fna FONDO NACIONAL DEL AHORRO	**FORMATO ÚNICO DE INVENTARIO DOCUMENTAL**	**GSO-GD-FO-026**
	PROCESO DE GESTIÓN DOCUMENTAL	
	REFERENCIA - ACUERDO No. 001 DE 2004 AGN	**VERSIÓN: 2**

ENTIDAD REMITENTE

ENTIDAD PRODUCTORA	FONDO NACIONAL DEL AHORRO S.A.
UNIDAD ADMINISTRATIVA:	VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL
OFICINA PRODUCTORA:	GERENCIA DE ESTRATEGIA TI Y ASEGURAMIENTO INFORMATICO
OBJETO:	ENTREGA DE DOCUMENTOS A GERENCIA DE CONTRATACIÓN

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

NO° DE ORDEN	**CÓDIGOS**			**NONBRE DE LA SERIE, SUBSERIE O ASUNTOS**	**NOMBRE DE LA UNIDAD DOCUMENTAL**	**FECHAS EXTREMAS (dd-mm-aaaa)**		**SOPORTE O FORMATO**		**FÍSICO**						**ELECTRÓNICO**			**FRECUENCIA DE CONSULTA**	**OBSERVACIONES**
										UNIDAD DE CONSERVACIÓN										
										PAPEL				**OTRO**						
	CÓDIGO OFICINA	**SERIE**	**SUBSERIE**			**Inicial**	**Final**	**Físico**	**Electrónico**	**Caja**	**Carpeta**	**Tomo**	**Número de folios**	**Tipo**	**Cantidad**	**Ubicación**	**Cantidad de documentos**	**Tamaño de los documentos**		
1	1501	13	3	Contrato prestación de servicios	Contrato No. 173-2023 CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA - Soportes Informe Seguimiento para pago Nro.25 factura Nro. FE34 orden de pago No. 5300180274	13-feb-25	11-mar-25		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	228	16,7 MB		

Autorizado por:	**Jessebell Cristina Mejias Linares**	**Entregado por:**	**Jessebell Cristina Mejias Linares**	**Recibido por:**	
Cargo:	**Auxiliar Administrativo 01**	**Cargo:**	**Auxiliar Administrativo 01**	**Cargo:**	
Firma:		**Firma:**		**Firma:**	
Lugar:	**Bogotá D.C.**	**Lugar:**	**Bogotá D.C.**	**Lugar:**	
Fecha:	**17-03-2025**	**Fecha:**	**17/03/2025**	**Fecha:**	

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

INFORME No 25 **FACTURA No**

No. DE ACEPTACIÓN: 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363

FECHA		
13	02	25
dd	mm	aaaa

1. GENERALIDADES DEL CONTRATO

CONTRATO No 173 (Número de Contrato) **DE** 2023 (Año de suscripción) **TIPO DE CONTRAT** Prestación de servicios (Prestación de servicios, interventoria, consultoría, Convenio)

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

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

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

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

APOYO SUPERVISIÓN Enrique Arrazola (Nombre de la persona delegada para apoyar la supervisión del contrato) — Luz Helena Riaño - Leonardo Rivera (Nombre de la persona delegada para apoyar la supervisión del contrato)

OBJETO DEL CONTRATO

CONTRATAR UNIDAD DE CIBERSEGURIDAD QUE PROPORCIONE SERVICIOS DE SEGURIDAD INTEGRADOS AL FONDO NACIONAL DEL AHORRO

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

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

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

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

REGISTRO PRESUPUESTAL No. 5400001604 - 6200000102 - 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 MCTE ($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	
No.	PLAZO

ADICIONES		
No.	VALOR	RP
1	$ 19.922.987.493	5400001890

SUSPENSIONES		
No	DESDE	HASTA

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	$ 36.499.583.610,00	**64,69%**
Adiciones	$ 19.922.987.493,00	**35,31%**
VALOR TOTAL DEL CONTRATO	**$ 56.422.571.103,00**	**100,00%**
Valor ejecutado antes del presente pago	$ 26.354.918.094,00	**46,71%**
Valor del pago aprobado con el presente informe	$ 269.280.340,00	**0,48%**
VALOR TOTAL EJECUTADO	**$ 26.624.198.434,00**	**47,19%**
Porcentaje de ejecución presupuestal programado a la fecha		**47,23%**
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		**-0,04%**

OBSERVACIONES

Cuenta 25: administración y soporte en sitio durante el período del 22 de noviembre de 2024 al 21 de diciembre de 2024. . items 1 al 10 prefactura C-2-26
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	**59%**
Porcentaje de ejecución de actividades realizado a la fecha	**59%**
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CONTRATO	**0%**

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

*La fase de ejecución corresponde a desarrollo de Software de propiedad del FNA	**SI** [ ]	**NO** [X]
*Si corresponde a Software del FNA marque la fase correspondiente	**Investigación** [ ]	**Desarrollo** [ ]

OBSERVACIONES

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

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

4. CONCEPTO SUPERVISOR O INTERVENTOR

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de DOCIENTOS SESENTA Y NUEVE MILLONES DOSCIENTOS OCHENTA MIL TRESCIENTOS CUARENTA PESOS MCTE ($ 269.280.340).

5. EVALUACIÓN CONTRATISTA (Escala de 0 - 5)

EVALUACION PARCIAL	
Cumplimiento del contrato	4
Plazos	4
Aspectos administrativos	4

6. CERTIFICACIÓN PARA PAGO

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

CERTIFICA:

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

ANEXOS PRESENTE INFORME

ANEXO		No FOLIOS	DESCRIPCION
Certificado pago Seguridad Social	X	**PDF**	**Certificaciones, planilla pago parafiscales, CC y T.P.**
Informes	X	**PDF**	**Informe de Supervisión** **Informe Gestión Proveedor**
Actas	X	**PDF**	**Acta Seguimiento Mensual ANS**
OTROS	X	**PDF**	**Pre-factura** **Certificación Cuenta Bancaría** **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

Trece (día en letras) **13** (día en números) días del mes de **febrero** (mes en letras) de **2025** (Año)

Mónica Grand Villada

Firmado digitalmente por Mónica Grand Villada
Fecha: 2025.02.24 14:08:41 -05'00'

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

Revisó y aprobó: Enrique Arrazola - Leonardo Rivera - 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			
Nº doc.	5100000341	Sociedad	1000	Ejercicio	2025	
Fe.docum.	25.02.2025	Fecha contab.	25.02.2025	Período	02	
Calc.impuestos	☑					
Referen.	34					
Moneda doc.	COP					
Txt.cab.doc.	02-2303-202502250261353					

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	252,725,256-
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	172,862,970
5	81	5130950401	CENTRO OPER SEG		W0	0
6	86	2511950101	CXP PROVED EM/RF		W0	27,906,690
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%			7,920,010-
11	50	2519053801	RTE IVA TARIFA GENER			6,449,151-
12	50	2519054408	SERVICIOS 304 BOGOTA			2,185,923-

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 34

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	25/02/2025, 10:01
Expedición	25/02/2025, 10:04
Vencimiento	27/03/2025

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Administración y soporte de la plataforma XDR. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	3,957,940.00
2	Administración y soporte de la plataforma SOAR. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	17,406,130.00
3	Administración y soporte de la plataforma THREAT INTELLIGENCES. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	33,078,430.00
4	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	66,632,860.00
5	Administración y soporte Servicio de MONITOREO DE DNS. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	61,978,770.00
6	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT. Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	9,852,010.00
7	Administración y soporte de la plataforma CIBERDEFENSA Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	6,990,060.00
8	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	10,003,140.00
9	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM). Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	27,906,690.00
10	Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (IAM). Contrato No. 173-2023 N° de aceptación 1000054356 / 1000054357 / 1000054358 / 1000054361 / 1000054363	1.00	0.00	31,474,310.00

Total items: 10

Valor en Letras:
Doscientos sesenta y nueve millones doscientos ochenta mil trescientos cuarenta pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Otro - Crédito - Cuota No. 001 vence el 2025-03-27 por $ 269,280,340.00

Observaciones:

Total Bruto	226,286,000.00
IVA 19%	42,994,340.00
Total a Pagar	**269,280,340.00**

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

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: a333298c842b8e5cf84b967247b4bab79cca16b60eb53389e9aa8e9bf6b522bb9e218fcc344b9f2cecfb79e753aa7f76

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

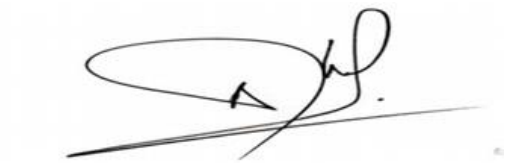
NIT 901.781.625-1

CERTIFICA QUE:

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

Para constancia de lo anterior se firma en Bogotá a los Veinte (20) días del mes de Enero de dos mil veinticuatro (2025).

Atentamente,



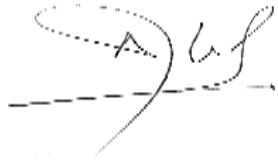
HUMBERTO DE JESUS VELEZ CASTRO
Representante Legal **CONSORCIO SOC-NOC-MINTIC**
C.C. No. 8.770.446 expedida en Soledad-Atlántico.
Dirección: Calle 99 No. 10 – 19 Oficina 502 Edificio Trade Center de Bogotá D.C.
Teléfono: 6913133 – 310 8569109
Correo electrónico: h.dejesusvelez@mnemo.com

MNEMO

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

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

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002. Dada en Bogotá D.C., a los Veinte (20) días del mes de Enero de 2024.



HUMBERTO DE JESUS VELEZ CASTRO
C.C. 8.770.446 de Soledad – Atlántico
T.P. No. 61.061-T de la Junta Central de Contadores de Colombia


CEDULA DE CIUDADANIA
REPÚBLICA DE COLOMBIA
NUIP 8.770.446
VELEZ CASTRO
HUMBERTO DE JESUS
COL
1.70
M
26 JUL 1970
B+
BARRANQUILLA (ATLANTICO)
15 SEPT 1988, SOLEDAD
29 DIC 2030


0000163555
REGISTRADOR NACIONAL
ICCOL0000163550030 52<<<<<<<<<<<
7007282M3012291COL8770446<<<<8
VELEZ<CASTRO<<HUMBERTO<DE<JESU



UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

61061-T

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

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

251625 69149



UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

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

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

FIRMA

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

En mi calidad de revisor fiscal de la compañía **MNEMO CYBER SEC S.A.S.,** identificada con NIT**: 901.447.968-1**, he efectuado los procedimientos de revisión que se detallan a continuación con el propósito de verificar el pago efectuado por la compañía por concepto de **aportes a los sistemas de salud, pensión y riesgos laborales y a las cajas de compensación familiar, instituto colombiano de bienestar familiar (ICBF) y servicio nacional de aprendizaje (SENA)**, por el periodo de **(6)** seis meses comprendidos entre el **1 de julio de 2024 y 31 de diciembre del 2024**. El pago de dichos aportes es responsabilidad de la administración de la compañía como parte de mi gestión.

Los procedimientos de revisión realizados fueron los siguientes:

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

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

3. Obtención del listado de liquidación de aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA),preparado por la compañía por el periodo de **(6) meses** comprendidos entre el **1 de julio de 2024 y 31 de diciembre del 2024.**

4. El ultimo pago de aportes corresponde a **pensión diciembre** del año **2024 y salud enero** 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 julio de 2024 y 31 de diciembre del 2024**, informo que, a la fecha del presente informe, la compañía se encuentra al día en el pago de los aportes a los Sistemas de Salud, Pensiones y Riesgos Laborales y a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Esta certificación se emite a los veinte (20) días, del mes de enero 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 julio de 2024 al 20 de enero 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 enero 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

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

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

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-12	2025-01	1202836794	9480408596	E	2025/01/17	2025/01/20	BANCO BBVA COLOMBIA S.A.	3	$46,865,600

LIQUIDACION DETALLADA DE APORTES

EMPLEADO				NOVEDADES																	PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación		Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Días	Codigo	Dias	Codigo	Días	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (33 Afiliados)																															
Centro de Trabajo: CENTRO TRABAJO 1 (32 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (32 Afiliados)																															
1	CC	80180206	AMAZO RAMIREZ WALTER JAIR																		230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
2	CC	1000985154	ARIAS BALLEN ANDRES FELIPE									X									230301	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
3	CC	1233493654	BARGAS GARCIA JULIAN ANDRES										X		X						230301	9	EPS005	9	CCF24	6	14-25	9	0.000%	6	Si
4	CC	1233493654	BARGAS GARCIA JULIAN ANDRES		X							X								X	230301	11	EPS005	11	CCF24	11	14-25	11	0.522%	11	Si
5	CC	1015425546	CAITA CORREA CHRISTIAM GERMAN																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
6	CC	1070981128	COLLAZOS FONSECA MATEO																		25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
7	CC	79619776	ENCISO ALARCON JOHN JAIRO																		230301	30	MIN002	30	CCF24	30	14-25	30	0.522%	30	Si
8	CC	1016043734	GARCIA BUITRAGO JEISSON ALEJANDRO																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
9	CC	1022394508	GUARIN MORA JOHN ALEXANDER									X									230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
10	CC	1024460422	JIMENEZ JIMENEZ BRAYAN STEVEN									X									25-14	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
11	CC	1015474263	LOZANO ESCAMILLA JOHAN ALEXIS									X									25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
12	CC	1019138524	MALLAMA MEJIA JOHNNY ALBEIRO									X									230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
13	CC	13871620	MARTINEZ CARREÑO HECTOR MANUEL																		230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
14	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																		230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
15	CC	80182122	MEDINA ROJAS EDWIN FERNEY																		231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
16	CC	1018453849	MERCHAN SANCHEZ LUISA FERNANDA									X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
17	CC	1012373695	MONTERO BARRETO SINDY JOHANNA									X									230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
18	CC	1019024612	MORA MENDOZA MAGDA PAOLA																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	No
19	CC	1023937645	MORENO DIAZ WENDY JOHANNA									X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
20	CC	1233901826	MOYAN SANTANA CRISTIAN CAMILO									X									230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
21	CC	1019079260	PABON AMAYA PEDRO YULIAN									X									230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
22	CC	80093909	PICO CARREÑO MAURO JAVIER																		25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
23	CC	1072431635	RAMIREZ CASTAÑEDA RAMIRO ANDRES									X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
24	CC	1110459814	SANABRIA ROJAS LUIS ALFONSO																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
25	CC	1002048195	TABORDA GAMARRA YESSID									X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si

Planilla Resumen

26	CC	1073515030	TAYLOR CASALLAS BRANDON DAVID									X									23100 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
27	CC	79729048	URIBE RUIZ WILSON																		25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
28	CC	1031143384	URREGO BOLIVAR SANDRO JAVIER													X					23020 1	1	EPS002	1	CCF24	1	14-25	1	0.000%	1	Si
29	CC	1031143384	URREGO BOLIVAR SANDRO JAVIER									X									23020 1	29	EPS002	29	CCF24	29	14-25	29	0.522%	29	Si
30	CC	1025142024	VALERO RICAURTE JOHAN STIF									X									23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	79992504	VANEGAS RODRIGUEZ YAIR ALEXIS													X					23100 1	5	MIN002	5	CCF24	5	14-25	5	0.000%	5	Si
32	CC	79992504	VANEGAS RODRIGUEZ YAIR ALEXIS		X																23100 1	25	MIN002	25	CCF24	25	14-25	25	0.522%	25	Si
33	CC	1015404947	VARGAS MARTINEZ JOSE DAVID																		23100 1	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
34	CC	1070307880	ZAMBRANO OSORIO OSCAR ANDRES													X					23020 1	11	EPS041	11	CCF24	11	14-25	11	0.000%	11	Si
35	CC	1070307880	ZAMBRANO OSORIO OSCAR ANDRES									X								X	23020 1	19	EPS041	19	CCF24	19	14-25	19	0.522%	19	Si
36	CC	1022438994	ZARAMA CAMPOS JUAN SEBASTIAN									X									23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																															
37	CC	1070917650	HERNANDEZ PEREZ YENNY FERNANDA											X		X					23020 1	2	EPS005	2	CCF24	1	14-25	2	0.000%	1	No
38	CC	1070917650	HERNANDEZ PEREZ YENNY FERNANDA																		23020 1	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	No
Total	**Afiliados(33)**																														

PLANILLA PAGADA

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

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

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-12	2025-01	1202836794	9480408596	E	2025/01/17	2025/01/20	BANCO BBVA COLOMBIA S.A.	3	$46,865,600

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				33	$28,734,500	$54,700	$0	$28,789,200
COLFONDOS	231001	800,227,940	6	4	$4,008,500	$7,700	$0	$4,016,200
COLPENSIONES	25-14	900,336,004	7	7	$8,146,000	$15,500	$0	$8,161,500
PORVENIR	230301	800,224,808	8	14	$9,777,800	$18,500	$0	$9,796,300
PROTECCION	230201	800,229,739	0	7	$5,612,200	$10,600	$0	$5,622,800
SKANDIA	230901	800,253,055	2	1	$1,190,000	$2,400	$0	$1,192,400
ARL (ADMINISTRADORAS: 1)				33	$942,600	$1,800	$0	$944,400
COLMENA	14-25	800,226,175	3	33	$942,600	$1,800	$0	$944,400
CCF (ADMINISTRADORAS: 1)				33	$6,985,900	$13,200	$0	$6,999,100
COMPENSAR	CCF24	860,066,942	7	33	$6,985,900	$13,200	$0	$6,999,100
EPS (ADMINISTRADORAS: 10)				33	$8,946,100	$17,500	$0	$8,963,600
CAPITAL SALUD	EPSC34	900,298,372	9	1	$122,700	$300	$0	$123,000
COMPENSAR	EPS008	860,066,942	7	5	$878,300	$1,700	$0	$880,000
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	2	$286,600	$600	$0	$287,200
FAMISANAR	EPS017	830,003,564	7	4	$752,500	$1,500	$0	$754,000
FOSYGA	MIN001	901,037,916	1	1	$300,000	$600	$0	$300,600
FOSYGA RÉGIMEN DE EXCEPCIÓN	MIN002	901,037,916	1	2	$640,100	$1,300	$0	$641,400
NUEVA E.P.S.	EPS037	900,156,264	2	3	$379,800	$800	$0	$380,600
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	$126,900	$300	$0	$127,200
SALUD TOTAL	EPS002	800,130,907	4	5	$758,800	$1,500	$0	$760,300
SANITAS	EPS005	800,251,440	6	9	$4,700,400	$8,900	$0	$4,709,300
ICBF (ADMINISTRADORAS: 1)				2	$700,200	$1,400	$0	$701,600
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	2	$700,200	$1,400	$0	$701,600
SENA (ADMINISTRADORAS: 1)				2	$466,800	$900	$0	$467,700
SENA	PASENA	899,999,034	1	2	$466,800	$900	$0	$467,700
TOTAL				**33**	**$46,776,100**	**$89,500**	**$0**	**$46,865,600**

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

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

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-12	2025-01	1208054826	9480493094	E	2025/01/21	2025/01/20	BANCO BBVA COLOMBIA S.A.	0	$159,696,900

LIQUIDACION DETALLADA DE APORTES

EMPLEADO			NOVEDADES																PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Días	Codigo	Dias	Codigo	Días	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (92 Afiliados)																													

Planilla Resumen

Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (21 Afiliados)

Ciudad: BOGOTA Depto: BOGOTA D.E. (21 Afiliados)

1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																		230201	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
2	CC	93387321	ARANA REYES JAMES GUSTAVO																		25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No
3	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	No
4	CC	1122651302	CARO ROA JONATHAN													X					230301	1	EPS005	1	CCF24	1	14-25	1	0.000%	1	Si
5	CC	1122651302	CARO ROA JONATHAN													X					230301	4	EPS005	4	CCF24	4	14-25	4	0.000%	4	Si
6	CC	1122651302	CARO ROA JONATHAN													X					230301	5	EPS005	5	CCF24	5	14-25	5	0.000%	5	Si
7	CC	1122651302	CARO ROA JONATHAN																		230301	20	EPS005	20	CCF24	20	14-25	20	1.044%	20	Si
8	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																		230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
9	CC	1013592039	EMBUS IPIA JULIAN ANDRES											X							231001	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	No
10	CC	1013592039	EMBUS IPIA JULIAN ANDRES									X									231001	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	No
11	CC	6319789	ESPAÑA MOSQUERA JESUS ARBEY																		230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
12	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
13	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO									X									231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
14	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO													X					230301	1	EPS008	1	CCF24	1	14-25	1	0.000%	1	Si
15	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																	X	230301	29	EPS008	29	CCF24	29	14-25	29	1.044%	29	Si
16	CC	79865487	PUENTES CASTRO DAVID EDUARDO																		230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
17	CC	1018429259	RODRIGUEZ MATEUS JEAMY PAMMELA											X							230901	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	No
18	CC	1018429259	RODRIGUEZ MATEUS JEAMY PAMMELA																		230901	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	No
19	CC	79717549	RODRIGUEZ JOHN FERNANDO																		230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
20	CC	80791790	ROJAS ARIAS RICARDO													X					230201	8	EPS005	8	CCF24	8	14-25	8	0.000%	8	No
21	CC	80791790	ROJAS ARIAS RICARDO																	X	230201	22	EPS005	22	CCF24	22	14-25	22	1.044%	22	No
22	CC	80066361	ROMERO ARCHILA DANIEL DARIO													X					230201	1	MIN001	1	CCF24	1	14-25	1	0.000%	1	Si
23	CC	80066361	ROMERO ARCHILA DANIEL DARIO																		230201	29	MIN001	29	CCF24	29	14-25	29	1.044%	29	Si
24	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																		231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
25	CC	24659147	VALDES RAMIREZ ALBA LIBIA																			0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
26	CC	79950164	VARGAS HINCAPIE FERNANDO									X									230301	30	EPS002	30	CCF24	30	14-25	30	1.044%	30	Si
27	CC	1032410736	VARGAS HINCAPIE HENRY																		230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
28	CC	1022411758	VARGAS LEON MARIA CAMILA													X					230301	30	EPS008	30	CCF24	30	14-25	30	0.000%	30	Si
29	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																			0	EPS002	30		0		0	0.000%	0	No

Centro de Trabajo: ADMINISTRACION (67 Afiliados)

Ciudad: BOGOTA Depto: BOGOTA D.E. (67 Afiliados)

30	CC	1014306151	ABRIL MONTES SERGIO LEONARDO									X									230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
32	CC	1023953140	ARIAS NATALIA MELIZA									X									230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si

PLANILLA PAGADA

33	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER																		231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
34	CC	1026295259	BEJARANO QUIROGA ANDRES FELIPE									X									25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
35	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER																		230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
36	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN																		230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
37	CC	1122512867	CAMPOS MARTINEZ JUAN ALEJANDRO									X									230301	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
38	CC	1014856015	CARDENAS LOPEZ NICOLAS ENRIQUE									X									230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
39	CC	1034397473	CASTILLO IDROBO JHON FABER																		230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
40	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID									X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
41	CC	1012976046	DIAZ MARIN CAMILO ARTURO									X									230301	30	EPS005	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	1023957895	GIL MURILLO JAVIER EDUARDO									X									25-14	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
44	CC	1001326677	GOMEZ PARRA CRISTIAN CAMILO									X									230201	30	EPS001	30	CCF24	30	14-25	30	0.522%	30	Si
45	CC	1019009180	GOMEZ ROJAS YENNY PAOLA											X							230301	2	EPS037	2	CCF24	0	14-25	2	0.000%	0	Si
46	CC	1019009180	GOMEZ ROJAS YENNY PAOLA																		230301	28	EPS037	28	CCF24	28	14-25	28	0.522%	28	Si
47	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
48	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
49	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL									X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
50	CC	1001326941	GUERRA JIMENEZ BRAYAN ALEXIS									X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
51	CC	1010840818	GUEVARA GUANCHA ERWIN SANTIAGO	X																	25-14	21	EPS017	21	CCF24	21	14-25	21	0.522%	21	Si
52	CC	1082874657	GUEVARA RIZZO SANTIAGO	X																	230301	21	EPS005	21	CCF24	21	14-25	21	0.522%	21	Si
53	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
54	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
55	CC	1099374748	LEAL GOMEZ DANIELA																		230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
56	CC	52953219	LEON CERON MARIA ALEXANDRA																		231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
57	CC	1069769484	LOPEZ ZAMORA JUAN DAVID													X					230301	1	EPS002	1	CCF24	1	14-25	1	0.000%	1	Si
58	CC	1069769484	LOPEZ ZAMORA JUAN DAVID																		230301	29	EPS002	29	CCF24	29	14-25	29	0.522%	29	Si
59	CC	1000149678	LOZANO GUTIERREZ MARIA CAMILA									X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
60	CC	1193088387	LUENGAS CORTES DAVID STIWEN									X									230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
61	CC	79992827	MARROQUIN GUTIERREZ DIDIER																		230201	30	MIN002	30	CCF24	30	14-25	30	0.522%	30	Si
62	CC	1000032122	MARTIN GARCES JUAN DAVID									X									230301	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	1023885573	MARTINEZ CASAS EDWARD ALEJANDRO									X									25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
64	CC	1000719172	MARTINEZ BECERRA MARIA JOSE									X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
65	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE													X					230201	1	EPS017	1	CCF24	1	14-25	1	0.000%	1	Si
66	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE									X								X	230201	29	EPS017	29	CCF24	29	14-25	29	0.522%	29	Si
67	CC	1000717997	MELO MOSQUERA DANIEL RENE									X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si

PLANILLA PAGADA

68	CC	98632570	MESA MENDEZ CARLOS MANUEL																	230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
69	CC	1022947945	MOLANO JIMENEZ JESUS RICARDO								X									230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
70	CC	1033711407	MURCIA TORRES JHON FREDY																	230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
71	CC	1034660019	MURCIA CARVAJAL KAROL DANIELA																		0	EPS005	30		0		0	0.000%	0	No
72	CC	1011087203	MURCIA GUERRERO SAMUEL																		0	EPS037	30		0		0	0.000%	0	No
73	CC	1032479763	ORJUELA CALDERON PAULA NATALIA												X					231001	12	EPS005	12	CCF24	12	14-25	12	0.000%	12	Si
74	CC	1032479763	ORJUELA CALDERON PAULA NATALIA								X									231001	18	EPS005	18	CCF24	18	14-25	18	0.522%	18	Si
75	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER								X									230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
76	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN												X					230301	12	EPS017	12	CCF24	12	14-25	12	0.000%	12	Si
77	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN																	230301	18	EPS017	18	CCF24	18	14-25	18	0.522%	18	Si
78	CC	1019127504	PERDOMO GUZMAN JESSICA LILIANA								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
79	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO																	230901	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
80	CC	1030618626	PINZON ROJAS ANDRES CAMILO																	230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
81	CC	1023972445	PRIETO SILVA NICOL																	230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
82	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN								X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
83	CC	1019110870	RAMIREZ ALARCON CAMILO																	230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
84	TI	1011096205	RIOS MONTAÑEZ DIEGO ALEXANDER																		0	EPS037	30		0		0	0.000%	0	No
85	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES								X									25-14	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
86	CC	1003712217	RODRIGUEZ PENAGOS JOAN SEBASTIAN								X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
87	CC	52505417	ROJAS PEÑA NILSA YAMILE																	25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
88	CC	1030697447	ROJAS PEREZ VALENTINA								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
89	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO												X					230201	8	EPS008	8	CCF24	8	14-25	8	0.000%	8	Si
90	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO																X	230201	22	EPS008	22	CCF24	22	14-25	22	0.522%	22	Si
91	CC	1000470126	SILVA BELTRAN JULIAN ANDRES	X																230201	29	EPS005	29	CCF24	29	14-25	29	0.522%	29	Si
92	CC	1003916380	SUAREZ BERDUGO SAMUEL ELIAS								X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
93	CC	1030539604	TAMAYO RIVERA FABIO ANDRES																	230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
94	CC	1020808701	TIBADUIZA CALDERON SEBASTIAN																	231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
95	CC	1018408876	TOVAR LOZANO JAIRO DAVID																	230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
96	CC	1014279176	URBANO ARDILA SEBASTIAN								X									25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
97	CC	80247522	VARGAS HINCAPIE CARLOS																	25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
98	CC	1075280531	VARGAS POLANIA JAIRO ALEXANDER																	230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
99	CC	1014197302	VELASQUEZ RAMOS JOHAN SEBASTIAN																	25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
100	CC	8770446	VELEZ CASTRO HUMBERTO DE JESUS																	230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	No
101	CE	667352	VICENT FERNANDEZ CARLOS																		0	EPS005	30	CCF24	30	14-25	30	0.522%	30	No

Planilla Resumen

No.		Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Pension Codigo	Pension Dias	Salud Codigo	Salud Dias	CCF Codigo	CCF Dias	Riesgos Codigo	Riesgos Dias	Tarifa	Parafiscales Dias	Exonerado SENA e ICBF
102	CC	1012343172	VIVAS TOVAR EDUAR ALEXANDER																			0	EPS010	30		0		0	0.000%	0	No
Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																															
103	CC	1019024746	MUÑOZ OROZCO BERTHA JUDITH																		25-14	30	EPS017	30	CCF24	30	14-25	30	1.044%	30	Si
Centro de Trabajo: MENSAJERIA (3 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (3 Afiliados)																															
104	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS																		230201	30	EPS008	30	CCF24	30	14-25	30	4.350%	30	Si
105	CC	79840394	RODRIGUEZ ANGARITA ELKIN																		230301	30	EPS008	30	CCF24	30	14-25	30	4.350%	30	Si
106	CC	91462884	SERRANO BONILLA JILMER													X					230301	8	MIN001	8	CCF24	8	14-25	8	0.000%	8	Si
107	CC	91462884	SERRANO BONILLA JILMER																		230301	22	MIN001	22	CCF24	22	14-25	22	4.350%	22	Si

LIQUIDACION DETALLADA DE APORTES

EMPLEADO				NOVEDADES																	PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación		Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: FAMISANAR (1 Afiliados)																															
Centro de Trabajo: FAMISANAR - ADMINISTRATIVO (1 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																															
108	CC	80155666	CHAVES MARTINEZ JORGE ANDRES													X					230201	1	EPS005	1	CCF24	1	14-25	1	0.000%	1	Si
109	CC	80155666	CHAVES MARTINEZ JORGE ANDRES									X								X	230201	29	EPS005	29	CCF24	29	14-25	29	0.522%	29	Si
Total		**Afiliados(93)**																													

PLANILLA PAGADA

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

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

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-12	2025-01	1208054826	9480493094	E	2025/01/21	2025/01/20	BANCO BBVA COLOMBIA S.A.	0	$159,696,900

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				86	$83,968,900	$0	$0	$83,968,900
COLFONDOS	231001	800,227,940	6	7	$13,547,900	$0	$0	$13,547,900
COLPENSIONES	25-14	900,336,004	7	15	$14,529,200	$0	$0	$14,529,200
PORVENIR	230301	800,224,808	8	33	$22,431,700	$0	$0	$22,431,700
PROTECCION	230201	800,229,739	0	27	$26,756,600	$0	$0	$26,756,600
SKANDIA	230901	800,253,055	2	4	$6,703,500	$0	$0	$6,703,500
ARL (ADMINISTRADORAS: 1)				88	$4,284,700	$0	$0	$4,284,700
COLMENA	14-25	800,226,175	3	88	$4,284,700	$0	$0	$4,284,700
CCF (ADMINISTRADORAS: 1)				88	$22,830,600	$0	$0	$22,830,600
COMPENSAR	CCF24	860,066,942	7	88	$22,830,600	$0	$0	$22,830,600
EPS (ADMINISTRADORAS: 10)				93	$39,001,500	$0	$0	$39,001,500
ALIANSALUD EPS (ANTES COLMEDICA)	EPS001	830,113,831	0	3	$1,957,100	$0	$0	$1,957,100
CAPITAL SALUD	EPSC34	900,298,372	9	1	$114,900	$0	$0	$114,900
COMPENSAR	EPS008	860,066,942	7	15	$4,959,300	$0	$0	$4,959,300
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	3	$412,100	$0	$0	$412,100
FAMISANAR	EPS017	830,003,564	7	11	$1,666,100	$0	$0	$1,666,100
FOSYGA	MIN001	901,037,916	1	8	$3,516,200	$0	$0	$3,516,200
FOSYGA RÉGIMEN DE EXCEPCIÓN	MIN002	901,037,916	1	1	$200,000	$0	$0	$200,000
NUEVA E.P.S.	EPS037	900,156,264	2	7	$1,171,600	$0	$0	$1,171,600
SALUD TOTAL	EPS002	800,130,907	4	9	$1,265,800	$0	$0	$1,265,800
SANITAS	EPS005	800,251,440	6	35	$23,738,400	$0	$0	$23,738,400
ICBF (ADMINISTRADORAS: 1)				11	$5,766,700	$0	$0	$5,766,700
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	11	$5,766,700	$0	$0	$5,766,700
SENA (ADMINISTRADORAS: 1)				11	$3,844,500	$0	$0	$3,844,500
SENA	PASENA	899,999,034	1	11	$3,844,500	$0	$0	$3,844,500
TOTAL				**93**	**$159,696,900**	**$0**	**$0**	**$159,696,900**

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

Acta N°	19	**Tema:**	Reunión de revisión de ANS, contrato 173 de 2023
Fecha:	20/01/2024	**Ubicación:**	Virtual.
Hora inicio:	10:00 am	**Hora fin:**	11:00 am

Objetivo	Reunión de revisión de ANS, contrato 173-2023 para el periodo comprendido entre el 22/11/2024 a 21/12/2024		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	**Dependencia**	**Cargo**	**¿Asistió?**
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 03	Si
Plinio Esteban Palomino López	Mnemo	Gerente de Proyecto Mnemo	Si

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

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

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 noviembre de 2024 al 21 de diciembre de 2024.
- Informes técnicos por solución o servicio

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

2.2. Cumplimiento del sistema de gestión de calidad

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

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 21 peticiones de soporte.

PETICIONES

Número	Estado	Título
RF415270	Closed	RE: CORREO RETENIDO // -25412 NOTIFICACION JUDICIAL DEMANDA LABORAL JUZGADO 02 CIVIL-2541125
RF415299	Closed	CORREO RETENIDO // DOMINA EXCEL 365 Y GOOGLE SHEETS CON IA 100 PR&#225
RF415301	Closed	CORREO RETENIDO // DOMINA EXCEL 365 Y GOOGLE SHEETS CON IA 100 PR&#225
RF415502	Closed	SOLICITUD LIBERACIÓN CORREO
RF415509	Closed	SOLICITUD LIBERACIÓN CORREO
RF415613	Closed	DESBLOQUEO DE CORREO DESPRENDIBLES DE PAGO
RF416068	Closed	SOLICITUD AYUDA CORREO RETENIDO
RF417121	Closed	Correo Retenido // Invitaci&#243
RF417193	Closed	CORREO RETENIDO // DOCUMENTO DE JULIAN BERNAL
RF417580	Closed	Correo Retenido // PROCESO DE TITULACI&#211
RF417593	Closed	EJECUCION DE SCRIPT PARA DESBLOQUEO DE USUARIO RF417349
RF417853	Closed	CORREO RETENIDO // &#127876
RF417856	Closed	Correo Retenido // &#127876
RF417858	Closed	Correo Retenido // &#127876

RF417866	Closed	Correo Retenido // &#127876
RF417872	Closed	CORREOS SPAM
RF417875	Closed	RV:
RF417887	Closed	IN147866: P.A. JAGGUA ETAPA 4 99219 Informes de Movimientos por Unidad y Pendientes de Identificar c
RF417907	Closed	REPORTE CORREO MALICIOSO
RF417910	Closed	RV: RECIBO DE PAGO DICIEMBRE 2024
RF417912	Closed	RV: CORREO RETENIDO // ? ¡NUEVO PORTAL Y TU PRIMA NAVIDEñA TE ESPERAN! ?
RF415270	Closed	RE: CORREO RETENIDO // -25412 NOTIFICACION JUDICIAL DEMANDA LABORAL JUZGADO 02 CIVIL-2541125

CAMBIOS

No se generaron cambios en el periodo.

2.4. Cumplimiento del cronograma

El avance en el cronograma del contrato 173-2023 para el periodo en cuestión, a corte de 21-12-24, corresponde al 59% esperado vs 59% completado, sin que se presente desviación general.

A continuación, captura de pantalla del cronograma actualizado:

% completado	% completado esperadoT1	Nombre de tarea	Duración	Comienzo	Fin
59%	59%	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
59%	59%	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
45%	45%	Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25
45%	44%	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 periodica del nivel de madurez (monitoreo y mejora continua)	366 días	lun 22/07/24	mar 9/12/25
100%	100%	Adquisición de herramientas tecnológicas	6 días	vie 22/12/23	lun 1/01/24
100%	100%	Despliegue de herramientas tecnológicas	162 días	vie 22/12/23	jue 1/08/24
100%	100%	Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24
49%	49%	Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26
47%	47%	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

2.5. Disponibilidad de Plataformas

2.5.1. Disponibilidad solución Darktrace

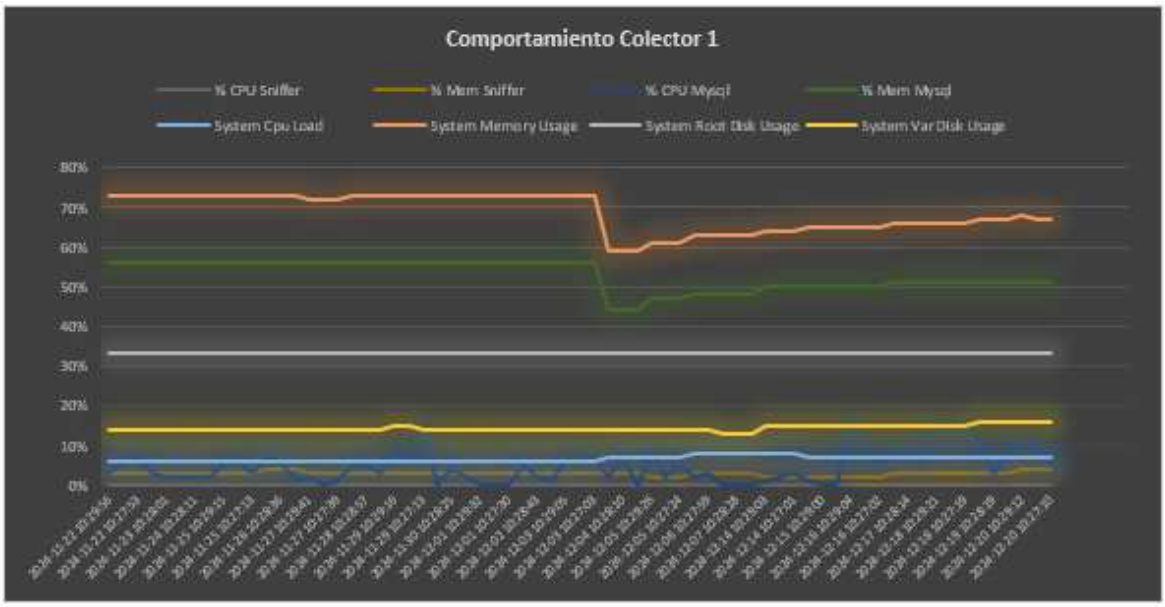
1. Disponibilidad de la plataforma DARKTRACE					
Garantizar la disponibilidad y acceso a los servicios ofrecidos por la plataforma Darktrace					
Disponibilidad del servicio	**ANS Establecido**	**Número de incumplimientos**	**Compensación**	**Valor a Descontar**	**Observación**
99,80% de disponibilidad.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

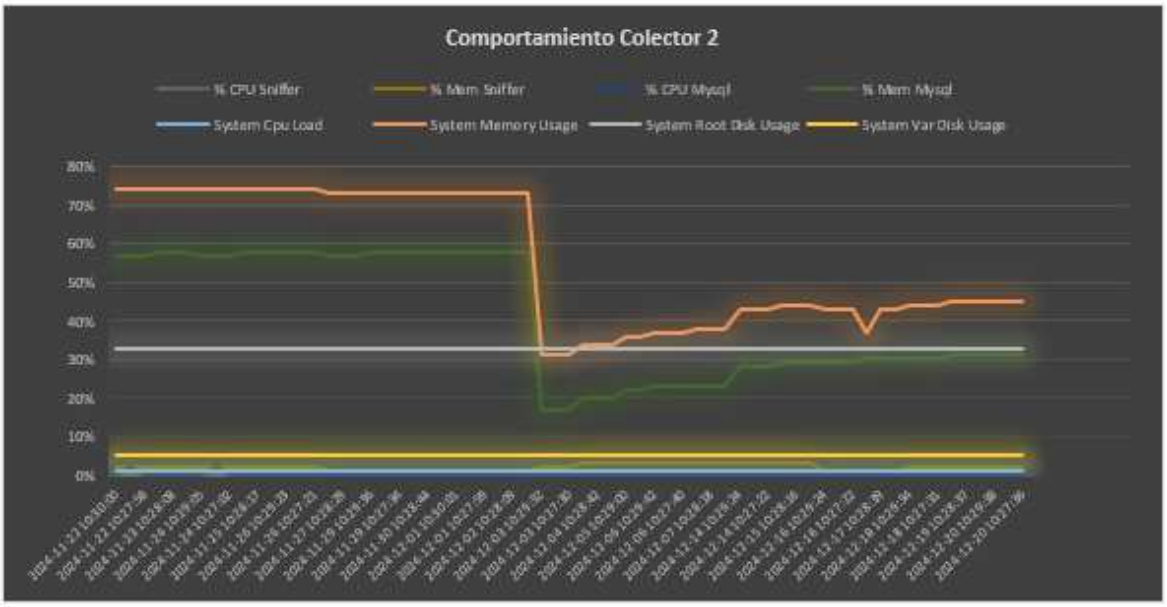


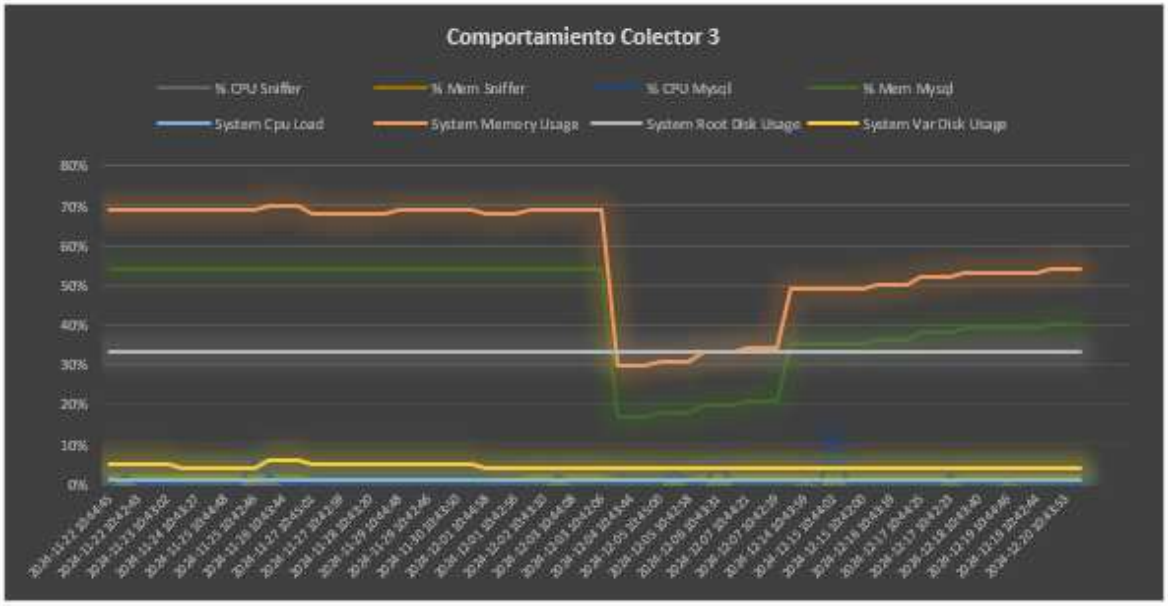
2.5.2. Disponibilidad solución DAM

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


Comportamiento Agregador
% CPU Sniffer
% Mem Sniffer
% CPU Mysql
% Mem Mysql
System Cpu Load
System Memory Usage
System Root Disk Usage
System Var Disk Usage
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

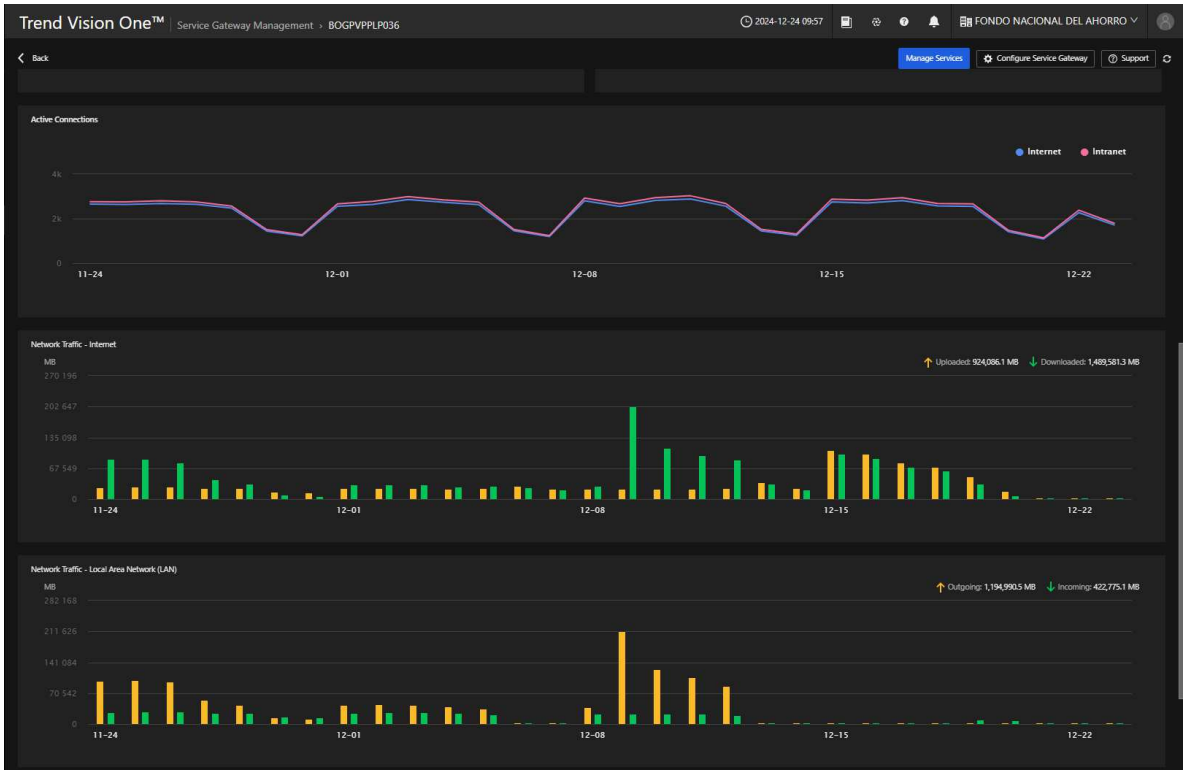

Comportamiento Colector 1
% CPU Sniffer
% Mem Sniffer
% CPU Mysql
% Mem Mysql
System Cpu Load
System Memory Usage
System Root Disk Usage
System Var Disk Usage
80%
70%
60%
50%
40%
30%
20%
10%
0%



