

	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
UNIDAD ADMINISTRATIVA:
OFICINA PRODUCTORA:
OBJETO:

FONDO NACIONAL DEL AHORRO S.A.
VICEPRESIDENCIA DE TECNOLOGÍA Y TRANSFORMACION DIGITAL
GERENCIA DE ESTRATEGIA TI Y ASEGURAMIENTO INFORMATICO
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 (dd-mm-aaaa)		SOPORTE O FORMATO		FÍSICO						ELECTRÓNICO			FRECUENCIA DE CONSULTA	OBSERVACIONES																														
	CÓDIGO OFICINA	SERIE	SUBSERIE			Inicial	Final	Físico	Electrónico	UNIDAD DE CONSERVACIÓN						Ubicación	Cantidad de documentos	Tamaño de los documentos																																
										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.27 factura Nro. FE36 orden de pago No. 5300274089	21-mar-25	9-abr-25		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	229	15,1 MB																																
<table><tr><td>Autorizado por:</td><td>Jessebell Cristina Mejías Linares</td><td>Entregado por:</td><td>Jessebell Cristina Mejías Linares</td><td>Recibido por:</td><td></td></tr><tr><td>Cargo:</td><td>Auxiliar Administrativo 01</td><td>Cargo:</td><td>Auxiliar Administrativo 01</td><td>Cargo:</td><td></td></tr><tr><td>Firma:</td><td></td><td>Firma:</td><td></td><td>Firma:</td><td></td></tr><tr><td>Lugar:</td><td>Bogotá D.C.</td><td>Lugar:</td><td>Bogotá D.C.</td><td>Lugar:</td><td></td></tr><tr><td>Fecha:</td><td>30-04-2025</td><td>Fecha:</td><td>30/04/2025</td><td>Fecha:</td><td></td></tr></table>																					Autorizado por:	Jessebell Cristina Mejías Linares	Entregado por:	Jessebell Cristina Mejías Linares	Recibido por:		Cargo:	Auxiliar Administrativo 01	Cargo:	Auxiliar Administrativo 01	Cargo:		Firma:		Firma:		Firma:		Lugar:	Bogotá D.C.	Lugar:	Bogotá D.C.	Lugar:		Fecha:	30-04-2025	Fecha:	30/04/2025	Fecha:	
Autorizado por:	Jessebell Cristina Mejías Linares	Entregado por:	Jessebell Cristina Mejías Linares	Recibido por:																																														
Cargo:	Auxiliar Administrativo 01	Cargo:	Auxiliar Administrativo 01	Cargo:																																														
Firma:		Firma:		Firma:																																														
Lugar:	Bogotá D.C.	Lugar:	Bogotá D.C.	Lugar:																																														
Fecha:	30-04-2025	Fecha:	30/04/2025	Fecha:																																														

	INFORME DE SEGUIMIENTO Y DE EVALUACIÓN CONTRACTUAL		Código: GLC-CONT-FO-016				
	PROCESO CONTRATACION		Versión: 1				
INFORME No 27		FACTURA No		FECHA			
No. DE ACEPTACIÓN: 1000055114 / 1000055115 / 1000055116 / 1000055117				21	03	25	
				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		Jaime Becerra					
(Nombre de la persona delegada para apoyar la supervisión del contrato)		(Nombre de la persona delegada para apoyar la supervisión del contrato)					
OBJETO DEL CONTRATO							
CONTRATAR UNIDAD DE CIBERSEGURIDAD QUE PROPORCIONE SERVICIOS DE SEGURIDAD INTEGRADOS AL FONDO NACIONAL DEL AHORRO							
DEPENDENCIA EJECUCIÓN CONTRATO		VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL (Gerencia de Estrategia TI y aseguramiento informatico)					
		(Indique el nombre de la dependencia responsable del contrato)					
PLAZO DE EJECUCIÓN DEL CONTRATO		24 Meses					
		(Indique en este espacio el número de días o de meses para ejecutar el contrato)					
FECHA DE INICIACIÓN DEL CONTRATO		22	DE	dic	DE	2023	
		(Día)		(Mes)		(Año)	
FECHA DE TERMINACIÓN DEL CONTRATO		21	DE	dic	DE	2025	
		(Día)		(Mes)		(Año)	
REGISTRO PRESUPUESTAL No.		5400001604 - 6200000102 - 5400001890					
VALOR DEL CONTRATO							
TREINTA Y SEIS MIL CUATROCIENTOS NOVENTA Y NUEVE MILLONES QUINIENTOS OCHENTA Y TRES MIL SEISCIENTOS DIEZ PESOS MONEDA CORRIENTE (\$36.499.583.610,00) M/CTE INCLUIDO IVA Y DEMÁS CONTRIBUCIONES A LAS QUE HAYA LUGAR. ADICIÓN NRO. 1 DIECINUEVE MIL NOVECIENTOS VEINTIDOS MILLONES NOVECIENTOS OCHENTA Y SIETE MIL CUATROCIENTOS NOVENTA Y TRES PESOS M/CTE (\$19.922.987.493)							
El valor del presente contrato es hasta la suma DE CINCUENTA Y SEIS MIL CUATROCIENTOS VEINTIDÓS MILLONES QUINIENTOS SETENTA Y UN MIL CIENTO TRES PESOS M/CTE (\$56.422.571.103)							
(Indique en este espacio el valor del contrato en letras)							
PRÓRROGAS		ADICIONES			SUSPENSIONES		
No.	PLAZO	No.	VALOR	RP	No	DESDE	HASTA
		1	\$ 19.922.987.493	5400001890			

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 31.243.603.434,00	55,37%
Valor del pago aprobado con el presente informe	\$ 423.428.180,00	0,75%
VALOR TOTAL EJECUTADO	\$ 31.667.031.614,00	56,12%
Porcentaje de ejecución presupuestal programado a la fecha		56,17%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,04%

OBSERVACIONES

Cuenta 27:administración y soporte en sitio durante el el período del 22 de diciembre de 2024 al 21 de enero de 2025. Items 1 al 11 Pre-factura C_2_29
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	61%
Porcentaje de ejecución de actividades realizado a la fecha	61%
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

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

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

4. CONCEPTO SUPERVISOR O INTERVENTOR

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de CUATROCIENTOS VEINTITRES MILLONES CUATROCIENTOS VENTIOCHO MIL CIENTO OCHENTA PESOS MCTE (\$ 423.428.180).

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 INFORMÁTICO, 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

(día en letras)

21

(día en números)

días del mes de

marzo

(mes en letras)

de

2025

(Año)

Mónica
Grand Villada

Firmado digitalmente por
Mónica Grand Villada
Fecha: 2025.03.25
14:19:49 -05'00'

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

Revisó y aprobó: Enrique Arrazola - Jaime Becerra Apoyo a la supervisión

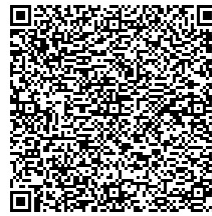
Estadística de datos	Cantidad
Registros transferidos	12

Cl.doc. : RE (Factura bruto) Documento normal					
Reg.prelim.por		NTUIRAN	Contab.por		MRINCONZ
N° doc.	5100000635	Sociedad	1000	Ejercicio	2025
Fe.docum.	25.03.2025	Fecha contab.	25.03.2025	Período	03
Calc.impuestos	☒				
Referen.	36				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202503260439469				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	397,396,242-
2	86	2511950101	CXP PROVED EM/RF		W0	37,036,370
3	81	5130950408	GESTION Y MON SGSI		W0	0
4	86	2511950101	CXP PROVED EM/RF		W0	317,007,670
5	81	5130950401	CENTRO OPER SEG		W0	0
6	86	2511950101	CXP PROVED EM/RF		W0	37,909,830
7	81	5130950408	GESTION Y MON SGSI		W0	0
8	86	2511950101	CXP PROVED EM/RF		W0	31,474,310
9	81	5130950409	SERV SEGURID INFORMA		W0	0
10	50	2519051101	SERVICIO 3.5%			12,453,770-
11	50	2519053801	RTE IVA TARIFA GENER			10,140,927-
12	50	2519054408	SERVICIOS 304 BOGOTA			3,437,241-



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 36

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	25/03/2025, 12:32
Expedición	25/03/2025, 12:35
Vencimiento	24/04/2025

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Administración y soporte de la plataforma XDR. N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	3,957,940.00
2	Administración y soporte de la plataforma THREAT INTELLIGENCE (TIP). N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	33,078,430.00
3	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING. N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	66,632,860.00
4	Administración y soporte Servicio de MONITOREO DE DNS servidor infoblox 1405 series, Serial No: 1405202201700334 N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	61,978,770.00
5	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSEEMNET N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	9,852,010.00
6	Administración y soporte de la plataforma CIBERDEFENSA N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	6,990,060.00
7	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	10,003,140.00
8	Administración y soporte de la plataforma SOAR N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	17,406,130.00
9	Análisis de vulnerabilidades (dos(2) obligatorios al año, al total de activos de la plataforma tecnológica) N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	154,147,840.00
10	Administración y soporte de la plataforma MONITOREO DE LA BASE DE DATOS (DAM). N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	27,906,690.00
11	Administración y soporte de la plataforma SOLUCION GOBIERNO DE INDETIDADES (IAM). N° de aceptación 1000055114 / 1000055115 / 1000055116 / 1000055117	1.00	0.00	31,474,310.00

Total items: 11

Valor en Letras:

Cuatrocientos veintitres millones cuatrocientos veintiocho mil ciento ochenta pesos m/cte

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2025-04-24 por \$ 423,428,180.00

Observaciones:

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	355,822,000.00
IVA 19%	67,606,180.00
Total a Pagar	423,428,180.00

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764085737391 aprobado en 20241219 prefijo FE desde el número 33 al 5000 Vigencia: 12 Meses**

Responsable de IVA - Actividad Económica 6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Tarifa 9.66

CUFE: 9238400191b61d198f388e6a45d15c5dbf6af1a07f3beb3ed513d27c1eb013057660c292999ebf97a46758a1cf93c5e2

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 Veinte (20) días del mes de Marzo de dos mil veinticinco (2025).

Atentamente,



HUMBERTO DE JESUS VELEZ CASTRO

Representante Legal **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA**

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

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

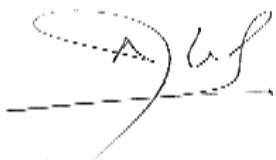
Teléfono: 6913133 - 310 8569109

Correo electrónico: h.dejesusvelez@mnemo.com

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

HUMBERTO DE JESUS VELEZ CASTRO, identificado con cédula de ciudadanía No. **8.770.446** de Soledad - Atlántico, y con Tarjeta Profesional No. 61.061-T de la Junta Central de Contadores de Colombia, en mi condición de Revisor Fiscal de la sociedad extranjera con sucursal en Colombia **CONSORCIO MNEMO SOC MHCP**, identificada con NIT 901.778.397-6, 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 veinte (20) días del mes de Marzo de 2025.



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 septiembre de 2024 y 28 de febrero del 2025**. 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 septiembre de 2024 y 28 de febrero del 2025**.
4. El ultimo pago de aportes corresponde a **pensión febrero** del año **2025 y salud marzo** del año **2025**.
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 septiembre de 2024 y 28 de febrero del 2025**, 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 veinte (20) días, del mes de marzo del año 2025.



JAIRO DAVID TOVAR LOZANO

C.C. 1.018.408.876

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

EL SUSCRITO REVISOR FISCAL

C E R T I F I C A

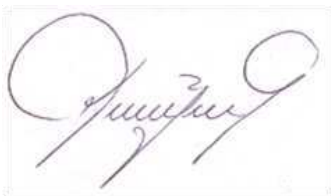
Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO COLOMBIA S.A.S., con NIT 900.396.176-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, D.C., dedicada a la actividad de desarrollo de sistemas informáticos CIIU 6201, durante el período de los **ÚLTIMO SEIS MESES**, comprendido entre el 1 de octubre de 2024 al 20 de marzo de 2025, 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 (20) veinte días del mes de marzo de 2025.

At.



JOSE IGNACIO SALAZAR GOMEZ

Revisor Fiscal T.P. 27.398-T

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

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

DATOS GENERALES DE LA LIQUIDACION									
Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco		Valor
2025-02	2025-03	1350333801	9483305144	E	2025/03/19	2025/03/20	BANCO BBVA COLOMBIA S.A.		\$170,981,500

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 (92 Afiliados)																														
Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (20 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (20 Afiliados)																														
1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																	230201	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
2	CC	93387321	ARANA REYES JAMES GUSTAVO																	25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No
3	CC	67016350	BOCANEGRA VALBUENA ANA MARIA										X							25-14	2	EPS001	2	CCF24	0	14-25	2	0.000%	0	No
4	CC	67016350	BOCANEGRA VALBUENA ANA MARIA										X							25-14	2	EPS001	2	CCF24	0	14-25	2	0.000%	0	No
5	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																	25-14	26	EPS001	26	CCF24	26	14-25	26	1.044%	26	No
6	CC	1122651302	CARO ROA JONATHAN																	230301	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
7	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																	230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
8	CC	1013592039	EMBUS IPIA JULIAN ANDRES								X									231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
9	CC	6319789	ESPAÑA MOSQUERA JESUS ARBEY																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
10	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																	25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
11	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO								X									231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
12	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
13	CC	79865487	PUENTES CASTRO DAVID EDUARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
14	CC	79717549	RODRIGUEZ JOHN FERNANDO											X						230201	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
15	CC	79717549	RODRIGUEZ JOHN FERNANDO																	230201	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	Si
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																	230901	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																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
23	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																	0	EPS002	30		0		0	0.000%	0	No	
Centro de Trabajo: ADMINISTRACION (68 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (68 Afiliados)																														

24	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO															25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
25	CC	1023953140	ARIAS NATALIA MELIZA					X										23020 1	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
26	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER						X									23100 1	15	EPS008	15	CCF24	15	14-25	15	0.000%	15	Si
27	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER												X			23100 1	15	EPS008	15	CCF24	15	14-25	15	0.522%	15	Si
28	CC	1023978779	BARRERA PACHECO YURANY PAOLA						X									23030 1	1	EPS005	1	CCF24	0	14-25	1	0.000%	0	Si
29	CC	1023978779	BARRERA PACHECO YURANY PAOLA															23030 1	29	EPS005	29	CCF24	29	14-25	29	0.522%	29	Si
30	CC	1026295259	BEJARANO QUIROGA ANDRES FELIPE					X										25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER															23020 1	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
32	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN															23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
33	CC	1113858520	CAMACHO PIRA CRISTIAN ALEXANDER															25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
34	CC	1122512867	CAMPOS MARTINEZ JUAN ALEJANDRO					X										23030 1	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
35	CC	1014856015	CARDENAS LOPEZ NICOLAS ENRIQUE					X										23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
36	CC	1034397473	CASTILLO IDROBO JHON FABER															23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
37	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID						X									23030 1	13	EPS005	13	CCF24	13	14-25	13	0.000%	13	Si
38	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID					X										23030 1	17	EPS005	17	CCF24	17	14-25	17	0.522%	17	Si
39	CC	80731020	DESALVADOR RESTREPO MARCELO															25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
40	CC	1012976046	DIAZ MARIN CAMILO ARTURO					X										23030 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
41	CC	80102292	DIAZ TORRES CHRISTIAN ALEXANDER															23030 1	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
42	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER															25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
43	CC	1001326677	GOMEZ PARRA CRISTIAN CAMILO					X										23020 1	30	EPS001	30	CCF24	30	14-25	30	0.522%	30	Si
44	CC	1019009180	GOMEZ ROJAS YENNY PAOLA															23030 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
45	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO															23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
46	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN															23030 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
47	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL					X										23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
48	CC	1010840818	GUEVARA GUANCHA ERWIN SANTIAGO					X										25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
49	CC	1082874657	GUEVARA RIZZO SANTIAGO					X										23030 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
50	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES															23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
51	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA															23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
52	CC	1099374748	LEAL GOMEZ DANIELA						X									23020 1	2	EPS037	2	CCF24	2	14-25	2	0.000%	2	Si
53	CC	1099374748	LEAL GOMEZ DANIELA															23020 1	28	EPS037	28	CCF24	28	14-25	28	0.522%	28	Si
54	CC	52953219	LEON CERON MARIA ALEXANDRA															23100 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
55	CC	1069769484	LOPEZ ZAMORA JUAN DAVID					X										23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
56	CC	1000149678	LOZANO GUTIERREZ MARIA CAMILA					X										23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
57	CC	1193088387	LUENGAS CORTES DAVID STIWEN					X										23030 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si

[illegible]

Página 4 de 5

DATOS GENERALES DEL APORTANTE											
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal		Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS		B - MENOS DE 200 COTIZANTES		PRINCIPAL		CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION											
Periodo		Clave		Tipo	Fecha		Pago				
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco		Dias Mora	Valor	
2025-02	2025-03	1350333801	9483305144	E	2025/03/19	2025/03/20	BANCO BBVA COLOMBIA S.A.		1	\$170,981,500	
RESUMEN DE PAGO											
RIESGO		CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES		VALOR A PAGAR	
AFP (ADMINISTRADORAS: 5)					86	\$90,926,600	\$57,500	\$0		\$90,984,100	
COLFONDOS		231001	800,227,940	6	6	\$15,540,600	\$9,800	\$0		\$15,550,400	
COLPENSIONES		25-14	900,336,004	7	16	\$16,534,900	\$10,400	\$0		\$16,545,300	
PORVENIR		230301	800,224,808	8	33	\$23,785,500	\$15,000	\$0		\$23,800,500	
PROTECCION		230201	800,229,739	0	27	\$28,273,300	\$17,800	\$0		\$28,291,100	
SKANDIA		230901	800,253,055	2	4	\$6,792,300	\$4,500	\$0		\$6,796,800	
ARL (ADMINISTRADORAS: 1)					88	\$4,704,100	\$3,000	\$0		\$4,707,100	
COLMENA		14-25	800,226,175	3	88	\$4,704,100	\$3,000	\$0		\$4,707,100	
CCF (ADMINISTRADORAS: 1)					88	\$23,651,900	\$14,900	\$0		\$23,666,800	
COMPENSAR		CCF24	860,066,942	7	88	\$23,651,900	\$14,900	\$0		\$23,666,800	
EPS (ADMINISTRADORAS: 10)					93	\$41,710,400	\$26,600	\$0		\$41,737,000	
ALIANSA SALUD EPS (ANTES COLMEDICA)		EPS001	830,113,831	0	3	\$2,132,200	\$1,400	\$0		\$2,133,600	
CAPITAL SALUD		EPSC34	900,298,372	9	1	\$119,900	\$100	\$0		\$120,000	
COMPENSAR		EPS008	860,066,942	7	16	\$5,249,300	\$3,300	\$0		\$5,252,600	
EPS SURA (ANTES SUSALUD)		EPS010	800,088,702	2	3	\$428,500	\$300	\$0		\$428,800	
FAMISANAR		EPS017	830,003,564	7	10	\$1,821,300	\$1,200	\$0		\$1,822,500	
FOSYGA		MIN001	901,037,916	1	8	\$3,527,600	\$2,300	\$0		\$3,529,900	
FOSYGA RÉGIMEN DE EXCEPCIÓN		MIN002	901,037,916	1	1	\$200,000	\$200	\$0		\$200,200	
NUEVA E.P.S.		EPS037	900,156,264	2	6	\$1,096,300	\$700	\$0		\$1,097,000	
SALUD TOTAL		EPS002	800,130,907	4	9	\$1,255,600	\$800	\$0		\$1,256,400	
SANITAS		EPS005	800,251,440	6	36	\$25,879,700	\$16,300	\$0		\$25,896,000	
ICBF (ADMINISTRADORAS: 1)					10	\$5,928,200	\$3,800	\$0		\$5,932,000	
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR		PAICBF	899,999,239	2	10	\$5,928,200	\$3,800	\$0		\$5,932,000	
SENA (ADMINISTRADORAS: 1)					10	\$3,952,000	\$2,500	\$0		\$3,954,500	
SENA		PASENA	899,999,034	1	10	\$3,952,000	\$2,500	\$0		\$3,954,500	
TOTAL					93	\$170,873,200	\$108,300	\$0		\$170,981,500	

DATOS GENERALES DEL APORTANTE								
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Dirección	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
2025-02	2025-03	1343477422	9483214244	E	2025/03/17	2025/03/17	BANCO BBVA COLOMBIA S.A.	\$40,582,700

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES												PENSION		SALUD		CCF		RIESGOS		PARAFISCALES							
No.	Identificación	Nombre	ing	ret	tdc	tae	tdp	tap	vsp	cor	vst	sin	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (31 Afiliados)																														

Centro de Trabajo: CENTRO TRABAJO 1 (30 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	Planilla	Limite	Pago	Banco	Dias Mora	Valor	
2025-02	2025-03	1343477422	9483214244	E	2025/03/17	2025/03/17	BANCO BBVA COLOMBIA S.A.	0	\$40,582,700	

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				31	\$25,581,300	\$0	\$0	\$25,581,300
COLFONDOS	231001	800,227,940	6	3	\$2,648,200	\$0	\$0	\$2,648,200
COLPENSIONES	25-14	900,336,004	7	7	\$8,188,800	\$0	\$0	\$8,188,800
PORVENIR	230301	800,224,808	8	13	\$7,791,900	\$0	\$0	\$7,791,900
PROTECCION	230201	800,229,739	0	7	\$5,762,400	\$0	\$0	\$5,762,400
SKANDIA	230901	800,253,055	2	1	\$1,190,000	\$0	\$0	\$1,190,000
ARL (ADMINISTRADORAS: 1)				31	\$865,000	\$0	\$0	\$865,000
COLMENA	14-25	800,226,175	3	31	\$865,000	\$0	\$0	\$865,000
CCF (ADMINISTRADORAS: 1)				31	\$6,200,100	\$0	\$0	\$6,200,100
COMPENSAR	CCF24	860,066,942	7	31	\$6,200,100	\$0	\$0	\$6,200,100
EPS (ADMINISTRADORAS: 9)				31	\$7,288,500	\$0	\$0	\$7,288,500
CAPITAL SALUD	EPSC34	900,298,372	9	1	\$130,800	\$0	\$0	\$130,800
COMPENSAR	EPS008	860,066,942	7	6	\$954,500	\$0	\$0	\$954,500
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	2	\$286,700	\$0	\$0	\$286,700
FAMISANAR	EPS017	830,003,564	7	4	\$783,000	\$0	\$0	\$783,000
FOSYGA	MIN001	901,037,916	1	2	\$620,000	\$0	\$0	\$620,000
NUEVA E.P.S.	EPS037	900,156,264	2	3	\$322,000	\$0	\$0	\$322,000
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	\$159,200	\$0	\$0	\$159,200
SALUD TOTAL	EPS002	800,130,907	4	5	\$805,600	\$0	\$0	\$805,600
SANITAS	EPS005	800,251,440	6	7	\$3,226,700	\$0	\$0	\$3,226,700
ICBF (ADMINISTRADORAS: 1)				1	\$388,700	\$0	\$0	\$388,700
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	1	\$388,700	\$0	\$0	\$388,700
SENA (ADMINISTRADORAS: 1)				1	\$259,100	\$0	\$0	\$259,100
SENA	PASENA	899,999,034	1	1	\$259,100	\$0	\$0	\$259,100
TOTAL				31	\$40,582,700	\$0	\$0	\$40,582,700

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

Acta N°	24	Tema:	Reunión de revisión de ANS, contrato 173 de 2023
Fecha:	13/02/2025	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 22/12/2024 a 21/01/2025		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	Dependencia	Cargo	¿Asistió?
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 03	Si
Jaime Alejandro Becerra	Apoyo a la Supervisión CTO 173-2023	Profesional 03	Si
Juan Carlos Alarcón S.	Mnemo	Gerente de Proyecto Mnemo	Si
Maria Camila Vargaz	Mnemo	Apoyo a gerencia de proyecto Mnemo	SI

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

Revisión cumplimiento de ANS del período del 22 de diciembre de 2024 al 21 de enero de 2025.

De manera conjunta, el FNA y Mnemo, verificaron cada uno de los siguientes niveles de servicio para la actividad desarrollada.

2. Acuerdos de niveles de servicio generales

2.1. Documentación

Durante el periodo evaluado se entregaron los siguientes documentos:

- Informe mensual de gestión del 22 de diciembre de 2024 al 21 de enero de 2025.
- 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.

2.2. Cumplimiento del sistema de gestión de calidad

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

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.

1.2. 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

2.3. Atención de casos de soporte

Para el tiempo cubierto por la presente revisión, se generaron 12 peticiones de soporte.

PETICIONES (Informe técnico Darktrace numeral 7.2)

Número	Estado	Título
RF418767	Closed	CORREO RETENIDO // KMORENOD, PAGINAS WEB A MITAD DE PRECIO
RF419034	Closed	VALIDACION DE CORREO ELECTRONICO FRAUDE- NO CORRESPONDE AL FONDO NACIONAL DEL AHORRO
RF419475	Closed	RV: PÓLIZAS FNA
RF419710	Closed	RV: CORREO RETENIDO // FWD: ESCRITURA
RF419844	Closed	RV: CONSOLIDACION DE CESANTIAS 2024
RF420133	Closed	RV: CORREO RETENIDO // NOTIFICA SENTENCIA TUTELA
RF420456	Closed	CORREO RETENIDO // NOTIFICACI
RF420783	Closed	RV: CESANTES MES DE NOV
RF420826	Closed	CORREO CONTACTENOS ARCHIVO BLOQUEADO POR POLÍTICAS
RF420897	Closed	ARCHIVO DE CORREO EXTERNO BLOQUEADO POR ANTIVIRUS
RF421048	Closed	RV: CORREO RETENIDO // ESPERANDO EL PAGO
RF421301	Closed	CONSOLIDADO CESANTIAS 2024

CAMBIOS (Informe técnico Darktrace numeral 7.1)

No se generaron cambios en el periodo.

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

2.4. Cumplimiento del cronograma

El avance en el cronograma del contrato 173-2023 para el periodo en cuestión, a corte de 21-01-25, corresponde al 6% esperado vs 6% completado, sin que se presente desviación general.

Cronograma de actividades antes de la adición de nuevas funcionalidades

% completado	% completado esperadoT1	Nombre de tarea	Duración	Comienzo	Fin	Pre
61%	61%	▲ 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	
61%	61%	▲ Fase de ejecución	556 días	vie 22/12/23	jue 29/01/26	
100%	100%	▷ Implementación de la unidad de ciberseguridad	80 días	jue 8/02/24	mar 28/05/24	
48%	48%	▷ Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25	
48%	48%	▷ 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	
33%	33%	▷ 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	
100%	100%	▷ Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24	
52%	52%	▷ Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26	
50%	50%	▷ Fase de monitoreo y control	509 días	dom 28/01/24	mar 30/12/25	
0%	0%	▷ Fase de cierre	75 días	mié 1/10/25	mar 13/01/26	

Cronograma de control y seguimiento con las nuevas tareas asociadas a las nuevas funcionalidades

i	% completado	% completado esperadoT1	Nombre de tarea	Duración	Comienzo	Fin	P
	6%	6%	▲ FNA 173 2023	266 días	dom 22/12/24	lun 22/12/25	
	88%	88%	▷ Fase de planeación	25 días	dom 22/12/24	jue 23/01/25	
	6%	6%	▲ Fase de operación	266 días	dom 22/12/24	lun 22/12/25	
	7%	7%	▲ Operación herramientas actuales	266 días	dom 22/12/24	lun 22/12/25	
	7%	7%	▷ Opeación SIEM	266 días	dom 22/12/24	lun 22/12/25	
	7%	7%	▷ Operación DAM	266 días	dom 22/12/24	lun 22/12/25	
	7%	7%	▷ Operación IAM	266 días	dom 22/12/24	lun 22/12/25	
	3%	3%	▷ Operación TrendMicro	266 días	dom 22/12/24	lun 22/12/25	
	8%	8%	▷ Operación y monitoreo Qualys	266 días	dom 22/12/24	lun 22/12/25	
	8%	8%	▷ Operación y monitoreo Darktrace	266 días	dom 22/12/24	lun 22/12/25	
3	8%	8%	▷ Operación y monitoreo WAF	266 días	dom 22/12/24	lun 22/12/25	
3	8%	8%	▷ Operación y monitoreo InfoBlox	266 días	dom 22/12/24	lun 22/12/25	
8	9%	9%	▷ Análisis de vulnerabilidades y ETH	266 días	dom 22/12/24	lun 22/12/25	
	0%	0%	▷ Ingeniería social	63 días	jue 25/09/25	vie 19/12/25	
3	0%	0%	▷ Ataque cibernético	18 días	lun 6/10/25	mié 29/10/25	
3	8%	8%	▷ Vigilancia Digital	266 días	dom 22/12/24	lun 22/12/25	
3	0%	0%	▲ Operación herramientas adición 2025	214 días	lun 3/03/25	lun 22/12/25	
3	0%	0%	▷ Cyber Analítica - Data Fabric	214 días	lun 3/03/25	lun 22/12/25	
1	0%	0%	▷ IPAM	187 días	mar 8/04/25	lun 22/12/25	
3	0%	0%	▷ ASM & IE	193 días	lun 31/03/25	lun 22/12/25	
5	0%	0%	▷ MAS	196 días	mié 26/03/25	lun 22/12/25	
7	0%	0%	▷ CyberArk PAM	201 días	jue 20/03/25	lun 22/12/25	
3	4%	4%	▲ Servicios de consultoría	266 días	dom 22/12/24	lun 22/12/25	
3	5%	5%	▷ Integración del UCS a los procedimientos de SI del FNA	266 días	dom 22/12/24	lun 22/12/25	
1	0%	0%	▷ Hallazgos y recomendaciones de auditoría	243 días	mié 22/01/25	lun 22/12/25	
1	0%	0%	▷ Seguimineto quincenal	225 días	jue 6/02/25	jue 11/12/25	
5	0%	0%	▷ Fase de cierre	7 días	vie 12/12/25	lun 22/12/25	

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

A partir del periodo 22 de enero de 2025, el cronograma de proyecto presentará las tareas unificadas de la planificación inicial y la adición, por lo tanto el calculo de avance real y porcentaje completado de tareas reflejará una disminución debido a la adición de nuevas tareas y sus esfuerzos asociados.

2.5. Disponibilidad de Plataformas

2.5.1. 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



2.5.2. 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
99,80% de disponibilidad.	Disponibilidad igual o superior a 99,80%	0	0	0	Ninguna

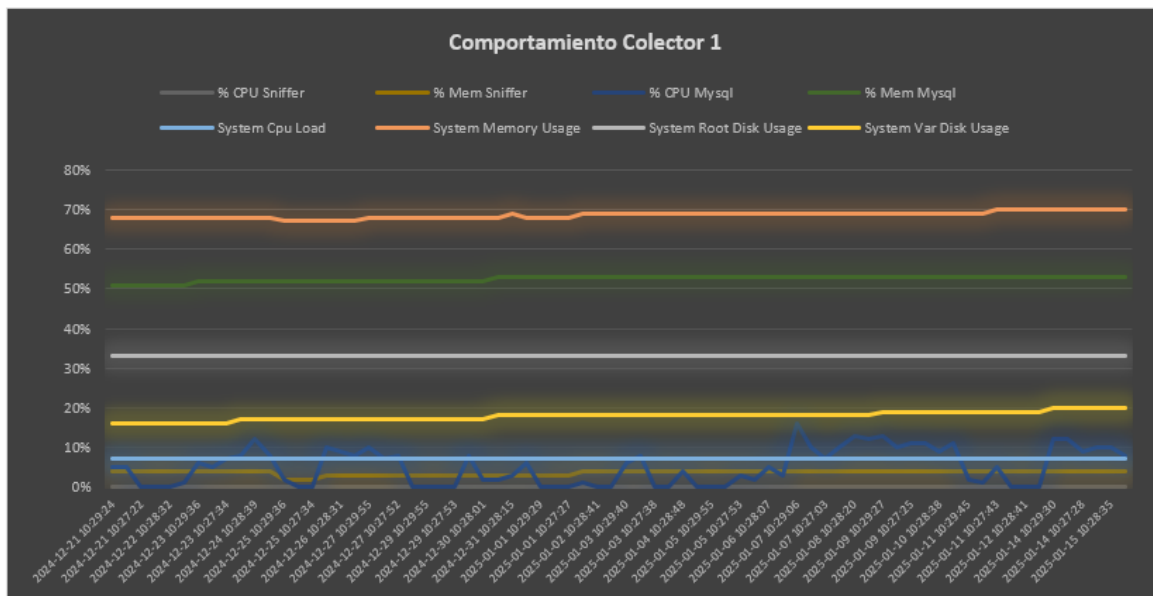
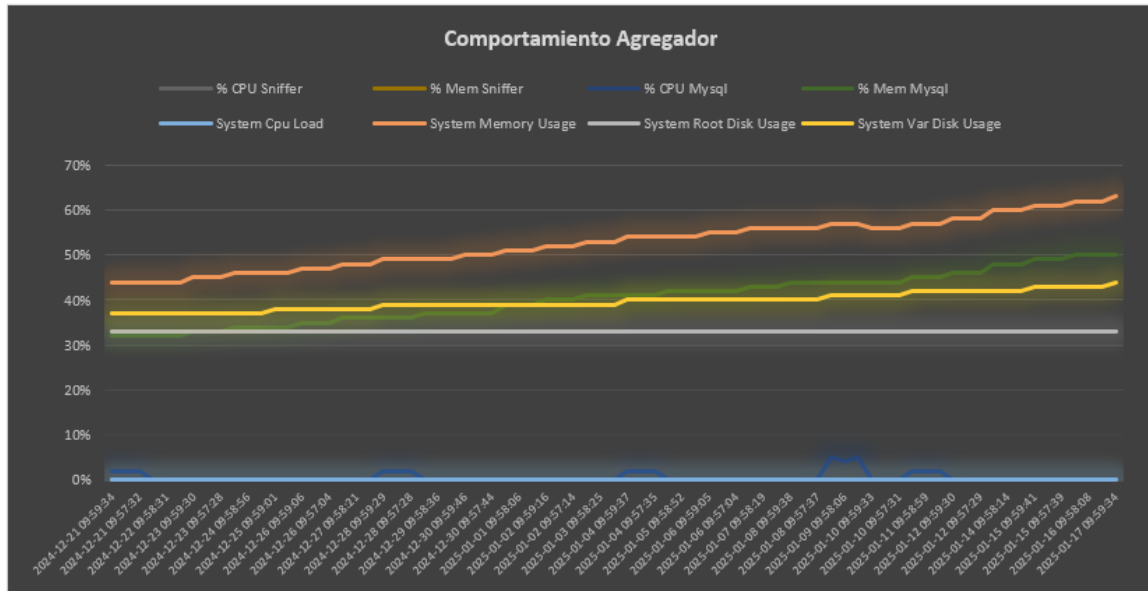


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



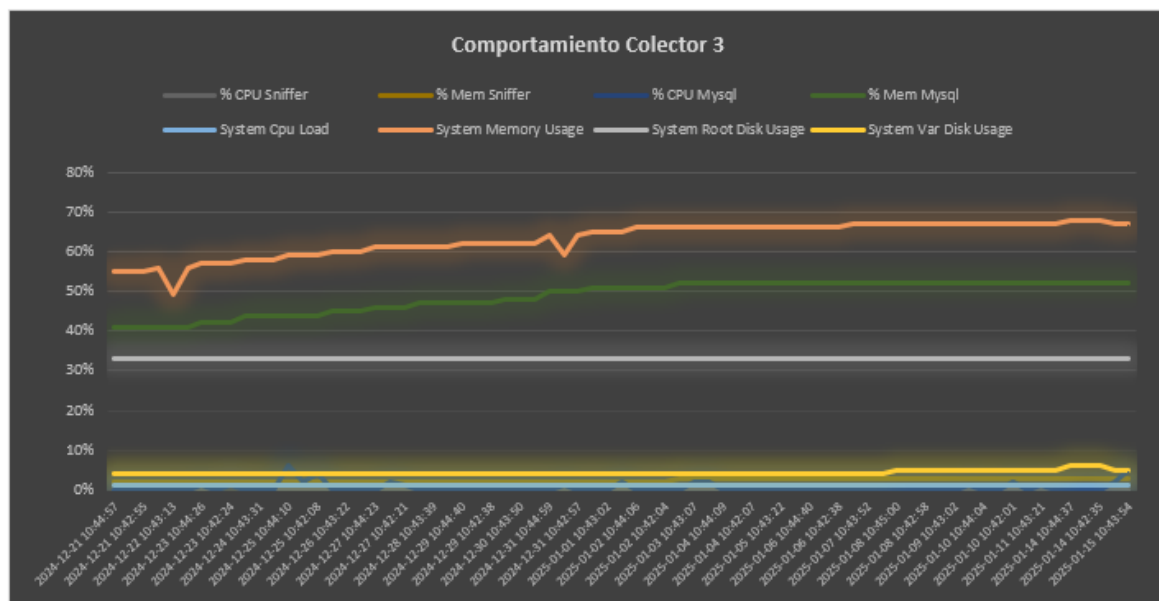
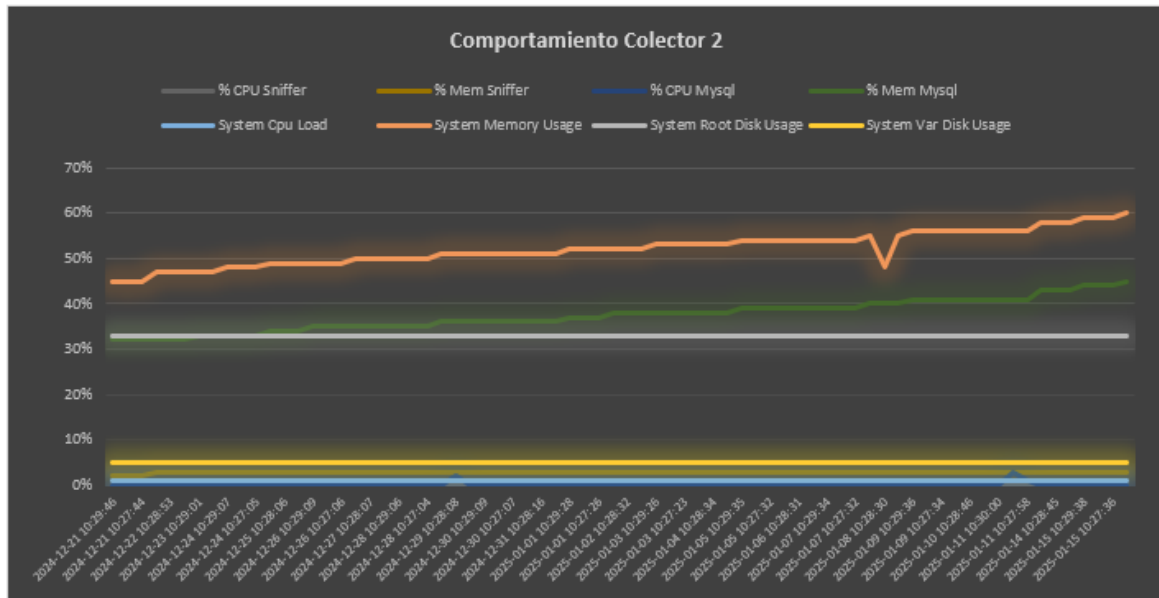


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



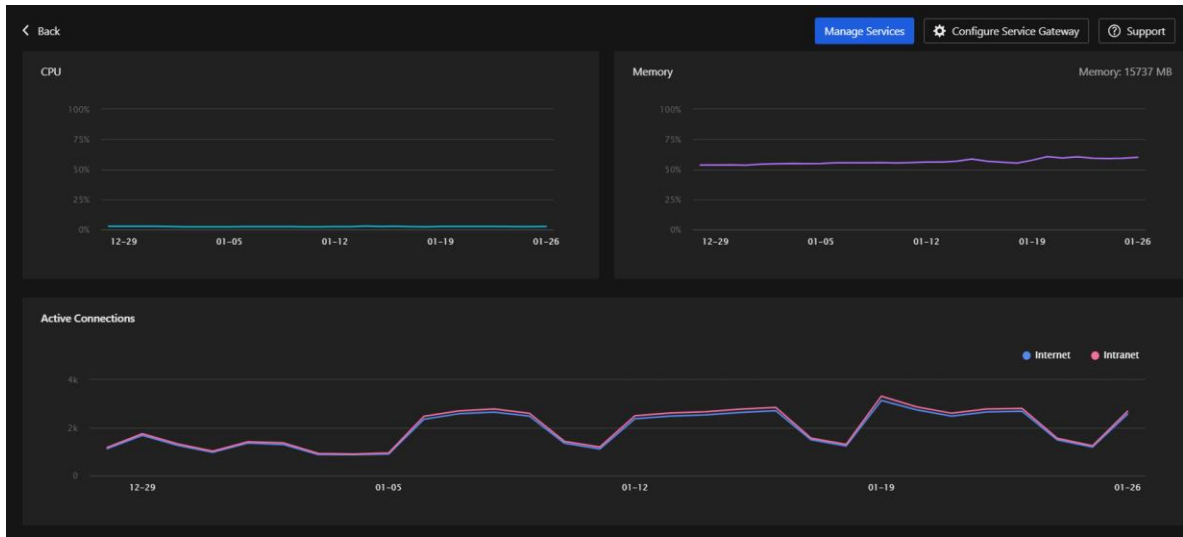
2.5.3. Disponibilidad solución Antimalware

3. Disponibilidad de la plataforma ANTIMALWARE

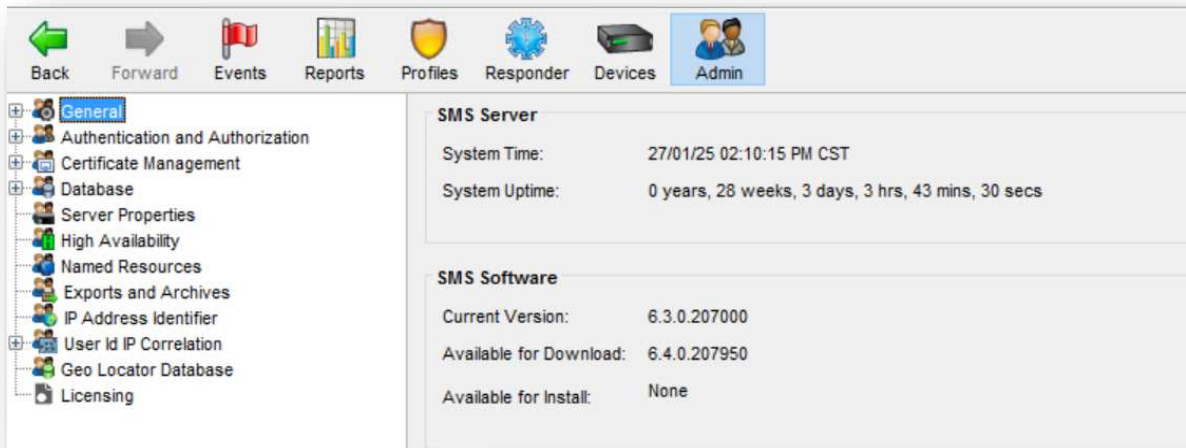
Garantizar la disponibilidad y acceso a los servicios ofrecidos por las plataformas Antimalware

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

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



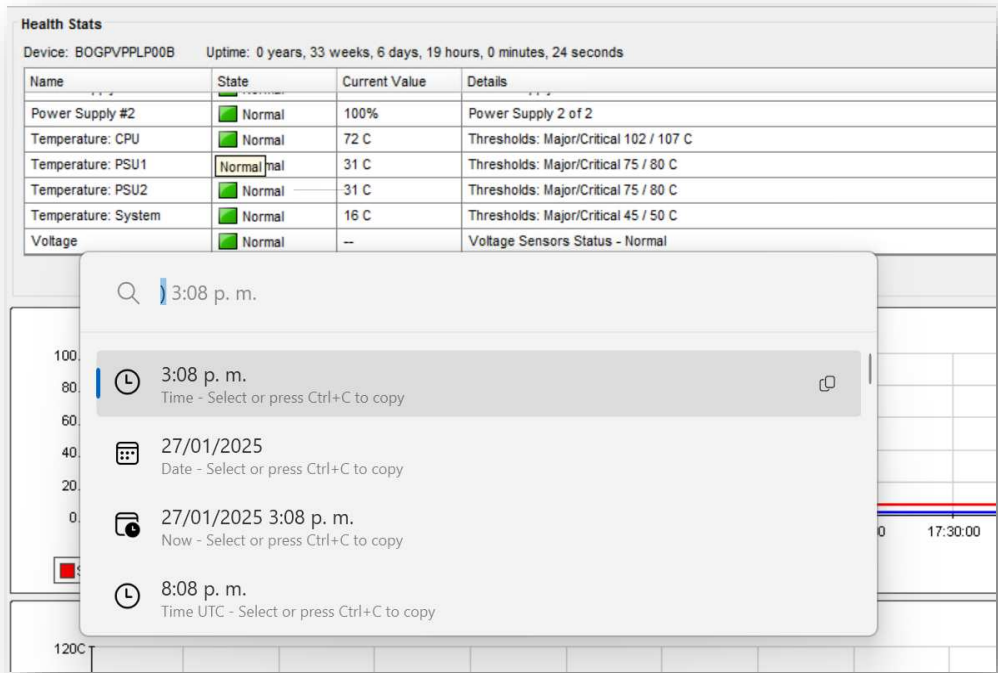
1. *Imagen de conexiones durante el periodo.*



The screenshot shows the 'Admin' section of the SMS Server console. The left sidebar lists various configuration options, with 'General' selected. The main panel displays the following information:

- SMS Server:**
 - System Time: 27/01/25 02:10:15 PM CST
 - System Uptime: 0 years, 28 weeks, 3 days, 3 hrs, 43 mins, 30 secs
- SMS Software:**
 - Current Version: 6.3.0.207000
 - Available for Download: 6.4.0.207950
 - Available for Install: None

