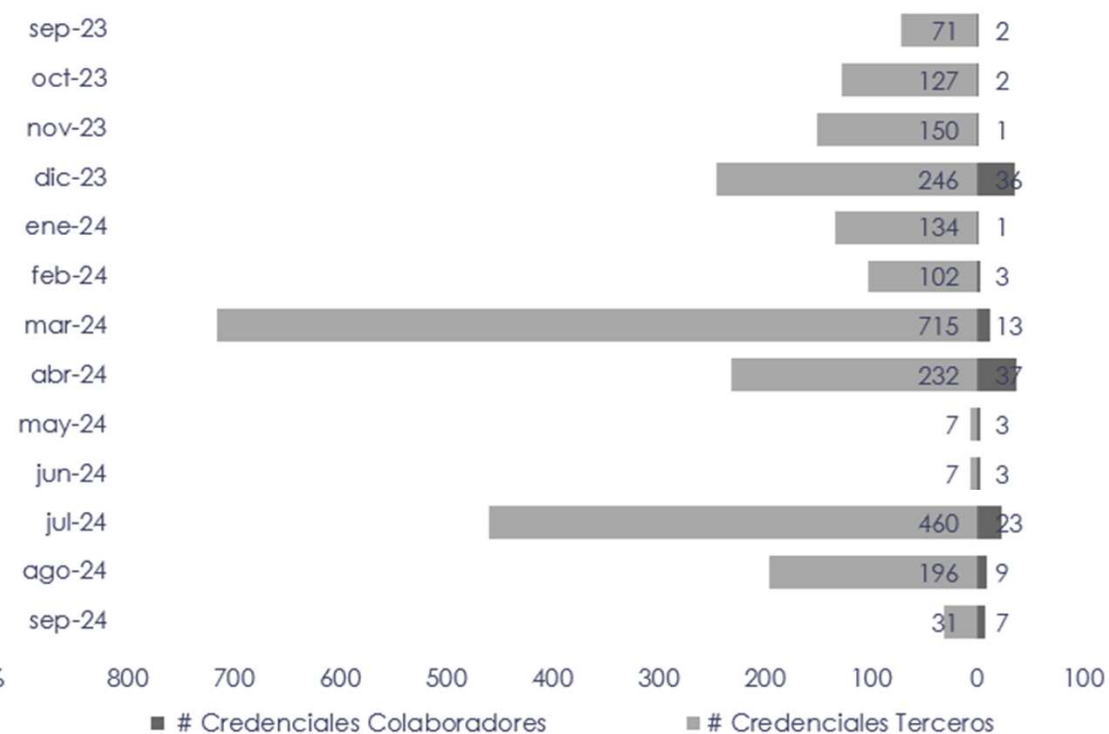
Resultados Monitoreo de marca

Histórico > Evolución del servicio a nivel mensual

% detección terceros VS colaboradores

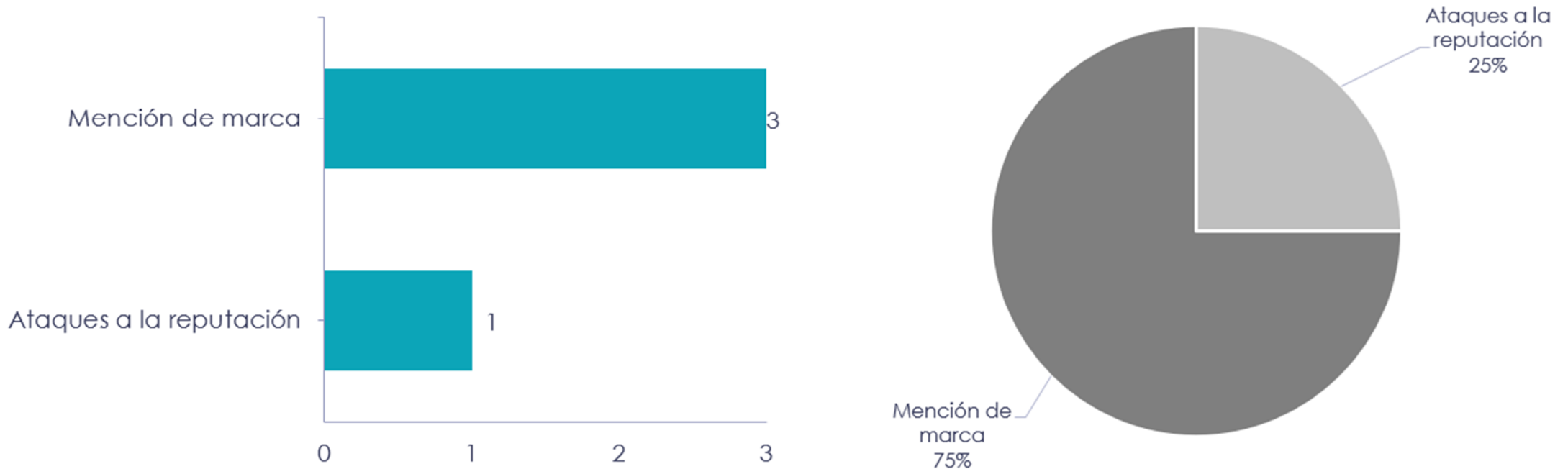


de credenciales identificadas terceros VS colaboradores



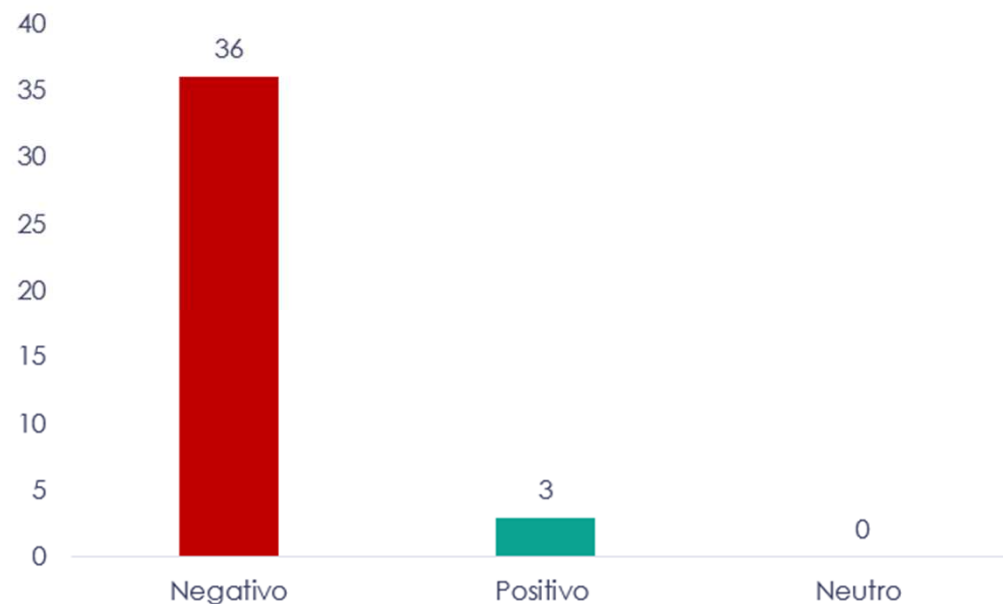
Resultados Monitoreo de marca

4. Menciones de marca



Resultados Monitoreo de marca

5. Percepción general de los eventos presentados



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 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

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 agosto hasta el 21 de septiembre del año 2024.

0

Ethical Hacking

0

Retest Ethical Hacking

4

Retest Análisis de
Vulnerabilidades

3

Análisis de
Vulnerabilidades

0

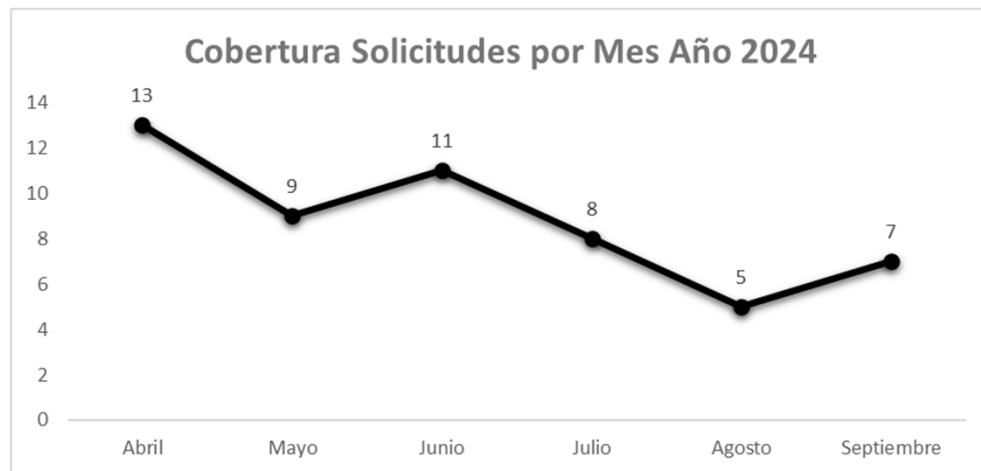
Analisis deCodigo

0

Ingeniería Social

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

Durante el periodo, se documentaron un total de 7 solicitudes. Se evidencia un aumento de 2 solicitudes respecto al periodo anterior, como se ilustra en el gráfico adjunto.



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

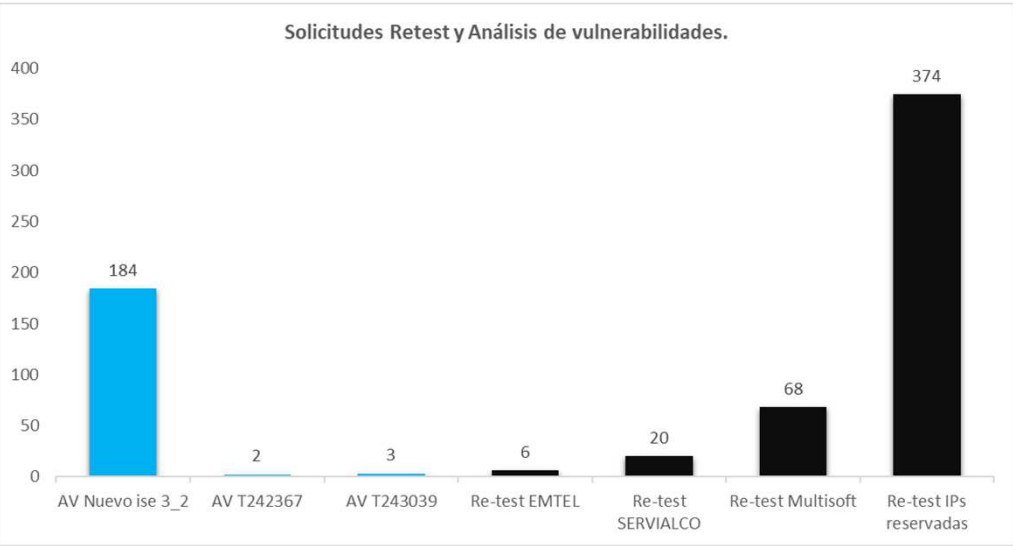


Para el periodo reportado, se ejecutaron 4 solicitudes acerca de Retest referentes a análisis de vulnerabilidades (RAV) 3 análisis de vulnerabilidades (AV).

Resultados de solicitudes (Retest y AV)

Resultados Retest - General

Resultados – De los retest solicitados fueron reportadas **468** vulnerabilidades para su respectivo escaneo y validación. En cuanto a los análisis de vulnerabilidades se identificaron **189** hallazgos. Las actividades se muestran a continuación:



Resultados – A continuación, se muestra el porcentaje por nivel de criticidad de las vulnerabilidades de retest reportada, se organizan desde las más críticas llegando a las bajas.



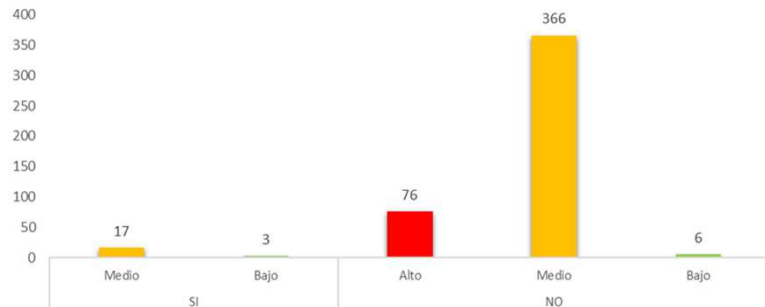
Impacto	Cantidad
Alto	76
Medio	383
Bajo	9
Total	468

Resultados de solicitudes (Retest y AV)

Resultados Retest y Análisis de Vulnerabilidades Remediadas - General

De las **468** vulnerabilidades reportadas en los re-test, **20** fueron remediadas y **448** continúan activas. Se identifican **189** vulnerabilidades nuevas reportadas de los AV. Se recalca que dentro de las vulnerabilidades **remediadas** hay de impacto **medio y bajo**.

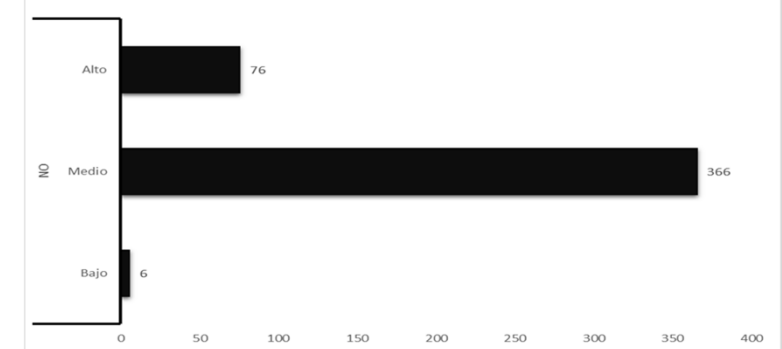
Cantidad de Vulnerabilidades Gestionadas/No Gestionadas



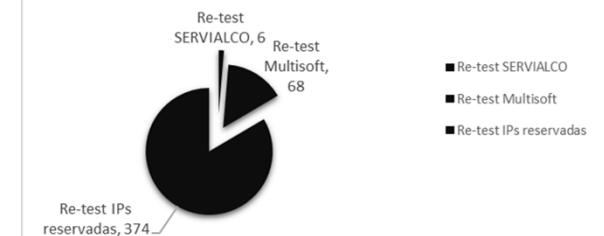
SI	20
Medio	17
Bajo	3
NO	448
Alto	76
Medio	366
Bajo	6
Total	468

En los retest del periodo reportado, se **evidencian** varias **vulnerabilidades** de nivel **altas, medias y bajas** que aún están **activas**.

Vulnerabilidades Activas



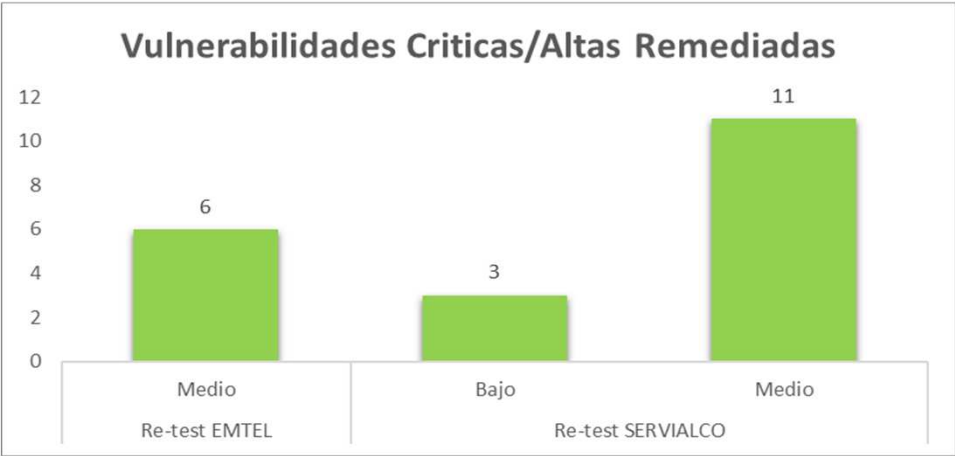
Cantidad de Vulnerabilidades Activas



Resultados de solicitudes (Retest y AV)

Resultados Retest AV Remediadas - General

De las **20** vulnerabilidades remediadas se destaca la efectividad de solución de las críticas y altas.