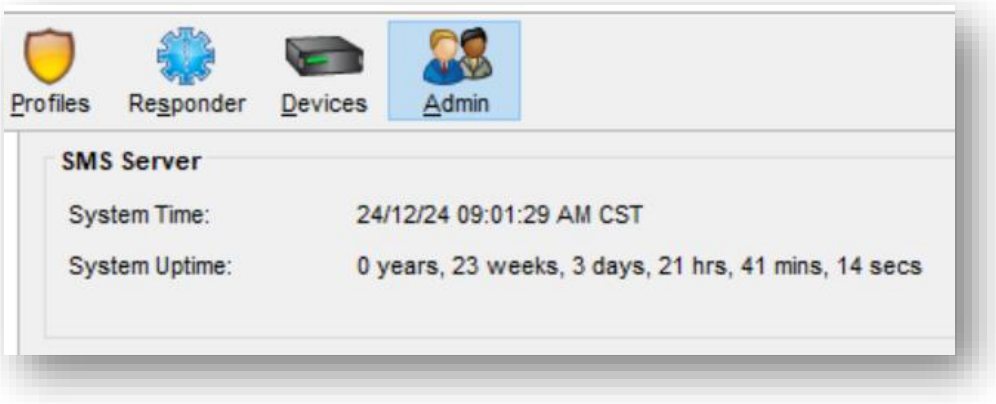


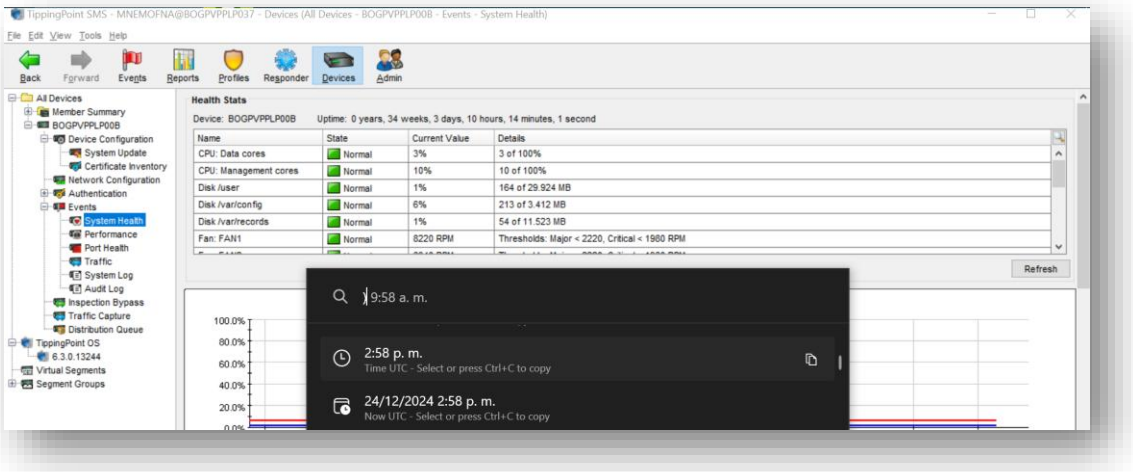
2.5.3. Disponibilidad solución Antimalware

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



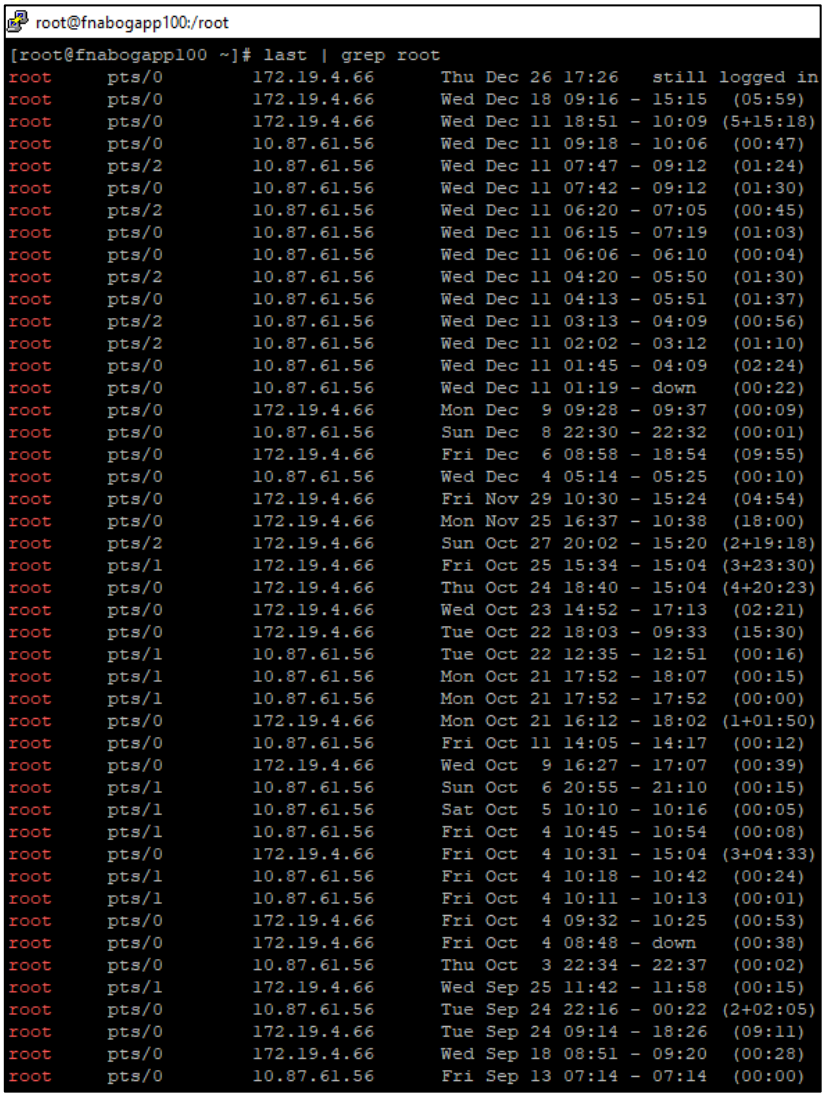
1. *Imagen de conexiones durante el periodo.*





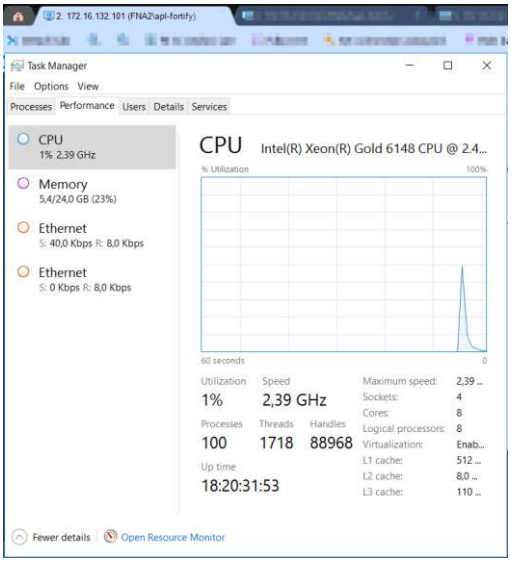
2.5.4. Disponibilidad Plataformas de Correlación SIEM

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

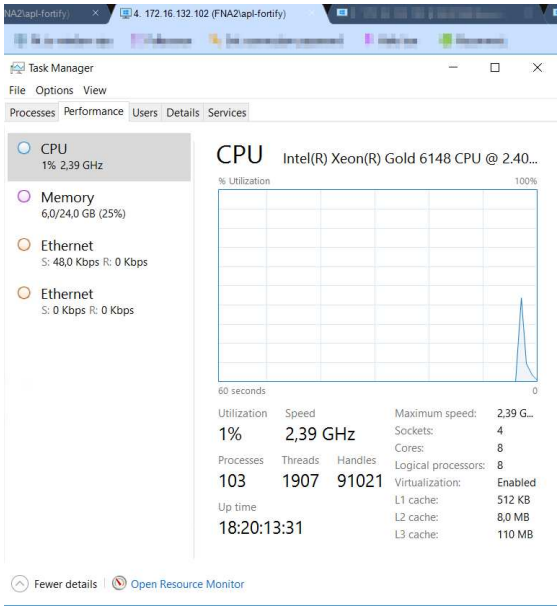


2.5.5. Disponibilidad Secure Development Assesment (Fortify)

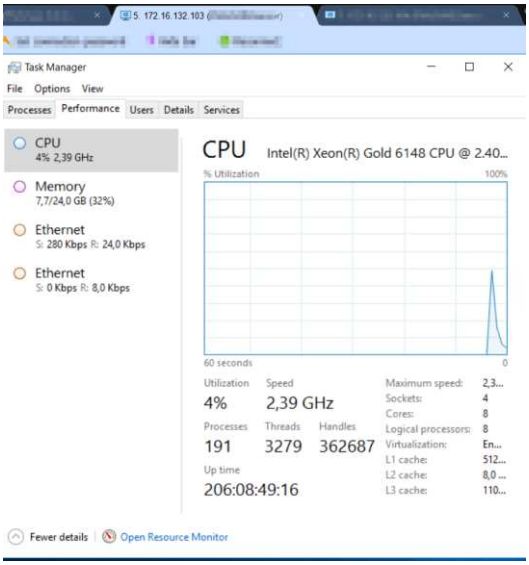
Fortify – 172.16.132.101



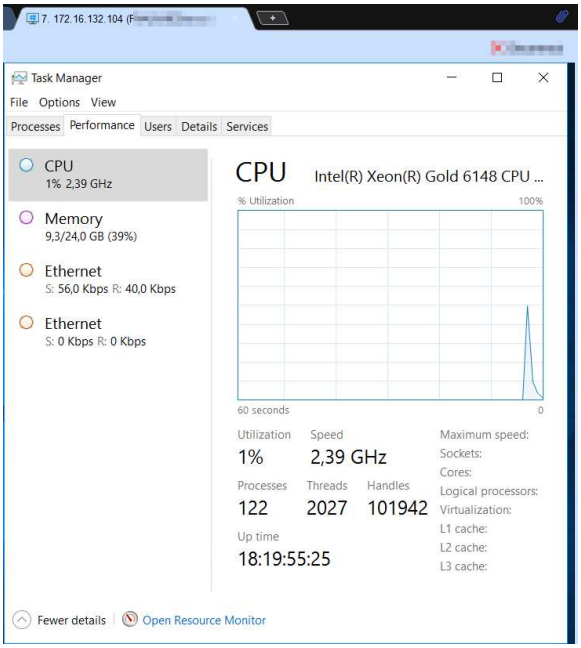
Fortify – 172.16.132.102



Fortify – 172.16.132.103

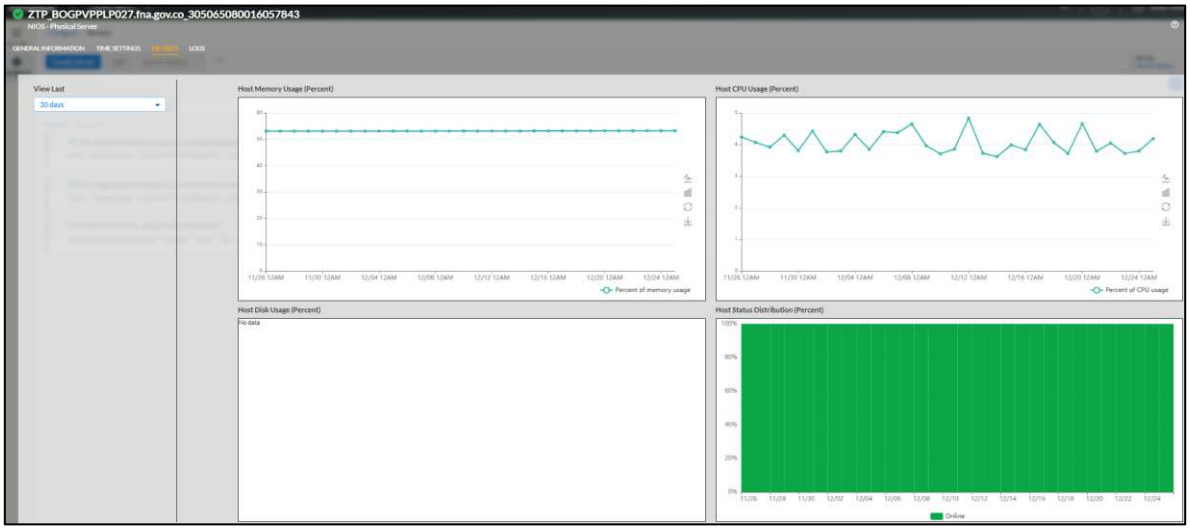


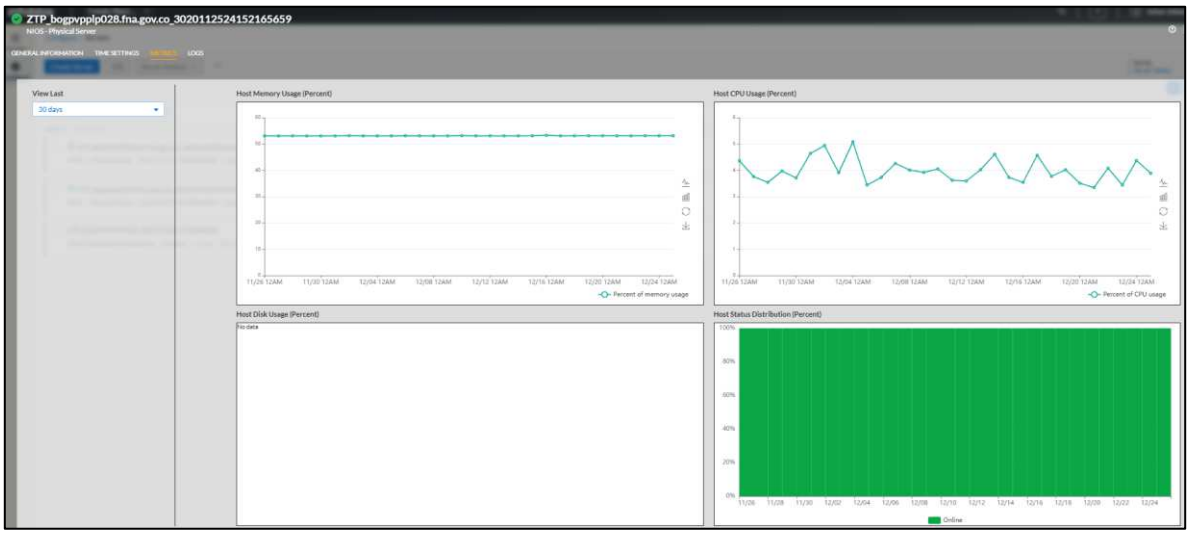
Fortify – 172.16.132.104

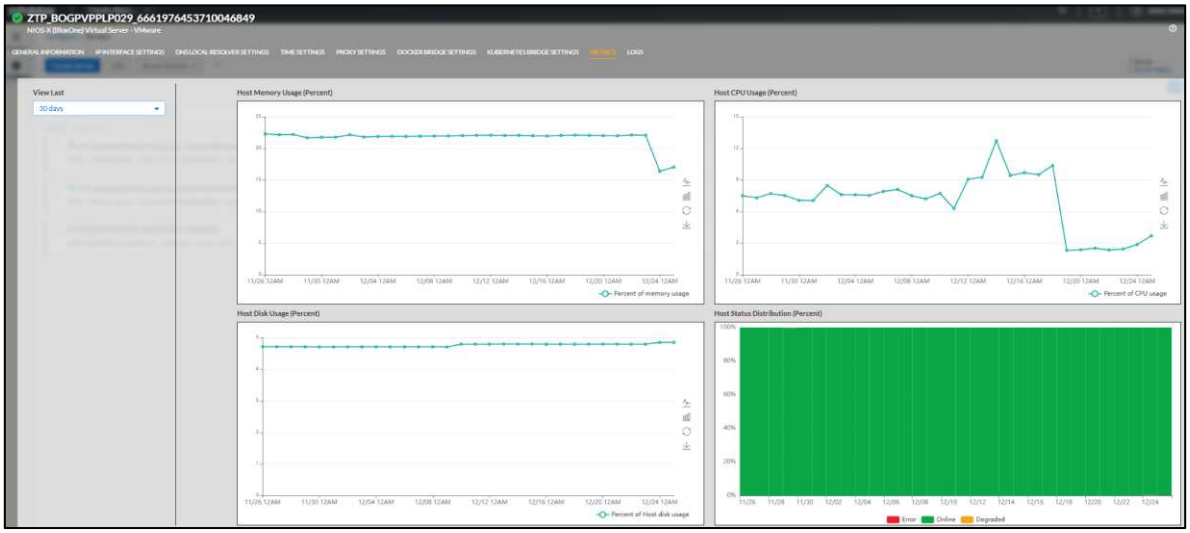


2.5.6. Disponibilidad monitoreo especiales DNS


ZTP_BOGPVPPLP027.fna.gov.co_3050650800160...
Online
NIOS | Physical Server | 8.6.4-51177-72c485de7d02 | License UID: f44dc3a938be4914821734d01adcdafb
ZTP_bogpvpplp028.fna.gov.co_302011252415216...
Online
NIOS | Physical Server | 8.6.4-51177-72c485de7d02 | License UID: 3c1e361631384fdf9a58f448f6fc07e5
ZTP_BOGPVPPLP029_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

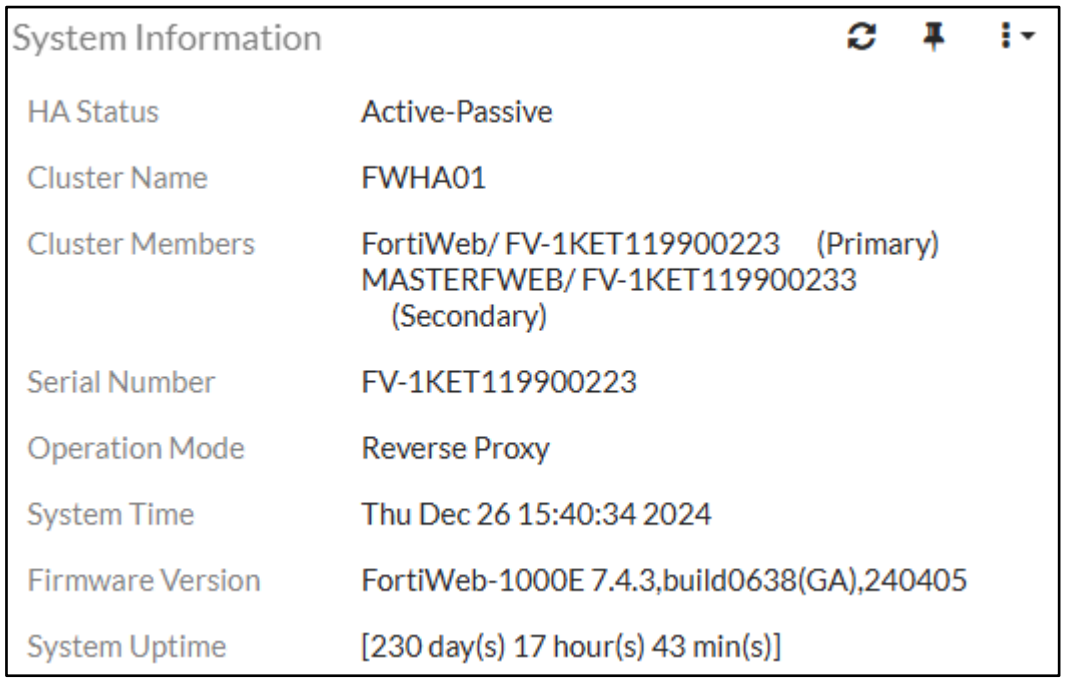

ZTP_BOGPVPPLP027.fna.gov.co_305065080016057843
Host Memory Usage (Percent)
Host CPU Usage (Percent)
Host Disk Usage (Percent)
Host Status Distribution (Percent)


ZTP_bogpvpplp028.fna.gov.co_302011252415216559
Host Memory Usage (Percent)
Host CPU Usage (Percent)
Host Disk Usage (Percent)
Host Status Distribution (Percent)



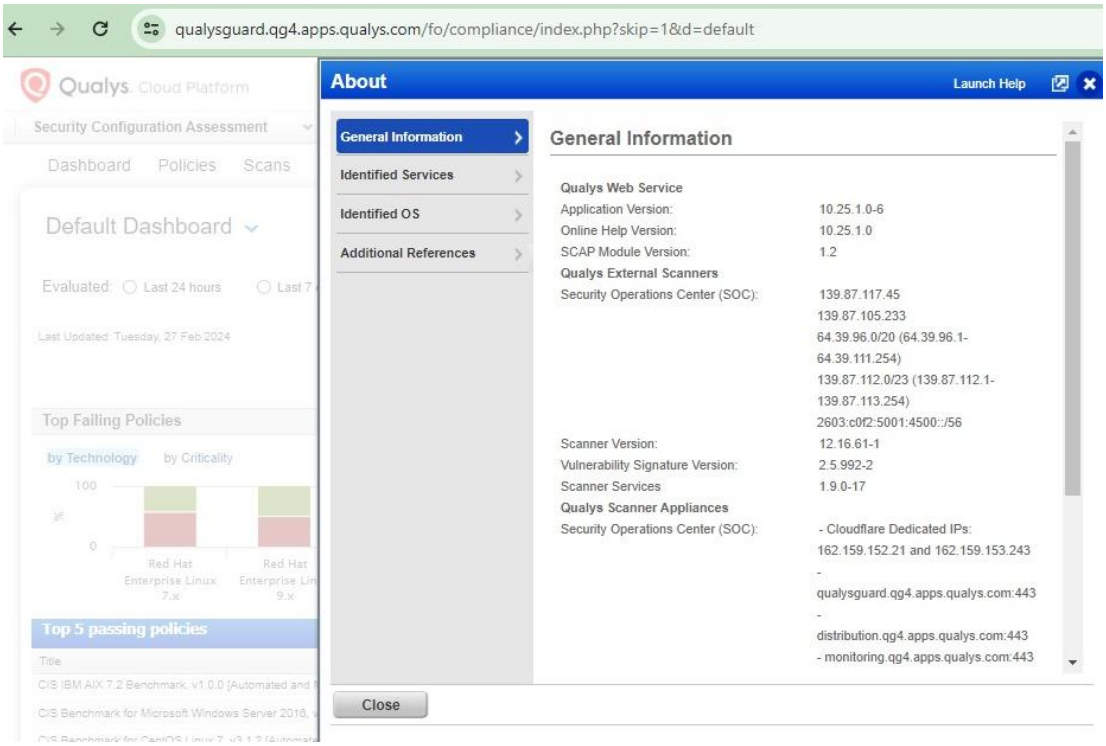
2.5.7. Disponibilidad monitoreo especiales Portales Web

Unit	Status	HA Role	Up Time	CPU Usage	Memory Usage	Log Disk Usage	HTTP Connections	HTTP Throughput
FV-1KET119900223		PRIMARY	230 days 17 hours 46 minutes	1%	30%	79%	Total Connections: 1840 Total Connections/Sec: 20	Throughput: 49.671 Mbps
FV-1KET119900233		SECONDARY	230 days 17 hours 47 minutes	1%	40%	79%	Total Connections: 0 Total Connections/Sec: 0	Throughput: 0.000 Kbps



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



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**

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 iran 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.

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.

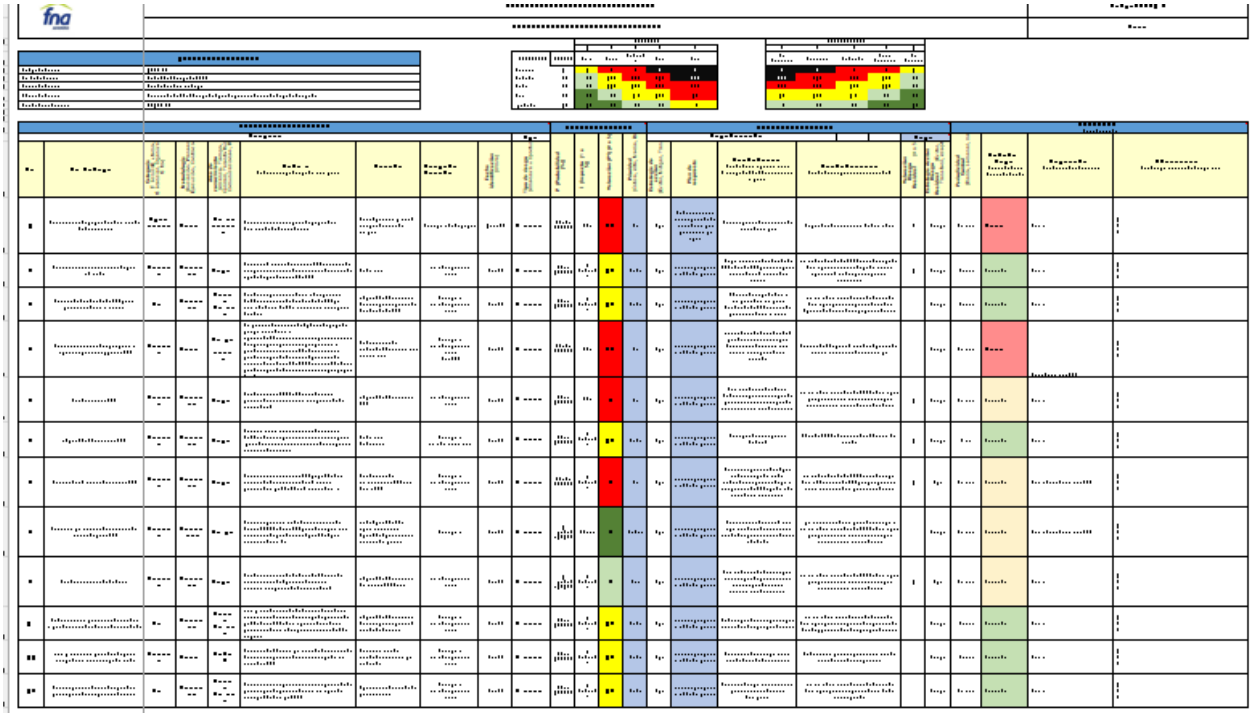
3.9. Análisis comportamiento usuarios.

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.



5. Informe de ejecución presupuestal

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor inicial del contrato	$ 36.499.583.610	100,00%
Adiciones	$ -	0,00%
VALOR TOTAL DEL CONTRATO	**$ 36.499.583.610**	**100,00%**
Valor Ejecutado antes del presente pago	$ 26.747.647.844	73,28%
Valor del pago aprobado con el presente informe	$ 269.280.340	0,74%
VALOR TOTAL EJECUTADO	**$ 27.016.928.184**	**74,02%**
Descuento por ANS	$ -	
DIFERENCIA EN LA EJECUCIÓN PRESUPUESTAL DEL CONTRATO	**$ -**	

6. Determinación del valor a facturar

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	$ 3.326.000	$ -	$ 3.326.000	$ 631.940	$ 3.957.940
Administración y soporte de la plataforma SOAR	$ 14.627.000	$ -	$ 14.627.000	$ 2.779.130	$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	$ 27.797.000	$ -	$ 27.797.000	$ 5.281.430	$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	$ 55.994.000	$ -	$ 55.994.000	$ 10.638.860	$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	$ 52.083.000	$ -	$ 52.083.000	$ 9.895.770	$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	$ 8.279.000	$ -	$ 8.279.000	$ 1.573.010	$ 9.852.010

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma CIBERDEFENSA	$ 5.874.000	$ -	$ 5.874.000	$ 1.116.060	$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	$ 8.406.000	$ -	$ 8.406.000	$ 1.597.140	$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	$ 23.451.000	$ -	$ 23.451.000	$ 4.455.690	$ 27.906.690
Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (IAM)	$ 26.449.000	$ -	$ 26.449.000	$ 5.025.310	$ 31.474.310
Valor Total	**$ 226.286.000**	**$ -**	**$ 226.286.000**	**$ 42.994.340**	**$ 269.280.340**

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

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

SUPERVISIÓN AL CONTRATO No. 173 de 2023
FONDO NACIONAL DEL AHORRO
Informe No. 25

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 noviembre de 2024 al 21 de diciembre de 2024.

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

Bogotá, D.C. enero 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 noviembre de 2024 al 21 de diciembre de 2024** referente al **12vo** 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)

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

Informe de gestión por cada una de las soluciones objeto del contrato SOC, SIEM y SOAR anexo “08. Informe-FNA-173-Diciembre-2024 v2, 149 folios”, están estipulados los parámetros más importantes asociados al servicio de monitoreo y servicio de correlación, así como las configuraciones realizadas sobre la plataforma de correlación por parte del equipo de SOC-CERT de Mnemo Colombia S.A.S., para el Fondo Nacional del ahorro.

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

1. XDR / ANTIMALWARE

- CASB, exclusión de dominio de Camacol de correos entrantes ya que se bloqueaba como SPAM.
- IPS, Antivirus, se asiste a las sesiones de auditorías de las soluciones de Trend Micro, dentro de la de Antivirus se encuentra algunos dispositivos que no tiene agente instalado, por lo que se hace seguimiento con mesa
- protección correo, Activación en modo de prueba del módulo de protección BEC, se envía información a seguridad de la información acerca de las alertas generadas.
- Se crea cambio para la solicitud de permisos, para la conexión de DDAN y V1, además de ZTNA Internet Access para su funcionamiento del módulo.
- IPS, validación de indicador de alerta en el servidor, se desactivan filtros que no hacen ningún match y que generan alto consumo de CPU, además se apagan las interfaces sin uso.

- Se evidencian un total de 1161 eventos de amenazas gestionados por Trend Micro, en su mayoría es por la detección por la regla Possible_Hifrm-6, se requiere validar los eventos para comprobar si son necesario excluirlos o son válidos.
- Se encontró el archivo Agent Dexon 5.1.3.222.exe, se requiere realizar seguimiento sobre el reporte del ejecutable en el dispositivo VGA-TCC-03-2331.
- Behavior Monitoring, se detectaron por este módulo el archivo TRAMITES.exe y Ahorro.exe estos se detectaron como archivos nuevos.
- Application Control, se encontró la ejecución de la aplicación Conda.exe, encontrada dentro de la lista de aplicaciones bloqueadas.
- El módulo de Device control, bloquea el uso no autorizado de dispositivos extraíbles, el usuario que mayor cantidad de eventos registra es aeguerrero con 16 registros.
- En el tipo de dispositivos que mayor cantidad de eventos registra, son dispositivos móviles.
- Dentro de las alertas más relevantes se encuentran las siguientes técnicas utilizadas, en las diferentes detecciones.
- Análisis inicial de compromiso: Técnicas relacionadas con phishing, archivos maliciosos y bypass de controles (e.g., MITRE.T1204.002, MITRE.T1548.002).
- Detección de persistencia y evasión: Abuso de DLL, herramientas legítimas, y manipulación de configuraciones (e.g., MITRE.T1574.001, XSAE.F3256).
- Movimiento lateral y exfiltración: Protocolo SMB y transferencias de archivos (e.g., MITRE.T1021.002, MITRE.T1105).
- XDR, En el top de eventos por nombre de acuerdo con el nombre de los archivos ejecutados, está el uso de la herramienta QuickAssist, para conexión remota, también el uso de MMC para administración de usuarios y la ejecución de Windows Powershell para desactivación de Windows Defender.
- administrativas, se recomienda el no uso del comando por borrado completo de información y no recomendado en entornos virtuales.
- 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.
- Domain Trust Discovery, está vinculado al intento de descubrimiento de relaciones de relaciones de confianza del dominio, este evento se genera por el despliegue de la herramienta Intune, de forma valida.

- El ultimo evento corresponde al acceso de la URL https://fulzzar[.]blogspot[.]com/favicon.ico, como pruebas realizadas por parte del administrador de DarkTrace.
- Se registran 4 eventos en el servidor FNABOGAPP015, por la regla de detección objetos embebidos en archivos. En específico, por el archivo 52 Informe de selecciÃ³n 023.pdf
- El módulo de Firewall de hosts ha sido activado en servidores, esto inicialmente en modo observación. De acuerdo a este módulo se generaron 3820 eventos, El evento que mayor cantidad de registros género es Retransmit, Ya se encuentra la mayoría de las reglas activas en modo bloqueo.
- 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.
- La mayoría de los eventos 3800 fueron bloqueados o denegados, los otros 20 fueron de auditoría.
- Los eventos que mayor cantidad de eventos registraron fueron los relacionados con los servicios de DNS y LDAP.
- El módulo de IPS de host en servidores se encuentra activo con el fin de identificar tráfico con comportamiento malicioso y vulnerabilidades de cara a la red. En el top de eventos se encuentra la regla: "Invalid Compression Denial of Service"
- 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, se requiere validar los servidores con las alertas.
- Inteligencia de amenazas se adicionan 93 reputaciones nuevas adicionadas por la integración con Threat Q, correspondientes a correos electrónicos y direcciones IP.
- Attack Surface Discovery, En el top de eventos, se registra los servidores bogpvpplp022, bogpvpplp015 y bogpvpplp019, con 86 vulnerabilidades y fallos en la configuración, con clasificación alta, es necesario mitigar las vulnerabilidades encontradas.
- Attack Surface Discovery, no se observa ninguna clasificación alta, la página con clasificación más alta es agendamiento.fna.gov.co.
- Para la cuenta de vigildap tiene la mayor clasificación, se clasifica con riesgo alto, porque tiene bastantes permisos sobre la cuenta y porque tiene deshabilitada la opción de que la contraseña expire, entre otras vulnerabilidades.

- Attack Surface Discovery, la aplicación anyrun con clasificación media es la que mayor cantidad de visitas tiene.
- Attack Surface Discovery, en 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.
- IPS, Del total de los 139716 eventos, en su mayoría con clasificación major con el 58 % de los eventos.
- 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.
- IPS, el top de IP de origen 185.243.5.55 de Polonia con 23633 eventos.
- IPS, el top de destino se encuentra la dirección IP 172.16.125.33, con 9161 registros.
- IPS, En el top de eventos por país, se encuentra Estados unidos con mayor cantidad de registros, seguido de Hong Kong y Romania.
- CASB, se presentaron un total de 76942 eventos registrados por la solución CASB, 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 anomalías.
- CASB, En los eventos por nombre de anomalía, se encuentran correos con rutas compartidas, correos de marketing y correos relacionados con el malware Bazar.
- CASB, La cuenta que mayor cantidad de detecciones presenta es logistica@sumicorp.com y mailer-daemon@googlemail.com.
- CASB, En el top de correos remitentes de phishing esta la cuenta alertasynotificaciones[@]notificacionesbancolombia[.]com y dianisjulieth[.]07@hotmail.com.
- se relaciona el informe de 2190 dispositivos instalados en el periodo que comprende el periodo de 22 de noviembre al 21 de diciembre del 2024.

2. THREAT INTELLIGENCE

Actividades de Gestión de la plataforma

- Se generaron 48 alertas y eventos en MISP.
- De las 48 alertas se han compartido un total de 51.676 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 34 actores de amenazas identificados.
- Fueron generadas 7 alertas que contienen información sobre vulnerabilidades que pueden afectar la infraestructura de la compañía.
- Las alertas tempranas se han compartido junto a la solución o mitigación brindada por el fabricante responsable de publicar las actualizaciones de los productos afectados.
- Se realizaron ajustes en las fuentes de datos de Threat Intelligence que funcionan como ingestores de indicadores de compromiso en la plataforma TIP, con el fin de mejorar tanto la confiabilidad y utilidad de la información recopilada como la actualización de los indicadores obtenidos.
- Se ajusta la priorización y enriquecimiento de los indicadores de compromiso que son ingestados por la plataforma de inteligencia de amenazas.

Threat Hunting

- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se crearon 2 reglas Sigma en la que se identifican comportamientos de ejecución de la amenaza Loki Locker ransomware.
- Las reglas SIGMA identifican la des habilitación del firewall y el administrador de tareas de windows.
- Se realizaron análisis focalizados sobre las amenazas Lumma Stealer y Trinity Ransomware, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.
- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 120 análisis de muestras sospechosas.
- Utilizando herramientas de Threat Hunting, el equipo ha recopilado muestras de diversas fuentes, teniendo en cuenta las tendencias de ataques en la región.
- Análisis de muestras aportadas por el equipo de monitoreo de herramientas de FNA.
- Identificación de las tácticas, técnicas y procedimientos utilizados por los actores de amenazas a través de cada una de las muestras recolectadas, obteniendo así las tendencias de ataque perpetrado por los cibercriminales.
- Los indicadores de compromiso se tienen en cuenta para ser agregados a eventos en la herramienta de MISP así como a la herramienta de Threat Intelligence Platform TIP donde se enriquecen los indicadores con información como actores de amenaza, familias de malware, tácticas y técnicas de la matriz de Mitre ATT&CK. Por consiguiente, los indicadores son agregados a las herramientas de seguridad del cliente.

3. BRAND CYBERSECURITY MONITORING

Actividades de Gestión de la plataforma de monitoreo de marca

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

4. SECURE DEVELOPMENT ASSESSMENT

Actividades de Gestión de la plataforma Fortify

- 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.
- Durante el período comprendido, la suite Fortify ha operado de manera estable y sin interrupciones, sin registrar caídas ni fallas. El mantenimiento y las actualizaciones se han gestionado de forma constante, lo que ha garantizado la disponibilidad continua de la herramienta y su rendimiento óptimo en todo momento, asegurando que esté siempre lista para su uso cuando se necesite.

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.
- Se identifica que el volumen de consultas a portales de pornografía aumentó en la resolución de DNS.
- Para el periodo en mención se evidenció un aumento de 224 eventos en la categoría de DoHservice en las consultas DNS, para la categoría malware download generic se evidenció una disminución de 2,546 siendo las categorías con más consultas dentro del DNS.

6. MONITOREO DE LINEAS BASE DE SEGURIDAD

Actividades de Gestión de la plataforma QUALYS

- 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)
- Todos los meses se encuentran en promedio 5 servidores que son dados de baja, en caso de que estos lleguen a ser reemplazados, es importante realizar la notificación vía electrónica para realizar su adición a través del proceso de instalación de agente en estos dispositivos o servidores nuevos.
- El 20 de agosto los servidores el grupo de servidores Windows 2008 R2 (BOGPVPPWP023, FNABOGAPP001, FNABOGDCL01N6, FNABOGDPCL01N1) dejó de transmitir información a la nube a través del Gateway, después de múltiples reuniones de acompañamiento se pudo determinar que el error es debido a la ausencia de confianza de los servidores en el Gateway, ya sea porque este no ofrece un certificado para cifrar la comunicación o el certificado ofrecido no es confiable para los servidores, para mitigar este inconveniente se realizó la instalación del certificado del QCG de forma local en el OS de estos mismos servidores, a pesar de esto dichos servidores siguen sin transmitir.

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 realiza validación de los correos recibidos de la cuenta notaria2barranquilla@hotmail.com para facturacionelectronica@fna.gov.co, NO se evidencian correos
- Se genera reporte al área de seguridad informática para la validación de 382 correos del remitente coordinadorabso@serviasesorias.com.co
- Se crea modelo "FNA - Service Gateway Vigilancia puerto 80" para la vigilancia de las conexiones externas del equipo con direccion IP 172.16.125.250 (Service Gateway Trend Micro)
- Se envía listado de equipos con Agente de Darktrace instalado por Incidente IM157726 Generado por lentitud de la red
- Se realiza acompañamiento y validación de eventos para actividad de "Simulación ejercicio Ciberseguridad ante posibles amenazas digitales"
- Se genera reporte al área de seguridad de la información para la validación de los correos del dominio comunicados@fnaqov.co
- 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

- Solicitud información planes SAP HANA/COBIS.
- Seguimiento a política COBIS.
- Múltiples eventos base de datos COBIS. Relay correo.
- Despliegue parches seguridad.
- Corrección certificados próximos vencer.
- En comparación con el periodo pasado, la regla para **XSS** aumentó un aproximado de 3 veces su valor. Para la regla **Data Exfiltration**, el aumento fue de 1.5 veces con el valor anterior, para las regla de **OS Command Injection** se duplicó, y para **SQL Injection - Tautology,** aumentaron un aproximado de 4 veces.

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 continúa 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 después del paso a producción.
- Se programan reuniones técnicas con los equipos de Vigía y E-Finac para validación técnica de integración con Verify.
- Se sigue con las pruebas para salida a producción de la integración con Cobis.
- Se siguen realizando las gestiones correspondientes con las áreas involucradas para el proceso de integración hacia Verify con las demás aplicaciones.

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	$ 26.354.918.094,00	**46,71%**
Valor del pago aprobado con el presente informe	$ 269.280.340,00	**0,48%**
VALOR TOTAL EJECUTADO	**$ 26.624.198.434,00**	**47,19%**
Porcentaje de ejecución presupuestal programado a la fecha		**47,23%**
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 noviembre de 2024 al 21 de diciembre de 2024.**

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

Porcentaje de ejecución proyectado	**59%**
Porcentaje de ejecución realizado	**59%**
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	**0%**

% completado	% completado	Nombre de tarea	Duración	Comienzo	Fin
59%	59%	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
59%	59%	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
45%	45%	Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25
46%	44%	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 periodica del nivel de madurez (monitoreo y mejora continua)	366 días	lun 22/07/24	mar 9/12/25
100%	100%	Adquisición de herramientas tecnológicas	6 días	vie 22/12/23	lun 1/01/24
100%	100%	Despliegue de herramientas tecnológicas	162 días	vie 22/12/23	jue 1/08/24
100%	100%	Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24
49%	49%	Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26
47%	47%	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.

6.1 Valor a Facturar de Conformidad a Oferta Económica

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	$ 3.326.000	$ -	$ 3.326.000	$ 631.940	$ 3.957.940
Administración y soporte de la plataforma SOAR	$ 14.627.000	$ -	$ 14.627.000	$ 2.779.130	$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	$ 27.797.000	$ -	$ 27.797.000	$ 5.281.430	$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	$ 55.994.000	$ -	$ 55.994.000	$ 10.638.860	$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	$ 52.083.000	$ -	$ 52.083.000	$ 9.895.770	$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	$ 8.279.000	$ -	$ 8.279.000	$ 1.573.010	$ 9.852.010
Administración y soporte de la plataforma CIBERDEFENSA	$ 5.874.000	$ -	$ 5.874.000	$ 1.116.060	$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	$ 8.406.000	$ -	$ 8.406.000	$ 1.597.140	$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	$ 23.451.000	$ -	$ 23.451.000	$ 4.455.690	$ 27.906.690
Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (IAM)	$ 26.449.000	$ -	$ 26.449.000	$ 5.025.310	$ 31.474.310
Valor Total	$ 226.286.000	$ -	$ 226.286.000	$ 42.994.340	$ 269.280.340

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	Acta revisión ANS	Bueno	20/01/2024	Ninguna
2	Informe-FNA-173-diciembre-2024.pdf	Bueno	28/12/2024	Ninguna
3	Acta Seguimiento Mensual Proyecto	Bueno	31/01/2024	Ninguna

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

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

8. CONCLUSIÓN

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de **DOCIENTOS SESENTA Y NUEVE MILLONES DOSCIENTOS OCHENTA MIL TRESCIENTOS CUARENTA PESOS MCTE ($ 269.280.340).**

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

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

Se firma a los 31 días del mes de enero de 2025.