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



2.5.4. Disponibilidad Plataformas de Correlación SIEM

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

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

```

root@fnabogapp100:/root
[root@fnabogapp100 ~]# last | grep root
root      pts/0        172.19.4.66    Mon Jan 27 09:41    still logged in
root      pts/0        172.19.4.66    Tue Jan 21 18:45 - 11:33 (2+16:48)
root      pts/0        10.87.61.56    Mon Jan 20 01:05 - 01:22 (00:16)
root      pts/0        10.87.61.56    Mon Jan 20 00:56 - 01:04 (00:07)
root      pts/0        172.19.4.66    Mon Jan 13 15:20 - 18:04 (02:44)
root      pts/0        10.87.61.56    Sun Jan 12 18:15 - 19:52 (01:37)
root      pts/0        10.87.61.56    Sun Jan 12 17:39 - 18:13 (00:34)
root      pts/0        10.87.61.56    Sun Jan 12 16:45 - 17:17 (00:31)
root      pts/1        172.19.4.66    Sun Jan 12 13:03 - 11:03 (21:59)
root      pts/0        172.19.4.66    Sun Jan 12 12:57 - 13:17 (00:20)
root      pts/0        172.19.4.66    Sun Jan 12 12:52 - down (00:01)
root      pts/1        172.19.4.66    Thu Jan  2 17:12 - 09:22 (1+16:09)
root      pts/0        172.19.4.66    Thu Jan  2 14:51 - 17:12 (02:21)
root      pts/0        172.19.4.66    Thu Jan  2 14:42 - 14:51 (00:08)
root      pts/1        10.87.61.56    Thu Jan  2 13:33 - 15:57 (02:23)
root      pts/1        10.87.61.56    Thu Jan  2 13:30 - 13:32 (00:02)
root      pts/1        10.87.61.56    Thu Jan  2 13:29 - 13:30 (00:00)
root      pts/0        172.19.4.66    Thu Jan  2 12:00 - 14:42 (02:42)
root      pts/0        172.19.4.66    Fri Dec 27 15:54 - 18:04 (02:09)
root      pts/0        172.19.4.66    Thu Dec 26 17:26 - 01:56 (08:29)
root      pts/0        172.19.4.66    Wed Dec 18 09:16 - 15:15 (05:59)
root      pts/0        172.19.4.66    Wed Dec 11 18:51 - 10:09 (5+15:18)
root      pts/0        10.87.61.56    Wed Dec 11 09:18 - 10:06 (00:47)
root      pts/2        10.87.61.56    Wed Dec 11 07:47 - 09:12 (01:24)
root      pts/0        10.87.61.56    Wed Dec 11 07:42 - 09:12 (01:30)
root      pts/2        10.87.61.56    Wed Dec 11 06:20 - 07:05 (00:45)
root      pts/0        10.87.61.56    Wed Dec 11 06:15 - 07:19 (01:03)
root      pts/0        10.87.61.56    Wed Dec 11 06:06 - 06:10 (00:04)
root      pts/2        10.87.61.56    Wed Dec 11 04:20 - 05:50 (01:30)
root      pts/0        10.87.61.56    Wed Dec 11 04:13 - 05:51 (01:37)
root      pts/2        10.87.61.56    Wed Dec 11 03:13 - 04:09 (00:56)
root      pts/2        10.87.61.56    Wed Dec 11 02:02 - 03:12 (01:10)
root      pts/0        10.87.61.56    Wed Dec 11 01:45 - 04:09 (02:24)
root      pts/0        10.87.61.56    Wed Dec 11 01:19 - down (00:22)
root      pts/0        172.19.4.66    Mon Dec  9 09:28 - 09:37 (00:09)
root      pts/0        10.87.61.56    Sun Dec  8 22:30 - 22:32 (00:01)
root      pts/0        172.19.4.66    Fri Dec  6 08:58 - 18:54 (09:55)
root      pts/0        10.87.61.56    Wed Dec  4 05:14 - 05:25 (00:10)
root      pts/0        172.19.4.66    Fri Nov 29 10:30 - 15:24 (04:54)
root      pts/0        172.19.4.66    Mon Nov 25 16:37 - 10:38 (18:00)
root      pts/2        172.19.4.66    Sun Oct 27 20:02 - 15:20 (2+19:18)
root      pts/1        172.19.4.66    Fri Oct 25 15:34 - 15:04 (3+23:30)
root      pts/0        172.19.4.66    Thu Oct 24 18:40 - 15:04 (4+20:23)

```

2.5.5. Disponibilidad Secure Development Assesment (Fortify)

Fortify – 172.16.132.101

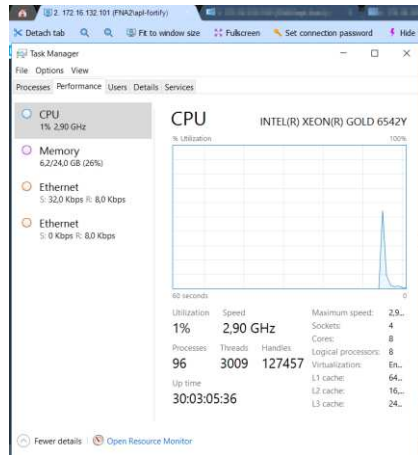


FORMATO ACTA DE REUNIÓN

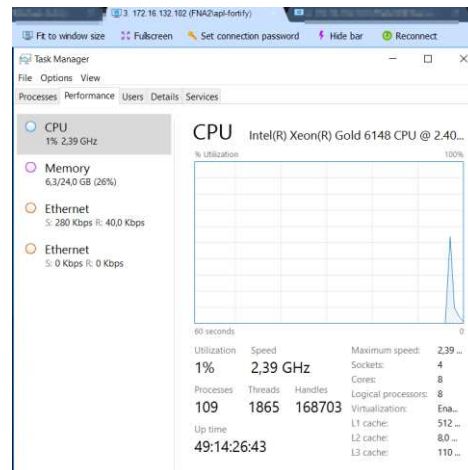
Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

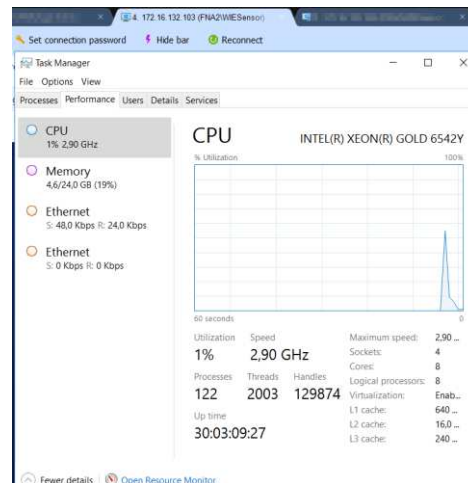
Versión: 0



Fortify – 172.16.132.102

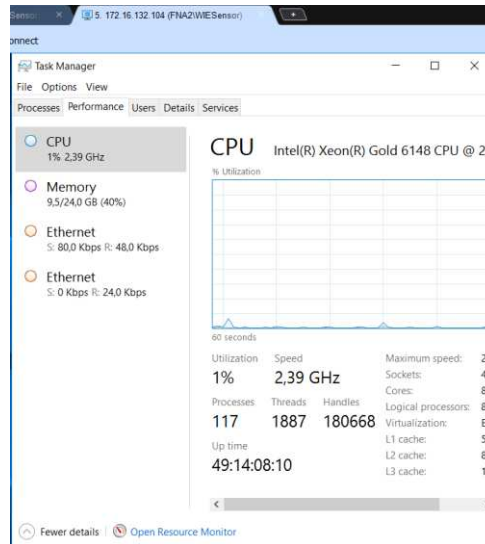


Fortify – 172.16.132.103



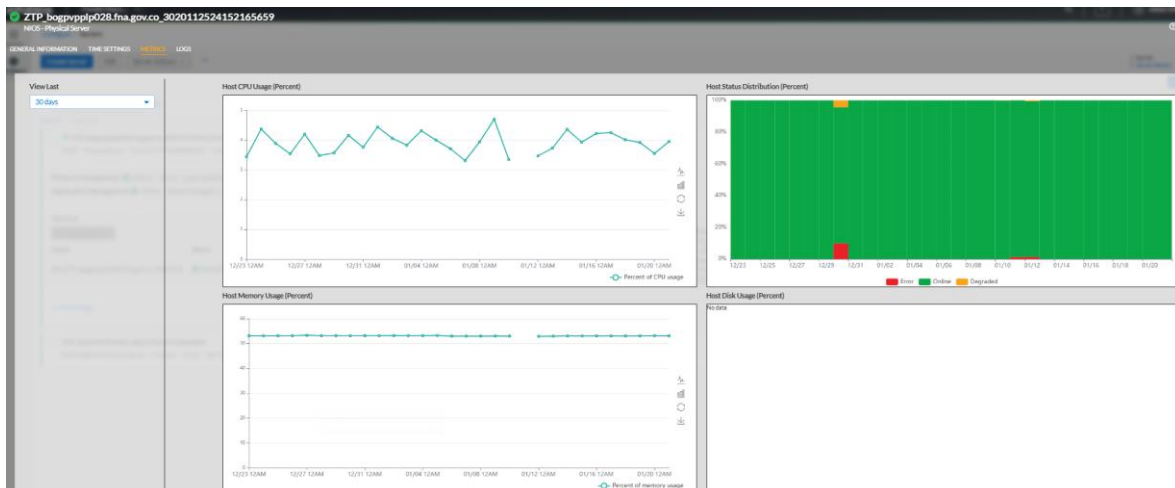
Fortify – 172.16.132.104

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



2.5.6. Disponibilidad monitoreo especiales DNS

☐	 ZTP_bogvpplp028.fna.gov.co_302011252415216...	 Online
NIOS Physical Server 8.6.4-51177-72c485de7d02 License UID: 3c1e361631384fdf9a58f448f6fc07e5		
☐	ZTP_BOGPVPLP029_6661976453710046849	 Online
NIOS-X (BloxOne) Virtual Server VMware v5.4.6 SN: VMware-42 00 6e cf d8 da a8 ff-7b 91 15 23 01 06 b2 55		



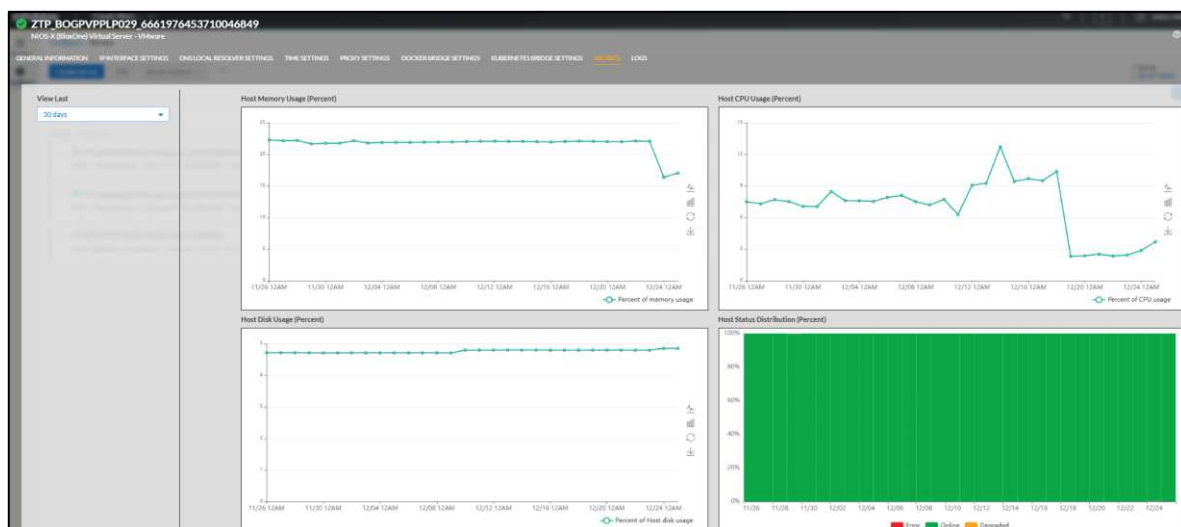
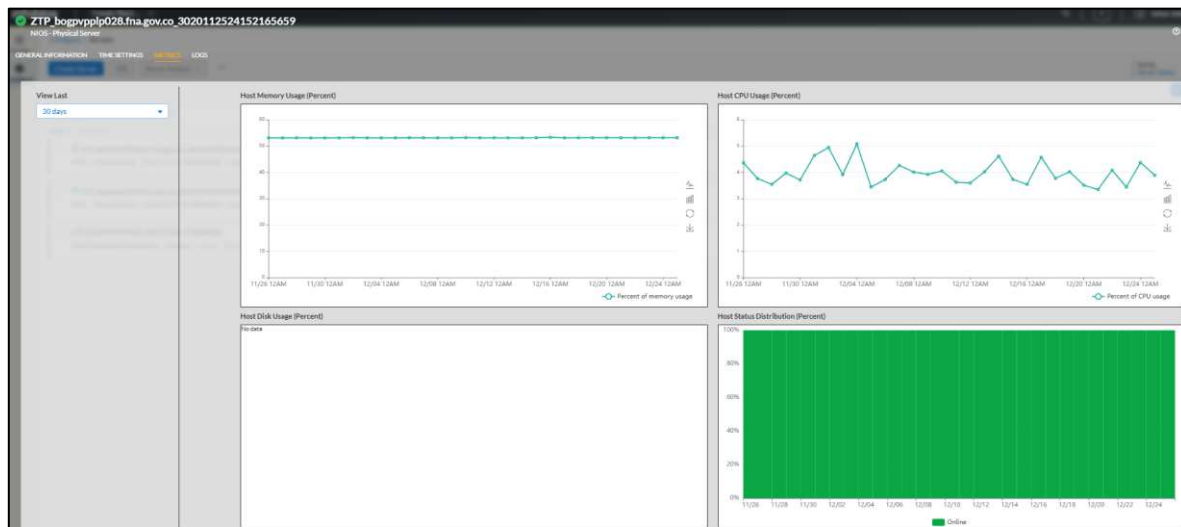
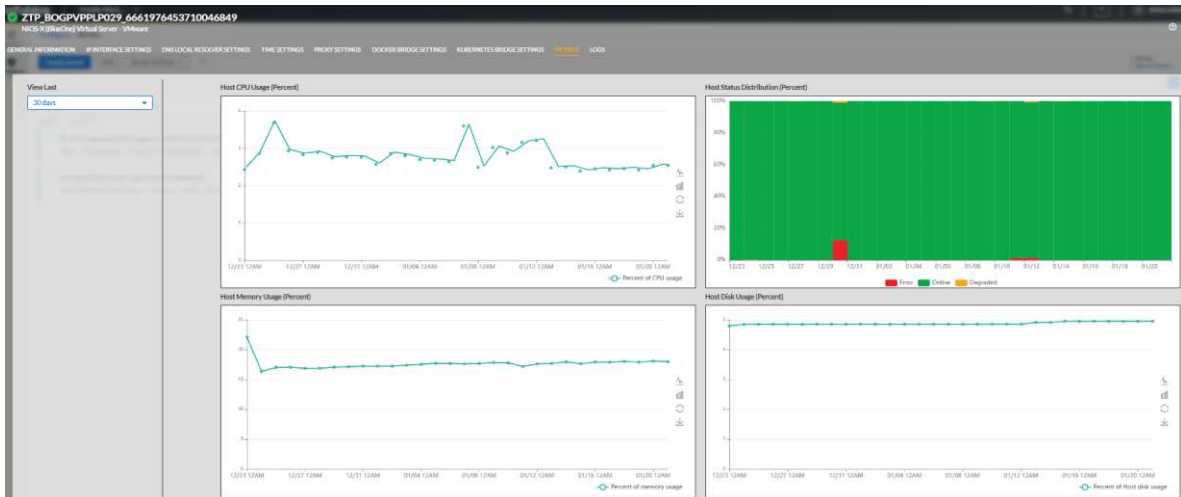


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



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

2.5.7. Disponibilidad monitoreo especiales Portales Web

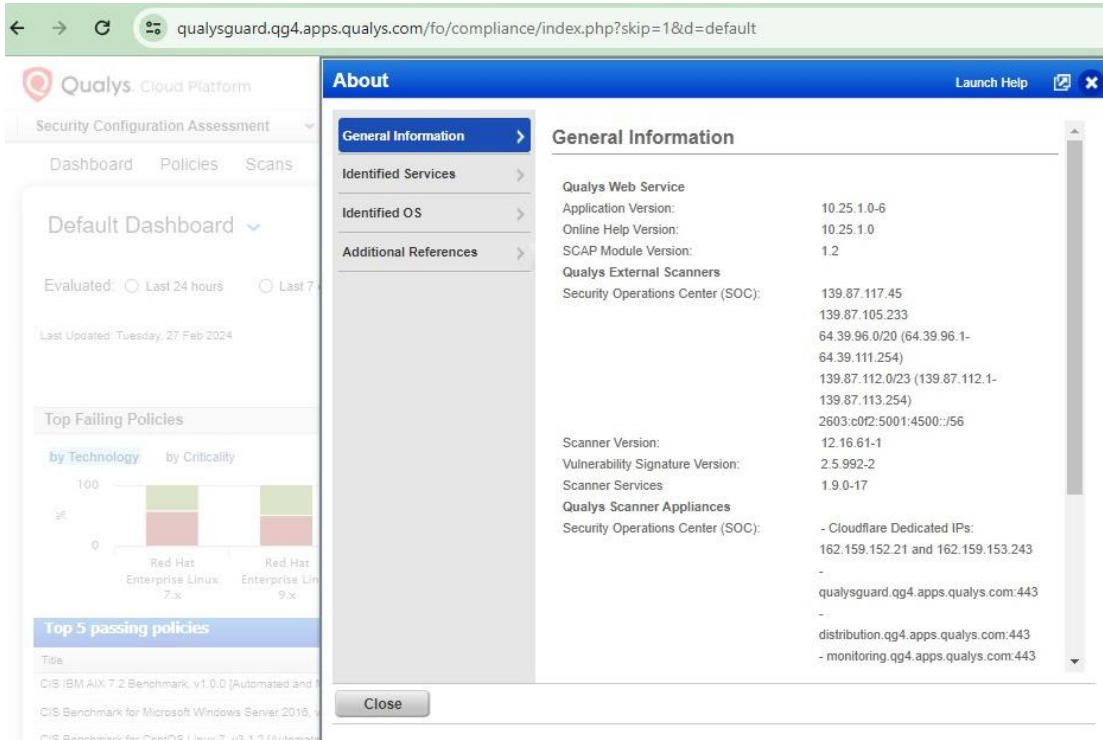
Unit	Status	HA Role	Up Time	CPU Usage	Memory Usage	Log Disk Usage	HTTP Connections	HTTP Throughput
FV-1KET119900223		PRIMARY	257 days 10 hours 8 minutes				Total Connections: 1748 Total Connections/Sec: 62	Throughput: 104.506 Mbps
FV-1KET119900233		SECONDARY	257 days 10 hours 9 minutes				Total Connections: 0 Total Connections/Sec: 0	Throughput: 0.000 Kbps

System Information		  
HA Status	Active-Passive	
Cluster Name	FWHA01	
Cluster Members	FortiWeb/ FV-1KET119900223 (Primary) MASTERFWEB/ FV-1KET119900233 (Secondary)	
Serial Number	FV-1KET119900223	
Operation Mode	Reverse Proxy	
System Time	Wed Jan 22 08:03:51 2025	
Firmware Version	FortiWeb-1000E 7.4.3,build0638(GA),240405	
System Uptime	[257 day(s) 10 hour(s) 7 min(s)]	

2.5.8. 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

	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.:

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

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

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 Pre-factura 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.

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.

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

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

Durante el periodo no se evidenció la materialización de los riesgos identificados dentro de la matriz de riesgos del proyecto, consignados en el formato PE-FO-102.

Se relaciona a continuación la matriz de riesgos del proyecto.

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

		*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****										*****									
--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--	-------	--	--	--	--	--	--	--	--	--

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

COMPROMISOS PACTADOS	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO	FECHA DE CUMPLIMIENTO DEL COMPROMISO
Realizar los ajustes en el cronograma general del proyecto para reflejar la inclusión de las nuevas tareas y recalcular líneas base	Juan Carlos Alarcon S.	22/febrero/2025	N/A

APROBÓ	APROBÓ
 Juan Carlos Alarcon Gerente de Proyecto Mnemo Colombia S.A.S.	 Enrique Arrázola Apoyo a la supervisión 173-2023 Gerencia de Estrategia de TI y Aseguramiento Informático
 Jaime Alejandro Becerra Apoyo a la Supervisión contrato C173-2023	

SUPERVISIÓN AL CONTRATO No. 173 de 2023
FONDO NACIONAL DEL AHORRO
Informe No. 27

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), solución GOBIERNO DE IDENTIDADES (IAM) y SOAR del periodo comprendido del 22 de diciembre de 2024 al 21 de enero de 2025.

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

Bogotá, D.C. marzo de 2025

1. INTRODUCCIÓN

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

2. RESUMEN EJECUTIVO

En cumplimiento al apoyo a la supervisión asignada por la 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 diciembre de 2024 al 21 de enero de 2025** referente al **13vo** 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
10. Solución GOBIERNO DE IDENTIDADES (IAM)

Y 2do ejercicio de Análisis de vulnerabilidades obligatorio del año 2024, al total de activos de la plataforma tecnológica.

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 diciembre de 2024 al 21 de enero de 2025**, donde se detalla lo siguiente:

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

1. XDR / ANTIMALWARE

- Se realiza una validación del scoring de indicadores de compromiso, que permite a la herramienta priorizar indicadores de compromiso, dependiendo de las fuentes campañas y criticidad de la amenaza, entregando mejores indicadores de compromiso, actualizados y con el contexto necesario para que su bloqueo evite compromisos y daños a la seguridad de la información de la entidad.
- Se han validado indicadores de compromiso cargados por la TIP a la herramienta XDR, validando la efectividad del bloqueo en los equipos de la entidad.
- Se realizan ajustes en las fuentes de datos que entregan indicadores de compromiso a la herramienta, priorizando fuentes que contienen información de valor para el sector empresarial y el entorno geográfico.
- Se han agregado indicadores de compromiso de manera manual, teniendo en cuenta aquellos indicadores que no se han tenido en cuenta por parte de otras fuentes de datos, aprovechando las capacidades de Threat Hunting del equipo de ciber inteligencia de amenazas.
- Creación cambio C66791 permisos ZTNA, con el fin de continuar con las tareas de prueba para la implementación de la solución de proxy cloud.
- Caso escalado con fabricante para la integración de la solución de workmanager aplicación de terceros, con el sandbox DDAN, se encuentra en pruebas debido a errores al enviar las muestras.

-
- Se realiza sesión con Media commerce, redes LAN y administradores de servicios de red, debido a que se está realizando migración de administrador de ancho de banda, el cual está conectado como destino del primer par de inspección del IPS, se concertó arquitectura para la migración pendiente de pruebas por parte de redes y nosotros para validación del tráfico.
 - Es necesario realizar la validación de la regla HIFRM6 ya que genera bastantes eventos sobre archivos pdf, registrados como archivos con objetos embebidos específicamente para el usuario MMedinaL y mrojasm.
 - Se detectaron 26 aplicaciones nuevas por Behavior Monitoring, estas alimentan la base de datos de application control, se sugiere validar aplicaciones nuevas para ser ingresadas dentro de App Control.
 - En la cantidad de dispositivos no autorizados conectados. Se encuentra dispositivos móviles 1937 eventos y 149 dispositivos USB.
 - Actualmente se encuentran 18 usuarios con permisos para el uso de dispositivos. • Workbench genero las siguientes alertas:
 - La ejecución de Deletion of Volume Shadow Copies, se registra como una alerta debido a que puede ser utilizado por ransomware, en este caso es válido por parte de los administradores.
 - El evento que mayor cantidad de registros muestra, es la ejecución de comando PowerShell
"C:\Windows\system32\windowspowershell\v1.0\powershell.exe" -Command Set-MpPreference -DisableRealtimeMonitoring \$true este no afecta al antivirus de Trend Micro ya que intenta desactivar Windows Defender.
 - Possible Account Compromise - Impossible Travel: Hace referencia a conexiones distantes una de otra en un tiempo muy corto por lo que resulta sospechoso, The user (jbalantac@fna.gov.co) has successfully signed in from (CO) (3.7231,-75.4832) and (MX)(16.75838,-93.11016)). The short time difference indicates a possible account compromise.
 - Es necesario realizar validación con SOC, para creación de casos de uso que alerte automáticamente los eventos generados por WorkBench ya que solamente se están generando alertas por el evento de posibles intentos de desactivación de antivirus.
 - Se registran 4 eventos en servidores, relacionados con los servidores FNABOGCLM y BOGPVPPWP0B0, por la ejecución de las aplicaciones PdfCompressorService.exe y MeshAgent.exe respectivamente. Para la solución de servidores, se encuentran módulos adicionales, como app control, activity monitoring y log inspection que puede ser habilitada.
 - La solución de IPS para servidores, registro 3820 eventos, El evento que mayor cantidad de registros género es Retransmit. Se continuará con la validación de las reglas para activar o desactivarlas en caso de ser necesarias.

-
- En el top de dispositivos con mayor cantidad de eventos de host, se encuentra FNABOGMP2, por eventos de retransmisión, descartados por el módulo de firewall con origen el servidor FNABOGPBVL.
 - para los módulos de IPS y Firewall para servidores, los eventos que mayor cantidad de eventos registraron fueron los relacionados con los servicios de DNS y LDAP.
 - Para IPS en servidores las siguientes reglas estuvieron en el top de eventos: Evento 1011843 (Django): Un atacante puede sobrecargar servidores Django enviando solicitudes maliciosas. Actualiza Django y utiliza WAF para mitigarlo.
 - Evento 1008555 (Active Directory): Un atacante puede interrumpir funciones críticas de red explotando solicitudes LDAP maliciosas. Actualiza Windows y configura adecuadamente el servicio LDAP.
 - La solución de Inteligencia de amenazas registra 42 reputaciones nuevas.
 - Attack Surface Discovery se registra los servidores bogvpplp019 y bogvpplp015, con 87 vulnerabilidades y fallos en la configuración, con clasificación alta.
 - Attack Surface Discovery la página con clasificación más alta es agendamiento.fna.gov.co con una clasificación media
 - Attack Surface Discovery, la cuenta con mayor riesgo identificada es Centro de Monitoreo, esto debido a que se encuentra identificada dentro de una base de datos como expuesta.
 - Para las aplicaciones Cloud y local identificadas por Attack Surface Discovery, se recomienda realizar la validación si es necesario incluir alguna dentro de las aplicaciones bloqueadas.
 - IPS, registro 100381 eventos en su mayoría con clasificación Mayor con el 54% de los eventos totales.
 - IPS en el top de ataques se encuentra la regla 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute. y 13012: SIP: SipVicious Brute Force SIP Tool.
 - IPS En el top de IP de origen 185.243.5.55 de Polonia con 14193 eventos.
 - IPS En el top de destino se encuentra la dirección IP 172.16.125.29, con 6761 registros.
 - En el top de eventos por país, se encuentra Estados Unidos con mayor cantidad de registros, seguido de Hong Kong y Rumania. Se recomienda validar la opción de crear reglas de protección por geolocalización.
 - se presentaron un total de 17426 eventos registrados por la solución CASB
 - Protección correo En los eventos por nombre de anomalía, se encuentran correos con rutas compartidas, correos de marketing y correos relacionados con el malware Bazar.

2. THREAT INTELLIGENCE

Actividades de Gestión de la plataforma

- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 54 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.
- 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.
- Se realiza una validación del scoring de indicadores de compromiso, que permite a la herramienta priorizar indicadores de compromiso, dependiendo de las fuentes campañas y criticidad de la amenaza, entregando mejores indicadores de compromiso, actualizados y con el contexto necesario para que su bloqueo evite compromisos y daños a la seguridad de la información de la entidad.
- Se han validado indicadores de compromiso cargados por la TIP a la herramienta XDR, validando la efectividad del bloqueo en los equipos de la entidad.
- Se realizan ajustes en las fuentes de datos que entregan indicadores de compromiso a la herramienta, priorizando fuentes que contienen información de valor para el sector empresarial y el entorno geográfico.
- Se han agregado indicadores de compromiso de manera manual, teniendo en cuenta aquellos indicadores que no se han tenido en cuenta por parte de otras fuentes de datos, aprovechando las capacidades de Threat Hunting del equipo de ciber inteligencia de amenazas.
- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se creó 1 regla Sigma en la que se identifican comportamientos de ejecución de la amenaza StrelaStealer.
- La regla SIGMA identifica la descarga de una librería maliciosa por medio de un archivo JavaScript.
- Se realizaron análisis focalizados sobre las amenazas Arcus Media Ransomware y DarkVision RAT, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.

-
- Durante el periodo reportado, el equipo de CTI Mnemo ha analizado distintos tipos de muestras sospechosas, esto con el fin de encontrar nuevas tácticas y técnicas utilizadas por actores de amenazas para infectar a sus víctimas a través de nuevos y elaborados ejecutables maliciosos.
 - Los ficheros han sido elegidos de amenazas que se encuentran en tendencia, campañas de phishing vistas recientemente en diferentes compañías, y actividades de Threat Hunting llevadas a cabo por el equipo de CTI Mnemo.
 - 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.

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

Observación: Se evidencia una disminución en el volumen de credenciales identificadas para la tipología de credenciales de terceros.

Observación: Se tuvo una efectividad del 74% al momento de realizar las gestiones de baja solicitadas.

4. SECURE DEVELOPMENT ASSESSMENT

Actividades de Gestión de la plataforma Fortify

- Restablecimiento de credenciales de usuario en el dominio de la suite Fortify: A través de la mesa de ayuda, se gestionan y restablecen las credenciales de acceso de los usuarios del dominio, garantizando un acceso seguro y adecuado a la suite Fortify.
- Actualización de Rulespacks del módulo SSC: Se lleva a cabo la actualización periódica de los Rulespacks en el módulo SSC para asegurar

que las reglas de seguridad estén actualizadas, mejorando así la detección de vulnerabilidades y adaptándose a las nuevas amenazas emergentes.

- Actualización de Rulespacks del módulo Audit Workbench: Se realiza la actualización de los Rulespacks en el módulo Audit Workbench, optimizando el análisis de código y permitiendo una evaluación más precisa y eficiente de las aplicaciones auditadas.

5. MONITOREO DNS

Actividades de Gestión de la plataforma INFOBLOX

- Monitoreo de plataforma Infoblox para la verificación de conexiones sospechosas y maliciosas.
- 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 evidenció una disminución de 676 eventos en la categoría de DoHservice en las consultas DNS, para la categoría malware download generic se evidenció una disminución de 1.043 siendo las categorías con más consultas dentro del 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 de información sobre servidores Windows sin reportar en más de un mes
- Solicitud de información sobre servidores AIX sin reportar en más de un mes
- Solicitud de información sobre servidores Linux sin reportar en más de un mes
- identificación de causa de duplicidad de activos
- Generación de reportes de cumplimiento bajo demanda
- Sesiones de entendimiento de plataforma e informes generados

-
- Solicitud de inventario 2025 de dispositivos de red, bases de datos y servidores (Linux, AIX y Windows)
 - Actualización de políticas en plataforma, programación de escaneos y reportes mensuales

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 solicita al area de redes informe de consumo de los días 5,12 y 19 de diciembre, a las siguientes direcciones:
 - 45421590.live.darktracesensor.com
 - cdn.live.darktracesensor.com
- Se genera exclusión para el equipo Almacenamiento ExaGrid - BackUP172.16.125.33, para el modelo Antigena Internal Data Transfer Block .Se realiza cierre del Incidente IM157937, a traves de logs los consumos en otras fechas son las mismas.
- Se genera reporte al área de seguridad de la información para la validación de los correos masivos (172) de remitentes con dominio info1@desarrollo25.email
- Se genera cronograma de actividades y/o mejoras para la administración de la solución de Darktrace
- Se reporta al área de seguridad de la información el correo de la solicitud RF421048, correo con remitente la misma cuenta del destinatario
- 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

- Reporte agente STAP, SAP HANA.
- Solicitud monitoreo agentes.
- Solicitud destinatarios eventos roles COBIS/SAPHANA.
- Alertas SOC.
- Modificación tiempo de retención

9. SOAR

- Para este periodo se identificó un aumento en el alertamiento con respecto al periodo anterior, debido a que se sigue realizando un proceso 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
Directorio Activo	En Pruebas Internas
Trend Micro Vision One	OPERATIVA
FortiWeb	OPERATIVA

10. Solución GOBIERNO DE IDENTIDADES (IAM)

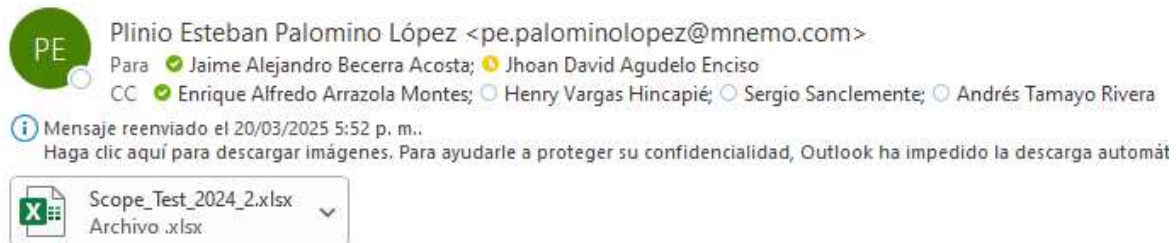
- Para este periodo se continua con el monitoreo de la ejecución de las integraciones con SAP, Directorio activo, Service Manager y la activación de Autogestión en producción para la estabilización y mejora del sistema.
- Se programan reuniones técnicas con los equipos de Administración de Usuario.
- Se solucionan los inconvenientes con la integración de Cobis y se configuran los conectores en producción.

- Se hace el acompañamiento en la prueba de recorrido para la verificación del funcionamiento de la solución de autogestión de contraseñas con resultados satisfactorios.
- Se hace el acompañamiento en la Reunión Prueba de Recorrido Requerimiento RF-ITGCs
- Se siguen realizando las gestiones correspondientes con las áreas involucradas para el proceso de integración hacia Verify con las demás aplicaciones.
- Para el 28 de enero de 2025 se programa el inicio de la capacitación del portal de Autogestión para los funcionarios del FNA.

2do ejercicio de Análisis de vulnerabilidades obligatorio año 2024

- Realización y entrega a la Gerencia de Estrategia de TI y aseguramiento informático del informe correspondiente al 2do semestre de 2024.

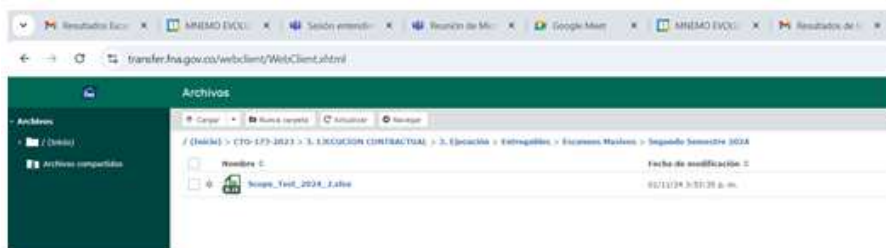
Fwd: Resultados Escaneo Masivo Segundo Semestre



Jaime / Jhoan buenas tardes

Remitimos el resultado del Análisis masivo de vulnerabilidades del segundo semestre.

El mismo queda cargado en Transfer:



- Scope_Test_2024_2
- Matriz de vulnerabilidades _23012025



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

- Informe gerencial FNA AnálisisVuln Masivo II Semestre 2024
- Informe diferencial FNA AnálisisVuln Masivo II Semestre 2024

5.1 INFORMACIÓN DE AVANCE PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 31.243.603.434,00	55,37%
Valor del pago aprobado con el presente informe	\$ 423.428.180,00	0,75%
VALOR TOTAL EJECUTADO	\$ 31.667.031.614,00	56,12%
Porcentaje de ejecución presupuestal programado a la fecha		56,17%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,04%

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 diciembre de 2024 al 21 de enero de 2025**.

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

Porcentaje de ejecución proyectado	61%
Porcentaje de ejecución realizado	61%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	0%

% completado	% completado esperado T1	Nombre de tarea	Duración	Comienzo	Fin	Pro
61%	61%	# 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	
61%	61%	# Fase de ejecución	556 días	vie 22/12/23	jue 29/01/26	
100%	100%	▷ Implementación de la unidad de ciberseguridad	80 días	jue 8/02/24	mar 28/05/24	
48%	48%	▷ Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25	
48%	48%	▷ 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	
33%	33%	▷ 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	
100%	100%	▷ Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24	
52%	52%	▷ Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26	
50%	50%	▷ Fase de monitoreo y control	509 días	dom 28/01/24	mar 30/12/25	
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	\$ 0	\$ 3.326.000	\$ 631.940	\$ 3.957.940
Administración y soporte de la plataforma THREAT INTELLIGENCE (TIP)	\$ 27.797.000	\$ 0	\$ 27.797.000	\$ 5.281.430	\$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	\$ 55.994.000	\$ 0	\$ 55.994.000	\$ 10.638.860	\$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS, Servidor Infoblox 1405 Series, Serial No: 1405202201700334	\$ 52.083.000	\$ 0	\$ 52.083.000	\$ 9.895.770	\$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	\$ 8.279.000	\$ 0	\$ 8.279.000	\$ 1.573.010	\$ 9.852.010
Administración y soporte de la plataforma CIBERDEFENSA	\$ 5.874.000	\$ 0	\$ 5.874.000	\$ 1.116.060	\$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	\$ 8.406.000	\$ 0	\$ 8.406.000	\$ 1.597.140	\$ 10.003.140
Administración y soporte de la plataforma SOAR	\$ 14.627.000	\$ 0	\$ 14.627.000	\$ 2.779.130	\$ 17.406.130
Análisis de Vulnerabilidades (dos (2) obligatorios al año, al total de activos de la plataforma tecnológica)	\$ 129.536.000	\$ 0	\$ 129.536.000	\$ 24.611.840	\$ 154.147.840
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	\$ 23.451.000	\$ 0	\$ 23.451.000	\$ 4.455.690	\$ 27.906.690
Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (IAM)	\$ 26.449.000	\$ 0	\$ 26.449.000	\$ 5.025.310	\$ 31.474.310
Valor Total	\$ 355.822.000	\$ 0	\$ 355.822.000	\$ 67.606.180	\$ 423.428.180

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-enero-2025	Bueno	5/02/2024	Ninguna
2	Scope Test 2024 2	Bueno	5/02/2024	Ninguna
3	Matriz de vulnerabilidades 23012025	Bueno	5/02/2024	Ninguna
4	Informe gerencial FNA AnálisisVuln Masivo II Semestre 2024	Bueno	5/02/2024	Ninguna
5	Informe diferencial FNA AnálisisVuln Masivo II Semestre 2024	Bueno	5/02/2024	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 **CUATROCIENTOS VEINTITRES MILLONES CUATROCIENTOS VENTIOCHO MIL CIENTO OCHENTA PESOS MCTE (\$ 423.428.180).**

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

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



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

Se firma a los 25 días del mes de marzo de 2024.

Mónica
Grand
Villada

Firmado digitalmente
por Mónica Grand
Villada
Fecha: 2025.03.25
14:18:38 -05'00'

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

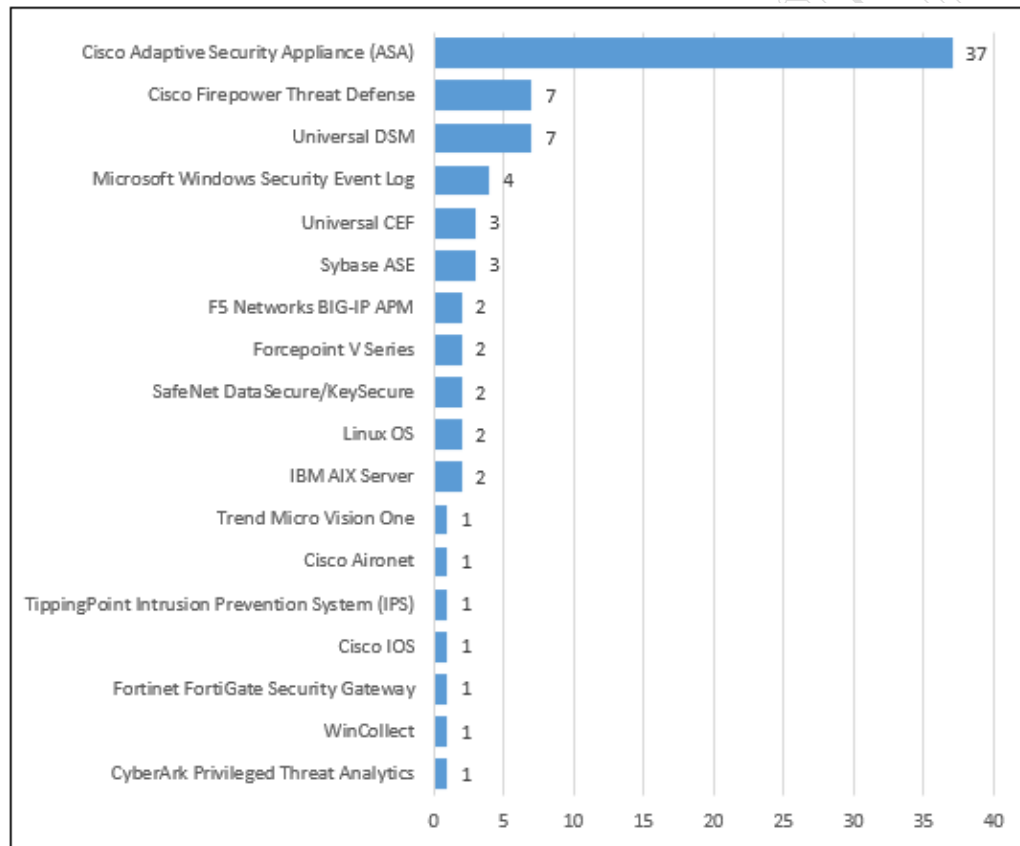
ENRIQUE A. ARRAZOLA MONTES
Profesional 03
Apoyo supervisión CTO 173 de 2023

JAIME ALEJANDRO BECERRA ACOSTA
Profesional Administrativo 3
Apoyo supervisión CTO 173 de 2023

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

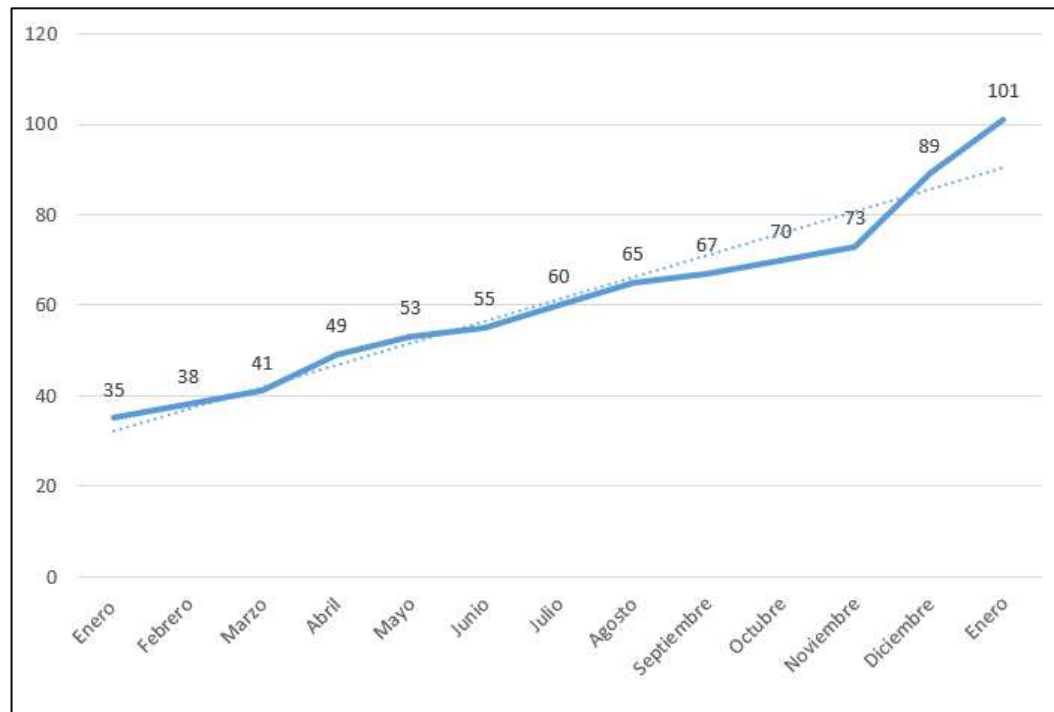
ID	Name	Enabled	Log Source Type	Creation Date
562	Aironet @ 10.200.51.121	Yes	Cisco Aironet	May 21, 2024 5:48 PM (-05)
571	CiscoFirepowerThreatDefense @ 172.17.1.250	Yes	Cisco Firepower Threat Defense	Jul 12, 2024 11:37 AM (-05)
615	IOS @ 192.168.3.168	Yes	Cisco IOS	Sep 24, 2024 12:12 PM (-05)
616	IOS @ 192.168.3.170	Yes	Cisco IOS	Sep 24, 2024 3:42 PM (-05)
614	IOS @ 192.168.4.3	Yes	Cisco IOS	Sep 24, 2024 11:46 AM (-05)
613	IOS @ 192.168.4.4	Yes	Cisco IOS	Sep 24, 2024 11:45 AM (-05)
612	Wism @ 192.168.47.231	Yes	Cisco Wireless Services Module (WiSM)	Sep 24, 2024 11:45 AM (-05)

CASOS DE USO

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

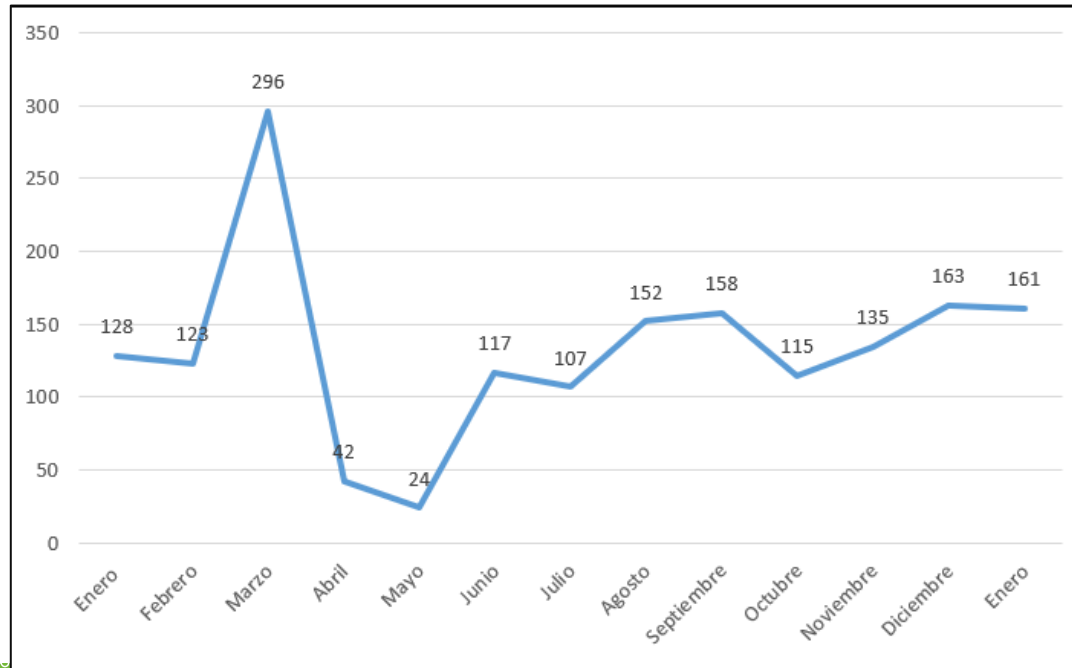
Para este periodo se realizó un incremento de 12 casos de uso

FNA_GUARDIUM_Grant Commands, PII Objects
FNA_GUARDIUM_Failed Login
FNA_GUARDIUM_Uncommon Other
FNA_GUARDIUM_Uncommon real traffic
FNA_CyberArk_Login_PTA_inusual_
FNA_Modificacion_Fondo en línea empresas
FNA_Modificacion_Afiliaciones Digitales
FNA_Modificacion_Cobis AVC
FNA_Modificacion_Fondo en Línea
FNA_SAPHANA_Gerencia Seguridad De La información_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia Saro_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Secretaría General_Eliminación_de_Roles



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

27 de diciembre:

- Sesión de pruebas de alertamiento SIEM sobre el cambio de datos personales en ATC.