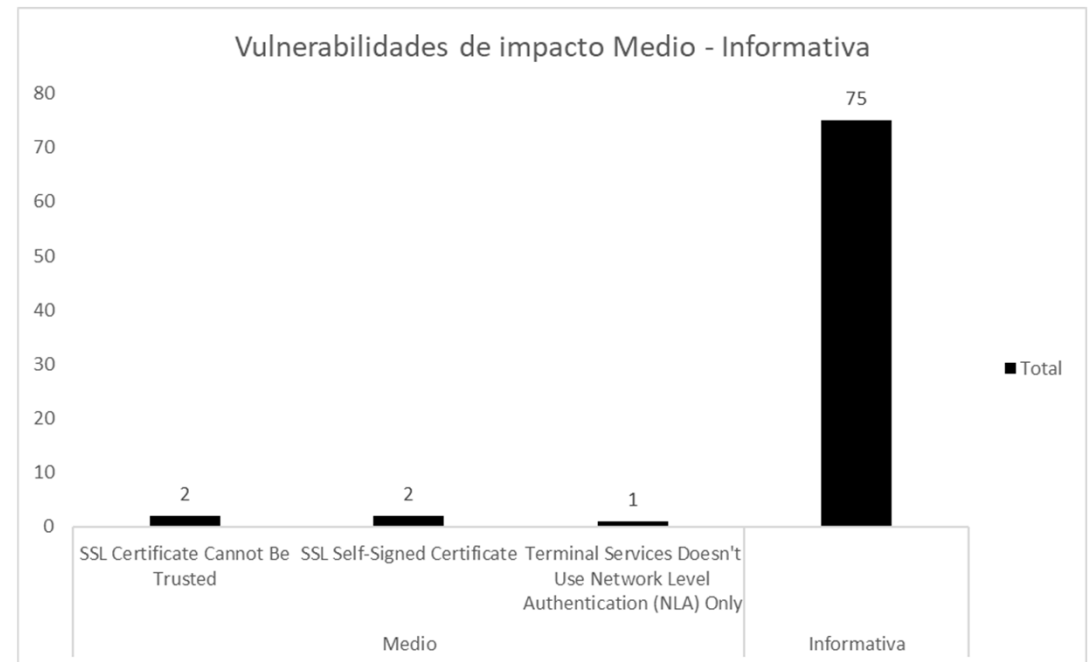
Del total de **vulnerabilidades activas (448)** los activos que se destacan con **más vulnerabilidades** son 172.17.106.191 (**24 vuln**), 172.17.108.235 (**14 vuln**) y 172.17.108.230 (**14 vuln**) los activos identificados como IP reservadas.

Host	Critico	Alto	Medio	Bajo	Total
172.17.106.191	0	4	20	0	24
172.17.108.235	0	2	12	0	14
172.17.108.230	0	2	12	0	14
172.17.105.67	0	2	10	0	12
172.17.105.68	0	2	10	0	12

Resultados de solicitudes Análisis de vulnerabilidades (AV)

Resultados Análisis de vulnerabilidades - General

A continuación se muestra el resultado de los ejercicios realizados en el mes de septiembre, donde se evidencia la cantidad de vulnerabilidades discriminadas por nivel de impacto, así como los hallazgos más relevantes en cuanto a impacto crítico alto y medio.



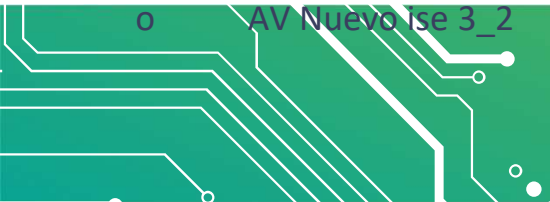
Actividades realizadas

- Se ejecutan los siguientes ejercicios de retest de análisis de vulnerabilidades, los activos pertenecen a los siguientes proveedores encargados de la administración:
 - Re-test Multisoft
 - Re-test IP Reservadas
 - Re-test SERVIALCO
 - Re-test EMTEL
- Se ejecutan los siguientes ejercicios de análisis de vulnerabilidades:
 - ○ AV T242367
 - ○ AV T243039
 - ○ AV Nuevo ise 3_2



Recomendaciones y conclusiones

1. Durante el re-test, se ha observado una disminución significativa en el número total de vulnerabilidades únicas detectadas, pasando de **26** a **17** vulnerabilidades respecto al mes anterior, y con un total de **468** hallazgos que se trataron con los re-test respectivos.
2. Las vulnerabilidades activas que afectan al mayor número de activos están relacionadas con "SSL Certificate Cannot Be Trusted", "SSL Self-Signed Certificate" y " TLS Version 1.0 Protocol Detection", todas con un nivel de impacto medio.
3. Las actividades de re-test de vulnerabilidades se llevaron a cabo en plataformas como, Comware, Servialco, IPs reservadas y Multisoft.
4. Es relevante destacar que las vulnerabilidades identificadas y reportadas durante el análisis son de impacto medio, con 4 clasificadas como de prioridad media y el resto como hallazgos informativos. Esto refleja un compromiso sólido con la seguridad de la empresa, con un enfoque particular en abordar de manera significativa las vulnerabilidades críticas y de alto riesgo.
5. Los escaneos de vulnerabilidades se realizaron bajo las siguientes tareas asignadas en la herramienta service mánager:
 - o AV T242367
 - o AV T243039
 - o AV Nuevo Ise 3_2





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 agosto y el 21 de septiembre.

Objetivos

- Evaluar los controles comprendidos en las 17 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

395

Activos evaluados

0

Activos duplicados

17

Activos sin controles

15

Activos sin conexión en un mes

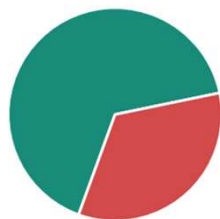
17

Políticas evaluadas

3.136

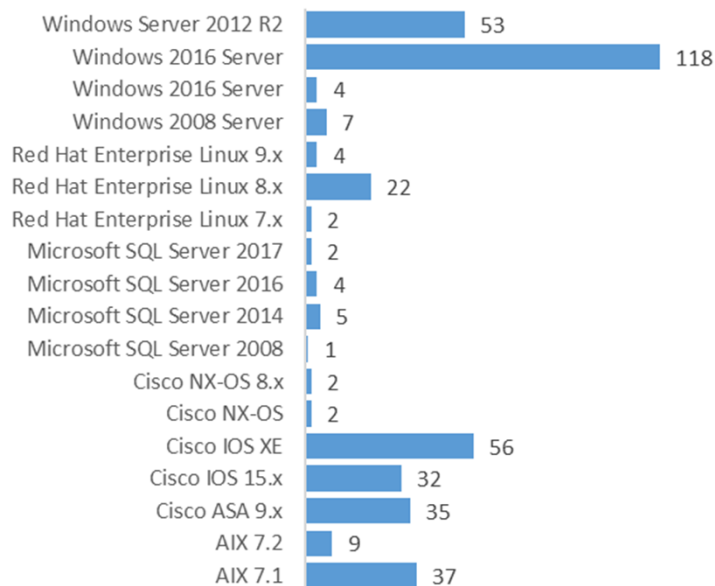
Controles evaluados

66,20%
Controles superados

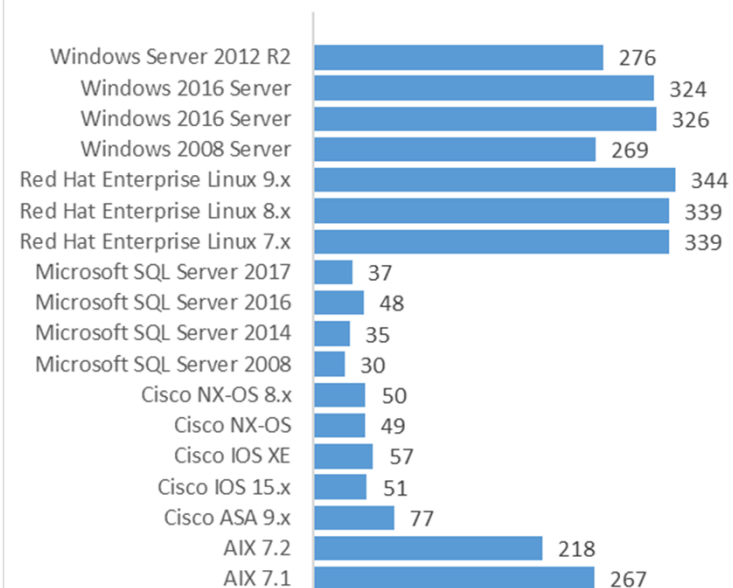


33,80%
Controles fallidos

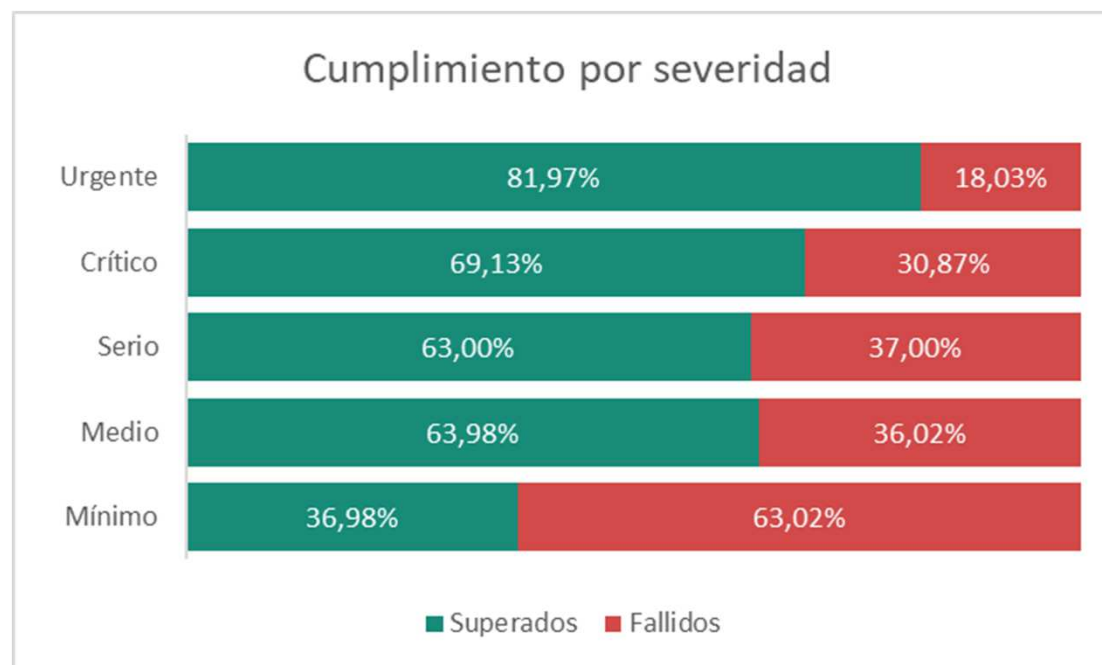
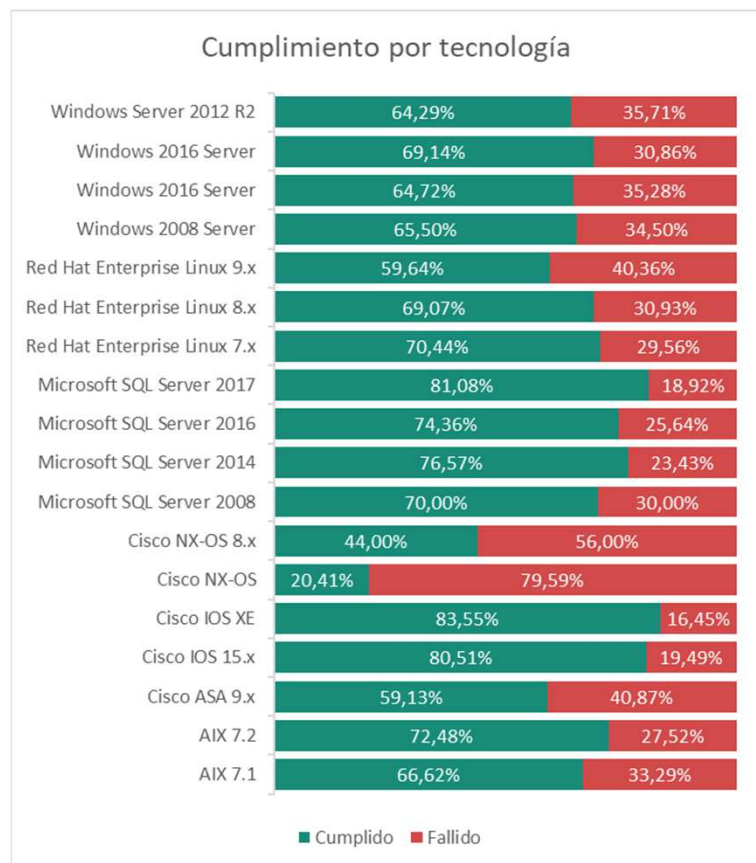
Activos evaluados por tecnología



Controles evaluados por tecnología



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

- La desaparición de la evaluación de dos políticas se debe a que ya no existen sistemas operativos CentOS7 ni RedHat6, estos fueron o dados de baja o migrados a versiones más recientes, esto, según informó el administrador de servidores Linux.
- Actualmente se encuentra con alcance y autenticación a casi todos los dispositivos compartidos por el FNA, a pesar de esto, no todos cuentan con políticas de cumplimiento por parte del COMWARE (192.168.64.249)
- La razón por la que no se había logrado autenticar a las BBDD es porque las IPs y Hostnames compartidos al administrador de la plataforma Qualys no correspondían a los servidores en los que se encontraban las instancias de base de datos sino a los clusters que controlaban dichas instancias
- Cuando en los registros de autenticación de base de datos se pretende el auto descubrimiento de instancias de base de datos y puertos es necesario contar con credenciales de Windows para los mismos activos, esto con el fin de que primero el scanner se autentique como Windows, identifique instancias y puertos y luego con la autenticación de base de datos se apunte directamente a estas instancias-puertos, mencionado lo anterior, hay dos opciones para lograr la autenticación correcta en bases de datos
 - Añadir credenciales de Windows a la plataforma. Requisito, que se compartan credenciales de dominio para la plataforma y que todos los servidores estén en el dominio.
 - Añadir un registro de autenticación por cada combinación host-instancia-puerto existente. Requisito, que cada vez que se cree una nueva instancia se notifique para que un nuevo registro de autenticación sea creado
- La cantidad de controles del CIS y los visualizados en el SCA de Qualys suelen tener diferencias, esto es debido a que el CIS agrupa varias validaciones en un mismo control, mientras que SCA los divide en diferentes controles

GESTIÓN PLATAFORMA – ACTIVIDADES REALIZADAS

1. Se realizó revisión semanal para revisar el estado de los agentes en su etiquetado, duplicidad y última conexión
2. Se identificaron los agentes que llevan más de un mes sin reportar conexión
3. Solicitud información dispositivos de red faltantes, progreso con 192.168.35.130, 192.168.39.130 y 192.168.43.130, pendiente 192.168.64.249
4. Solicitud de instalación Cloud Agent en Windows (**C62893**)
5. Solicitud de instalación Cloud Agent en Linux (**C62010**)
6. Solicitud de información sobre servidores AIX sin reportar en más de un mes
7. Solicitud de información sobre servidores Windows sin reportar en más de un mes
8. identificación de causa de duplicidad de activos, en su mayoría se trató de reinstalaciones o migraciones de OS, estos duplicados fueron eliminados manualmente. En su mayoría AIX y RedHat





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 agosto y el 21 de septiembre.

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 el periodo actual, no se ejecutaron análisis de código.

Integraciones y Automatizaciones (Desarrollos):

- Durante el periodo actual no se realizaron integraciones, estaremos atentos a solicitudes de integración con algún otro proveedor de desarrollo.