Mónica Grand Villada

Firmado digitalmente por Mónica Grand Villada
Fecha: 2025.02.24 14:13:37 -05'00'

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

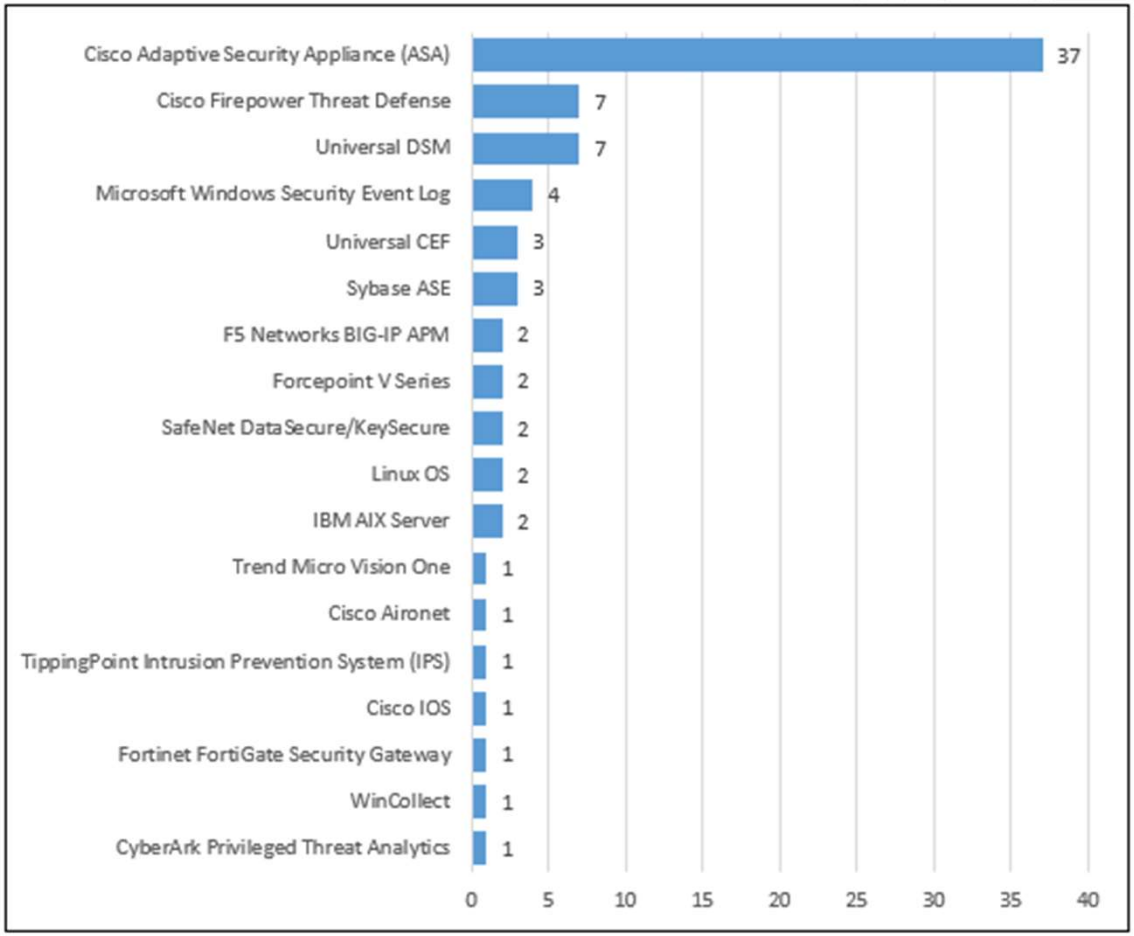
ENRIQUE A. ARRAZOLA MONTES
Profesional 03
Apoyo supervisión CTO 173 de 2023

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

VALIDACIÓN DE FUENTES

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

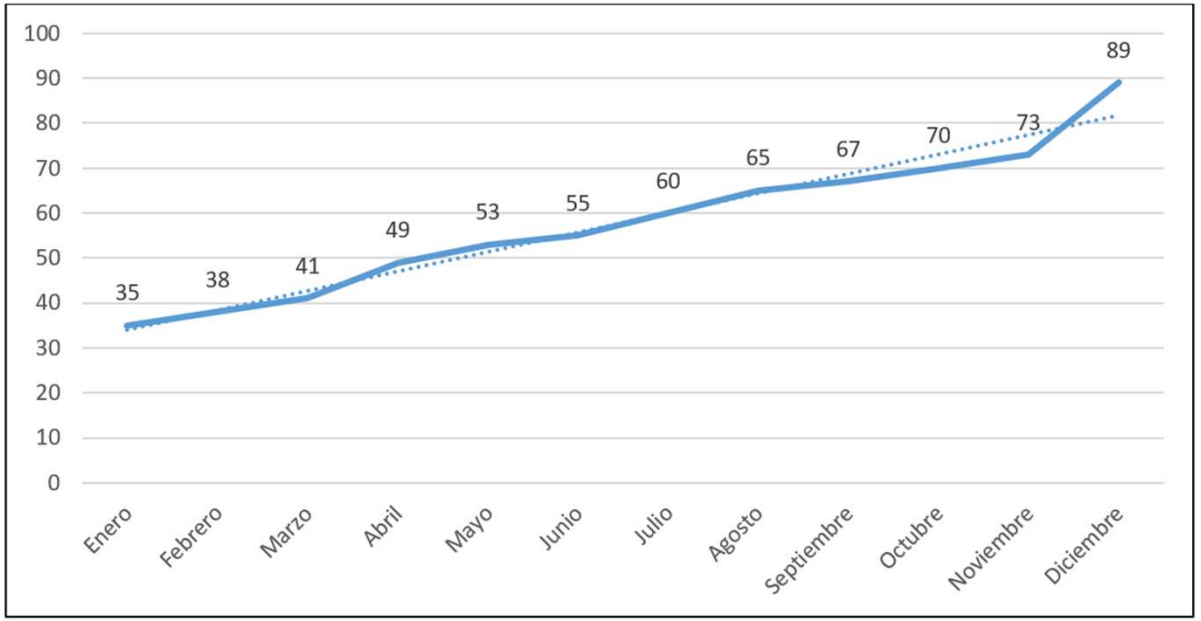
ID	Name	Enabled	Log Source Type	Creation Date
562	Aironet @ 10.200.51.121	Yes	Cisco Aironet	May 21, 2024 4:48 PM (CST)
524	ASA @ 192.168.13.130	Yes	Cisco Adaptive Security Appliance (ASA)	May 6, 2024 8:49 AM (CST)
233	ASA @ 192.168.16.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 20, 2024 11:06 PM (CST)
265	ASA @ 192.168.20.130	Yes	Cisco Adaptive Security Appliance (ASA)	Apr 2, 2024 11:30 AM (CST)
241	ASA @ 192.168.29.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 20, 2024 11:06 PM (CST)
526	ASA @ 192.168.31.130	Yes	Cisco Adaptive Security Appliance (ASA)	May 6, 2024 9:09 AM (CST)
254	ASA @ 192.168.33.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 20, 2024 11:08 PM (CST)
260	ASA @ 192.168.38.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 21, 2024 8:01 PM (CST)
525	ASA @ 192.168.41.130	Yes	Cisco Adaptive Security Appliance (ASA)	May 6, 2024 9:01 AM (CST)
248	ASA @ 192.168.46.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 20, 2024 11:06 PM (CST)
243	ASA @ 192.168.48.130	Yes	Cisco Adaptive Security Appliance (ASA)	Mar 20, 2024 11:06 PM (CST)
571	CiscoFirepowerThreatDefense @ 172.17.1.250	Yes	Cisco Firepower Threat Defense	Jul 12, 2024 10:37 AM (CST)

CASOS DE USO

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

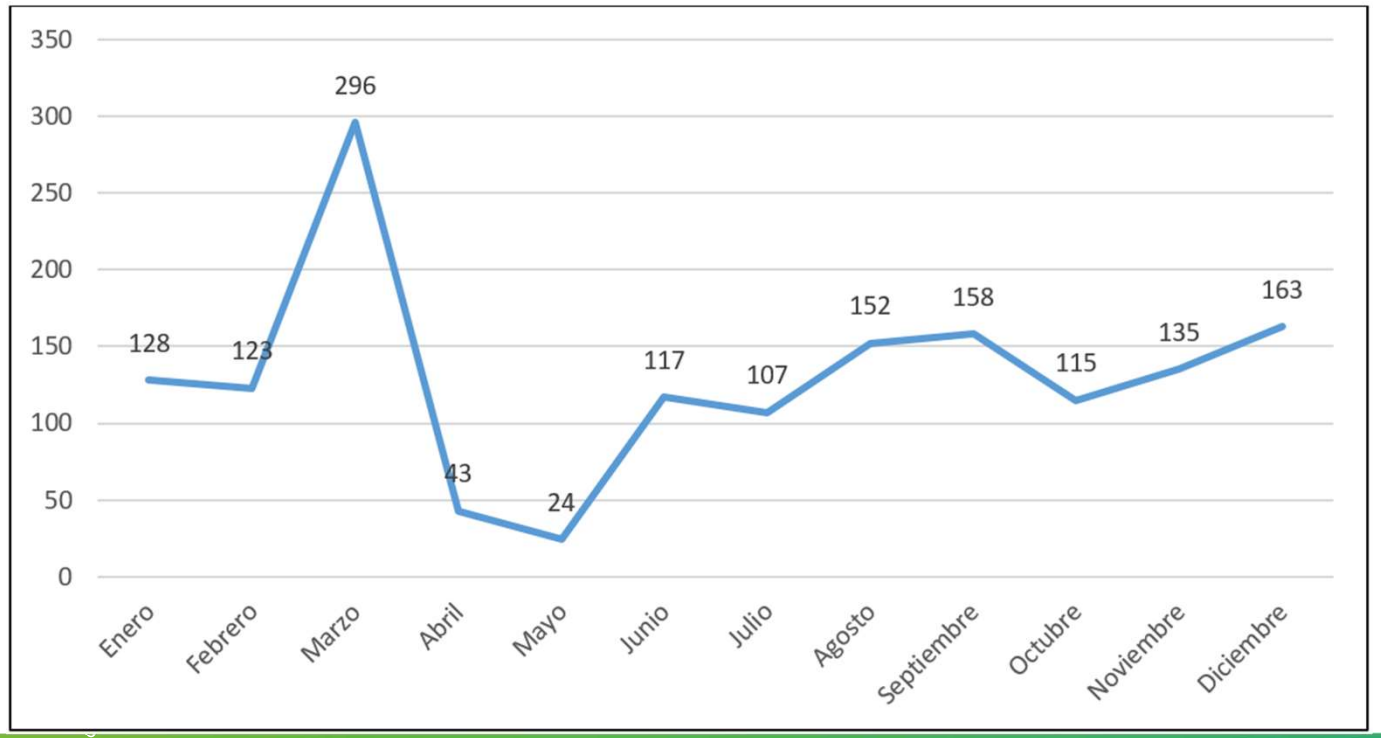
Para este periodo se realizó un incremento de 16 casos de uso

FNA_SAPHANA_Gerencia_SAC_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia_Cartera_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Vicepresidencia_financiera_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia_Cuentas_Personas_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Vicepresidencia_JurÃdica_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia Asesorias Y Conceptos_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia Representacion Judicial_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia Planeacion Financiera_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia de Legalizadora_ Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Secretaria General_Asignacion_Roles_A_Otras_Cuentas
FNA_SAPHANA_Gerencia_SAC_Eliminacion_Roles
FNA_SAPHANA_Gerencia_Cartera_Eliminacion_de_Roles
FNA_SAPHANA_Vicepresidencia_financiera_Eliminacion_de_Roles
FNA_SAPHANA_Gerencia_Cuentas_Personas_Eliminacion_de_Roles
FNA_SAPHANA_Vicepresidencia_Juridica_Eliminacion_de_Roles
FNA_SAPHANA_Gerencia Asesorias Y Conceptos_Eliminacion_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

- **Adición de Campos en COBIS**
  - **Estado Actual:** En seguimiento y validación.
  - **Fecha Clave:** 29 de noviembre.
  - **Actividades Pendientes:**
    1. Validar la correcta adición de los campos requeridos en COBIS.
    2. Realizar pruebas funcionales para verificar que los cambios no afecten otros procesos.
    3. Documentar los resultados de las pruebas y generar un informe final.
- **Prueba de Recorrido en COBIS y SAP**
  - **Estado Actual:** Pendiente de ejecución.
  - **Fecha Clave:** 30 de noviembre.
  - **Actividades Pendientes:**
    1. Coordinar con los equipos responsables de COBIS y SAP para realizar el recorrido.
    2. Validar la interacción entre ambas plataformas durante el recorrido.
    3. Documentar cualquier incidencia encontrada y proponer soluciones.
- **Control de Cambios y Elevación de Permisos en Firewall**
  - **Estado Actual:** Programado.
  - **Fecha Clave:** 6 de diciembre.
  - **Actividades Pendientes:**
    1. Revisar la solicitud de cambios para la elevación de permisos en el firewall.
    2. Coordinar con el equipo de infraestructura para implementar los cambios.
    3. Validar que los permisos otorgados cumplan con las políticas de seguridad establecidas.
- **Modificación de Alertamiento en ASA y AD**
  - **Estado Actual:** Programado.
  - **Fecha Clave:** 9 de diciembre.
  - **Actividades Pendientes:**
    1. Ajustar las alertas configuradas en el ASA para reflejar eventos críticos.
    2. Revisar y modificar alertas en el Directorio Activo para mejorar su precisión.
    3. Realizar pruebas para validar los nuevos ajustes de alertamiento.
- **Creación de Casos de Uso (16 al 20 de diciembre)**

Estado Actual: Casos creados, en seguimiento.

- **Casos Creados:**
  - **Asignación de Roles:**
    - FNA_SAPHANA_Gerencia_SAC_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia_Cartera_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Vicepresidencia_financiera_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia_Cuentas_Personas_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Vicepresidencia_Jurídica_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia Asesorías y Conceptos_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia Representación Judicial_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia Planeación Financiera_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Gerencia de Legalizadora_Asignacion_Roles_A_Otras_Cuentas
    - FNA_SAPHANA_Secretaría General_Asignacion_Roles_A_Otras_Cuentas
  - **Eliminación de Roles:**
    - FNA_SAPHANA_Gerencia_SAC_Eliminacion_Roles
    - FNA_SAPHANA_Gerencia_Cartera_Eliminacion_de_Roles
    - FNA_SAPHANA_Vicepresidencia_financiera_Eliminacion_de_Roles
    - FNA_SAPHANA_Gerencia_Cuentas_Personas_Eliminacion_de_Roles
    - FNA_SAPHANA_Vicepresidencia_Jurídica_Eliminacion_de_Roles
    - FNA_SAPHANA_Gerencia Asesorías y Conceptos_Eliminacion_de_Roles

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.

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

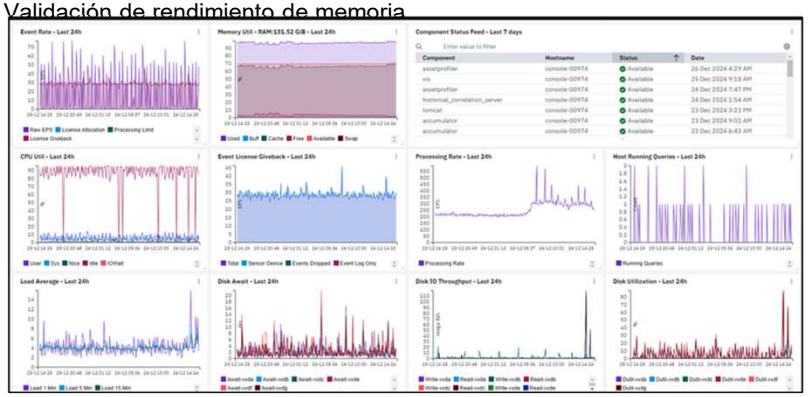
Actualmente se mantienen para TrendMicro 18 playbook los cuales permiten la interacción y ejecución de tareas automatizadas.

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



Seguimiento y estados de los diferentes servicios

Component	Total Outage(min)	Current Status	Last Outage Starttime	Last Outage Duration
assetprofiler	1.00	Available	26 Dec 2024 4:29 AM	1.00
vis	2.00	Available	25 Dec 2024 9:17 AM	2.00
historical_correlation_server	3.00	Available	24 Dec 2024 1:52 AM	3.00
tomcat	2.00	Available	23 Dec 2024 3:22 PM	2.00
accumulator	2.00	Available	23 Dec 2024 9:00 AM	2.00
ecs-ep	2.00	Available	23 Dec 2024 3:52 AM	2.00
ecs-ec	1.00	Available	23 Dec 2024 1:34 AM	1.00
ecs-ec-ingress	3.00	Available	22 Dec 2024 8:12 AM	3.00
offline_forwarder	2.01	Available	21 Dec 2024 2:21 AM	2.01

Disponibilidad:

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

```
root@fnabogapp100:/root
[root@fnabogapp100 ~]# last | grep root
root     pts/0        172.19.4.66      Thu Dec 26 17:26   still logged in
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)
```

48
Alertas Preventivas

7
Alertas Tempranas

51.676
IoC reportados

105
Amenazas reportadas

34
Actores de amenazas identificados

Informe CTI

2024

Objetivo

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

Objetivos específicos

- Resumen de investigaciones realizadas.
- Resumen de actividades.

Alcance

Los temas a tratar sobre este informe son:

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

Resumen de investigaciones

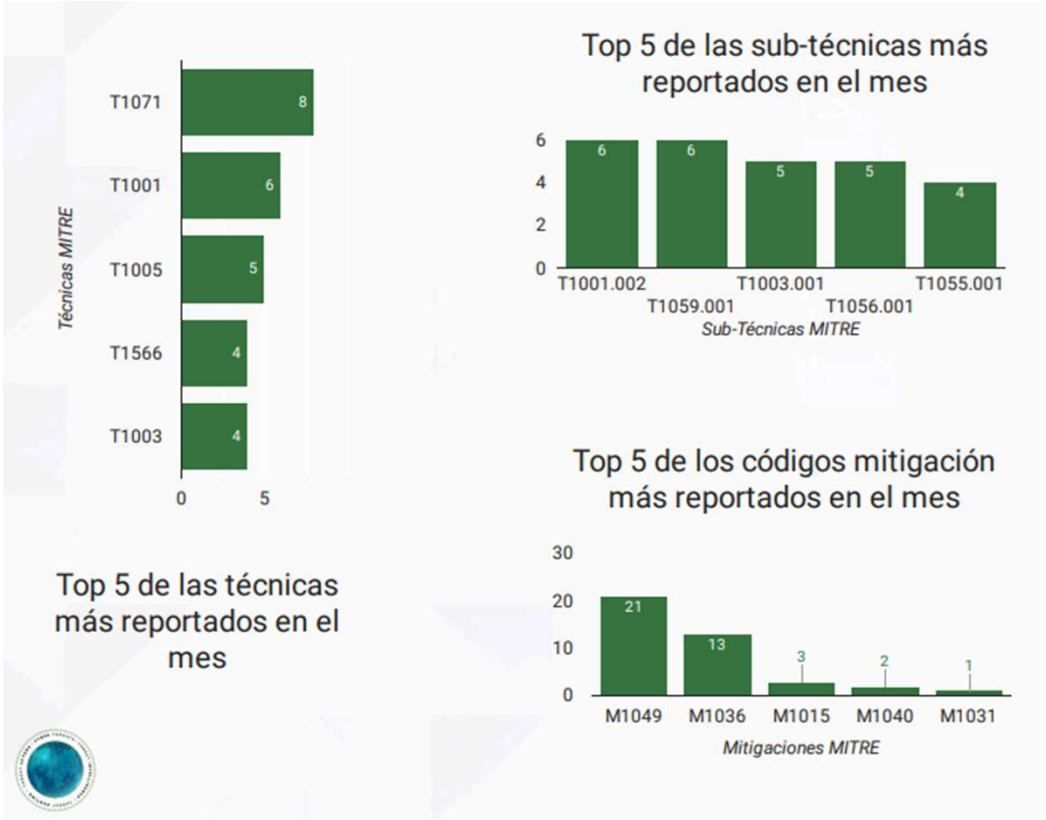
En el periodo evaluado se realizaron un total de 48 investigaciones, cada una de ellas se convirtió en una **alerta preventiva** que fue compartida vía correo electrónico y eventos en MISP.





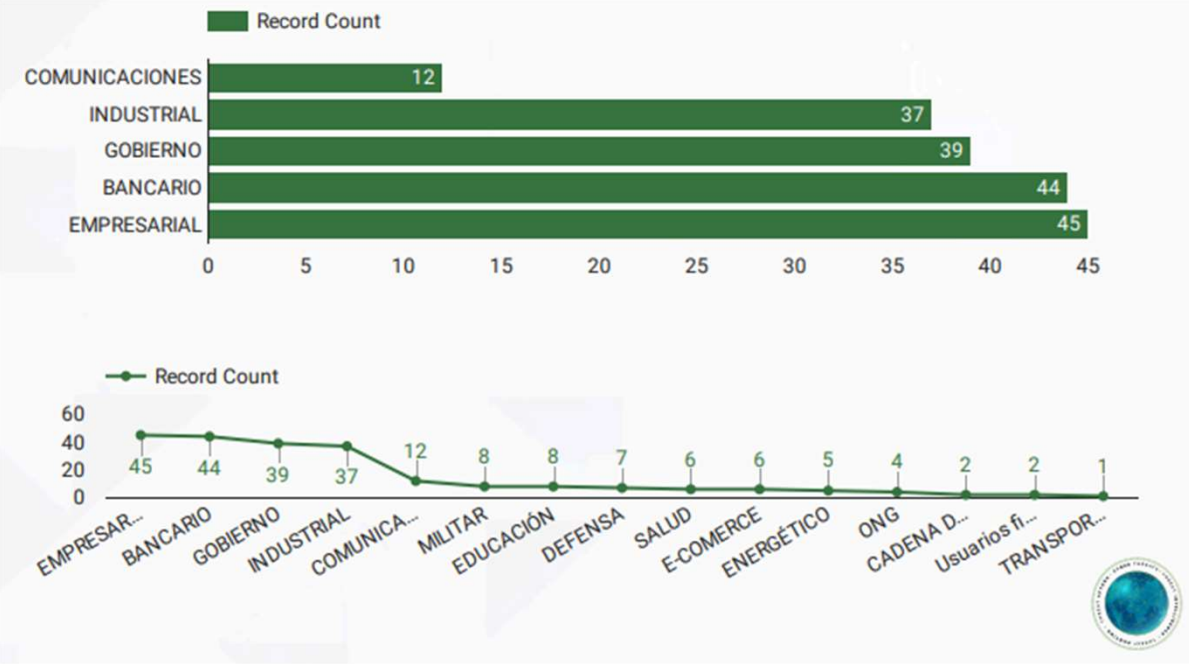
En el periodo evaluado se generaron 7 **alertas tempranas,** cada una de ellas fue compartida vía correo electrónico.

Mitre Att&CK en la investigación de CTI



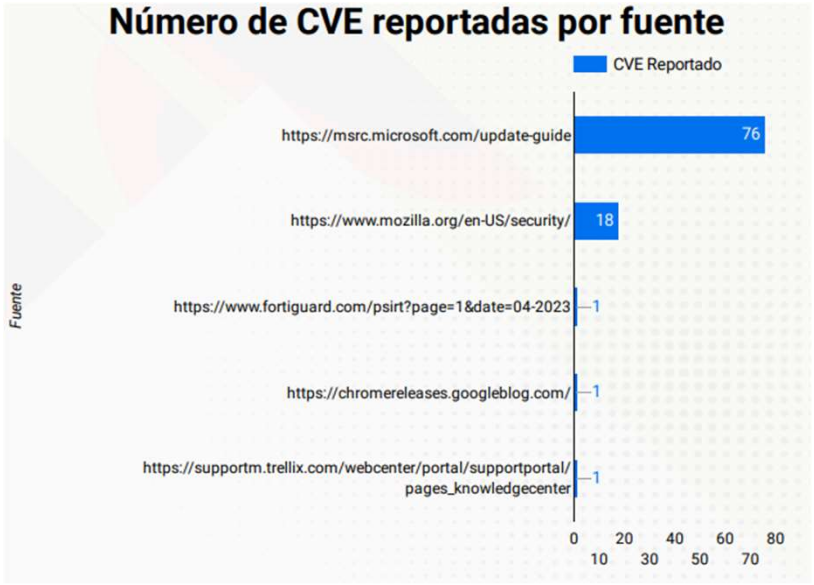
En los gráficos a la izquierda se pueden observar las técnicas y subtécnicas (framework de referencia: MITRE ATT&CK) más identificadas durante el periodo analizado, además, también se pueden observar las mitigaciones relacionadas con dichas técnicas.

Industria objetivo de cibercriminales

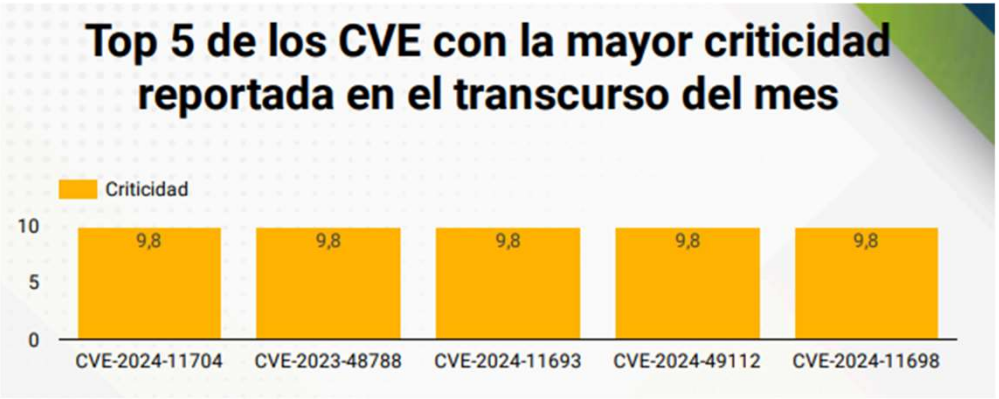


En este gráfico se pueden observar los sectores de la industria que fueron afectados por las amenazas investigadas durante el periodo informado.

Vulnerabilidades reportadas



Se reportaron 106 vulnerabilidades de 75 productos pertenecientes a 5 fabricantes distintos



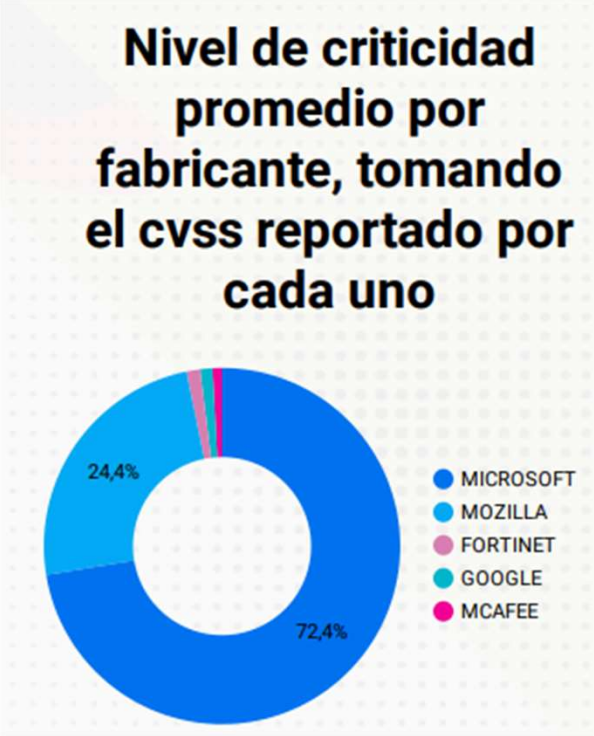
Se reportaron 7 vulnerabilidades de importancia crítica al tener un puntaje de clasificación superior a 9.0 en CVSS Score. Estas vulnerabilidades pueden ser explotadas con mayor facilidad y significan un riesgo más alto en cuanto al impacto que se tiene sobre la compañía.

Actividades realizadas

- Se generaron 48 alertas y eventos en MISP.
- De las 48 alertas se han compartido un total de 51.676 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 34 actores de amenazas identificados.
- Fueron generadas 7 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.



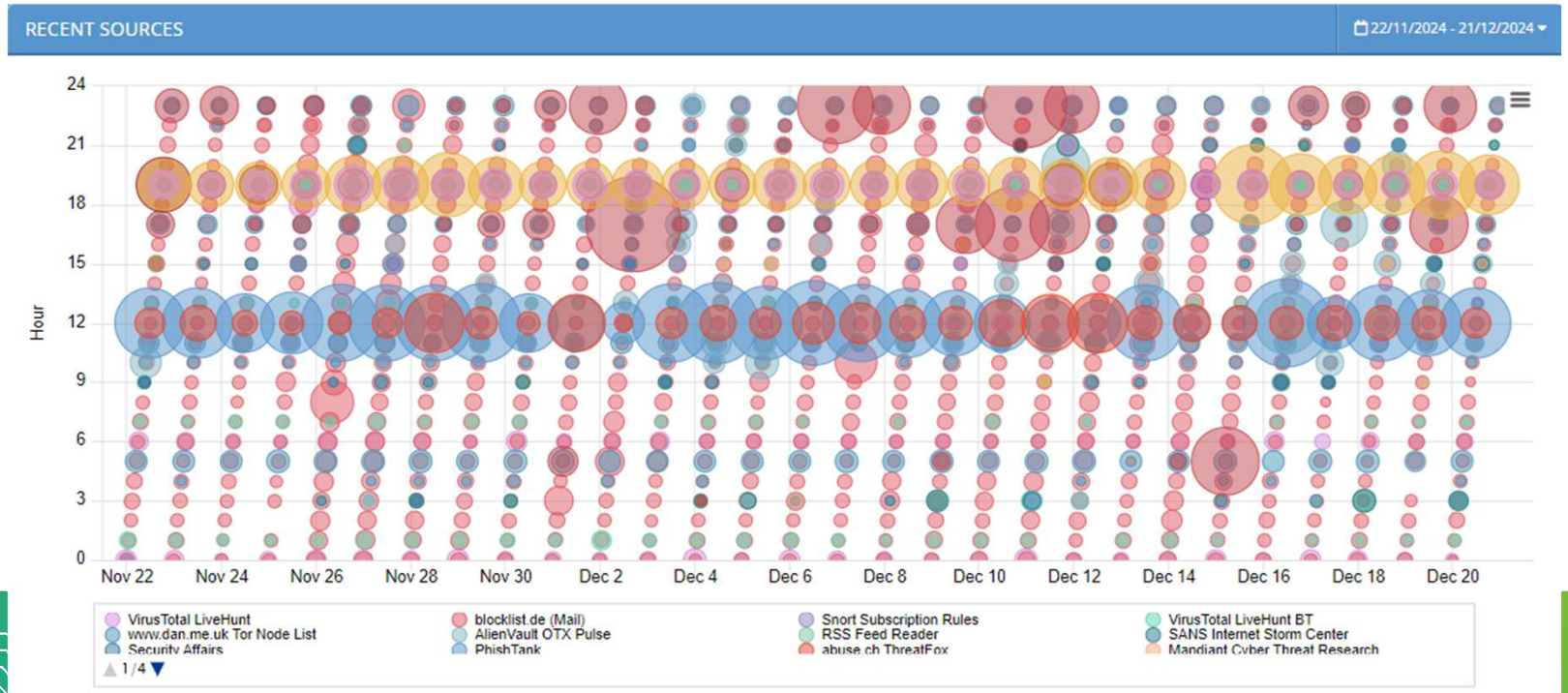
Recomendaciones y conclusiones



- 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.

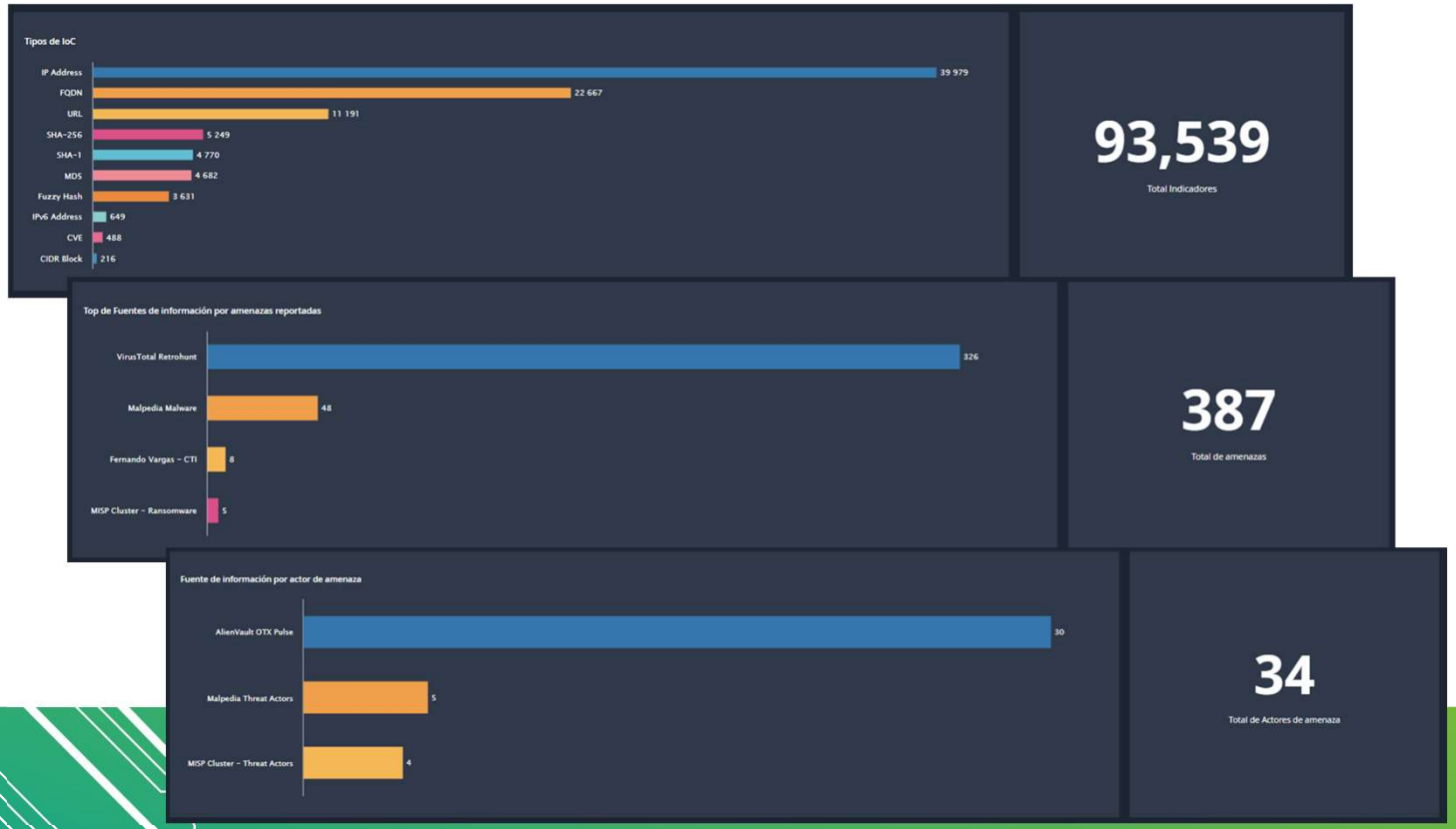
Resumen de objetos obtenidos - TIP

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 realizaron ajustes en las fuentes de datos de Threat Intelligence que funcionan como ingestores de indicadores de compromiso en la plataforma TIP, con el fin de mejorar tanto la confiabilidad y utilidad de la información recopilada como la actualización de los indicadores obtenidos.
- Se ajusta la priorización y enriquecimiento de los indicadores de compromiso que son ingestados por la plataforma de 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.

Informe Threat Hunting

2024

02

Reglas a nivel de comportamiento

02

Análisis de amenazas en profundidad y focalizado

Objetivo

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

Objetivos específicos

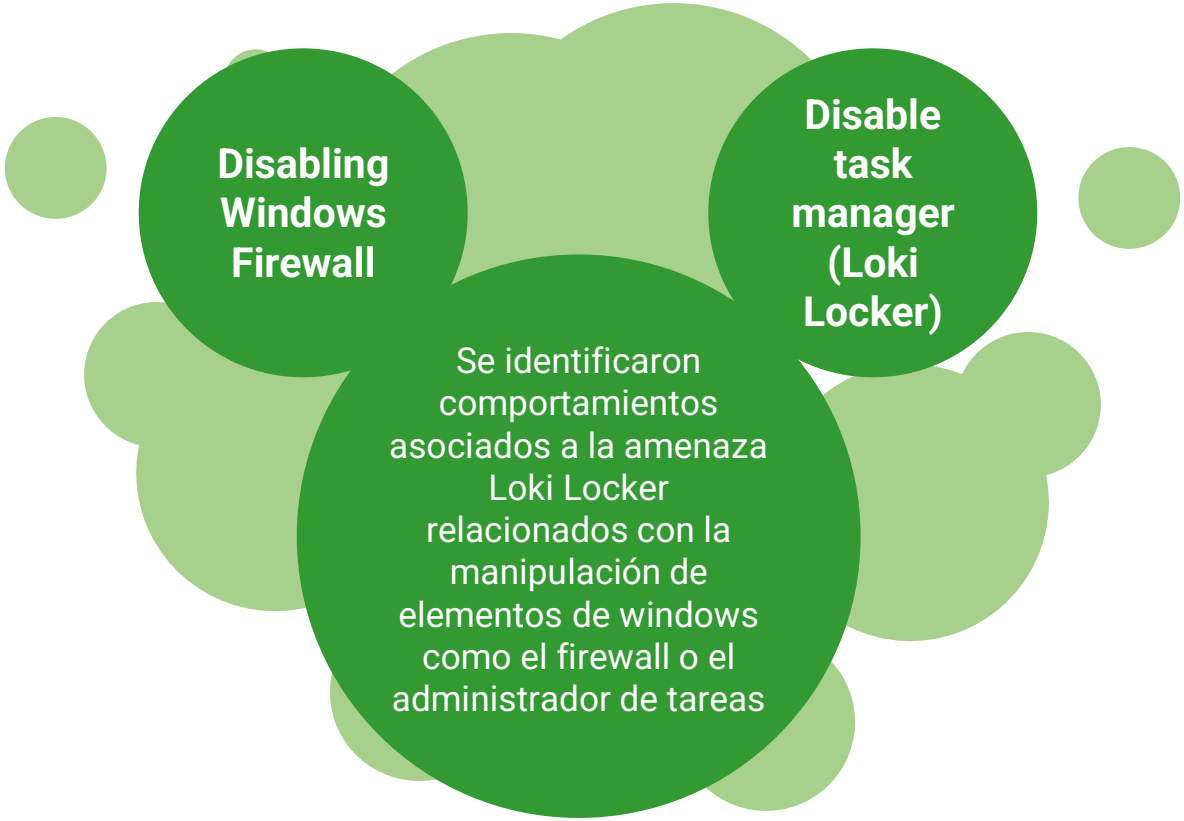
- Generar un resumen de las reglas SIGMA compartidas por el equipo de CTI para el Fondo Nacional del Ahorro
- Resumen de actividades realizadas durante el periodo reportado.

Alcance

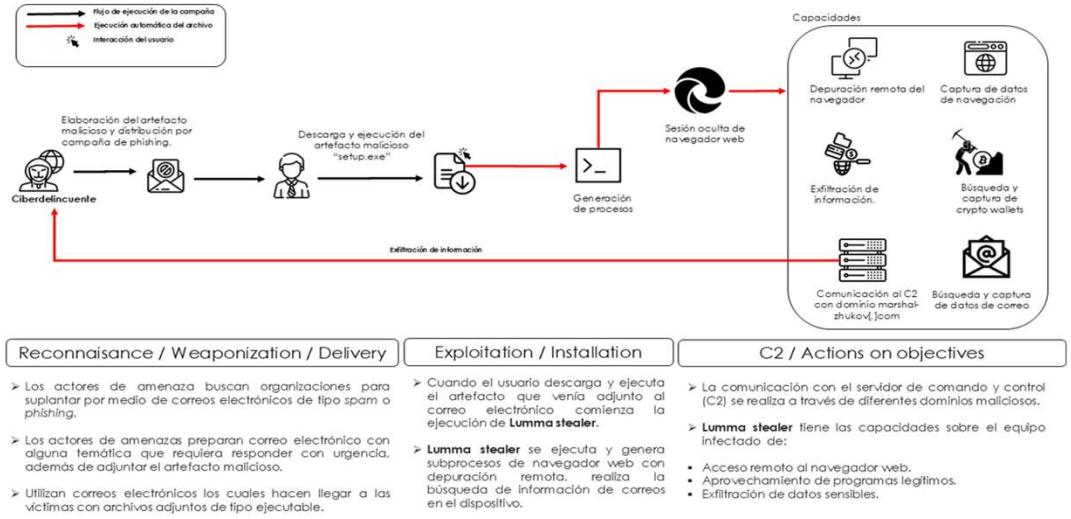
Los temas a tratar sobre este informe son:

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

Resumen de reglas compartidas

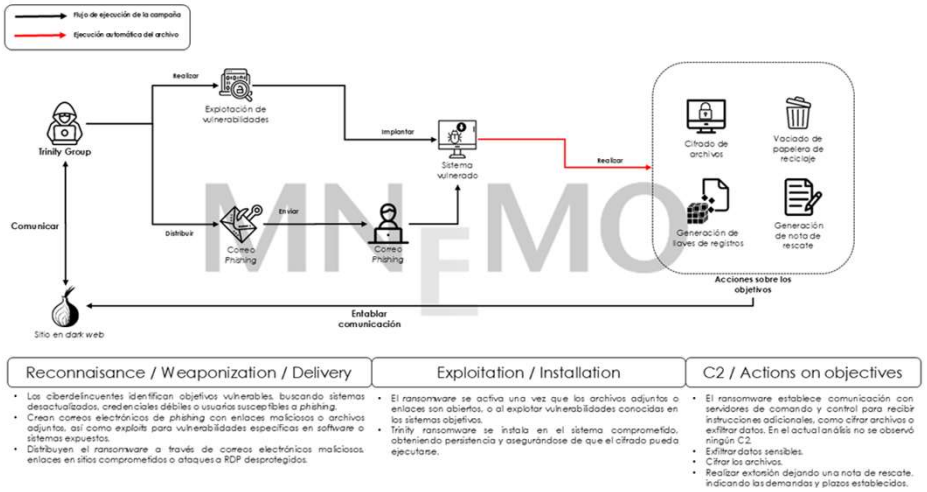


Análisis de amenazas focalizados



- Se realizó un Tailored Threat Analysis sobre la amenaza Lumma Stealer, un stealer capaz de crear una sesión remota y oculta del navegador web, donde captura y exfiltra información sensible .
- El análisis se encarga de mostrar el funcionamiento de la amenaza, así como sus métodos de exfiltración de información una vez ha infectado un equipo de cómputo.

Análisis de amenazas focalizados

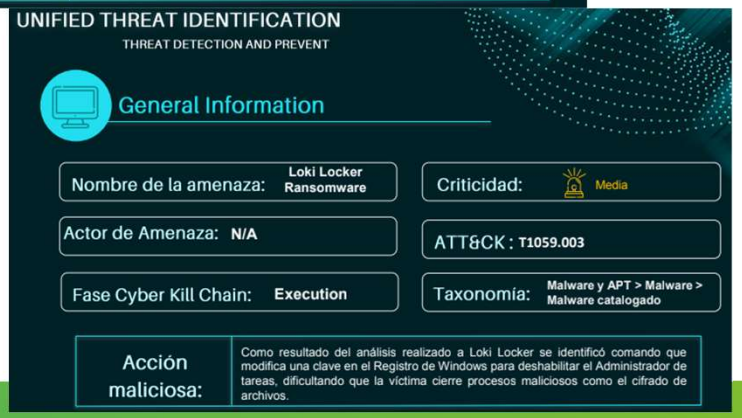


- Se realizó un Tailored Threat Analysis sobre Trinity ransomware, una amenaza capaz de capturar y exfiltrar información sensible, para luego cifrar la información del dispositivo y pedir una recompensa.
- El análisis se encarga de mostrar el funcionamiento de la amenaza, así como sus métodos de persistencia, exfiltración y cifrado de información una vez ha infectado un equipo de cómputo.

Actividades realizadas

- Tanto los indicadores de comportamiento como de compromiso fueron ingresados en la TIP.
- Se crearon 2 reglas Sigma en la que se identifican comportamientos de ejecución de la amenaza Loki Locker ransomware.
- La reglas SIGMA identifican la deshabilitación del firewall y el administrador de tareas de windows.
- Se realizaron análisis focalizados sobre las amenazas Lumma Stealer y Trinity Ransomware, dando detalles de su funcionamiento, distribución y recomendaciones que permiten detectar y contener la amenaza.





Informe Laboratorio avanzado de malware

2024

120

Muestras sospechosas analizadas

105

Muestras confirmadas con algún tipo de malware

Objetivo

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

Objetivos específicos

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

Alcance

Los temas a tratar en este informe son:

• Capacidades del laboratorio de malware.

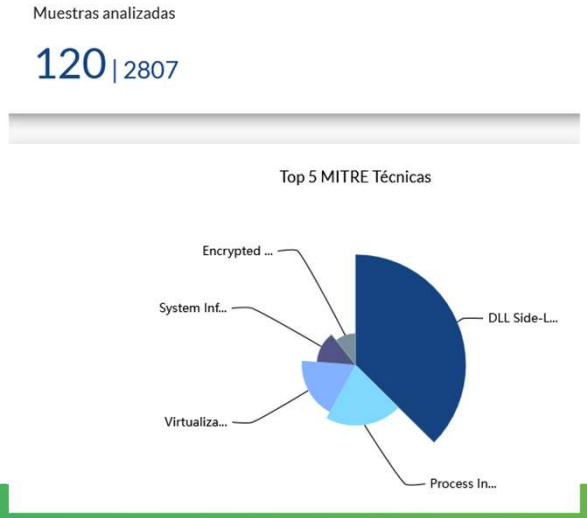
• Dar una visión de las muestras que continuamente se analizan durante el ejercicio de Threat Hunting.

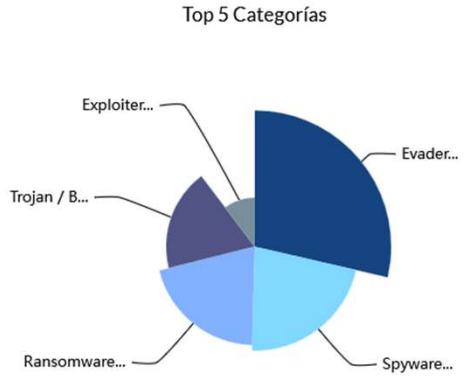
Resumen de análisis de muestras sospechosas

Durante el período informado, el laboratorio de malware ha analizado 120 muestras, de las cuales 105 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.