Entre el 20 de diciembre y el 21 de enero:

- Creación de los siguientes casos:
 - **FNA_GUARDIUM_Grant Commands, PII Objects:** Identificación de comandos otorgados relacionados con objetos de información personal identificable.
 - **FNA_GUARDIUM_Failed Login:** Seguimiento a intentos fallidos de inicio de sesión para determinar anomalías.
 - **FNA_GUARDIUM_Uncommon Other:** Análisis de comportamientos inusuales en otras actividades del sistema.
 - **FNA_GUARDIUM_Uncommon Real Traffic:** Monitoreo y validación de tráfico real que no se alinea con patrones conocidos.
 - **FNA_CyberArk_Login_PTA_inusual:** Revisión de accesos inusuales detectados en CyberArk PTA.
 - **FNA_Modificación_Fondo en Línea Empresas:** Validación de cambios realizados en la funcionalidad de Fondo en Línea para empresas.
 - **FNA_Modificación_Afiliaciones Digitales:** Revisión de modificaciones en el proceso de afiliaciones digitales.
 - **FNA_Modificación_COBIS AVC:** Validación de ajustes en módulos del sistema COBIS relacionados con AVC.
 - **FNA_Modificación_Fondo en Línea:** Revisión de cambios en la funcionalidad general de Fondo en Línea.
 - **FNA_SAPHANA_Gerencia Seguridad de la Información_Asignación_Roles_A_Otras_Cuentas:** Auditoría de roles asignados a cuentas externas por parte de la Gerencia de Seguridad de la Información.
 - **FNA_SAPHANA_Gerencia Saro_Asignación_Roles_A_Otras_Cuentas:** Validación específica de roles asignados a cuentas en el entorno Saro.
 - **FNA_SAPHANA_Secretaría General_Eliminación_de_Roles:** Seguimiento a la eliminación de roles en SAP HANA gestionados por la Secretaría General.

2 de enero:

- Sesión de validación de alertas de seguridad AD (No Logs) para las IPs 172.16.0.70, 172.16.0.71 y 172.16.0.72.
- Validación de logs para los directorios activos:
 - Identificación de posibles eventos perdidos en los registros.
 - Revisión de integridad y correlación con otros sistemas de seguridad.

3 de enero:

- Creación del reporte "FNA_Reporte Semanal Canal Atención a Clientes":
 - Consolidación de métricas de atención.
 - Análisis de tiempos de respuesta y seguimiento a casos críticos.

8 de enero:

- Identificación de canales en COBIS:
 - Clasificación de canales activos.
 - Revisión de accesos y usuarios asociados a cada canal.

17 de enero:

- Sesión de socialización del alertamiento AD:
 - Presentación de resultados obtenidos en validaciones anteriores.
 - Recomendaciones para optimizar las alertas y su gestión.

20 de enero:

- Validación de usuario y comprobación de permisos en el directorio activo:
 - Auditoría de usuarios con privilegios elevados.
 - Confirmación de permisos necesarios para operaciones críticas.

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
Directorio Activo	En Pruebas Internas
Trend Micro Vision One	OPERATIVA
FortiWeb	OPERATIVA

SEGUIMIENTO SOAR

- **Cisco Firepower**

- **Estado Actual: En pruebas.**

- **Actividades Pendientes:**

1. Coordinar sesiones con el ingeniero Jonathan para validar configuraciones y ajustes necesarios.
2. Revisar la documentación actual y generar un checklist de pruebas faltantes.
3. Realizar simulaciones controladas para validar la eficacia de las reglas y políticas implementadas.

- **Directorio Activo**

- **Estado Actual: En periodo de pruebas internas para integración.**

- **Actividades Pendientes:**

1. Coordinar sesiones de validación técnica con el ingeniero Jonathan, enfocadas en la integración y pruebas de roles.
2. Ejecutar pruebas funcionales para asegurar que las políticas aplicadas sean consistentes.
3. Diseñar un plan de implementación final, incluyendo fechas tentativas y responsables.

- **Trend Micro Vision One**

- **Estado Actual: Operativa.**

- **Actividades Pendientes:**

1. Seguimiento a las funcionalidades implementadas para detectar posibles mejoras.
2. Explorar y probar playbooks disponibles para la automatización de respuestas.
3. Identificar casos de uso adicionales que puedan fortalecer la postura de seguridad.

- **FortiWeb**

- **Estado Actual: Operativa.**

- **Actividades Pendientes:**

1. Revisión de las configuraciones actuales para asegurar el cumplimiento de las mejores prácticas.
2. Pruebas de funcionalidad, especialmente en la detección y mitigación de ataques comunes.
3. Exploración de funcionalidades avanzadas y playbooks que puedan complementar la operación actual.
4. Seguimiento continuo para garantizar la correcta interpretación de logs y alertas.

PLAYBOOKS FORTIWEB

Actualmente se mantienen para fortiweb 20 playbook los cuales permiten la interacción y ejecución de tareas automatizadas.

Customizations Field (internal)	Campo de incidencia
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
fortiweb_domain_optional	Entrada de función
fortiweb_end_time	Entrada de función
fortiweb_endpoint_id	Entrada de función

fortiweb_endpoint_ip	Entrada de función
fortiweb_extra_domains	Entrada de función
fortiweb_global_cdn_status	Entrada de función
fortiweb_log_category	Entrada de función
fortiweb_log_filter	Entrada de función
fortiweb_log_timespan	Entrada de función
fortiweb_offset_hours	Entrada de función
fortiweb_owasp_timeframe	Entrada de función

PLAYBOOKS TRENDMICRO VISION ONE

Actualmente se mantienen para TrendMicro 18 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

Tareas de Gestión Plataforma SIEM

Consumo de rendimiento:

Validación de rendimiento de memoria



Component	Total Outage(min)	Current Status	Last Outage Starttime
tomcat	1.00	Available	27 Jan 2025 1:40 PM
vis	2.00	Available	27 Jan 2025 11:45 AM
ecs-ec	0.98	Available	27 Jan 2025 11:45 AM
historical_correlation_server	3.00	Available	27 Jan 2025 2:52 AM
hostcontext	2.00	Available	26 Jan 2025 12:08 PM
ecs-ep	3.99	Available	25 Jan 2025 4:56 PM
ariel_proxy_server	2.00	Available	25 Jan 2025 4:37 PM
assetprofiler	3.00	Available	25 Jan 2025 8:04 AM
ecs-ec-ingress	3.00	Available	24 Jan 2025 2:32 PM
offline_forwarder	2.00	Available	23 Jan 2025 12:35 PM
reporting_executor	1.00	Available	22 Jan 2025 5:03 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 | grep root
root pts/0 172.19.4.66 Mon Jan 27 09:41 still logged in
root pts/0 172.19.4.66 Tue Jan 21 18:45 - 11:33 (2:16:49)
root pts/0 10.87.61.56 Mon Jan 20 01:05 - 01:22 (00:16)
root pts/0 10.87.61.56 Mon Jan 20 00:56 - 01:04 (00:07)
root pts/0 172.19.4.66 Mon Jan 13 15:20 - 18:04 (02:44)
root pts/0 10.87.61.56 Sun Jan 12 18:15 - 19:52 (01:37)
root pts/0 10.87.61.56 Sun Jan 12 17:39 - 18:13 (00:34)
root pts/0 10.87.61.56 Sun Jan 12 16:45 - 17:17 (00:31)
root pts/1 172.19.4.66 Sun Jan 12 13:03 - 11:03 (2:59)
root pts/0 172.19.4.66 Sun Jan 12 12:57 - 13:17 (00:20)
root pts/0 172.19.4.66 Sun Jan 12 12:52 - down (00:01)
root pts/1 172.19.4.66 Thu Jan 2 17:12 - 09:22 (1+16:09)
root pts/0 172.19.4.66 Thu Jan 2 14:51 - 17:12 (02:21)
root pts/0 172.19.4.66 Thu Jan 2 14:42 - 14:51 (00:08)
root pts/1 10.87.61.56 Thu Jan 2 13:33 - 15:57 (02:23)
root pts/1 10.87.61.56 Thu Jan 2 13:30 - 13:32 (00:02)
root pts/1 10.87.61.56 Thu Jan 2 13:29 - 13:30 (00:00)
root pts/0 172.19.4.66 Thu Jan 2 12:00 - 14:42 (02:42)
root pts/0 172.19.4.66 Fri Dec 27 15:54 - 18:04 (02:09)
root pts/0 172.19.4.66 Thu Dec 26 17:26 - 01:56 (08:29)
root pts/0 172.19.4.66 Wed Dec 18 09:16 - 15:15 (05:59)
root pts/0 172.19.4.66 Wed Dec 11 18:51 - 10:09 (5+15:18)
root pts/0 10.87.61.56 Wed Dec 11 09:18 - 10:06 (00:47)
root pts/0 10.87.61.56 Wed Dec 11 07:47 - 09:12 (01:24)
root pts/0 10.87.61.56 Wed Dec 11 07:42 - 09:12 (01:30)
root pts/2 10.87.61.56 Wed Dec 11 06:20 - 07:05 (00:45)
root pts/0 10.87.61.56 Wed Dec 11 06:15 - 07:19 (01:03)
root pts/0 10.87.61.56 Wed Dec 11 06:06 - 06:10 (00:04)
root pts/2 10.87.61.56 Wed Dec 11 04:20 - 05:50 (01:30)
root pts/0 10.87.61.56 Wed Dec 11 04:13 - 05:51 (01:37)
root pts/2 10.87.61.56 Wed Dec 11 03:13 - 04:09 (00:56)
root pts/2 10.87.61.56 Wed Dec 11 02:02 - 03:12 (01:10)
root pts/0 10.87.61.56 Wed Dec 11 01:45 - 04:09 (02:24)
root pts/0 10.87.61.56 Wed Dec 11 01:19 - down (00:22)
root pts/0 172.19.4.66 Mon Dec 9 09:28 - 09:37 (00:09)
root pts/0 10.87.61.56 Sun Dec 8 22:30 - 22:32 (00:01)
root pts/0 172.19.4.66 Fri Dec 6 08:58 - 18:54 (09:55)
root pts/0 10.87.61.56 Wed Dec 4 05:14 - 05:25 (00:10)
root pts/0 172.19.4.66 Fri Nov 29 10:30 - 15:24 (04:54)
root pts/0 172.19.4.66 Mon Nov 25 16:37 - 10:38 (18:00)
root pts/2 172.19.4.66 Sun Oct 27 20:02 - 15:20 (2+19:18)
root pts/1 172.19.4.66 Fri Oct 25 15:34 - 15:04 (3+23:30)
root pts/0 172.19.4.66 Thu Oct 24 18:40 - 15:04 (4+20:23)
```

65

Alertas Preventivas

24

Alertas Tempranas

42.728

IoC reportados

60

Amenazas reportadas

11

Actores de amenazas
identificados

Informe CTI

2025

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

Número de alertas

65

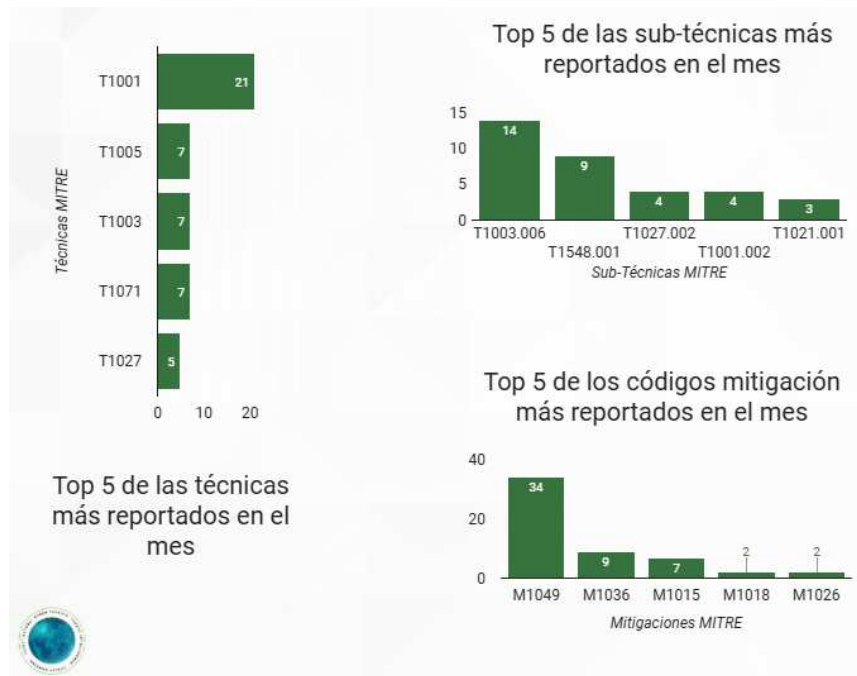
Alertas y eventos
MISP reportados

ALERTAS
REPORTADAS

24

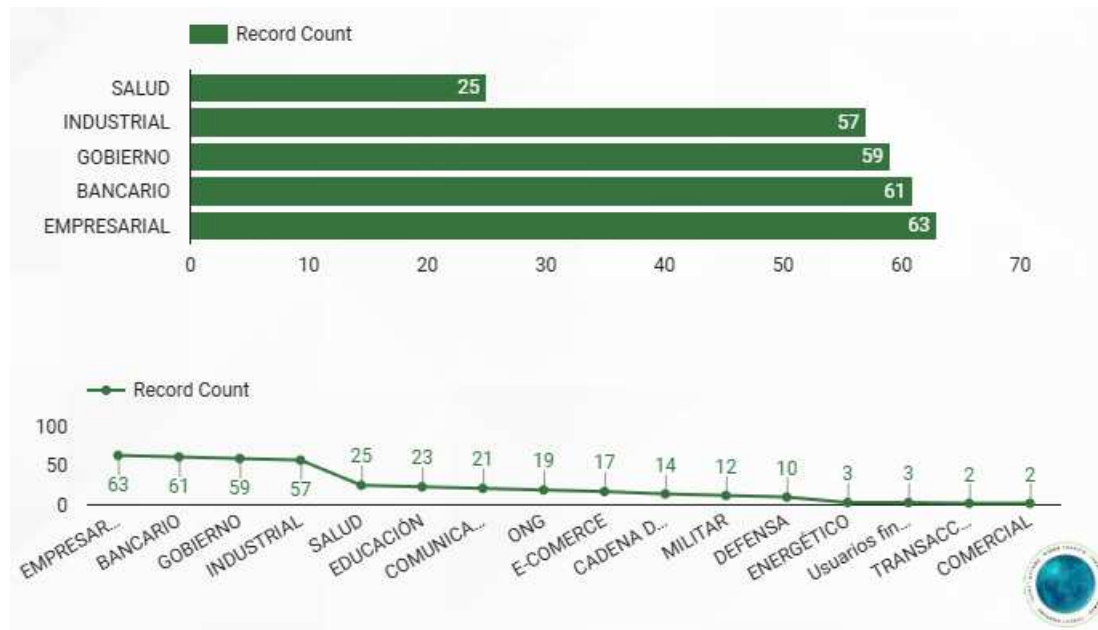
En el periodo evaluado se generaron 24 **alertas tempranas**, cada una de ellas fue compartida vía correo electrónico.

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.

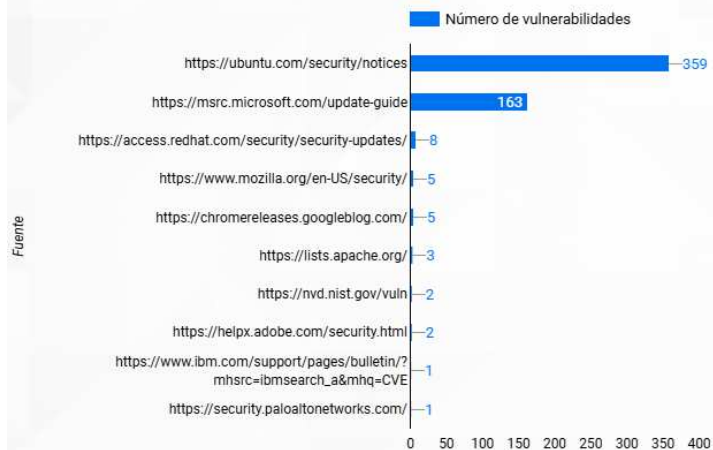
Industria objetivo de cibercriminales



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

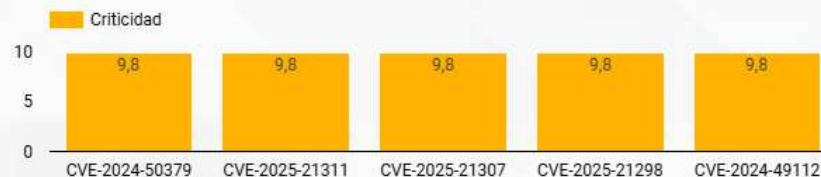
Vulnerabilidades reportadas

Número de CVE reportadas por fuente



Se reportaron 552 vulnerabilidades de 173 productos pertenecientes a 13 fabricantes distintos

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



Se reportaron 10 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.

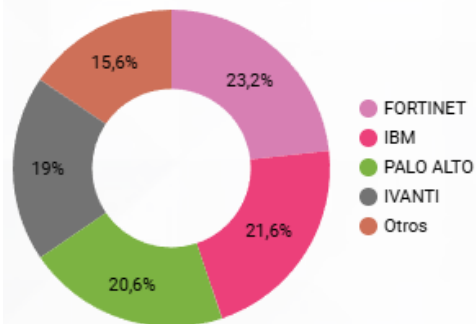
Actividades realizadas

- Se generaron 65 alertas y eventos en MISP.
- De las 65 alertas se han compartido un total de 3.928 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 11 actores de amenazas identificados.
- Fueron generadas 24 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

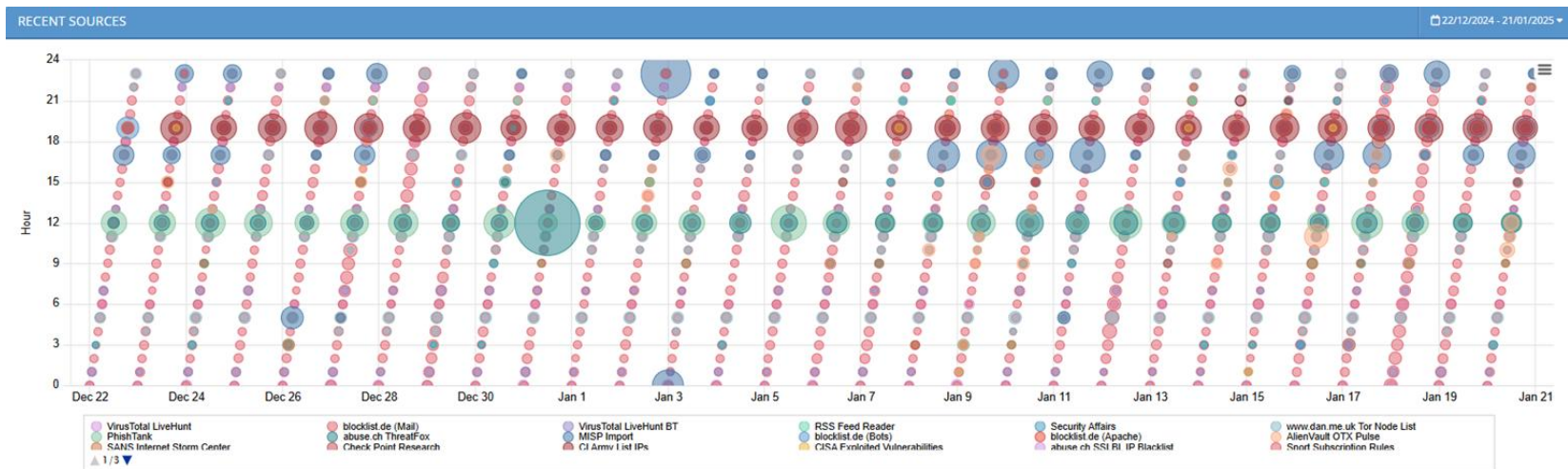
Nivel de criticidad promedio por fabricante, tomando el cvss reportado por cada uno



- Durante el periodo reportado, el servicio de Cyber Threat Intelligence llevó a cabo un análisis detallado de las tendencias y patrones asociados a las amenazas emergentes en el entorno cibernético global. Este trabajo abarcó la detección de nuevas variantes de malware, el monitoreo de técnicas de ataque, la identificación de vectores de amenaza más frecuentes y la actualización de indicadores de compromiso. Además, se dio seguimiento a amenazas previamente reportadas en eventos anteriores.
- Se recomienda configurar las herramientas de seguridad para automatizar la incorporación de indicadores de compromiso proporcionados por el equipo de CTI Mnemo.
- Se recomienda mantener una política estricta y constante de actualización y aplicación de parches en el software corporativo, con el fin de reducir vulnerabilidades y fortalecer la seguridad de los sistemas.

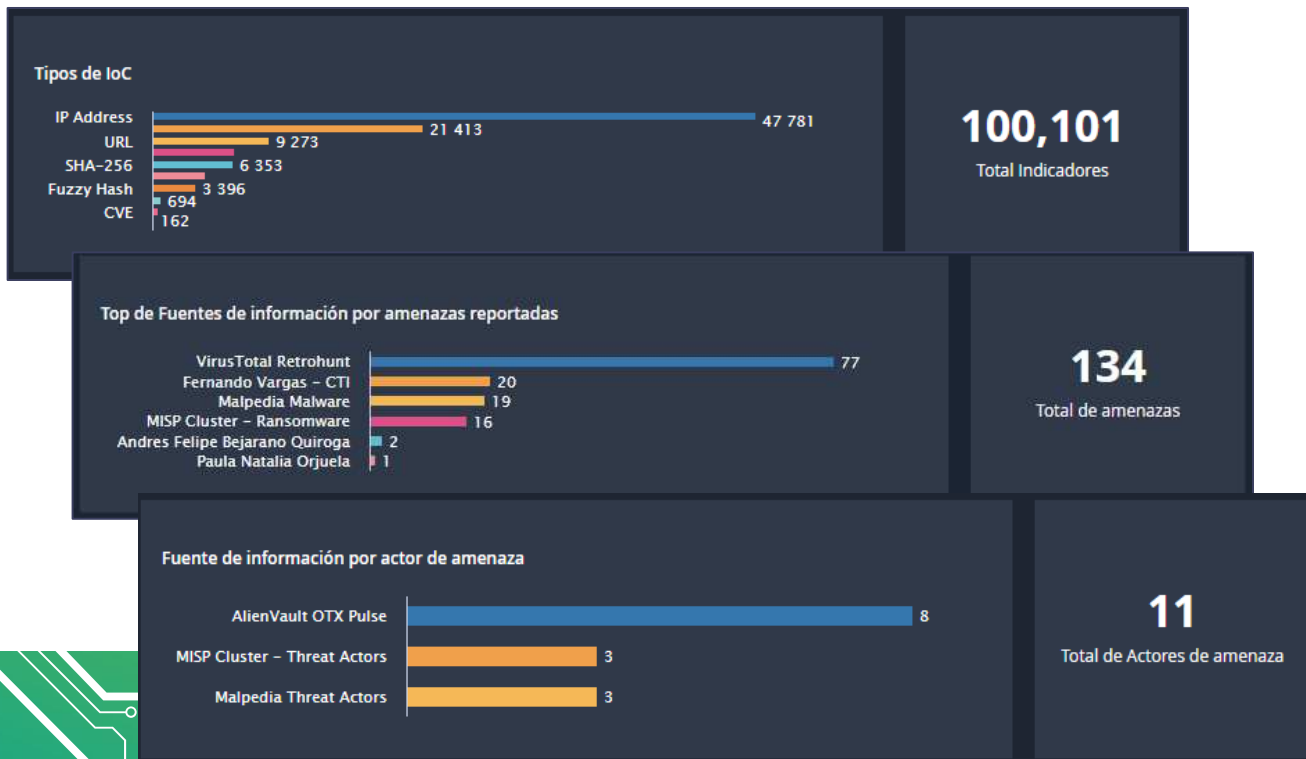
Resumen de objetos obtenidos – TIP

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 realiza una validación del scoring de indicadores de compromiso, que permite a la herramienta priorizar indicadores de compromiso, dependiendo de las fuentes campañas y criticidad de la amenaza, entregando mejores indicadores de compromiso, actualizados y con el contexto necesario para que su bloqueo evite compromisos y daños a la seguridad de la información de la entidad.
- Se han validado indicadores de compromiso cargados por la TIP a la herramienta XDR, validando la efectividad del bloqueo en los equipos de la entidad.
- Se realizan ajustes en las fuentes de datos que entregan indicadores de compromiso a la herramienta, priorizando fuentes que contienen información de valor para el sector empresarial y el entorno geográfico.
- Se han agregado indicadores de compromiso de manera manual, teniendo en cuenta aquellos indicadores que no se han tenido en cuenta por parte de otras fuentes de datos, aprovechando las capacidades de Threat Hunting del equipo de ciber inteligencia de amenazas.



Recomendaciones y conclusiones

- Durante el período observado, se identificó que el indicador de compromiso con más presencia en la información ingestada por la TIP continúan siendo las direcciones IP maliciosas. Por lo tanto, 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.



01

Regla a nivel de
comportamiento

02

Análisis de amenazas en
profundidad y focalizado

Informe Threat Hunting

2025

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:

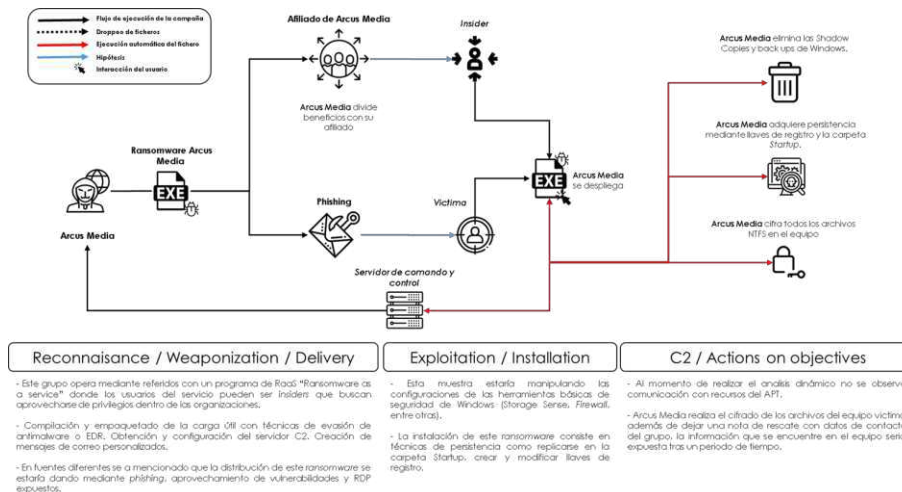
- Resumen de investigaciones.
- Actividades realizadas.
- Recomendaciones y conclusiones.

Resumen de regla compartida

Disabling
Windows
Firewall
with
MpsSvc

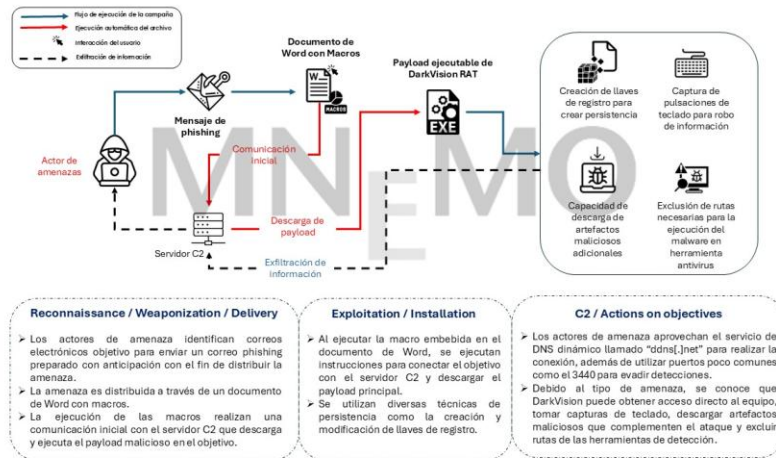
Se identificó un comportamiento de deshabilitación del Firewall de Windows Defender por parte de la amenaza Blackmoon. El comportamiento puede ser detectado de manera temprana con la aplicación de esta regla sigma

Análisis de amenazas focalizados



- Se realizó un Tailored Threat Analysis sobre la amenaza Arcus Media Ransomware, un malware capaz de cifrar los archivos de un equipo víctima, y de generar una nota de rescate con datos de contacto del grupo Arcus Media.
- El análisis se encarga de mostrar el funcionamiento de la amenaza, así como sus métodos de cifrado de información.

Análisis de amenazas focalizados



- Se realizó un Tailored Threat Analysis sobre la amenaza DarkVision RAT, una amenaza capaz de crear una puerta trasera para permitir a un atacante crear conexiones remotas con el equipo víctima, además de capturar información de actividad como las entradas del teclado y exfiltrarla.
- El análisis se encarga de mostrar el funcionamiento de la amenaza, así como sus métodos de persistencia, exfiltración y comunicación con el servidor de Comando y Control.

Actividades realizadas

- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se creó 1 regla Sigma en la que se identifican comportamientos de ejecución de la amenaza StrelaStealer.
- La regla SIGMA identifica la descarga de una librería maliciosa por medio de un archivo JavaScript.
- Se realizaron análisis focalizados sobre las amenazas Arcus Media Ransomware y DarkVision RAT, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.

UNIFIED THREAT IDENTIFICATION
THREAT DETECTION AND PREVENT

General Information

Nombre de la amenaza: StrelaStealer

Criticidad:  Media

Actor de Amenaza: N/A

ATT&CK: T1059.003

Fase Cyber Kill Chain: Execution

Taxonomía: Malware y APT > Malware > Malware catalogado

Acción maliciosa:

Como resultado del análisis realizado a StrelaStealer se identificó un comando que descarga una librería maliciosa desde un archivo JavaScript.

TLP: RED

54

Muestras sospechosas
analizadas

52

Muestras confirmadas con
algún tipo de malware

Informe Laboratorio avanzado de malware 2025

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 54 muestras, de las cuales 52 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.

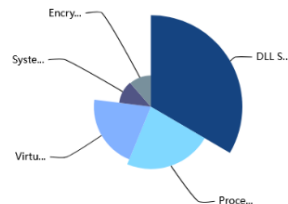
Además, permite mantener una estadística de las amenazas más prevalentes, lo que ayuda a desarrollar un panorama de los posibles ataques prevalentes en la región y en la industria.

Muestras analizadas

54 | 2862



Top 5 MITRE Técnicas

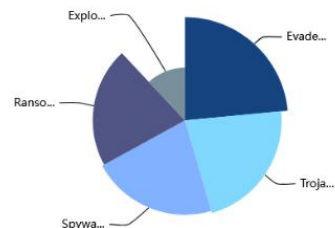


Malware

52 | 2537

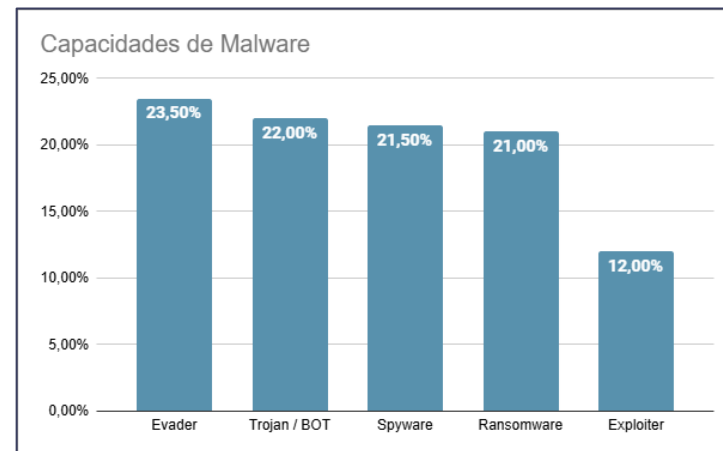
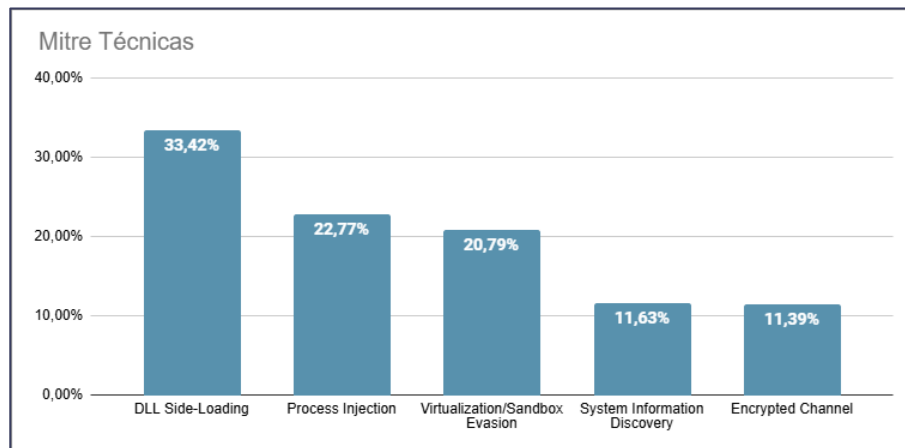


Top 5 Categorías



Técnicas más utilizadas y categorías de malware más detectadas

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



Tácticas y técnicas utilizadas

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Execution through API	DLL Side Loading	Process Injection	Process Injection	Input Capture	System Information Discovery	Remote Desktop Protocol	Archive Collected Data	Exfiltration Over Alternative Protocol	Encrypted Channel
Replication Through Removable Media	Command-Line Interface	Registry Run Keys / Startup Folder	DLL Side Loading	DLL Side Loading	Credential Dumping	Security Software Discovery	Taint Shared Content	Input Capture		Standard Application Layer Protocol
	Windows Management Instrumentation	Scheduled Task	Registry Run Keys / Startup Folder	Obfuscated Files or Information	Credentials In Files	Virtualization/ Sandbox Evasion		Clipboard Data		Standard Non-Application Layer Protocol
	Scheduled Task	Scripting	Access Token Manipulation	Virtualization/ Sandbox Evasion	Credentials in Registry	Process Discovery		Data from Local System		Non-Standard Port
	PowerShell	Windows Service	Scheduled Task	Masquerading		Application Window Discovery		Email Collection		Remote File Copy
	Exploitation for Client Execution	Valid Accounts	Exploitation for Privilege Escalation	Disable or Modify Tools		File and Directory Discovery		Screen Capture		Remote Access Tools
	Service Execution	Create Account	Windows Service	Deobfuscate/ Decode Files or Information		System Time Discovery				Web Service
		Obfuscated Files or Information	Valid Accounts	Software Packing		System Owner/ User Discovery				Data Obfuscation
		Bootkit	Bypass User Access Control	Access Token Manipulation		Account Discovery				
			Abuse Elevation Control Mechanism	Bypass User Access Control		System Network Configuration Discovery				

Análisis de muestras propias FNA

- Durante el periodo reportado no fue solicitado el análisis de una muestra proporcionada directamente por el Fondo.



Actividades realizadas

- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 54 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.
- 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

- Durante el periodo reportado, el equipo de CTI Mnemo ha analizado distintos tipos de muestras sospechosas, esto con el fin de encontrar nuevas tácticas y técnicas utilizadas por actores de amenazas para infectar a sus víctimas a través de nuevos y elaborados ejecutables maliciosos.
- Los ficheros han sido elegidos de amenazas que se encuentran en tendencia, campañas de phishing vistas recientemente en diferentes compañías, y actividades de Threat Hunting llevadas a cabo por el equipo de CTI Mnemo.
- 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.



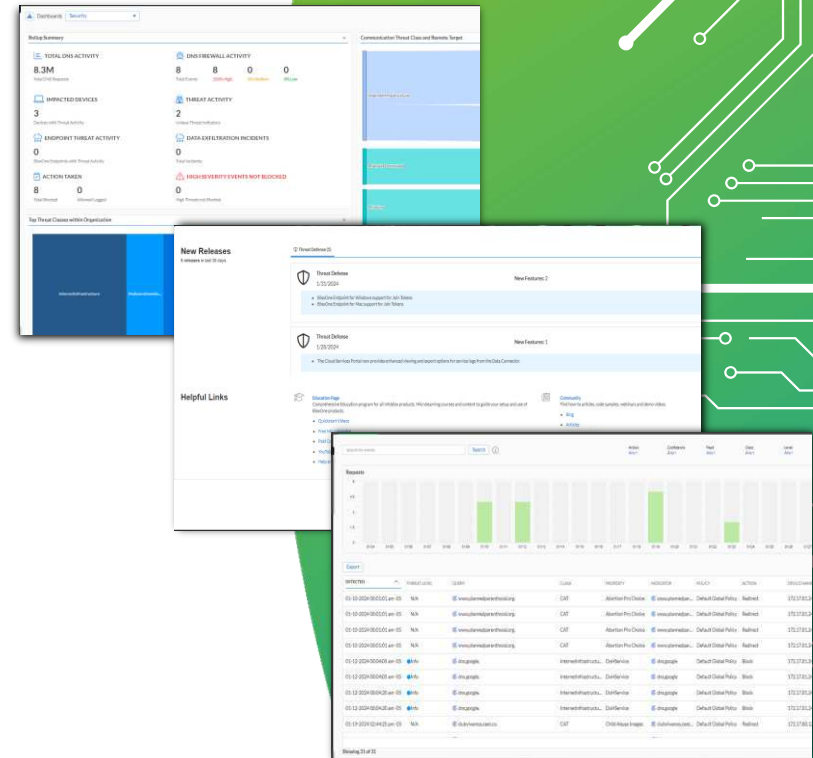


DEFINICIONES

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

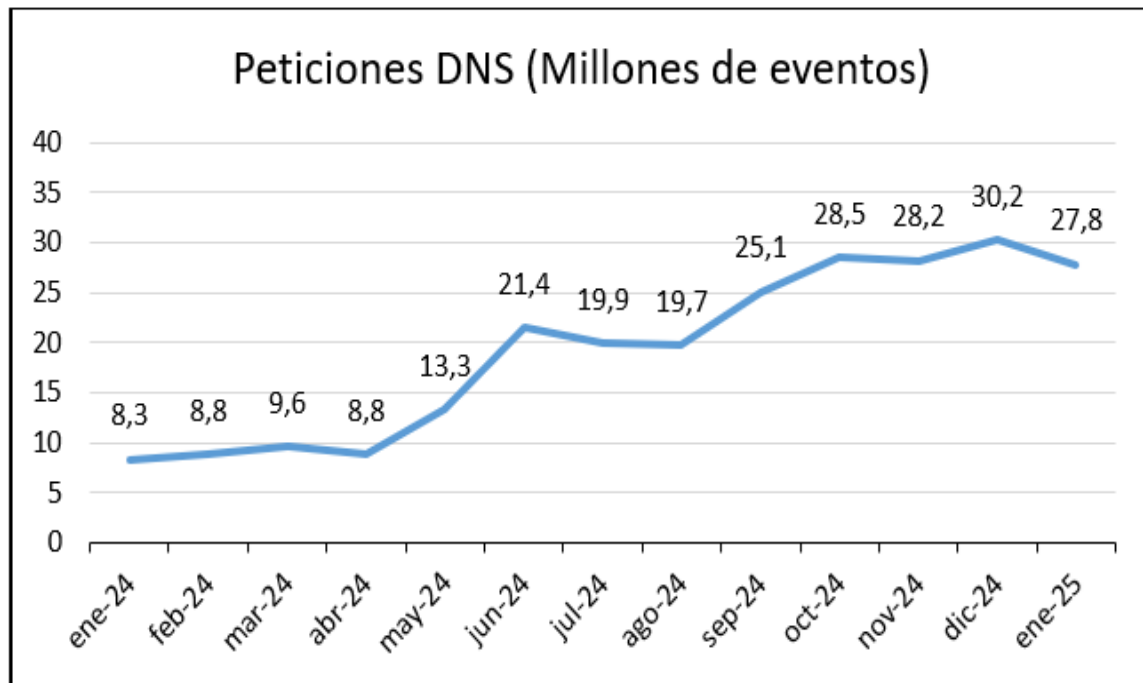
Política: cuenta con una serie de políticas que rigen cómo opera la empresa. Estas políticas se establecen para proteger a los empleados, clientes y socios de Infoblox, así como para garantizar que la empresa cumpla con todas las leyes y regulaciones aplicables.

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 se presentó una disminución 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.



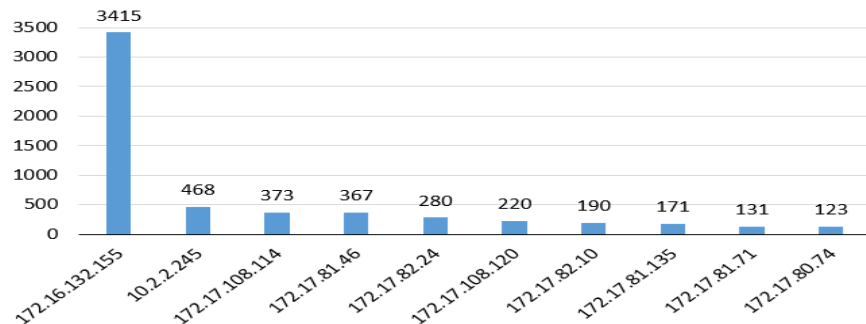
INDICADOR AMENAZAS



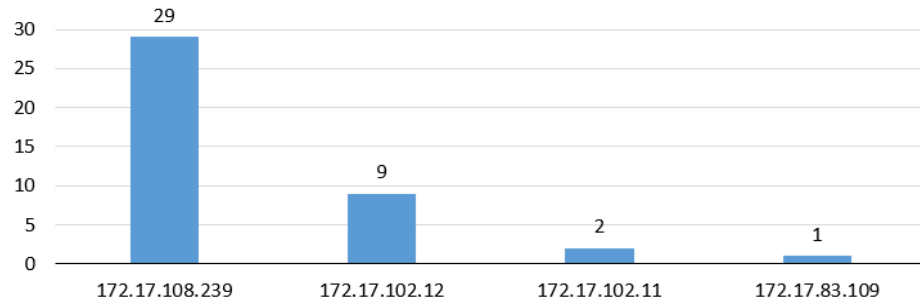
DNS SECURITY – INFOBLOX

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

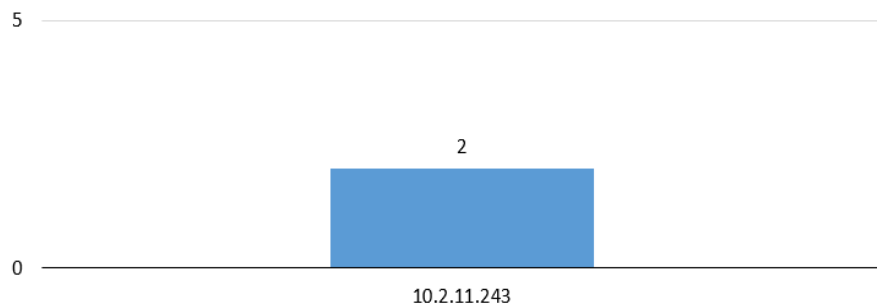
Internet Infrastructure



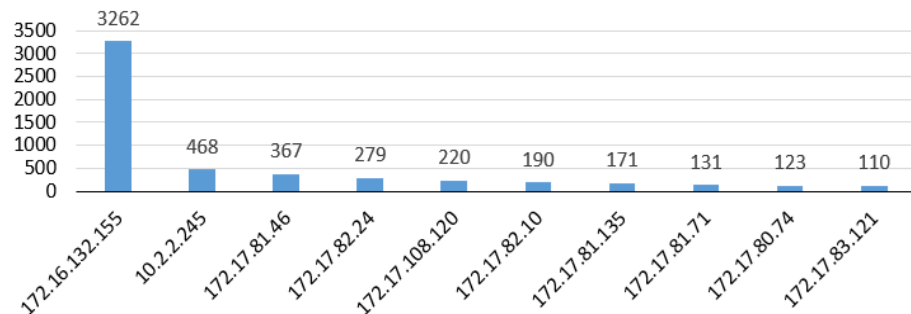
Phishing



Suspicious



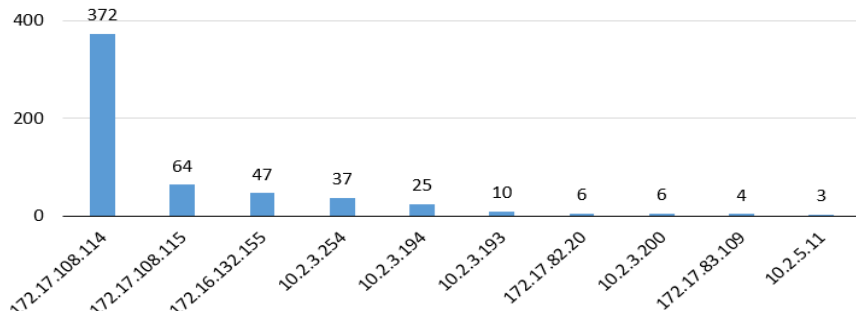
Top 10 Infrastructure



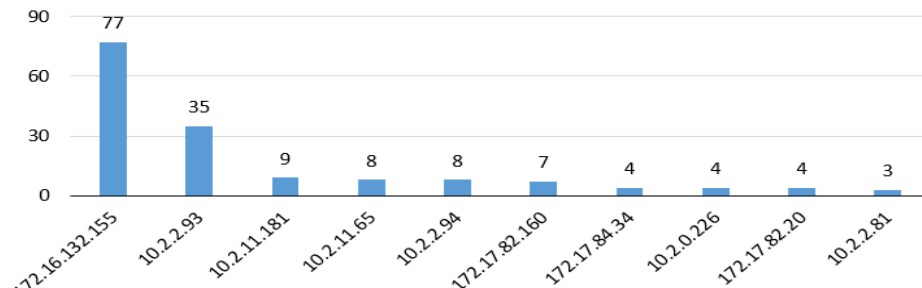
DNS SECURITY – INFOBLOX

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

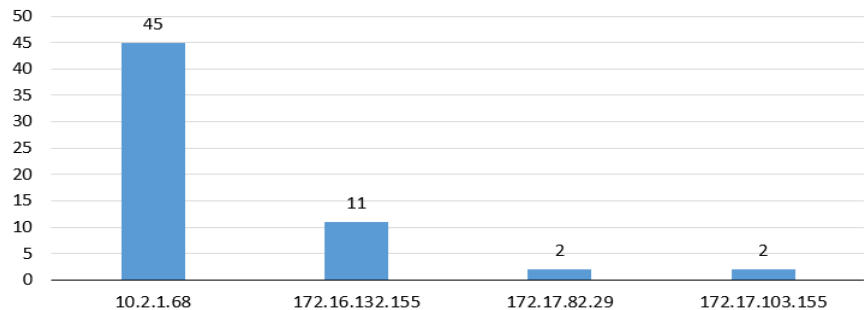
Top 10 Malware Download



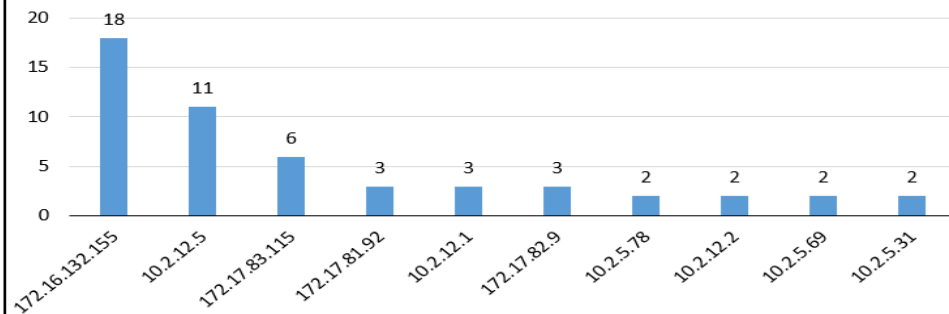
Top 10 Malicious



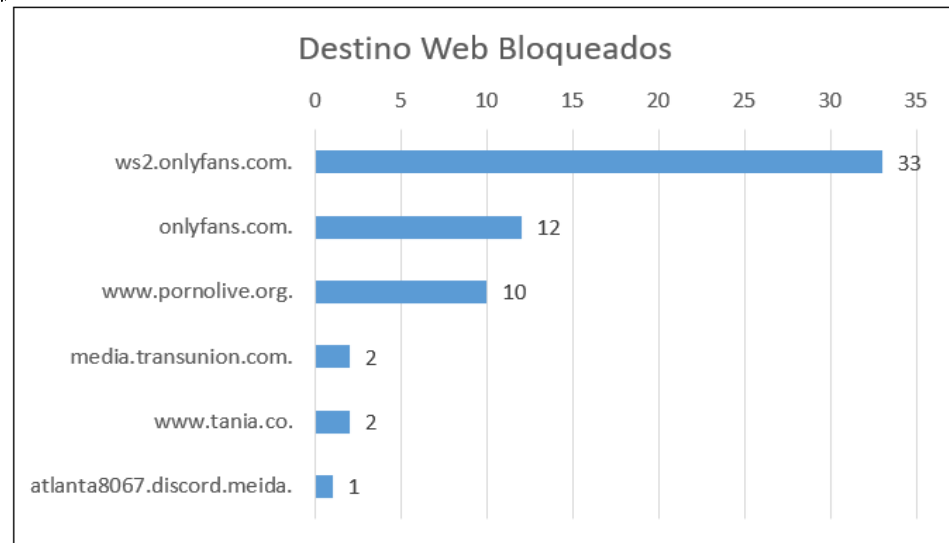
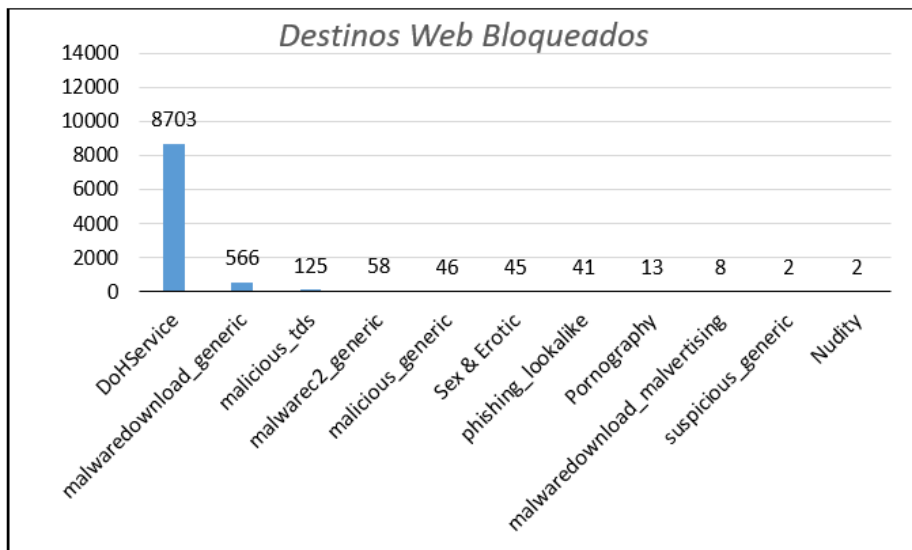
Top Cat



Top 10 Malware



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

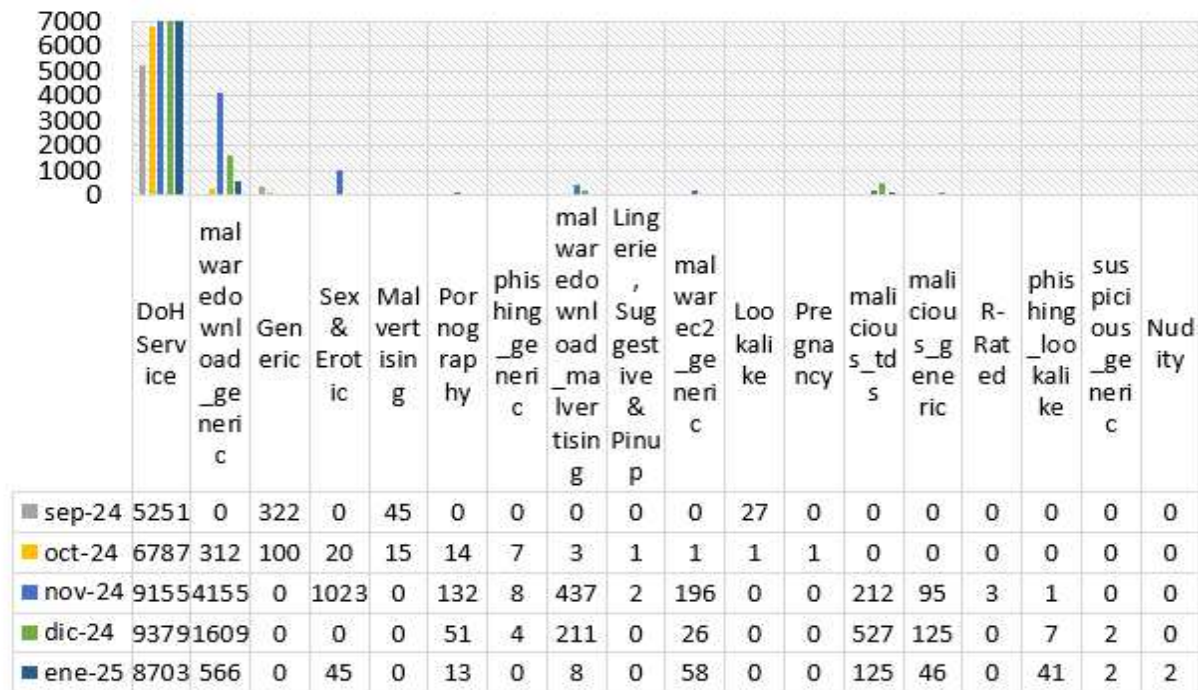


Para el periodo en mención se evidencia un aumento con relación al mes anterior en cuanto al índice de amenazas detectadas, de igual forma se identifica que el volumen de consultas a portales de pornografía aumentó en la resolución de DNS.

GENERAL DNS – INFOBLOX

Para el periodo en mención se evidenció una disminución de 676 eventos en la categoría de DoHservice en las consultas DNS, para la categoría malware download generic se evidenció una disminución de 1.043 siendo las categorías con más consultas dentro del DNS.

CONTENIDO CONSULTADO - DNS SECURITY



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.

Actividades semanales:

- Monitoreo de eventos revisión de los eventos para detectar cualquier actividad inusual o anómala que pueda indicar un posible ataque.
- Análisis de direcciones IP esto con el de identificar si se encuentran direcciones inactivas.
- Validación de disponibilidad de la plataforma Infoblox.
- Revisión plataforma Infoblox para evaluar el estado general de tu infraestructura.
- Actividades Proceso:

Cambio 00501624 con fabricante para validar error de servidor.



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

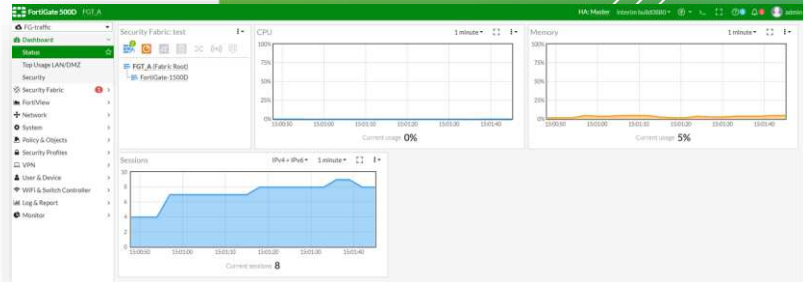
Protección multicapa contra los 10 principales ataques a aplicaciones de OWASP, incluido el aprendizaje automático para defenderse de ataques conocidos y desconocidos.

Protección API

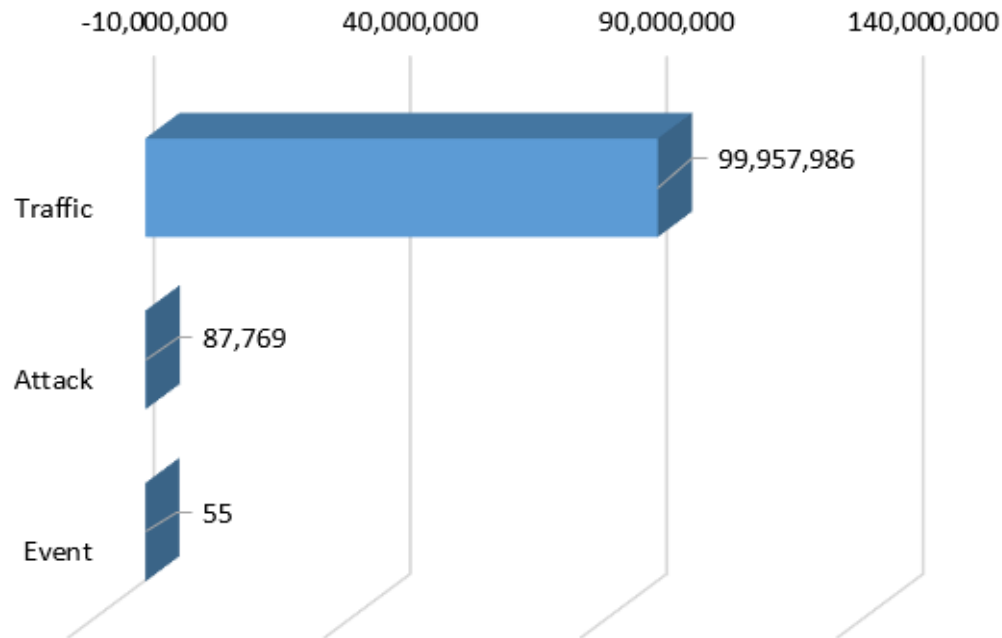
Protege los API de actores maliciosos aplicando automáticamente lo positivo y lo negativo. políticas de seguridad. Integra la seguridad API en su proceso de CI/CD.

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



+100 M

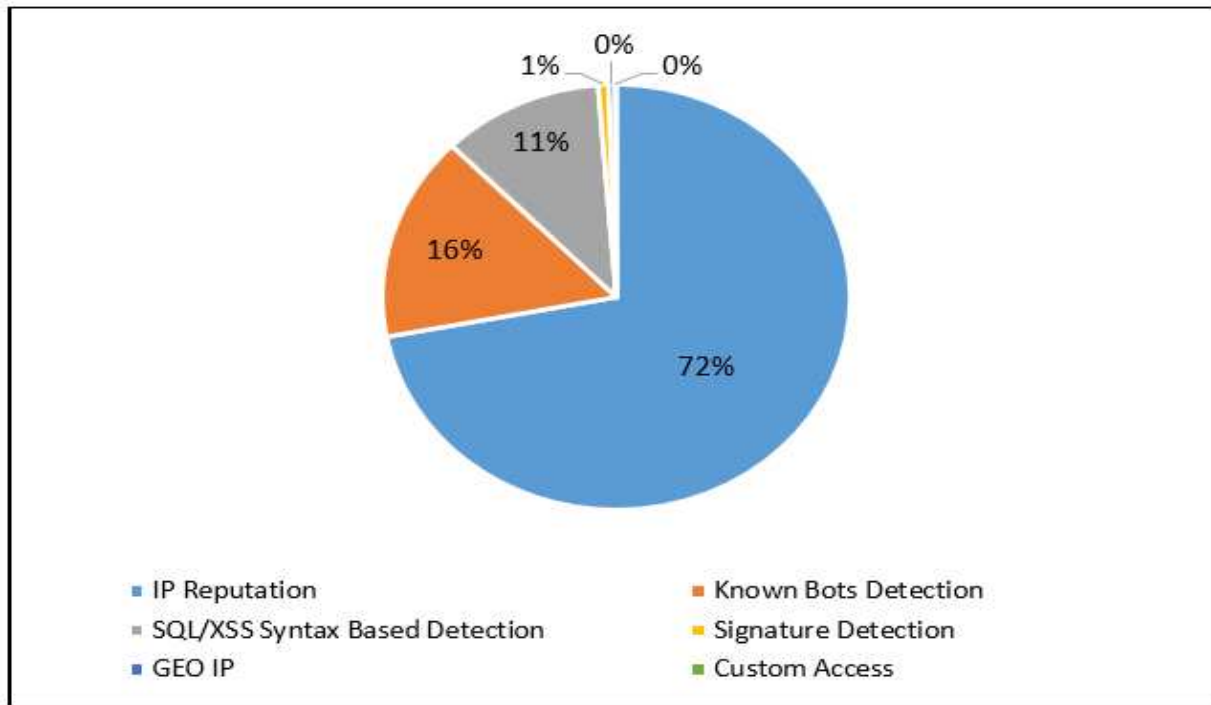
Eventos verificados por el WAF

0,1%

Del tráfico total es
categorizado como
amenaza

Durante el presente periodo, se visualizó tráfico a través del WAF de aproximadamente 100 Millones de peticiones de los cuales el 0,1% están dentro de la categoría de Amenaza.

GENERAL WAF – FORTIWEB

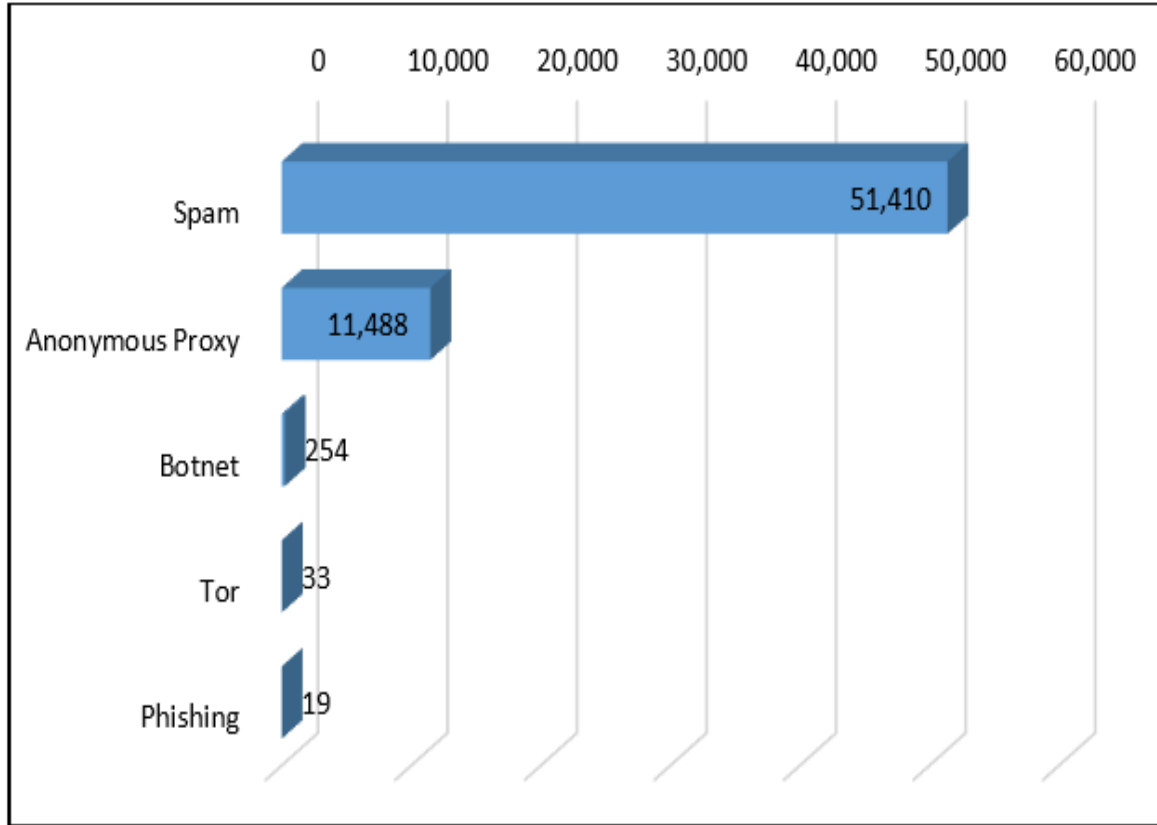


6

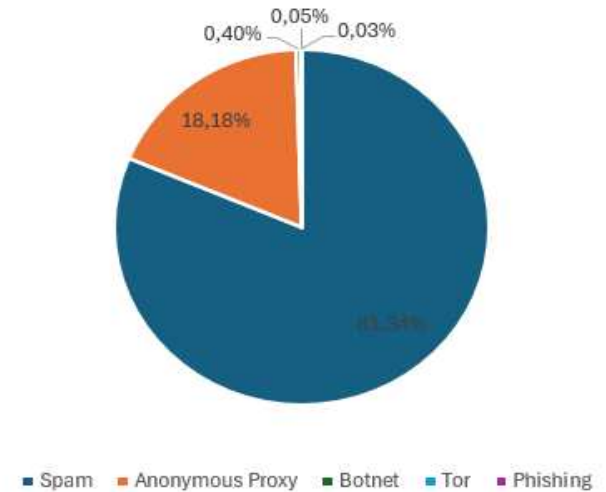
Eventos identificados
por el WAF

Durante el periodo en mención, se visualizó tráfico a través del WAF con una activación total de 6 categoría de Amenaza de acuerdo a la información extraída.

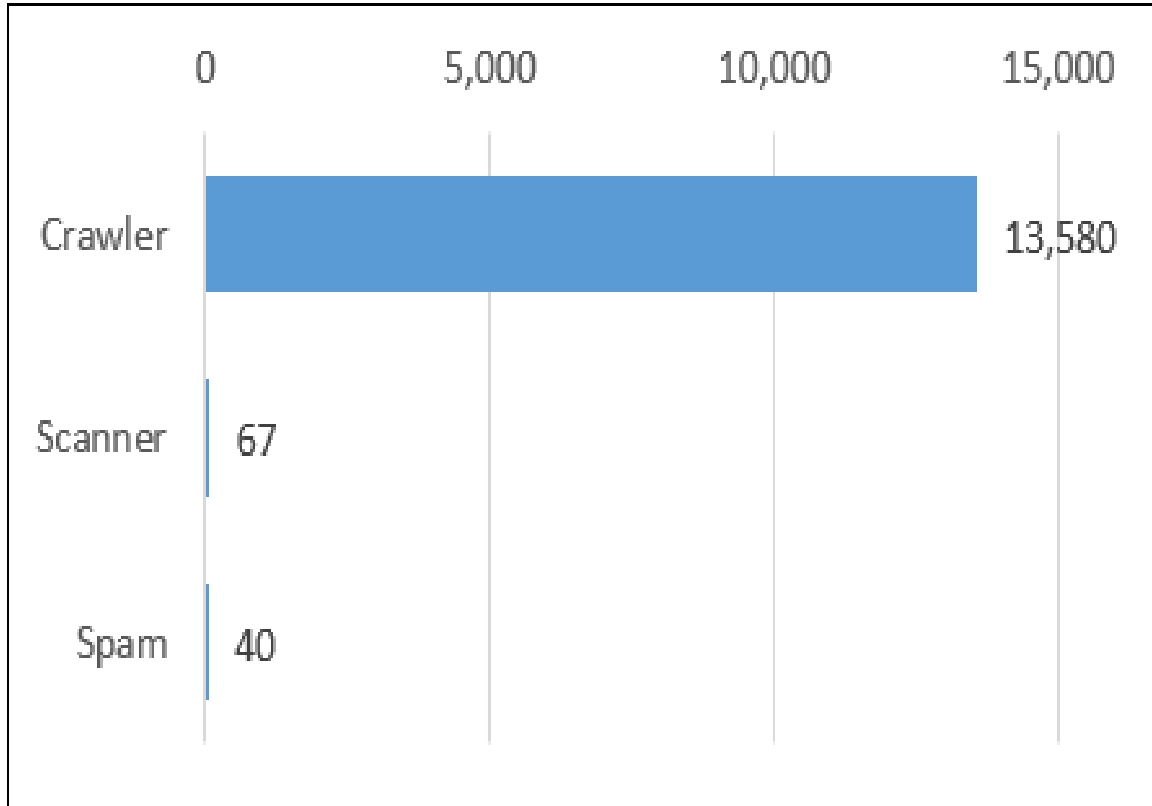
GENERAL WAF - IP REPUTATION



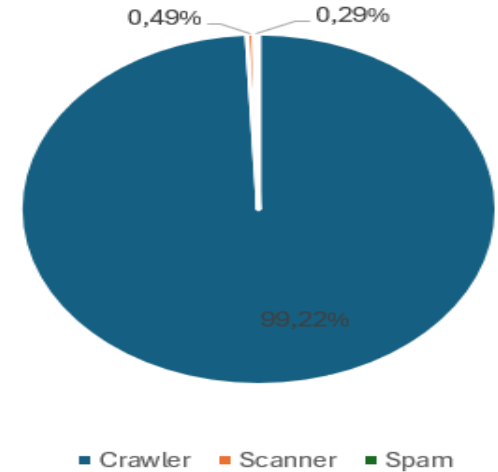
72,01 %
63,204
IP Reputation



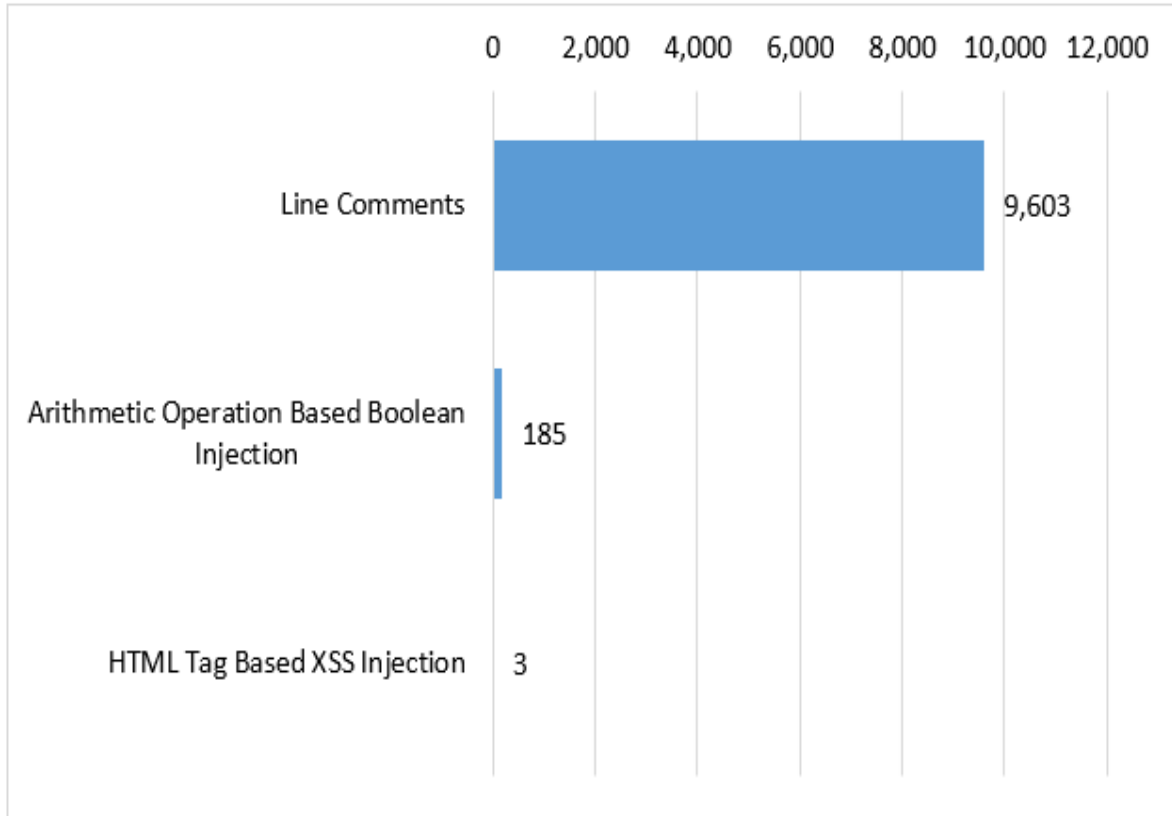
GENERAL WAF – KNOWN BOTS DETECTION



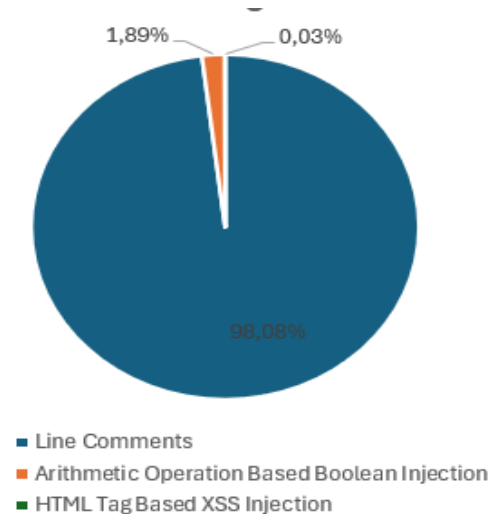
15,59 %
13,687
Known Bots



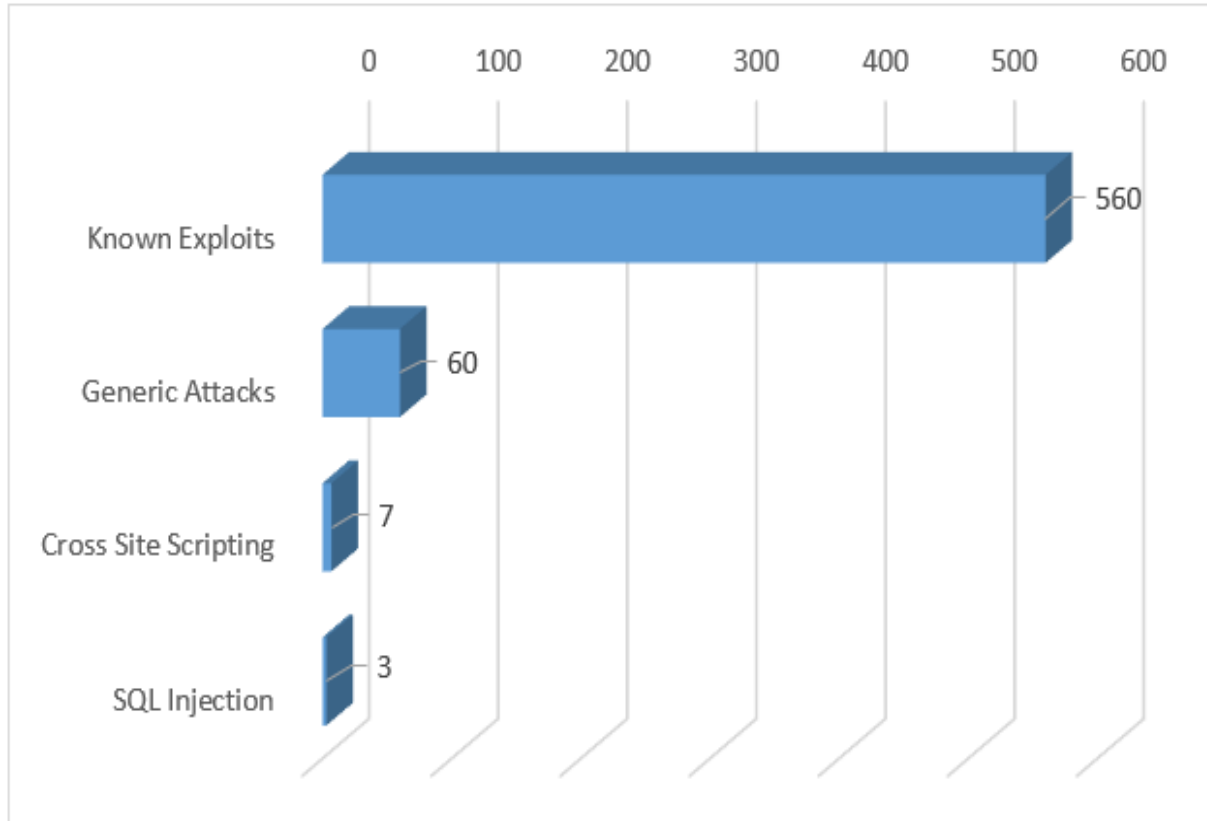
GENERAL WAF – SQL/XSS Syntax Based Detection



11,16 %
9,791
SQL/XSS



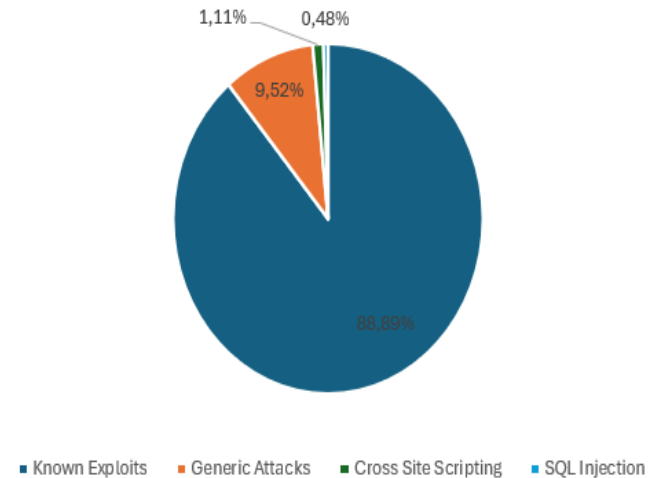
GENERAL WAF – SIGNATURE DETECTION



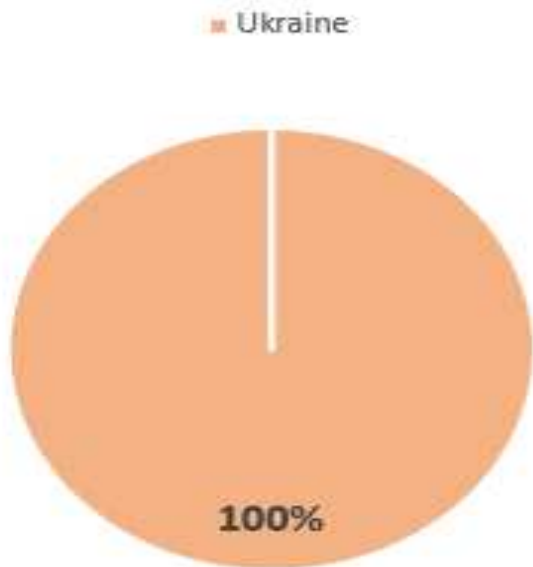
0,72 %

630

Signature Detection



GENERAL WAF - GEO IP



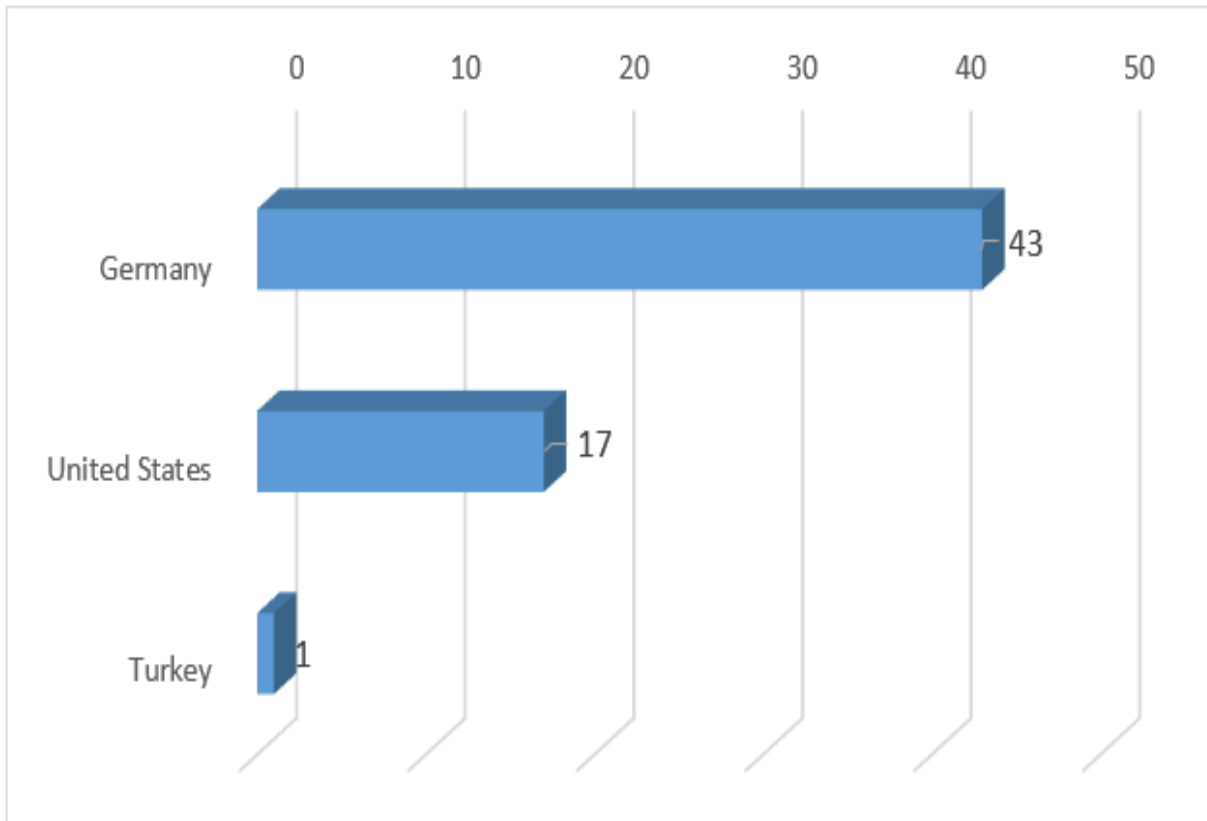
0,45 %

396

GEO IP

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

GENERAL WAF - CUSTOM ACCESS



0,07%

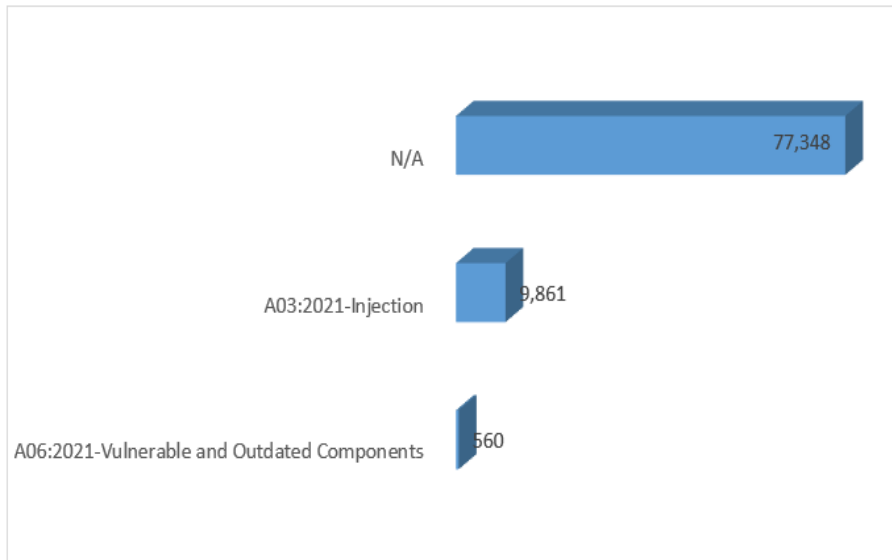
Eventos Identificados

61

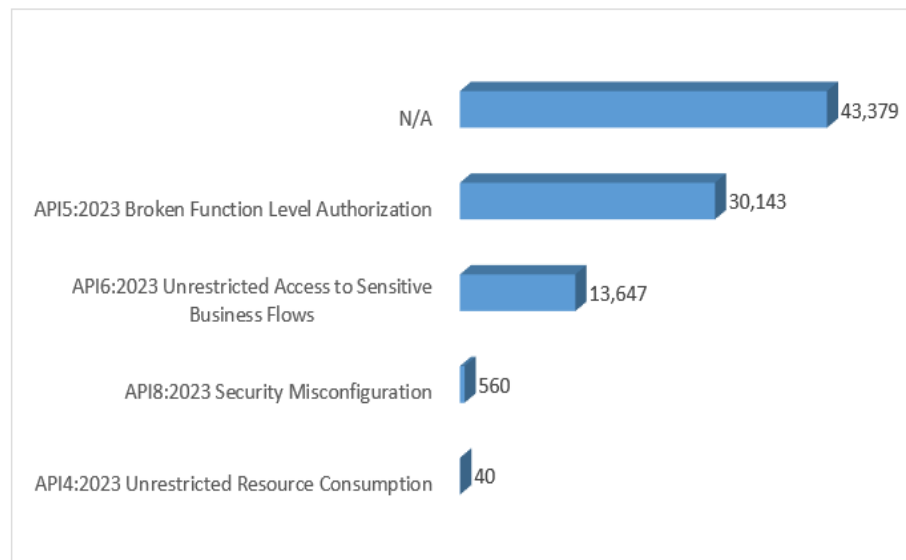
Custom Access

GENERAL WAF – FORTIWEB

OWASP TOP 10



OWASP API TOP 10



Actividades realizadas

Actividades diarias:

- **Análisis y revisión de alertas:** Análisis de eventos específicos, como ataques bloqueados o intentos de acceso no autorizados. Para estas alertas se verifica que el SIEM las recibe correctamente.
- **Revisión de registros:** Revisión de los registros del WAF de información sobre los eventos del sistema del dispositivo en busca de alertas de fallas o bajo rendimiento que pueda afectar la disponibilidad del WAF.
- **Revisión de las Actualizaciones de seguridad:** Revisión del estado de la actualización de las firmas, protección web y estado de security fabric.

Actividades semanales:

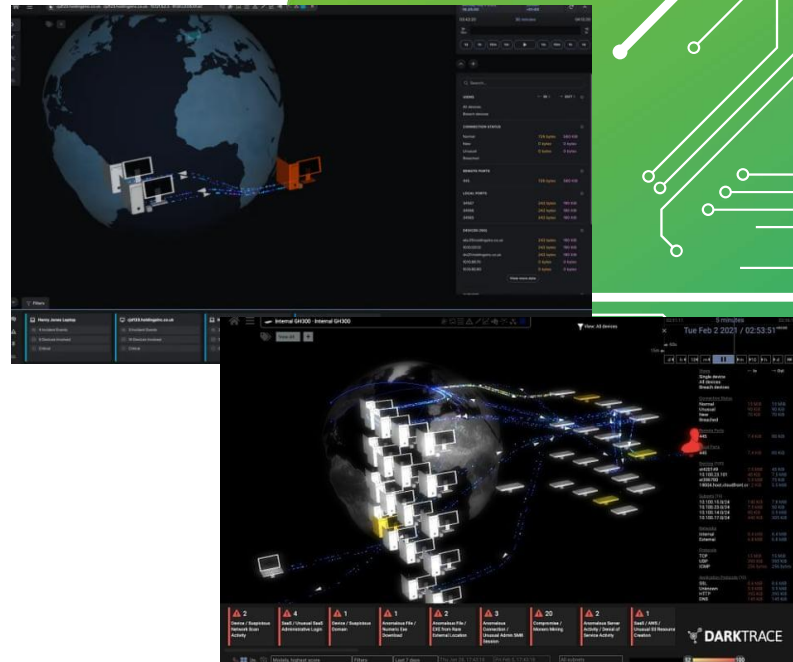
- **Limpieza de registros:** Limpiar registros y archivos temporales para mantener un estado saludable en el espacio del dispositivo.
- **Revisión del firmware:** Asegurar que el WAF Fortiweb esté ejecutando una versión de firmware soportada por fabricante con las últimas correcciones de seguridad y mejoras de rendimiento.
- **Realizar una verificación de integridad del sistema:** Verificar que el sistema operativo del WAF esté funcionando correctamente y que no haya archivos corruptos.
- **Verificación y actualización de los IOC compartidos desde CTI:** validar que los IOC compartidos desde CTI cumplan con requisitos y apliquen al entorno de la protección de portales del FNA.



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.



6.727

Dispositivos
modelados

219

Subredes

883

Dispositivos en
brechas

1.224

Brechas

116

Modelos

Informe solución Darktrace/Respond 2025

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

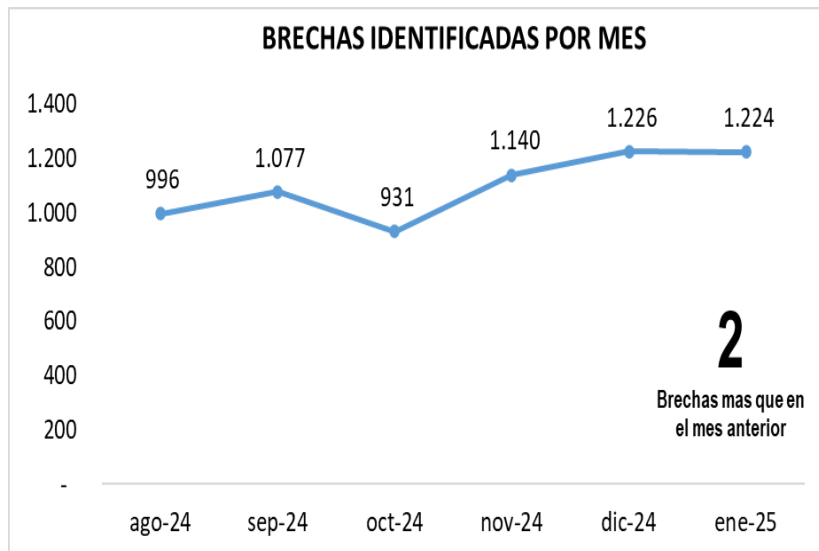
Los hallazgos presentados en el presente informe fueron detectados durante el periodo comprendido entre el 22 de Diciembre y el 21 de Enero de 2025, comprendiendo los siguientes temas.

- 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.

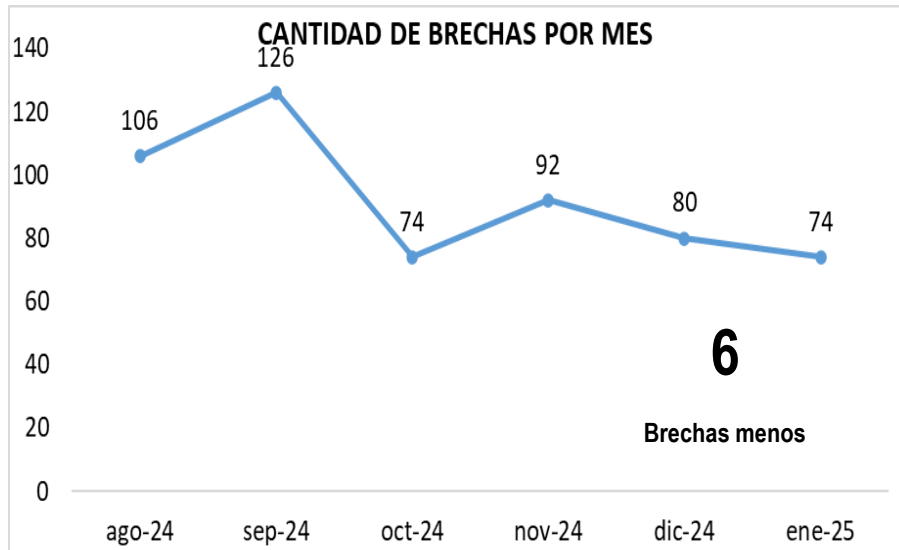
Distribución de Brechas

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.



Modelos Darktrace/Respond

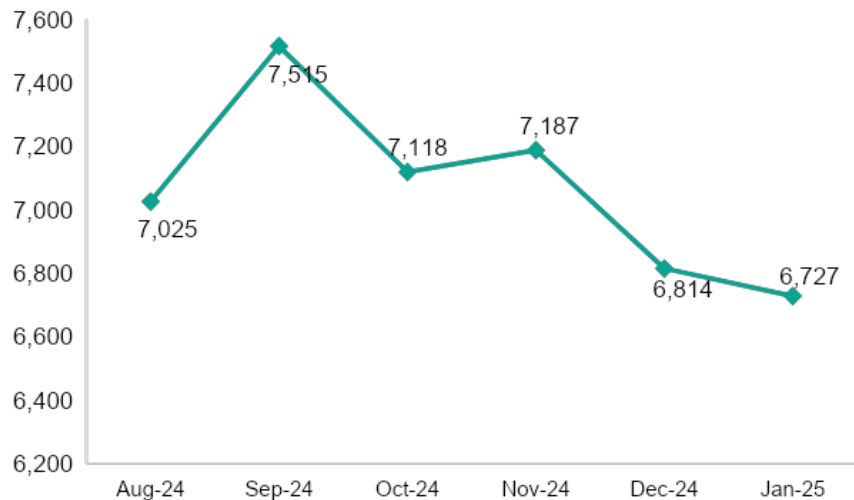


Brechas identificadas por categoría

Licenciamiento

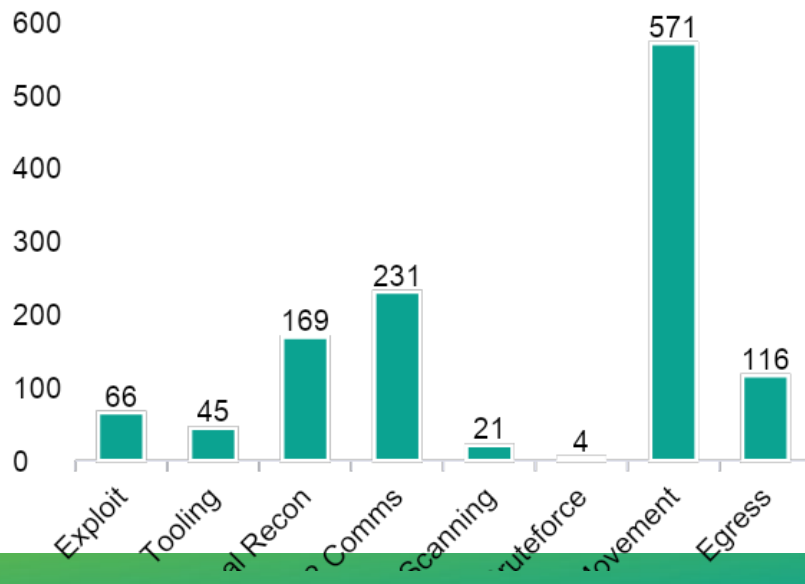
Los modelos de ciberdefensa se pueden organizar de acuerdo con la fase de ataque que es más probable que detecten. Los modelos de monitoreo de acuerdo con estas categorías pueden permitir que el patrón de comportamiento característico de un ataque en curso sea observado.

DISPOSITIVOS MODELADOS POR MES



Distribución de Brechas

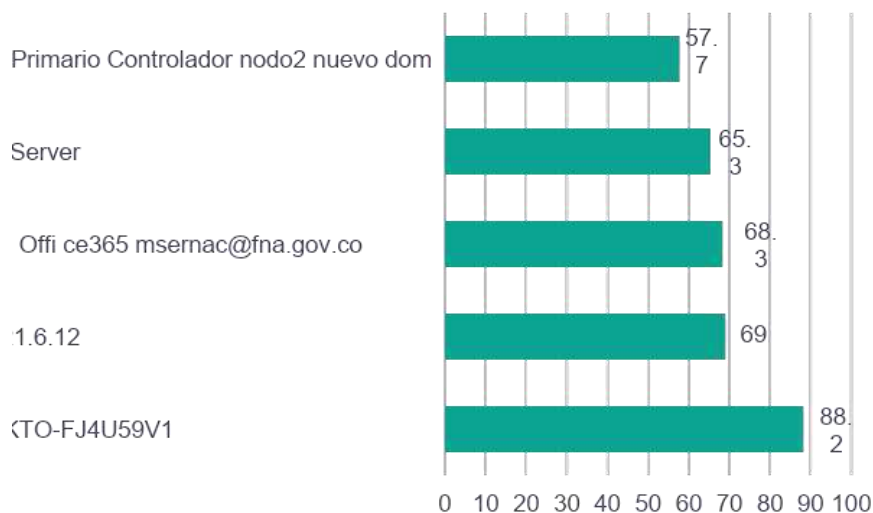
CANTIDAD DE BRECHAS POR CATEGORIA



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

DESKTO-FJ4U59V1

Suspicious SMB Scanning Activity
Attack and Recon Tools

172.21.6.12

HTTP to Suspicious Subdomain

SaaS Offi ce365 msernac@fna.gov.co

Possible Exfiltration of Files By Email

Print Server

Attack and Recon Tools

DNS Primario Controlador nodo2 nuevo dom

Increase in New RPC Services

199.346

Correos Entrantes

5.006

Correos con accion

194.346

Correos Entregados

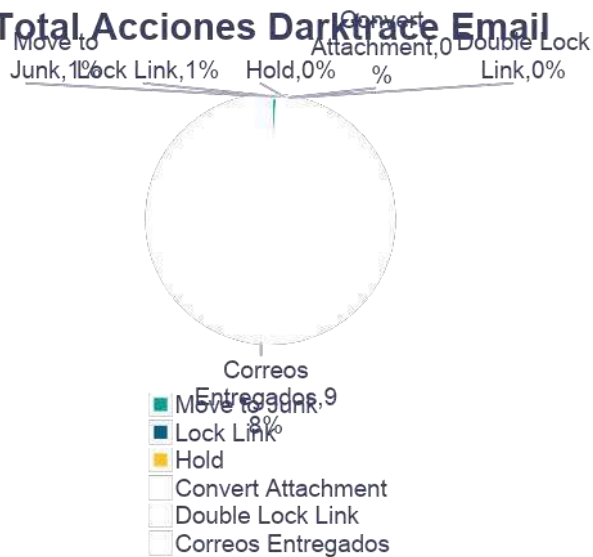
777.405

Correos Salientes

Informe solución Darktrace/Email

2025

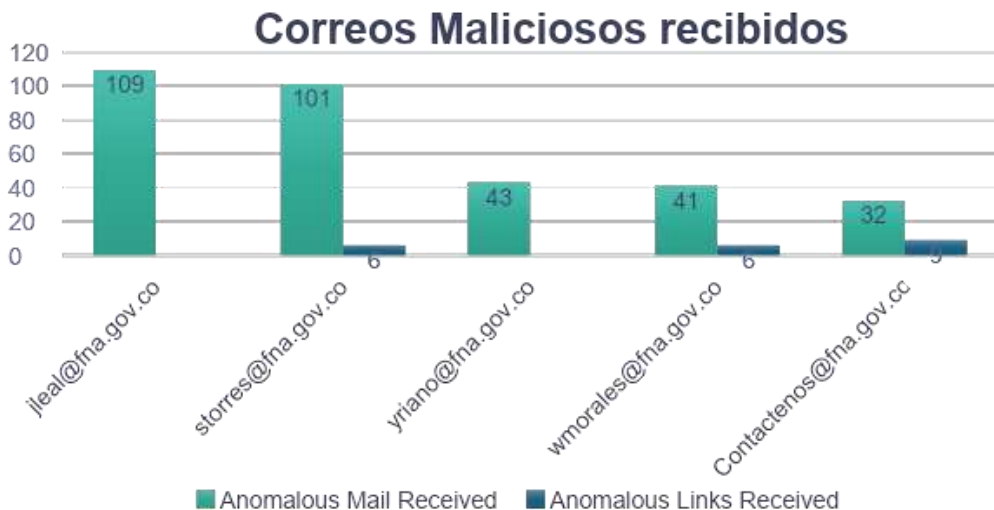
Total Acciones Darktrace Email



Top Acciones	Total, Acciones	% total de correos
Move to Junk	2.438	1%
Lock Link	1.440	0,7%
Hold	552	0,3%
Convert Attachment	290	0,1%
Double Lock Link	286	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.

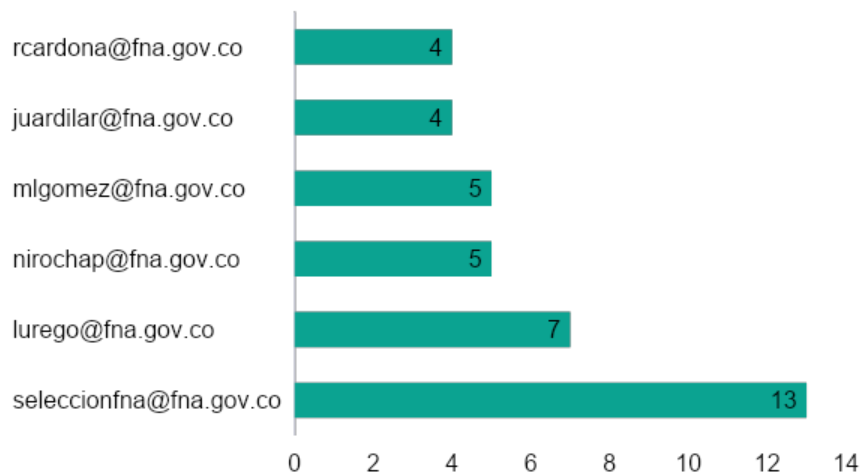


Las cuentas de correo ileal@fna.gov.co y storres@fna.gov.co , en su gran mayoría de los correos retenidos corresponden del remitente exams@certiprof-exams.com , del cual reciben ofertas, estos fueron movidos a la carpeta de **No deseado**

Administración Email

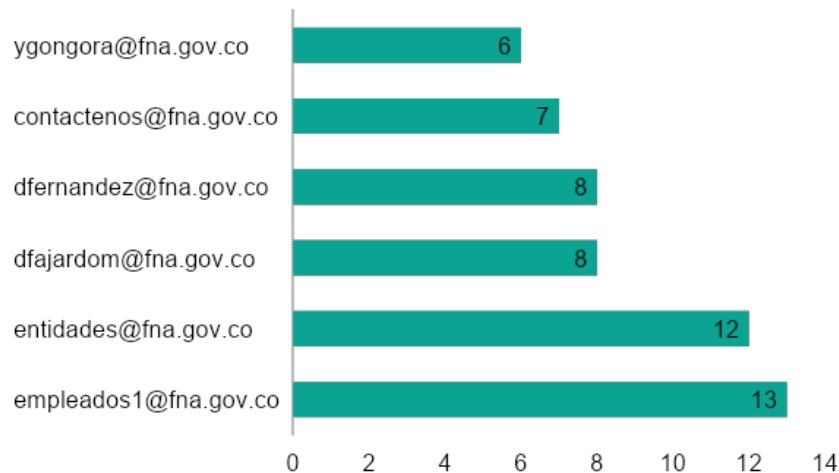
Múltiples anomalías han elevado la puntuación de este correo electrónico por encima del umbral (threshold) de retención.

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

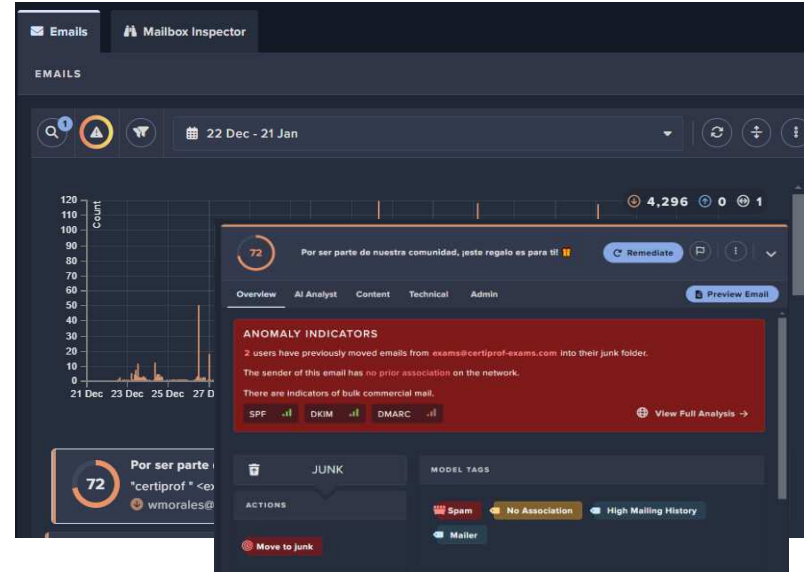
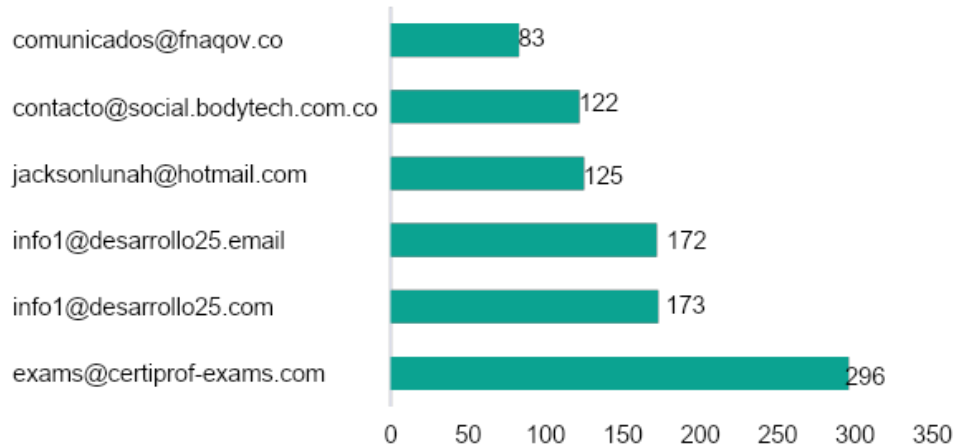
Top Destinatarios Email Retenido



Administración Email

El TOP de remitentes bloqueados por la herramienta de Darktrace Email. Esta lista mostrará a los remitentes que han sido identificados como potencialmente peligrosos o maliciosos, y que han sido bloqueados automáticamente por la herramienta para proteger la seguridad de la red y los datos de la organización.