Rendimiento y Disponibilidad:

- No hubo ningún tiempo de inactividad planificado ni no planificado, y el rendimiento del sistema se mantuvo dentro de los parámetros normales incluso durante períodos de carga máxima.

Planes para futuras mejoras o actualizaciones:

- Actualmente, hemos actualizado nuestra suite a la última versión estable publicada por el fabricante. A medida que este lance nuevas versiones, realizaremos pruebas de laboratorio para asegurar la estabilidad de cada una. Los plugins de seguridad se actualizan conforme el fabricante publique nuevas versiones.



Gestión y actividades

- **Monitoreo del sistema:**

Se realiza una verificación periódica del estado de cada servidor y los componentes que aloja la suite de Fortify. Hasta el 21 de septiembre, los servidores y la aplicación no han presentado ninguna falla que haya afectado la disponibilidad del servicio.

Fortify Source Code Analyzer (SCA): Actualización de las últimas reglas de análisis y parches de seguridad.

Software Security Center (SSC): Validar funcionamiento y actualizaciones de las políticas de seguridad personalizadas para la ejecución de informes de las aplicaciones auditadas.

Fortify WebInspect Enterprise (WIE): Se valida la integración con el módulo SSC para asegurarse de que no se estén generando errores, y se realiza un monitoreo constante del estado de los escaneos ejecutados.

Fortify WebInspect Sensor (WIS): Se valida el estado del sensor para asegurar la disponibilidad del módulo WebInspect.

- **Gestión de usuarios y permisos:**

-Por medio de la mesa de ayuda se restablecen credenciales usuarios de dominio suite fortify.

En la suite, están configurados los usuarios correspondientes para la administración y ejecución de la suite de Fortify.

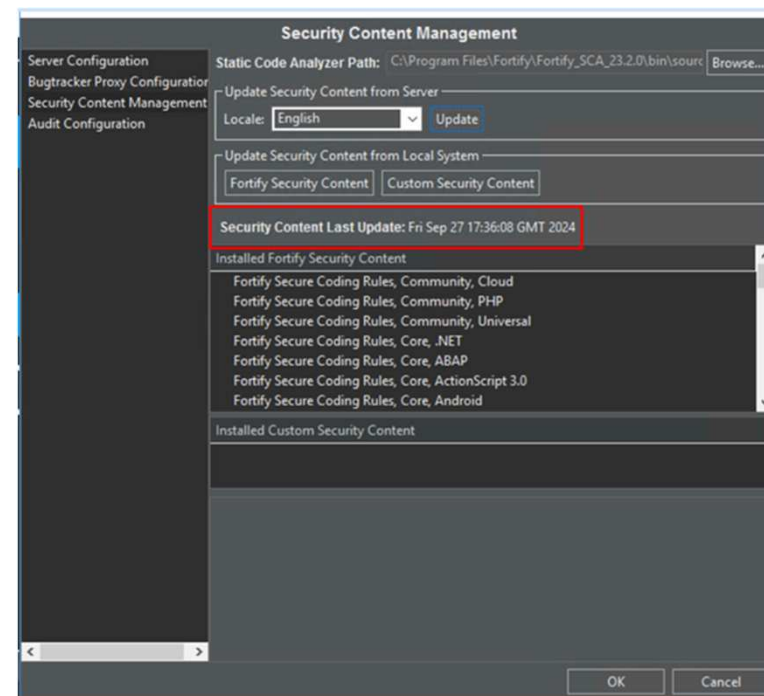


Gestión y actividades

- **Seguimiento de actualización nuevas versiones de Fortify y sus componentes:**

Actualmente, hemos actualizado nuestra suite a la última versión estable publicada por el fabricante. También hemos actualizado el Rulespack de seguridad para realizar un análisis de código más efectivo, detectando las últimas vulnerabilidades existentes.

Name	Type	Latest Version	Programming Language	Locale
☐ Fortify Secure Coding Rules, Community, Cloud	SCA	2024.2.0.0008	configuration	en
☐ Fortify Secure Coding Rules, Community, PHP	SCA	2024.2.0.0008	php	en
☐ Fortify Secure Coding Rules, Community, Universal	SCA	2024.2.0.0008	configuration	en
☐ Fortify Secure Coding Rules, Core, .NET	SCA	2024.2.0.0008	dotnet	en
☐ Fortify Secure Coding Rules, Core, ABAP	SCA	2024.2.0.0008	abap	en
☐ Fortify Secure Coding Rules, Core, ActionScript 3.0	SCA	2024.2.0.0008	actionscript	en
☐ Fortify Secure Coding Rules, Core, Android	SCA	2024.2.0.0008	java	en
☐ Fortify Secure Coding Rules, Core, Annotations	SCA	2024.2.0.0008	java	en
☐ Fortify Secure Coding Rules, Core, Apex	SCA	2024.2.0.0008	apex	en
☐ Fortify Secure Coding Rules, Core, C/C++	SCA	2024.2.0.0008	cpp	en



Actividades realizadas

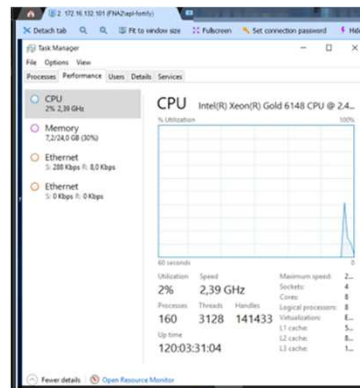
- Restablecer credenciales usuarios de dominio suite fortify.
- Actualización de Rulpacks del modulo SSC.
- Actualización de Rulpacks del modulo Audith WorkBench.



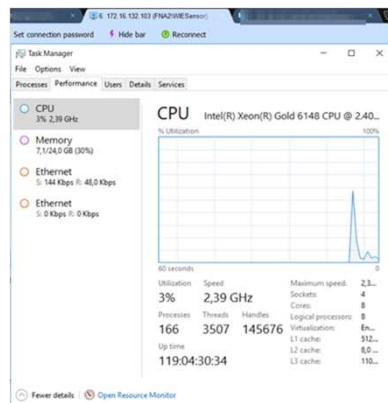
Disponibilidad y rendimiento del sistema.

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

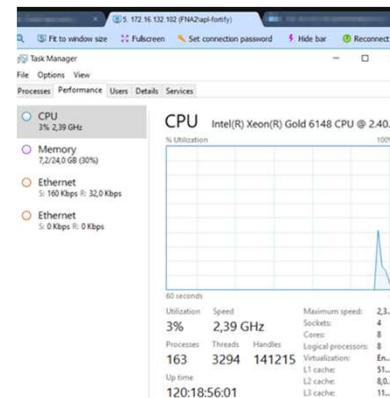
172.16.132.101



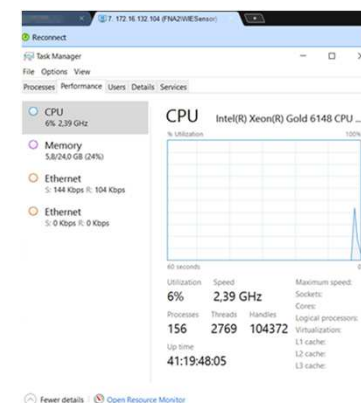
172.16.132.103



172.16.132.102



172.16.132.104



Conclusiones

- Durante el período comprendido, la suite de Fortify ha funcionado correctamente sin experimentar caídas ni fallas. Se ha gestionado el mantenimiento y la actualización de manera constante, asegurando así la disponibilidad de la herramienta cuando se necesite.



Recomendaciones

- Continuar con las actividades de gestión y mantenimiento para garantizar el correcto funcionamiento de la suite de Fortify.
- Priorizar la gestión de copias de seguridad, el control de cambios y la realización de pruebas para garantizar la integridad y disponibilidad de los datos de la nueva suite Fortify.
- Continuar con el monitoreo constante de la suite de Fortify para detectar cualquier anomalía o tendencia inusual que pueda requerir atención.
- Revisar y actualizar regularmente las políticas de seguridad y configuración de Fortify para adaptarse a las necesidades cambiantes del entorno de desarrollo.





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 julio al 21 de agosto 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

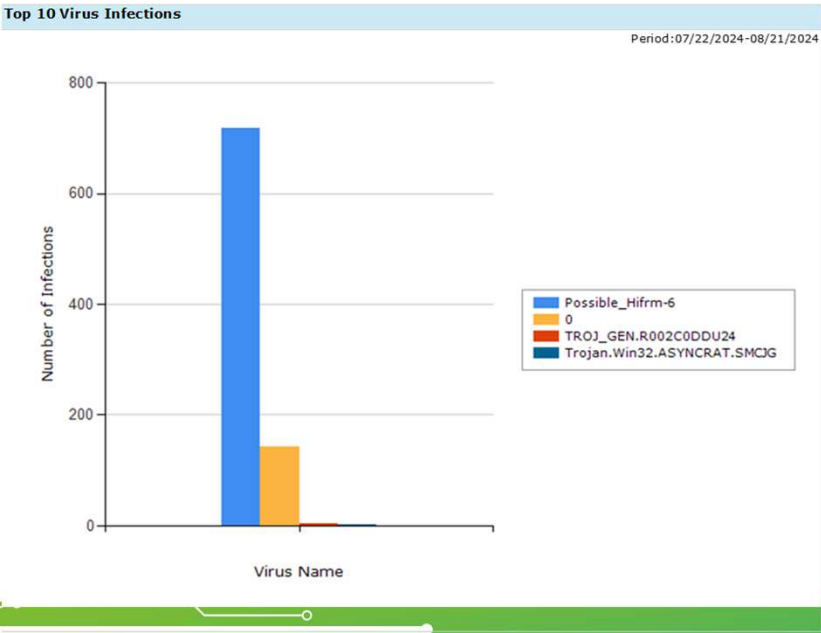
Exponer los eventos identificados y gestión en el servicio de las soluciones antimalware gestionadas por Mnemo Colombia durante el periodo comprendido entre el 22 de julio hasta el 21 de agosto del año 2024.



Estadísticas Generales de detección

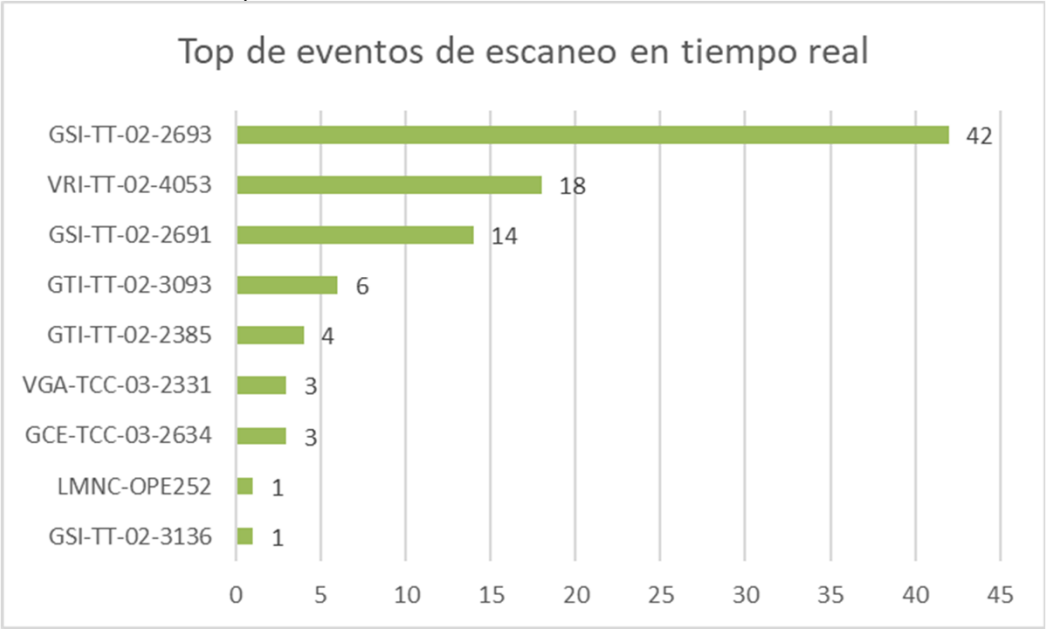
Detecciones en puntos finales Trellix

Se evidencian un total de **864 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 grupo Gre Gestión Humana que genera archivos PDF detectados por la regla.



Top de equipos con mayor cantidad de detecciones

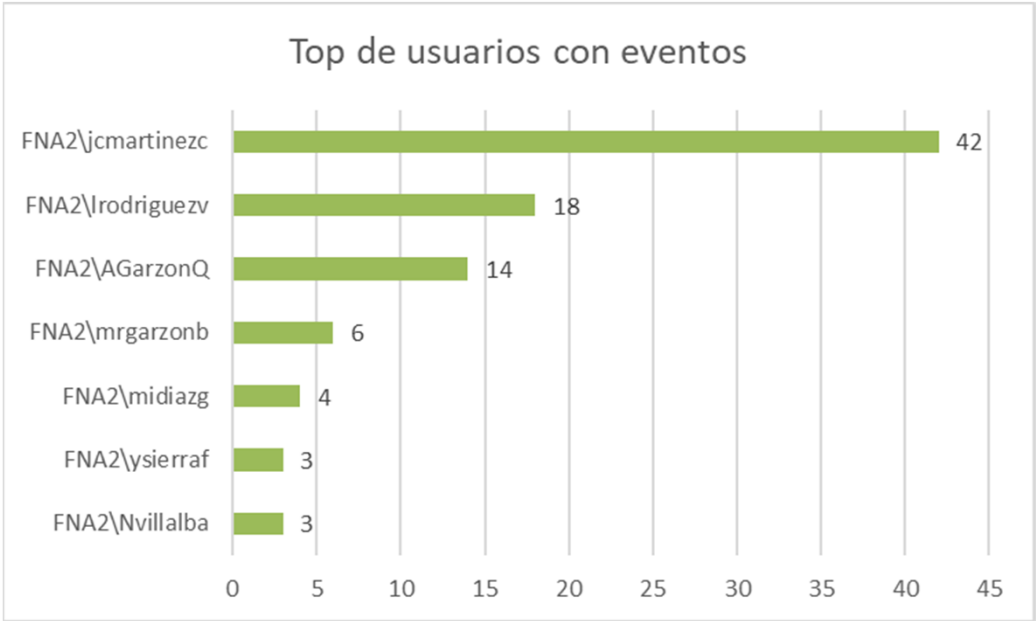
En el top de equipos se encuentra **GSI-TT-02-2693** por archivos posiblemente maliciosos, casi todos en la carpeta de descargas, 13 archivos con el nombre TestDeviceRegConnectivity-main.zip, ejecutados por el usuario Jcmartinezc, estos fueron excluidos ya que hacían parte de pruebas de un aplicativo. El segundo dispositivo con mayor cantidad de registros es **VRI-TT-02-4053** por la misma detección.



Estadísticas Generales de detección

Top de usuarios con mas eventos.

En el top de usuarios se encuentra **jcmartinezc** y **lrodriguezv** relacionado con las mismas detecciones por la ejecución TestDeviceRegConnectivity-main.zip



Behavior Monitoring

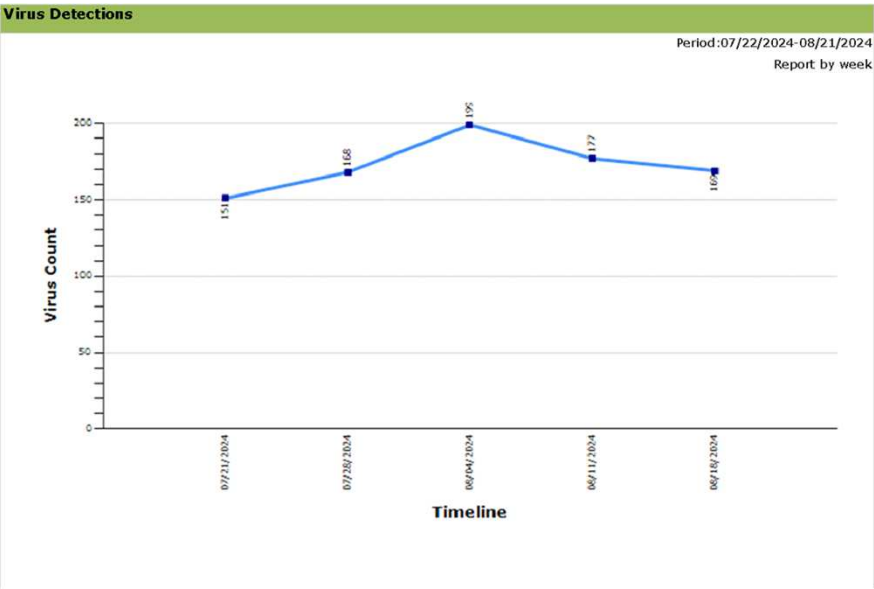
El módulo de Behavior Monitoring monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo el archivo **Ahorro.exe** y **CESENTID.exe** estos se detectaron como archivos adjuntos al correo y se registraron solo como monitoreo.