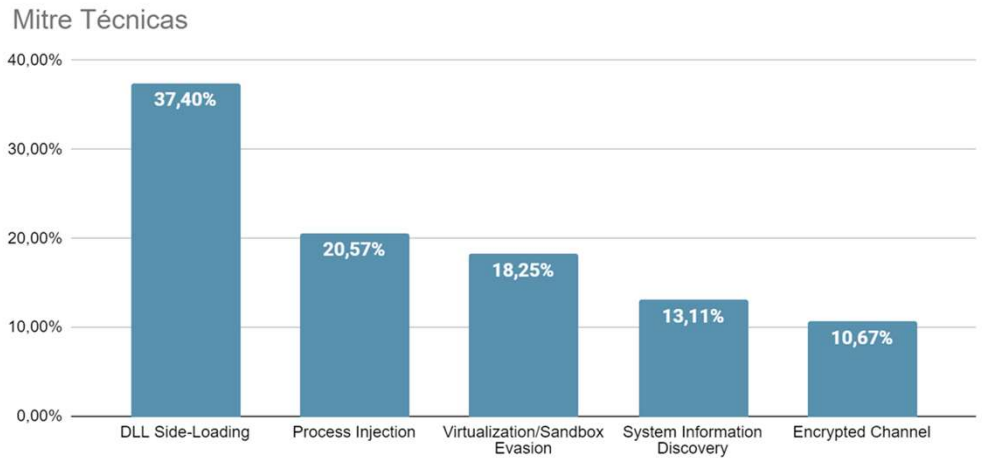


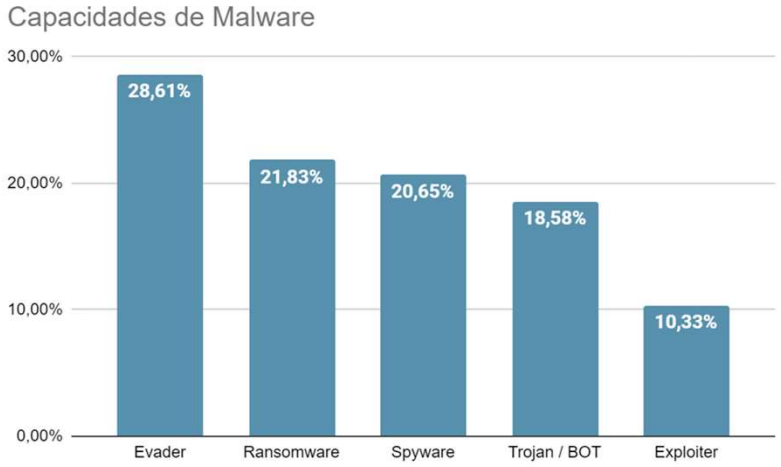




Técnicas más utilizadas y categorías de malware más detectadas

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	DLL Side-Loading	DLL Side-Loading	Input Capture	System Information Discovery	Taint Shared Content	Archive Collected Data		Encrypted Channel
Replication Through Removable Media	Windows Management Instrumentation	Scripting	Process Injection	Process Injection	Credential Dumping	Security Software Discovery	Remote Desktop Protocol	Input Capture		Standard Application Layer Protocol
	Command-Line Interface	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Virtualization/Sandbox Evasion	Credential API Hooking	Virtualization/Sandbox Evasion		Clipboard Data		Standard Non-Application Layer Protocol
	PowerShell	Windows Service	Windows Service	Obfuscated Files or Information	Credentials In Files	Process Discovery		Email Collection		Remote File Copy
	Service Execution	Scheduled Task	Access Token Manipulation	Masquerading	Credentials in Registry	File and Directory Discovery		Data from Local System		Non-Standard Port
	Scheduled Task	Valid Accounts	Scheduled Task	Software Packing		System Time Discovery		Screen Capture		Web Service
	Exploitation for Client Execution	Services File Permissions Weakness	Valid Accounts	Disable or Modify Tools		Application Window Discovery		Credential API Hooking		Remote Access Tools
		Obfuscated Files or Information	Exploitation for Privilege Escalation	Deobfuscate/Decode Files or Information		System Owner/User Discovery		Man in the Browser		Connection Proxy
		LSASS Driver	Abuse Elevation Control Mechanism	Access Token Manipulation		Account Discovery				
		Create Account	Extra Window Memory Injection	File Deletion		Remote System Discovery				
		Image File Execution Options Injection	Services File Permissions Weakness	Valid Accounts		System Network Configuration Discovery				
			Bypass User Access Control	Hidden Files and Directories		Network Share Discovery				

Análisis de muestras propias FNA

- Desde el servicio de Laboratorio avanzado de Malware se recibió un archivo ejecutable, el cual se solicitó analizar para verificar la seguridad del mismo, ya que se tenía contemplados para instalar en equipos de la compañía.
- El resultado del análisis arrojó que el ejecutable era legítimo, y que su instalación no representaba ningún riesgo en primera medida. Sin embargo, en las recomendaciones del informe se indicó que el riesgo de los ejecutables radica en las configuraciones que sean aplicadas en su instalación, por ejemplo abrir puertos de red a internet que queden expuestos a que actores de amenaza puedan detectar y atacar con amenazas de cualquier tipo.

Actividades realizadas

- En el periodo reportado, el equipo del Cyber Threat Intelligence ha llevado a cabo 120 análisis de muestras sospechosas.
- Utilizando herramientas de Threat Hunting, el equipo ha recopilado muestras de diversas fuentes, teniendo en cuenta las tendencias de ataques en la región.
- Análisis de muestras aportadas por el equipo de monitoreo de herramientas de FNA.
- Identificación de las tácticas, técnicas y procedimientos utilizados por los actores de amenazas a través de cada una de las muestras recolectadas, obteniendo así las tendencias de ataque perpetrado por los cibercriminales.
- Los indicadores de compromiso se tienen en cuenta para ser agregados a eventos en la herramienta de MISP así como a la herramienta de Threat Intelligence Platform TIP donde se enriquecen los indicadores con información como actores de amenaza, familias de malware, tácticas y técnicas de la matriz de Mitre ATT&CK. Por consiguiente, los indicadores son agregados a las herramientas de seguridad del cliente.

Recomendaciones y conclusiones

- 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 ejecutables 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.
- Como resultado del análisis del ejecutable “ue_spanish_64.exe” se identificó que no presenta características maliciosas y en caso de implementar su uso se recomienda actualizar constantemente este software para prevenir la explotación de vulnerabilidades que se identifiquen para dicho programa.
- Se recomienda reportar cualquier tipo de archivo sospechoso que sea detectado al interior de la infraestructura de la empresa provenientes de correos electrónicos sospechosos, descargas de software no autorizadas, dispositivos de almacenamiento no autorizados, etc.

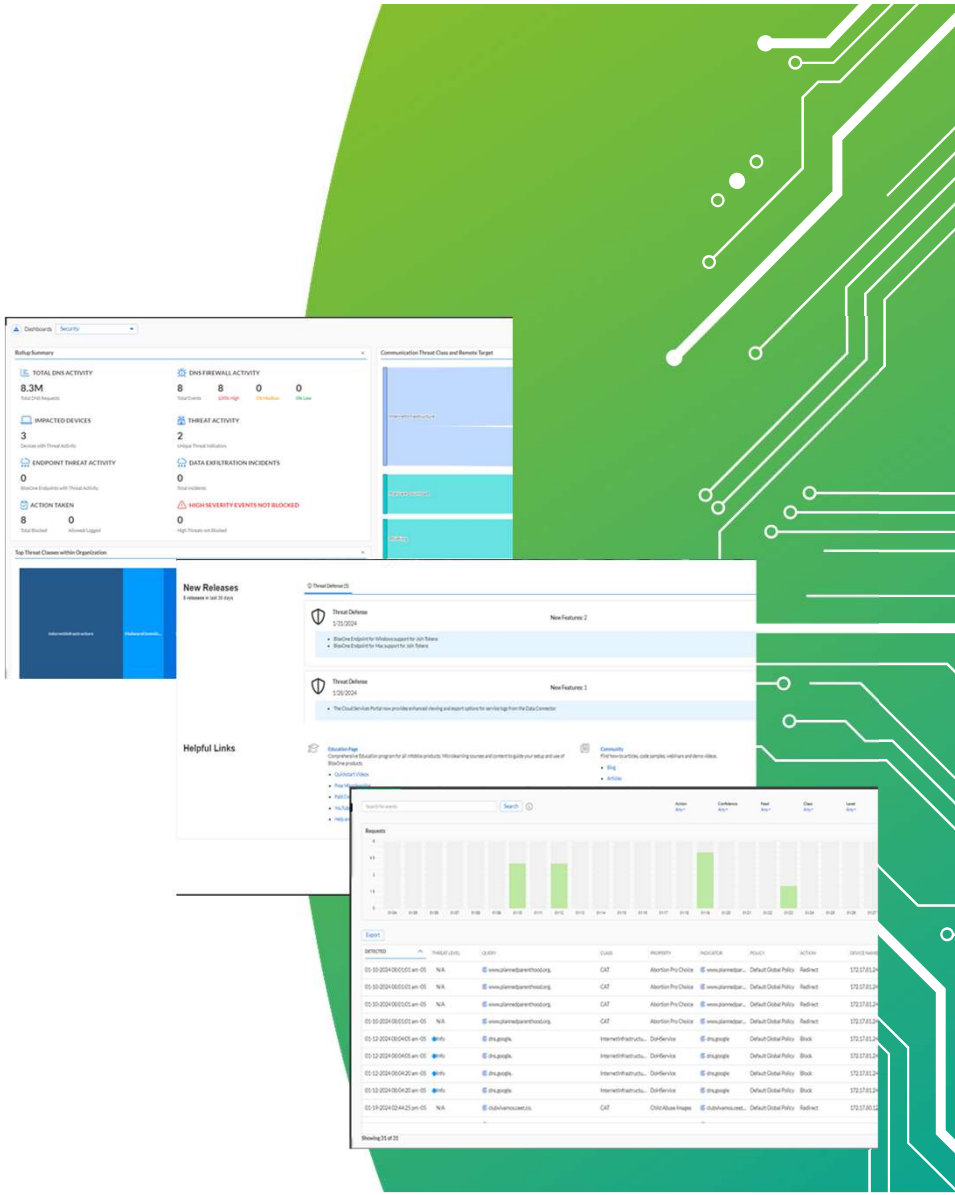
Infoblox

DEFINICIONES

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

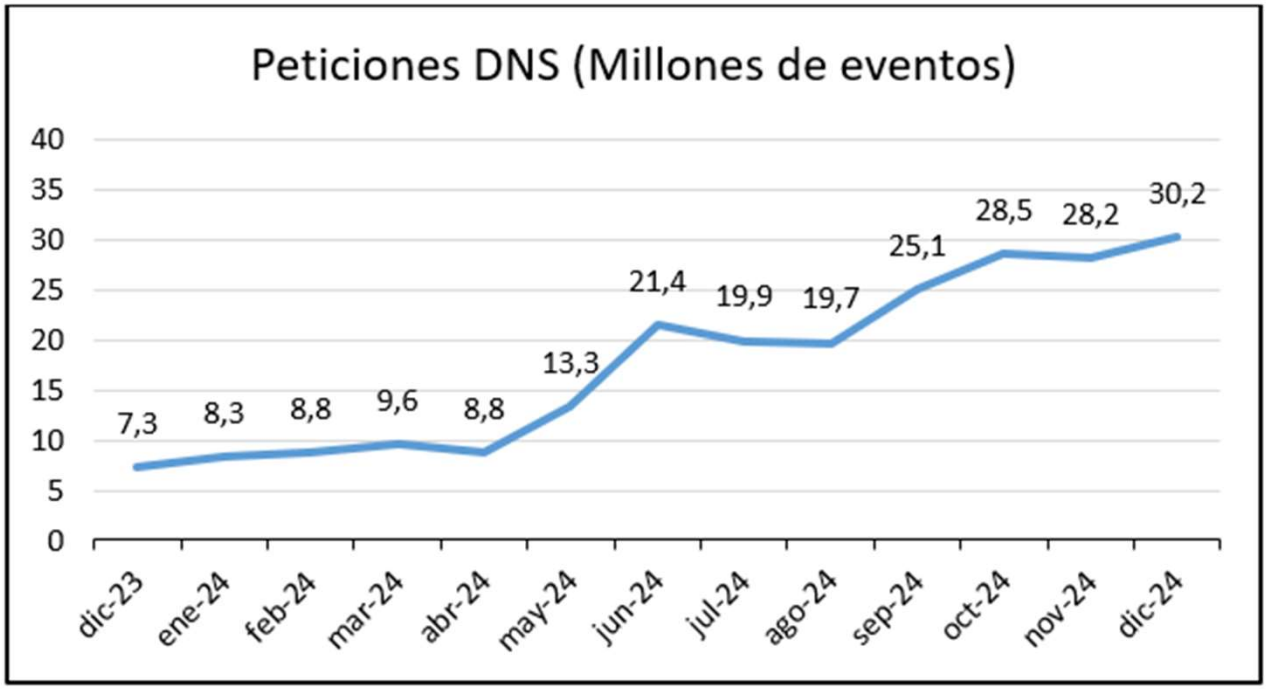
Política: cuenta con una serie de políticas que rigen cómo opera la empresa. Estas políticas se establecen para proteger a los empleados, clientes y socios de Infoblox, así como para garantizar que la empresa cumpla con todas las leyes y regulaciones aplicables.

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

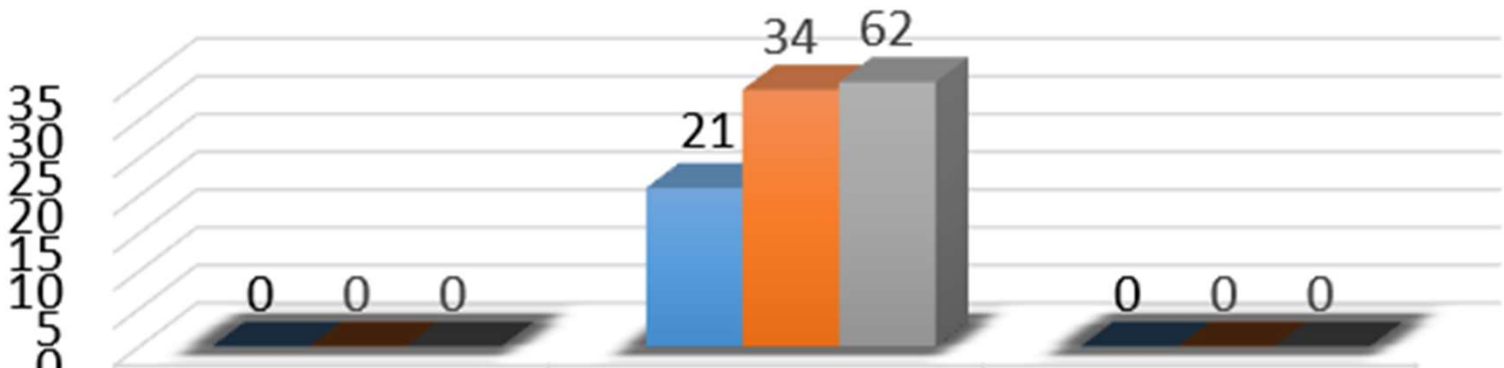


DNS SECURITY - INFOBLOX (Millones de eventos)

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



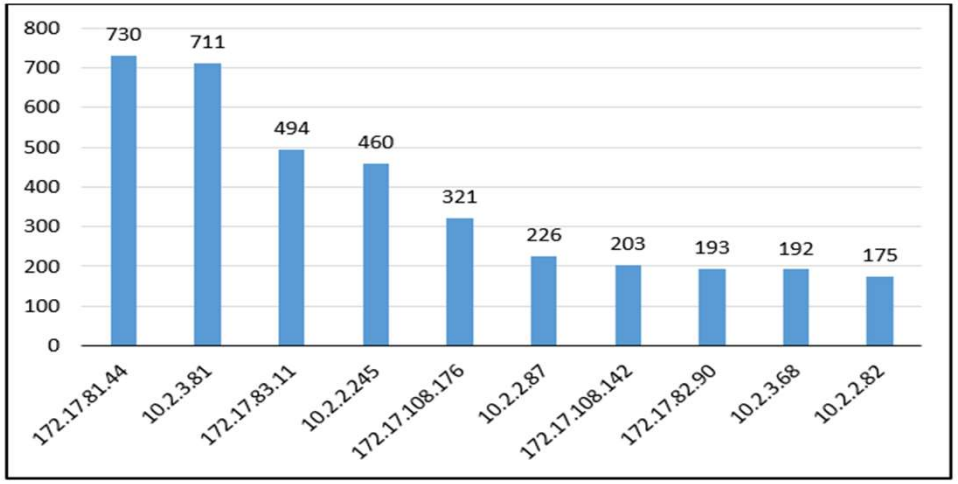
INDICADOR AMENAZAS

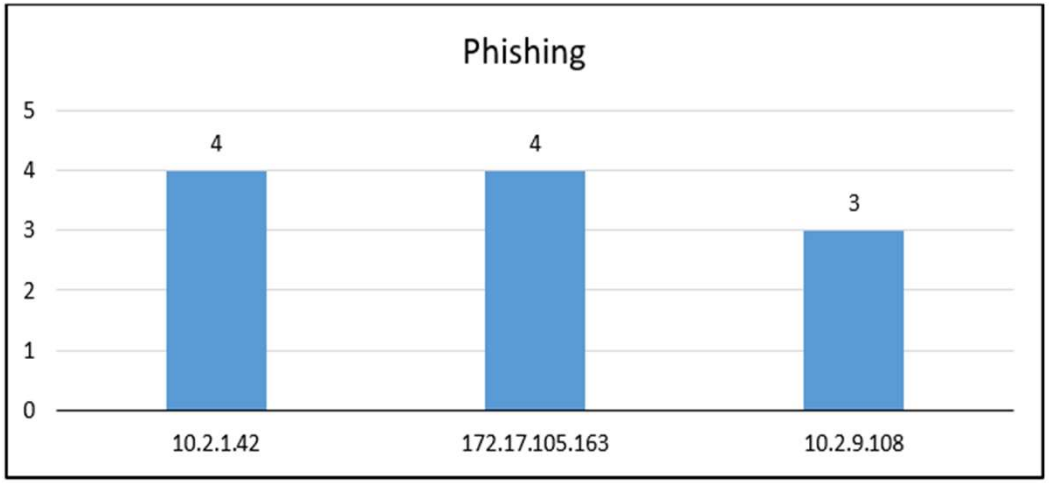


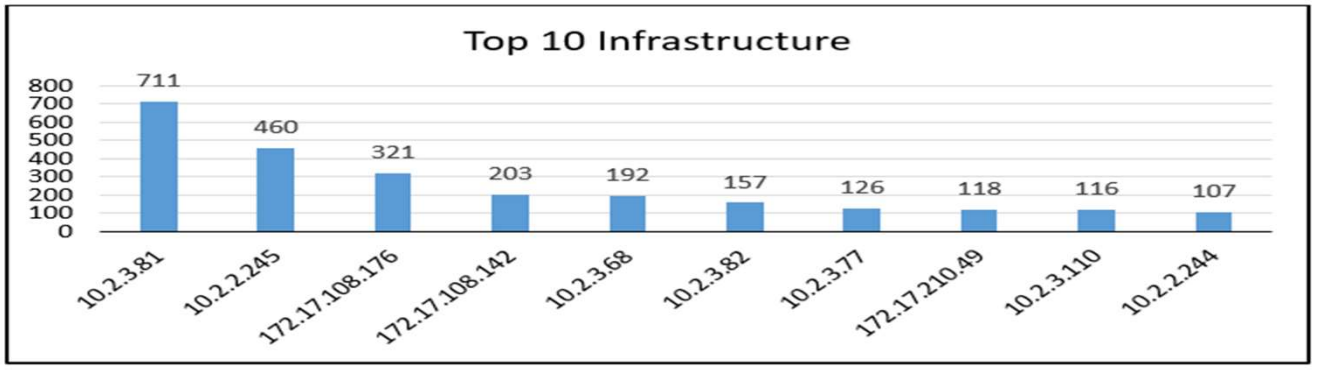
	EVENTOS CRITICOS	ACTIVIDAD DE AMANAZA	INCIDENTES DE EXFILTRACIÓN
oct-24	0	21	0
nov-24	0	34	0
dic-24	0	62	0

DNS SECURITY – INFOBLOX

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

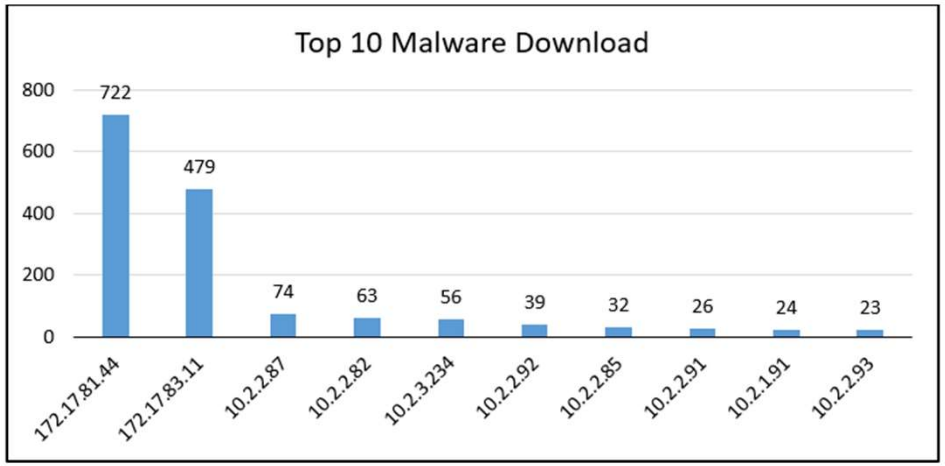


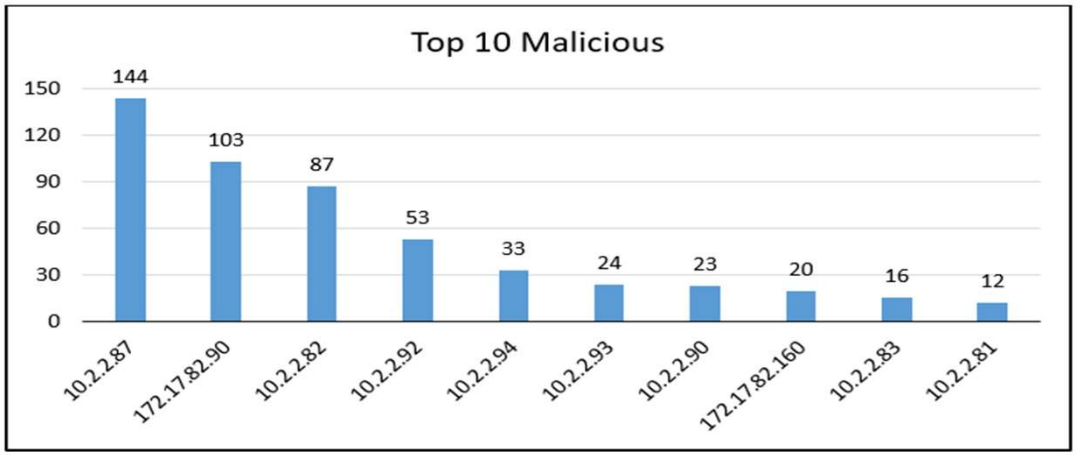


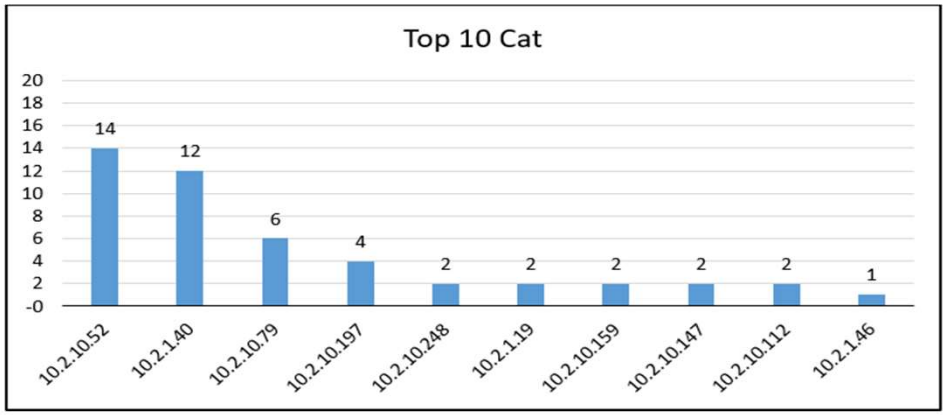


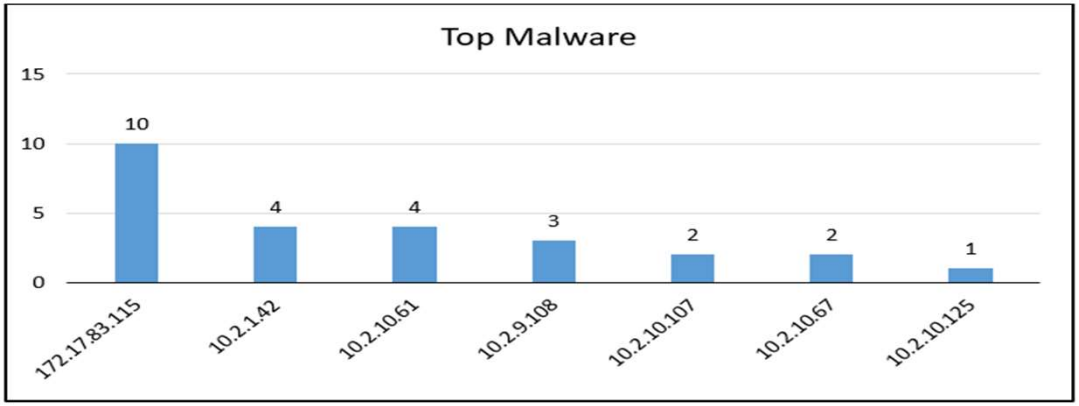
DNS SECURITY – INFOBLOX

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

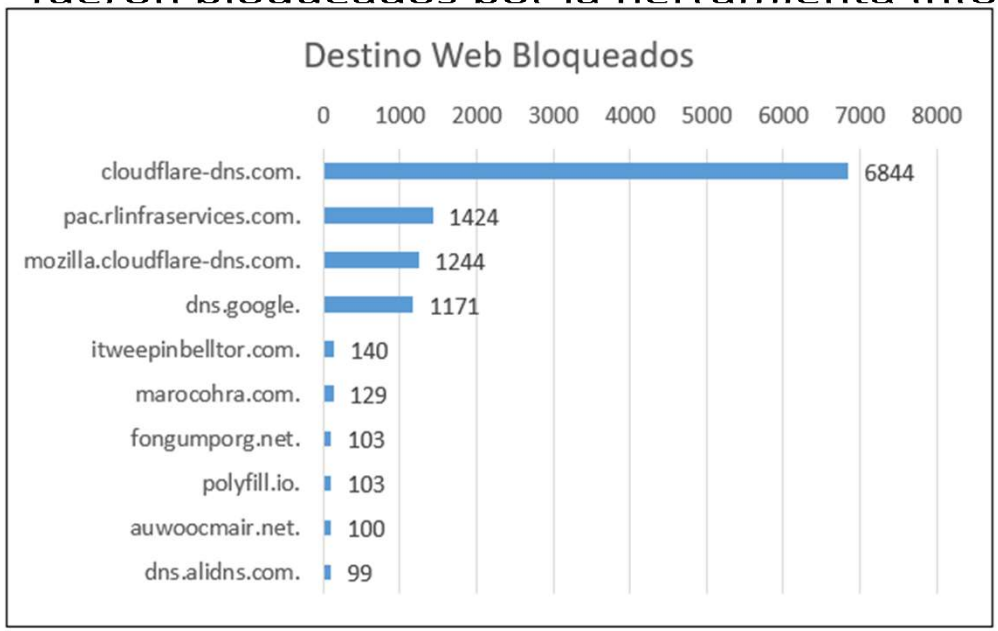


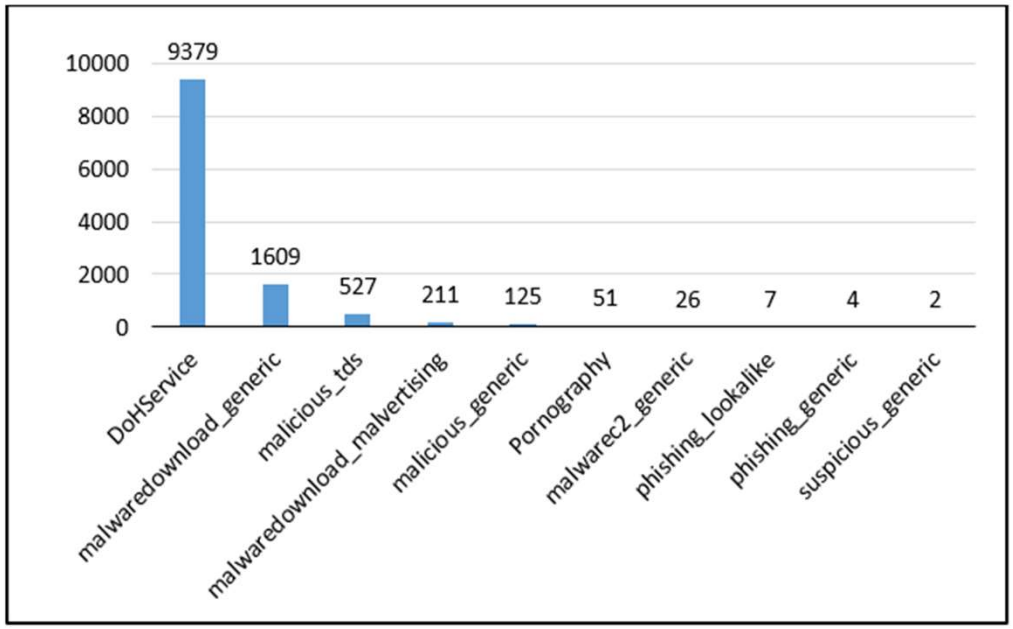






Top de los destinos malintencionados consultados a nivel interno del FNA, los cuales fueron bloqueados por la herramienta Infoblox

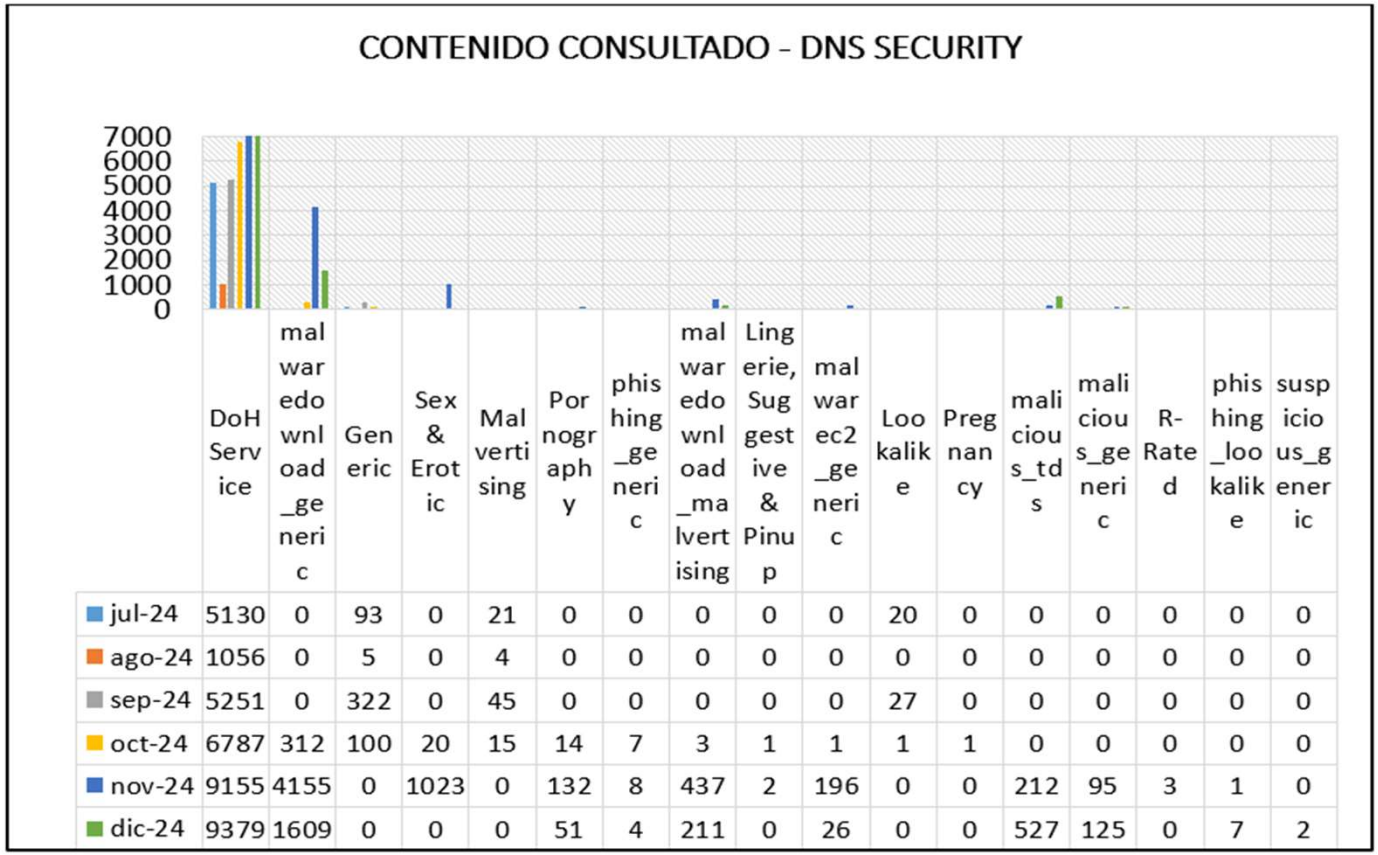




Para el periodo en mención se evidencia un aumento con relación al mes anterior en cuanto al índice de amenazas detectadas, de igual forma se identifica que el volumen de consultas a portales de pornografía aumentó en la resolución de DNS.

GENERAL DNS – INFOBLOX

Para el periodo en mención se evidenció un aumento de 224 eventos en la categoría de DoHservice en las consultas DNS, para la categoría malware download generic se evidenció una disminución de 2,546 siendo las categorías con más consultas dentro del DNS.



	DoH Service	malwaredownload_generic	Generic	Sex & Erotic	Malvertising	Pornography	phishing_generic	malwaredownload_malvertising	Lingerie, Suggestive & Pinup	malwarec2_generic	Lookalike	Pregnancy	malicious_tds	malicious_generic	R-Rated	phishing_lookalike	suspicious_generic
jul-24	5130	0	93	0	21	0	0	0	0	0	20	0	0	0	0	0	0
ago-24	1056	0	5	0	4	0	0	0	0	0	0	0	0	0	0	0	0
sep-24	5251	0	322	0	45	0	0	0	0	0	27	0	0	0	0	0	0
oct-24	6787	312	100	20	15	14	7	3	1	1	1	1	0	0	0	0	0
nov-24	9155	4155	0	1023	0	132	8	437	2	196	0	0	212	95	3	1	0
dic-24	9379	1609	0	0	0	51	4	211	0	26	0	0	527	125	0	7	2

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:

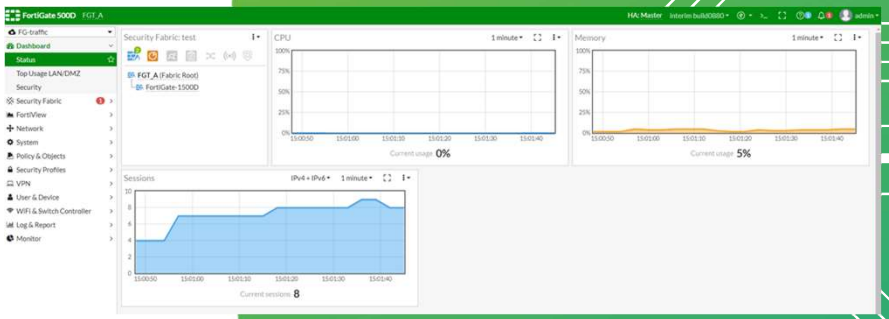
- Monitoreo de eventos revisión de los eventos para detectar cualquier actividad inusual o anómala que pueda indicar un posible ataque.
- Análisis de direcciones IP esto con el de identificar si se encuentran direcciones inactivas.
- Validación de disponibilidad de la plataforma Infoblox.
- Revisión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

FORTINET

FortiWeb™

GENERAL WAF – FORTIWEB

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



Protección de aplicaciones web

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

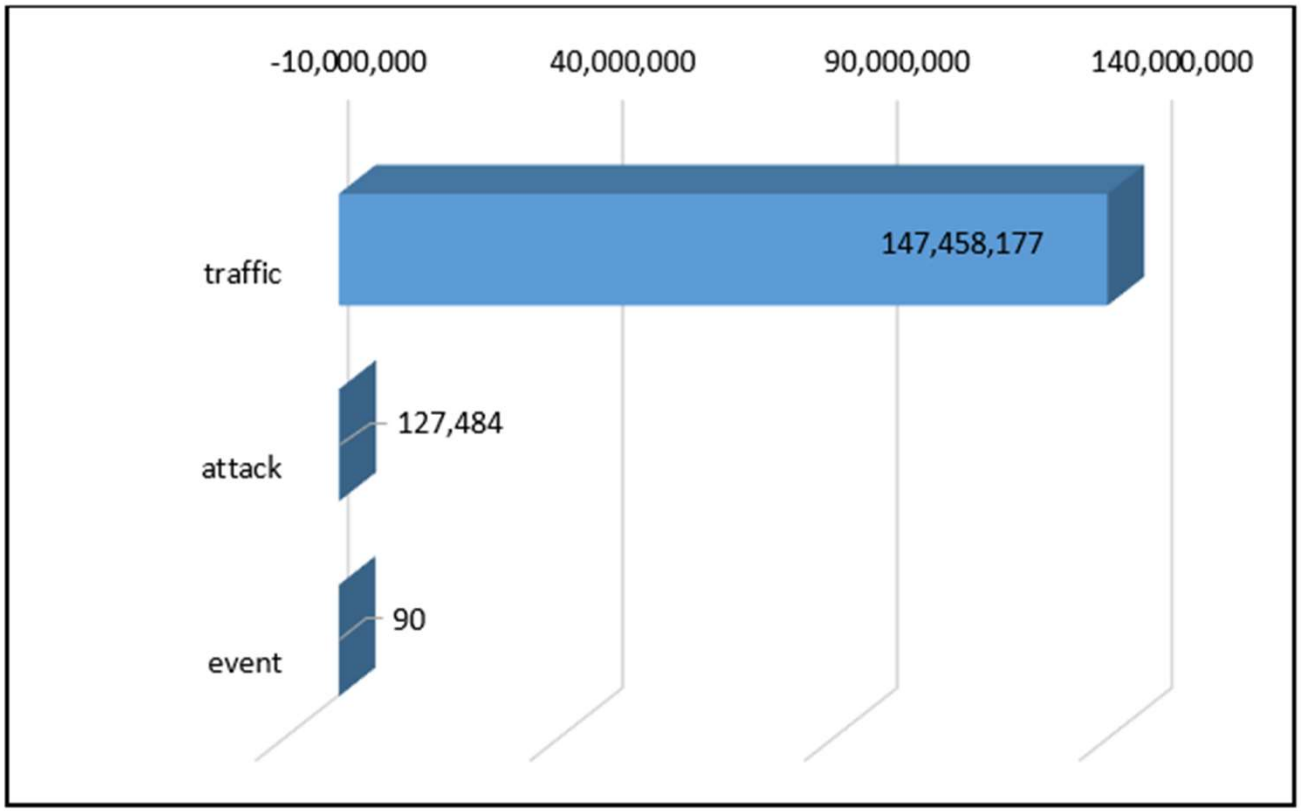
Protección API

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

Mitigación de Bots

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

GENERAL WAF – FORTIWEB



+147 M

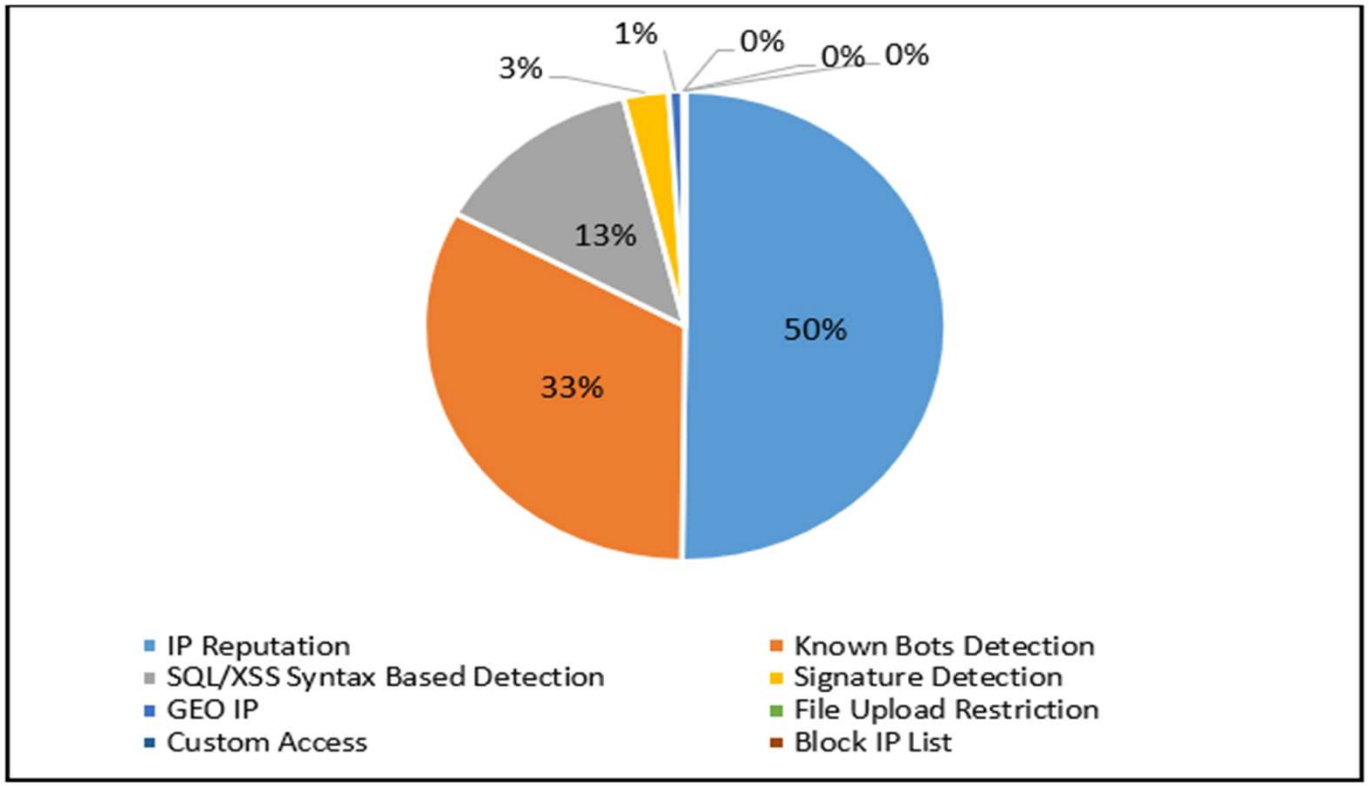
Eventos verificados por el WAF

-0,1%

Del tráfico total es categorizado como amenaza

Durante el presente periodo, se visualizó tráfico a través del WAF de aproximadamente 147 Millones de eventos de los cuales el 0,1% están dentro de la categoría de Amenaza.

GENERAL WAF – FORTIWEB

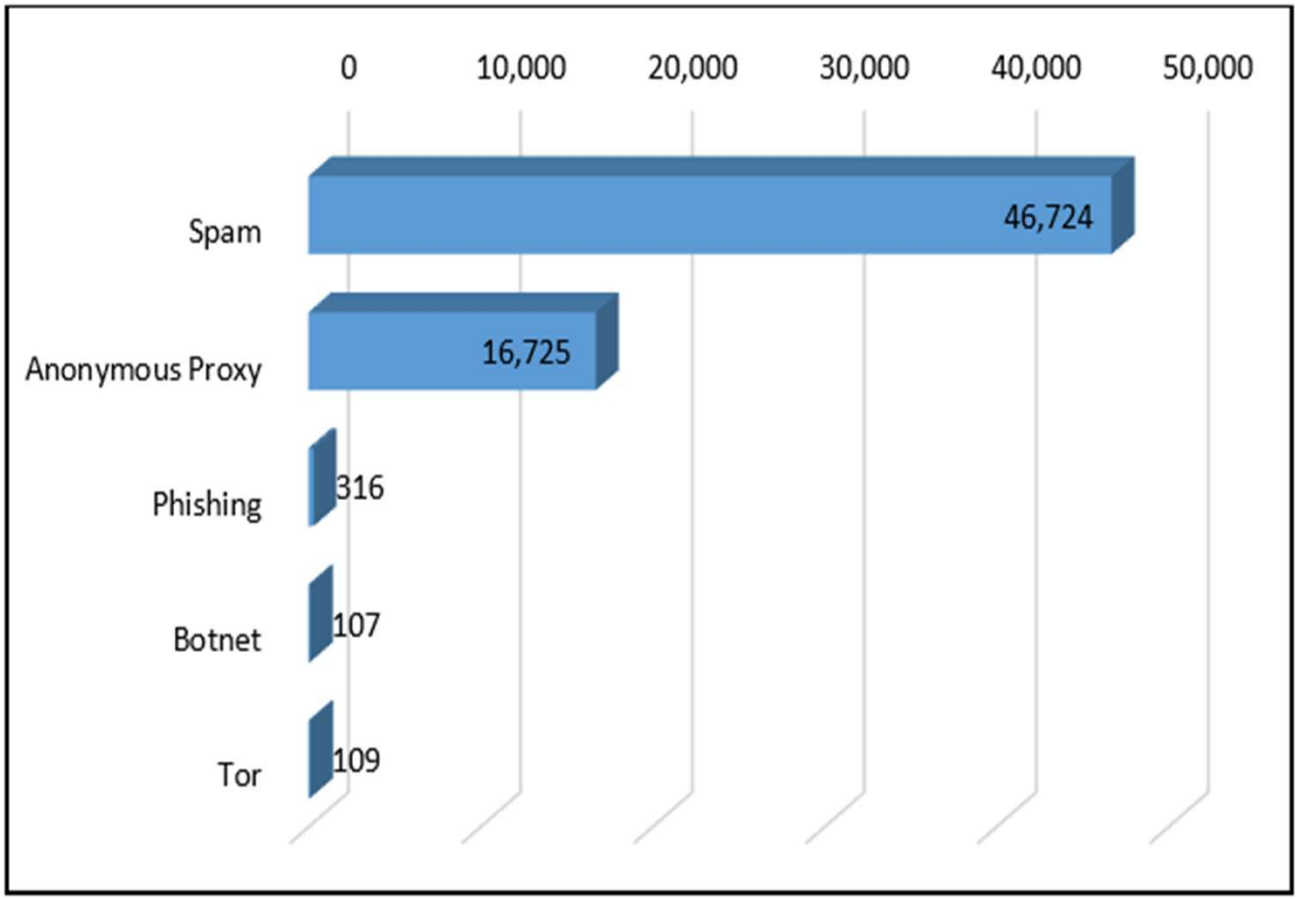


8

Eventos identificados por el WAF

Durante el periodo en mención, se visualizó tráfico a través del WAF con una activación total de 8 categoría de Amenaza de acuerdo a la información extraída.