Top Remitentes Bloqueados



ANALISIS DE ADMINISTRACION DARKTRACE.

- Durante el periodo del 22 de Diciembre al 21 de Enero se presento un aumento significativo de alertamiento del modelo **High Volume Client Data Transfer**, pasando de 33 alertamientos en el periodo anterior a 133 alertas.

Este aumento se debe actividades de Back UP de la herramienta “Almacenamiento ExaGrid - BackUP”, de acuerdo con lo anterior se genera exclusión para el equipo Almacenamiento ExaGrid - BackUP172.16.125.33, para el modelo **Antigena Internal Data Transfer Block**.

- Se realiza análisis del IM157937, AFECTACION DE RED EN PUNTOS DE ATENCION, donde se indicó en su momento de alto consumo de red y los sitios usados por el agente de Darktrace estaba como TOP.

De acuerdo al Incidente se realiza la solicitud al área de redes de suministrar los logs de consumo de los días 5,12 y 19 de Diciembre, a las siguientes direcciones:

- 45421590.live.darktracesensor.com
- cdn.live.darktracesensor.com"

Dado el análisis de las tres fechas solicitadas incluida la del día del incidente (19 de Diciembre), se evidencia que el consumo es la misma para los otros días donde no se presentan alertamientos de consumo de RED.



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 solicita al area de redes informe de consumo de los días 5,12 y 19 de Diciembre, a las siguientes direcciones:
 - 45421590.live.darktracesensor.com
 - cdn.live.darktracesensor.com
- Se genera exclusión para el equipo Almacenamiento ExaGrid - BackUP172.16.125.33, para el modelo Antigena Internal Data Transfer Block
- Se realiza cierre del Incidente IM157937, a traves de logs los consumos en otras fechas son las mismas.
- Se genera reporte al área de seguridad de la información para la validación de los correos masivos (172) de remitentes con dominio info1@desarrollo25.email
- Se genera cronograma de actividades y/o mejoras para la administración de la solución de Darktrace
- Se reporta al área de seguridad de la información el correo de la solicitud RF421048, correo con remitente la misma cuenta del destinatario
- 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 diciembre de 2024 y el 21 de enero de 2025, la plataforma presentó estabilidad y normalidad en su operación.

Actividades macro ejecutadas	Actividades a ejecutar
● Reporte agente STAP, SAP HANA. ● Solicitud monitoreo agentes. ● Solicitud destinatarios eventos roles COBIS/SAPHANA. ● Alertas SOC. ● Modificación tiempo de retención.	● Configuration Audit System(agente). ● Definición alertamiento reglas COBIS producción. ● Validación y ajuste sobre políticas de seguridad. ● Alertamiento SOC. ● Monitoreo y reglas alcance negocio.

Enfoque en servidores productivos

Regla	Cantidad de eventos
Data Exfiltration	77363
SQL Injection - Tautology	11752
OS Command Injection	8920
Cross-Site Scripting (XSS)	452

A continuación el comportamiento de algunos de los usuarios, de las bases de datos que se encuentran monitoreadas por guardium:

Servidor base de datos Usuario de base de datos	Cross-Site Scripting (XSS)	Data Exfiltration	OS Command Injection	SQL Injection - Tautology
172.16.126.68				
ESBFILE		1308		
ETLSYB	27			
IIBSCHM		1083		
INSTAP01	2	1140		
172.16.128.20				
CNX_COBISNS		38		
CNX_MON_ASEPROD		5		
CNXCONTROLGARANTIAS		1041		1232
COBISCTS3	2			1
COBROJUR		3		
CPPALACIOSR		15		
ETLSYB	23	16107		3199
GESTIONTRASLADOS				959
GGONZALEZ		1		
INTRANETPOOL		248		
JEMORENOR		31	1	
LIOPEREZQ		43		
OJURIDICA		58		70
OPBATCH		6083	7252	229
OPCRUZ		43		6
SA_OPERMON			1567	
172.16.131.128				
FNA2\SRVADMSQLPRO			1476	
NT SERVICE\SQLTELEMETRY\$MSSQL2017_1			57	
NT SERVICE\SQLTELEMETRY\$MSSQL2017OTP			14	
172.16.131.129				
FNA2\SRVADMSQLPRO			70	
NT SERVICE\SQLTELEMETRY\$MSSQL2017_1			12	
NT SERVICE\SQLTELEMETRY\$MSSQL2017OTP			54	
172.16.131.57				
BOGPVPPWP023\CTS_BV (OS USER)		313		
FNA2\BACKUP				187
FNA2\FRARODRIGUEZO				1
FNA2\ILCERRASE				2
FNA2\ILCERRASE (OS USER)				1
FNA2\SQLSERVICEPRO		3	100	119
192.168.180.153				
MONITOR		73		
SAPABAP1	398	37620		4063
SAPJAVA1		12107		

FNA_Basic
Data Security
Policy

FNA_Data Privacy - PII

Reglas bajo las cuales se generaron eventos para los siguientes usuarios, de las bases de datos monitoreadas por guardium:

Servidor base de datos Usuario de base de datos	Failed Login - Alert if repeated	Grant Commands, PII Objects - Log INFO	Uncommon other	Uncommon real traffic
172.16.126.68				
ESBFILE	1814			
IIBSCHM	1952			
INSTAP01	3			
172.16.128.20				
CNX_COBISNS	48			
GGONZALEZ	1			
JEMORENOR			1	1
LJOPEREZQ				3
OPORTIZ	1			
SRODRIGUEZ		12		
172.16.131.57				
FNA2\SQLSERVICEPRO	2		4	

Política asignación roles

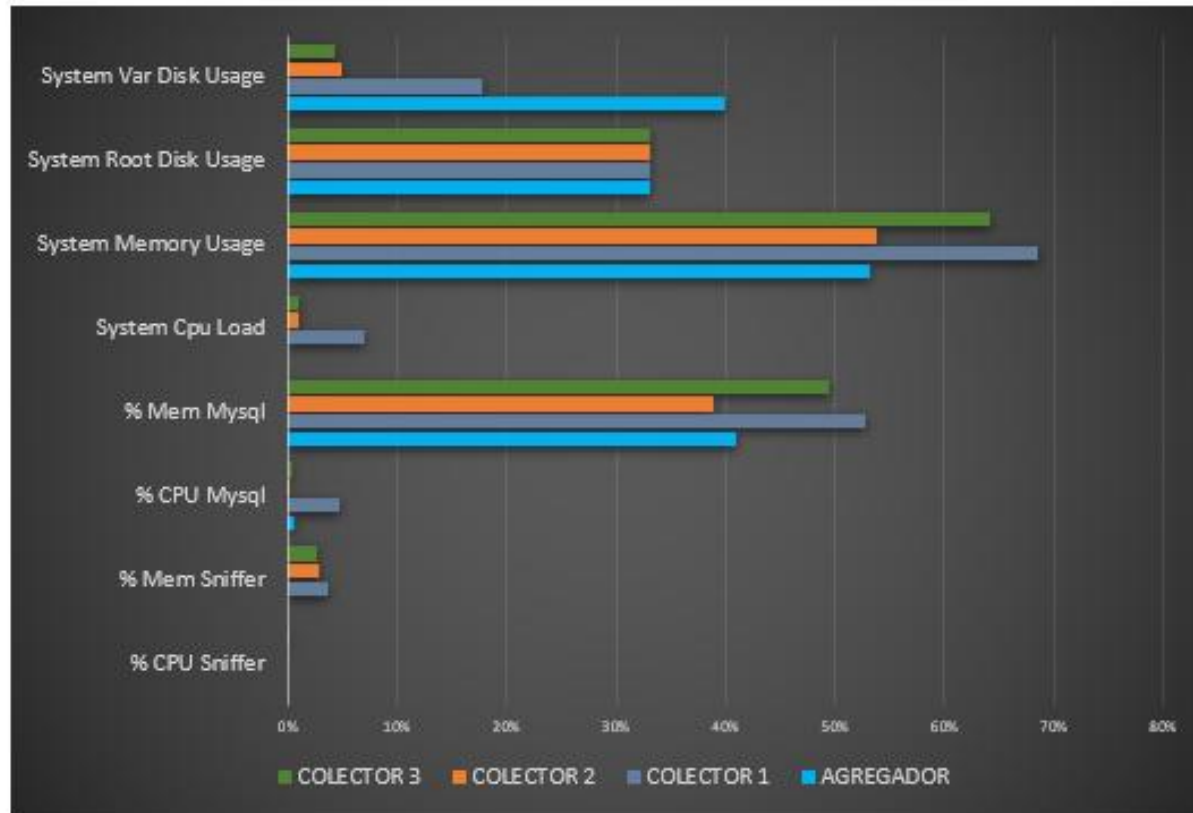
COBIS

182 eventos de
asignación de roles /
181 eventos de
eliminación de roles,
para usuarios de
aplicación

SAPHANA

46 eventos de
asignación de roles / 61
eventos de eliminación
de roles, para usuarios
de aplicación

Comportamiento plataforma, 22 de diciembre de 2024 al 21 de enero de 2025

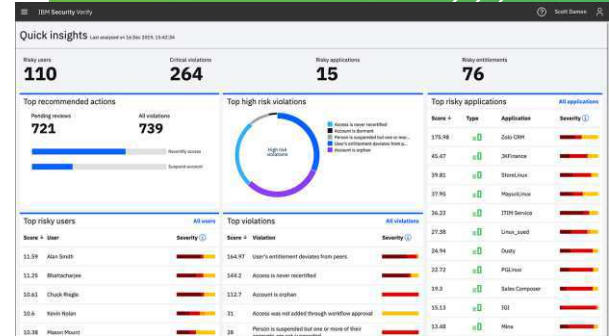




Verify

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 prescindir por completo de contraseñas para acceder más rápidamente a los datos y las aplicaciones.



Verify

Durante el desarrollo de gestión y administración de Verify en el periodo actual, se siguen monitoreando y ajustando las integraciones con directorio activo, service manager y SAP, no se presentan incidencias relacionadas con la disponibilidad del servicio.

Para las nuevas integraciones se realizaron las siguientes reuniones:

- **Integración - Administración de Usuarios: se realiza reunión el 16 de enero de 2025 para validar el estado de los desarrollos para la integración, por parte de fábrica nos informan que se sigue trabajando en el Backend, se define hacer una nueva reunión para revisar avances queda pendiente por definir la fecha.**

Verify

A la fecha del 21 de enero de 2025 para las siguientes integraciones nuevas no nos han definido fecha para las reuniones de avances:

- **Integración Verify – Sistema de turnos**
- **Integración Verify – E-Finac:**
- **Integración Verify – WorkManager**
- **Integración Verify – Bizagi**

Operaciones realizadas por Verify

En el periodo de diciembre 22 de 2024 a enero 21 de 2025 Verify realizó un total de 13937 operaciones discriminadas por servicios de acuerdo con el siguiente cuadro:

Total de operaciones realizadas por Verify entre Diciembre 22 de 2024 a Enero 21 de 2025

Servicio	Cambiar contraseña	Crear cuenta	Modificar cuenta	Restaurar cuenta	Suprimir cuenta	Suspender cuenta	Total por Servicio
Directorio Activo	1000	25	163	1253	0	1449	3890
SAP	0	70	62	737	0	829	1698
Service Manager	0	25	163	1253	0	1449	2890
Verify	1277	25	24	1297	0	1452	4075
Cobis	0	26	15	687	0	656	1384
Total Operaciones Solucion							13937

Las operaciones de Suspender cuenta y Restaurar cuenta tuvieron un incremento significativo en este periodo de acuerdo con las ausencias reportadas por vacaciones y permisos de fin de año.

Directorio Activo

Para el periodo de diciembre 22 de 2024 a enero 21 de 2025 se continúa monitoreando la ejecución de los Jobs configurados en producción Verify y se atienden los casos específicos que nos envían de la mesa de servicio y gestión de accesos; se revisan las solicitudes atendidas con respecto al servicio del directorio activo para mejora y estabilización del sistema después del paso a producción.

Cancelar solicitud		Renovar				
Selec	Estado	Tipo de solici...	Fecha de envío	Solicitante	Solicitada para	Nombre de s...
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:11:16	Usuario Integracion SM	Jacobo Barrios Solano	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:11:11	Usuario Integracion SM	Jacobo Barrios Solano	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:07:11	Usuario Integracion SM	Jorge Eduardo Gomez Echavarria	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:07:11	Usuario Integracion SM	Jorge Eduardo Gomez Echavarria	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:06:42	Usuario Integracion SM	Camilo Andres Vargas Sanchez	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:06:42	Usuario Integracion SM	Camilo Andres Vargas Sanchez	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:06:12	Usuario Integracion SM	Sandra Cristina Jimenez Cifuentes	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:06:12	Usuario Integracion SM	Sandra Cristina Jimenez Cifuentes	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 15:10:47	Usuario Integracion SM	Nelson Enrique Ceballos Reyes	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 15:10:27	Usuario Integracion SM	Nelson Enrique Ceballos Reyes	Directorio Activo
	✓ Satisfactorio	Conciliación	27 de diciembre de 2024 12:01:25	Sistema		Directorio Activo
	✓ Satisfactorio	Adoptar cuenta	27 de diciembre de 2024 10:39:36	NELSON SARMIENTO	Caroline Ivonne Ballesteros Camargo	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 10:21:10	Usuario Integracion SM	Claudia Juliana Marin Zuluaga	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 10:21:05	Usuario Integracion SM	Claudia Juliana Marin Zuluaga	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 10:20:45	Usuario Integracion SM	Claudia Juliana Marin Zuluaga	Directorio Activo
	✓ Satisfactorio	Conciliación	27 de diciembre de 2024 0:01:29	Sistema		Directorio Activo
	✓ Satisfactorio	Adoptar cuenta	26 de diciembre de 2024 16:15:00	NELSON SARMIENTO	Leidy Briggitt Mosquera Cauca	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	26 de diciembre de 2024 14:40:47	Usuario Integracion SM	Lisseth Tatiana Molina Carvajal	Directorio Activo
	✓ Satisfactorio	Cambiar cuenta	26 de diciembre de 2024 14:40:27	Usuario Integracion SM	Lisseth Tatiana Molina Carvajal	Directorio Activo
	✓ Satisfactorio	Conciliación	26 de diciembre de 2024 12:00:51	Sistema		Directorio Activo
	✓ Satisfactorio	Restaurar cuenta	26 de diciembre de 2024 11:30:56	NELSON SARMIENTO	Alvaro Tavera Torres	Directorio Activo
	✓ Satisfactorio	Conciliación	26 de diciembre de 2024 0:00:49	Sistema		Directorio Activo
Página 1 de 1		Total: 22 Visualizados: 22 Seleccionados: 0				

SERVICE MANAGER

Para el periodo de diciembre 22 de 2024 a enero 21 de 2025 se continúa monitoreando la ejecución de los Jobs configurados en producción y se atienden los casos específicos que nos envían de gestión de accesos y el equipo de Service Manager; se revisan las solicitudes atendidas con respecto Service Manager para mejora y estabilización del sistema después del paso a producción.

De parte del equipo de service manager no nos han informado fecha para iniciar pruebas desde verify hacia el ambiente que están migrando a la nueva versión.

SAP

Para el periodo de diciembre 21 de 2024 a enero 22 de 2025 se continúa monitoreando la ejecución en producción y se atienden los casos específicos que nos envían de gestión de accesos; se revisan las solicitudes atendidas con respecto SAP para mejora y estabilización del sistema después del paso a producción.

Cancelar solicitud		Renovar				
☐ Select ^	Estado ^	Tipo de solici... ^	Fecha de envío ^	Solicitante ^	Solicitada para ^	Nombre de s... ^
	✓ Satisfactorio	Conciliación	27 de diciembre de 2024 23:01:00	Sistema		SAP - PRD
	✓ Satisfactorio	Suspender cuenta	27 de diciembre de 2024 17:11:16	Usuario Integracion SM	Jacobó Barrios Solano	SAP - PRD
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 17:11:11	Usuario Integracion SM	Jacobó Barrios Solano	SAP - PRD
	✓ Satisfactorio	Suspender cuenta	27 de diciembre de 2024 15:10:52	Usuario Integracion SM	Nelson Enrique Ceballos Reyes	SAP - PRD
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 15:10:47	Usuario Integracion SM	Nelson Enrique Ceballos Reyes	SAP - PRD
	✓ Satisfactorio	Suspender cuenta	27 de diciembre de 2024 10:21:10	Usuario Integracion SM	Claudia Juliana Marin Zuluaga	SAP - PRD
	✓ Satisfactorio	Cambiar cuenta	27 de diciembre de 2024 10:21:05	Usuario Integracion SM	Claudia Juliana Marin Zuluaga	SAP - PRD
	✓ Satisfactorio	Conciliación	26 de diciembre de 2024 23:00:25	Sistema		SAP - PRD
	✓ Satisfactorio	Cambiar cuenta	26 de diciembre de 2024 14:40:52	Usuario Integracion SM	Lisseth Tatiana Molina Carvajal	SAP - PRD
	✓ Satisfactorio	Cambiar cuenta	26 de diciembre de 2024 14:40:47	Usuario Integracion SM	Lisseth Tatiana Molina Carvajal	SAP - PRD
Página 1 de 1		Total: 10 Visualizados: 10 Seleccionados: 0				

Cobis

El día 24 de diciembre de 2024 se soluciona el inconveniente y se sigue configurando el adaptador de Verify y poder ponerlo en producción.

El adaptador de integración de verify queda listo y funcionando en producción la primera semana de enero de 2025

Se monitorea la ejecución de los Jobs configurados en Verify y se atienden los casos específicos que nos envían de la mesa de servicio, gestión de accesos.

Cancelar solicitud		Renovar				
☐ Seleccionar	Estado	Tipo de solicitud	Fecha de envío	Solicitante	Solicitada para	Nombre de servicio
	☒ Satisfactorio	Cambiar cuenta	14 de enero de 2025 12:26:12	Usuario Integracion SM	Julian David Portilla Pinzon	COBIS
	☒ Satisfactorio	Cambiar cuenta	14 de enero de 2025 8:56:09	Usuario Integracion SM	Diana Carolina Vasquez Rodriguez	COBIS
	☒ Satisfactorio	Cambiar cuenta	13 de enero de 2025 15:10:24	Usuario Integracion SM	Edison Fabian Dominguez Leon	COBIS
	☒ Satisfactorio	Cambiar cuenta	13 de enero de 2025 15:10:23	Usuario Integracion SM	Edison Fabian Dominguez Leon	COBIS
	☒ Satisfactorio	Cambiar cuenta	13 de enero de 2025 15:10:21	Usuario Integracion SM	Edison Fabian Dominguez Leon	COBIS
	☒ Satisfactorio	Cambiar cuenta	13 de enero de 2025 15:10:20	Usuario Integracion SM	Edison Fabian Dominguez Leon	COBIS
Página 1 de 1		Total: 6 Visualizados: 6 Seleccionados: 0				

ADMINISTRACION DE USUARIOS

El jueves 16 de enero de 2025 se realizó una reunión con el equipo de administración de usuarios donde nos confirman que siguen trabajando en el Backend, no nos dan fecha aproximada de entrega.

AUTOGESTION

Para el periodo de diciembre 22 de 2024 a enero 21 de 2025 se continúa monitoreando la ejecución en producción y se atienden los casos específicos que nos envían la mesa de servicio; se revisan las solicitudes atendidas con respecto a Autogestión para mejora y estabilización del sistema después del paso a producción

Buscar solicitudes	206 de 233 de 233	1...7 8 9 10	Clasificar por: Fecha ▼ Solicitada para Estado
Solicitudes actuales			
Historial de solicitudes			
Fecha inicial:			
22/12/2024			
Fecha de finalización:			
22/1/2025			
Para			
Maria Fernanda Amezcua Sanchez			
Liliana Vargas Daza			
Jorman David Rojas Peña			
Mayra Alejandra Espinosa Rodriguez			
Adriana Rojas Gonzalez			
✓	Nancy Carolina Castañeda Alvarez - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8361720830542223863	Ver detalles	
✓	Alexandra Jimenez Hernandez - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8357459426159132981	Ver detalles	
✓	Leidy Johanna Sanchez Castro - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 835706050670683106	Ver detalles	
✓	Diana Mercedes Arcos Muñoz - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8356904752138017124	Ver detalles	
✓	Leidy Johanna Sanchez Castro - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8354786003060502947	Ver detalles	
✓	Diana Mercedes Arcos Muñoz - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8353971152396563108	Ver detalles	
✓	Diana Mercedes Arcos Muñoz - Editar perfil	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8353782854417583597	Ver detalles	
✓	Andrea Liliana Escobar Correa - Cambiar contraseña	Completada: 23/12/2024	
Cumplido	Solicitado por: NELSON SARMIENTO Número de solicitud: 8335038647705426575	Ver detalles	
206 de 233 de 233	1...7 8 9 10		

Recomendaciones y conclusiones

Para este periodo se continua con el monitoreo de la ejecución de las integraciones con SAP, Directorio activo, Service Manager y la activación de Autogestión en producción para la estabilización y mejora del sistema.

Se programan reuniones técnicas con los equipos de Administración de Usuario.

Se solucionan los inconvenientes con la integración de Cobis y se configuran los conectores en producción.

Se hace el acompañamiento en la prueba de recorrido para la verificación del funcionamiento de la solución de autogestión de contraseñas con resultados satisfactorios.

Se hace el acompañamiento en la Reunión Prueba de Recorrido Requerimiento RF-ITGCs

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

Para el 28 de enero de 2025 se programa el inicio de la capacitación del portal de Autogestión para los funcionarios del FNA.



37

Eventos reportados

25

Identity Fraud

9

Data protection

3

Brand protection

Informe Monitoreo de marca

2025

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 enero de 2025.

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

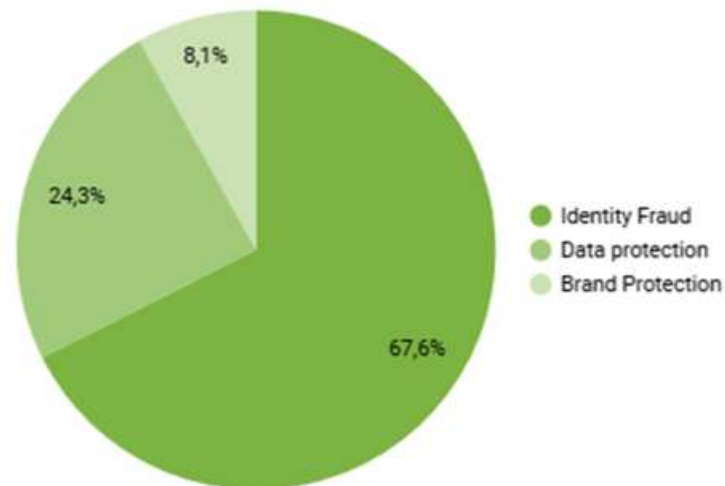
En el monitoreo de marca se busca realizar una captación de la información durante el periodo en mención, en la cual podemos identificar la presencia que tiene la entidad en la Clear, Deep y Dark Web, empleando distintas técnicas digitales que nos permita acceder. En un servicio 7x24 para la identificación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

Resultados Monitoreo de Marca



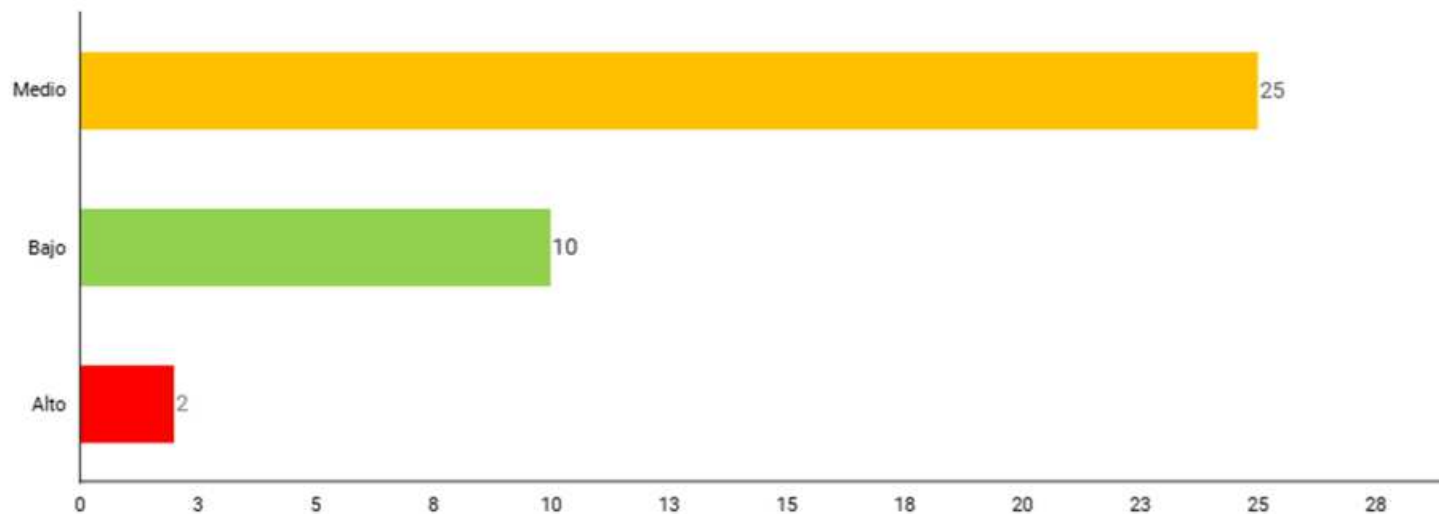
1. Comportamiento del servicio global Vigilancia

% de afectación por subservicio

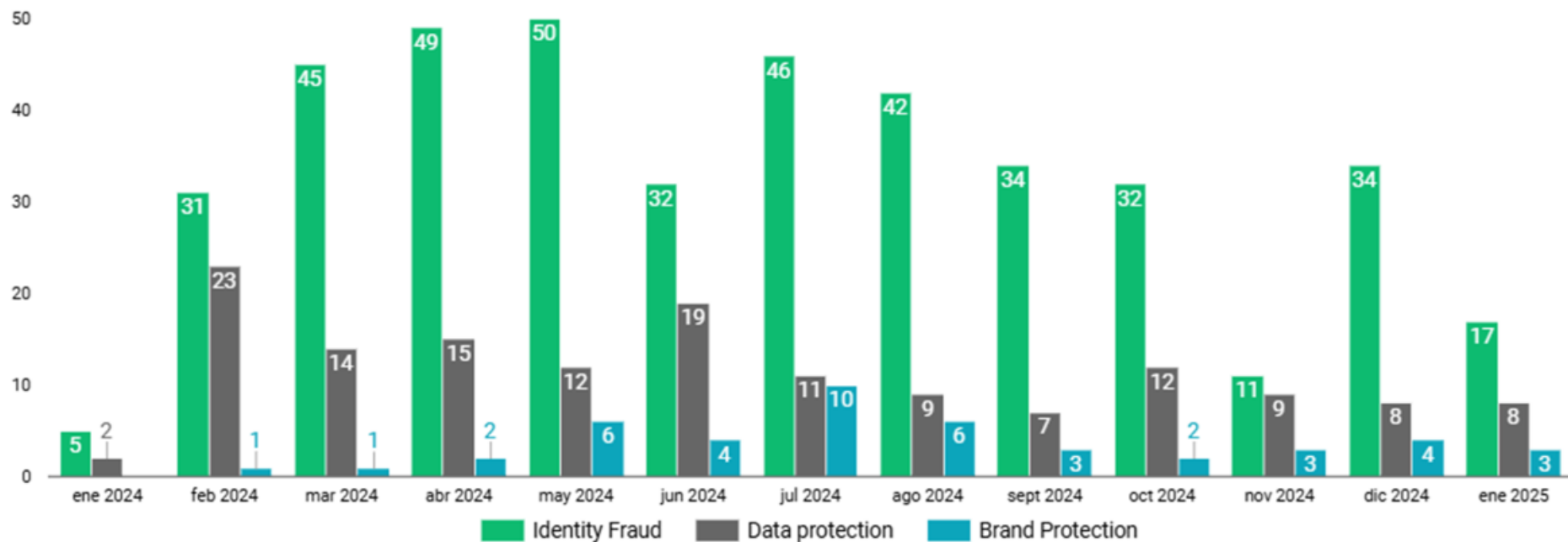


KPIs > Comportamiento del servicio global

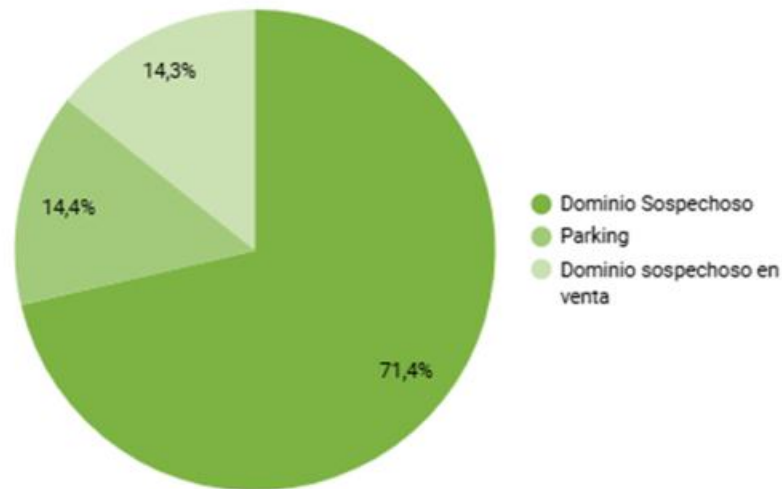
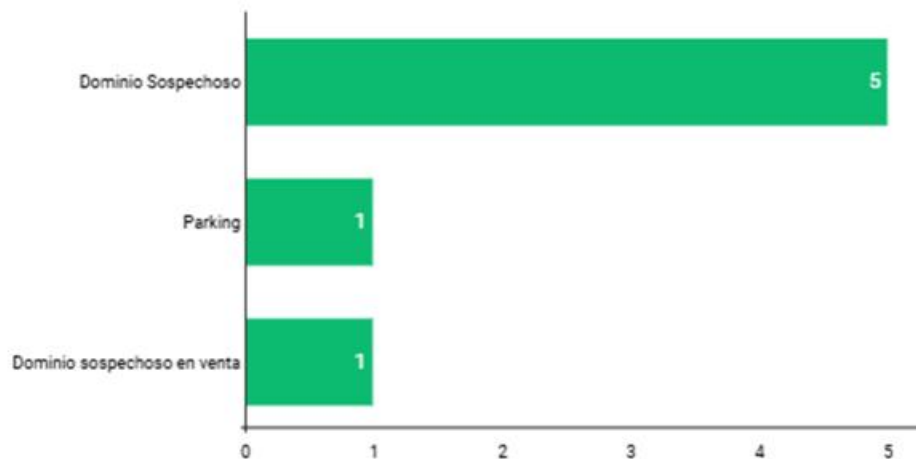
ALERTAS CLASIFICADAS POR CRITICIDAD



Evolución del servicio a nivel mensual



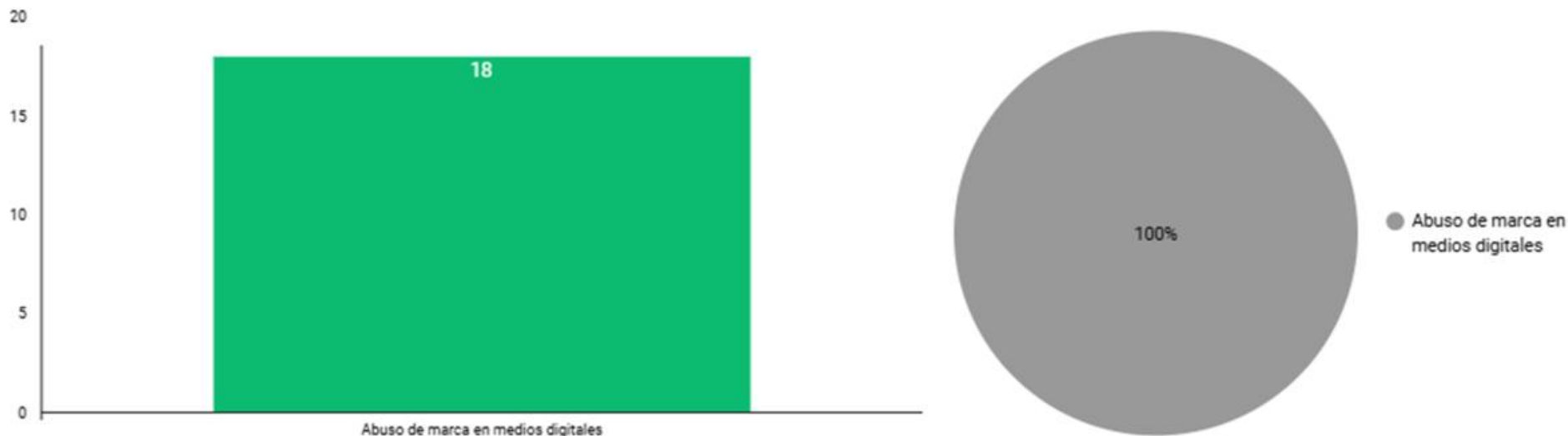
Resultados Monitoreo de Marca



Resultados Monitoreo de Marca

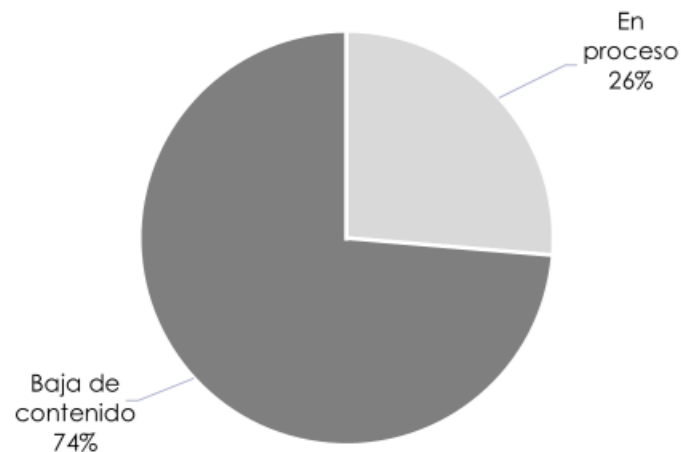
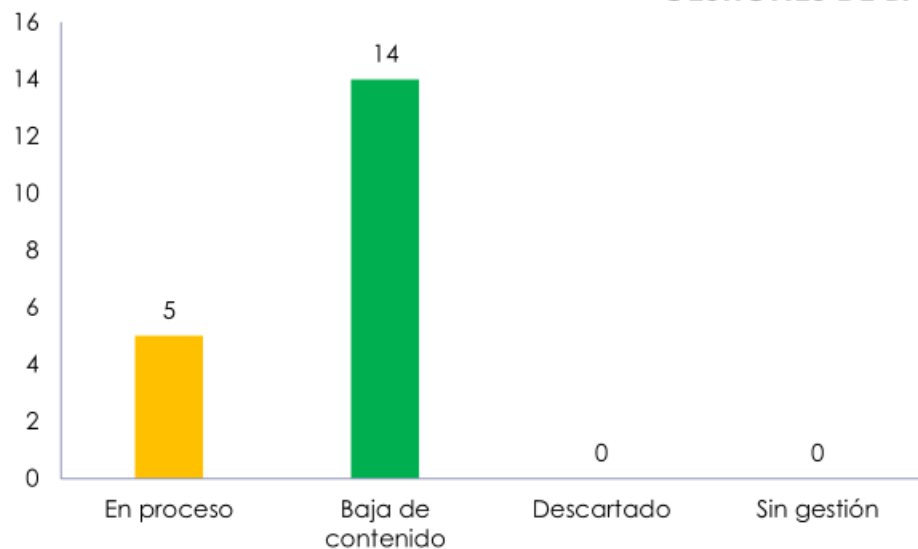
2. Abuso de marca

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

GESTIONES DE BAJA



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.

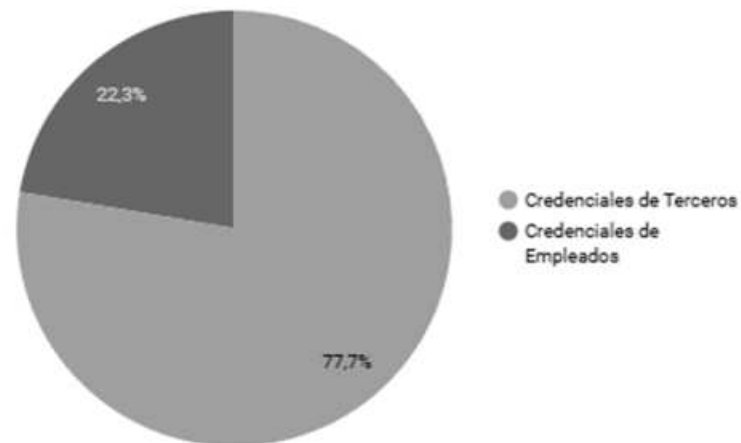
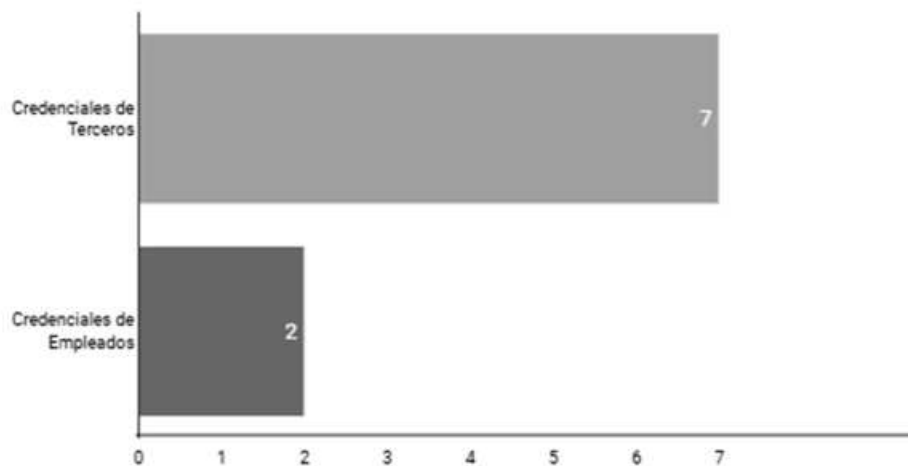
Sin gestión: Eventos sin gestionar. Pendientes de la solicitud del cliente.

Resultados Monitoreo de marca

3. Información Expuesta – Credenciales filtradas

Volumetría por tipo de fuga

Nº Total de Alertas enviadas: 9

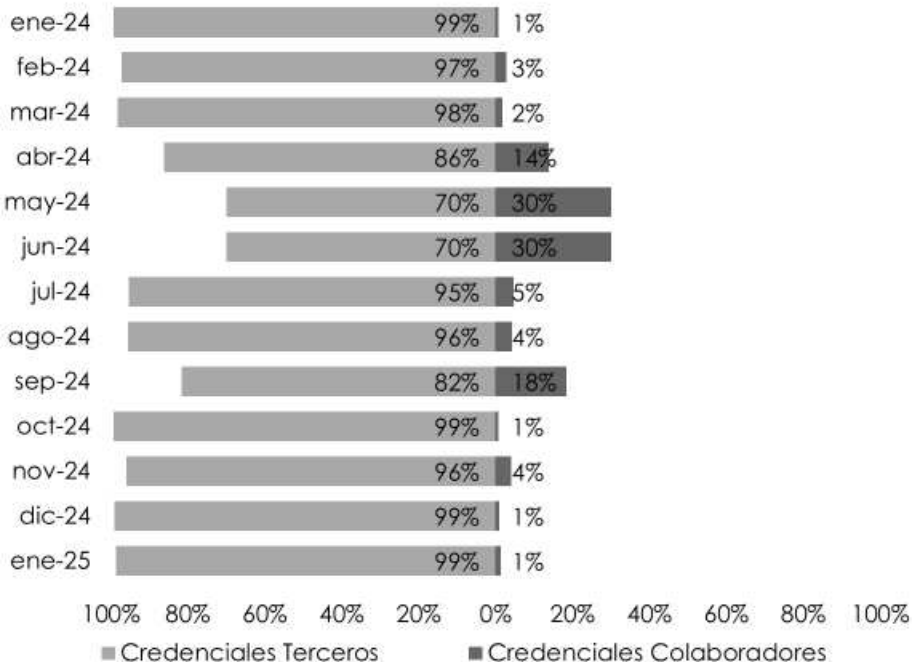


Resultados Monitoreo de marca

Histórico > Evolución del servicio a nivel mensual

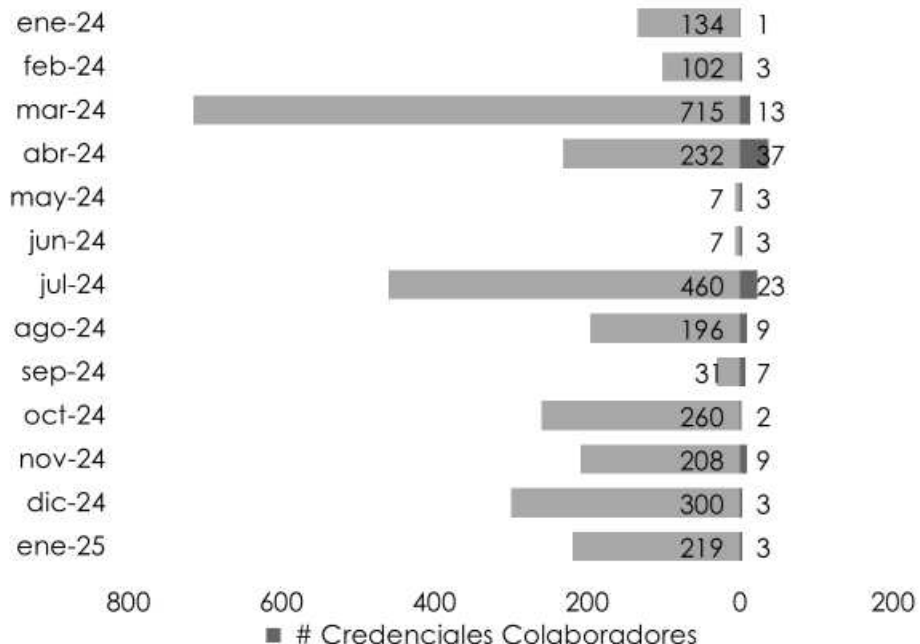
Deteccion de credenciales

% deteccion terceros VS colaboradores



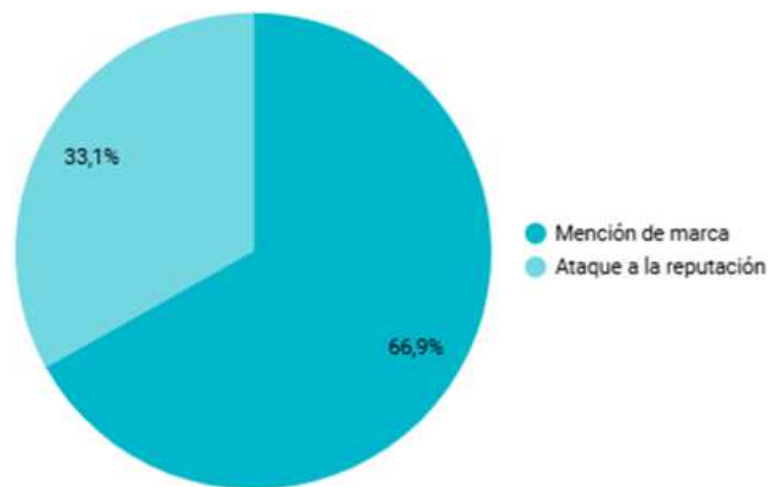
Deteccion de credenciales

de credenciales identificadas terceros VS colaboradores



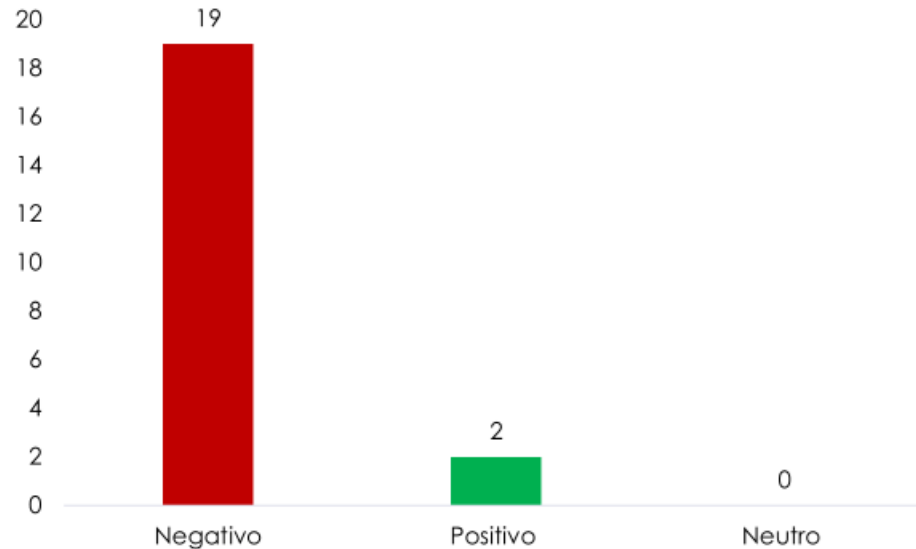
Resultados Monitoreo de marca

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 una disminución en el volumen de credenciales identificadas para la tipología de credenciales de terceros.

Observación: Se tuvo una efectividad del 74% al momento realizar las gestiones de baja solicitadas.



Informe Seguridad Ofensiva

2025

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 diciembre hasta el 21 de enero del año 2025.

0

Ethical Hacking

0

Retest Ethical Hacking

8

Retest Análisis de Vulnerabilidades

2

Análisis de Vulnerabilidades

0

Análisis de Código

1

Ingeniería Social

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

Durante el periodo evaluado, se documentaron un total de 11 solicitudes. Este número refleja una igualdad de solicitudes con respecto al periodo anterior, lo que indica una ligera actividad en la gestión de solicitudes. A continuación, se presenta un gráfico que ilustra esta tendencia de incremento.



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

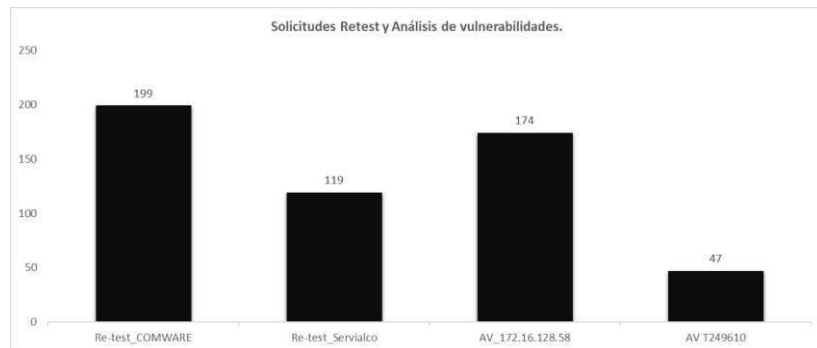


Durante el periodo reportado, se ejecutaron un total de 8 solicitudes de Retest relacionadas con análisis de vulnerabilidades (RAV), así como 2 análisis de vulnerabilidades adicionales y 1 ejercicio de ingeniería social. Estas actividades tuvieron como objetivo verificar la remediación de las vulnerabilidades previamente identificadas y asegurar que las medidas correctivas implementadas fueran efectivas.

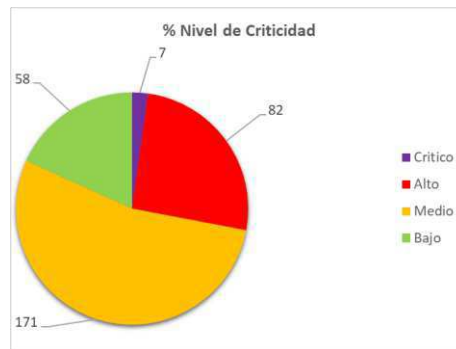
Resultados de solicitudes (Retest y AV)

Resultados Retest - General

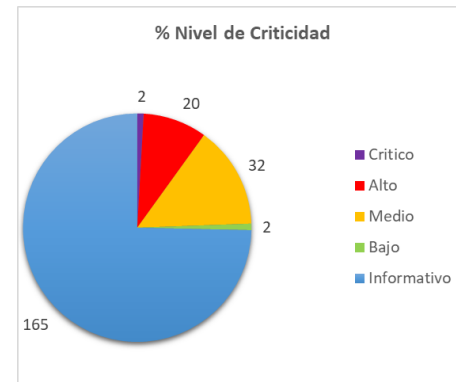
Resultados – De las solicitudes de Retest realizadas, se reportaron un total de **318** vulnerabilidades para su respectivo escaneo y validación. En cuanto a los escaneos iniciales en busca de vulnerabilidades se identificaron **221** hallazgos, los cuales fueron debidamente analizados y clasificados. A continuación, se detallan las actividades realizadas durante este proceso:



Resultados – A continuación, se presenta el porcentaje por nivel de criticidad de las vulnerabilidades identificadas durante los ejercicios de **Retest** reportados. Las vulnerabilidades se organizan desde las de mayor criticidad hasta las de menor criticidad, lo que permite visualizar claramente las áreas que requieren atención inmediata y las que pueden ser abordadas en un plazo más largo.



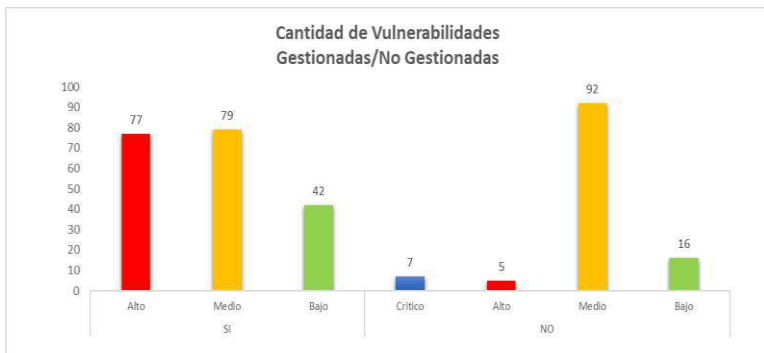
Resultados – A continuación, se presenta el porcentaje por nivel de criticidad de las vulnerabilidades identificadas durante los ejercicios de **análisis de vulnerabilidades** reportados.



Resultados de solicitudes (Retest y AV)

Resultados Retest y Análisis de Vulnerabilidades Remediadas - General

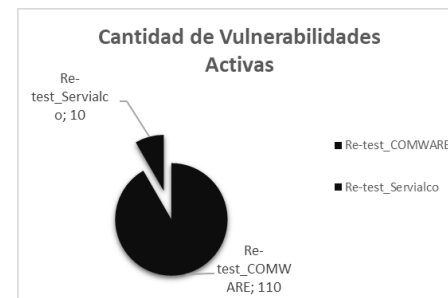
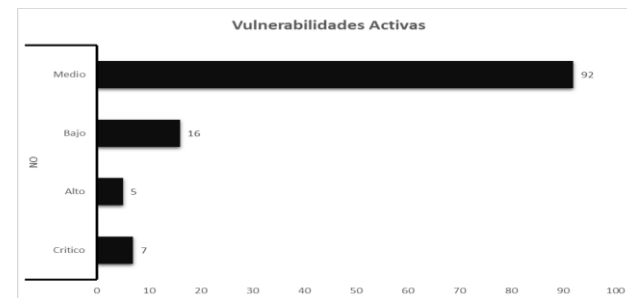