File	Cuenta de Subject
Newly Encountered Programs	41
C:\Users\aarrieta\Music\TransferWMCapture\setup.exe	1
C:\Compilado_BETA_7\Record_Launcher.exe	2
C:\Soporte\Recursos Capture y Servicio TransferWmCapture V4\TransferWMCapture\setup.exe	2
C:\Compilado_BETA_7\SmartyRecordUploader.exe	3
C:\Compilado_BETA_7\CSPlugins\FFmpeg\x86\ffmpeg.exe	3
C:\Program Files (x86)\GSE\Biometric\Desktop\BiometricDesktop.exe	5
C:\Compilado_BETA_7\SmartyRecorder.exe	7
C:\COBIS\Cesantias\Entidades\CESENTID.exe	8
C:\COBIS\AhorroVoluntario\Ahorro.exe	10
Total general	41

Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta el historial del total de amenazas presentadas por semana, se muestra detección similar para todas las semanas con un pico en la tercera semana para el total de 864 eventos registrados.



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 Gestión Humana con 705 eventos, relacionados con la regla Possible_Hifrm-6 que detectó archivos pdf sospechosos. Dentro de los grupos con mayor cantidad de eventos es Gre de seguridad de la información, por la ejecución de archivos posiblemente maliciosos dentro de los cuales algunos fueron excluidos porque eran archivos de prueba.



Estadísticas Generales de detección

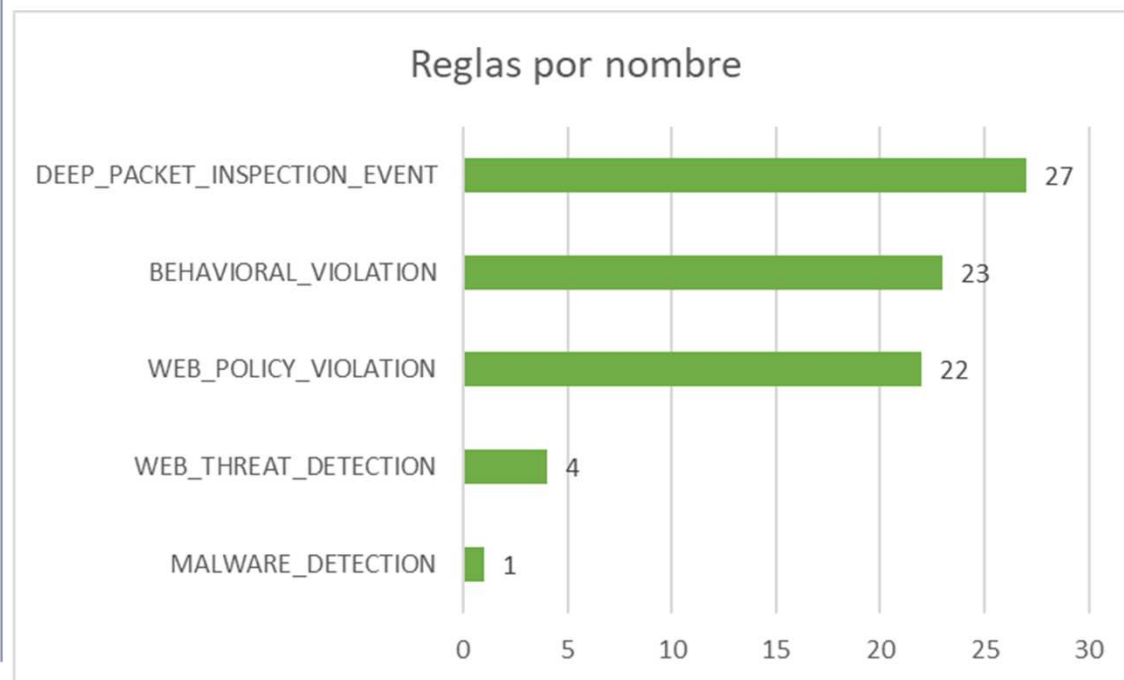
Reglas por nombre

Dentro de las detecciones la mayor cantidad de eventos, se registran en equipos finales con 46 eventos con el módulo de violación de comportamiento.

Etiquetas de fila	Cuenta de eventName
Cloud Email and Collaboration Protection	4
WEB_THREAT_DETECTION	4
Server & Workload Protection	27
DEEP_PACKET_INSPECTION_EVENT	27
Standard Endpoint Protection	46
MALWARE_DETECTION	1
WEB_POLICY_VIOLATION	22
BEHAVIORAL_VIOLATION	23
Total general	77

Eventos por regla de la detección XDR

Dentro del top de eventos de XDR por regla, se identifica la regla de Deep Packet Inspection, esto debido a que se evidencia la siguiente vulnerabilidad Apache Struts2 Remote Code Execution Vulnerability (**CVE-2017-5638**) en los servidores (**BOGPVPPLP001, BOGPVPPLP002 y BOGPVPPLP003**).



Estadísticas Generales de detección

Workbench Events

Dentro de las alertas de Workbench se evidencian un total de 10 alertas, la mayoría con la modificación de los binarios de la herramienta de conexión ssh plink, seguido de intentos para elevar privilegios eludiendo los controles de UAC

Alert View



Score	Workbench ID	Model	Model severity	Impact scope	Data source / processor	Created
78	WB-35600-20240820-00001	[Heuristic Attribute] Possible OS Credential Dumping	High	1 1	Endpoint Sensor	2024-08-20 12:50:34
63	WB-35600-20240730-00002	[Heuristic Attribute] Possible Abuse Elevation Control Mechanism	High	1 1 1	Endpoint Sensor	2024-07-30 12:44:13
63	WB-35600-20240730-00001	[Heuristic Attribute] Possible Abuse Elevation Control Mechanism	High	1 1 1	Endpoint Sensor	2024-07-30 12:44:47
62	WB-35600-20240805-00003	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-08-05 07:01:37
62	WB-35600-20240723-00005	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-07-23 16:33:53
62	WB-35600-20240805-00002	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-08-04 20:26:25
62	WB-35600-20240804-00000	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-08-04 13:45:57
62	WB-35600-20240803-00000	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-08-03 17:36:13
62	WB-35600-20240801-00002	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-08-01 15:59:02
62	WB-35600-20240730-00000	Execution of Renamed Plink	High	1 1	Endpoint Sensor	2024-07-30 10:09:17

Incidentes XDR.

Se registran 9 incidentes n XDR relacionados principalmente con intento de desinstalación de antivirus y uso de webutil por parte de Ccleaner, eventos relacionados con tareas ejecutadas por parte de soporte en sitio con el usuario FNAUSRA

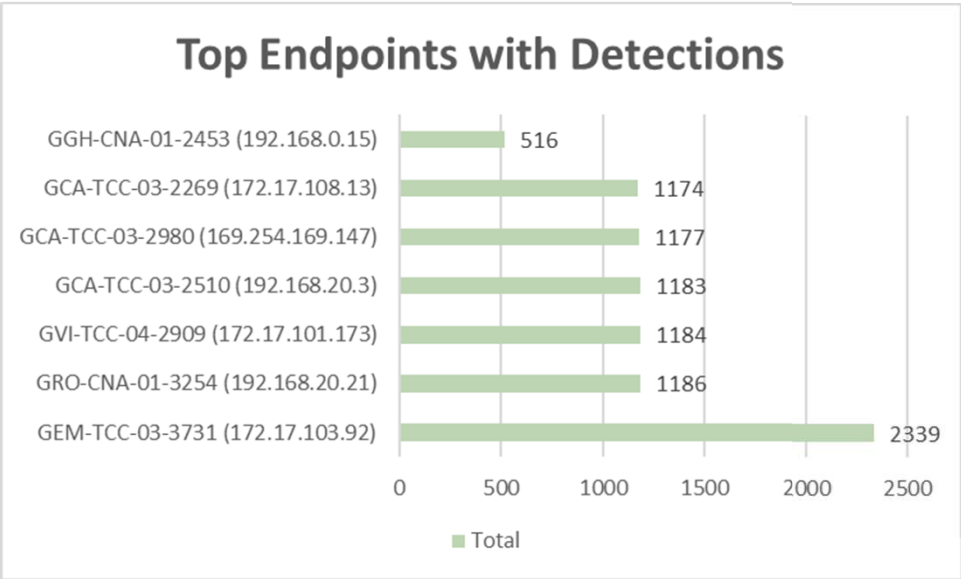
Incident View

Score	Incident ID	Incident name	Last updated	Associated alerts	Impact scope	Created
81	IC-35600-20240730-00000	[Heuristic Attribute] Possible Abuse Elevation Control Mechanism	2024-07-30 12:44:52 (New alert correlated)	2 (Active:2)	2 2 1	2024-07-30 12:41:20
78	IC-35600-20240801-00001	Detection avoidance by Hide Artifacts	2024-08-05 15:37:59 (New alert correlated)	9 (Active:9)	1 1	2024-08-01 15:57:08
70	IC-35600-20240820-00000	System-Defined Event Logs Cleared via Webutil (14)	2024-08-20 14:08:30 (New alert correlated)	14 (Active:14)	14 14	2024-08-20 15:48:01
58	IC-35600-20240808-00000	System-Defined Event Logs Cleared via Webutil (4)	2024-08-13 11:32:07 (New alert correlated)	4 (Active:4)	4 4	2024-08-08 12:29:27
56	IC-35600-20240723-00000	Possible Disabling of Antivirus Software (6)	2024-07-30 13:05:01 (New alert correlated)	6 (Active:6)	1 1	2024-07-22 22:42:56
47	IC-35600-20240806-00000	Possible Disabling of Antivirus Software (3)	2024-08-06 12:27:39 (New alert correlated)	3 (Active:3)	1 1	2024-08-06 11:19:21
44	IC-35600-20240725-00000	Possible Disabling of Antivirus Software (2)	2024-07-24 20:17:31 (New alert correlated)	2 (Active:2)	1 1	2024-07-24 20:15:33
39	IC-35600-20240813-00000	Possible Disabling of Antivirus Software (2)	2024-08-13 13:59:14 (New alert correlated)	2 (Active:2)	2 2	2024-08-13 13:57:15
34	IC-35600-20240801-00000	Possible Disabling of Antivirus Software (2)	2024-08-01 11:02:47 (New alert correlated)	2 (Active:2)	2 2	2024-08-01 11:00:55

Estadísticas Generales de detección

Top de equipos con detecciones

En el top de equipo con detecciones por XDR se encuentra el equipo GEM-TCC-03-3731 y GRO-CNA-01-3254 esto debido al uso de Ccleaner.exe, que por sus utilidades se reconoce como posiblemente malicioso.



Peticiones por país

En los países con mayor cantidad de peticiones adicional a Colombia es Estados unidos.

Location	Users	Devices
Colombia - Bogotá	2451	2
Colombia - Medellin	1684	1197
Colombia - La Trinidad	1620	1093
Colombia - Santa Fe	1505	8
Colombia - Calderon Tejada	1006	2
Colombia - Bogota	889	86
United States - Boydtton	726	0
United States - Washington	527	0
United States - San Antonio	256	0
United States - Des Moines	207	0

Imagen de detección IC-35600-20240711-00000 Execution of Renamed Plink

Estadísticas Generales de detección

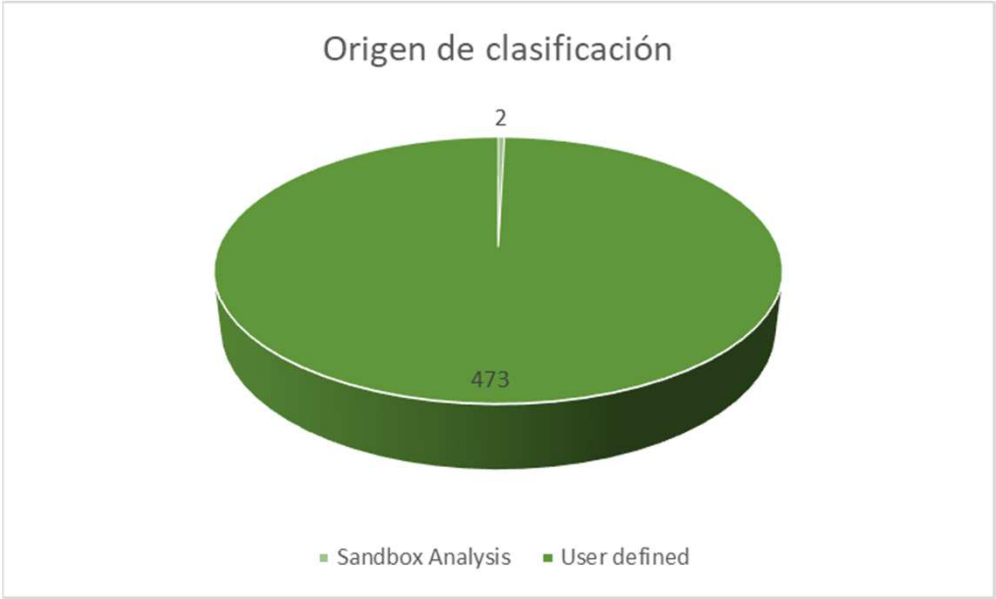
Eventos Servidores

Se registran 21 eventos en servidores, el **85%** por el servidor FNABOGAPP009, esto por el siguiente archivo **E:\aplicaciones\FnaCargueAportes\FnaCargeAportesWindowsService.exe**, como evento de monitoreo.

%	Computer	Malware
(85.7%)	FNABOGAPP009	HEU_AEGIS_CRYPT
(9.5%)	FNABOGAPP015	Possible_Hifrm-6
(4.8%)	FNABOGBZG	HEU_AEGIS_CRYPT

Threat Intelligent

Durante el periodo de **22 de julio al 21 de agosto del 2024** se adicionan **475** reputaciones nuevas la mayoría, gracias a la integración de Threat Q que automáticamente carga los IOC a Vision One, otras adicionadas por el análisis de sandbox.