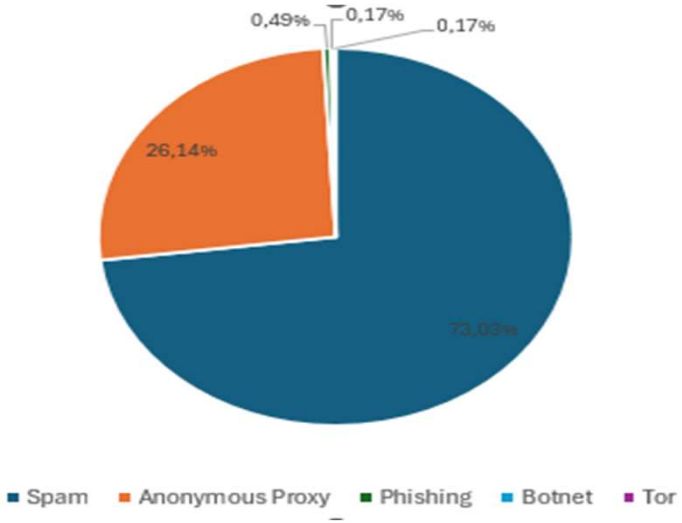
GENERAL WAF – IP REPUTATION



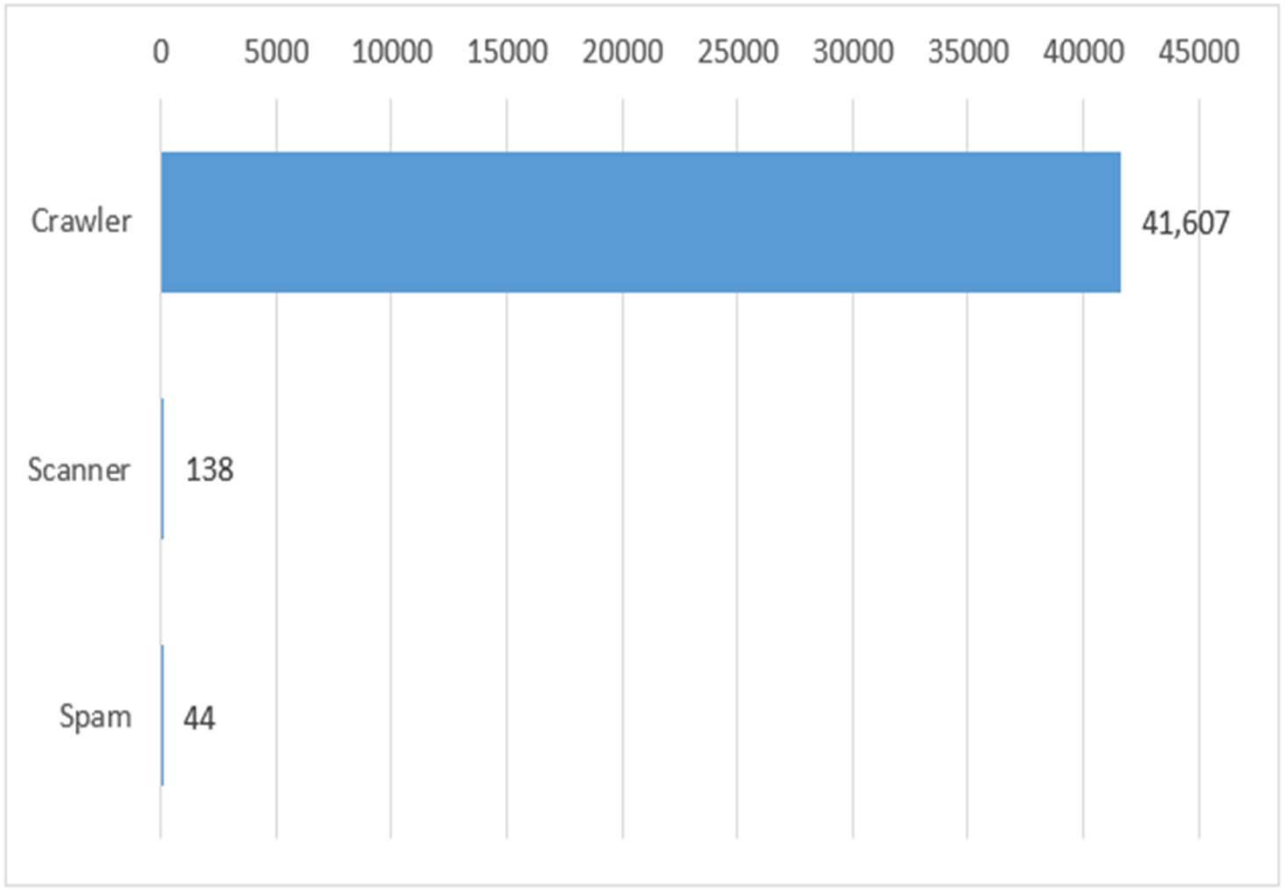
50,19 %

63,981

IP Reputation



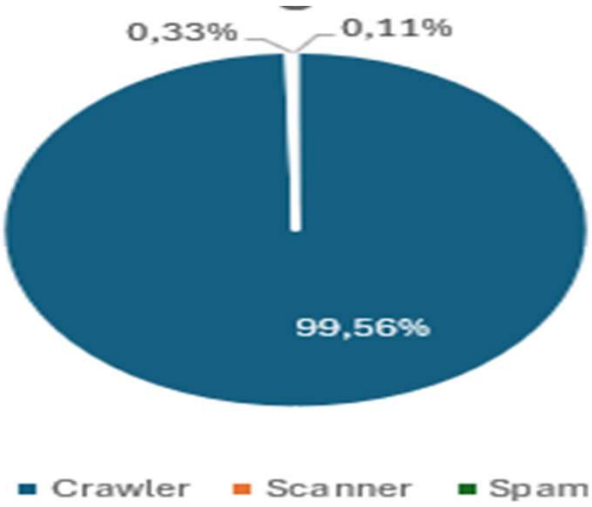
GENERAL WAF – KNOWN BOTS



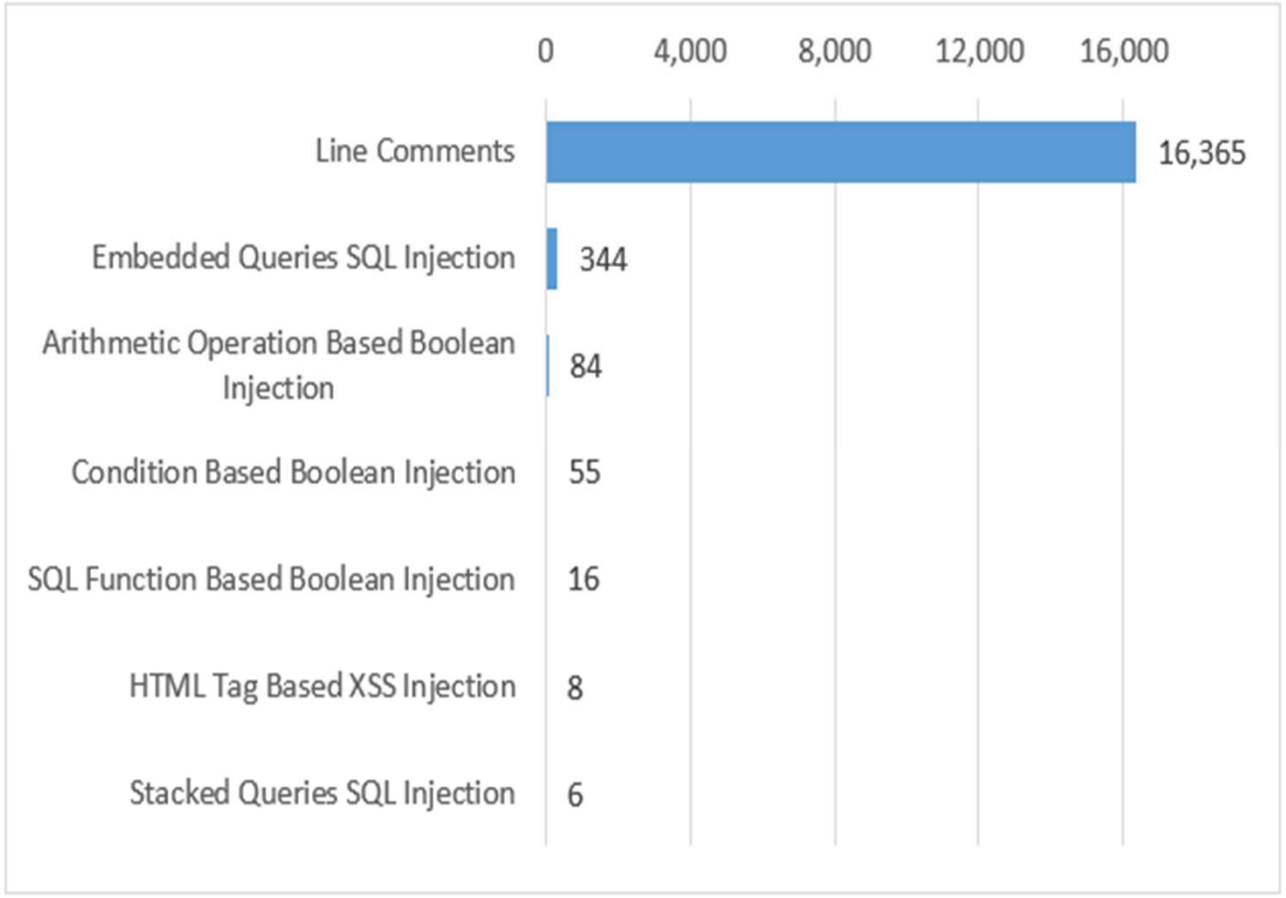
32,78 %

41,789

Known Bots



GENERAL WAF – SQL/XSS Syntax Based Detection

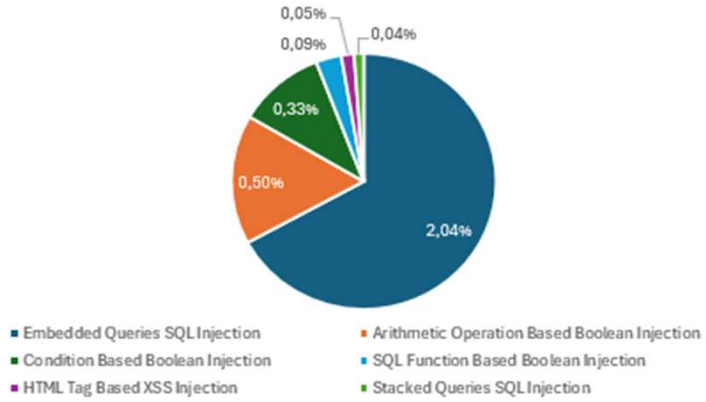


13,24%

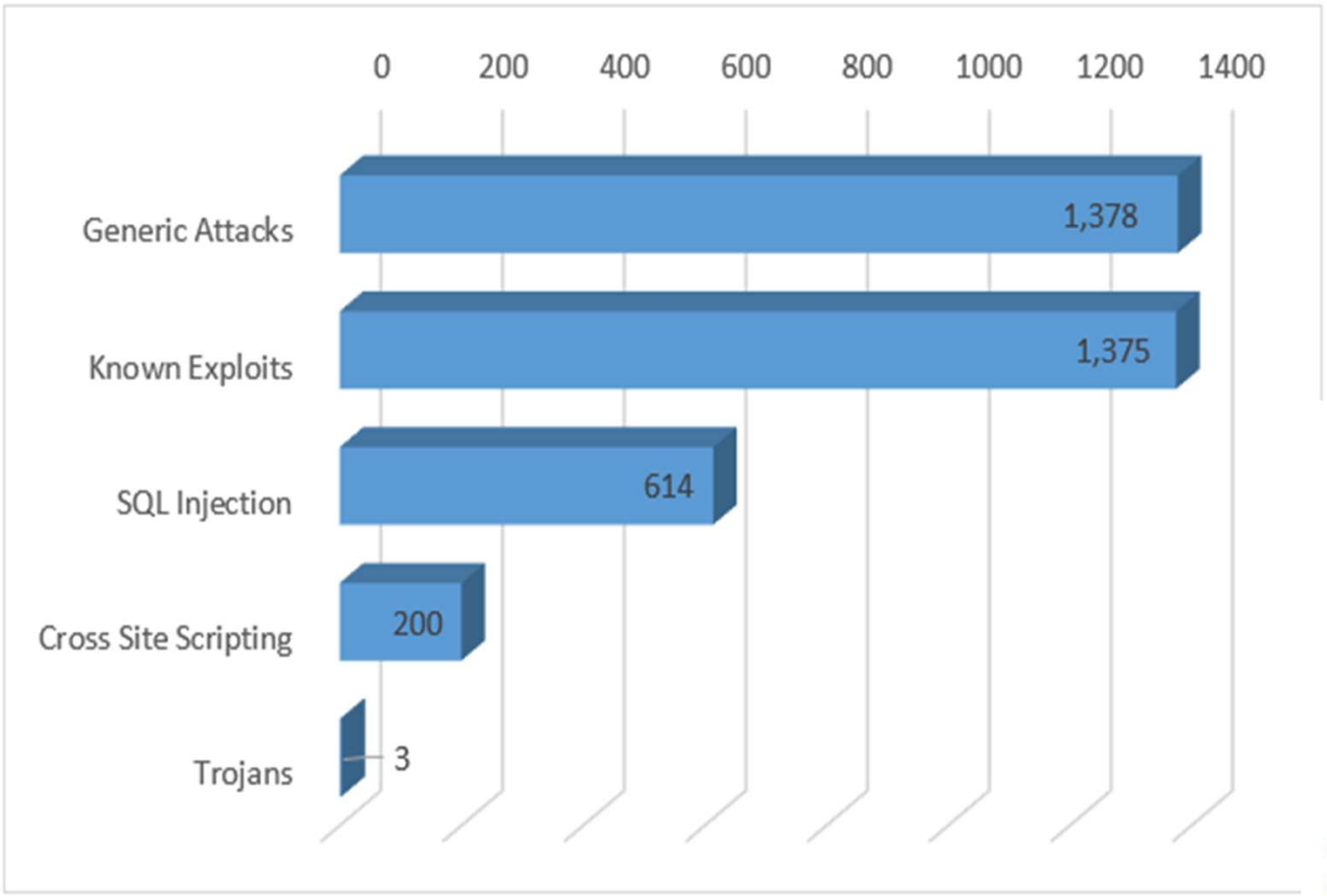
16,878

96,96%

Line Comments
SQL/XSS



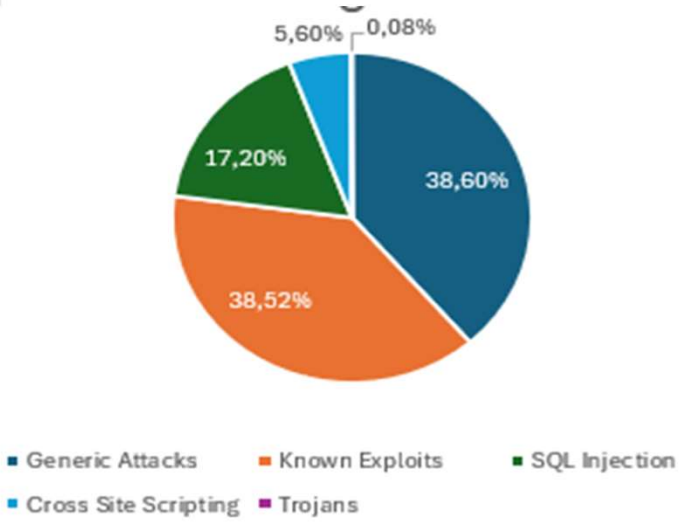
GENERAL WAF – SIGNATURE DETECTION



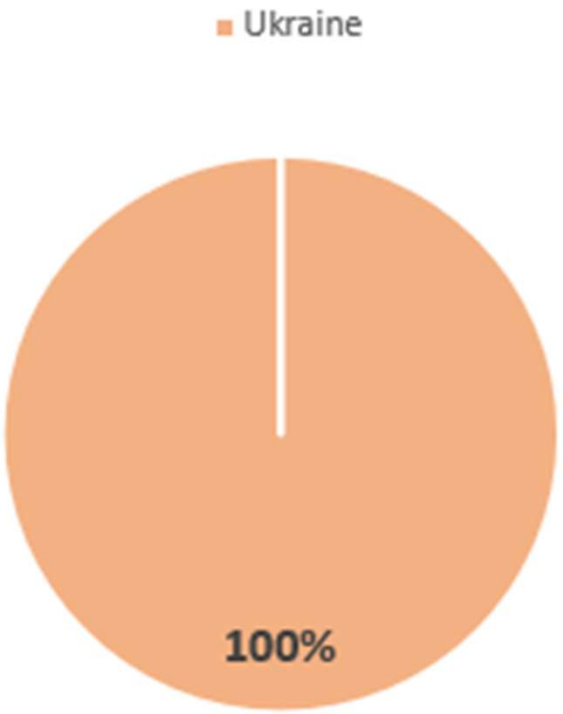
2,80%

3,570

Signature Detection



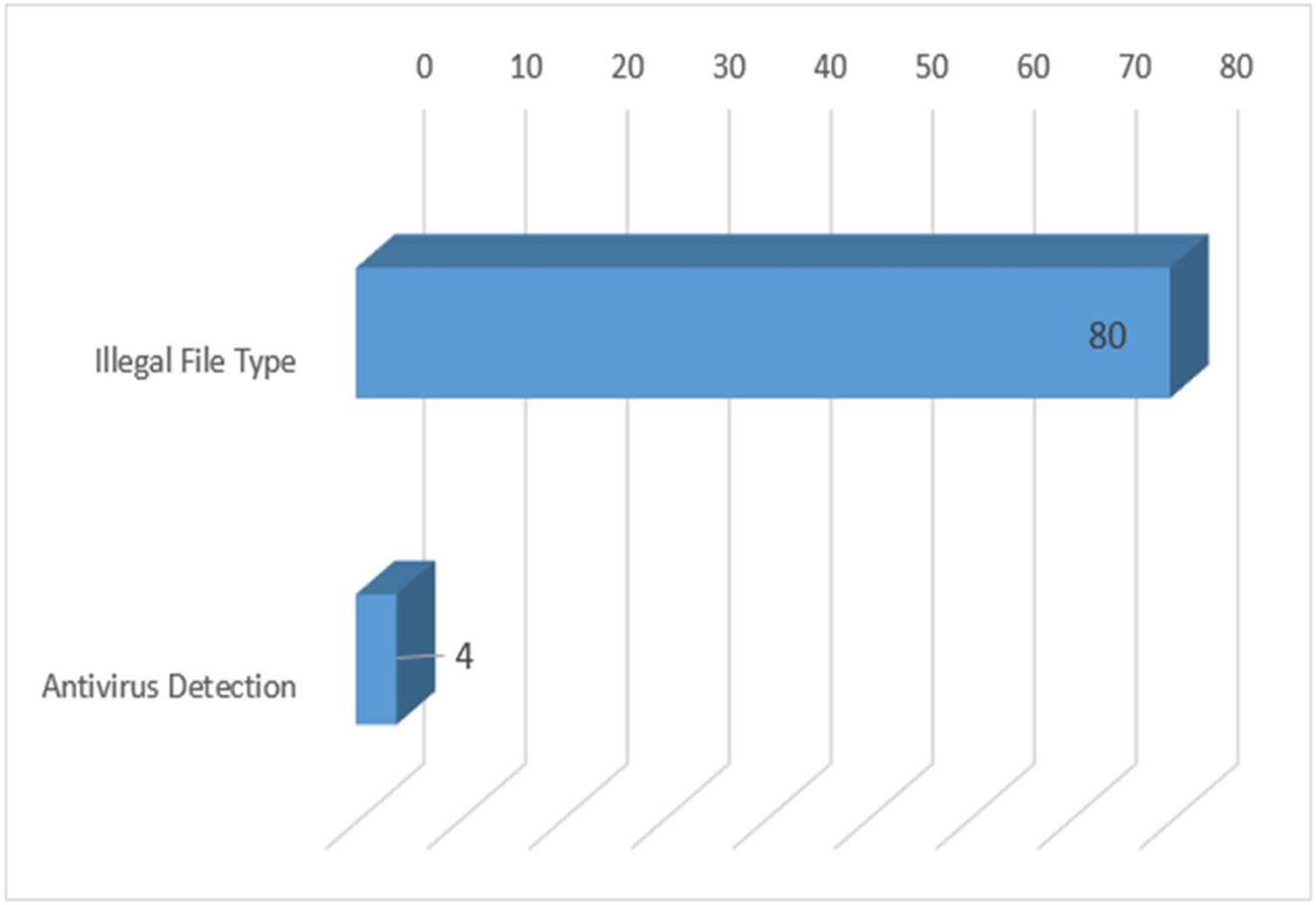
GENERAL WAF – GEO IP



1,097
GEO IP

FNA se ha dispuesto bloquear el
ıfico desde Rusia y Ucrania.

GENERAL WAF – FILE UPLOAD RESTRICTION



84

File Upload Restriction

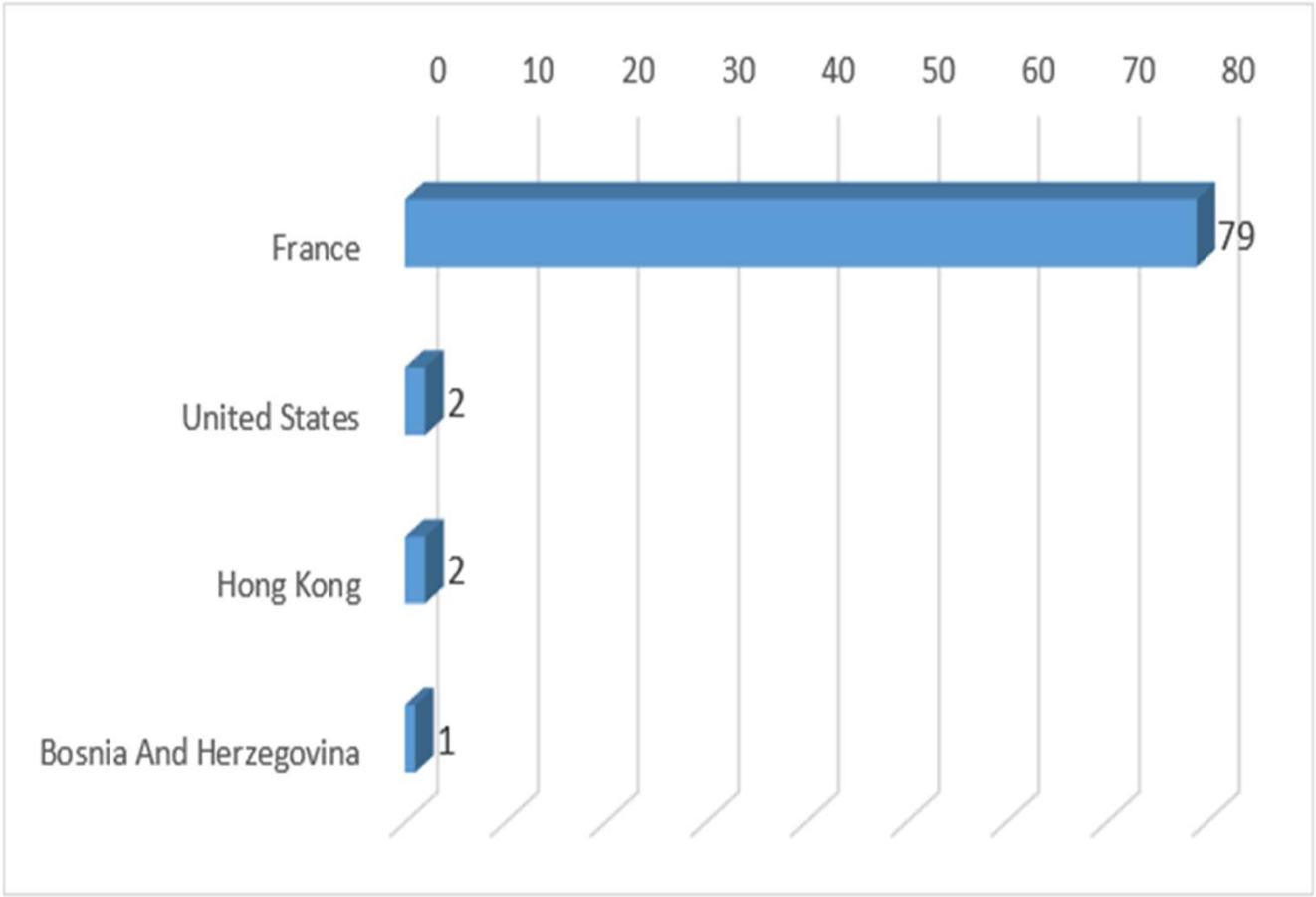
95,24%

Illegal File Type

4,76%

Antivirus Detection

GENERAL WAF - CUSTOM ACCESS



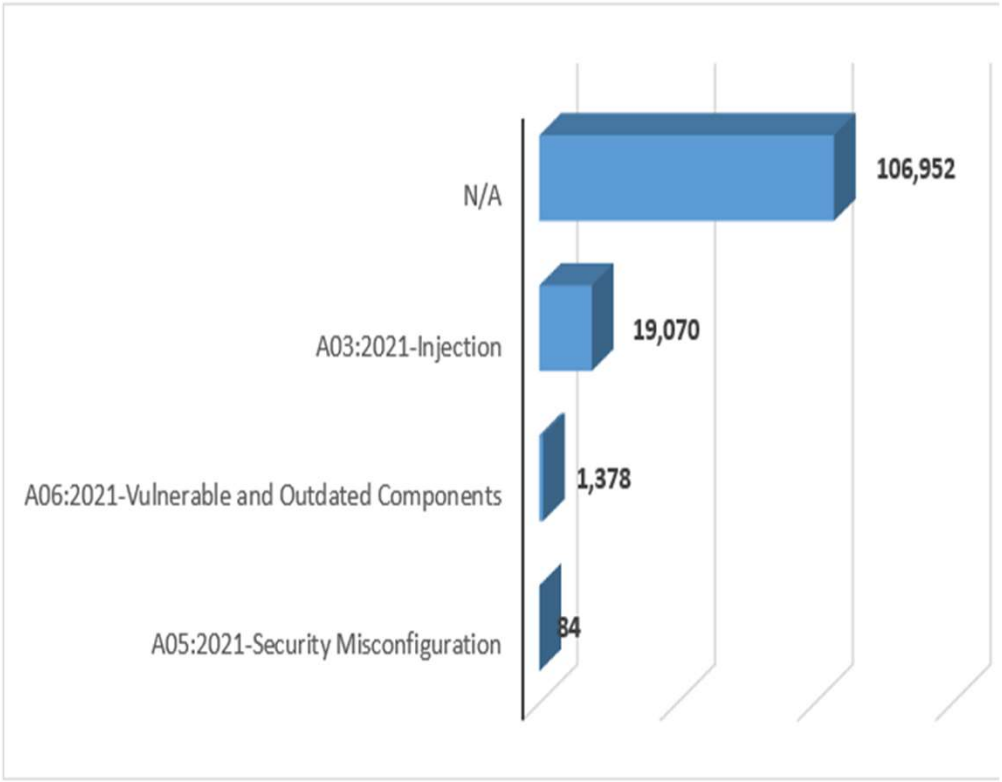
0,07%

84

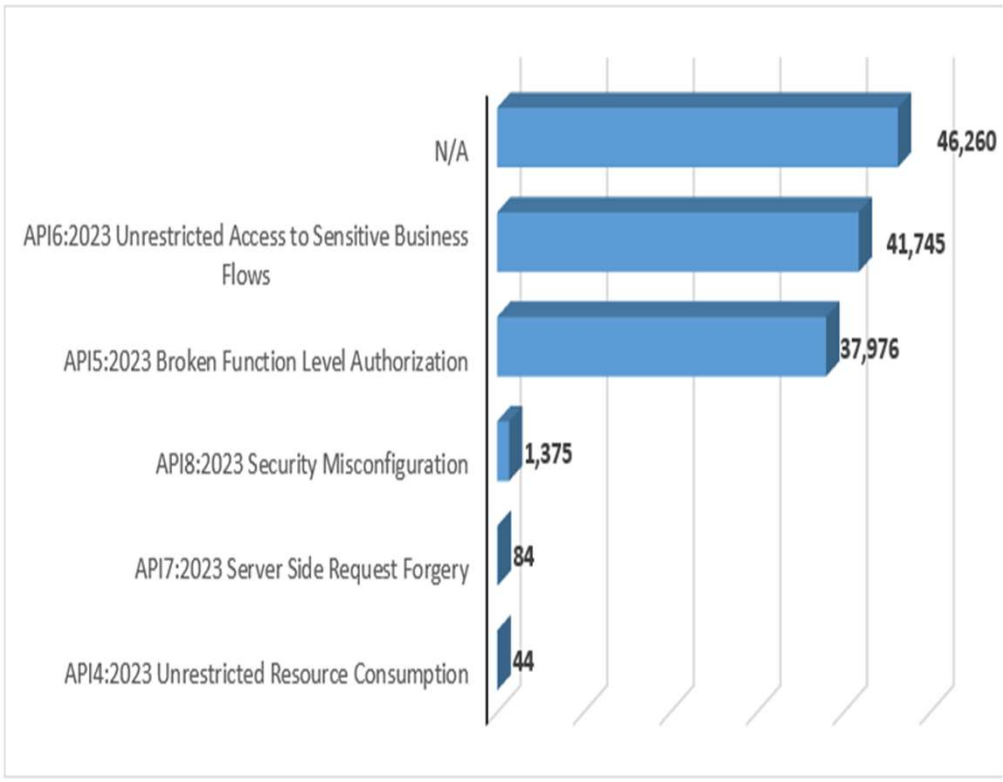
Custom Access

GENERAL WAF – FORTIWEB

OWASP TOP 10



OWASP API TOP 10



Actividades realizadas

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

Actividades diarias:

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

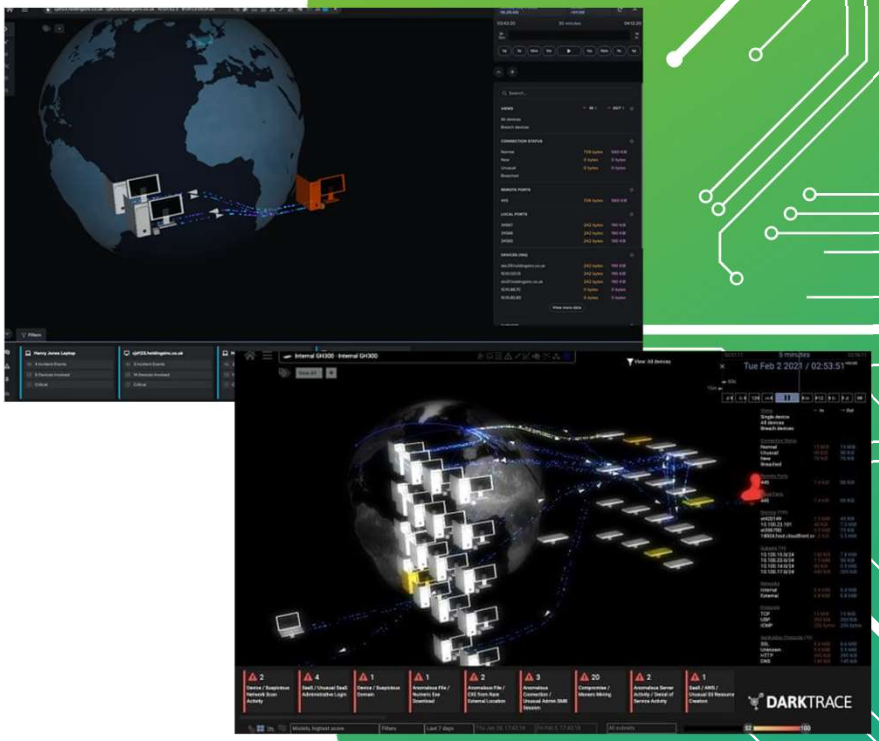
Actividades semanales:

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

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.



6.814
Dispositivos modelados

200
Subredes

826
Dispositivos en brechas

1.226
Brechas

133
Modelos

Informe solución Darktrace/Respond

2024

Objetivo

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

Alcance

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

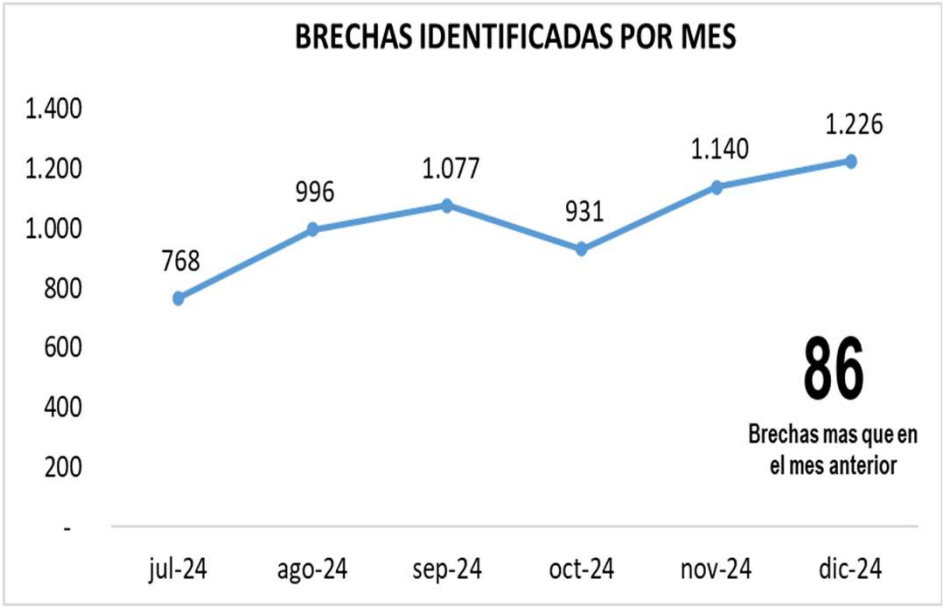
- Dar a conocer las estadísticas generales de la solución de Ciberdefensa.
- Presentar los modelos que se alertaron durante el periodo.
- Dar a conocer los sistemas identificados en los modelos presentados.
- Recomendaciones.

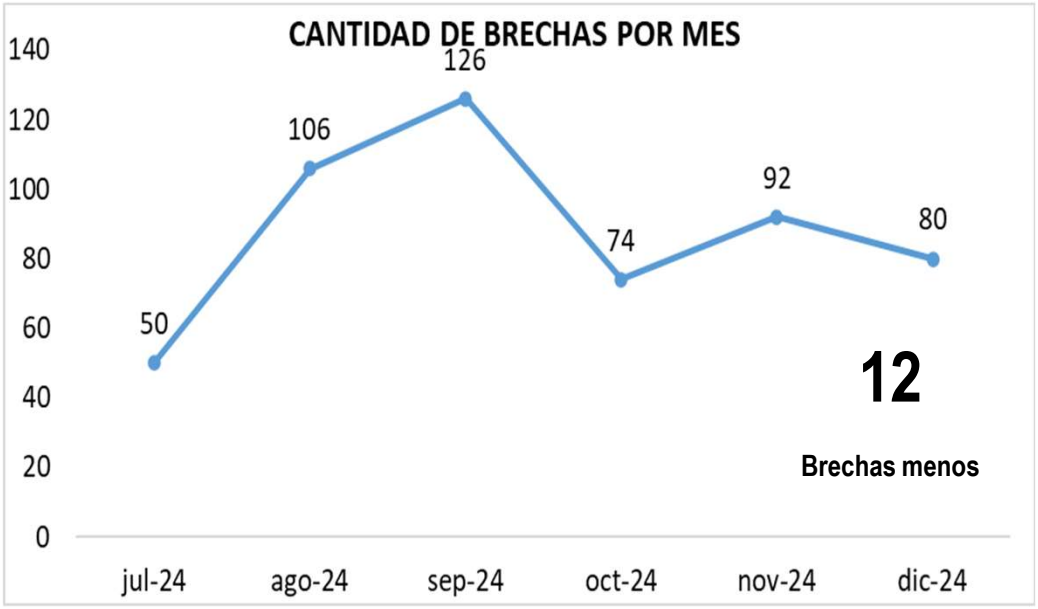
Distribución de Brechas

Brechas Darktrace/Detected

Modelos Darktrace/Respond

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



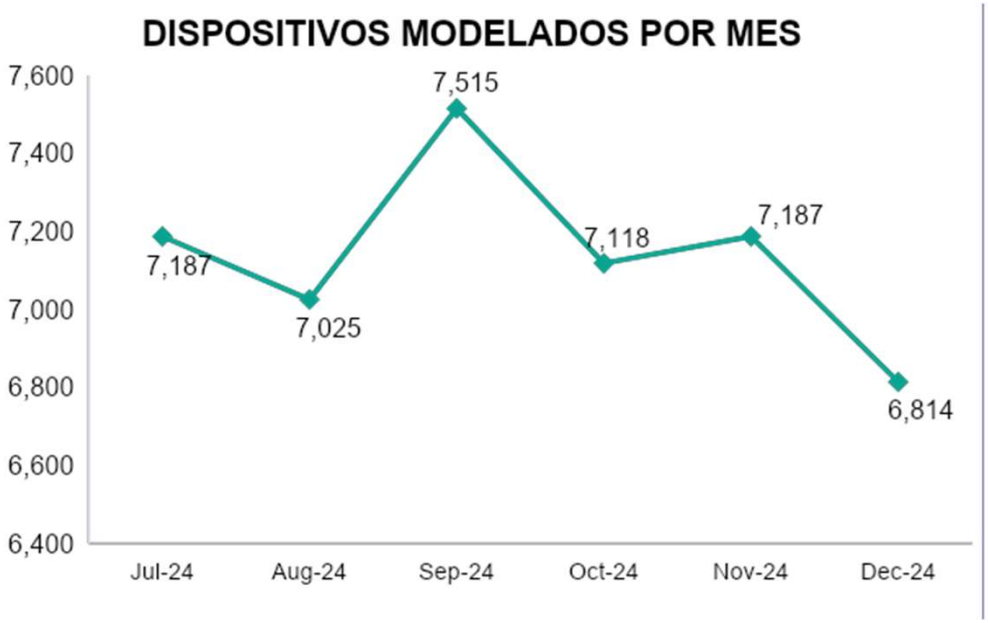


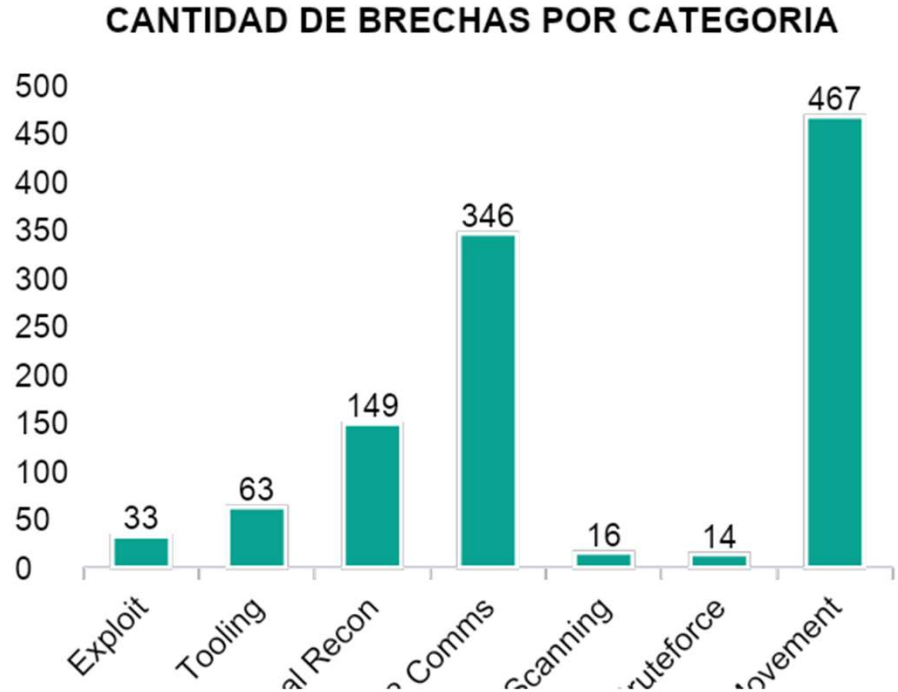
Brechas identificadas por categoría

Licenciamiento

Distribución de Brechas

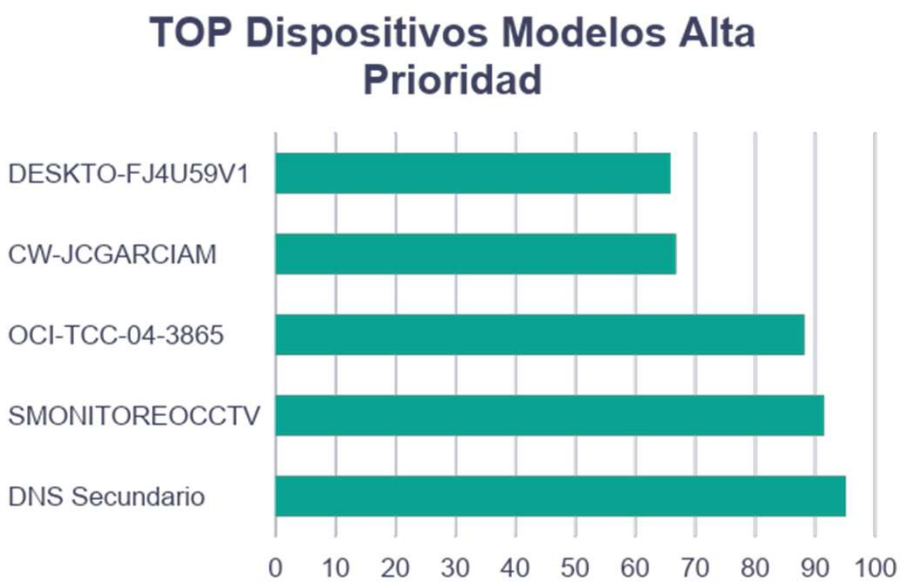
Los modelos de ciberdefensa se pueden organizar de acuerdo con la fase de ataque que es más probable que detecten. Los modelos de monitoreo de acuerdo con estas categorías pueden permitir que el patrón de comportamiento característico de un ataque en curso sea observado.