De las **318** vulnerabilidades reportadas en los re-test, **198** fueron remediadas y **120** continúan activas.



SI	198
Alto	77
Medio	79
Bajo	42

NO	120
Critico	7
Alto	5
Medio	92
Bajo	16

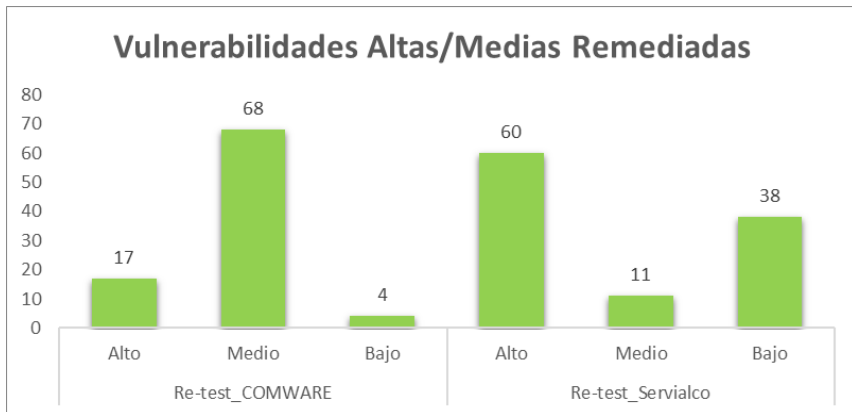
En los retest del periodo reportado, **se evidencian** varias **vulnerabilidades** de nivel **críticas, altas, medias y bajas** que aún están **activas**.



Resultados de solicitudes (Retest y AV)

Resultados Retest AV Remediadas - General

De las **198** vulnerabilidades remediadas se destaca la efectividad de solución de las medias.



Del total de **vulnerabilidades activas (120)** los activos que se destacan con **más vulnerabilidades** son 172.16.126.52 (**11 vuln**), 172.16.132.44 (**10 vuln**) y 172.31.1.10 (**10 vuln**) los activos identificados hacen parte de la administración de Comware y Servialco.

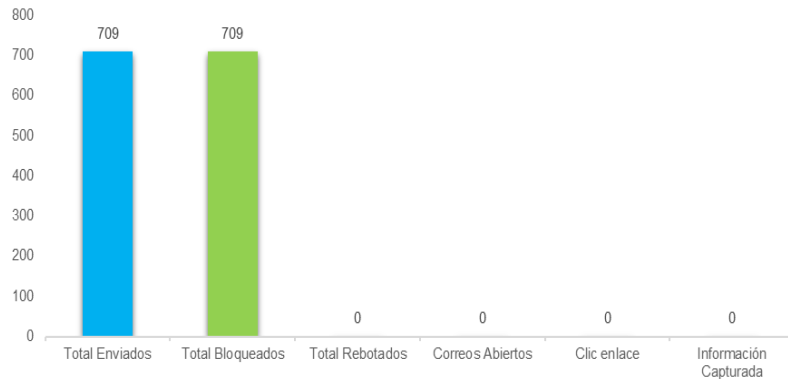
Host	Critico	Alto	Medio	Bajo	Total
172.16.126.52	2	2	5	2	11
172.16.132.44	0	1	9	0	10
172.31.1.10	1	0	6	3	10
172.16.132.41	0	0	7	2	9
172.16.132.39	0	0	8	0	8

Resultados Ingeniería Social

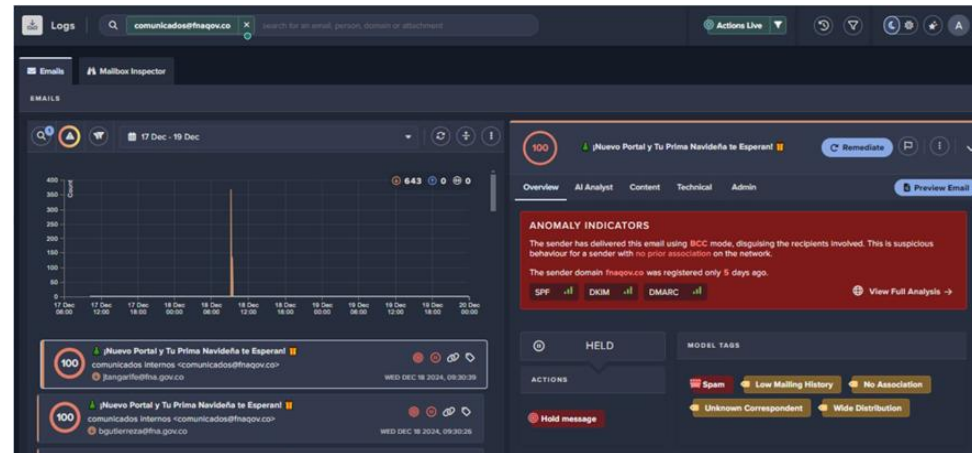
Resultados Ingeniería Social (Phishing Entorno Real) - General

En la campaña se envió a un total de **709** destinatarios de correo electrónico durante el tiempo del ejercicio comprendido desde el **18 y 19** de diciembre, los resultados se pueden visualizar mejor en las siguientes gráficas.

Resultado General



De los **709** correos enviados, la mayoría fueron bloqueados por los controles de seguridad, demostrando su eficacia. Además, **14** correos fueron reportados por los usuarios, reflejando una respuesta proactiva, aunque persiste la necesidad de mejorar los filtros y la capacitación del personal.



Resultados Ingeniería Social

Resultados Ingeniería Social (Phishing Entorno Controlado) - General

En la campaña se envió a un total de **1703** destinatarios de correo electrónico durante el tiempo del ejercicio comprendido desde el **26** hasta el **30** de diciembre, los resultados se pueden visualizar mejor en las siguientes gráficas.

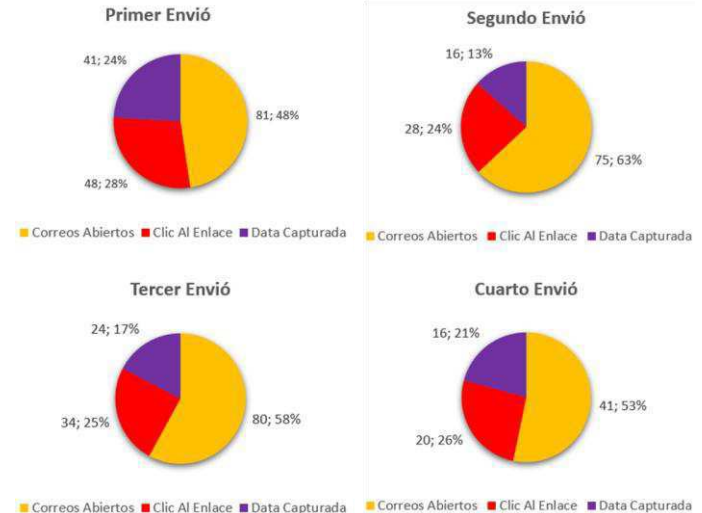
Primer Envío	
Correos Enviados	470
Correos Abiertos	81
Clic Al Enlace	48
Data Capturada	41

Segundo Envío	
Correos Enviados	475
Correos Abiertos	75
Clic Al Enlace	28
Data Capturada	16

Tercer Envío	
Correos Enviados	497
Correos Abiertos	80
Clic Al Enlace	34
Data Capturada	24

Cuarto Envío	
Correos Enviados	261
Correos Abiertos	41
Clic Al Enlace	20
Data Capturada	16

La campaña constó de **cinco** fases: cuatro con cerca de **500** correos cada una y una última con **261**. El asunto, “**Cambio requerido de contraseña en Verify,**” simulaba una actualización obligatoria de seguridad. El correo urgía a cambiar la contraseña antes del **31** de **diciembre** para evitar problemas de acceso, incluyendo un enlace a un portal falso diseñado para imitar el de la entidad.



Resultados Ingeniería Social

Resultados Ingeniería Social (Phishing Entorno Controlado) - General



74%

Usuarios
seguros



14%

Usuarios en
riesgo medio



12%

Usuarios en
riesgo alto

26 y 27 - DIC

Mayor flujo de actividad en correos

PUNTO FUERTE

¡Usuarios que no abrieron el
correo phishing!

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 31122024_COMWARE
 - Re-test 31122024_Servialco
 - Re-test 31122024_Servialco_2
 - Re-test 07012025_Servialco
 - Re-test 07012025_Servialco_2
 - Re-test 13012025_Servialco
 - Re-test 16012025_COMWARE
 - Re-test 20012025_SERVIALCO
- A continuación, se listan las actividades realizadas en los análisis de vulnerabilidades.
 - AV 172.16.128.58
 - AV T249610



Recomendaciones y conclusiones

- Durante el proceso de re-test, se observó un aumento considerable en el número total de vulnerabilidades únicas auditadas, que pasó de 30 a 28 en comparación con el mes anterior. En total, se gestionaron 318 hallazgos, los cuales fueron abordados mediante los re-tests correspondientes. Esta reducción en el número de vulnerabilidades refleja avances en la remediación de los problemas detectados y una mejora en la postura de seguridad, ya que se trató un número importante de vulnerabilidades de crítico y alto impacto.
- Las vulnerabilidades activas que afectan al mayor número de activos están relacionadas con los siguientes hallazgos:
 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
 - SSL Certificate Cannot Be Trusted
 - SSH Weak Key Exchange Algorithms Enabled
 - SSL Self-Signed Certificate
 - TLS Version 1.0 Protocol Detection
 - SSL Certificate Expiry
- Las campañas de phishing han tenido buena recepción, permitiendo recopilar datos útiles sobre la percepción de los usuarios ante simulaciones de ingeniería social. Los resultados evidencian un riesgo significativo desde las primeras fases.
- El control antispam existente es un punto fuerte, ya que logra evitar la llegada de correos maliciosos a las bandejas de entrada de los usuarios. Agregar el dominio de prueba a las listas blancas de la solución actual muestra una capacidad de adaptación para mejorar aún más las defensas contra correos maliciosos



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 diciembre de 2024 y el 21 de enero de 2025.

Objetivos

- Evaluar los controles comprendidos en las 18 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

390

Activos evaluados

0

Activos duplicados

4

Activos sin controles

13

Activos sin conexión en un mes

18

Políticas evaluadas

3.489

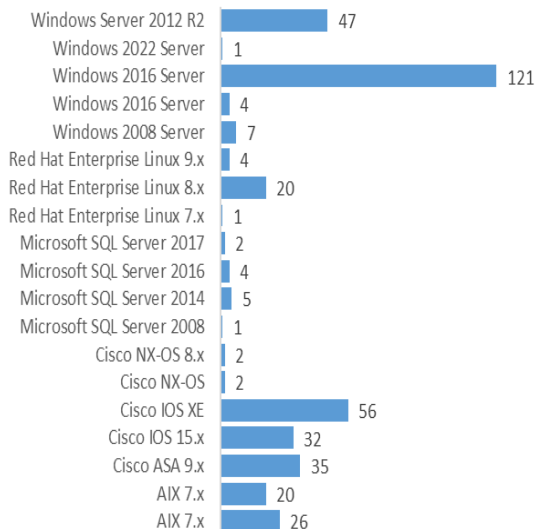
Controles evaluados

62,92%
Controles superados

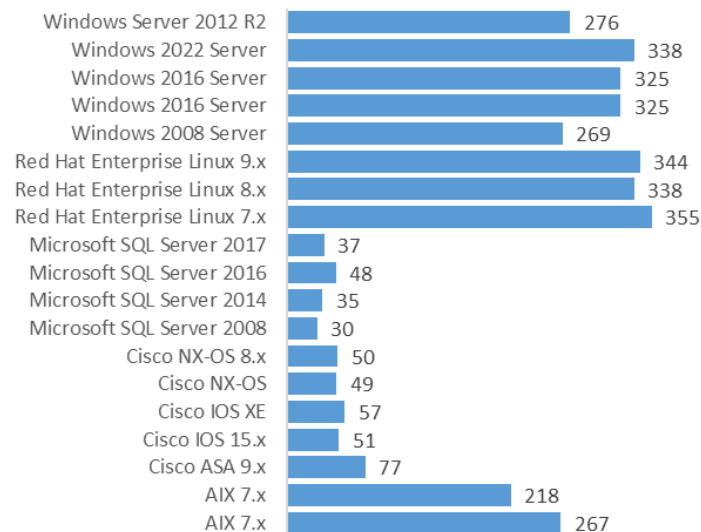


37,07%
Controles fallidos

Activos evaluados por tecnología

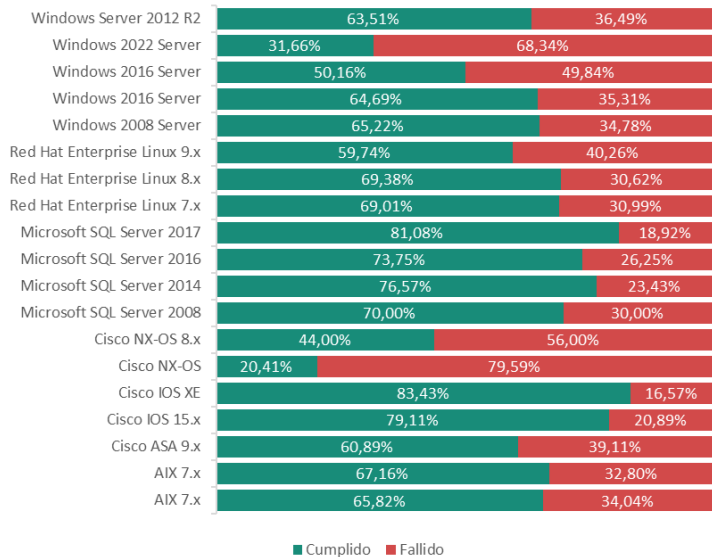


Controles evaluados por tecnología

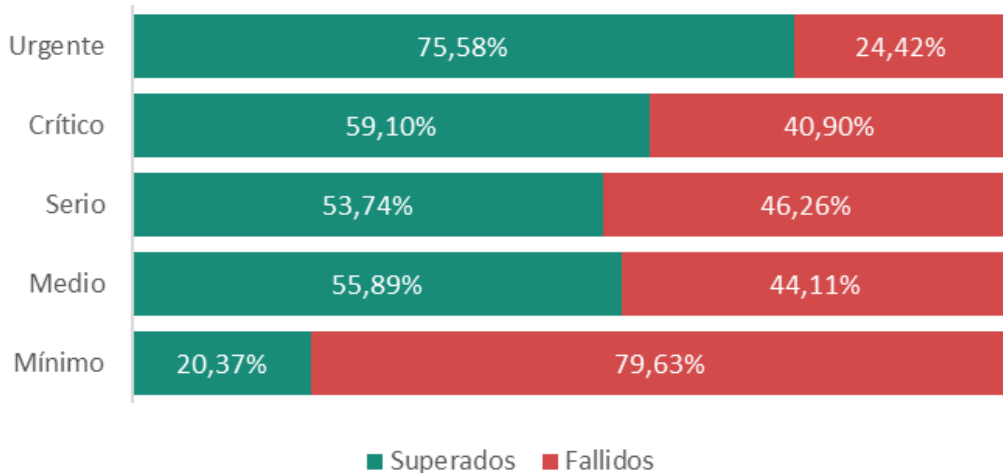


EVALUACIÓN DE LÍNEAS BASE

Cumplimiento por tecnología



Cumplimiento por severidad



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

- Los cambios en las métricas mostrados mes a mes se deben a la eliminación o adición de agentes, reinstalación de agentes, solución de problemas de conexión con el Gateway.
- 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).
- 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 de información sobre servidores Windows sin reportar en más de un mes
4. Solicitud de información sobre servidores AIX sin reportar en más de un mes
5. Solicitud de información sobre servidores Linux sin reportar en más de un mes
6. identificación de causa de duplicidad de activos
7. Generación de reportes de cumplimiento bajo demanda
8. Sesiones de entendimiento de plataforma e informes generados
9. Solicitud de inventario 2025 de dispositivos de red, bases de datos y servidores (Linux, AIX y Windows)
10. Actualización de políticas en plataforma, programación de escaneos y reportes mensuales



Fortify SCA

Informe de Actividades y Funcionamiento Fortify

2025

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 diciembre y el 21 de enero de 2025.

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 este período, no se llevaron a cabo integraciones.

Rendimiento y Disponibilidad:

No se registraron tiempos de inactividad, tanto planificados como no planificados. Además, el rendimiento del sistema se mantuvo dentro de los parámetros normales, incluso durante los picos de carga máxima.

Esta estabilidad refleja un nivel adecuado de operación y una infraestructura tecnológica sólida y bien gestionada. Se continúa con las prácticas actuales de monitoreo y gestión de la infraestructura para garantizar que el sistema mantenga su disponibilidad y rendimiento en niveles óptimos a medida que evolucionen las demandas de carga.

Planes para futuras mejoras o actualizaciones:

- Actualmente, la suite Fortify se encuentra actualizada a una versión estable proporcionada por el fabricante. Esta actualización asegura que la herramienta esté alineada con las últimas mejoras de seguridad, correcciones de errores y nuevas funcionalidades, lo que optimiza su rendimiento y fiabilidad en el proceso de auditoría de aplicaciones. Es recomendable continuar con el monitoreo de futuras actualizaciones para mantener la suite al día y aprovechar las mejoras tecnológicas que el fabricante continúe implementando.



Gestión y actividades

- **Monitoreo del sistema:**

Se lleva a cabo una verificación periódica del estado de cada servidor y los componentes que alojan la suite Fortify. Hasta la fecha, y hasta el 21 de enero de 2025, los servidores y la aplicación han operado sin presentar fallas que hayan afectado la disponibilidad del servicio. Este desempeño refleja una gestión eficaz de la infraestructura y un adecuado mantenimiento preventivo.

Se recomienda continuar con la monitorización constante de los servidores, así como con las acciones de mantenimiento preventivo, para garantizar la continuidad y estabilidad del servicio a largo plazo.

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

Software Security Center (SSC): Es fundamental validar de manera regular el funcionamiento y las actualizaciones de las políticas de seguridad personalizadas utilizadas para la ejecución de informes de las aplicaciones auditadas. Este proceso asegura que las políticas sigan siendo efectivas frente a las amenazas actuales y que estén alineadas con las mejores prácticas y normativas de seguridad, las cuales están en constante evolución.

Fortify WebInspect Enterprise (WIE): Se lleva a cabo una validación continua de la integración con el módulo SSC (Software Security Center) para asegurar que no se generen errores que puedan comprometer el proceso de seguridad. Además, se realiza un monitoreo constante del estado de los escaneos ejecutados, con el objetivo de garantizar que los análisis de seguridad se realicen de manera efectiva y sin interrupciones.

Fortify WebInspect Sensor (WIS): Se lleva a cabo una validación periódica del estado del sensor para garantizar la disponibilidad y el correcto funcionamiento del módulo WebInspect. Esta verificación asegura que el sensor opere de manera adecuada, permitiendo la ejecución efectiva de los escaneos de seguridad en las aplicaciones auditadas sin interrupciones.

Gestión y actividades

- **Restablecimiento de Contraseñas para Usuarios de Dominio:**

Se solicitó a través de la mesa de soporte el restablecimiento de contraseñas de los usuarios de dominio utilizados en la autenticación de los servidores que alojan la suite Fortify (caso SD1187244). Esta acción busca reforzar la seguridad y proteger las credenciales contra accesos no autorizados.

- **Configuración de Usuarios para Administración y Escaneos:**

En la suite Fortify, se han configurado los usuarios necesarios para la administración y ejecución de los escaneos de las aplicaciones auditadas. Estos usuarios cuentan con privilegios específicos que les permiten gestionar de manera eficiente los procesos de análisis de seguridad, asegurando el cumplimiento de los estándares y políticas de seguridad de la información.

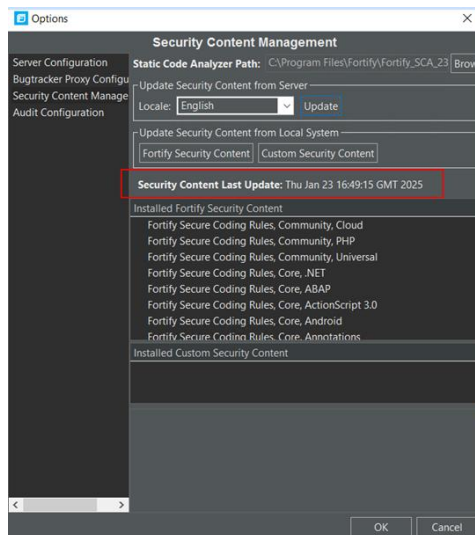


Gestión y actividades

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

Se realiza la actualización periódica de las políticas de seguridad y los rulepacks (conjuntos de reglas de seguridad) de los módulos SSC (Software Security Center), Audit Workbench y SCA. Estas actualizaciones son fundamentales para garantizar la efectividad de las herramientas de seguridad, adaptándolas a nuevas amenazas, vulnerabilidades emergentes y cambios en las regulaciones del sector.

Este proceso mejora la precisión en la detección de vulnerabilidades y optimiza los informes de seguridad generados durante las auditorías de aplicaciones.



Actividades realizadas

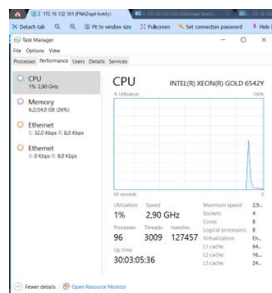
- **Restablecimiento de credenciales de usuario en el dominio de la suite Fortify:** A través de la mesa de ayuda, se gestionan y restablecen las credenciales de acceso de los usuarios del dominio, garantizando un acceso seguro y adecuado a la suite Fortify.
- **Actualización de Rulespacks del módulo SSC:** Se lleva a cabo la actualización periódica de los Rulespacks en el módulo SSC para asegurar que las reglas de seguridad estén actualizadas, mejorando así la detección de vulnerabilidades y adaptándose a las nuevas amenazas emergentes.
- **Actualización de Rulespacks del módulo Audit Workbench:** Se realiza la actualización de los Rulespacks en el módulo Audit Workbench, optimizando el análisis de código y permitiendo una evaluación más precisa y eficiente de las aplicaciones auditadas.



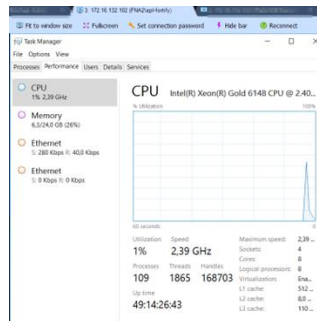
Disponibilidad y rendimiento del sistema.

A continuación, se detalla la disponibilidad y confiabilidad de la infraestructura, lo cual es clave para garantizar la continuidad del servicio de auditoría y análisis de seguridad sin interrupciones.

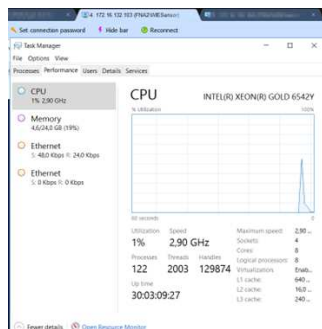
172.16.132.101



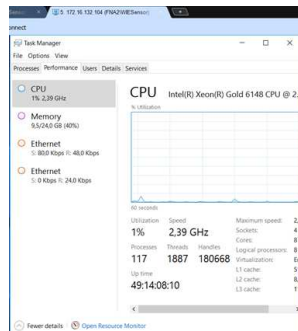
172.16.132.102



172.16.132.103



172.16.132.104



Conclusiones

- Durante el periodo indicado, la suite Fortify ha mantenido una operación estable y sin interrupciones, sin reportar caídas ni fallas. El mantenimiento y las actualizaciones constantes han garantizado su disponibilidad continua y un rendimiento óptimo, asegurando que la herramienta esté siempre lista para su uso.



Recomendaciones

- **Continuar con las actividades de gestión y mantenimiento**

Se debe continuar con las actividades de gestión y mantenimiento regulares para garantizar el funcionamiento continuo y eficiente de la suite Fortify, asegurando que la herramienta se mantenga operativa y alineada con las necesidades de seguridad del entorno.

- **Priorizar la gestión de copias de seguridad, control de cambios y pruebas**

Es esencial priorizar la gestión de copias de seguridad, el control de cambios y la ejecución de pruebas periódicas para asegurar la integridad y disponibilidad de los datos en la nueva suite Fortify. Estas acciones minimizarán el riesgo de pérdida de datos y garantizarán que cualquier modificación en el sistema se realice de manera adecuada, sin afectar el funcionamiento de la herramienta.

- **Monitoreo constante de la suite Fortify**

Mantener un monitoreo constante de la suite Fortify es esencial para identificar cualquier anomalía o patrón inusual que pueda requerir intervención. Este enfoque proactivo permitirá detectar y resolver posibles problemas de manera anticipada, reduciendo el impacto en la seguridad y el rendimiento del sistema.

- **Revisión y actualización regular de las políticas de seguridad y configuración**

Se recomienda realizar revisiones y actualizaciones periódicas de las políticas de seguridad y la configuración de Fortify para adaptarlas a las necesidades cambiantes del entorno de desarrollo. Esto asegurará que las configuraciones de seguridad estén siempre alineadas con las mejores prácticas y los requisitos normativos vigentes.



26

Archivos nuevos
encontrados por
behavior monitoring

1076

Eventos en equipos
finales

259

positivos

2086

s Device Control

186

en servidores

42

ciones nuevas

0381

entos IPS

17426

Eventos correo

Informe Soluciones Antimalware

2025

Objetivo

Presentar en detalle los eventos de disponibilidad, actividades e incidentes registrados en la operación y administración de MNEMO sobre las plataformas de seguridad de Trend Micro pertenecientes al Fondo Nacional del Ahorro para el periodo de 22 de diciembre al 21 de enero del 2025 .

Las actividades desarrolladas por parte de MNEMO corresponden a la gestión para la administración de las plataformas de Trend Micro.

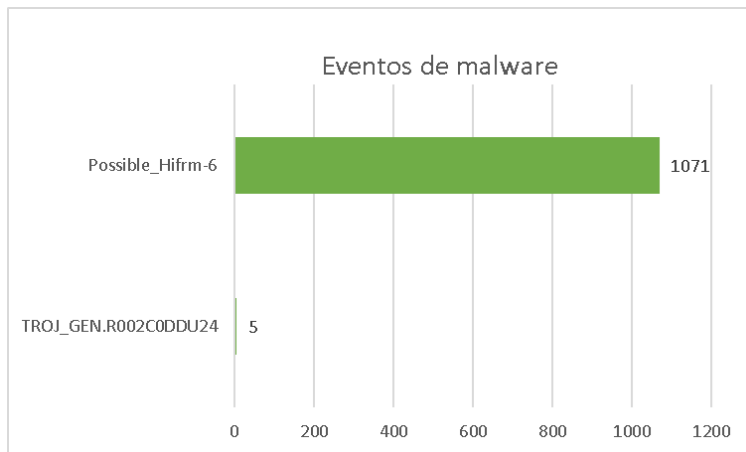
Alcance

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 diciembre hasta el 21 de enero del año 2025.

Estadísticas Generales de detección

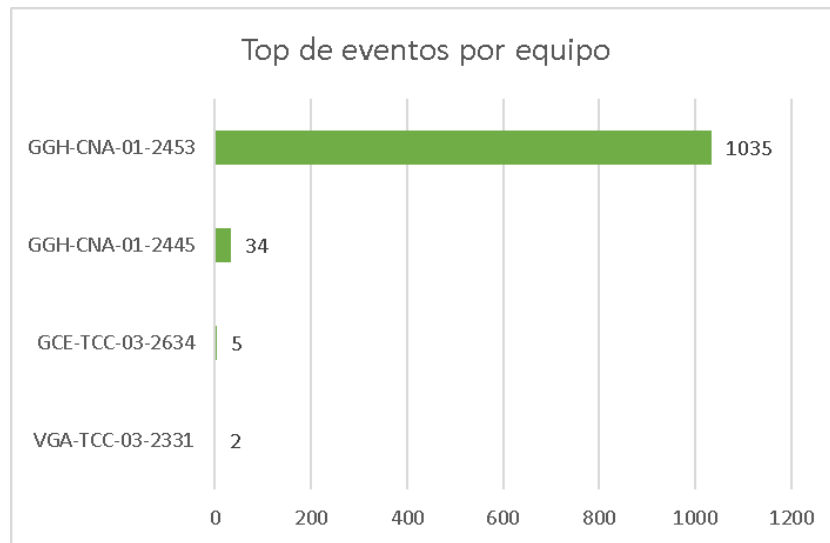
Detecciones en puntos finales Tren micro

Se evidencian un total de **1076 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. Luego se encuentra la detección de Troyanos, relacionados con **keygen** para craqueo de software por parte del usuario **Nvillalba**.



Top de equipos con mayor cantidad de detecciones

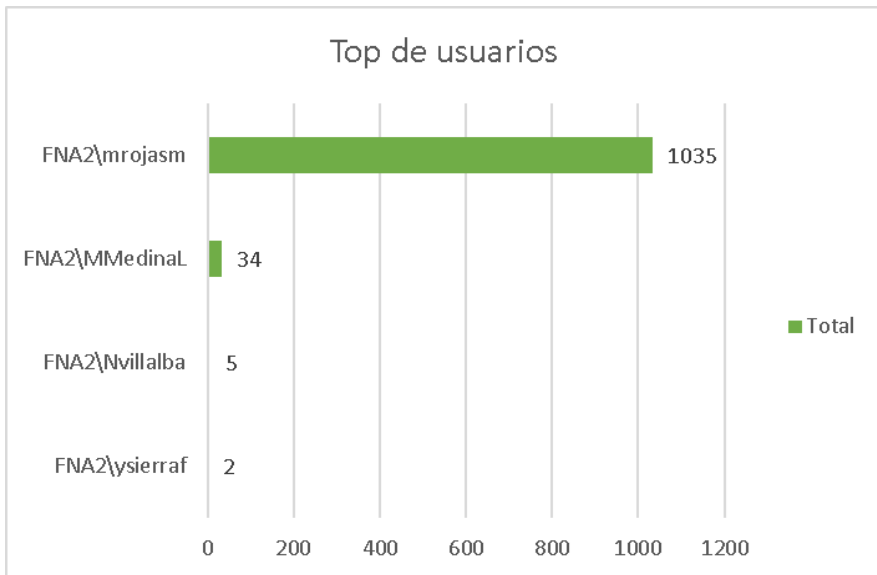
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **GCE-TCC-03-2634** por la detección de archivo tipo troyano.



Estadísticas Generales de detección

Top de usuarios con mas eventos.

En el top de usuarios se encuentra mrojas m por la detección de archivos con objetos embebidos, seguido de MMedinaL por el mismo tipo de detección.



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 **setup.exe** y **WMCapture** estos se detectaron como archivos nuevos.

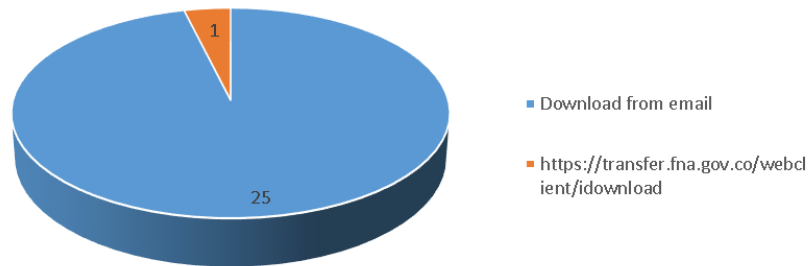
Eventos Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
C:\Users\Lhernandez\Downloads\documents_20241230\SB0PLO4304P_900-70002711\setup.exe	1
C:\Soporte\TransferWMCapture\setup.exe	1
C:\TransferWMCapture\setup.exe	1
C:\wm-capture-v4\setup\workmanager-capture-r2.exe	1
C:\Users\Lhernandez\Downloads\documents_20241230\SB0PLO4304P_900-70002711\setup.engine\SetupEngine.exe	1
C:\Users\Administrador\AppData\Local\Temp\RarSFX0\setup.engine\SetupEngine.exe	1
C:\Soporte\documents_20241224\SB0PLO4304P_900-70002711\setup.engine\SetupEngine.exe	1
C:\Users\ADMINI~1\AppData\Local\Temp\RarSFX0\setup.exe	1
C:\Soporte\documents_20241224\SB0PLO4304P_900-70002711\setup.exe	1
C:\Soporte\documents_20241224\SB0PLO4304P_900-70002711\setup.engine\actionagentproc.exe	2
C:\Users\Lhernandez\Downloads\documents_20241230\SB0PLO4304P_900-70002711\setup.engine\plat64\actionagentproc.exe	2
C:\COBIS\Credito\Tramites\TRAMITES.exe	3
C:\COBIS\Seguridad\segurid.exe	3
C:\Users\Lhernandez\Downloads\documents_20241230\SB0PLO4304P_900-70002711\setup.engine\actionagentproc.exe	3
C:\Users\Administrador\Downloads\documents_20250108\TransferWMCapture\setup.exe	4
Total, general	26

Estadísticas Generales de detección

Origen Behavior Monitoring

En el origen de eventos se puede ver que la mayoría corresponde a archivos descargados de correos y un evento relacionado por transfer.

Origen eventos Behavior Monitoring



Application Control

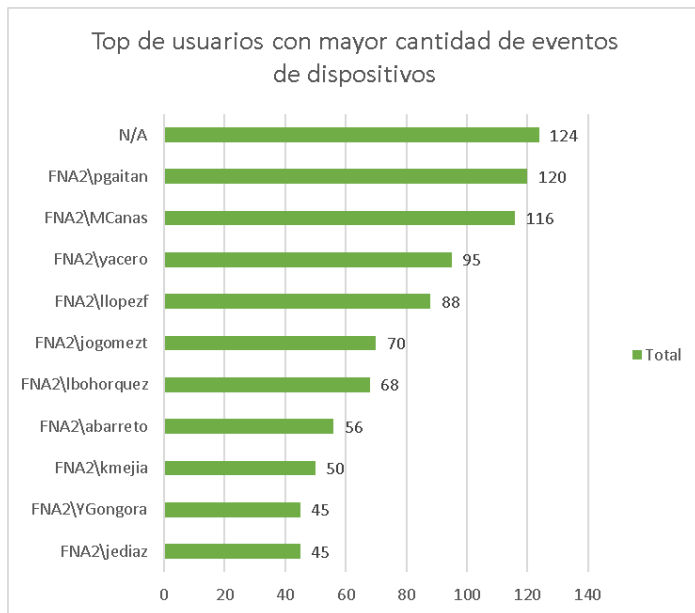
La política de application Control encontró el uso de la aplicación **conda.exe**, listado dentro de aplicaciones bloqueadas por la solución.

Eventos Application Control	
Etiquetas de fila	Cuenta de File
GAS-CNA-01-3694	6
conda.exe	6
GPF-TT-02-2782	1
vcredist_x86.exe	1
GPF-TT-02-2227	1
vcredist_x86.exe	1
Total, general	8

Estadísticas Generales de detección

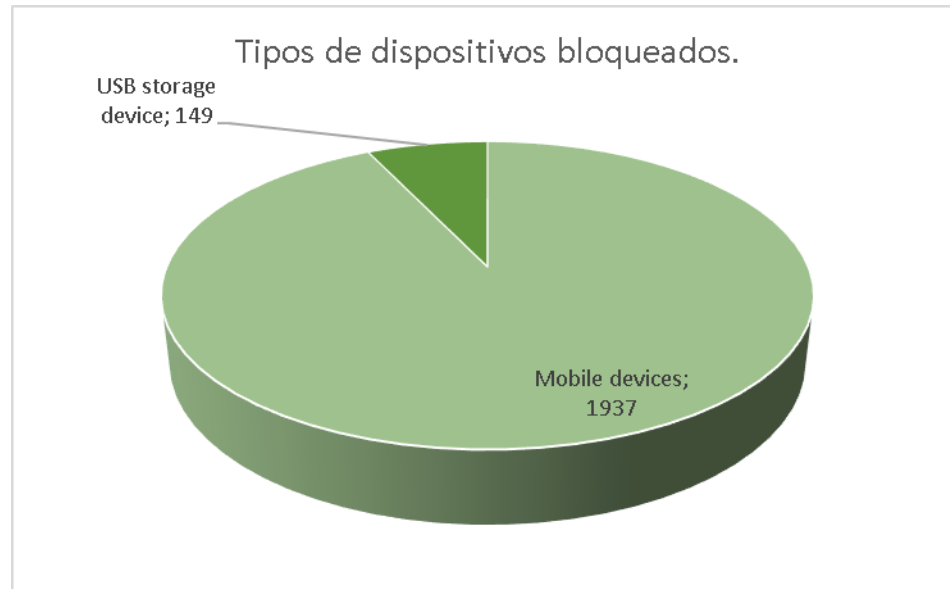
Device Control

El módulo de **device control**, bloquea el uso no autorizado de dispositivos extraíbles, el usuario que mayor cantidad de eventos registra es **pgaitan** con **120 registros**.



Device Control

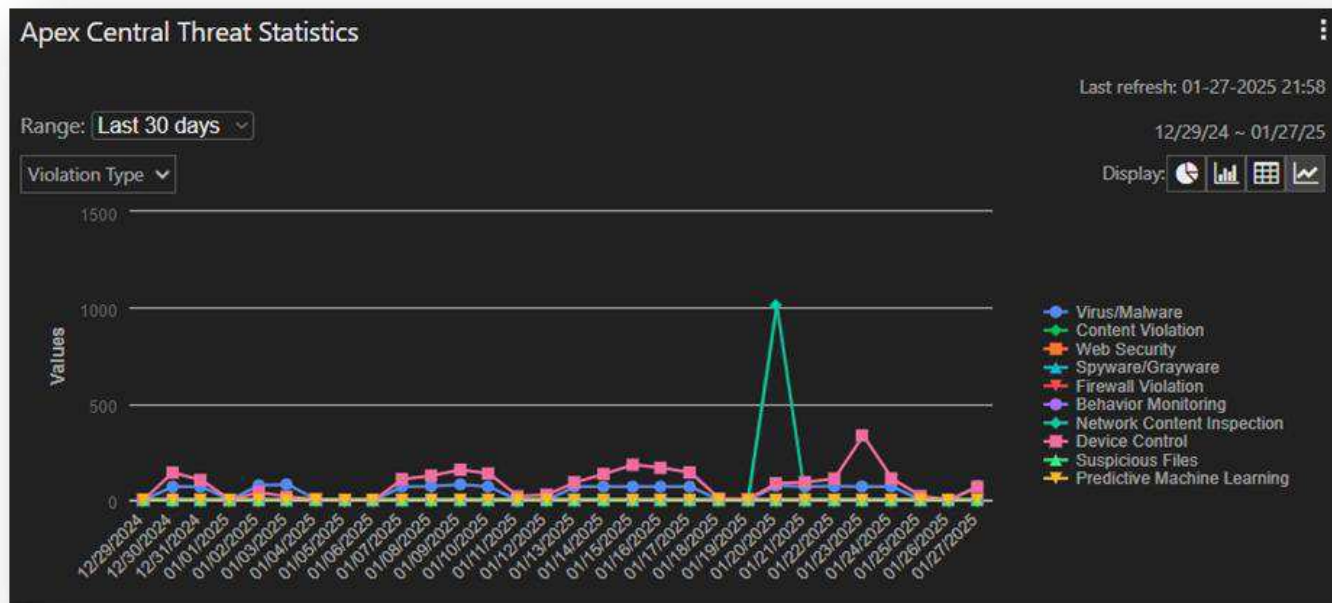
En el tipo de dispositivos que mayor cantidad de eventos registra, son dispositivos móviles.



Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta la cantidad de eventos por cada uno de los módulos de protección para dispositivos finales



Estadísticas Generales de detección

Eventos Workbench

Workbench, genera alertas de acuerdo con diferentes eventos correlacionados y les asigna una clasificación, se registraron 19 alertas ninguna con clasificación alta, dentro de estas se encuentra:

- La ejecución de Deletion of Volume Shadow Copies, se registra como una alerta debido a que puede ser utilizado por ransomware, en este caso es válido por parte de los administradores.

- El evento que mayor cantidad de registros muestra, es la ejecución de comando PowerShell "C:\Windows\system32\windowspowershell\v1.0\powershell.exe" - Command Set-MpPreference -DisableRealtimeMonitoring \$true este no afecta al antivirus de Trend Micro ya que intenta desactivar Windows Defender.

- Possible Account Compromise - Impossible Travel: Hace referencia a conexiones distantes una de otra en un tiempo muy corto por lo que resulta sospechoso, The user (jbalantac@fna.gov.co) has successfully signed in from (CO) (3.7231,-75.4832) and (MX)(16.75838,-93.11016)). The short time difference indicates a possible account compromise.

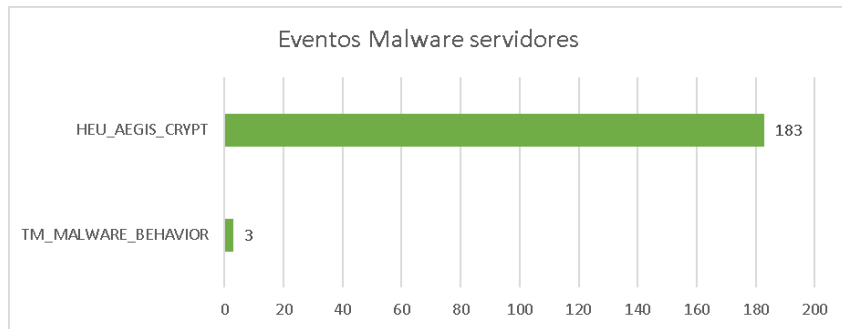
Eventos Workbench

Score	Insight	Workbench Insight				Last Updated	Created
		Impact Scope	Case	Attack Phase			
44	IC-35600-20250113-00000 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
44	IC-35600-20250109-00000 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	8/01/2025 22:25	#####
44	IC-35600-20241231-00000 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	31/12/2024 49:00	#####
44	IC-35600-20241229-00003 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
44	IC-35600-20241229-00002 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	29/12/2024 40:41	#####
44	IC-35600-20241229-00001 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
44	IC-35600-20241229-00000 Alert2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
41	WB-35600-20250127-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
41	WB-35600-20250125-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1		Execution Defensi	ve evasion	#####	####
41	WB-35600-20250121-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
41	WB-35600-20250111-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
41	WB-35600-20250108-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	8/01/2025 18:05	#####
41	WB-35600-20241229-00006 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	29/12/2024 41:09	#####
41	WB-35600-20241229-00005 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	29/12/2024 41:01	#####
41	WB-35600-20241229-00004 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	29/12/2024 41:00	#####