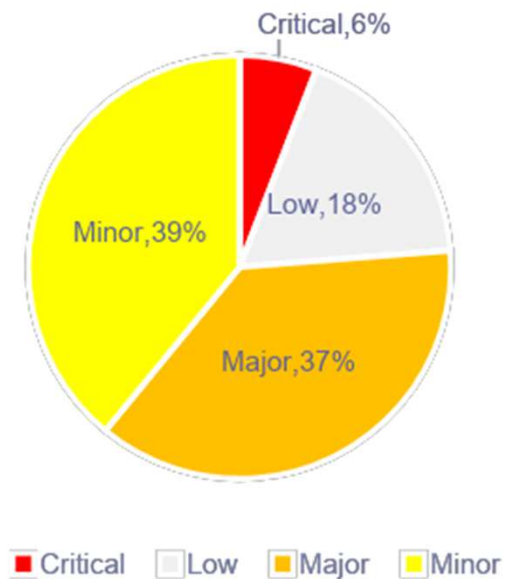


Estadísticas Generales de detección

IPS Eventos por clasificación

Durante el periodo analizado del periodo de **22 de julio al 21 de agosto** del 2024 , se encuentra el siguiente TOP de Eventos identificados por el IPS. Del total de los **116134** eventos, en su mayoría con clasificación menor con el **39 %** de los eventos

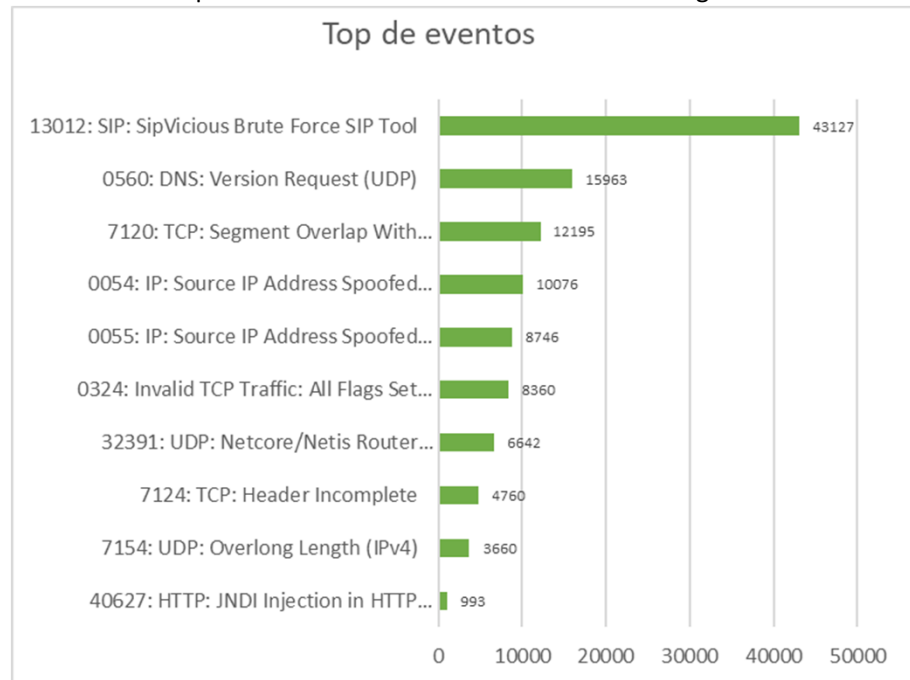
Top de eventos por criticidad



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 **43127** eventos 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.

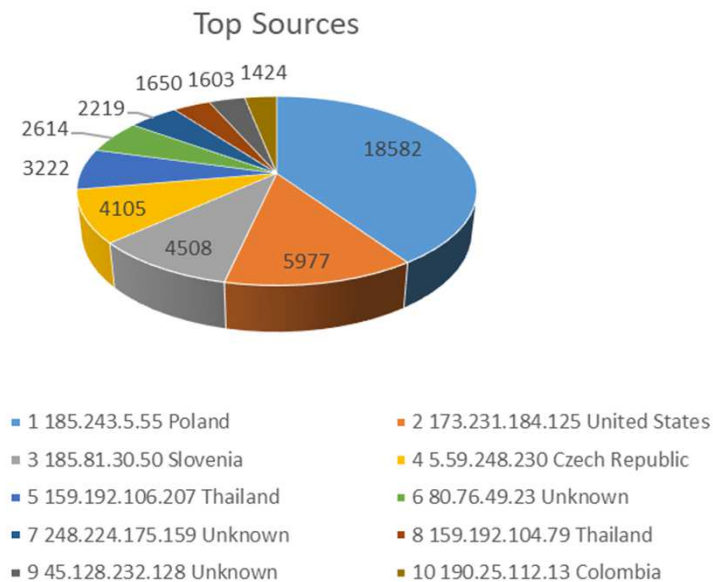
Top de eventos



Estadísticas Generales de detección

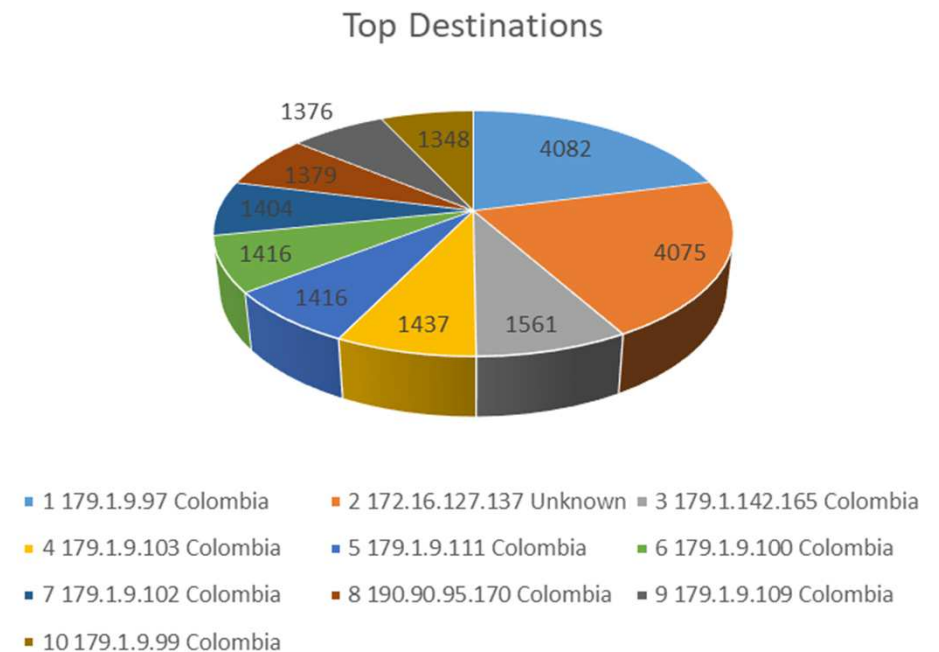
Top de origen de ataques

A continuación, se muestra el top de IP de origen 185.243.5.55 de Polonia con 18582 eventos.



Top de destino de ataques

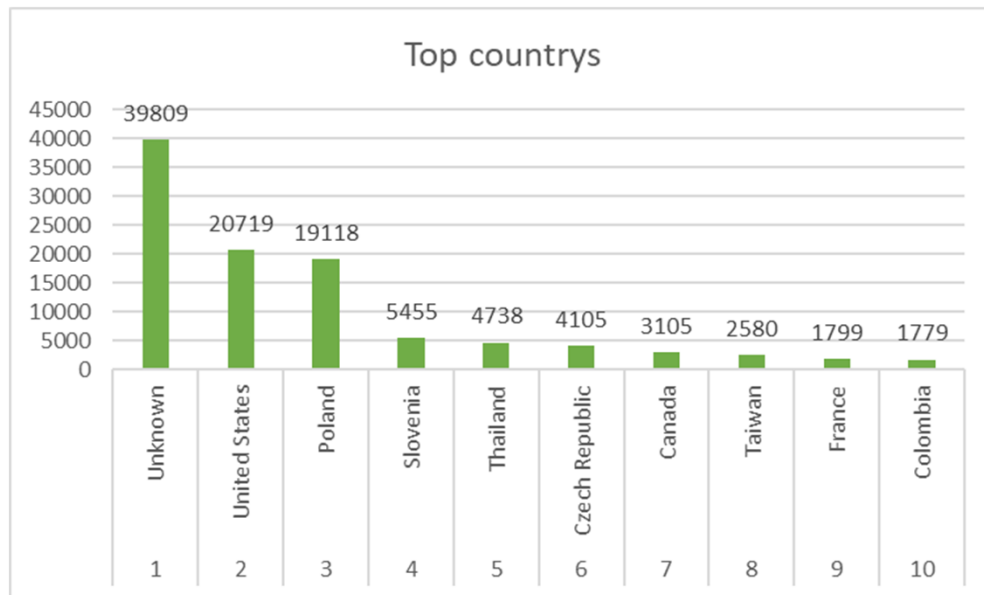
En el top de destinos está el equipo 179.1.9.97



Estadísticas Generales de detección

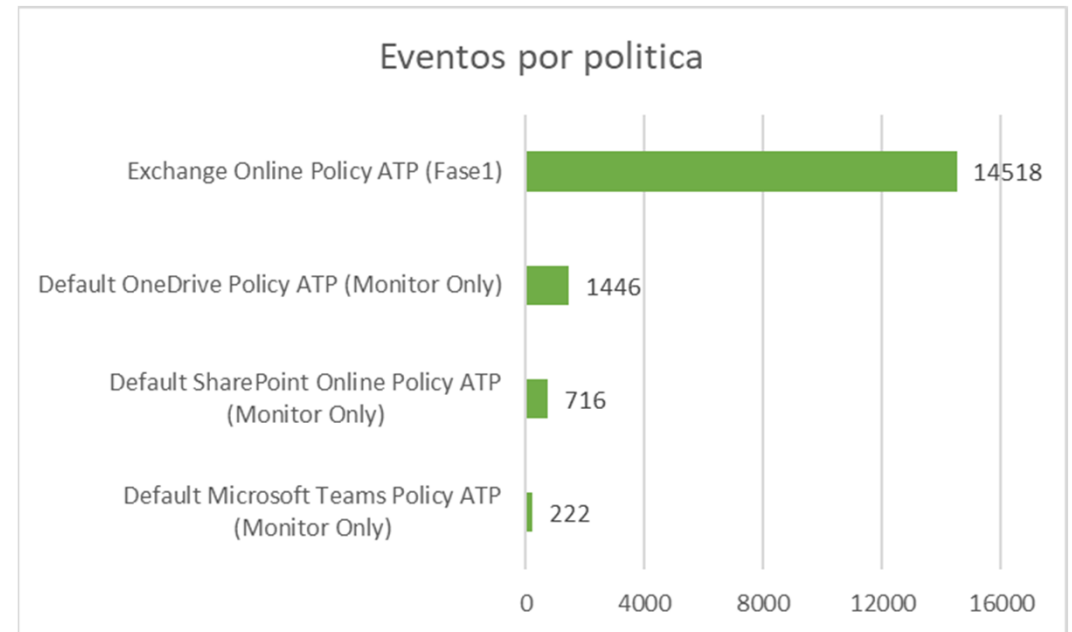
Top de países detectados por IPS

En el top de eventos por país, se encuentra Estados Unidos con mayor cantidad de registros, seguido de Polonia y Eslovenia.



Top de eventos por política CASB

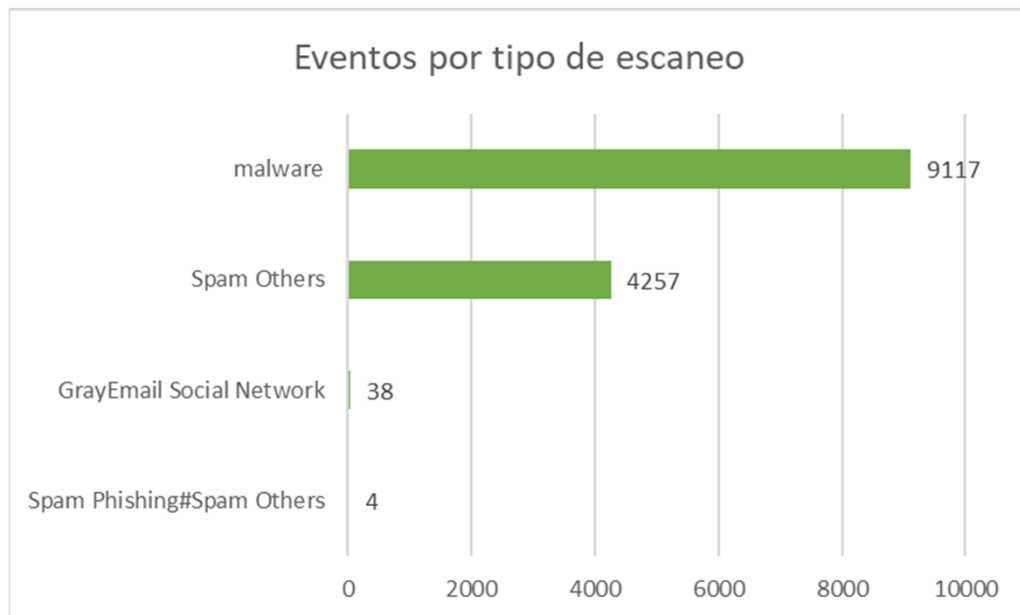
Para el periodo **de 22 de julio al 21 de agosto del 2024** se presentaron un total de **16902** eventos registrados por la solución CASB, la política que tiene mayor cantidad de eventos es Exchange policy encargada de validar eventos maliciosos en correo.



Estadísticas Generales de detección

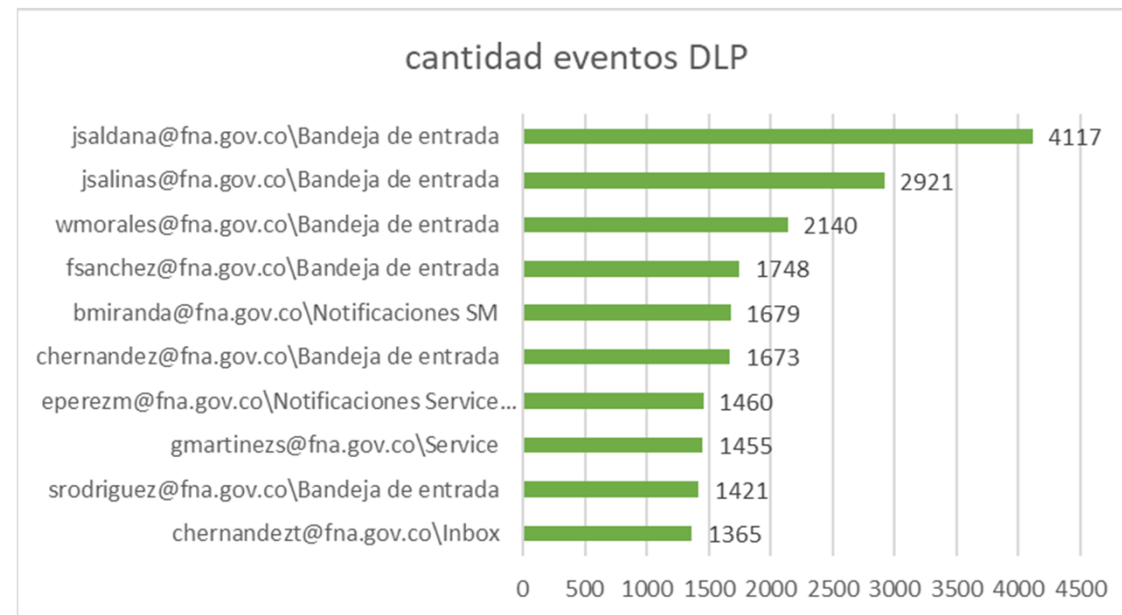
Top de eventos por regla.

Dentro de los eventos la mayoría corresponden eventos de malware, seguido de correos de spam.



Top de usuarios de DLP

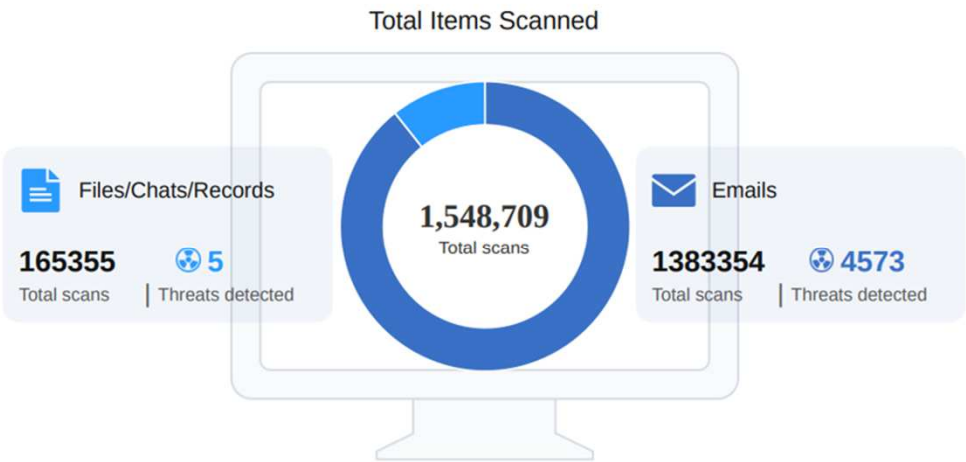
En el top de usuarios con mayor cantidad de eventos es jsaldana@fna.gov.co con 4117, esto debido a la detección de la regla de Database Analíticas y reglas de protección de Exchange Online.