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



Equipo /Modelo
DNS Secundario
Network Scan
Suspicious Network Scan Activity
MONITOREOCCTV
Suspicious SMB Scanning Activity
HTTP to Suspicious Subdomain
Attack and Recon Tools
OCI-TCC-04-3865
Unusual Large Internal Transfer
CW-JCGARCIAM
Attack and Recon Tools
DESKTO-FJ4U59V1
Unusual Large Internal Transfer

Informe solución Darktrace/Email

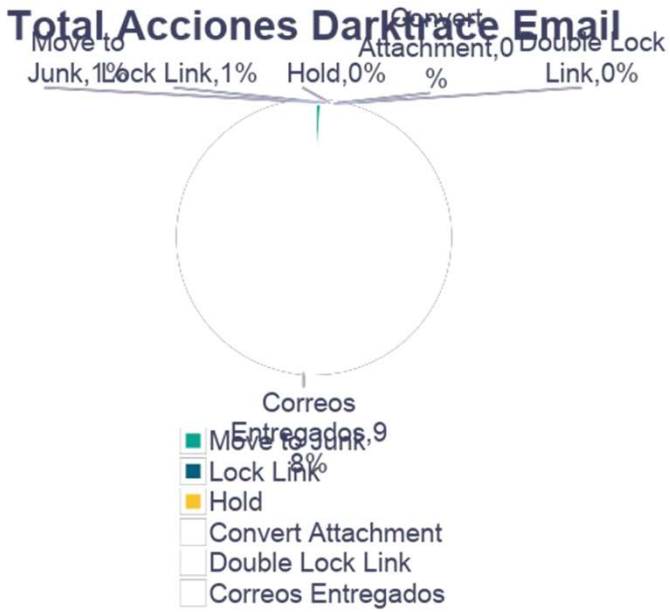
2024

274.516
Correos Entrantes

6.763
Correos con accion

267.753
Correos Entregados

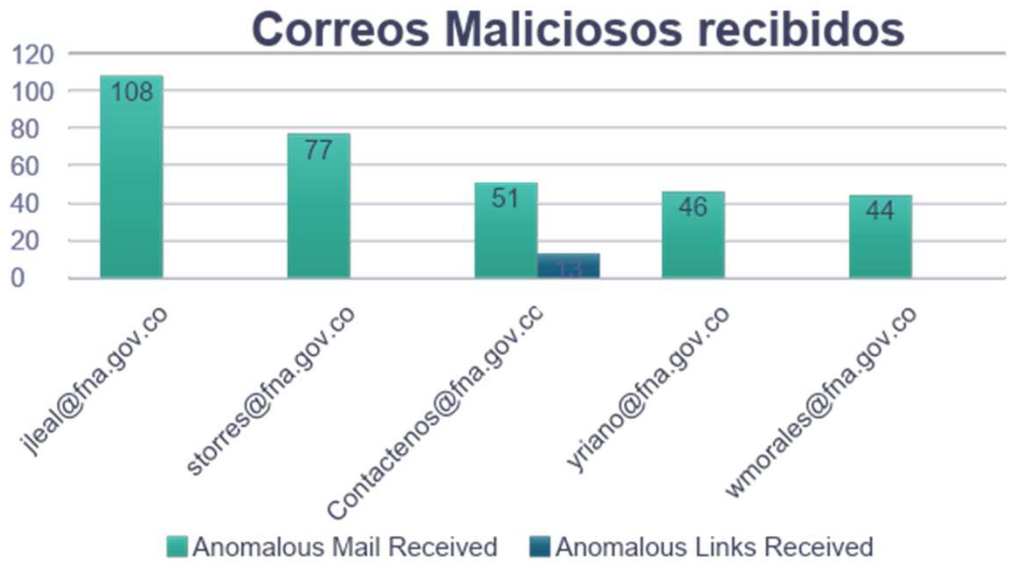
1.037.127
Correos Salientes



Top Acciones	Total, Acciones	% total de correos
Move to Junk	2.890	1%
Lock Link	1.915	0,7%
Hold	1.222	0,4%
Convert Attachment	425	0,2%
Double Lock LInk	311	0,1%

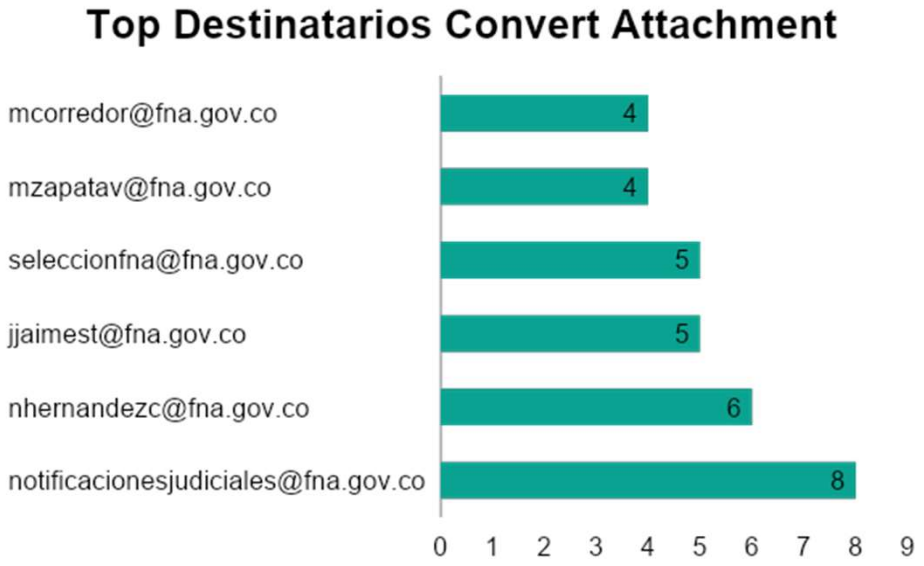
Administración Email

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

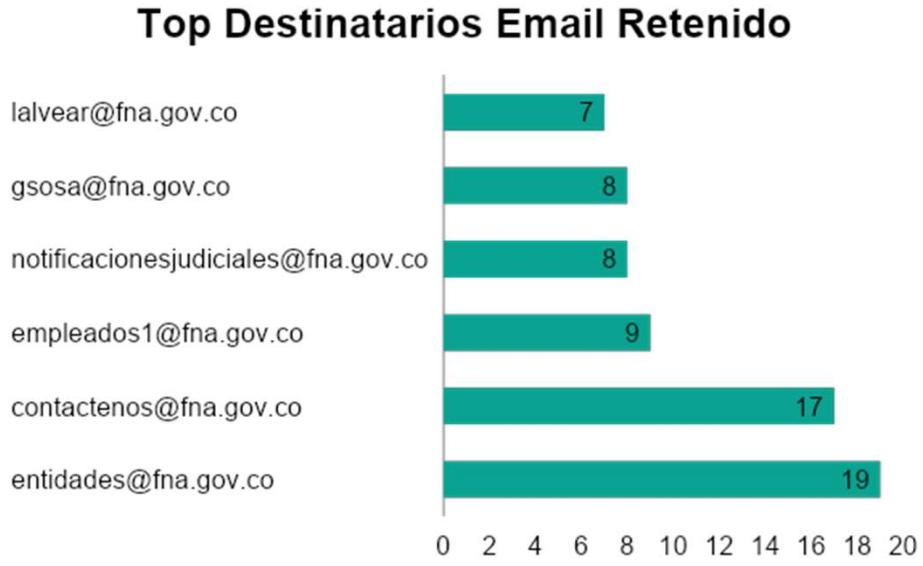


Administración Email

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

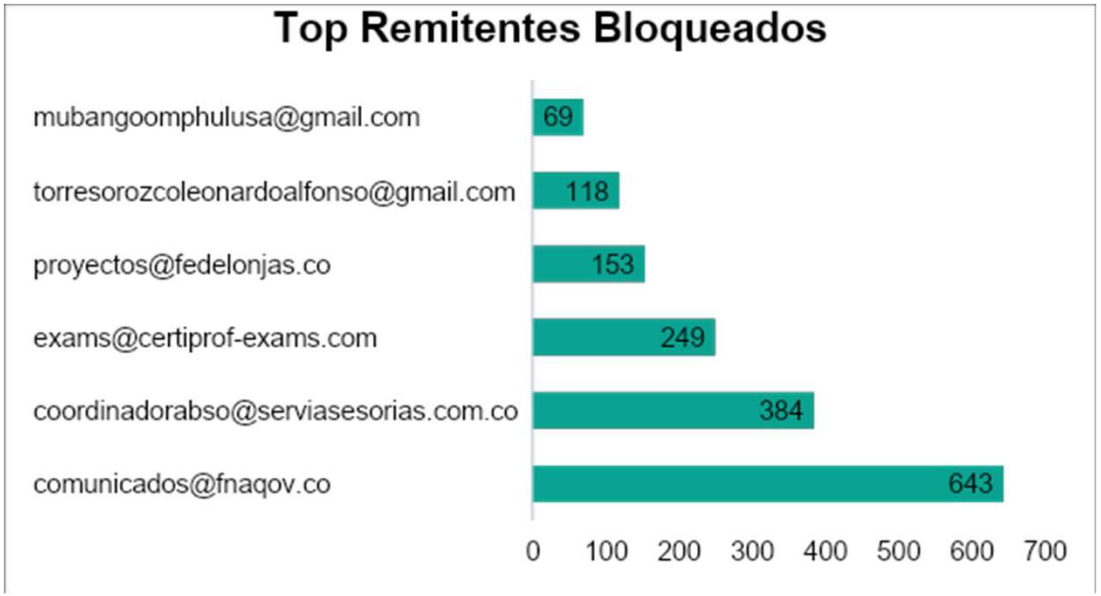


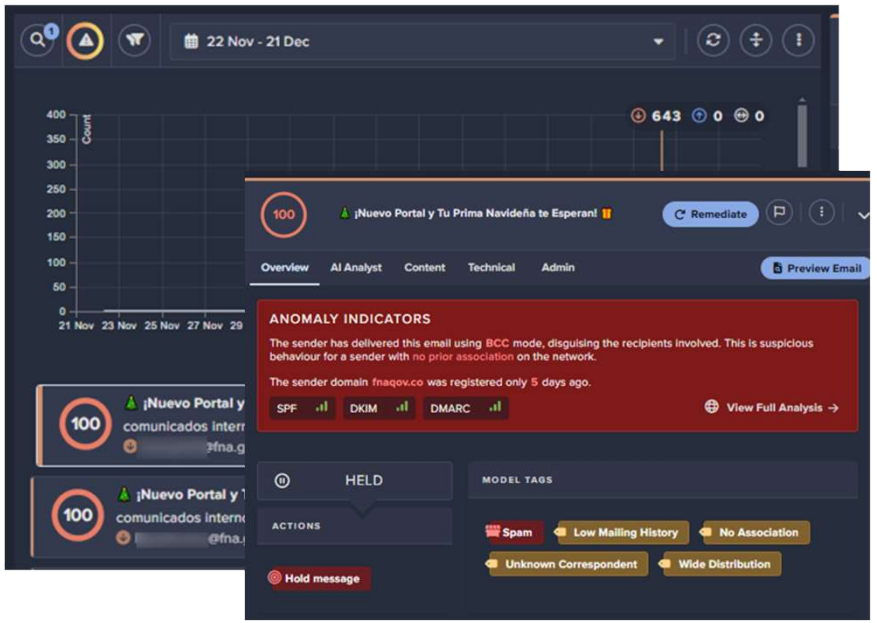
Destaca archivos adjuntos inesperados de corresponsales conocidos que pueden indicar que la cuenta de usuario del corresponsal externo ha sido comprometida



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.





Actividades realizadas

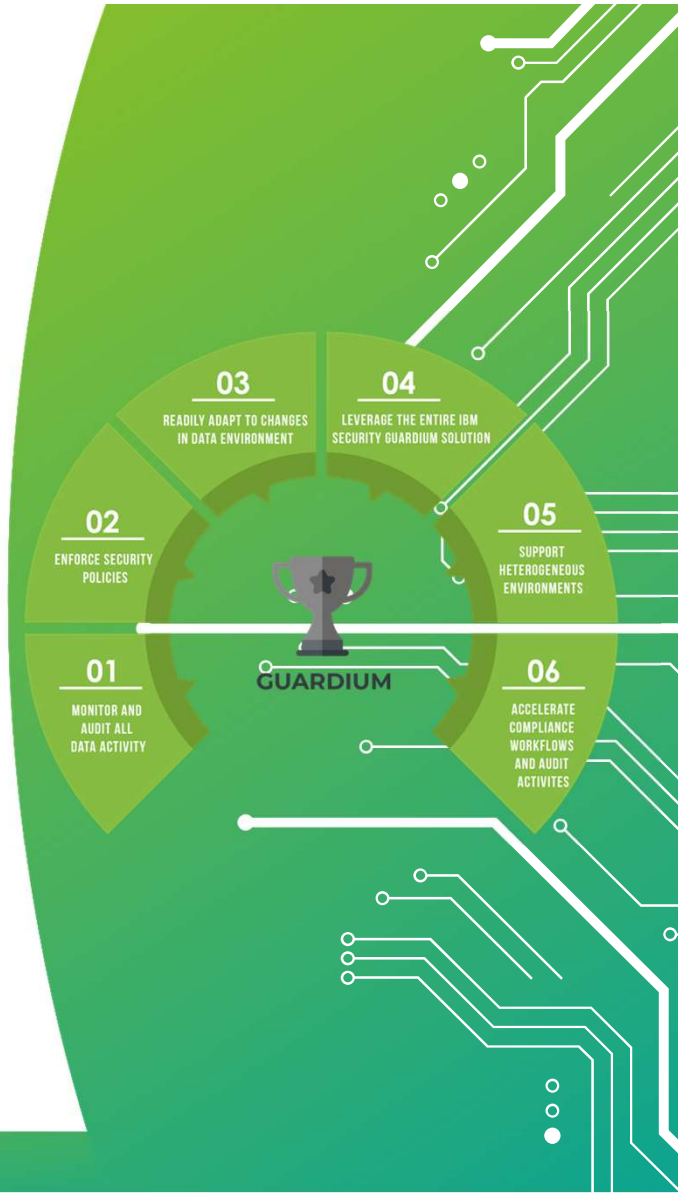
De acuerdo con los eventos generados en las diferentes herramientas y la gestión diaria dentro del FNA se dan las siguientes recomendaciones y conclusiones.

- Nombramiento de Subredes, de acuerdo con información suministrada por Redes.
- Se realiza Back up Semanal, el cual se conserva copia en el dispositivo de Darktrace y equipo administrador de la plataforma.
- Se realiza validación de los correos recibidos de la cuenta notaria2barranquilla@hotmail.com para facturacionelectronica@fna.gov.co, NO se evidencian correos
- Se genera reporte al área de seguridad informática para la validación de 382 correos del remitente coordinadorabso@serviasesorias.com.co
- Se crea modelo "FNA - Service Gateway Vigilancia puerto 80" para la vigilancia de las conexiones externas del equipo con direccion IP 172.16.125.250 (Service Gateway Trend Micro)
- Se envía listado de equipos con Agente de Darktrace instalado por Incidente IM157726 Generado por lentitud de la red
- Se realiza acompañamiento y validación de eventos para actividad de "Simulación ejercicio Ciberseguridad ante posibles amenazas digitales"
- Se genera reporte al área de seguridad de la información para la validación de los correos del dominio comunicados@fnaqov.co
- 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.

-

IBM Guardium

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 noviembre y el 21 de diciembre de 2024, la plataforma presentó estabilidad y normalidad en su operación.

Actividades macro ejecutadas	Actividades a ejecutar
• Solicitud información planes SAP HANA/COBIS. • Seguimiento a política COBIS. • Múltiples eventos base de datos COBIS. Relay correo. • Despliegue parches seguridad. • Corrección certificados próximos vencer.	• Configuration Audit System(agente). • Seguimiento reglas COBIS producción. • Monitoreo y reglas alcance negocio. • Validación y ajuste sobre políticas de seguridad. • Alertamiento SOC

NA_Basic
ata Security
olicy

En comparación con el periodo pasado, la regla para **XSS** aumentó un aproximado de 3 veces su valor. Para la regla **Data Exfiltration**, el aumento fue de 1.5 veces con el valor anterior, para las regla de **OS Command Injection** se duplicó, y para **SQL Injection - Tautology,** aumentaron un aproximado de 4 veces.

Regla	Cantidad de eventos
Cross-Site Scripting (XSS)	13407
Data Exfiltration	237123
OS Command Injection	2833
SQL Injection - Tautology	27752

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

Usuario de base de datos	Cross-Site Scripting (XSS)	Data Exfiltration	OS Command Injection	SQL Injection - Tautology
ADMESCOBARR		4	4	1
ADMINET		1		12
BE2IN_CERT				66
BIZAGICERT	1	163		
BIZAGIDEV		395	2	
BOGPVPPWP023\CTS_BV (OS USER)		99		
CNX_COBISNS		32		
CNX_SMPRE				16
CNXAFILIACIONESDIGITALESDBO_P				3
CNXCCONTROLGARANTIAS				39
CNXCONTROLGARANTIAS		765		2832
CNXNOTIFICACIONES_C	59			
CNXNOTIFICACIONESDBO_P	20			
CNXRADICACIONDBO_C	39			



NA_Data Privacy - PII

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

Usuario de base de datos	Failed Login - Alert if repeated	Grant Commands, PII Objects - Log INFO	Uncommon real traffic	Uncommon other
ADMCAT	2			
ARCSIGTH	3			
CNX_COBISNS	3916			
CNX_MON_ASEPROD	971			
CNXQRADAR	13			
COBISCTS3	980			
COBROJUR	54386			
CPPALACIOSR	1		2	
ESBFILE	1			
ETLSYB	137			
FNA2\SQLSERVICEPRO				4
GESTIONTRASLADOS	3			
HPAPM	1			
INTRANETPOOL	411			
JEMORENOR				1
LJOPEREZQ			2	1
OPCRUZ	8			
SA		900	3	68
SIMULADOR	119			

Política
signación
oles

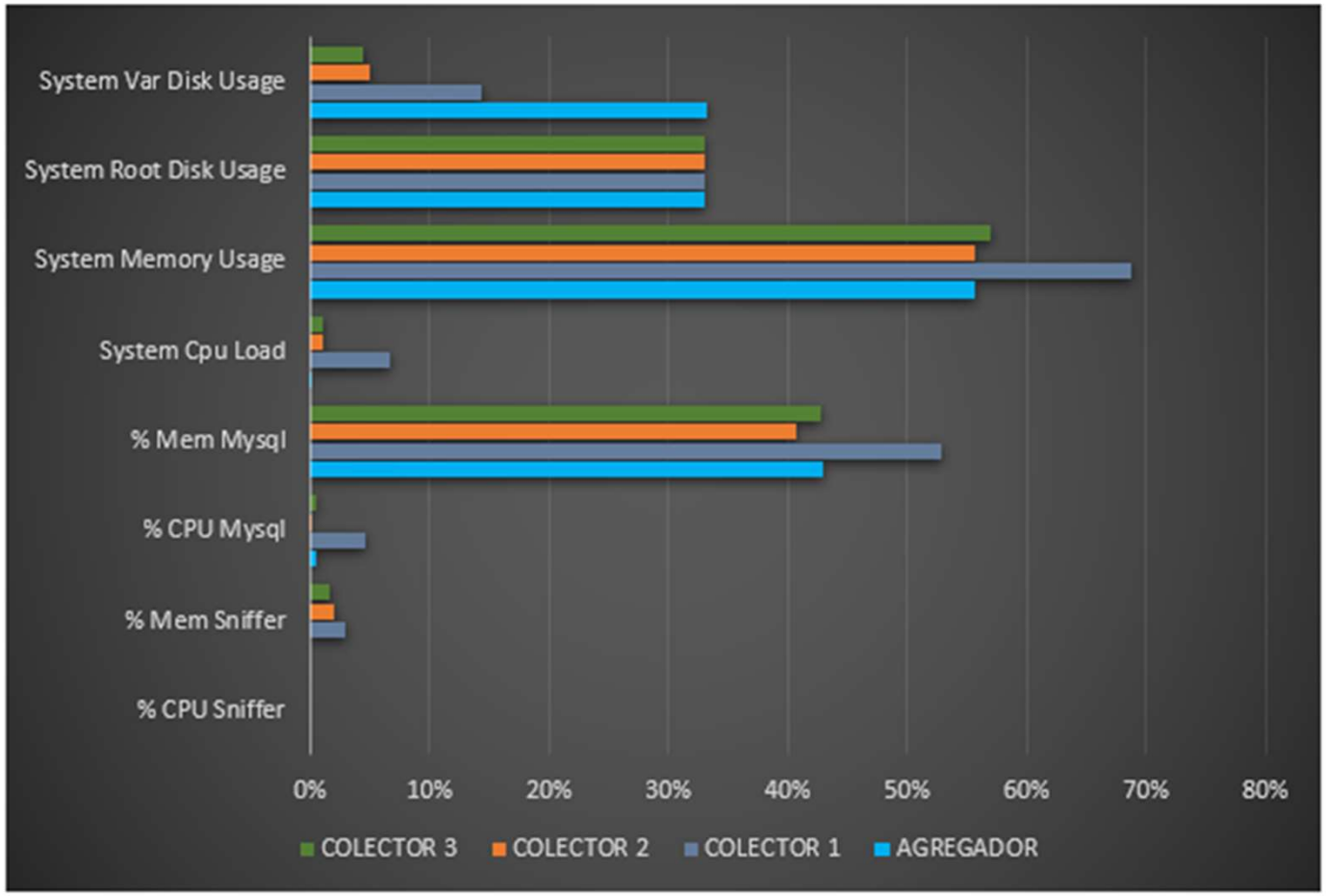
COBIS

239 ejecuciones de asignación/eliminación de roles, para usuarios de aplicación

SAPHANA

84 ejecuciones de asignación/eliminación de roles, para usuarios de aplicación

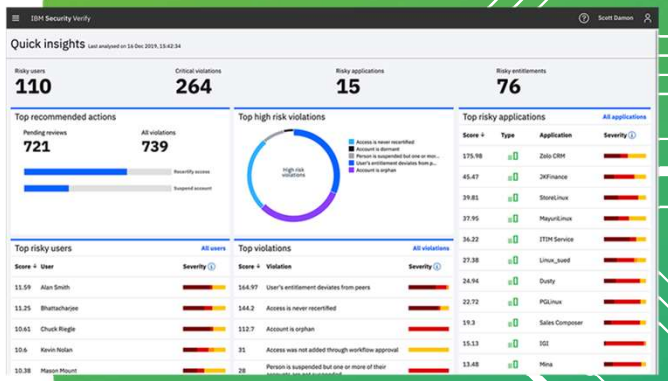
Comportamiento plataforma, 22 de noviembre al 21 de diciembre de 2024



IBM Security

Verify

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



Autenticación avanzada, incluida la autenticación sin contraseña

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

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.

Para las nuevas Integraciones

Se realizó la reunión de validación técnica para la integración de Verify con Vigia el 20 de noviembre donde el ingeniero de Vigía nos confirma que no tienen Webservices y por lo tanto se debe hacer la integración a través de la conexión directa con la base de datos.

Quedan programadas reuniones de validación técnica para integración con el sistema de Turnos el 25 de noviembre y con el sistema E-Finac para el 27 de Noviembre

Operaciones realizadas por Verify

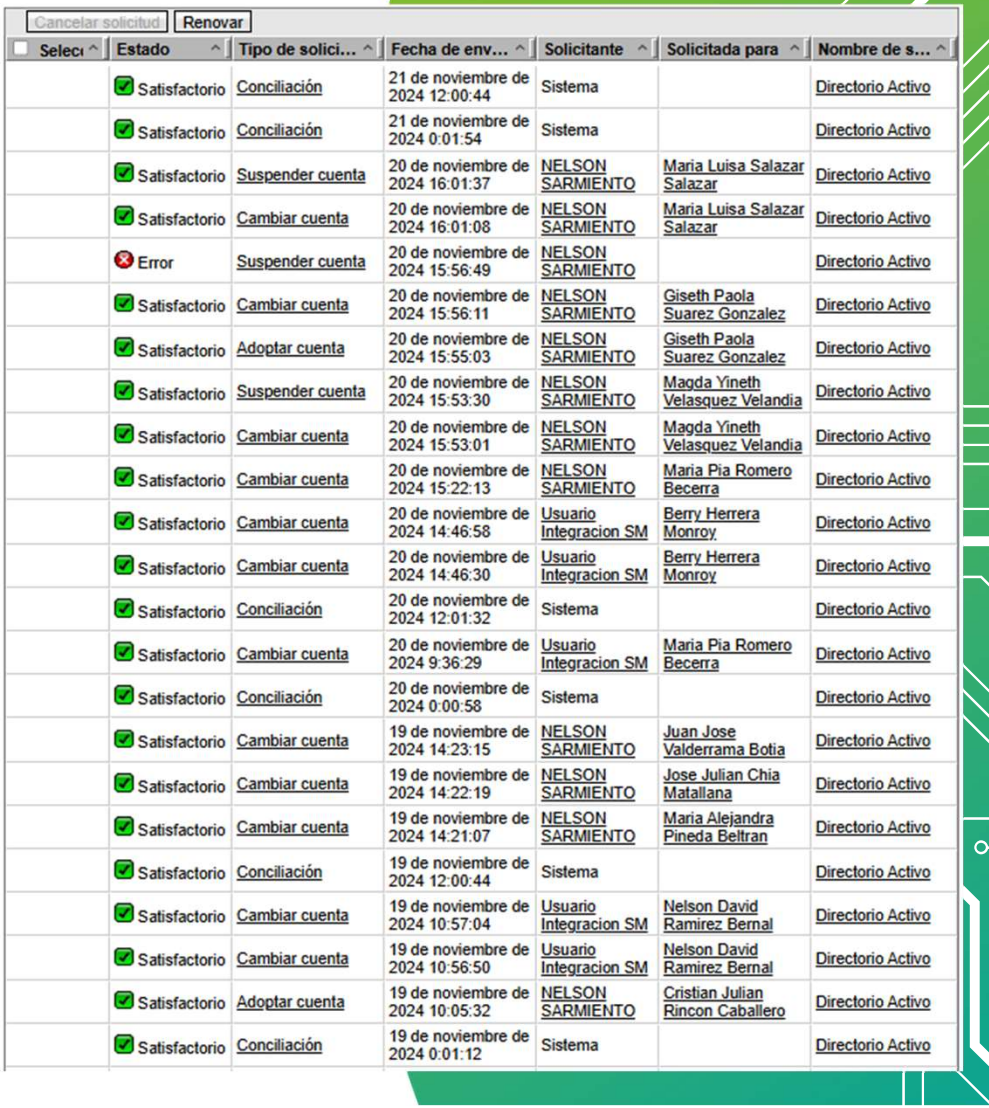
En el periodo de octubre 22 a noviembre 21 Verify realizo un total de 8052 operaciones discriminadas por servicios de acuerdo con el siguiente cuadro:

Total de operaciones realizadas por Verify entre Octubre 22 a Noviembre 21 de 2024

Servicio	*Cambiar contraseña*	*Crear cuenta*	*Modificar cuenta*	*Restaurar cuenta*	*Suprimir cuenta*	*Suspender cuenta*	*Total por Servicio*
Directorio Activo	1443	30	291	568	1	623	2956
SAP	0	76	68	301	0	339	784
Service Manager	0	30	291	568	0	623	1512
Verify	1557	26	4	576	4	629	2796
					Total Operaciones Solucion		**852**

Directorio Activo

Para el periodo de octubre 22 a Noviembre 21 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

Selecc	Estado	Tipo de solici...	Fecha de env...	Solicitante	Solicitada para	Nombre de s...
	Satisfactorio	Conciliación	21 de noviembre de 2024 12:00:44	Sistema		Directorio Activo
	Satisfactorio	Conciliación	21 de noviembre de 2024 0:01:54	Sistema		Directorio Activo
	Satisfactorio	Suspender cuenta	20 de noviembre de 2024 16:01:37	NELSON SARMIENTO	Maria Luisa Salazar Salazar	Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 16:01:08	NELSON SARMIENTO	Maria Luisa Salazar Salazar	Directorio Activo
	Error	Suspender cuenta	20 de noviembre de 2024 15:56:49	NELSON SARMIENTO		Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 15:56:11	NELSON SARMIENTO	Giseth Paola Suarez Gonzalez	Directorio Activo
	Satisfactorio	Adoptar cuenta	20 de noviembre de 2024 15:55:03	NELSON SARMIENTO	Giseth Paola Suarez Gonzalez	Directorio Activo
	Satisfactorio	Suspender cuenta	20 de noviembre de 2024 15:53:30	NELSON SARMIENTO	Magda Yineth Velasquez Velandia	Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 15:53:01	NELSON SARMIENTO	Magda Yineth Velasquez Velandia	Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 15:22:13	NELSON SARMIENTO	Maria Pia Romero Becerra	Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 14:46:58	Usuario Integracion SM	Berry Herrera Monroy	Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 14:46:30	Usuario Integracion SM	Berry Herrera Monroy	Directorio Activo
	Satisfactorio	Conciliación	20 de noviembre de 2024 12:01:32	Sistema		Directorio Activo
	Satisfactorio	Cambiar cuenta	20 de noviembre de 2024 9:36:29	Usuario Integracion SM	Maria Pia Romero Becerra	Directorio Activo
	Satisfactorio	Conciliación	20 de noviembre de 2024 0:00:58	Sistema		Directorio Activo
	Satisfactorio	Cambiar cuenta	19 de noviembre de 2024 14:23:15	NELSON SARMIENTO	Juan Jose Valderrama Botia	Directorio Activo
	Satisfactorio	Cambiar cuenta	19 de noviembre de 2024 14:22:19	NELSON SARMIENTO	Jose Julian Chia Matallana	Directorio Activo
	Satisfactorio	Cambiar cuenta	19 de noviembre de 2024 14:21:07	NELSON SARMIENTO	Maria Alejandra Pineda Beltran	Directorio Activo
	Satisfactorio	Conciliación	19 de noviembre de 2024 12:00:44	Sistema		Directorio Activo
	Satisfactorio	Cambiar cuenta	19 de noviembre de 2024 10:57:04	Usuario Integracion SM	Nelson David Ramirez Bernal	Directorio Activo
	Satisfactorio	Cambiar cuenta	19 de noviembre de 2024 10:56:50	Usuario Integracion SM	Nelson David Ramirez Bernal	Directorio Activo
	Satisfactorio	Adoptar cuenta	19 de noviembre de 2024 10:05:32	NELSON SARMIENTO	Cristian Julian Rincon Caballero	Directorio Activo
	Satisfactorio	Conciliación	19 de noviembre de 2024 0:01:12	Sistema		Directorio Activo

SERVICE MANAGER

Para el periodo de Octubre 22 a noviembre 21 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.

Con los ingenieros de Service Manager en reunión el 5 noviembre se revisan los flujos de las operaciones de retiro de usuarios ya que se estaban duplicando las tareas se hacen ajustes y se deja en monitoreo hasta la reunión del 12 de noviembre donde Liliana Miranda nos confirma que No se siguen duplicando las tareas.

SAP

Para el periodo de Octubre 22 a Noviembre 21 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.

Cobis

En el periodo del 22 de octubre al 21 de noviembre de 2024 se realizaron reuniones varias reuniones para seguir con la integración

Los días 23 de octubre, 30 de octubre y 1 de noviembre se realizan reuniónes con los ingenieros de Cobis donde se revisan los Web Services entregados en el periodo anterior, se realizaron pruebas exitosas.

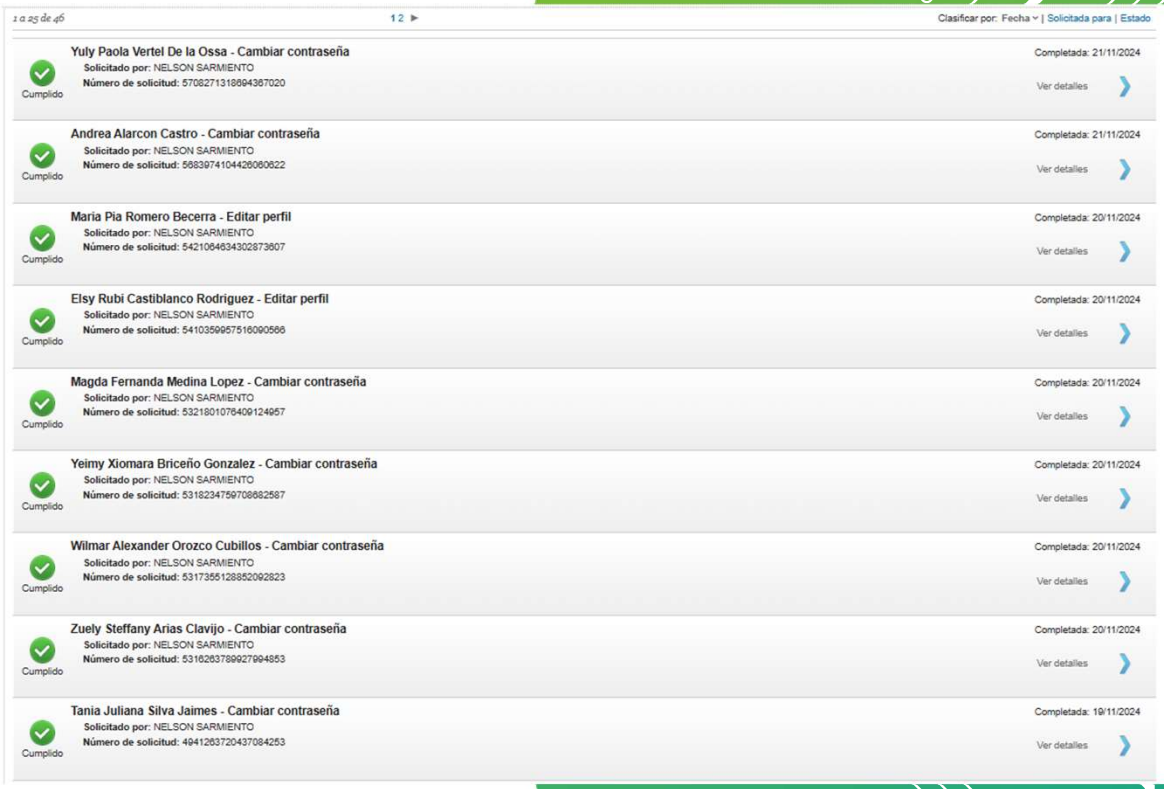
Los días 31 de octubre y el 12 de noviembre se realizan reuniones para verificar la arquitectura de la infraestructura de Cobis, donde se definieron los permisos que se deben solicitar para la conexión de los servidores de la solución de Verify y los servidores de Cobis; para estos permisos que creo el Cambio # C64364 el cual al día 22 de noviembre de 2024 se encuentra en el estado de Implementación.

ADMINISTRACIÓN DE USUARIOS

El martes 29 de octubre se realizó reunión con el equipo de administración de usuarios donde socializaron la documentación técnica y solicitaron la aprobación para iniciar a trabajar en las especificaciones técnicas del Backend, por parte del equipo de Verify se revisó y aprobó la documentación presentada, de parte del equipo de administración de usuarios inician con las tareas para la integración Verify – Administración de Usuarios.

AUTOGESTIÓN

Para el periodo de Octubre 22 a noviembre 21 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



Recomendaciones y conclusiones

Para este periodo se continúa 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 después del paso a producción.

Se programan reuniones técnicas con los equipos de Vigía y E-Finac para validación técnica de integración con Verify.

Se sigue con las pruebas para salida a producción de la integración con Cobis.

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

41
Eventos reportados

27
Identity Fraud

9
Data protection

5
Brand protection

Informe Monitoreo de marca

2024

Objetivo

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

Objetivos específicos.

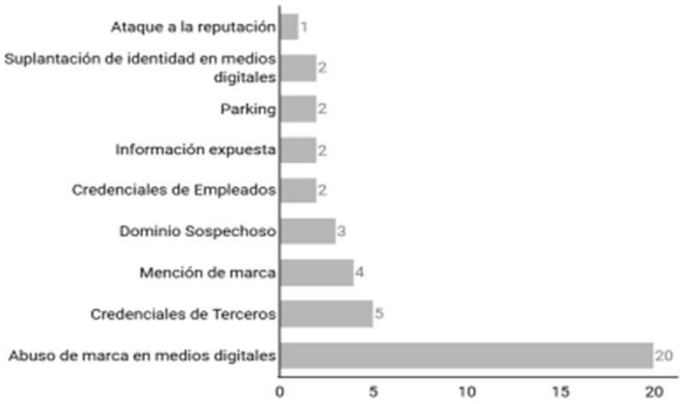
- Presentar los eventos identificados de acuerdo a las categorías y subcategorías definidas.
- Presentar los eventos que generen riesgo de manera inmediata a través de alertas en tiempo real.
- Identificar recomendaciones de mejora de acuerdo con los datos analizados.
- Presentar conclusiones relevantes.

Alcance

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

Resultados Monitoreo de Marca

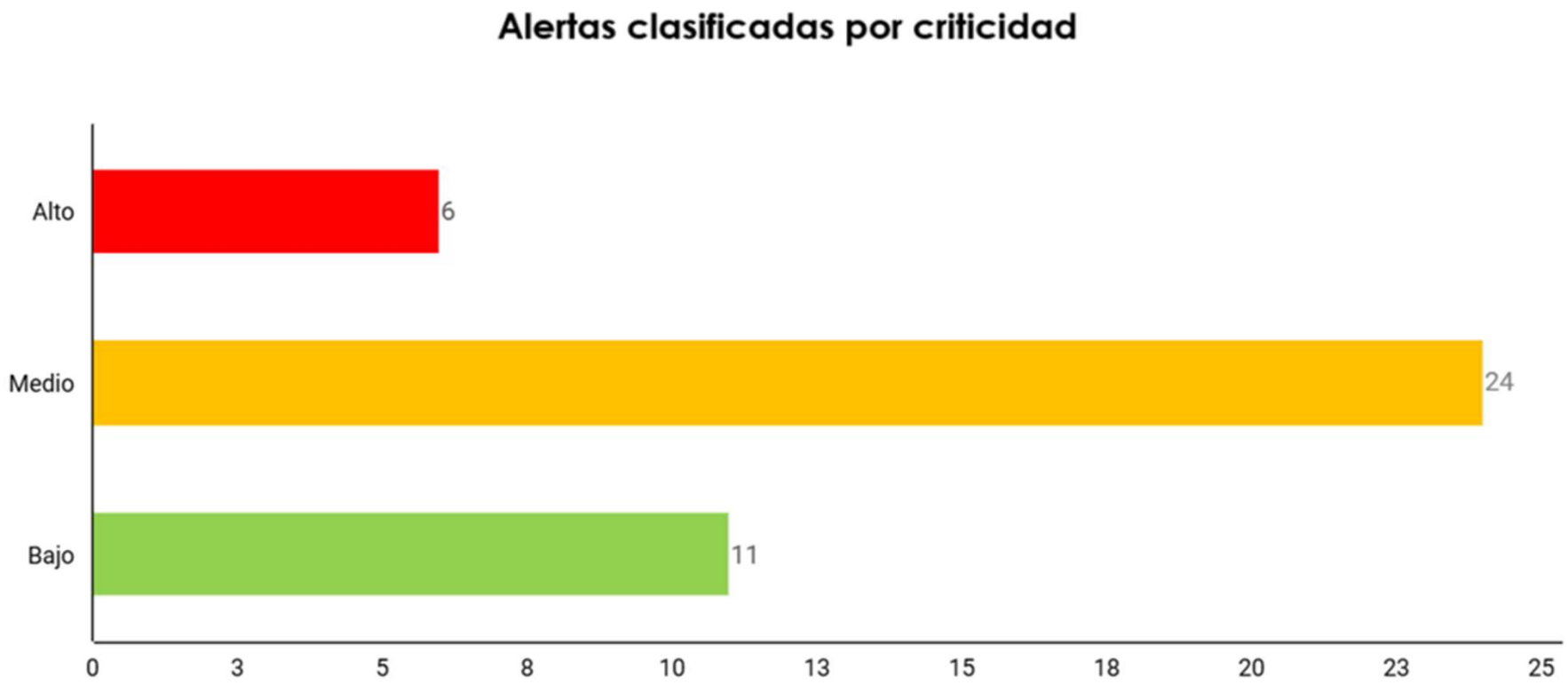




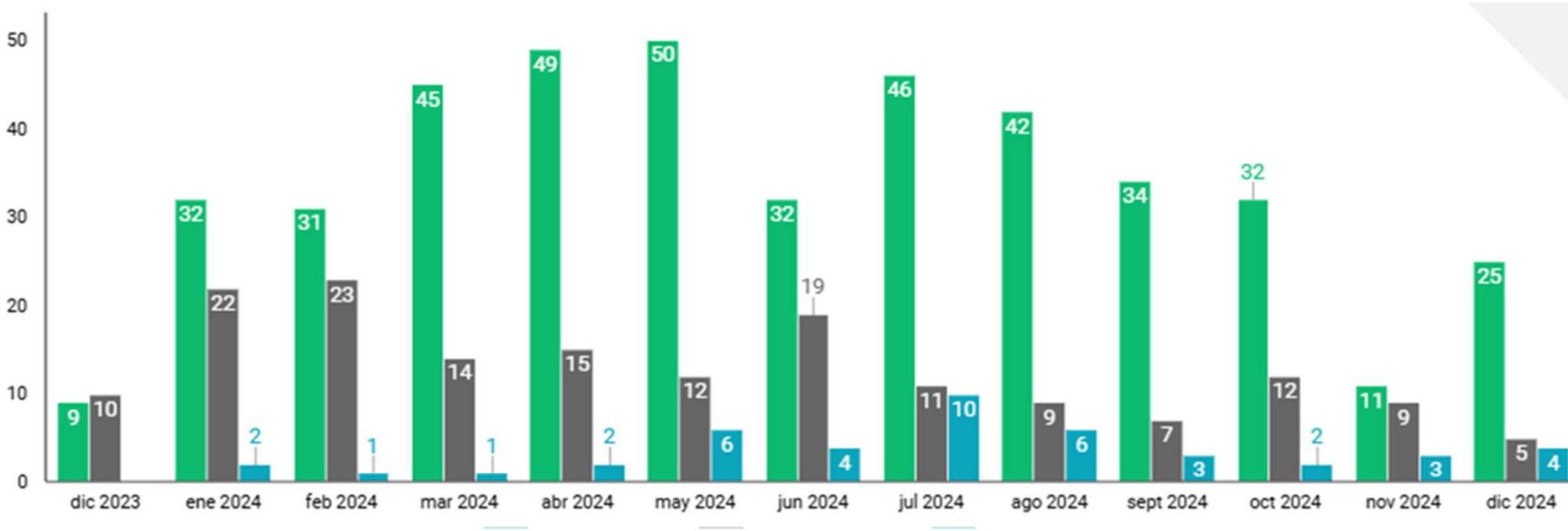
1. Comportamiento del servicio global Vigilancia



KPIs > Comportamiento del servicio global

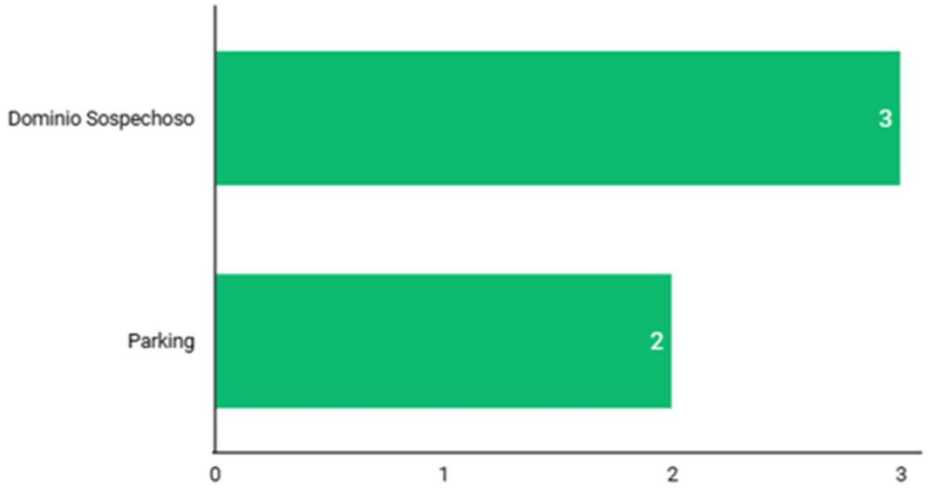


Evolución del servicio a nivel mensual

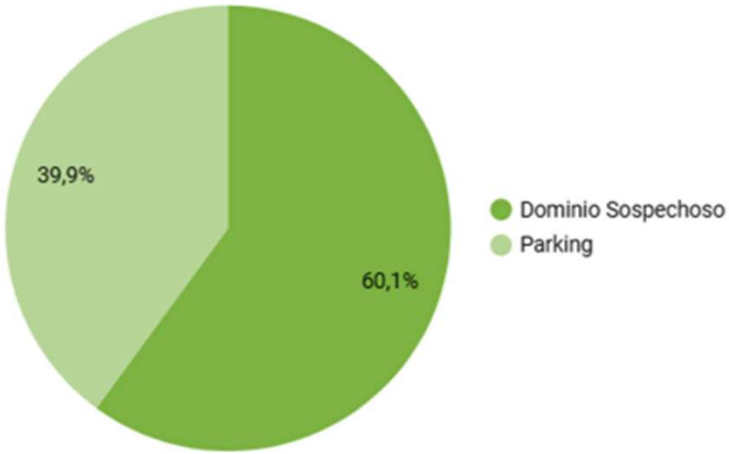


Resultados Monitoreo de Marca

Volumetría por tipo de dominio



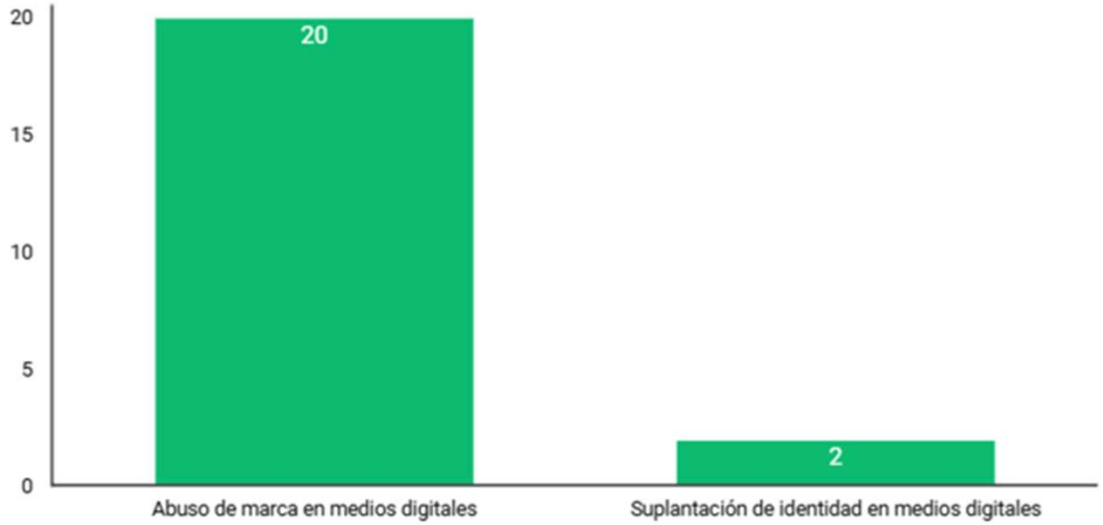
% de afectación por tipo de dominio

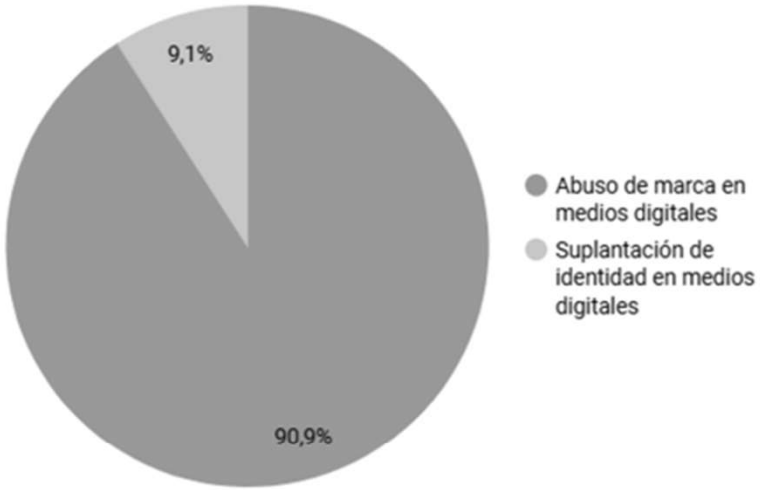


Resultados Monitoreo de Marca

2. Abuso de marca

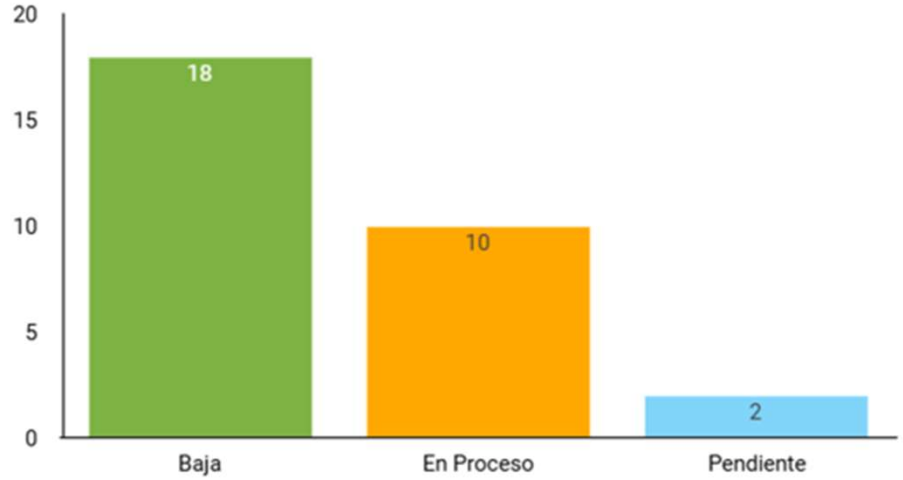
Se identificaron publicaciones en la red social de Facebook, haciendo referencia a ofrecimientos de servicios relacionados con el retiro cesantías y ofrecimientos de créditos en nombre del Fondo Nacional del Ahorro.