41	WB-35600-20241229-00000 Alert1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1	User	Execution Defensi	ve evasion	#####	####
31	IC-35600-20250120-00000 Alert2 Suspicious Deletion of Volume Shadow Copy (2)	Endpoint - Server: 1 User Account: 1	User	Impact		#####	####
23	WB-35600-20250123-00000 Alert1 Potential Information Gathering	Endpoint - Desktop: 1 User Account: 1		Discovery		23/01/2025 58:30	#####
15	WB-35600-20250101-00000 Alert1 Possible Account Compromise - Impossible Travel	User Account: 1				#####	####

Estadísticas Generales de detección

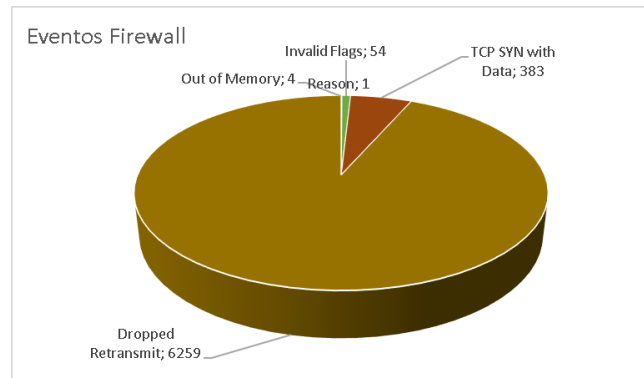
Eventos Servidores

Se registran 4 eventos en el servidor **BOGPVPPWP0B0**, esto por el uso de la aplicación **PdfCompressorService.exe** que utiliza servicios de cifrado por lo que lo registra como riesgoso, esta alerta es solo de observación. Para el dispositivo **FNABOGCLM**, el archivo **MeshAgent.exe** se registra como posiblemente malicioso, porque permite control remoto sobre otros dispositivos.



Eventos Firewall Servidores

El módulo de Firewall de hosts ha sido activado en servidores, esto inicialmente en modo observación. De acuerdo con este módulo se generaron **3820 eventos**, El evento que mayor cantidad de registros género es **Retransmit**: Si el firewall detecta paquetes que no coinciden con una sesión válida establecida, los considera retransmisiones sospechosas. Seguido de **TCP SYN with Data**: El evento de protección IPS "TCP SYN with Data" se refiere a un tipo de ataque conocido como **"SYN Flood"**. En este ataque, un programa envía múltiples paquetes de sincronización TCP (SYN) a un endpoint, lo que provoca que el endpoint envíe continuamente respuestas de reconocimiento de sincronización (SYN/ACK). Esto puede agotar la memoria del endpoint y eventualmente hacer que se bloquee.

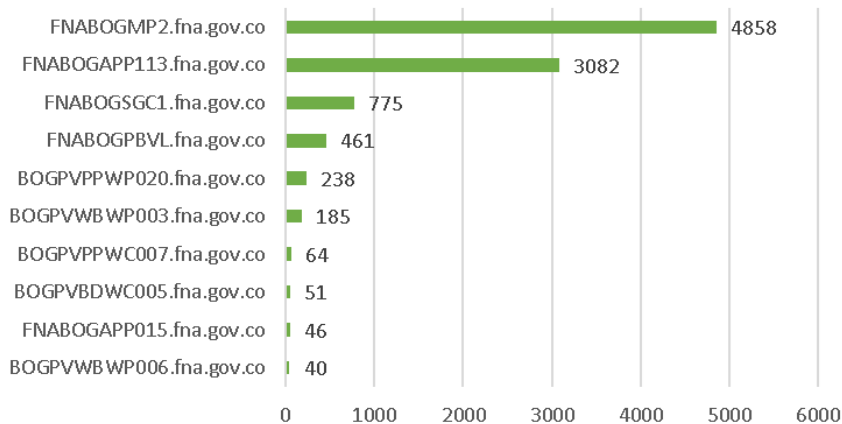


Estadísticas Generales de detección

Top Servidores.

En el top de dispositivos con mayor cantidad de eventos de host, se encuentra **FNABOGMP2**, por eventos de retransmisión, descartados por el módulo de firewall con origen el servidor **FNABOGPBVL**.

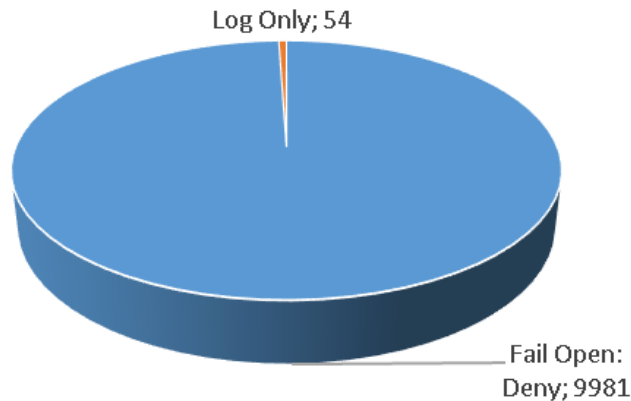
Top de equipos por evento



Eventos Acción Servidores

La mayoría de los eventos **3800** fueron bloqueados o denegados, los otros **20** fueron de auditoría.

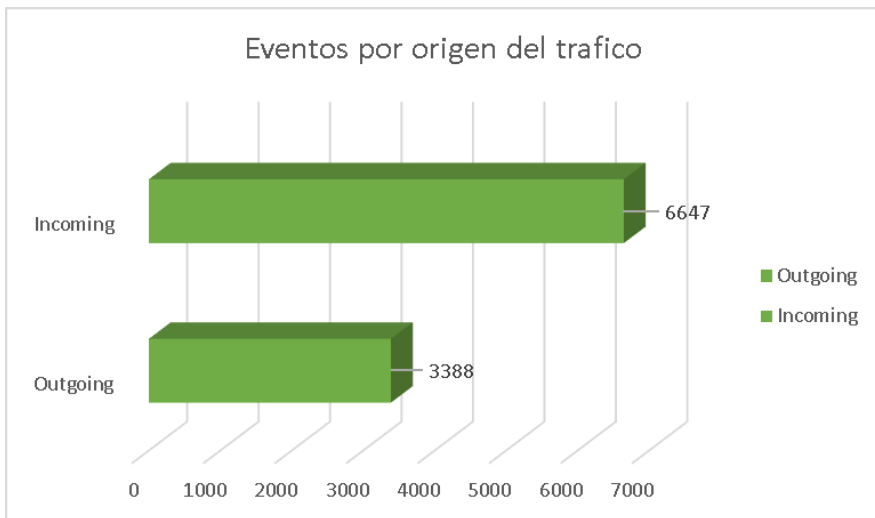
Eventos por acción tomada



Estadísticas Generales de detección

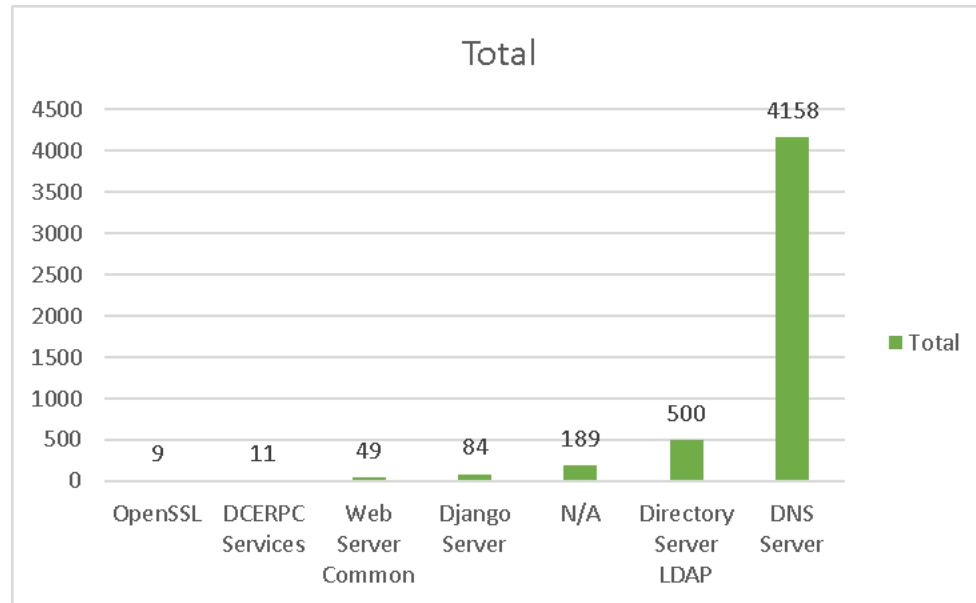
Eventos por origen de datos

La mayoría de los eventos corresponden a tráfico interno entrante.



Eventos por tipo de aplicación.

Los eventos que mayor cantidad de eventos registraron fueron los relacionados con los servicios de DNS y LDAP.



Estadísticas Generales de detección

Eventos IPS Servidores.

El modulo de IPS de host en servidores, se encuentra activo con el fin de identificar trafico con comportamiento malicioso y vulnerabilidades de cara a la red. En el top de eventos se encuentra la regla:

"Invalid Compression Denial of Service" en servidores DNS hace referencia a un mecanismo de detección diseñado para proteger contra ataques que explotan la funcionalidad de compresión en las respuestas DNS. Este tipo de ataque puede interrumpir o degradar el servicio DNS, afectando la disponibilidad de la red. Identificada en el servidor **BOGPVDCWP002** como origen y como destino el servidor **DNS 172.16.0.71**.

Otros eventos que mayor cantidad de registros tuvieron en varios servidores son:

- **Evento 1011843 (Django):** Un atacante puede sobrecargar servidores Django enviando solicitudes maliciosas. Actualiza Django y utiliza WAF para mitigarlo.
- **Evento 1008555 (Active Directory):** Un atacante puede interrumpir funciones críticas de red explotando solicitudes LDAP maliciosas. Actualiza Windows y configura adecuadamente el servicio LDAP.

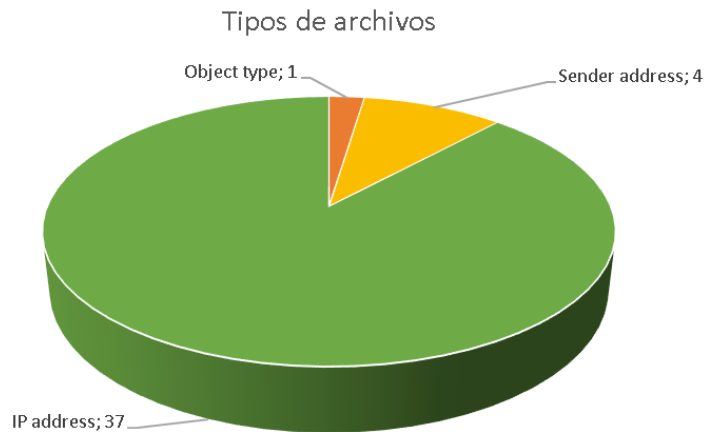
Eventos por tipo de aplicación.

Top de eventos IPS	
NombreHost, Evento	#
BOGPVPPWP048.fna.gov.co	36
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	23
Invalid Traversal	12
1000826 - OpenSSL SSL_get_shared_ciphers Function Buffer Overflow	1
BOGPVPPWP04A.fna.gov.co	37
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	21
Invalid Traversal	15
1000826 - OpenSSL SSL_get_shared_ciphers Function Buffer Overflow	1
BOGPVDCWP003.fna.gov.co	113
1008555 - Microsoft Windows Active Directory Denial of Service Vulnerability (CVE-2008-1445)	113
BOGPVDCWP001.fna.gov.co	2202
1004747 - DNS Invalid Compression Denial of Service	2053
1008555 - Microsoft Windows Active Directory Denial of Service Vulnerability (CVE-2008-1445)	149
BOGPVDCWP002.fna.gov.co	2334
1004747 - DNS Invalid Compression Denial of Service	2099
1008555 - Microsoft Windows Active Directory Denial of Service Vulnerability (CVE-2008-1445)	235

Estadísticas Generales de detección

Threat Intelligent

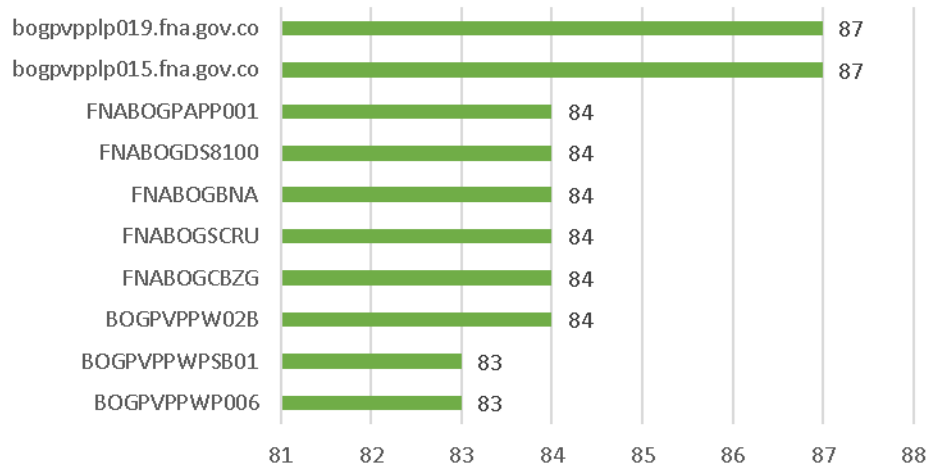
Durante el periodo de **22 de diciembre del 2024 al 21 de enero del 2025** se **adicionan 42 reputaciones nuevas** adicionadas por la integración con Threat Q, correspondientes a correos electrónicos y direcciones IP.



Attack Surface Discovery Devices

En el top de eventos, se registra los **servidores bogvpplp019 y bogvpplp015, con 87 vulnerabilidades** y fallos en la configuración, con clasificación alta. El número en la gráfica indica la clasificación, entre más cerca al 100 más alta es.

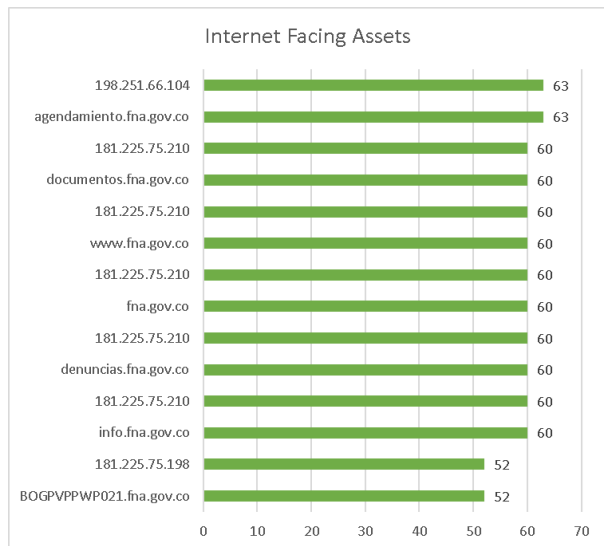
Top de dispositivos con vulnerabilidades



Estadísticas Generales de detección

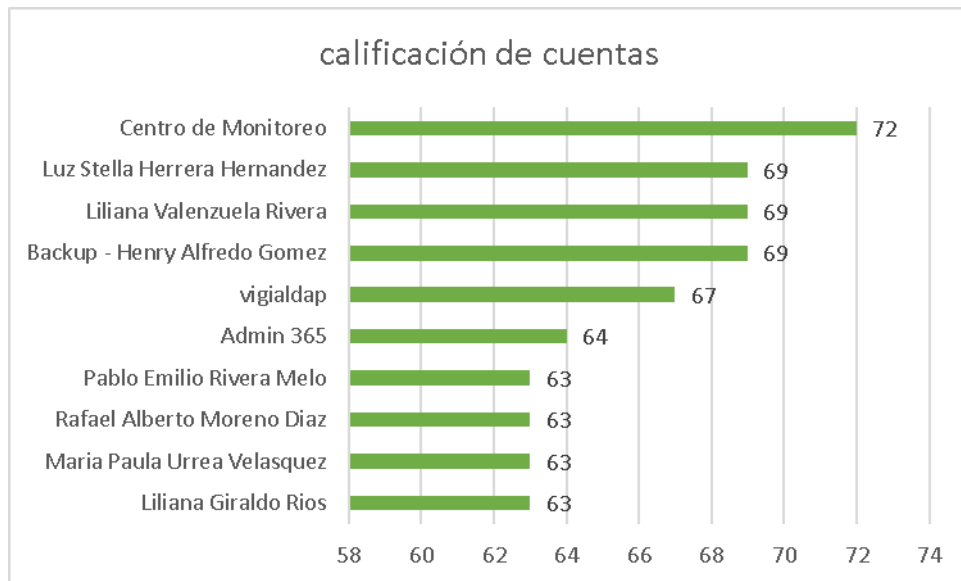
Attack Surface Discovery Internet Facing Assets

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 e Ips y su clasificación, que en este caso no se observa ninguna clasificación alta, la página con clasificación más alta es **agendamiento.fna.gov.co**.



Attack Surface Discovery Cuentas

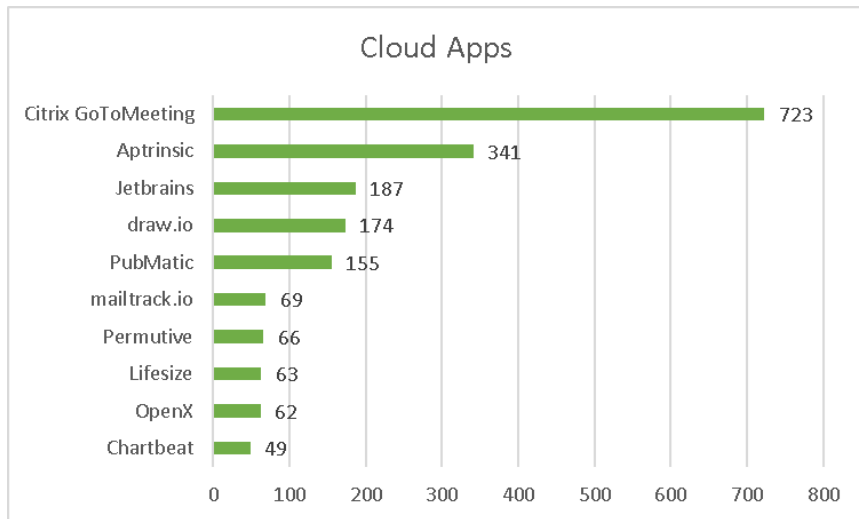
A continuación, se muestra el top de cuentas identificadas por Trend Micro



Estadísticas Generales de detección

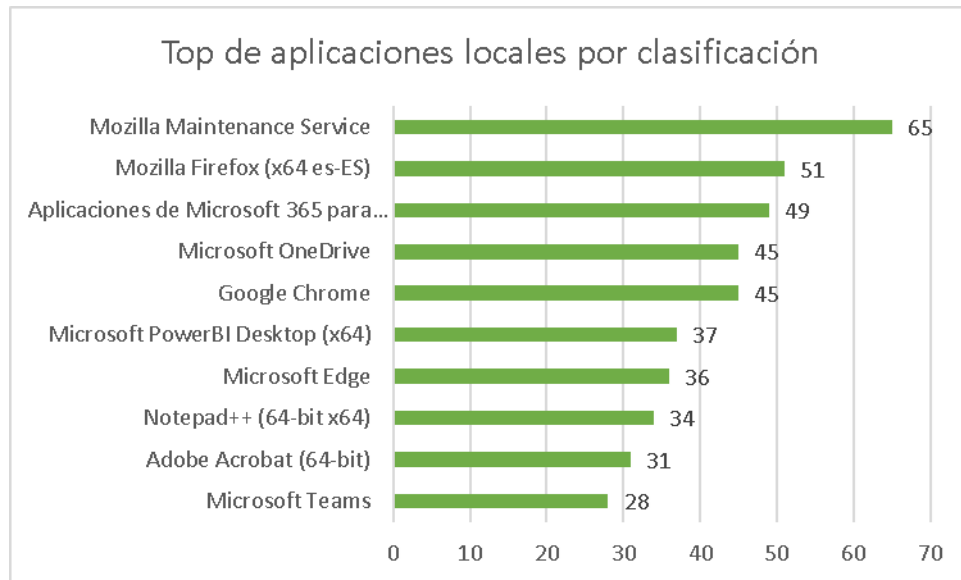
Attack Surface Discovery Cloud Apps

A continuación se muestra la lista del top de Cloud por cantidad de visitas realizadas y clasificación media.



Attack Surface Discovery Local Apps

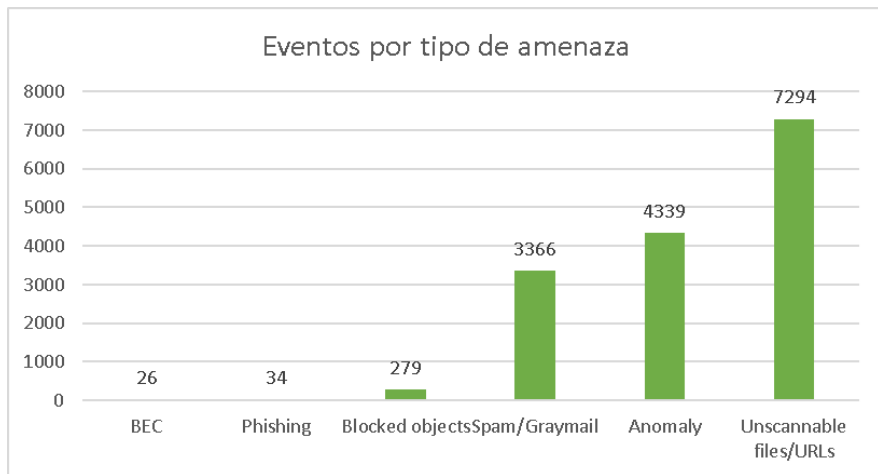
A continuación, se muestra el top de aplicaciones locales por calificación de riesgo, **Mozilla y Office 365** se encuentran en el top de acuerdo con vulnerabilidades encontradas en versiones específicas.



Estadísticas Generales de detección

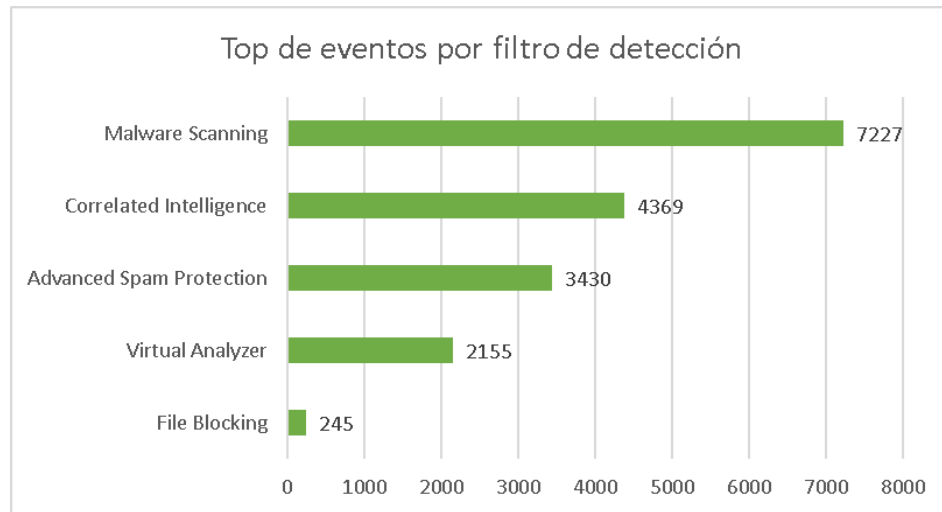
CASB Top de eventos por regla.

Para el periodo de 22 de diciembre del 2024 al 21 de enero del 2025 se presentaron un total de **17426 eventos** registrados por la solución de protección de correo, el módulo que tiene mayor cantidad de eventos es las políticas de protección de **fuga de información**, seguido de archivos no escaneables por su tamaño o nivel de cifrado y por último eventos de anomalías.



CASB Eventos por filtros de seguridad

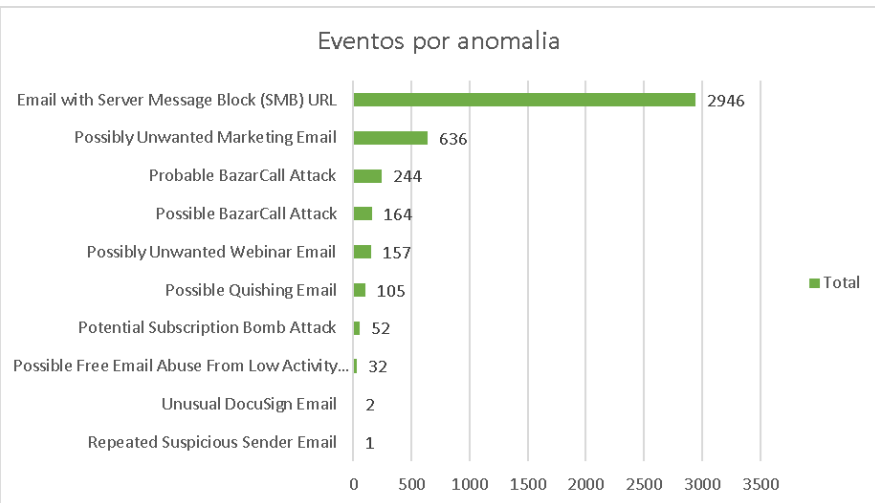
Dentro de los eventos la mayoría corresponden eventos de Data Loss Prevention, seguido de eventos de malware.



Estadísticas Generales de detección

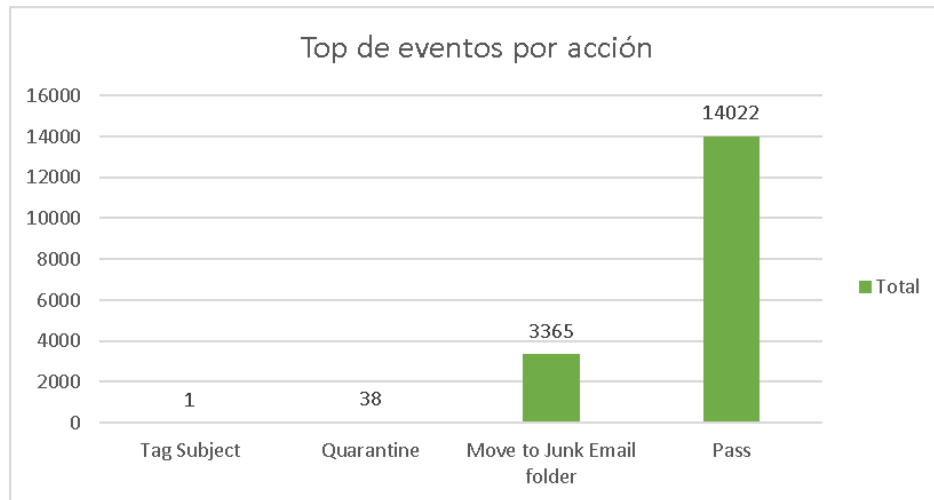
CASB Top de eventos por nombre de anomalía.

En los eventos por nombre de anomalía, se encuentran correos con rutas compartidas, correos de marketing y correos relacionados con el **malware Bazar**.



CASB Top de eventos por Acción.

En el top de acciones, se encuentra Pass esto debido a las reglas de anomalías que se encuentra en modo observación y de los archivos no escaneables por su tamaño y nivel de compresión. luego está la acción de mover a carpeta de no deseados, que en su mayoría son correos de spam.



Estadísticas Generales de detección

CASB Top de cuentas como origen de SPAM

La cuenta que mayor cantidad de detecciones presenta es **mailer-daemon@googlemail.com** y **alertasnotificaciones@notificacionesbancolombia.com**.

Top de remitentes clasificados como SPAM	
Sender	#Eventos
"Locatel colombia"<newsletter@locatelnews.com>	35
"sumicorp ltda"<mercadeo@sumicorp.com>	81
"okomos"<postmaster@okomos.tech>	82
"ins instituto nacional de seguros"<infoins@fasecolda.com>	86
"noticieroficial"<boletin@noticieroficial.com>	87
"zavadora @<socialmedia@zavadora.com>	88
"certiprof"<exams@certiprof-exams.com>	100
"dr. imanol belauteguigoitia - family business pro -	
"<actualizacion.profesional@corporativoindustrialmexico.com>	121
"alertas y notificaciones"<alertasnotificaciones@notificacionesbancolombia.com>	196
"Mail delivery subsystem"<mailer-daemon@googlemail.com>	538

CASB Top de cuentas como origen de Phishing.

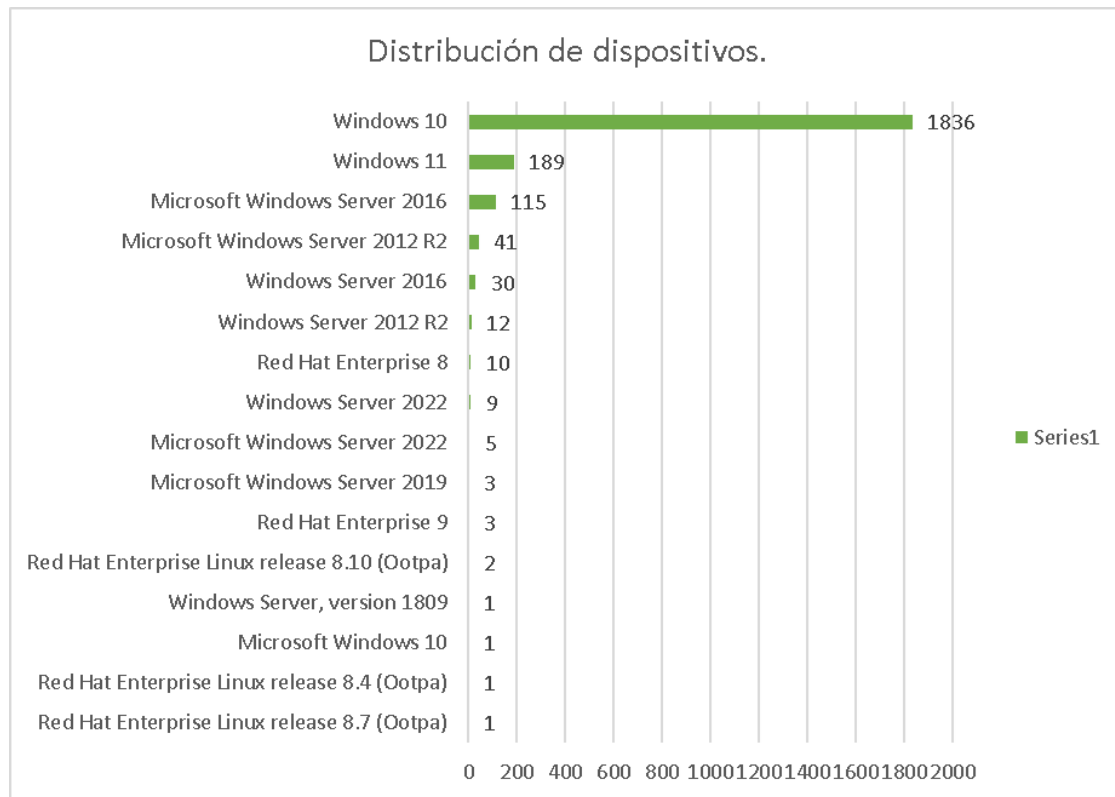
En el top de correos clasificados como phishing, no se visualiza correos repetitivos ya que se registran varios correos con cantidad de eventos similares.

Correos clasificados como Phishing	
Etiquetas de fila	Cuenta de Sender
"cristian cifuentez ordoñez"<chryznkyoj10066@hotmail.com>	1
"monica angarita"<monicangarita-12@hotmail.com>	1
"angelica maria ordoñez perdomo"<mariaangelica1002@hotmail.com>	1
"alvaro fuentes maussa"<alfuemaui@hotmail.com>	1
"karol pinilla ramirez"<karol7698@hotmail.com>	2
"luz guerrero rodriguez"<lumague2@hotmail.com>	2
"leonardo pineda segura"<leonarpi17@hotmail.com>	2
"marquez henao luisa fernanda"<luisa.marquez-h@uniminuto.edu.co>	2
"luis roberto bolaños"<nal0507@hotmail.com>	2
"sandra araujo"<jupelu248@hotmail.com>	2
"omar candela gantiva"<factorypartes@hotmail.com>	2
"carol andrea riaga gómez"<rolacarola@hotmail.com>	2

Estadísticas Generales de detección

Licenciamiento

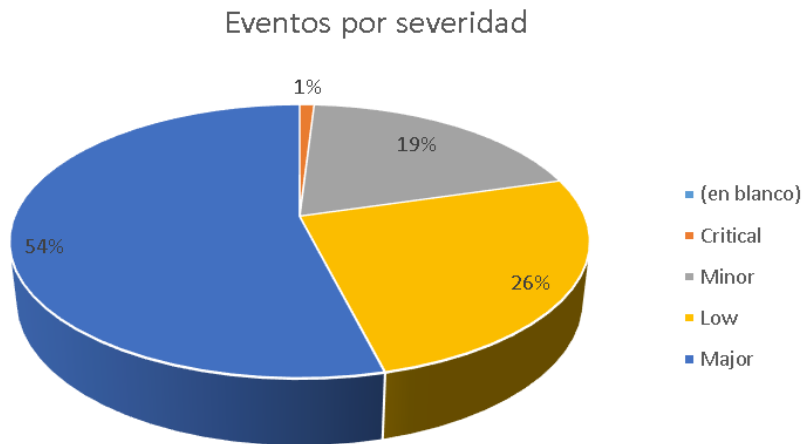
A continuación, se relaciona el informe de **2259 dispositivos** instalados en el periodo que comprende el periodo de 22 de diciembre del 2024 al 21 de enero del 2025.



Estadísticas Generales de detección

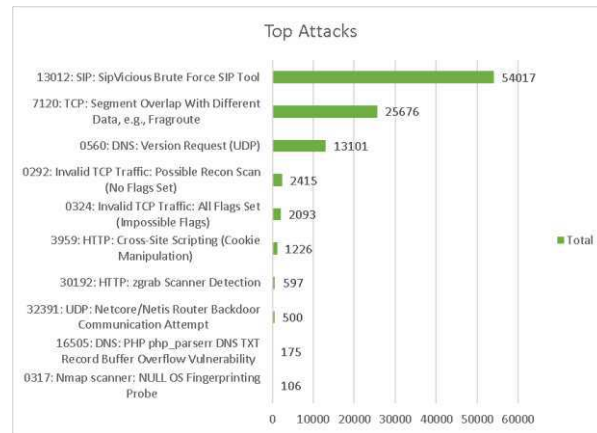
Top de ataques detectados IPS

Durante el periodo analizado del periodo **de 22 de diciembre del 2024 al 21 de enero del 2025**, se encuentra el siguiente TOP de Eventos identificados por el IPS. Del total de los **100381 eventos**, en su mayoría con clasificación mayor con el **54 % de los eventos**.



TOP DE ATAQUES IPS

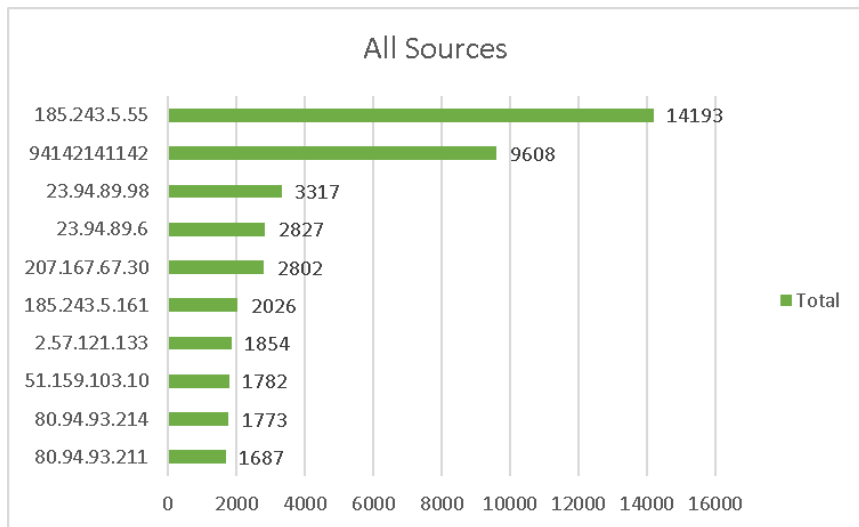
En el top de ataques se encuentra la regla **13012: SIP: SipVicious Brute Force SIP Tool**, por el uso de herramientas SIPVICIOUS para realizar intentos de ataque por fuerza bruta, este evento registra 80482 eventos del total. En segundo lugar se encuentra la regla **7120: TCP: Segment Overlap With Different Data, e.g., Fragroute**. Este tipo de alerta se genera cuando se detecta un intento de evasión de seguridad usando una técnica en la que diferentes segmentos TCP que forman parte de una misma transmisión contienen datos que se solapan entre sí, pero con contenido distinto. Esto puede ser utilizado para evitar la detección por parte de los sistemas de seguridad.



Estadísticas Generales de detección

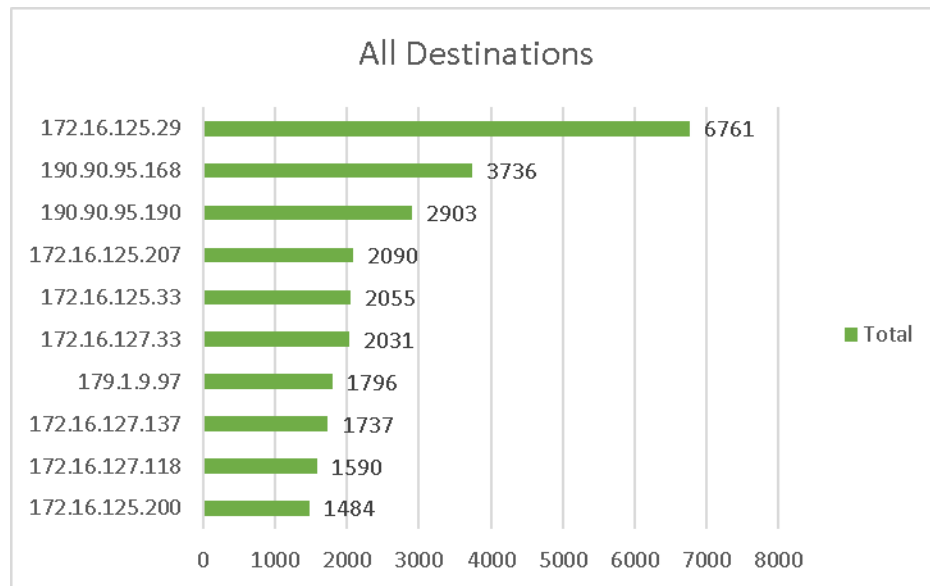
Top de origen.

A continuación, se muestra el top de IP de origen **185.243.5.55** de Polonia con **14193** eventos.



Top Destinos.

En el top de destino se encuentra la dirección IP **172.16.125.29**, con **6761** registros.



Estadísticas Generales de detección

Top de países

En el top de eventos por país, se encuentra Estados Unidos con mayor cantidad de registros, seguido de **Hong Kong y Romania**.

Top Attacks by country

Suma de Hit Count
94014
1358

Con tecnología de Bing

Top de países

Top Attacks by country

Etiquetas de fila	Suma de Hit Count
Germany	1358
Taiwan	1588
The Netherlands	1772
France	2402
Colombia	4206
Romania	8316
Russia	9785
Hong Kong	18314
Unknown	21476
United States	24797
Total, general	94014

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.

- Creación cambio C66791 permisos ZTNA, con el fin de continuar con las tareas de prueba para la implementación de la solución de proxy cloud.
- Caso escalado con fabricante para la integración de la solución de workmanager aplicación de terceros, con el sandbox DDAN, se encuentra en pruebas debido a errores al enviar las muestras.
- Se realiza sesión con Media commerce, redes LAN y administradores de servicios de red, debido a que se está realizando migración de administrador de ancho de banda, el cual está conectado como destino del primer par de inspección del IPS, se concertó arquitectura para la migración pendiente de pruebas por parte de redes y nosotros para validación del tráfico.
- Es necesario realizar la validación de la regla HIFRM6 ya que genera bastantes eventos sobre archivos pdf, registrados como archivos con objetos embebidos específicamente para el usuario MMedinal y mrojasm.
- Se detectaron 26 aplicaciones nuevas por Behavior Monitoring, estas alimentan la base de datos de application control, se sugiere validar aplicaciones nuevas para ser ingresadas dentro de App Control.
- En la cantidad de dispositivos no autorizados conectados. Se encuentra dispositivos móviles 1937 eventos y 149 dispositivos USB.
- Actualmente se encuentran 18 usuarios con permisos para el uso de dispositivos.
- Workbench genero las siguientes alertas:
 - La ejecución de Deletion of Volume Shadow Copies, se registra como una alerta debido a que puede ser utilizado por ransomware, en este caso es válido por parte de los administradores.
 - El evento que mayor cantidad de registros muestra, es la ejecución de comando PowerShell "C:\Windows\system32\windowspowershell\v1.0\powershell.exe" -Command Set-MpPreference -DisableRealtimeMonitoring \$true este no afecta al antivirus de Trend Micro ya que intenta desactivar Windows Defender.
 - Possible Account Compromise - Impossible Travel: Hace referencia a conexiones distantes una de otra en un tiempo muy corto por lo que resulta sospechoso, The user (jbalantac@fna.gov.co) has successfully signed in from (CO) (3.7231,-75.4832) and (MX)(16.75838,-93.11016)). The short time difference indicates a possible account compromise.



- Es necesario realizar validación con SOC, para creación de casos de uso que alerte automáticamente los eventos generados por WorkBench ya que solamente se están generando alertas por el evento de posibles intentos de desactivación de antivirus.
- Se registran 4 eventos en servidores, relacionados con los servidores FNABOGCLM y BOGPVPPWPOB0, por la ejecución de las aplicaciones PdfCompressorService.exe y MeshAgent.exe respectivamente. Para la solución de servidores, se encuentran módulos adicionales, como app control, activity monitoring y log inspection que puede ser habilitada.
- La solución de IPS para servidores, registro 3820 eventos, El evento que mayor cantidad de registros género es Retransmit. Se continuará con la validación de las reglas para activar o desactivarlas en caso de ser necesarias.
- En el top de dispositivos con mayor cantidad de eventos de host, se encuentra FNABOGMP2, por eventos de retransmisión, descartados por el módulo de firewall con origen el servidor FNABOGPBVL.
- para los módulos de IPS y Firewall para servidores, los eventos que mayor cantidad de eventos registraron fueron los relacionados con los servicios de DNS y LDAP.
- Para IPS en servidores las siguientes reglas estuvieron en el top de eventos: Evento 1011843 (Django): Un atacante puede sobrecargar servidores Django enviando solicitudes maliciosas. Actualiza Django y utiliza WAF para mitigarlo.
- Evento 1008555 (Active Directory): Un atacante puede interrumpir funciones críticas de red explotando solicitudes LDAP maliciosas. Actualiza Windows y configura adecuadamente el servicio LDAP.
- La solución de Inteligencia de amenazas registra 42 reputaciones nuevas.
- Attack Surface Discovery se registra los servidores bogvpplp019 y bogvpplp015, con 87 vulnerabilidades y fallos en la configuración, con clasificación alta.
- Attack Surface Discovery la página con clasificación más alta es agendamiento.fna.gov.co con una clasificación media
- Attack Surface Discovery, la cuenta con mayor riesgo identificada es Centro de Monitoreo, esto debido a que se encuentra identificada dentro de una base de datos como expuesta.
- Para las aplicaciones Cloud y local identificadas por Attack Surface Discovery, se recomienda realizar la validación si es necesario incluir alguna dentro de las aplicaciones bloqueadas.
- IPS, registro 100381 eventos en su mayoría con clasificación Major con el 54% de los eventos totales.
- IPS en el top de ataques se encuentra la regla 7120: TCP: Segment Overlap With Different Data, e.g., Fragroute. y 13012: SIP: SipVicious Brute Force SIP Tool.



- IPS En el top de IP de origen 185.243.5.55 de Polonia con 14193 eventos.
- IPS En el top de destino se encuentra la dirección IP 172.16.125.29, con 6761 registros.
- En el top de eventos por país, se encuentra Estados Unidos con mayor cantidad de registros, seguido de Hong Kong y Rumania. Se recomienda validar la opción de crear reglas de protección por geolocalización.
- se presentaron un total de 17426 eventos registrados por la solución CASB
- Protección correo En los eventos por nombre de anomalía, se encuentran correos con rutas compartidas, correos de marketing y correos relacionados con el malware Bazar.
- Protección correo, en el top de acciones, se encuentra Pass esto debido a las reglas de anomalías que se encuentra en modo observación y de los archivos no escaneables, por su tamaño y nivel de compresión. Luego está la acción de mover a carpeta de no deseados, que en su mayoría son correos de spam.
- Protección correo, la cuenta que mayor cantidad de detecciones presenta es mailer-daemon@googlemail.com y alertasynotificaciones@notificacionesbancolombia.com.
- se relaciona el informe de 2259 dispositivos instalados en el periodo que comprende el periodo de 22 de diciembre del 2024 al 21 de enero del 2025. Se está realizando tareas para la instalación en equipos faltantes, encontrados durante auditoría 85 en total.
- Para la solución de ISE se encuentra varios dispositivos dentro de la consola de antivirus que se registran con error en su instalación por lo que se escala con soporte en sitio para su reinstalación.
- Se trabaja en documento para seguimiento del estado de los equipos y validación de su despliegue y actualización.
- Durante el periodo se gestionaron 17 peticiones en service manager.
- Se realiza proceso de eliminación de dispositivos dados de baja de la entidad.
- Se realiza creación de planes de mejora para el 2025, que incluye tareas para mejora de las políticas y soluciones de Trend Micro.
- se encuentra en validación las reglas de protección BEC para correo, en las cuales se realizó pruebas con los correos de estrategia y aseguramiento TI y Seguridad de la información.



Informe de Consultoría

2025

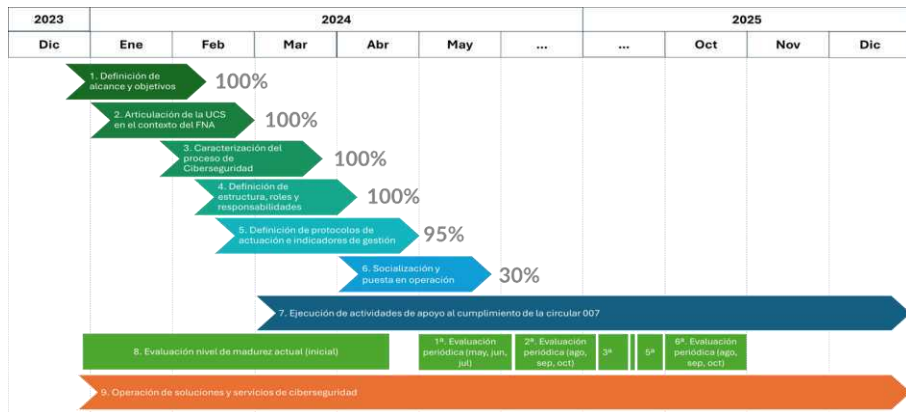
Objetivo

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.

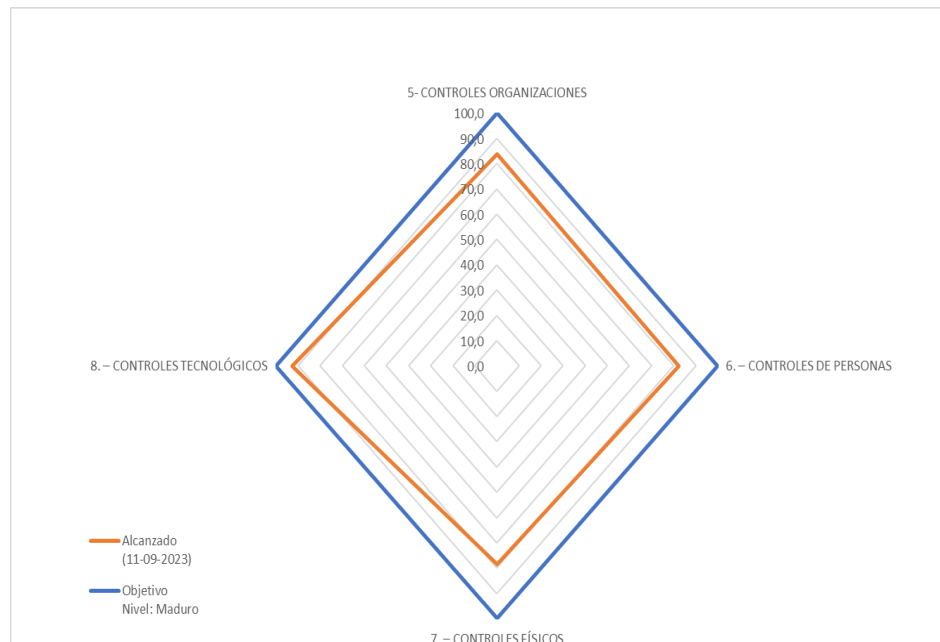
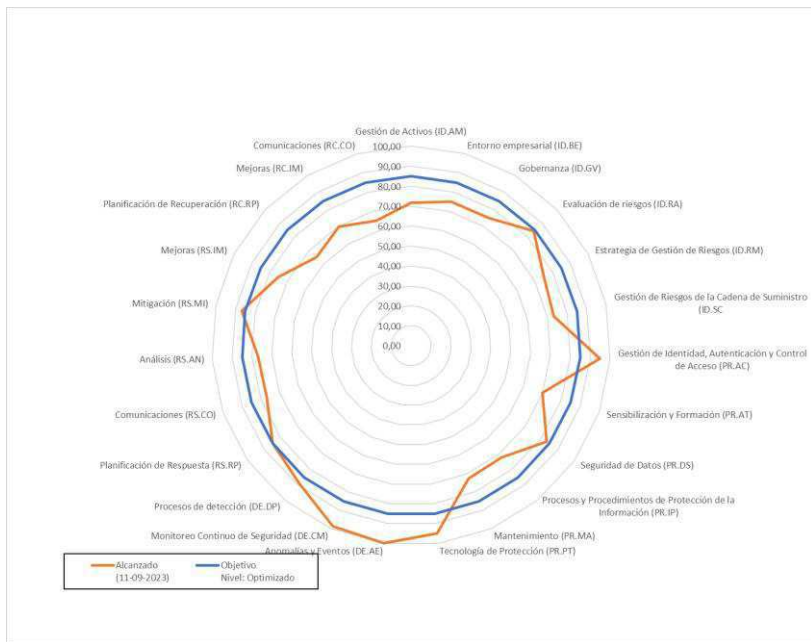
Plan de construcción de protocolos de actuación

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



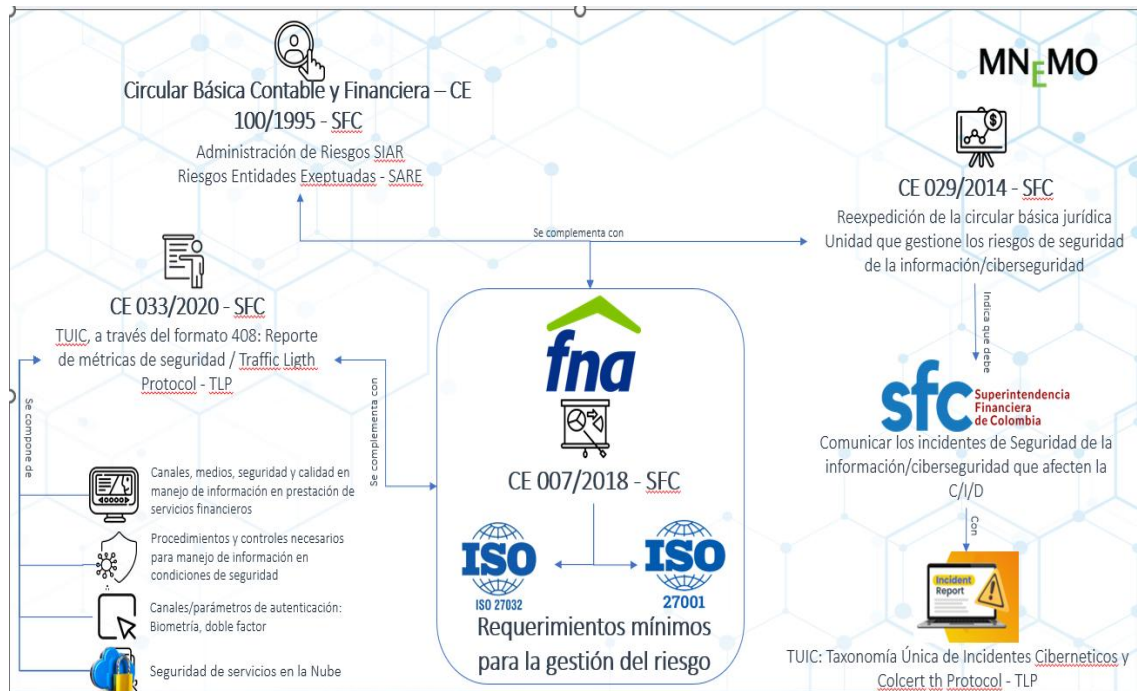
Construcción del modelo de análisis de nivel de madurez con base en marcos de referencia reconocidos como NIST, COBIT e ISO 27001.

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-2-29

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2025-03-20

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

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

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
1	Administración y soporte de la plataforma XDR	1.00	3,326,000.00	3,957,940.00	0.00
2	Administración y soporte de la plataforma THREAT INTELLIGENCE (TIP)	1.00	27,797,000.00	33,078,430.00	0.00
3	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	1.00	55,994,000.00	66,632,860.00	0.00
4	Administración y soporte Servicio de MONITOREO DE DNS servidor infoblox 1405 series, Serial No: 1405202201700334	1.00	52,083,000.00	61,978,770.00	0.00
5	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSEEMNET	1.00	8,279,000.00	9,852,010.00	0.00
6	Administración y soporte de la plataforma CIBERDEFENSA	1.00	5,874,000.00	6,990,060.00	0.00
7	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	1.00	8,406,000.00	10,003,140.00	0.00
8	Administración y soporte de la plataforma SOAR	1.00	14,627,000.00	17,406,130.00	0.00
9	Análisis de vulnerabilidades (dos(2) obligatorios al año, al total de activos de la plataforma tecnológica)	1.00	129,536,000.00	154,147,840.00	0.00
10	Administración y soporte de la plataforma MONITOREO DE LA BASE DE DATOS (DAM)	1.00	23,451,000.00	27,906,690.00	0.00
11	Administración y soporte de la plataforma SOLUCION GOBIERNO DE INDETIDADES (IAM)	1.00	26,449,000.00	31,474,310.00	0.00

Total Bruto 355,822,000.00
Subtotal 355,822,000.00
IVA 19% 67,606,180.00
Total a Pagar 423,428,180.00

SUMA EN LETRAS: Cuatrocientos veintitrés millones cuatrocientos veintiocho mil ciento ochenta 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

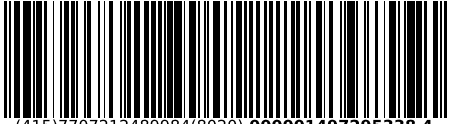
Que nuestro(a) cliente **CONSORCIO UNIDAD DECIBERSEGURIDAD FNA**, identificado(a) con NIT número **901.781.625-1** se encuentra vinculado(a) a nuestra entidad a través de la CUENTA **CUENTA DE AHORROS EM No. 0136002901** apertura el **19 de diciembre del 2023**, cuenta **ACTIVA** y que a la fecha ha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

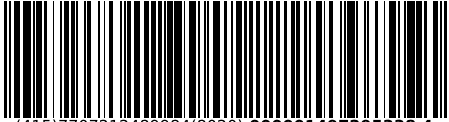
Esta certificación se expide a solicitud del titular con destino a quien interese, el **20 de marzo del 2025**.

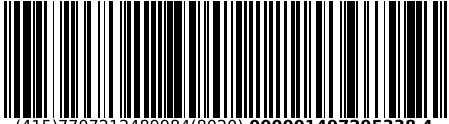