Estadísticas Generales de detección

Detecciones de seguridad

Durante el periodo se realizó un total de 1.548.709 escaneos, se realizó 165.355 escaneos a archivos chats y grabaciones con 5 amenazas detectadas. Para correos se realizó escaneo de 1.383.354 con 4573 amenazas detectadas.



Filtros de detección.

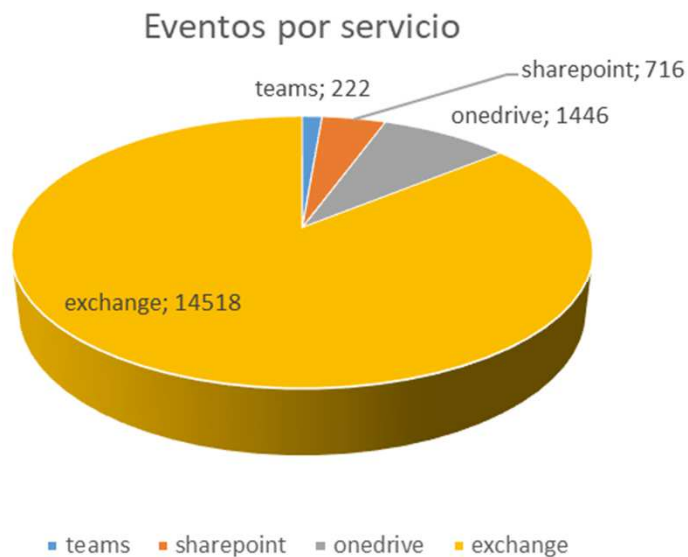
En las detecciones los objetos, que mayor cantidad de registros genera por políticas de seguridad son adjuntos, seguido de archivos maliciosos dentro del cuerpo del correo y archivos.

Etiquetas de fila	Cuenta de objectType
attachment	9117
malware	9117
email	4420
GrayEmail Social Network	38
Spam Others	4257
Spam Phishing#Spam Others	4
(en blanco)	121
FILE	3365
(en blanco)	3365
Total general	16902

Estadísticas Generales de detección

Top de eventos por servicio.

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



Top de usuarios de amenaza

En el top de cuentas que mayor cantidad de eventos genera, es la cuenta de servicio crojas@fna.gov.co, con 423 eventos, esto debido a correos de spam. El usuario yriano@fna.gov.co tiene detecciones en su mayoría por correos maliciosos o spam.

Top 5 Recipients with Spam Email Messages	
User	#
crojas@fna.gov.co	423
yriano@fna.gov.co	124
comercial@fna.gov.co	111
deraso@fna.gov.co	71
contactenos@fna.gov.co	68

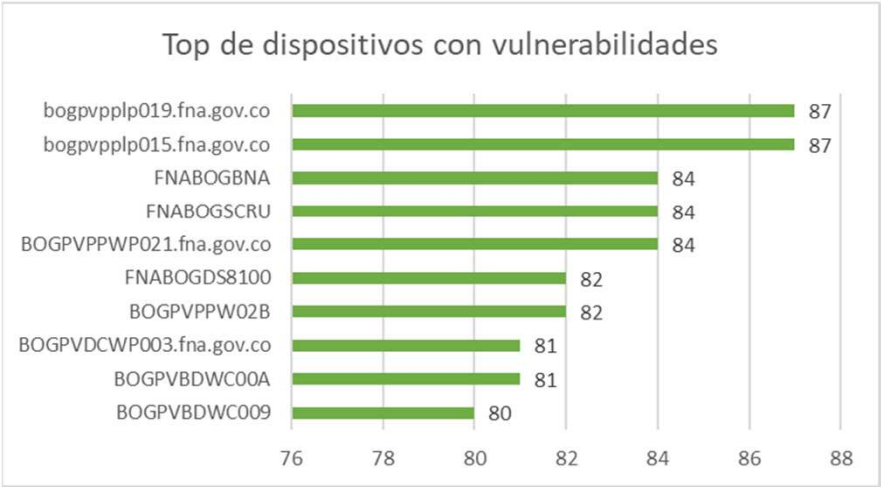
Estadísticas Generales de detección

Attack Surface Discovery

Attack Surface Discovery permite localizar activos corporativos que los actores de amenazas podrían utilizar para atacar la organización. Cada sección de la aplicación Attack Surface Discovery proporciona información sobre un tipo de activo dentro de su organización.

En el top de eventos, se registra los servidores bogvpplp015 y bogvpplp019, con mas de 35 vulnerabilidades con clasificación alta

El número en la gráfica indica la clasificación, entre más cerca al 100 más alta es.



Internet Facing Assets

Muestra todos los activos de dominio y IP descubiertos que son visibles desde ubicaciones externas de Internet y le permite ver evaluaciones detalladas de riesgos del perfil de IP. A continuación se ve la lista de los dominios y su clasificación, que en este caso no se observa ninguna clasificación alta.

Clasificación de sitios FNA	
Host	Asset Risk
chatbotcobranzas.fna.gov.co	44
autodiscover.fna.gov.co	46
agendamiento.fna.gov.co	49
natazure.fna.gov.co	49
fna.gov.co	53
www.fna.gov.co	53
denuncias.fna.gov.co	53
documentos.fna.gov.co	53
info.fna.gov.co	53

Estadísticas Generales de detección

Internet Facing Assets

A continuación se ve la lista de direcciones IPS públicas y su clasificación, ninguna con clasificación alta.

Public IPs	Asset risk score	Host count	Host list	Location
179.1.9.97	53	5	denuncias.fna.gov.co documentos.fna.gov.co info.fna.gov.co fna.gov.co www.fna.gov.co	Colombia
179.1.96.64	53	2	www.fna.gov.co fna.gov.co	Colombia
190.90.95.186	49	1	natazure.fna.gov.co	Colombia
198.251.66.104	49	1	agendamiento.fna.gov.co	United States
34.226.4.94	44	1	chatbotcobranzas.fna.gov.co	United States

Cuentas

A continuación se muestra el top de cuentas identificadas por Trend Micro

User account	Asset risk score
Admin 365	64
Backup	63
Administración Exchange	63
Brayan Fernando Calderon Cristancho - Soft IG	61
Milena Rocio Garzon Barragan	61
ADMIN365	61
AGarzonQ	60
ad 365	60
Fondonal	60



Estadísticas Generales de detección

Cuentas

Para la cuenta de Admin 365 con mayor clasificación se evidencia que se clasifica con riesgo alto, por que tiene bastantes permisos sobre la cuenta y porque tiene deshabilitada la opción de que la contraseña expire, entre otras vulnerabilidades.

☐	Risk factor	Risk event	Data source / processor	Event risk level
☐	>  System configuration	Stale On-Premises AD Account	Microsoft Entra ID	Medium
☐	>  System configuration	Stale Microsoft Entra ID Account	Microsoft Entra ID	Medium
☐	>  System configuration	Excessive Synced On-Premises AD Administrator Account	Microsoft Entra ID	Medium
☐	>  System configuration	Excessive Highly-Privileged On-Premises AD Account	Microsoft Entra ID	Medium
☐	>  System configuration	On-Premises AD Account with Weak Sign-In Security Policy - Password Expiration Disabled	Microsoft Entra ID	Medium
☐	>  System configuration	Account with a Privileged Group ID	Active Directory (on-premises)	Medium

Cloud Apps

A continuación se muestra la lista de aplicaciones con clasificación media encontradas por Trend Micro, por el módulo Attack Surface Discovery, no se encuentran aplicaciones con clasificación alta.

Cloud app	Category	Risk level	Users	Devices	Visits
Avast	IT Security	Medium	6	6	3195
diagrams.net	Design & Creativity Development Tools	Medium	3	3	329
Opera	Content Management IT Services & Support	Medium	3	3	224
Citrix GoToMeeting	Communications Education	Medium	3	3	151
Jetbrains	Development Tools	Medium	5	5	59
WeTransfer	Cloud Sharing & Storage Knowledge Management	Medium	7	7	44
University of Waterloo	Online Service	Medium	1	1	27
PyPI	Development Tools	Medium	4	4	16
RStudio	Development Tools	Medium	3	3	14
Smallpdf	Collaboration	Medium	6	6	12
Flaticon	Online Service	Medium	1	1	11
Coupa	Business Process Management Finance & Accounting	Medium	2	2	11
Anaconda Cloud	Development Tools	Medium	5	5	11

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.

- Se realiza adición de exclusiones para servidores Linux
- como parte de las políticas de protección contra el uso de dispositivos no autorizados, se crea cambió y se formaliza GPO para el bloqueo de dispositivos externos incluyendo Micro SD, por medio del Directorio Activo.
- Se realiza activación de políticas de bloqueo en web control para servidores.
- Depuración Usuarios Ambientes Productivos _ No Productivos usuario MFER, se realiza eliminación por parte de admin Linux de usuario McAfee.
- permisos para la ejecución de *\TestDeviceRegConnectivity-main.zip, aplicación de prueba del Grupo de seguridad de la información
- Adición de exclusión para dispositivos en política de Behavior monitoring para dispositivos biométricos y para aplicación de monitoreo de videollamada.
- validación alerta SOC 125113 intentos de desinstalación antivirus
- validación de eventos de posible escaneo por puerto 22 en IPS, se realiza activación de bloqueo en la regla de IPS
- validación evento uso Ccleaner alerta WB-35600-20240826-00000, uso de esta herramienta por parte de soporte en sitio
- Se recomienda realizar la mitigación de la vulnerabilidad Apache Struts2 Remote Code Execution Vulnerability (CVE-2017-5638) realizando la actualización de apache en los servidores BOGPVPPLP001,BOGPVPPLP002 y BOGPVPPLP003
- El módulo de Attack Surface Discovery detectó los equipos bogvpvplp015 y bogvpvplp019 con clasificación alta por tener más de 35 vulnerabilidades.
- No se identifican dominios ni ips con clasificación alta por parte Attack Surface Discovery
- Las cuentas Admin 365 y Backup son las cuentas con clasificación de riesgo alto debido a los permisos asignados y la desactivación del vencimiento de la contraseña.



- El escaneo programado, es el que mayor cantidad de eventos registra con 772, luego con 92 eventos los escaneos en tiempo real.
- Se evidencian un total de 864 eventos de amenazas gestionados por Trend Micro
- En XDR los eventos con mayor cantidad de registros están relacionados con la herramienta de CCleaner
- El ips registra un total de 116134 eventos para el periodo del informe.
- se recomienda validar la lista de aplicaciones no permitidas, para alimentar la base de aplicaciones restringidas.
- se continua con la validación de reglas de las diferentes soluciones de Trend Micro, con el fin de optimizar las políticas, activando las reglas recomendadas de acuerdo a las mejores prácticas.
- Se realiza depuración de los dispositivos sin comunicación en los últimos meses, versiones de productos se encuentran en su mayoría cerca al 100 %
- Se realizaron análisis de sandbox, sobre los archivos mediante peticiones por correo, sin IOC activas para ninguna de las muestras
- Se agregaron las exclusiones para la solución de Device Control.
- 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 1987 hasta el momento del informe.
- Se mitigaron los 864 eventos presentados en los equipos final y 21 eventos de bloqueo en servidores.
- El IPS analizó 116134 eventos de los cuales 39% fueron categorizados con severidad menor.
- 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

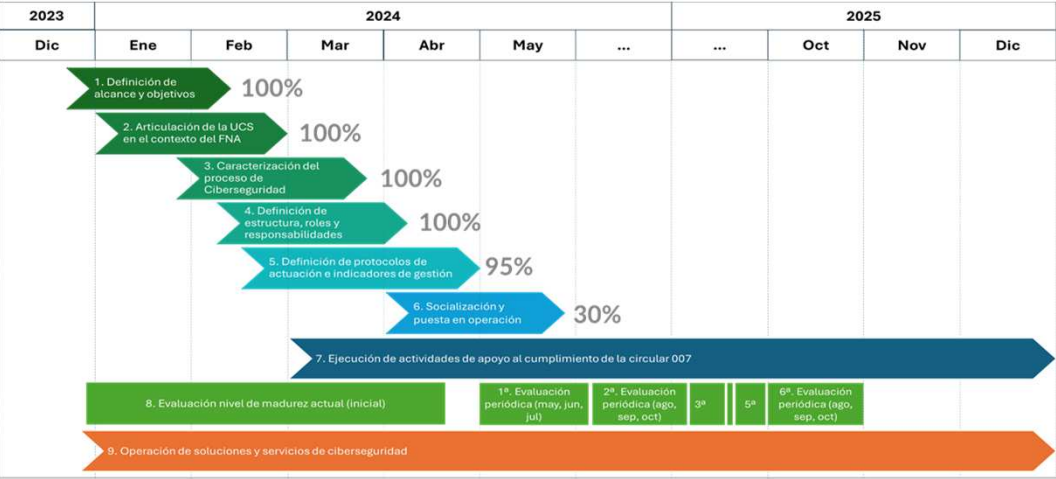
Presentar las principales actividades realizadas para la implementación de la unidad de ciberseguridad en el FNA indicando su estado actual y pasos a seguir.

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 realiza 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.



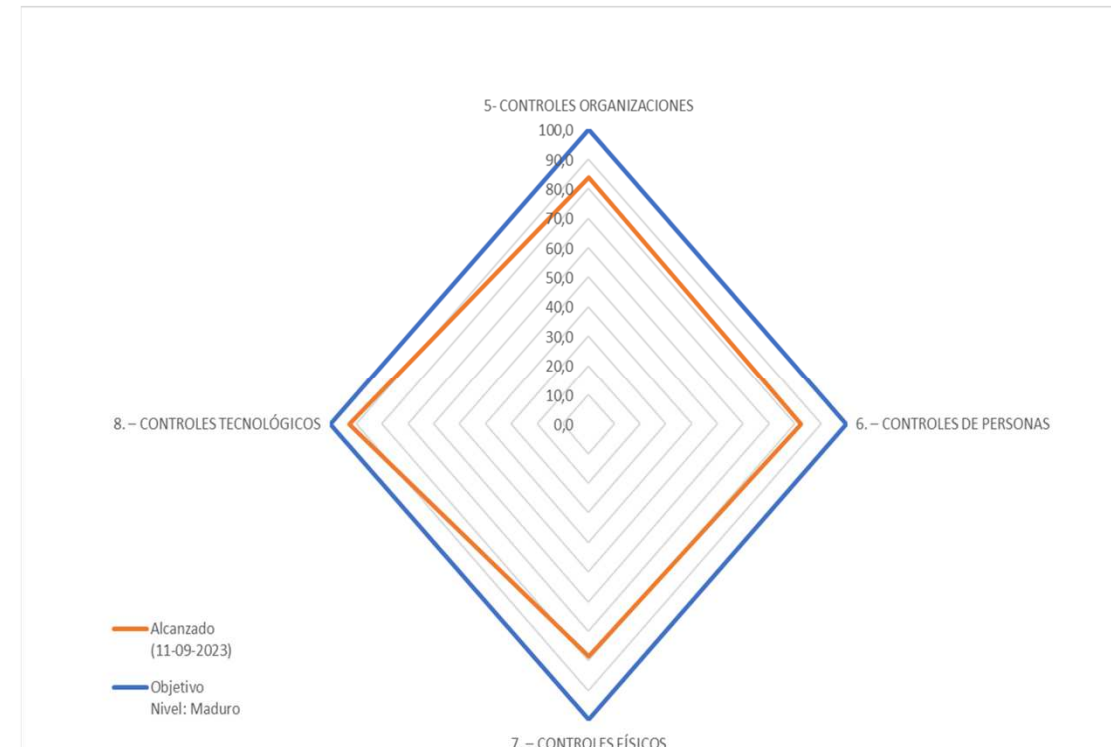
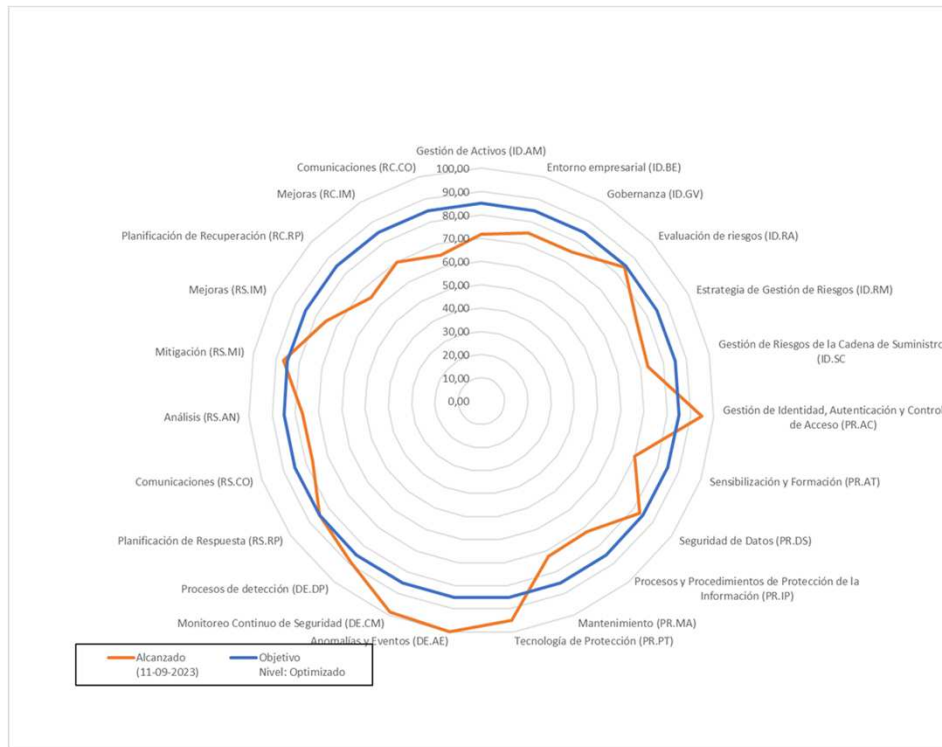
Plan de construcción de protocolos de actuación