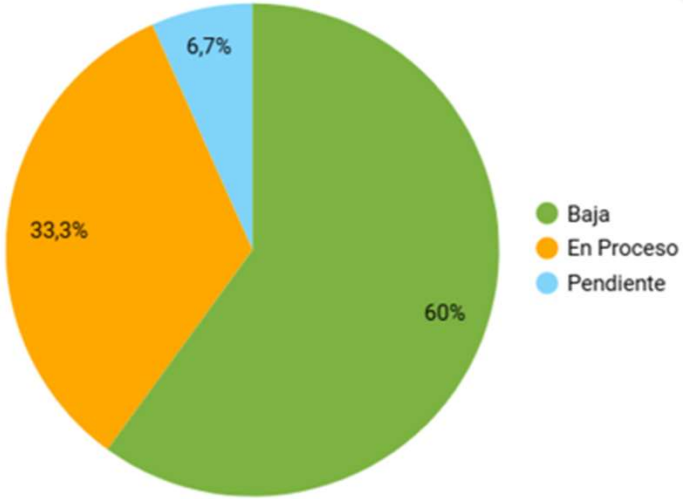




Resultados Monitoreo de marca

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.

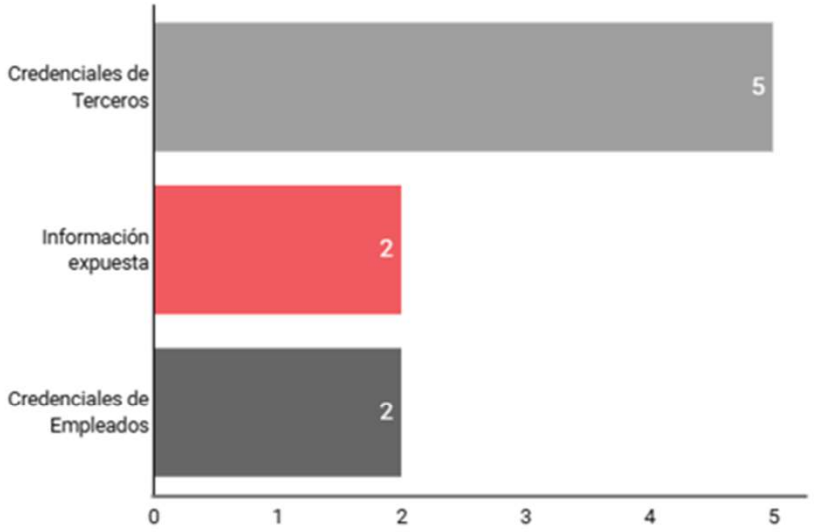
Sin gestión: Eventos sin gestionar. Pendientes de la solicitud del cliente.

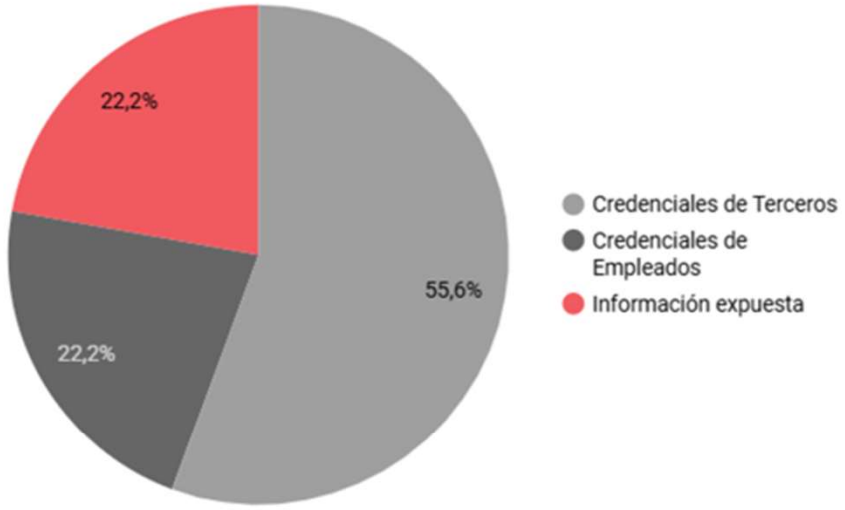
Resultados Monitoreo de marca

3. Información Expuesta – Credenciales filtradas

Volumetría por tipo de fuga

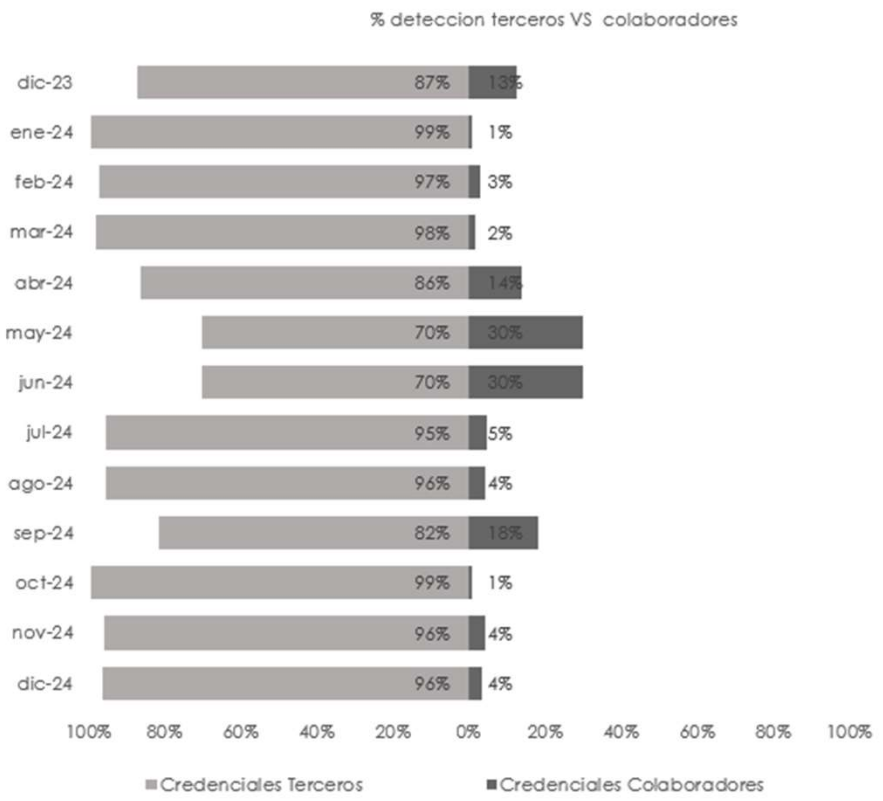
Nº Total de Alertas enviadas: 9

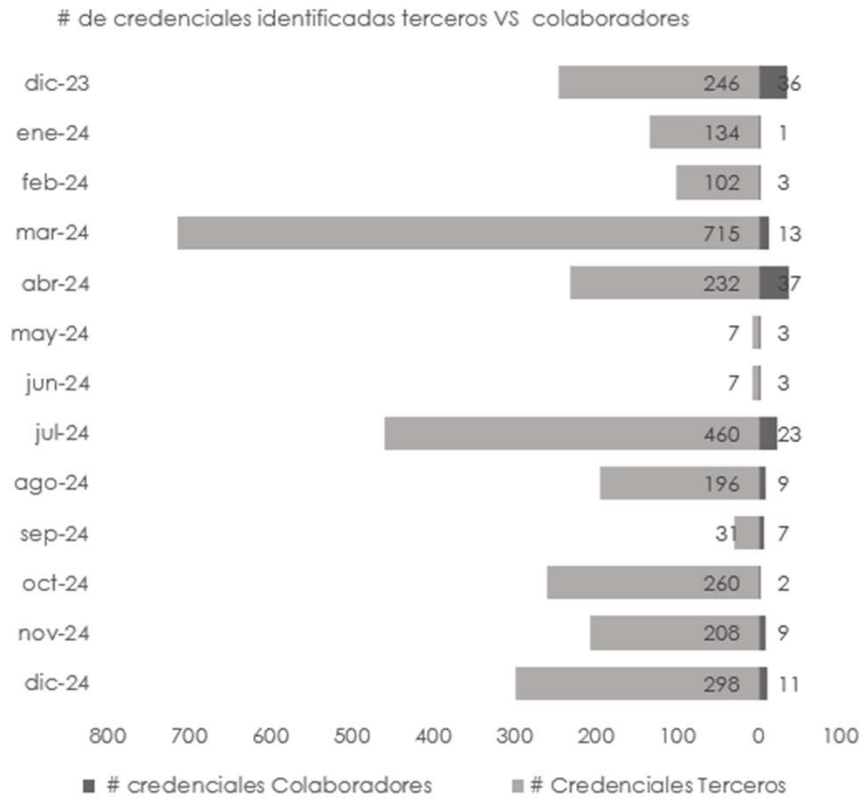




Resultados Monitoreo de marca

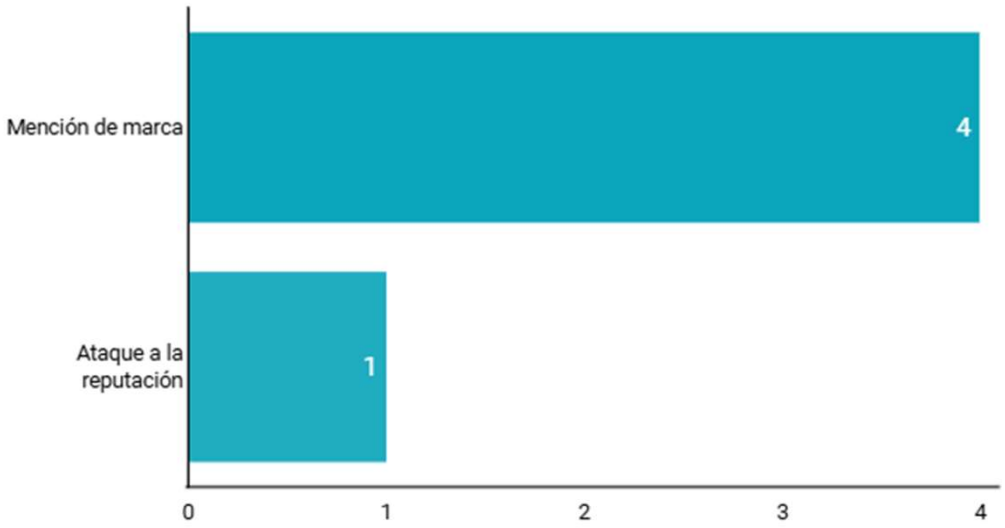
Histórico > Evolución del servicio a nivel mensual

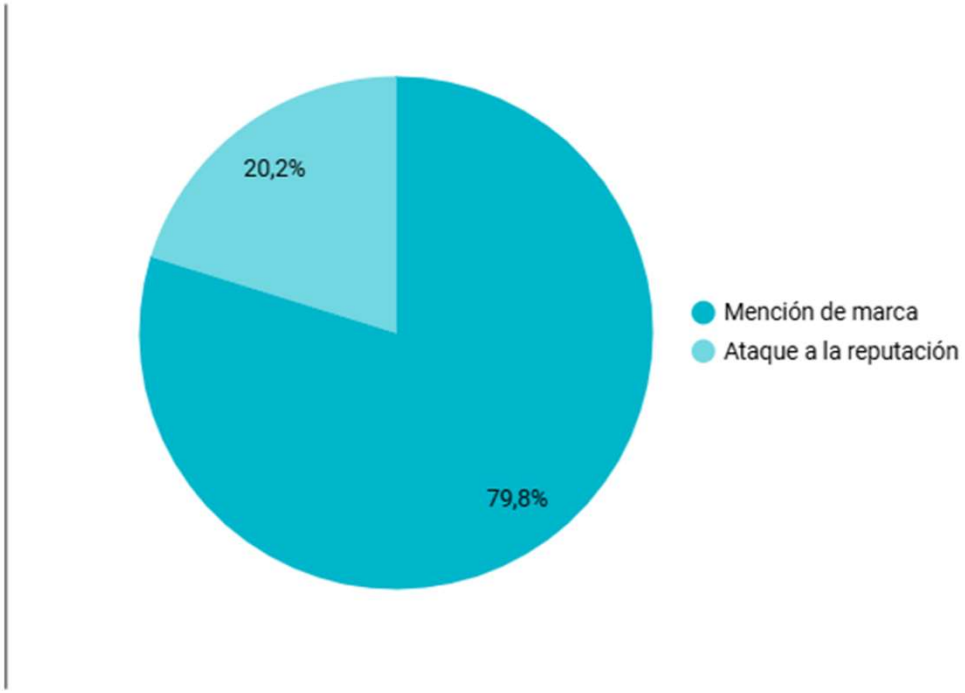




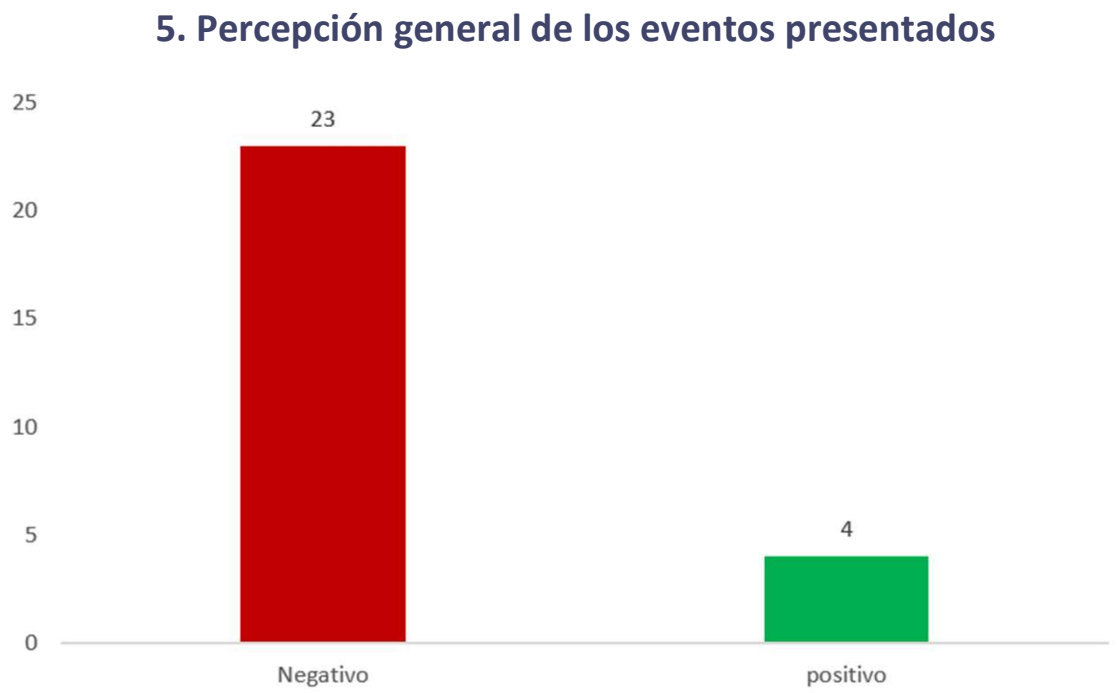
Resultados Monitoreo de marca

4. Menciones de marca





Resultados Monitoreo de marca



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

Actividades realizadas

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

Observaciones y conclusiones

Observación: Se evidencia un aumento en el volumen de credenciales identificadas para la tipología de credenciales de colaboradores.

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



Informe Seguridad Ofensiva

2024

Objetivo

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

Objetivos específicos

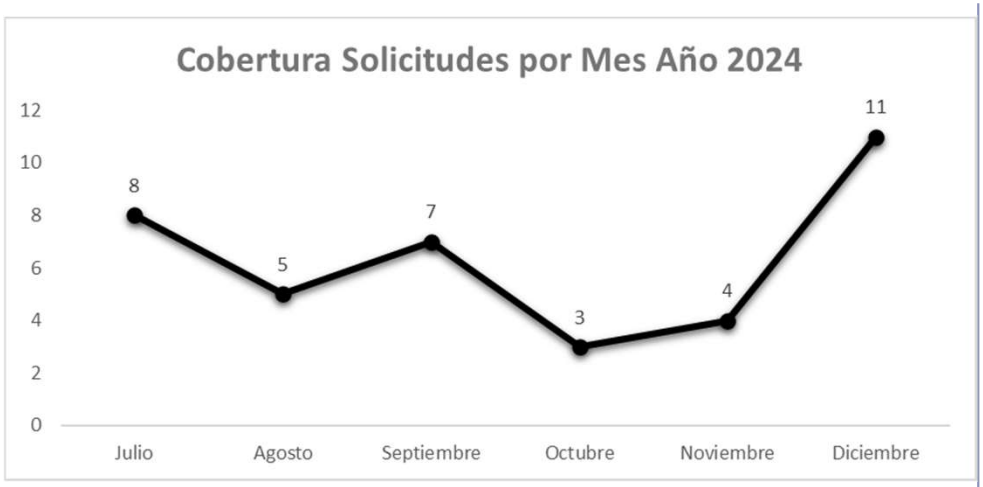
- Presentar las solicitudes recibidas y atendidas durante el periodo.
- Presentar las vulnerabilidades más relevantes.
- Identificar recomendaciones de mejora de acuerdo con los datos analizados.
- Presentar conclusiones relevantes.

Alcance

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

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

Durante el periodo evaluado, se documentaron un total de 11 solicitudes. Este número refleja un aumento de 7 solicitud en comparación con el periodo anterior, lo que indica una ligera mayor 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.

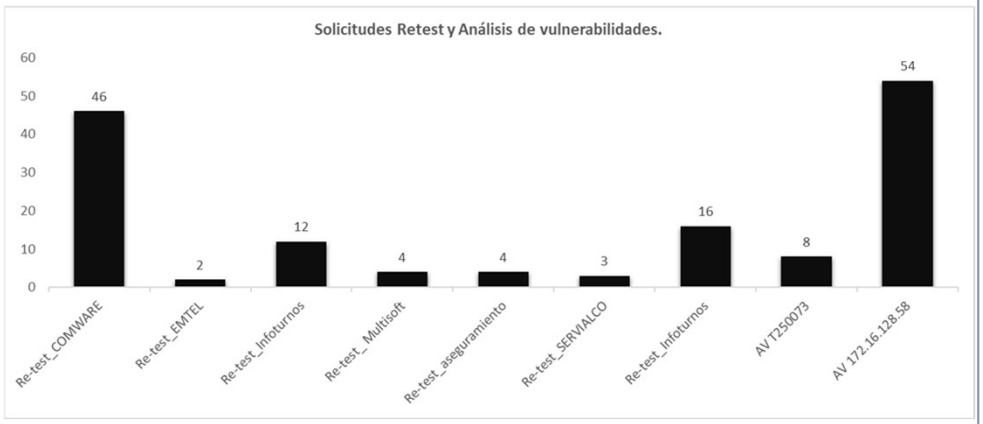


Durante el periodo reportado, se ejecutaron un total de 9 solicitudes de Retest relacionadas con análisis de vulnerabilidades (RAV), así como 2 análisis de vulnerabilidades adicional. Estas actividades tuvieron como objetivo verificar la remediación de las vulnerabilidades previamente identificadas y asegurar que las medidas correctivas implementadas fueran efectivas.

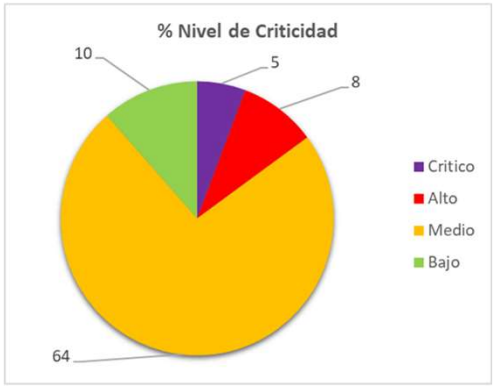
Resultados de solicitudes (Retest y AV)

Resultados Retest - General

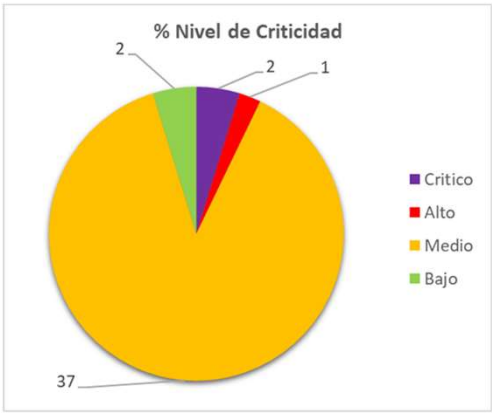
Resultados – De las solicitudes de Retest realizadas, se reportaron un total de **87** vulnerabilidades para su respectivo escaneo y validación. En cuanto a los escaneos iniciales en busca de vulnerabilidades se identificaron **62** hallazgos, los cuales fueron debidamente analizados y clasificados. 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.



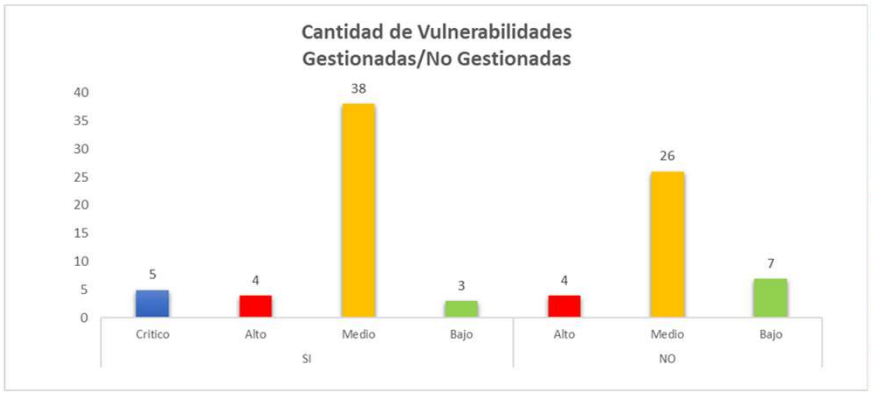
Resultados – A continuación, se presenta el porcentaje por nivel de criticidad de las vulnerabilidades identificadas durante los ejercicios de **análisis de vulnerabilidades** reportados.



Resultados de solicitudes (Retest y AV)

Resultados Retest y Análisis de Vulnerabilidades Remediadas - General

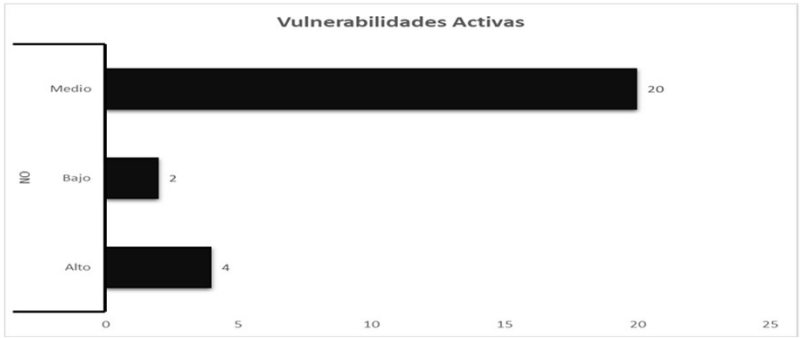
De las **87** vulnerabilidades reportadas en los re-test, **50** fueron remediadas y **37** continúan activas.

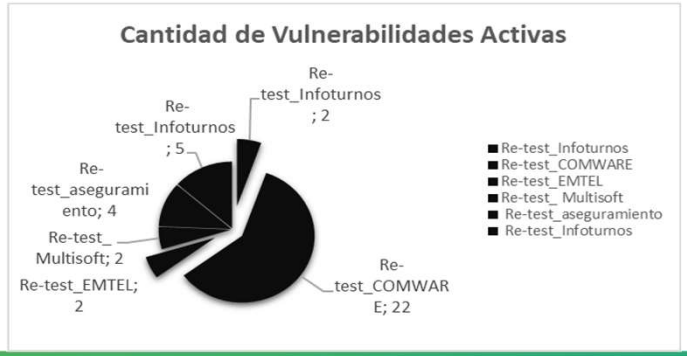


SI	50
Critico	5
Alto	4
Medio	38
Bajo	3

NO	37
Alto	4
Medio	26
Bajo	7
Total	87

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

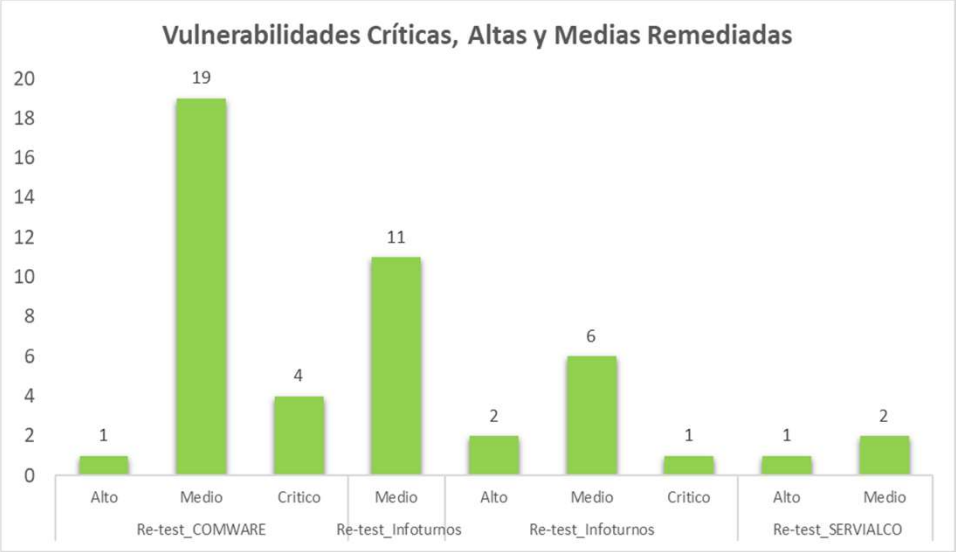




Resultados de solicitudes (Retest y AV)

Resultados Retest AV Remediadas - General

De las **50** vulnerabilidades remediadas se destaca la efectividad de solución de las medias.



Del total de **vulnerabilidades activas (37)** los activos que se destacan con **más vulnerabilidades** son 172.16.128.58 **(13 vuln)**, 172.16.124.157 **(9 vuln)** y 172.16.127.100 **(5 vuln)** los activos identificados hacen parte de la administración de Comware.

Host	Alto	Medio	Bajo	Total
172.16.132.147	0	0	1	1
172.16.132.149	0	0	1	1
172.16.132.126	0	2	0	2
172.16.132.124	0	2	0	2
172.31.1.128	0	2	0	2
172.16.123.227	0	2	0	2
172.16.127.100	0	2	3	5
172.16.124.157	0	8	1	9
172.16.128.58	4	8	1	13

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 22112024_COMWARE
  - Re-test 26112024_COMWARE
  - Re-test_27112024_Infoturnos
  - Re-test EMTEL_29112024
  - Re-test 02122024 - Multisoft
  - Re-test 03122024_aseguramiento
  - Re-test 04122024_COMWARE
  - Re-test 16122024_SERVIALCO
  - Re-test 17122024_Infoturnos

- A continuación, se listan las actividades realizadas en los análisis de vulnerabilidades.

  - AV T250073
  - test 172.16.128.58

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 15 a 30 en comparación con el mes anterior. En total, se gestionaron 87 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

- Ambas vulnerabilidades presentan un nivel de impacto crítico y afectan a múltiples activos dentro de la infraestructura auditada. Se recomienda abordar estas vulnerabilidades de manera prioritaria para mitigar posibles riesgos de seguridad.
- Las actividades de re-test se realizaron en diversas plataformas bajo la responsabilidad de Comware, Infoturnos, Multisoft y Servialco, lo que permitió asegurar que las vulnerabilidades detectadas fueran evaluadas en el contexto particular de cada sistema.

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 noviembre y el 21 de diciembre.

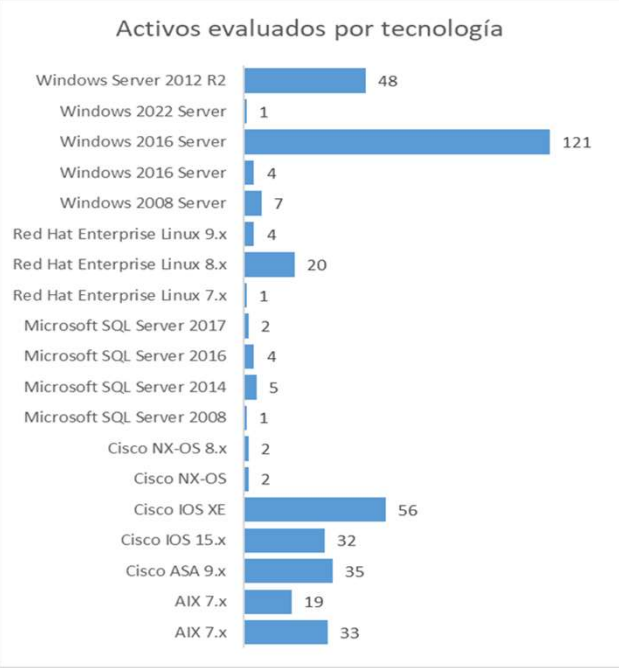
Objetivos

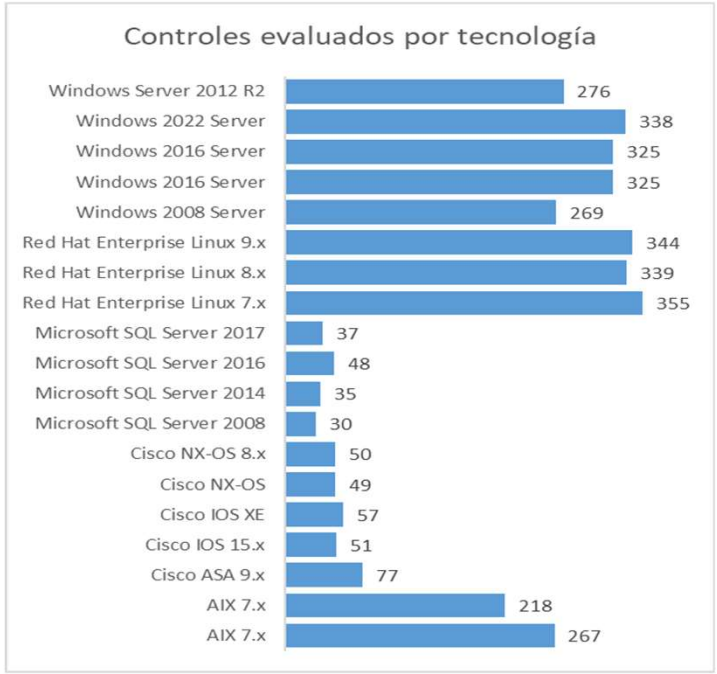
- Evaluar los controles comprendidos en las 18 políticas desplegadas.
- Analizar el nivel de riesgo que representa el incumplimiento de los controles de seguridad planteados por el CIS.
- Presentar un insumo de valor para la toma de decisiones en cuanto a la aplicación de controles de seguridad en los activos tecnológicos.
- Cumplir con estándares y regulaciones de seguridad de la información.

RESUMEN GENERAL

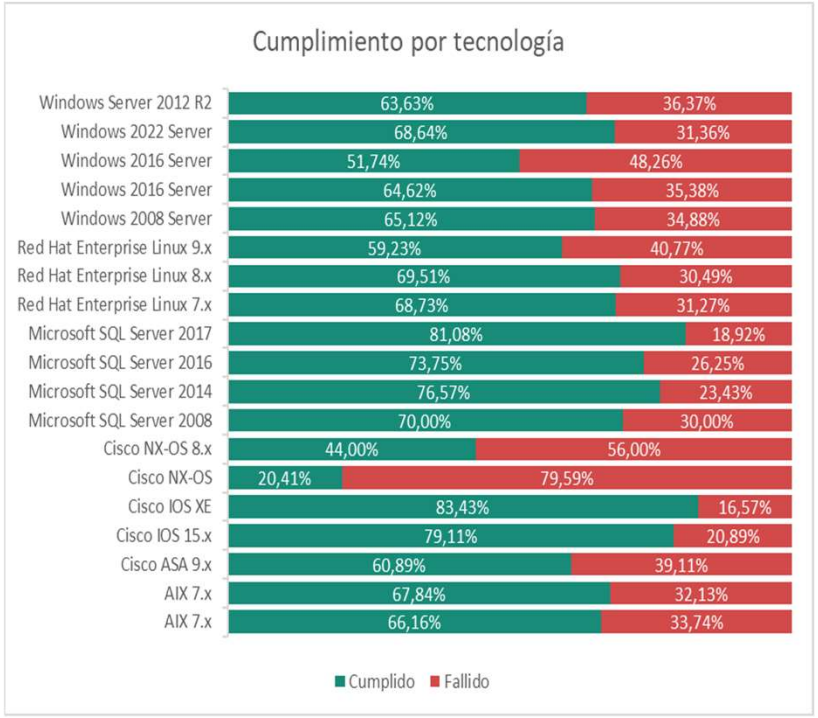
397	0	4	16	18	3.490
Activos evaluados	Activos duplicados	Activos sin controles	Activos sin conexión en un mes	Políticas evaluadas	Controles evaluados

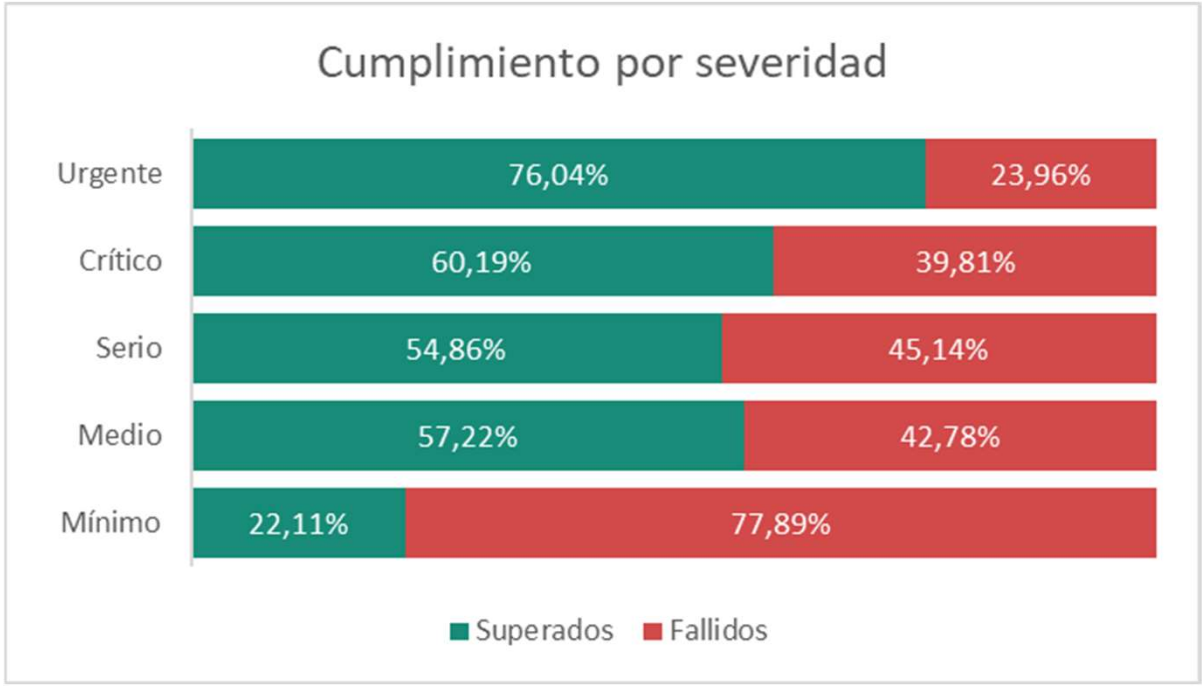






EVALUACIÓN DE LÍNEAS BASE





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

CONCLUSIONES Y RECOMENDACIONES

- 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)

- Todos los meses se encuentran en promedio 5 servidores que son dados de baja, en caso de que estos lleguen a ser reemplazados, es importante realizar la notificación vía electrónica para realizar su adición a través del proceso de instalación de agente en estos dispositivos o servidores nuevos.

- El 20 de agosto los servidores el grupo de servidores Windows 2008 R2 (BOGPVPPWP023, FNABOGAPP001, FNABOGDCL01N6, FNABOGDPCL01N1) dejó de transmitir información a la nube a través del Gateway, después de múltiples reuniones de acompañamiento se pudo determinar que el error es debido a la ausencia de confianza de los servidores en el Gateway, ya sea porque este no ofrece un certificado para cifrar la comunicación o el certificado ofrecido no es confiable para los servidores, para mitigar este inconveniente se realizó la instalación del certificado del QCG de forma local en el OS de estos mismos servidores, a pesar de esto dichos servidores siguen sin transmitir.

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. identificación de causa de duplicidad de activos

6. Generación de reportes de cumplimiendo bajo demanda

7. Eliminación de agentes por solicitud (C64428)

Fortify SCA

Informe de Actividades y Funcionamiento Fortify

2024

Resumen Ejecutivo

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

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. Estamos a la espera de que la nueva casa desarrolladora solicite la integración con Fortify.

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 diciembre de 2024, 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.

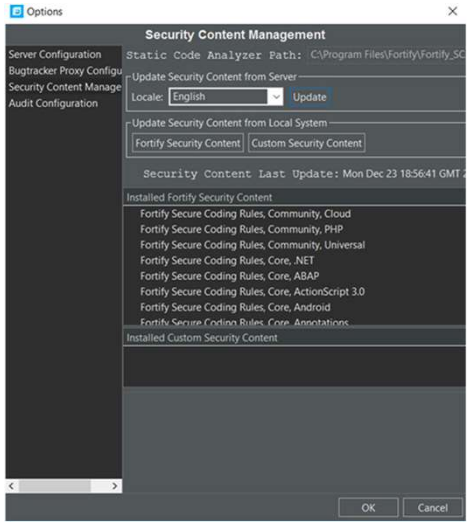
Gestión y actividades

- **Restablecimiento de Contraseñas para Usuarios de Dominio:**
  A través de la mesa de soporte, se solicita el restablecimiento de las contraseñas para los usuarios de dominio utilizados en la autenticación de los servidores que alojan la suite Fortify. Esta medida tiene como objetivo reforzar la seguridad en el acceso a los servidores, asegurando que las credenciales estén actualizadas y protegidas 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 lleva a cabo 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 esenciales para mantener la efectividad de las herramientas de seguridad, asegurando que se adapten a las nuevas amenazas y vulnerabilidades emergentes, así como a las actualizaciones regulatorias y normativas del sector.
  El proceso de actualización contribuye a mejorar la capacidad de los módulos para detectar vulnerabilidades de manera más precisa y a optimizar los informes de seguridad generados durante las auditorías de las 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.

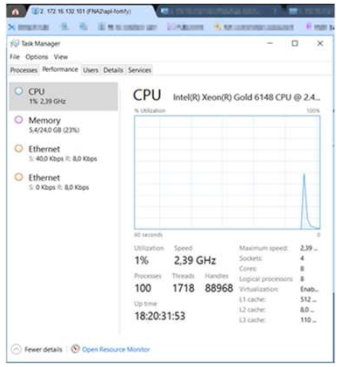
- **Actualización de Rulespacks del módulo SSC:** Se lleva a cabo la actualización periódica de los Rulespacks en el módulo SSC para asegurar que las reglas de seguridad estén actualizadas, mejorando así la detección de vulnerabilidades y adaptándose a las nuevas amenazas emergentes.

- **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.

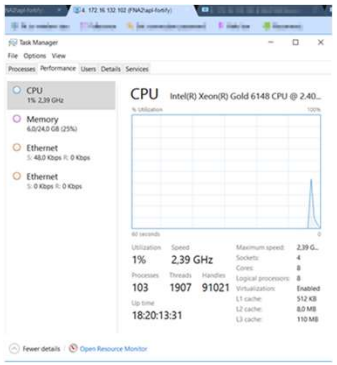
Disponibilidad y rendimiento del sistema.

A continuación, se detalla la disponibilidad de los servidores que alojan la suite Fortify durante el periodo de evaluación. Esta información refleja la estabilidad y confiabilidad de la infraestructura, lo cual es clave para garantizar la continuidad del servicio de auditoría y análisis de seguridad sin interrupciones.

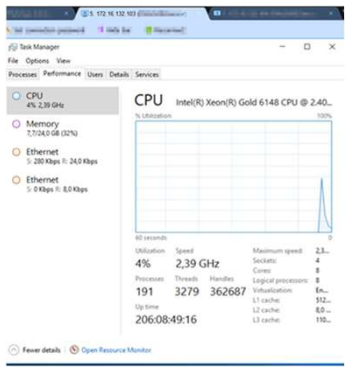
172.16.132.101



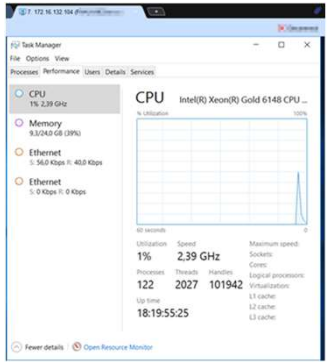
172.16.132.102



172.16.132.103



172.16.132.104



Conclusiones

- Durante el período comprendido, la suite Fortify ha operado de manera estable y sin interrupciones, sin registrar caídas ni fallas. El mantenimiento y las actualizaciones se han gestionado de forma constante, lo que ha garantizado la disponibilidad continua de la herramienta y su rendimiento óptimo en todo momento, asegurando que esté siempre lista para su uso cuando se necesite.

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 minimizaran 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.



Informe Soluciones Antimalware

2024

Objetivo

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

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

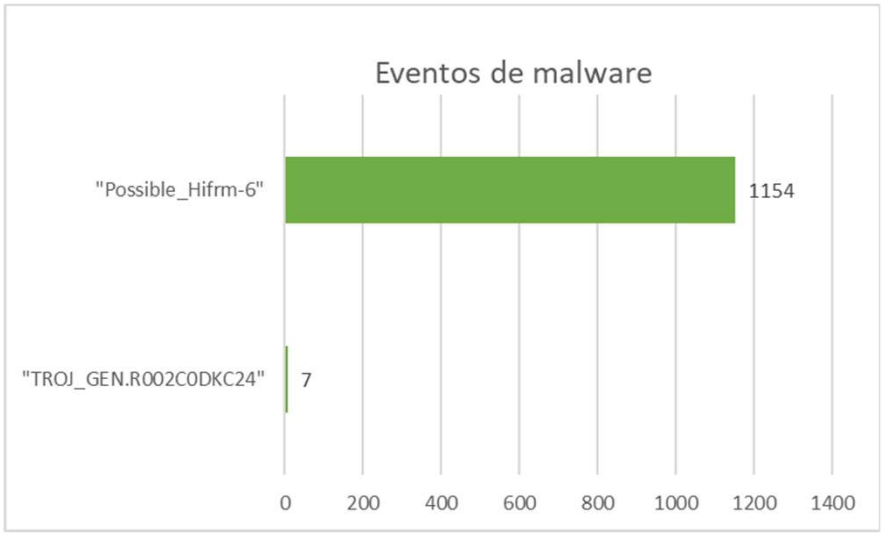
Alcance

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 noviembre hasta el 21 de diciembre del año 2024.