Para trámites de nómina, legales, internacionales y otros, también puedes usar las siguientes opciones de números de cuenta:

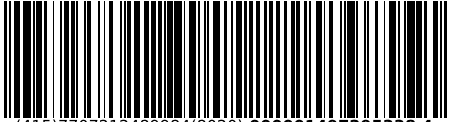
Cuenta de 10 dígitos:**0136002901**
Cuenta de 16 dígitos:**0136000200002901**
Cuenta de 20 dígitos:**00130136000200002901**

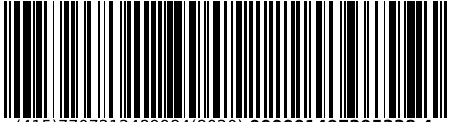
Firma autorizada
BBVA Colombia

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5		1		Impuestos de Bogotá		3 2	
IDENTIFICACIÓN							
24. Tipo de contribuyente		25. Tipo de documento		26. Número de Identificación			
Persona jurídica		1					
Lugar de expedición		28. País		29. Departamento		30. Ciudad/Municipio	
31. Primer apellido		32. Segundo apellido		33. Primer nombre		34. Otros nombres	
35. Razón social CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País		39. Departamento		40. Ciudad/Municipio			
COLOMBIA		Bogotá D.C.		Bogotá, D.C.		0 0 1	
41. Dirección principal		CL 99 # 10 - 19 OF 502 ED TRADE CENTER					
42. Correo electrónico		r.rojasarias@mnemo.com					
43. Código postal		44. Teléfono 1		45. Teléfono 2			
0 1 1 0 0 1		3 1 8 3 8 3 5 1 1 7		3 0 1 6 3 2 7 9 8 6			
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código		47. Fecha inicio actividad		48. Código		49. Fecha inicio actividad	
50. Código		1		2		51. Código	
6 2 0 1		2 0 2 3 1 2 1 4					
Responsabilidades, Calidades y Atributos							
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26							
53. Código 7 1 4 4 8 5 5							
07- Retención en la fuente a título de rent							
14- Informante de exogena							
48 - Impuesto sobre las ventas - IVA							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
1 2 3 4 5 6 7 8 9 10				55. Forma 56. Tipo Servicio 1 2 3			
54. Código				57. Modo			
11 12 13 14 15 16 17 18 19 20				58. CPC			
IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación							
Para uso exclusivo de la DIAN							
59. Anexos SI NO X				60. No. de Folios: 0			
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:				Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre VELEZ CASTRO HUMBERTO DE JESUS 985. Cargo Representante legal Certificado			

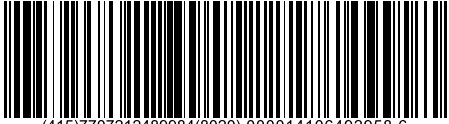
DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 5 Hoja 2		
			4. Número de formulario 14972953384		
 (415)7707212489984(8020) 000001497295338 4					
5. Número de Identificación Tributaria (NIT) 9 0 1 7 8 1 6 2 5 1		6. DV 1		12. Dirección seccional Impuestos de Bogotá	
				14. Buzón electrónico 3 2	
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica 3		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma			Composición del Capital		
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					
Vigencia					
80. Desde 2 0 2 3, 1 2, 1 3					
81. Hasta 2 0 2 5, 1 2, 3 1					
				82. Nacional 1 0 0 %	
				83. Nacional público 0 . 0 %	
				84. Nacional privado 1 0 0 . 0 %	
				85. Extranjero 0 %	
				86. Extranjero público 0 . 0 %	
				87. Extranjero privado 0 . 0 %	
Entidad de vigilancia y control					
88. Entidad de vigilancia y control					
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	
				96. DV.	
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

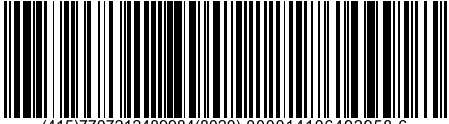
DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 5 Hoja 3			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5 1		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			

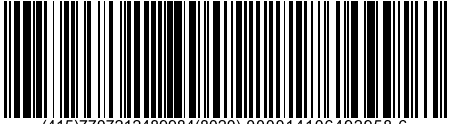
DIAN		Formulario del Registro Único Tributario Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales				001	
Espacio reservado para la DIAN				Página 4 de 5 Hoja 4			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 7 8 1 6 2 5 1		1		Impuestos de Bogotá		3 2	
Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales							
111. Tipo de documento NIT 3 1		112. Número de identificación 9 0 1 4 4 7 9 6 8		113. DV 114. Nacionalidad 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 5 0 2 0 2 3 1 1 2 3		123. Fecha de retiro	
111. Tipo de documento NIT 3 1		112. Número de identificación 9 0 0 3 9 6 1 7 6		113. DV 114. Nacionalidad 1 COLOMBIA		1 6 9	
115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres	
2119. Razón social MNEMO COLOMBIA SAS							
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso 4 9 2 0 2 3 1 1 2 3		123. Fecha de retiro	
111. Tipo de documento NIT 3 1		112. Número de identificación 9 0 1 3 0 6 6 8 7		113. DV 114. Nacionalidad 2 COLOMBIA		1 6 9	
115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres	
3119. Razón social MNEMO EVOLUTION & INTEGRATION SERVICES S.A.							
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso 1 2 0 2 3 1 1 2 3		123. Fecha de retiro	
111. Tipo de documento		112. Número de identificación		113. DV 114. Nacionalidad			
115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres	
4119. Razón social							
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	
111. Tipo de documento		112. Número de identificación		113. DV 114. Nacionalidad			
115. Primer apellido		116. Segundo apellido		117. Primer nombre		118. Otros nombres	
5119. Razón social							
120. Valor capital del socio		121. % Participación		122. Fecha de ingreso		123. Fecha de retiro	

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001			
Espacio reservado para la DIAN				Página 5 de 5 Hoja 5					
				4. Número de formulario 14972953384					
 (415)7707212489984(8020) 000001497295338 4									
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico			
9 0 1 7 8 1 6 2 5		1		Impuestos de Bogotá		3 2			
Revisor Fiscal y Contador									
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV			127. Número de tarjeta profesional	
	128. Primer apellido		129. Segundo apellido		130. Primer nombre			131. Otros nombres	
	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada				
	135. Fecha de nombramiento								
Revisor fiscal suplente	136. Tipo de documento		137. Número de identificación		138. DV			139. Número de tarjeta profesional	
	140. Primer apellido		141. Segundo apellido		142. Primer nombre			143. Otros nombres	
	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada				
	147. Fecha de nombramiento								
Contador	148. Tipo de documento		149. Número de identificación		150. DV			151. Número de tarjeta profesional	
	Cédula de Ciudadanía 1 3		1 0 3 0 6 1 8 6 2 6		4			2 8 1 3 8 9 T	
	152. Primer apellido		153. Segundo apellido		154. Primer nombre			155. Otros nombres	
	PINZON		ROJAS		ANDRES			CAMILO	
156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada					
159. Fecha de nombramiento		2 0 2 3 1 1 0 8							

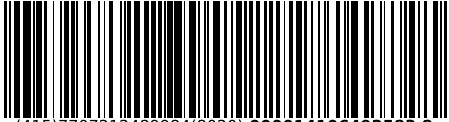
DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064929586			
5. Número de Identificación Tributaria (NIT) 9014479681				6. DV 1		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32							
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación			
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 110111				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		51. Código 2		52. Número establecimientos			
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			
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:				Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre VELEZ CASTRO HUMBERTO DE JESUS 985. Cargo Representante Legal Suplente Certificado			

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 141064929586		
			(415)7707212489984(8020) 000014106492958 6		
5. Número de Identificación Tributaria (NIT)		6. DV	12. Dirección seccional		14. Buzón electrónico
9 0 1 4 4 7 9 6 8		1	Impuestos de Bogotá		3 2
Características y formas de las organizaciones					
62. Naturaleza		2	63. Formas asociativas		1 2
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	
71. Clase		0 4			
72. Número					
73. Fecha		2 0 2 0 1 2 2 8			
74. Número de notaría					
75. Entidad de registro		0 3			
76. Fecha de registro		2 0 2 0 1 2 2 9			
77. No. Matricula mercantil		0 3 3 2 0 4 4 3			
78. Departamento		1 1			
79. Ciudad/Municipio		4			
Vigencia					
80. Desde		2 0 2 0 1 2 2 8			
81. Hasta		2 0 9 9 1 2 3 1			
Composición del Capital					
82. Nacional		1 0 0 %			
83. Nacional público		0 . 0 %			
84. Nacional privado		1 0 0 . 0 %			
85. Extranjero		0 %			
86. Extranjero público		0 . 0 %			
87. Extranjero privado		0 . 0 %			
Entidad de vigilancia y control					
88. Entidad de vigilancia y control					
Superintendencia de Sociedades					
5					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1	8 0	2 0 2 1 0 1 2 5		-	
2				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
				96. DV.	
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001		
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5				
				4. Número de formulario 141064929586				
 (415)7707212489984(8020) 000014106492958 6								
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico		
9 0 1 4 4 7 9 6 8		1		Impuestos de Bogotá		3 2		
Revisor Fiscal y Contador								
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV		127. Número de tarjeta profesional	
	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6				2 3 2 3 2 5 T	
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres	
	TOVAR		LOZANO		JAIRO		DAVID	
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada			
	135. Fecha de nombramiento		2 0 2 3 0 3 3 0					
	136. Tipo de documento		137. Número de identificación		138. DV		139. Número de tarjeta profesional	
	140. Primer apellido		141. Segundo apellido		142. Primer nombre		143. Otros nombres	
Contador	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada			
	147. Fecha de nombramiento							
	148. Tipo de documento		149. Número de identificación		150. DV		151. Número de tarjeta profesional	
	Cédula de Ciudadanía 1 3		1 0 3 0 6 1 8 6 2 6				2 8 1 3 8 9 T	
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres	
	PINZON		ROJAS		ANDRES		CAMILO	
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada			
	159. Fecha de nombramiento		2 0 2 2 0 2 2 3					

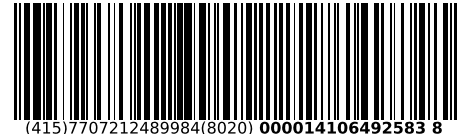
DIAN		Formulario del Registro Único Tributario		001	
2. Concepto 02 Actualización				4. Número de formulario 141064925838	
(415)7707212489984(8020) 000014106492583 8					
5. Número de Identificación Tributaria (NIT)		6. DV	12. Dirección seccional		14. Buzón electrónico
9 0 0 3 9 6 1 7 6		1	Impuestos de Bogotá		3 2
IDENTIFICACIÓN					
24. Tipo de contribuyente		25. Tipo de documento		26. Número de Identificación	
Persona jurídica		1			
Lugar de expedición		28. País		29. Departamento	
				30. Ciudad/Municipio	
31. Primer apellido		32. Segundo apellido		33. Primer nombre	
				34. Otros nombres	
35. Razón social					
MNEMO COLOMBIA SAS					
36. Nombre comercial					
37. Sigla					
UBICACIÓN					
38. País		39. Departamento		40. Ciudad/Municipio	
COLOMBIA		Bogotá D.C.		Bogotá, D.C.	
41. Dirección principal		42. Correo electrónico		43. Código postal	
CL 99 10 19 OF 502		recepcion.colombia@mnemo.com		1 1 0 1 1 1	
44. Teléfono 1		45. Teléfono 2		46. Teléfono 3	
3 1 8 3 8 3 5 1 1 7		5 7 5 5 2 7 2 1 0			
CLASIFICACIÓN					
Actividad económica					
Actividad principal		Actividad secundaria		Otras actividades	
46. Código		47. Fecha inicio actividad		48. Código	
6 2 0 1		2 0 1 0 1 1 1 2		6 2 0 2	
49. Fecha inicio actividad		50. Código		51. Código	
2 0 1 0 1 1 1 2		1 2		6 2 0 9 8 5 5 1	
Responsabilidades, Calidades y Atributos					
53. Código					
5 7 9 1 0 1 4 1 8 1 9 2 6 4 1 4 2 4 8 5 2 5 5					
05- Impto. renta y compl. régimen ordinario					
26- Declaración individual precios de tran					
07- Retención en la fuente a título de rent					
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					
55. Forma					
56. Tipo					
Servicio					
1					
2					
3					
57. Modo					
58. CPC					
59. Anexos					
SI NO X					
60. No. de Folios:					
0					
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012.					
Firma del solicitante:					
Sin perjuicio de las verificaciones que la DIAN realice.					
Firma autorizada:					
984. Nombre VELEZ CASTRO HUMBERTO DE JESUS					
985. Cargo Representante Legal Suplente Certificado					

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN		4. Número de formulario		Página 2 de 4 Hoja 2 141064925838	
				(415)7707212489984(8020) 000014106492583 8	
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	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma					
Documento		1. Constitución		2. Reforma	
71. Clase 0 4		72. Número 2 0 1 0 1 1 1 2		73. Fecha 2 0 1 3 0 4 1 8	
74. Número de notaría 0 3		75. Entidad de registro 2 0 1 0 1 1 1 9		76. Fecha de registro 0 2 0 4 5 1 6 2	
77. No. Matrícula mercantil 1 1		78. Departamento 4		79. Ciudad/Municipio	
Vigencia		80. Desde 2 0 1 0 1 1 1 2		81. Hasta	
Composición del Capital					
82. Nacional 0 %		83. Nacional público 0 . 0 %		84. Nacional privado 0 . 0 %	
85. Extranjero 1 0 0 %		86. Extranjero público 0 . 0 %		87. Extranjero privado 1 0 0 . 0 %	
Entidad de vigilancia y control					
88. Entidad de vigilancia y control Superintendencia de Sociedades					
5					
Estado y Beneficio					
Item		89. Estado actual		90. Fecha cambio de estado	
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		98. 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

141064925838



(415)7707212489984(8020) 000014106492583 8

5. Número de Identificación Tributaria (NIT)

9 0 0 3 9 6 1 7 6 1

6. DV

1

12. Dirección seccional

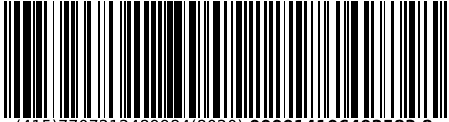
Impuestos de Bogotá

14. Buzón electrónico

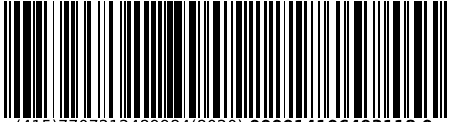
3 2

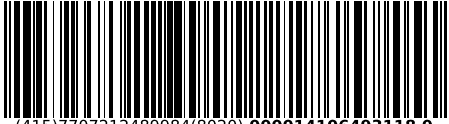
Representación

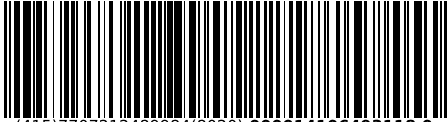
98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 1 7 0 8 2 9
100. Tipo de documento Cédula de Extranjeri 2 2	101. Número de identificación 6 6 7 3 5 2	102. DV 103. Número de tarjeta profesional
104. Primer apellido VICENT	105. Segundo apellido FERNANDEZ	106. Primer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

DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001				
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5						
				4. Número de formulario 141064925838						
 (415)7707212489984(8020) 000014106492583 8										
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico				
9 0 0 3 9 6 1 7 6		1		Impuestos de Bogotá		3 2				
Revisor Fiscal y Contador										
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV			127. Número de tarjeta profesional		
	Cédula de Ciudadanía 1 3		1 4 2 3 9 5 8 1					2 7 3 9 8 T		
	128. Primer apellido		129. Segundo apellido		130. Primer nombre			131. Otros nombres		
	SALAZAR		GOMEZ		JOSE			IGNACIO		
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada					
	135. Fecha de nombramiento		2 0 2 3 0 3 3 1							
	136. Tipo de documento		137. Número de identificación		138. DV			139. Número de tarjeta profesional		
	140. Primer apellido		141. Segundo apellido		142. Primer nombre			143. Otros nombres		
Contador	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada					
	147. Fecha de nombramiento									
	148. Tipo de documento		149. Número de identificación		150. DV			151. Número de tarjeta profesional		
	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6					2 3 2 3 2 5 T		
	152. Primer apellido		153. Segundo apellido		154. Primer nombre			155. Otros nombres		
	TOVAR		LOZANO		JAIRO			DAVID		
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada					
	159. Fecha de nombramiento		2 0 2 2 0 1 1 7							

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064931180			
5. Número de Identificación Tributaria (NIT) 901306687				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			
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 110111		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			
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:				Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre PARRA GAMBOA JOHN JAIRO 985. Cargo Representante legal Certificado			

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 141064931180		
 (415)7707212489984(8020) 000014106493118 0					
5. Número de Identificación Tributaria (NIT) 9 0 1 3 0 6 6 8 7		6. DV 2	12. Dirección seccional Impuestos de Bogotá		14. Buzón electrónico 3 2
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas 9 9		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma			Composición del Capital		
Documento	1. Constitución		2. Reforma		
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					

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

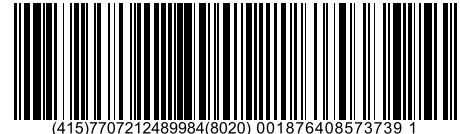
DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001	
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5			
				4. Número de formulario 141064931180			
 (415)7707212489984(8020) 000014106493118 0							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2	
Revisor Fiscal y Contador							
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV 127. Número de tarjeta profesional		
	Cédula de Ciudadanía 1 3		8 7 7 0 4 4 6		6 1 0 6 1		
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres
	VELEZ		CASTRO		HUMBERTO		DE JESUS
Revisor fiscal suplente	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						
	136. Tipo de documento		137. Número de identificación		138. DV 139. Número de tarjeta profesional		
Contador	140. Primer apellido		141. Segundo apellido		142. Primer nombre		143. Otros nombres
	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada		
	147. Fecha de nombramiento						
	148. Tipo de documento		149. Número de identificación		150. DV 151. Número de tarjeta profesional		
Contador	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6		2 3 2 3 2 5		
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres
	TOVAR		LOZANO		JAIRO		DAVID
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada		
159. Fecha de nombramiento							
2 0 2 1 0 6 0 1							

Espacio reservado para la DIAN



4. Número de formulario

18764085737391



(415)7707212489984(8020) 001876408573739 1

5. Número de Identificación Tributaria - NIT

6. DV

7. Primer apellido

8. Segundo apellido

9. Primer nombre

10. Otros nombres

9 0 1 7 8 1 6 2 5

1

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

12. Dirección seccional

Impuestos de Bogotá

Cód.

3 2

24. Dirección

CL 99 # 10 - 19 OF 502 ED TRADE CENTER

25. País

Colombia

26. Departamento

Bogotá D.C.

27. Municipio

Bogotá, D.C.

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

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

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

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

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

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

Firma del funcionario autorizado

Firma del solicitante



984. Apellidos y nombres

985. Cargo

989. Dependencia

990. Lugar administrativo SUBDIRECCION DE FACTURA ELECTRONICA Y SOLUCI

991. Organización

U.A.E. DIRECCION DE IMPUESTOS Y ADUANAS NACION

992. Área

993. Establecimiento

1001. Apellidos y nombres VELEZ CASTRO HUMBERTO DE JESUS

1002. Tipo documento Cédula de Ciudadanía

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

1004. DV 3

1005. Cod. Representación Representante Legal Principal

1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

997. Fecha formalización

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

Espacio reservado para la DIAN



4. Número de formulario

18764085737391



(415)7707212489984(8020) 001876408573739 1

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
9 0 1 7 8 1 6 2 5	1				

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

Rangos de numeración para autorizar, habilitar o inhabilitar

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



Bogotá, 20 de Marzo de 2025

Señores

FONDO NACIONAL DEL AHORRO SA

Ciudad.

REF: CIRCULAR 042 DE 2012

Respetados señores:

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

Agradecemos la atención a la presente,

Cordialmente,

HUMBERTO DE JESUS VELEZ CASTRO
Representante legal
MNENO COLOMBIA SAS

Gerencia Tesorería

Documento de Pago

No. ORDEN DE PAGO	36	FECHA DE CONTABILIZACION	09-abr-25
No. DOCUMENTO DE PAGO	5300274089	FECHA DE DOCUMENTO	09-abr-25
		FECHA DE COMPENSACION	09-abr-25
PROPUESTA	50222	FECHA DE LA PROPUESTA	09-abr-25

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:	FE36 RAD 02-2303-202503260439469		
NÚMERO DE CUENTA	2501050101	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	397.396.242		

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	5300274089	36	397.396.242	FE36 RAD 02-2303-202503260439469	6200000102	CTO 173 DE 2023

División de Presupuesto

Documento de Pago

N° ORDEN DE PAGO	5300274089	FECHA DE CONTABILIZACIÓN	25.03.2025
N° DE REFERENCIA	36	FECHA DE PAGO	09.04.2025

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

PROVEEDOR	CONSORCIO UNIDAD DE CIBERSEGURIDAD	N° IDENTIFICACION	9017816251
BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE		
N° IDENTIFICACION	9017816251	TIPO DE IDENTIFICACION	NIT
FORMA DE PAGO	PAGO ELECTRÓNICO	CIUDAD	BOGOTÁ
N° DE CUENTA	0136002901	BANCO	BANCO BBVA
TIPO DE CUENTA	CUENTA DE AHORROS	INFORME N°	CTO 173-20
N° FACTURA PROVEEDOR	FE36 RAD 02-2303-202503260439469		

OBSERVACIONES:

INFORMACIÓN PRESUPUESTAL						
SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
20001186	6200000102	00090	CTO 173 DE 2023 .	1000049730	5105630283	37.036.370
20001186	6200000102	00010	CTO 173 DE 2023 .	1000048947	5105630283	317.007.670
20001186	6200000102	00080	CTO 173 DE 2023 .	1000048952	5105630283	37.909.830
20001186	6200000102	00030	CTO 173 DE 2023 .	1000051924	5105630283	31.474.310
AFECTACIÓN PEDIDO						423.428.180
DETALLE DE LA ORDEN DE PAGO						
VALOR TOTAL FAC.		423.428.180,00				
DESCUENTOS		26.031.938,00				
NOTAS CRÉDITOS		0,00				
VALOR A PAGAR		397.396.242,00				