Plan de Construcción de Protocolos de Actuación		
Proceso	Protocolo	Guía
Atención de peticiones	Análisis de Vulnerabilidades y Hacking Ético	
	Evaluaciones 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
Gestión de la operación	Otros	
	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.

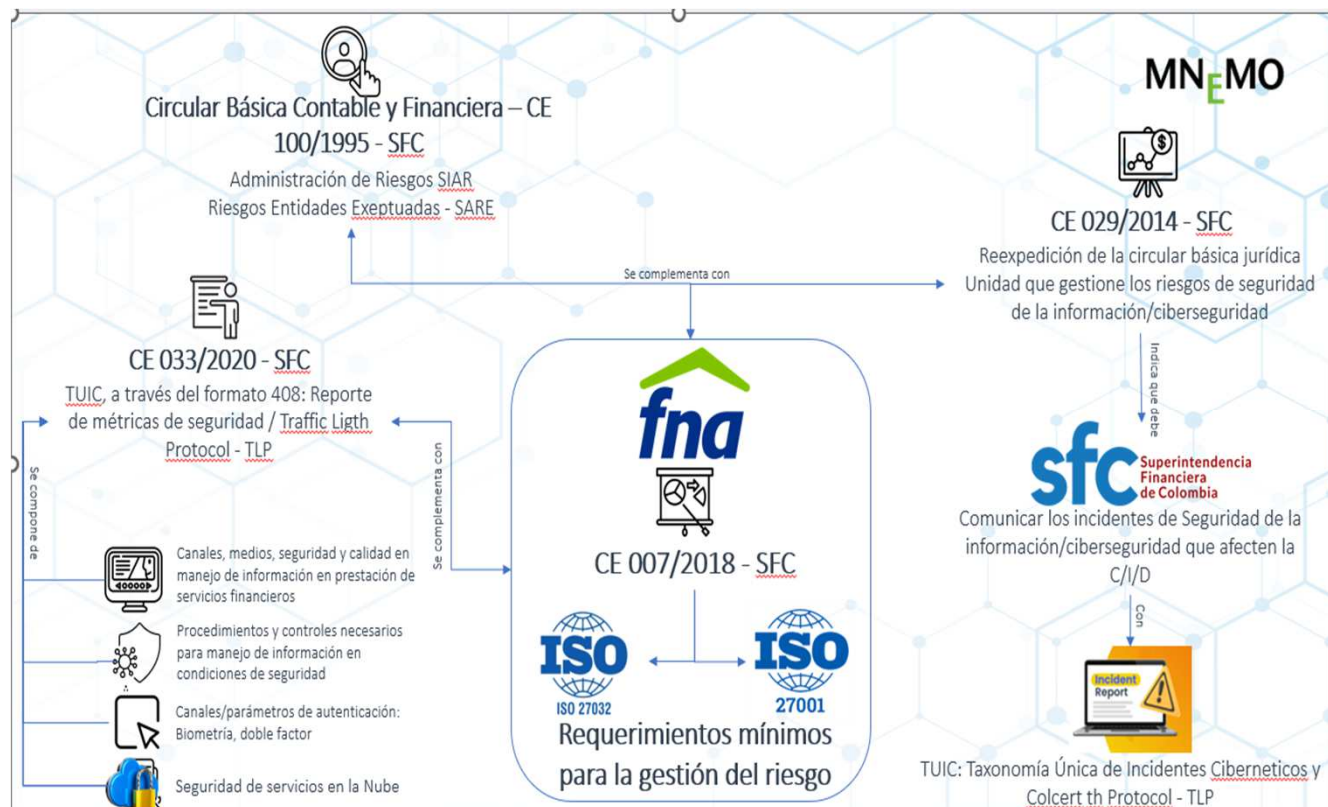


Diseño preliminar de tableros de control



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



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

PRE FACTURA
No. C-2-23

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2024-10-11

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

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	Administración y soporte de la plataforma XDR contrato 173-2023	1.00	3,326,000.00	3,957,940.00	0.00
2	Administración y soporte de la plataforma SOAR contrato 173-2023	1.00	14,627,000.00	17,406,130.00	0.00
3	Administración y soporte de la plataforma THREAT INTELLIGENCE contrato 173-2023	1.00	27,797,000.00	33,078,430.00	0.00
4	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING. contrato 173-2023	1.00	55,994,000.00	66,632,860.00	0.00
5	Administración y soporte Servicio de MONITOREO DE DNS contrato 173-2023	1.00	52,083,000.00	61,978,770.00	0.00
6	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT. contrato 173-2023	1.00	8,279,000.00	9,852,010.00	0.00
7	Administración y soporte de la plataforma CIBERDEFENSA contrato 173-2023	1.00	5,874,000.00	6,990,060.00	0.00
8	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD. contrato 173-2023	1.00	8,406,000.00	10,003,140.00	0.00
9	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM). contrato 173-2023	1.00	23,451,000.00	27,906,690.00	0.00

Total Bruto	199,837,000.00
Subtotal	199,837,000.00
IVA 19%	37,969,030.00
Total a Pagar	237,806,030.00

SUMA EN LETRAS: Doscientos treinta y siete millones ochocientos seis mil treinta pesos mcte.

Mnemo Colombia S.A.S. 49% NIT 900.396.176-1 Contribuyente

Mnemo Cyber Sec SAS 50% NIT 901.447.968-1 Contribuyente

Mnemo Evolution & integration Service SA 1% NIT:901.306.687-2 Contribuyente

DAVID TOVAR LOZANO
contadorjunior@mnemo.com
(3017710213)



BBVA Colombia
NIT 860.003.020-1
Certifica

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

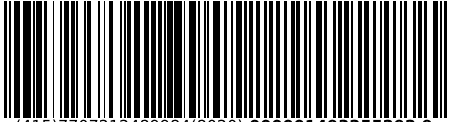
Esta certificación se expide a solicitud del titular con destino a quien interese, el **9 de julio del 2024**.

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

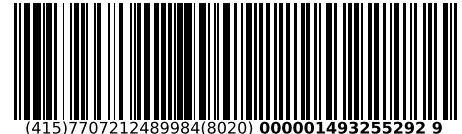
		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 14932552929			
5. Número de Identificación Tributaria (NIT) 9014479681				6. DV 1		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32							
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación		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 CYBER SEC S.A.S							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.		001	
41. Dirección principal CL 99 NO 10 19 OF 502							
42. Correo electrónico j.parra@mnemo.com							
43. Código postal				44. Teléfono 1 6913133		45. Teléfono 2	
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6201	47. Fecha inicio actividad 20201229	48. Código 6202	49. Fecha inicio actividad 20201229	50. Código 1	2	51. Código	
Responsabilidades, Calidades y Atributos							
53. Código 571442485255							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
52 - Facturador electrónico							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
54. Código 1234567891011121314151617181920				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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre VELEZ CASTRO HUMBERTO DE JESUS			
				985. Cargo Representante Legal Suplente Certificado			

		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 14932552929		
 (415)7707212489984(8020) 000001493255292 9					
5. Número de Identificación Tributaria (NIT) 9 0 1 4 4 7 9 6 8		6. DV 1	12. Dirección seccional Impuestos de Bogotá		14. Buzón electrónico 3 2
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas 1 2		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma			Composición del Capital		
Documento	1. Constitución		2. Reforma		
71. Clase	0 4				82. Nacional 1 0 0 %
72. Número					83. Nacional público 0 . 0 %
73. Fecha	2 0 2 0 1 2 2 8				84. Nacional privado 1 0 0 . 0 %
74. Número de notaría					85. Extranjero 0 %
75. Entidad de registro	0 3				86. Extranjero público 0 . 0 %
76. Fecha de registro	2 0 2 0 1 2 2 9				87. Extranjero privado 0 . 0 %
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				
Entidad de vigilancia y control					
88. Entidad de vigilancia y control Superintendencia de Sociedades 5					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1	8 0	2 0 2 1 0 1 2 5		-	
2				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
96. DV.					
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP		
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

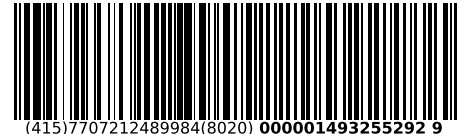
Representación

98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 2 0 1 2 2 8
100. Tipo de documento Cédula de Extranjeri 2 2	101. Número de identificación 6 6 7 3 5 2	102. DV 103. Número de tarjeta profesional
104. Primer apellido VICENT	105. Segundo apellido FERNANDEZ	106. Primer nombre CARLOS
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación REPRS LEGAL SUPL	1 9	99. Fecha inicio ejercicio representación 2 0 2 2 0 1 1 2
100. Tipo de documento Cédula de Ciudadan 1 3	101. Número de identificación 8 7 7 0 4 4 6	102. DV 103. Número de tarjeta profesional 6 1 0 6 1 - T
104. Primer apellido VELEZ	105. Segundo apellido CASTRO	106. Primer nombre HUMBERTO
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

Espacio reservado para la DIAN

4. Número de formulario

14932552929



(415)7707212489984(8020) 000001493255292 9

5. Número de Identificación Tributaria (NIT)

9 0 1 4 4 7 9 6 8 1

6. DV

12. Dirección seccional

Impuestos de Bogotá

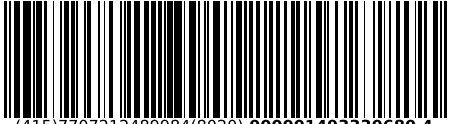
14. Buzón electrónico

3 2

Revisor Fiscal y Contador

Revisor fiscal principal	124. Tipo de documento Cédula de Ciudadanía	125. Número de identificación 1 0 1 8 4 0 8 8 7 6	126. DV	127. Número de tarjeta profesional 2 3 2 3 2 5 T
	128. Primer apellido TOVAR	129. Segundo apellido LOZANO	130. Primer nombre JAIRO	131. Otros nombres 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 Cédula de Ciudadanía	149. Número de identificación 1 0 3 0 6 1 8 6 2 6	150. DV	151. Número de tarjeta profesional 2 8 1 3 8 9 T
	152. Primer apellido PINZON	153. Segundo apellido ROJAS	154. Primer nombre ANDRES	155. Otros nombres 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			

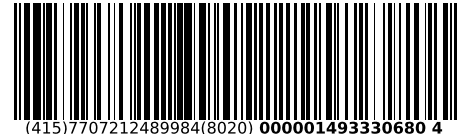
		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 14933306804			
5. Número de Identificación Tributaria (NIT) 901306872				6. DV 2		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32							
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación		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 EVOLUTION & INTEGRATION SERVICES S.A.							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.		001	
41. Dirección principal CL 99 10 19 OF 502							
42. Correo electrónico Jc.aponte@mnemo.com							
43. Código postal				44. Teléfono 1 6913133		45. Teléfono 2 3103243475	
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6201	47. Fecha inicio actividad 20190702	48. Código 6202	49. Fecha inicio actividad 20190702	50. Código 1 6209	2	51. Código	
Responsabilidades, Calidades y Atributos							
53. Código 5714424855							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
54. Código 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20				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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre PARRA GAMBOA JOHN JAIRO			
				985. Cargo Representante legal Certificado			

		Formulario del Registro Único Tributario				001	
Espacio reservado para la DIAN				Página 2 de 4 Hoja 2			
				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	
65. Fondos				66. Cooperativas			
68. Sin personería jurídica				69. Otras organizaciones no clasificadas			
				64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados			
				67. Sociedades y organismos extranjeros			
				70. Beneficio		1	
Constitución, Registro y Última Reforma							
Documento		1. Constitución		2. Reforma		Composición del Capital	
71. Clase		0 5				82. Nacional 0 %	
72. Número						83. Nacional público 0 . 0 %	
73. Fecha		2 0 1 9 0 7 2 6				84. Nacional privado 0 . 0 %	
74. Número de notaría		6 5					
75. Entidad de registro		0 3				85. Extranjero 1 0 0 %	
76. Fecha de registro		2 0 1 9 0 7 2 6				86. Extranjero público 0 . 0 %	
77. No. Matricula mercantil		0 0 0 3 1 4 4 6 0 3				87. Extranjero privado 1 0 0 . 0 %	
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					
Entidad de vigilancia y control							
88. Entidad de vigilancia y control							
Estado y Beneficio							
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV			
1	4 9	2 0 1 9 0 7 2 6		-			
2	8 1	2 0 1 9 0 7 2 6		-			
3				-			
4				-			
5				-			
Vinculación económica							
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.		
97. Nombre o razón social de la matriz o controlante							
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP			
173. Nombre o razón social de la sociedad o natural del exterior con EP							

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

98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 2 2 0 4 0 8
100. Tipo de documento Cédula de Ciudadaní 1 3	101. Número de identificación 8 0 8 0 8 4 2 0	102. DV 103. Número de tarjeta profesional
104. Primer apellido PARRA	105. Segundo apellido GAMBOA	106. Primer nombre JOHN
107. Otros nombres JAIRO	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

98. Representación	99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación
102. DV 103. Número de tarjeta profesional	
104. Primer apellido	105. Segundo apellido
106. Primer nombre	107. Otros nombres
108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

98. Representación	99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación
102. DV 103. Número de tarjeta profesional	
104. Primer apellido	105. Segundo apellido
106. Primer nombre	107. Otros nombres
108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

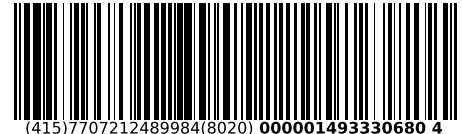
98. Representación	99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación
102. DV 103. Número de tarjeta profesional	
104. Primer apellido	105. Segundo apellido
106. Primer nombre	107. Otros nombres
108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

98. Representación	99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación
102. DV 103. Número de tarjeta profesional	
104. Primer apellido	105. Segundo apellido
106. Primer nombre	107. Otros nombres
108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

Espacio reservado para la DIAN

4. Número de formulario

14933306804



(415)7707212489984(8020) 000001493330680 4

5. Número de Identificación Tributaria (NIT)

9 0 1 3 0 6 6 8 7

6. DV

2

12. Dirección seccional

Impuestos de Bogotá

14. Buzón electrónico

3 2

Revisor Fiscal y Contador

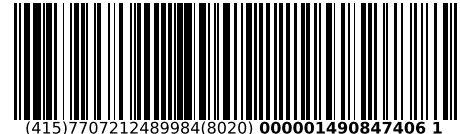
Revisor fiscal principal	124. Tipo de documento Cédula de Ciudadanía	125. Número de identificación 1 3 8 7 7 0 4 4 6	126. DV	127. Número de tarjeta profesional 6 1 0 6 1
	128. Primer apellido VELEZ	129. Segundo apellido CASTRO	130. Primer nombre HUMBERTO	131. Otros nombres DE JESUS
	132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada	
	135. Fecha de nombramiento 2 0 2 1 0 2 1 5			
Revisor fiscal suplente	136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional
	140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres
	144. Número de Identificación Tributaria (NIT)	145. DV	146. Sociedad o firma designada	
	147. Fecha de nombramiento			
Contador	148. Tipo de documento Cédula de Ciudadanía	149. Número de identificación 1 3 1 0 1 8 4 0 8 8 7 6	150. DV	151. Número de tarjeta profesional 2 3 2 3 2 5
	152. Primer apellido TOVAR	153. Segundo apellido LOZANO	154. Primer nombre JAIRO	155. Otros nombres DAVID
	156. Número de Identificación Tributaria (NIT)	157. DV	158. Sociedad o firma designada	
	159. Fecha de nombramiento 2 0 2 1 0 6 0 1			

		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 14908474061			
5. Número de Identificación Tributaria (NIT) 9003961761				6. DV 1		12. Dirección seccional Impuestos de Bogotá	
				14. Buzón electrónico 32			
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación		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		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.		001	
41. Dirección principal CL 99 10 19 OF 502							
42. Correo electrónico recepcion.colombia@mnemo.com							
43. Código postal				44. Teléfono 1 3183835117		45. Teléfono 2 6913333	
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6201	47. Fecha inicio actividad 20101112	48. Código 6202	49. Fecha inicio actividad 20101112	50. Código 1 6209	2 8551	51. Código	
Responsabilidades, Calidades y Atributos							
53. Código 57910141819264142485255							
05- Impto. renta y compl. régimen ordinario 26- Declaración individual precios de tran							
07- Retención en la fuente a título de renta 41- Declaración anual de activos en el exte							
09- Retención en la fuente en el impuesto 42- Obligado a llevar contabilidad							
10- Obligado aduanero 48- Impuesto sobre las ventas - IVA							
14- Informante de exogena 52- Facturador electrónico							
18- Precios de transferencia 55- Informante de Beneficiarios Finales							
19- Productor de bienes y/o servicios exen							
Usuarios aduaneros				Exportadores			
54. Código 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20				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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre VELEZ CASTRO HUMBERTO DE JESUS			
				985. Cargo Representante Legal Suplente Certificado			

Espacio reservado para la DIAN

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 1

6. DV

1

12. Dirección seccional

Impuestos de Bogotá

14. Buzón electrónico

3 2

Características y formas de las organizaciones

62. Naturaleza

2

63. Formas asociativas

1 2

64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados

67. Sociedades y organismos extranjeros

70. Beneficio

1

65. Fondos

66. Cooperativas

68. Sin personería jurídica

69. Otras organizaciones no clasificadas

Constitución, Registro y Última Reforma

Composición del Capital

Documento

1. Constitución

2. Reforma

71. Clase

0 4

0 4

72. Número

73. Fecha

2 0 1 0 1 1 1 2

2 0 1 3 0 4 1 8

74. Número de notaría

75. Entidad de registro

0 3

0 3

76. Fecha de registro

2 0 1 0 1 1 1 9

2 0 1 3 0 7 0 9

77. No. Matrícula mercantil

0 2 0 4 5 1 6 2

0 2 0 4 5 1 6 2

78. Departamento

1 1

1 1

79. Ciudad/Municipio

4

4

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

Superintendencia de Sociedades

5

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	8 0	2 0 1 6 0 1 0 1	-	-
2			-	-
3			-	-
4			-	-
5			-	-

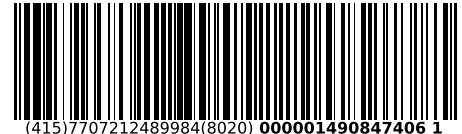
Vinculación económica

93. Vinculación económica	94. Nombre del grupo económico y/o empresarial	95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.
97. Nombre o razón social de la matriz o controlante			
170. Número de identificación tributaria otorgado en el exterior	171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP			

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

9 0 0 3 9 6 1 7 6 1

Impuestos de Bogotá

3 2

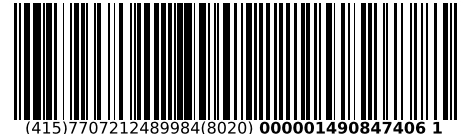
Representación

98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 1 7 0 8 2 9
100. Tipo de documento Cédula de Extranjeri 2 2	101. Número de identificación 6 6 7 3 5 2	102. DV 103. Número de tarjeta profesional
104. Primer apellido VICENT	105. Segundo apellido FERNANDEZ	106. Primer nombre CARLOS
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación REPRS LEGAL SUPL	1 9	99. Fecha inicio ejercicio representación 2 0 2 2 0 1 1 7
100. Tipo de documento Cédula de Ciudadan 1 3	101. Número de identificación 8 7 7 0 4 4 6	102. DV 103. Número de tarjeta profesional 6 1 0 6 1 - T
104. Primer apellido VELEZ	105. Segundo apellido CASTRO	106. Primer nombre HUMBERTO
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal
98. Representación	99. Fecha inicio ejercicio representación	
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
108. Número de Identificación Tributaria (NIT)	109. DV	110. Razón social representante legal

Espacio reservado para la DIAN

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

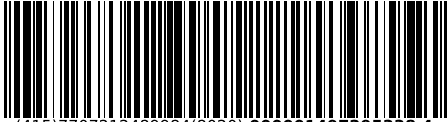
14. Buzón electrónico

3 2

Revisor Fiscal y Contador

Revisor fiscal principal	124. Tipo de documento Cédula de Ciudadanía	125. Número de identificación 1 4 2 3 9 5 8 1	126. DV	127. Número de tarjeta profesional 2 7 3 9 8 T
	128. Primer apellido SALAZAR	129. Segundo apellido GOMEZ	130. Primer nombre JOSE	131. Otros nombres IGNACIO
	132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada	
	135. Fecha de nombramiento 2 0 2 3 0 3 3 1			
Revisor fiscal suplente	136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional
	140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres
	144. Número de Identificación Tributaria (NIT)	145. DV	146. Sociedad o firma designada	
	147. Fecha de nombramiento			
Contador	148. Tipo de documento Cédula de Ciudadanía	149. Número de identificación 1 0 1 8 4 0 8 8 7 6	150. DV	151. Número de tarjeta profesional 2 3 2 3 2 5 T
	152. Primer apellido TOVAR	153. Segundo apellido LOZANO	154. Primer nombre JAIRO	155. Otros nombres DAVID
	156. Número de Identificación Tributaria (NIT)	157. DV	158. Sociedad o firma designada	
	159. Fecha de nombramiento 2 0 2 2 0 1 1 7			

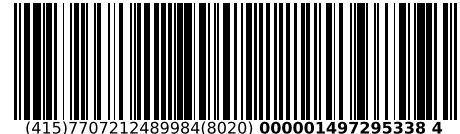
		Formulario del Registro Único Tributario				001	
2. Concepto 0 2 Actualización				4. Número de formulario 14972953384			
5. Número de Identificación Tributaria (NIT) 9 0 1 7 8 1 6 2 5				6. DV 1		12. Dirección seccional Impuestos de Bogotá	
				14. Buzón electrónico 3 2			
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		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 CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio 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 0 1 1 0 0 1				44. Teléfono 1 3 1 8 3 8 3 5 1 1 7		45. Teléfono 2 3 0 1 6 3 2 7 9 8 6	
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6 2 0 1	47. Fecha inicio actividad 2 0 2 3 1 2 1 4	48. Código	49. Fecha inicio actividad	50. Código 1 2	51. Código		
Responsabilidades, Calidades y Atributos							
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				Exportadores			
54. Código 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20				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.				Sin perjuicio de las verificaciones que la DIAN realice.			
Firma del solicitante:				Firma autorizada:			
				984. Nombre VELEZ CASTRO HUMBERTO DE JESUS			
				985. Cargo Representante legal Certificado			

		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 5 Hoja 2		
			4. Número de formulario 14972953384		
 (415)7707212489984(8020) 000001497295338 4					
5. Número de Identificación Tributaria (NIT) 9 0 1 7 8 1 6 2 5 1		6. DV 1		12. Dirección seccional Impuestos de Bogotá	
				14. Buzón electrónico 3 2	
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica 3		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma					
Documento		1. Constitución		2. Reforma	
71. Clase 0 2					
72. Número					
73. Fecha 2 0 2 3, 1 1, 2 3					
74. Número de notaría					
75. Entidad de registro 9 8					
76. Fecha de registro 2 0 2 3, 1 2, 1 3					
77. No. Matricula mercantil					
78. Departamento 1 1					
79. Ciudad/Municipio 0 0 1					
Composición del Capital					
Vigencia					
80. Desde 2 0 2 3, 1 2, 1 3				82. Nacional 1 0 0 %	
81. Hasta 2 0 2 5, 1 2, 3 1				83. Nacional público 0 . 0 %	
				84. Nacional privado 1 0 0 . 0 %	
				85. Extranjero 0 %	
				86. Extranjero público 0 . 0 %	
				87. Extranjero privado 0 . 0 %	
Entidad de vigilancia y control					
88. Entidad de vigilancia y control					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1				-	
2				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
97. Nombre o razón social de la matriz o controlante				96. DV.	
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

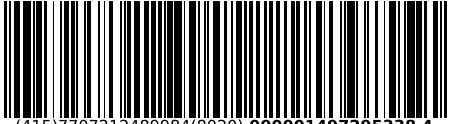
9 0 1 7 8 1 6 2 5 1

Impuestos de Bogotá

3 2

Representación

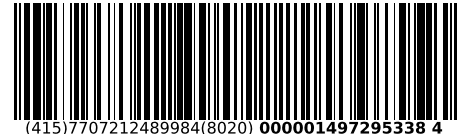
98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 2 3 1 1 2 3
100. Tipo de documento Cédula de Ciudadaní 1 3	101. Número de identificación 8 7 7 0 4 4 6	102. DV 103. Número de tarjeta profesional
104. Primer apellido VELEZ	105. Segundo apellido CASTRO	106. Primer nombre HUMBERTO
107. Otros nombres DE JESUS	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal
98. Representación REPRS LEGAL SUPL	1 9	99. Fecha inicio ejercicio representación 2 0 2 3 1 1 2 3
100. Tipo de documento Cédula de Ciudadan 1 3	101. Número de identificación 8 0 8 0 8 4 2 0	102. DV 103. Número de tarjeta profesional
104. Primer apellido PARRA	105. Segundo apellido GAMBOA	106. Primer nombre JOHN
107. Otros nombres JAIRO	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal
98. Representación		99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal
98. Representación		99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal
98. Representación		99. Fecha inicio ejercicio representación
100. Tipo de documento	101. Número de identificación	102. DV 103. Número de tarjeta profesional
104. Primer apellido	105. Segundo apellido	106. Primer nombre
107. Otros nombres	108. Número de Identificación Tributaria (NIT)	109. DV 110. Razón social representante legal

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

Espacio reservado para la DIAN

4. Número de formulario

14972953384



(415)7707212489984(8020) 000001497295338 4

5. Número de Identificación Tributaria (NIT)

9 0 1 7 8 1 6 2 5

6. DV

1

12. Dirección seccional

Impuestos de Bogotá

14. Buzón electrónico

3 2

Revisor Fiscal y Contador

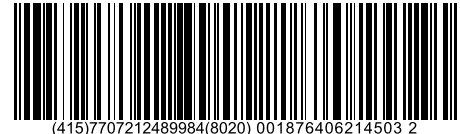
Revisor fiscal principal	124. Tipo de documento	125. Número de identificación	126. DV	127. Número de tarjeta profesional
	128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
	132. Número de Identificación Tributaria (NIT)	133. DV	134. Sociedad o firma designada	
	135. Fecha 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		

Espacio reservado para la DIAN



4. Número de formulario

18764062145032



(415)7707212489984(8020) 001876406214503 2

5. Número de Identificación Tributaria - NIT 9 0 1 7 8 1 6 2 5	6. DV 1	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
11. Razón social CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA					
12. Dirección seccional Impuestos de Bogotá					Cód. 3 2
24. Dirección CL 99 # 10 - 19 OF 502 ED TRADE CENTER					
25. País Colombia		26. Departamento Bogotá D.C.		27. Municipio Bogotá, D.C.	

La U.A.E. Dirección de Impuestos y Aduanas Nacionales, conforme a la facultad discrecional establecida en el artículo 684 - 2 del Estatuto Tributario y en virtud de lo estipulado en la Resolución 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 trámite establecido.

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

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

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

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

Firma del funcionario autorizado

Firma del solicitante



1001. Apellidos y nombres VELEZ CASTRO HUMBERTO DE JESUS
1002. Tipo documento Cédula de Ciudadanía
1003. No. Identificación 8 7 7 0 4 4 6 1004. DV 3
1005. Cod. Representación Representante Legal Principal
1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

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

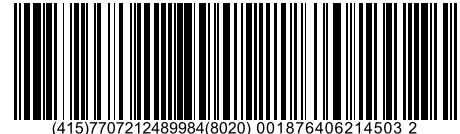
997. Fecha formalización 2 0 2 3 - 1 2 - 1 8 / 1 5 : 1 2 : 2 7

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

34. Tipo solicitud
AUTORIZACIÓN

Cód.
1



Bogotá, 11 de Octubre de 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	5300631158	FECHA DE CONTABILIZACIÓN	24.10.2024
N° DE REFERENCIA	29	FECHA DE PAGO	12.11.2024

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	FE29 RAD 02-2303-202410284171344		

OBSERVACIONES:

INFORMACIÓN PRESUPUESTAL						
SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
20001186	6200000102	00090	CTO 173 DE 2023 .	1000049730	5105628985	37.036.370
20001186	6200000102	00010	CTO 173 DE 2023 .	1000048947	5105628985	155.869.770
20001186	6200000102	00070	CTO 173 DE 2023 .	1000048951	5105628985	16.993.200
20001186	6200000102	00080	CTO 173 DE 2023 .	1000048952	5105628985	27.906.690
AFECTACIÓN PEDIDO						237.806.030
DETALLE DE LA ORDEN DE PAGO						
VALOR TOTAL FAC.	237.806.030,00					
DESCUENTOS	14.620.075,00					
NOTAS CRÉDITOS	0,00					
VALOR A PAGAR	223.185.955,00					



División de Tesorería

Documento de Pago

No. ORDEN DE PAGO	29	FECHA DE CONTABILIZACION	12-nov-24
No. DOCUMENTO DE PAGO	5300631158	FECHA DE DOCUMENTO	12-nov-24
		FECHA DE COMPENSACION	12-nov-24
PROPUESTA	47073	FECHA DE LA PROPUESTA	12-nov-24

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

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

BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSEGURIDAD		
No. IDENTIFICACIÓN	9017816251	TIPO DE IDENTIFICACIÓN	25
NOMBRE:	CONSORCIO UNIDAD DE		
OBSERVACIONES:	FE29 RAD 02-2303-202410284171344		
NÚMERO DE CUENTA	2501050101	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	223.185.955		

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	5300631158	29	223.185.955	FE29 RAD 02-2303-202410284171344	6200000102	CTO 173 DE 2023