Estadísticas Generales de detección

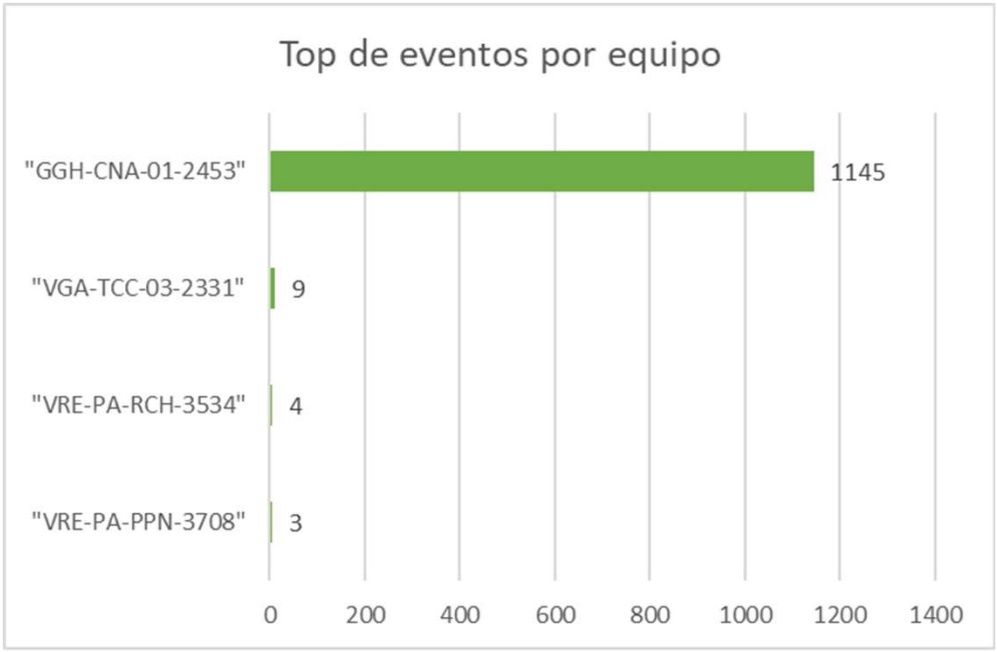
Detecciones en puntos finales Trendmicro

Se evidencian un total de **1161 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 entre esto se encuentra la detección de archivo de instalación de **Agent Dexon 5.1.3.222.exe**



Top de equipos con mayor cantidad de detecciones

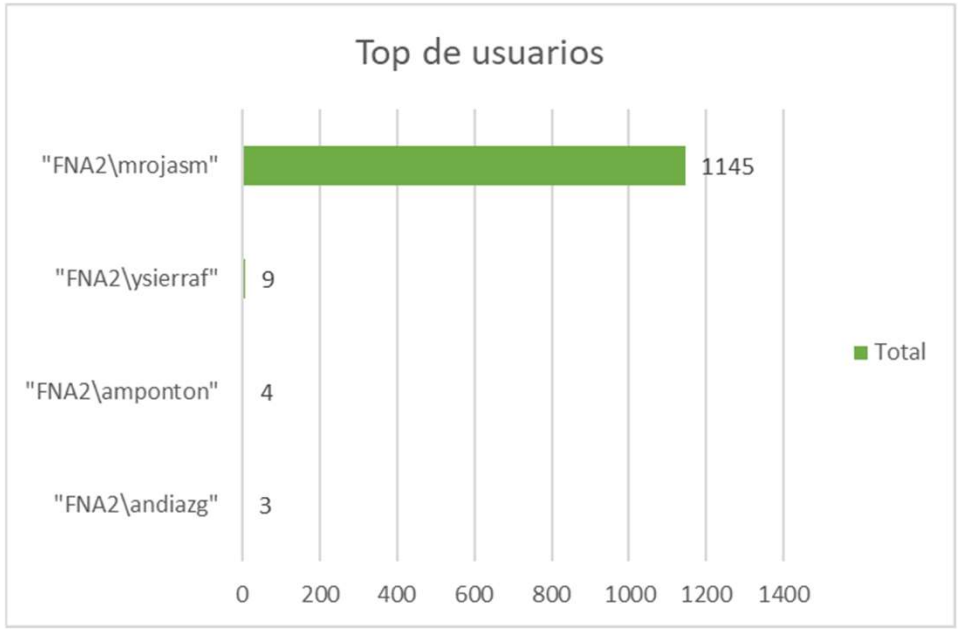
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **VGA-TCC-03-2331** por la detección del archivo **Agent Dexon 5.1.3.222.exe.**



Estadísticas Generales de detección

Top de usuarios con mas eventos.

En el top de usuarios se encuentra mrojasm por la detección de archivos con objetos embebidos, seguido de ysierraf por el mismo tipo de detección.



Behavior Monitoring

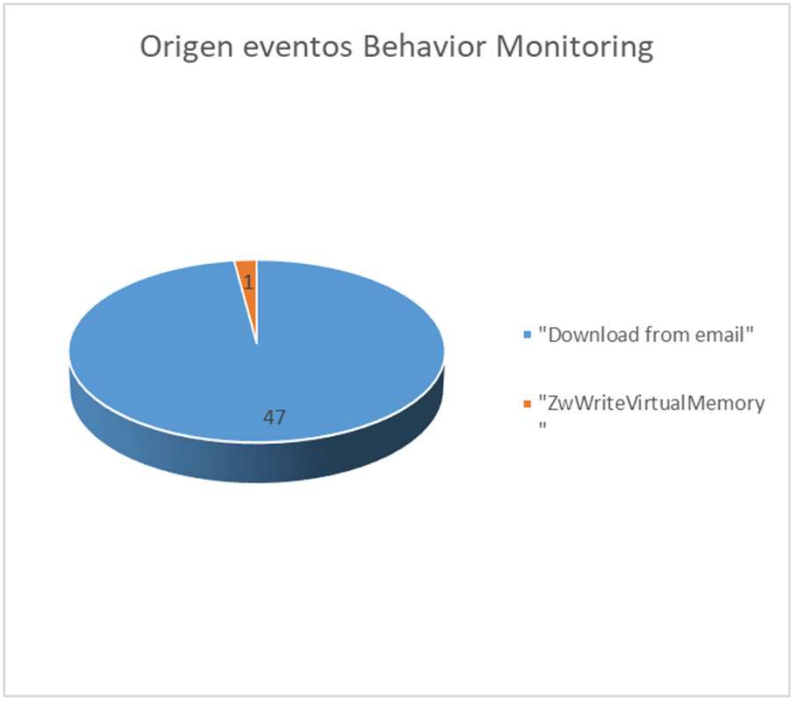
El módulo de Behavior Monitoring monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo el archivo **TRAMITES.exe y Ahorro.exe** estos se detectaron como archivos nuevos.

Eventos Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
"C:\COBIS\Credito\Gestion\GESTION.exe"	1
"C:\Users\acifuentesr\AppData\Local\Temp\7zO417A71FF\Facturas de Cobro Notificacion de Embargo #000047700001111258963210001458236971139397113952147968521478536000000000001436994161719368178965822719 63.exe"	1
"C:\Users\Administrador\Downloads\documents_20241220(2)\TransferWMCapture\setup.exe"	1
"C:\Soporte\BiometricDesktop_PROD_2.0.5.exe"	2
"C:\Soporte\Recursos Capture y Servicio TransferWmCapture V4\TransferWMCapture\setup.exe"	2
"C:\COBIS\Cobis-Clientes\mis.exe"	3
"C:\COBIS\Cesantias\Entidades\CESENTID.exe"	5
"C:\Users\ccardenast\Documents\output\regla1.exe"	5
"C:\COBIS\Cesantias\Cesantias\CESANTIA.exe"	6
"C:\COBIS\AhorroVoluntario\Ahorro.exe"	10
"C:\COBIS\Credito\Tramites\TRAMITES.exe"	12
Total general	48

Estadísticas Generales de detección

Origen Behavior Monitoring

En el origen de eventos se puede ver que la mayoría corresponde a archivos descargados de correos.



Application Control

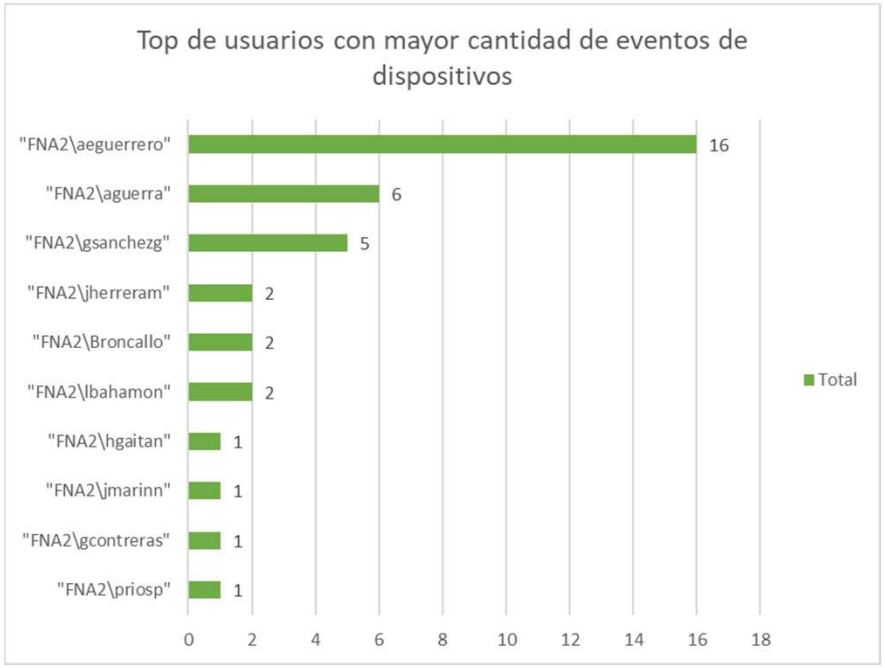
La política de application Control encontró el uso de la aplicación **conda.exe**, listado dentro de aplicaciones bloqueadas por la solución.

Eventos Application Control	
Etiquetas de fila	**Cuenta de File**
"GAS-CNA-01-3694"	40
"conda.exe"	40
"GAA-TT-02-2779"	10
"conda.exe"	10
"GAA-TT-02-2856"	97
"conda.exe"	97
Total general	147

Estadísticas Generales de detección

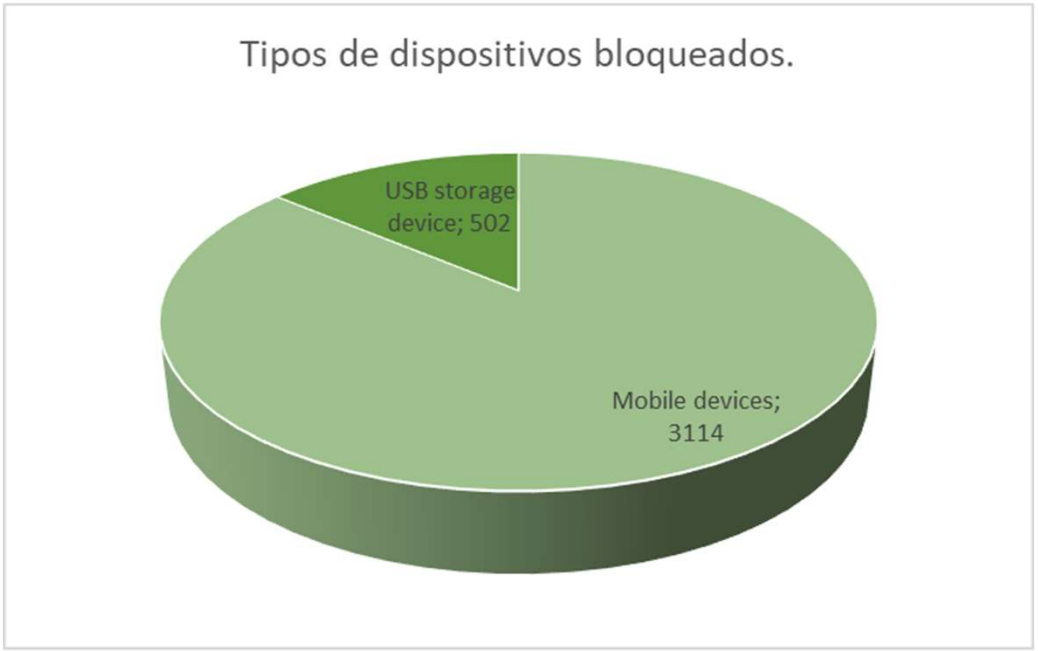
Device Control

El módulo de Device control, bloquea el uso no autorizado de dispositivos extraíbles, el usuario que mayor cantidad de eventos registra es **aeguerrero con 16** registros.



Device Control

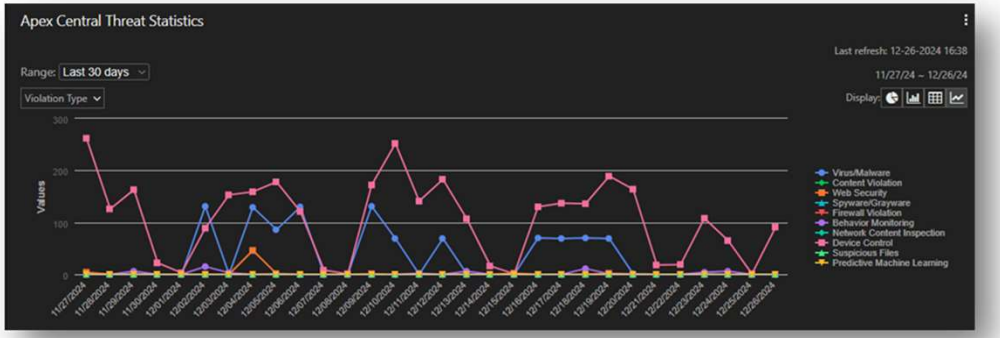
En el tipo de dispositivos que mayor cantidad de eventos registra, son dispositivos móviles.



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

XDR Eventos por categoría

En el top de eventos por técnicas de acuerdo con XDR, esta Device Access Violation por las políticas de Device control, seguido de MITRE.T103 por enmascaramiento, por la detección de archivos con objetos embebidos.

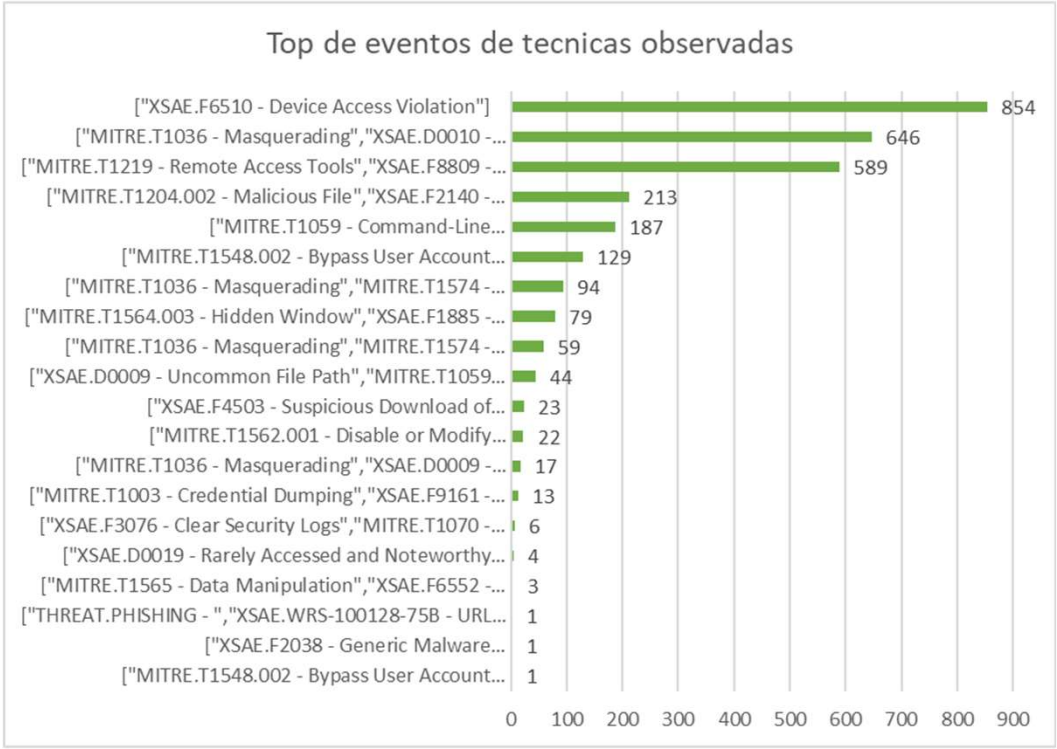
Dentro de las alertas mas relevantes se encuentran las siguientes técnicas utilizadas, en las diferentes detecciones.

•Análisis inicial de compromiso: Técnicas relacionadas con phishing, archivos maliciosos y bypass de controles (e.g., MITRE.T1204.002, MITRE.T1548.002).

•Detección de persistencia y evasión: Abuso de DLL, herramientas legítimas, y manipulación de configuraciones (e.g., MITRE.T1574.001, XSAE.F3256).

•Movimiento lateral y exfiltración: Protocolo SMB y transferencias de archivos (e.g., MITRE.T1021.002, MITRE.T1105).

XDR Eventos por categoría



Estadísticas Generales de detección

XDR Eventos por nombre.

En el top de eventos por nombre de acuerdo con el nombre de los archivos ejecutados, está el uso de la herramienta QuickAssist, para conexión remota, también el uso de MMC para administración de usuarios y la ejecución de Windows Powershell para desactivación de Windows Defender.

técnica
["MITRE.T1219 - Remote Access Tools","XSAE.F8809 - QuickAssist Remote Session Established"]
C:\Program Files\WindowsApps\MicrosoftCorporationII.QuickAssist_2.0.31.0_x64__8wekyb3d8bbwe\Microsoft.RemoteAssistance.QuickAssist\Quick
C:\Windows\System32\quickassist.exe
["MITRE.T1548.002 - Bypass User Account Control","MITRE.T1213 - Data from Information Repositories","XSAE.F3142 - Unusual LDAP in command line","XSAE.F5939 - UAC Bypass via Microsoft Management Console"]
C:\Windows\System32\mmc.exe
["MITRE.T1548.002 - Bypass User Account Control","XSAE.F5939 - UAC Bypass via Microsoft Management Console"]
C:\Windows\System32\mmc.exe
["MITRE.T1562.001 - Disable or Modify Tools","MITRE.T1059.001 - PowerShell","XSAE.F3256 - Disabling of Windows Defender via Powe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
["MITRE.T1564.003 - Hidden Window","XSAE.F1885 - Launch PowerShell With Hidden Window","MITRE.T1059 - Command-Line Interface","XSAE.F1518 - Compression of File or Folder via PowerShell","MITRE.T1059.001 - PowerShell","MITRE.T1560 - Archive Colle Data","MITRE.T1074 - Data Staged","MITRE.T1074.001 - Local Data Staging"]
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
["MITRE.T1565 - Data Manipulation","XSAE.F6552 - Modification of Hosts File via Text Editor"]
C:\Windows\System32\notepad.exe
["THREAT.PHISHING - ","XSAE.WRS-100128-75B - URL Access Blocked - Phishing","mitre.t1566.002 - ","XSAE.F4960 - Phishing Detection","threat.phishing - "]
(en blanco)
["XSAE.D0009 - Uncommon File Path","MITRE.T1059 - Command-Line Interface","MITRE.T1546.008 - Accessibility Features","MITRE.T Signed Binary Proxy Execution","MITRE.T1574.001 - DLL Search Order Hijacking","XSAE.F9885 - Extraction of Executable Binary From A Tool Via Command Line"]
C:\Program Files\WinRAR\WinRAR.exe
["XSAE.D0019 - Rarely Accessed and Noteworthy Domain","MITRE.T1071 - Standard Application Layer Protocol","MITRE.T1071.001 - W Protocols","XSAE.D0001 - Rarely Accessed Domain"]
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
C:\Program Files\WindowsApps\microsoft.windowscommunicationsapps_16005.14326.22098.0_x64__8wekyb3d8bbwe\HxOutlook.exe
["XSAE.F2038 - Generic Malware Detection","MITRE.T1204.002 - Malicious File","XSAE.F2140 - Malicious Software","XSAE.F3592 - Thre Prioritization Trojan Detection","THREAT.MALWARE - ","XSAE.F8178 - Heuristic File Detection - Blocked"]
(en blanco)
["XSAE.F3076 - Clear Security Logs","MITRE.T1070 - Indicator Removal on Host","MITRE.T1070.001 - Clear Windows Event Logs"]
C:\Windows\System32\svchost.exe
["XSAE.F4503 - Suspicious Download of File","XSAE.F4986 - Malware Detection","MITRE.T1105 - Remote File Copy","THREAT.MALWAR ","CVE.2000.0138 - "]
(en blanco)
["XSAE.F6510 - Device Access Violation"]
(en blanco)
System
(en blanco)
(en blanco)
Total general

Estadísticas Generales de detección

XDR Alertas Workbench.

Workbench, genera alertas de acuerdo con diferentes eventos correlacionados y les asigna una clasificación, se registraron 24 alertas ninguna con clasificación alta, dentro de estas se encuentra:

•Ejecución de comando sutil usn deletejournal /d /n c: y cipher /w:C:\, se escalo caso con administradores del servidor y se valido que correspondía a tareas administrativas, se recomienda el no uso del comando por borrado completo de información y no recomendado en entornos virtuales.

•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.

•Domain Trust Discovery, está vinculado al intento de descubrimiento de relaciones de relaciones de confianza del dominio, este evento se genera por el despliegue de la herramienta Intune, de forma valida.

•El ultimo evento corresponde al acceso de la URL https://fulzzar[.]blogspot[.]com/favicon.ico, como pruebas realizadas por parte del administrador de DarkTrace.

Score	Insight	Impact Scope	Case	Attack Phase
88	"IC-35600-20241123-00000| Alert 6 | Adversary is trying to do Indicator Removal on Host which leads the Disk Wipe: Disk Content Wipe"	"Endpoint - Server: 1 | User Account: 2"	"Defensive evasion| Impact"	6/12/2024 19:07
44	"IC-35600-20241212-00000| Alert 2 | Possible Disabling of Antivirus Software (2)"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241221-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241221-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241219-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Desktop: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241218-00004| Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241218-00002| Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241218-00003| Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241218-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241218-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241217-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Desktop: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241217-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241216-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241215-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	15/12/202 4 0:33
41	"WB-35600-20241212-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241210-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	######## ####
41	"WB-35600-20241206-00004| Alert 1 | Possible Disabling of Antivirus Software"	Endpoint - Server: 1	"Execution| Defensive evasion"	6/12/2024 16:36
41	"WB-35600-20241206-00002| Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	5/12/2024 22:18
41	"WB-35600-20241206-00001 | Alert 1 | Possible Disabling of Antivirus Software"	Endpoint - Server: 1	"Execution| Defensive evasion"	5/12/2024 21:00
41	"WB-35600-20241206-00000 | Alert 1 | Possible Disabling of Antivirus Software"	Endpoint - Server: 1	"Execution| Defensive evasion"	5/12/2024 20:26
41	"WB-35600-20241203-00001 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	2/12/2024 21:56
41	"WB-35600-20241203-00000 | Alert 1 | Possible Disabling of Antivirus Software"	"Endpoint - Server: 1 | User Account: 1"	"Execution| Defensive evasion"	2/12/2024 20:12
34	"IC-35600-20241122-00000| Alert 3 | Environment probing (Domain Trust Discovery) has been detected"	"Endpoint - Desktop: 1 | User Account: 1"	"Execution| Credential Access| Discovery"	######## ####
30	"WB-35600-20241213-00000 | Alert 1 | [Heuristic Attribute] URL Accessed Blocked by Web Reputation Service"	User Account: 1	#########	13/12/202 4 8:53

Estadísticas Generales de detección

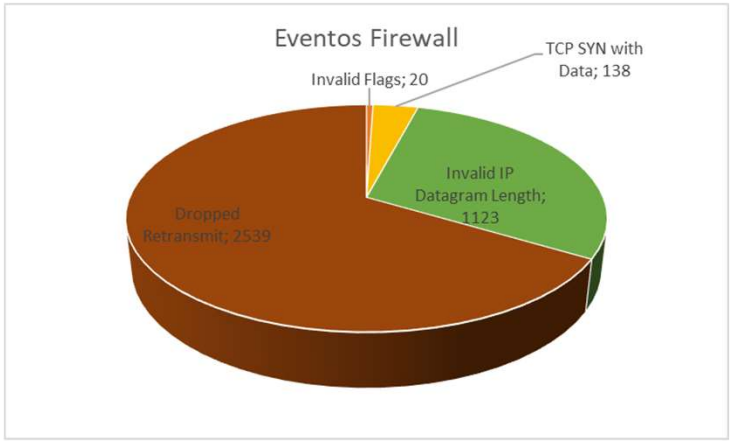
Eventos Servidores

Se registran 4 eventos en el servidor **FNABOGAPP015,** por la regla de detección objetos embebidos en archivos. En específico, por el archivo **52 Informe de selecciÃ³n 023.pdf**

Eventos servidores	
Etiquetas de fila	**Cuenta de ruleName**
Etiquetas de fila	Cuenta de Modified
FNABOGAPP015.fna.gov.co	4
Possible_Hifrm-6	4
Total general	4

Eventos Firewall Servidores

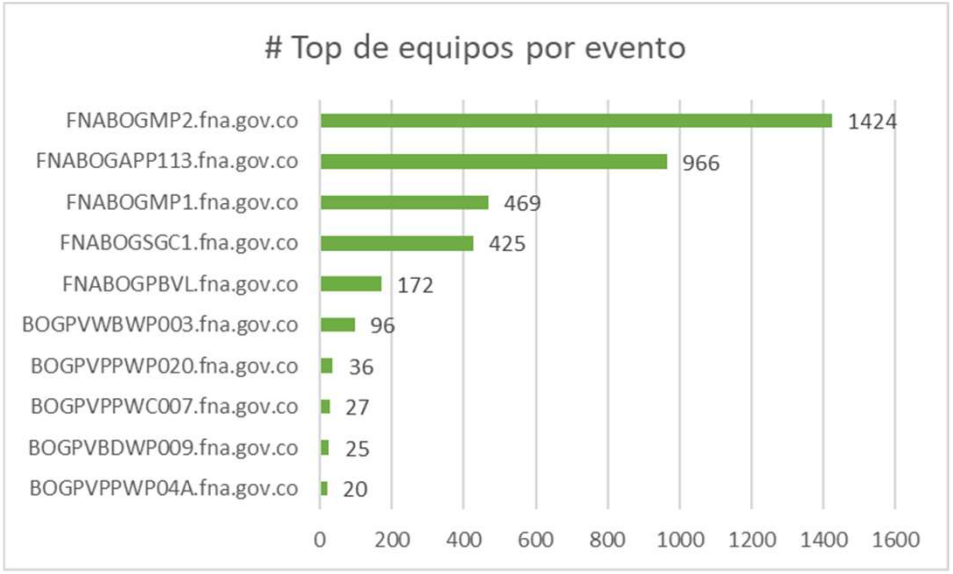
El módulo de Firewall de hosts ha sido activado en servidores, esto inicialmente en modo observación. De acuerdo con este módulo se generaron 3820 eventos, El evento que mayor cantidad de registros género es **Retransmit**: Si el firewall detecta paquetes que no coinciden con una sesión válida establecida, los considera retransmisiones sospechosas. Seguido **de Invalid Datagram Length**: El evento "Invalid IP Datagram Length" está relacionado con el procesamiento de paquetes IP en una red y se refiere a un datagrama IP que tiene un campo de longitud total que no es válido según las especificaciones del protocolo. Esto puede deberse a problemas en la configuración, errores en la transmisión o intentos de ataque.



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**.



Eventos Acción Servidores

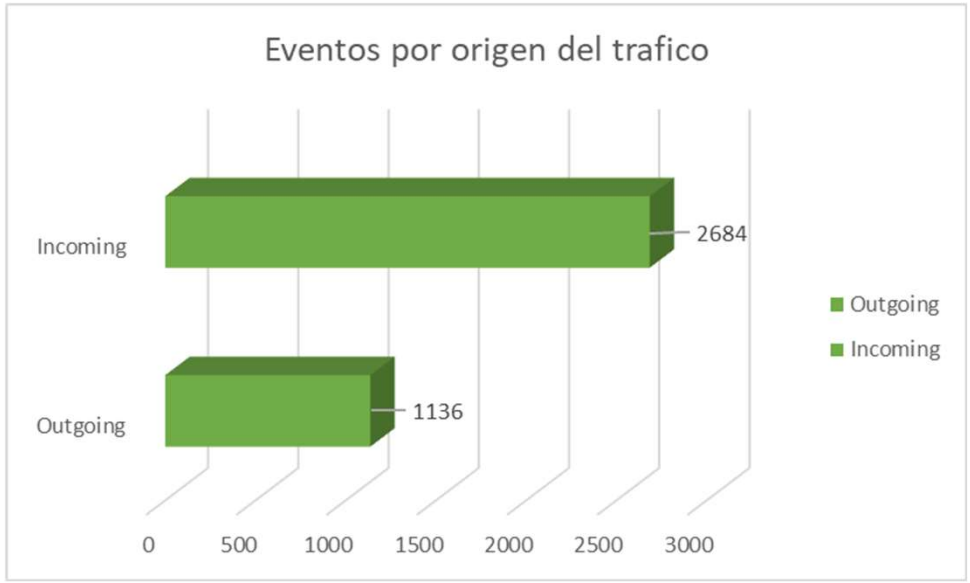
La mayoría de los eventos **3800 fueron bloqueados o denegados**, los otros 20 fueron de auditoría.



Estadísticas Generales de detección

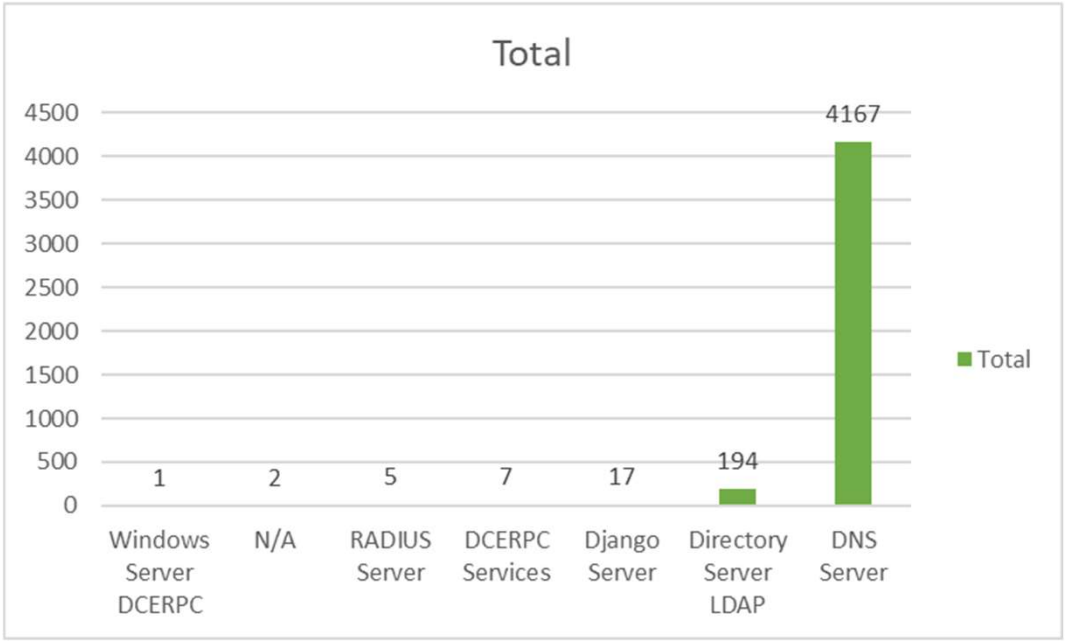
Eventos por origen de datos

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:

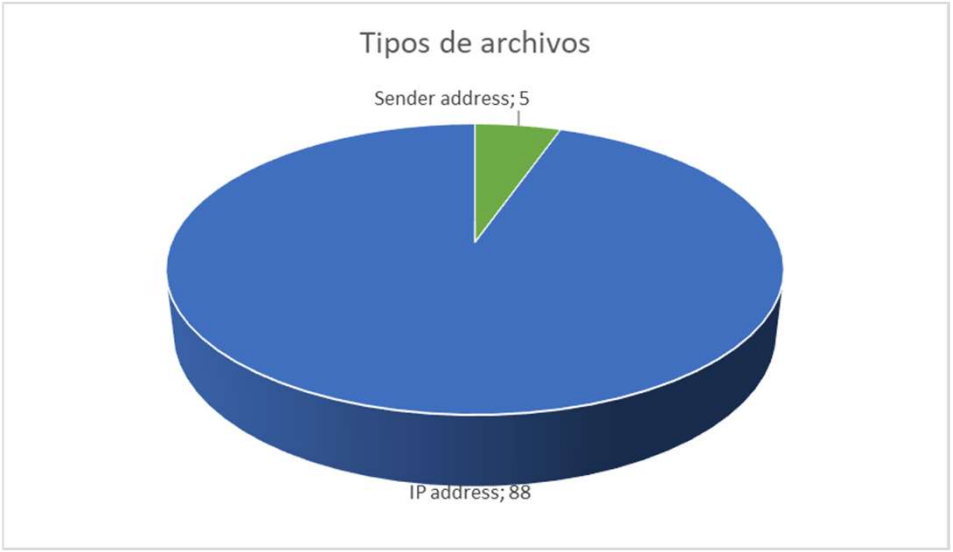
- **Evento 1011843 (Django):** Un atacante puede sobrecargar servidores Django enviando solicitudes maliciosas. Actualiza Django y utiliza WAF para mitigarlo.
- **Evento 1008555 (Active Directory**): Un atacante puede interrumpir funciones críticas de red explotando solicitudes LDAP maliciosas. Actualiza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

Top de eventos IPS	
NombreHost,Evento	#
FNABOGAPP015.fna.gov.co	1
1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share	1
FNABOGTS1.fna.gov.co	1
1012209 - Microsoft Windows Remote Desktop Licensing Service Denial of Service Vulnerability (CVE-2024-38071)	1
FNABOGWMH1CR.fna.gov.co	2
1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share	2
BOGPVPPWP048.fna.gov.co	3
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	2
Invalid Traversal	1
BOGPVPPWP049.fna.gov.co	4
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	4
FNABOGWMH2.fna.gov.co	4
1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share	4
BOGPVPPWP04A.fna.gov.co	5
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	5
BOGPVSWWP00A.fna.gov.co	5
1006372 - Microsoft Network Policy Server RADIUS Implementation Denial Of Service Vulnerability (CVE-2015-0015)	5
BOGPVPPWP047.fna.gov.co	7
1011843 - Django Denial of Service Vulnerability (CVE-2023-23969)	6
Invalid Traversal	1
BOGPVDCWP003.fna.gov.co	44
1008555 - Microsoft Windows Active Directory Denial Of Service Vulnerability (CVE-2008-1445)	44
BOGPVDCWP001.fna.gov.co	2076
1004747 - DNS Invalid Compression Denial Of Service	2023
1008555 - Microsoft Windows Active Directory Denial Of Service Vulnerability (CVE-2008-1445)	53
BOGPVDCWP002.fna.gov.co	2241
1004747 - DNS Invalid Compression Denial Of Service	2144
1008555 - Microsoft Windows Active Directory Denial Of Service Vulnerability (CVE-2008-1445)	97
Total general	4393

Estadísticas Generales de detección

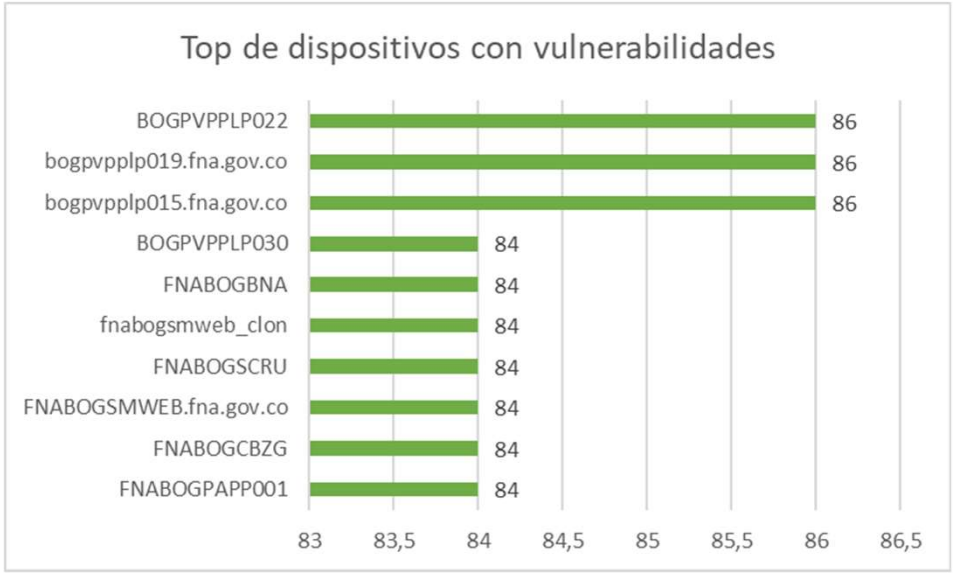
Threat Intelligent

Durante el periodo de 22 de noviembre al 21 de diciembre del 2024 se adicionan **93 reputaciones** nuevas adicionadas por la integración con Threat Q, correspondientes a correos electrónicos y direcciones IP.



Attack Surface Discovery Devices

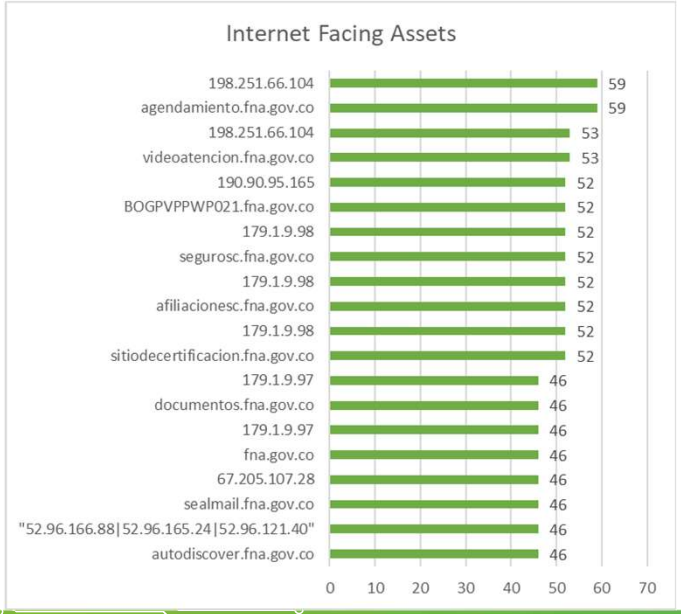
En el top de eventos, se registra los servidores **bogpvpplp022, bogpvpplp015 y bogpvpplp019, con 86 vulnerabilidades** y fallos en la configuración, con clasificación alta.
El número en la grafica indica la clasificación, entre mas cerca al **100** más alta es.



Estadísticas Generales de detección

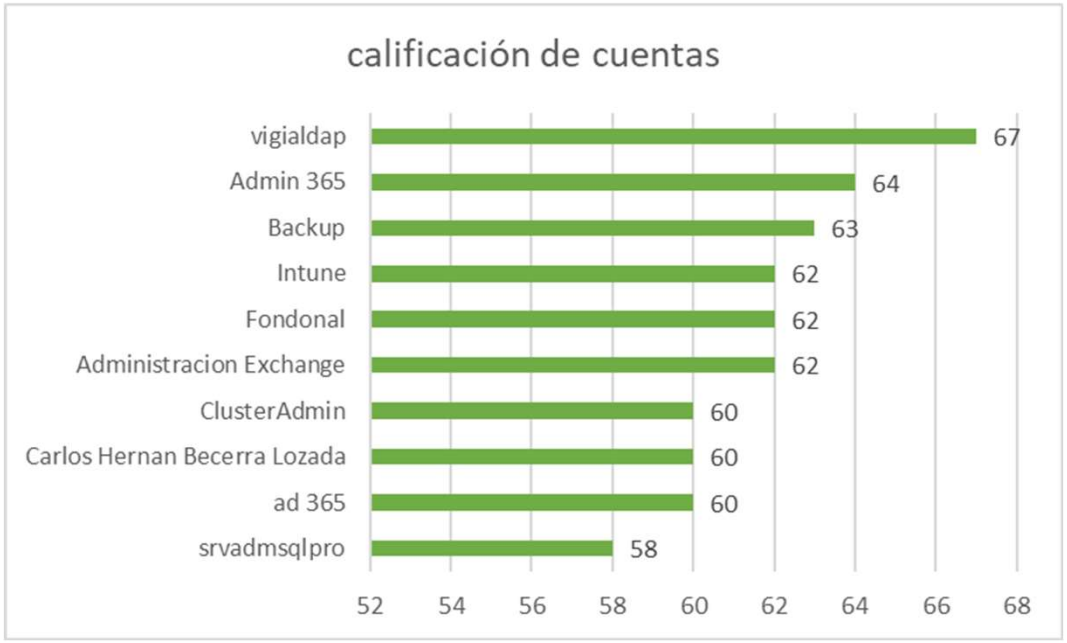
Attack Surface Discovery Internet Facing Assets

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 IP's 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

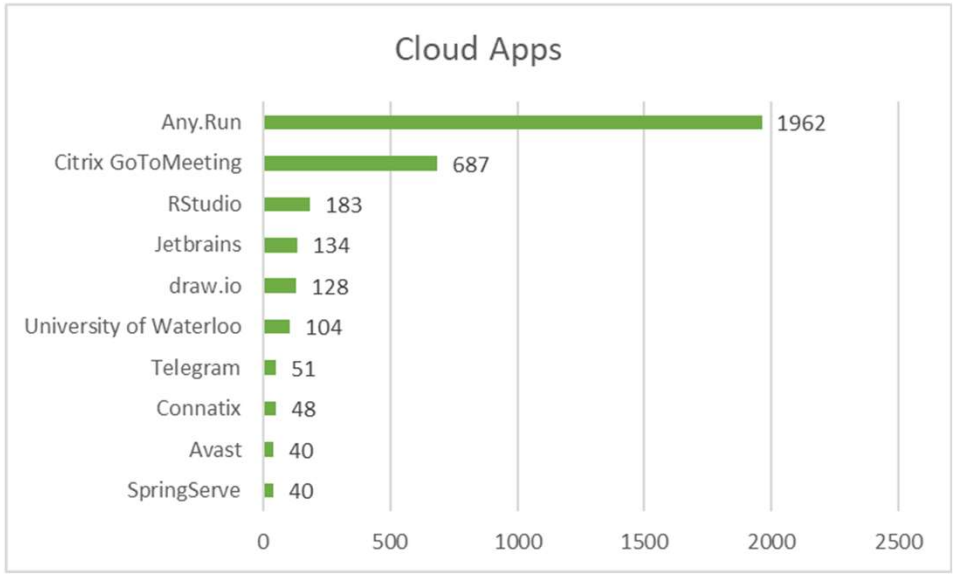
A continuación se muestra el top de cuentas identificadas por Trend Micro



Estadísticas Generales de detección

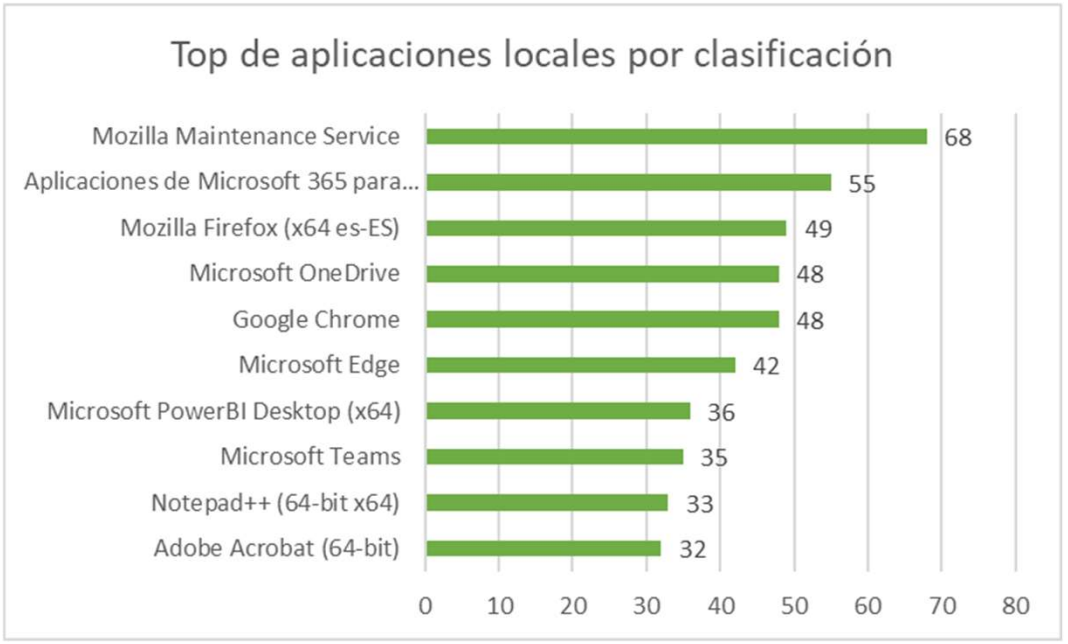
Attack Surface Discovery Cloud Apps

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



Attack Surface Discovery Local Apps

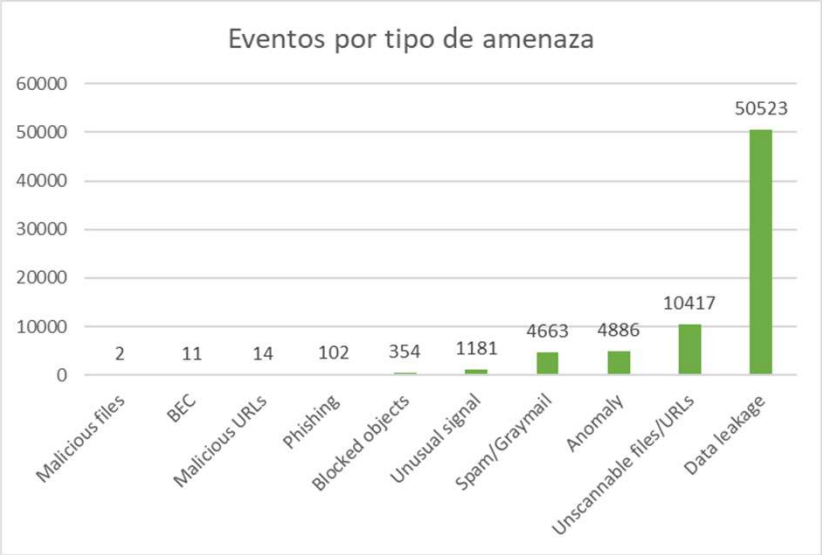
A continuación se muestra el top de aplicaciones locales por calificación de riesgo, **Mozilla y Office 365** se encuentran en el top de acuerdo con vulnerabilidades encontradas en versiones específicas.



Estadísticas Generales de detección

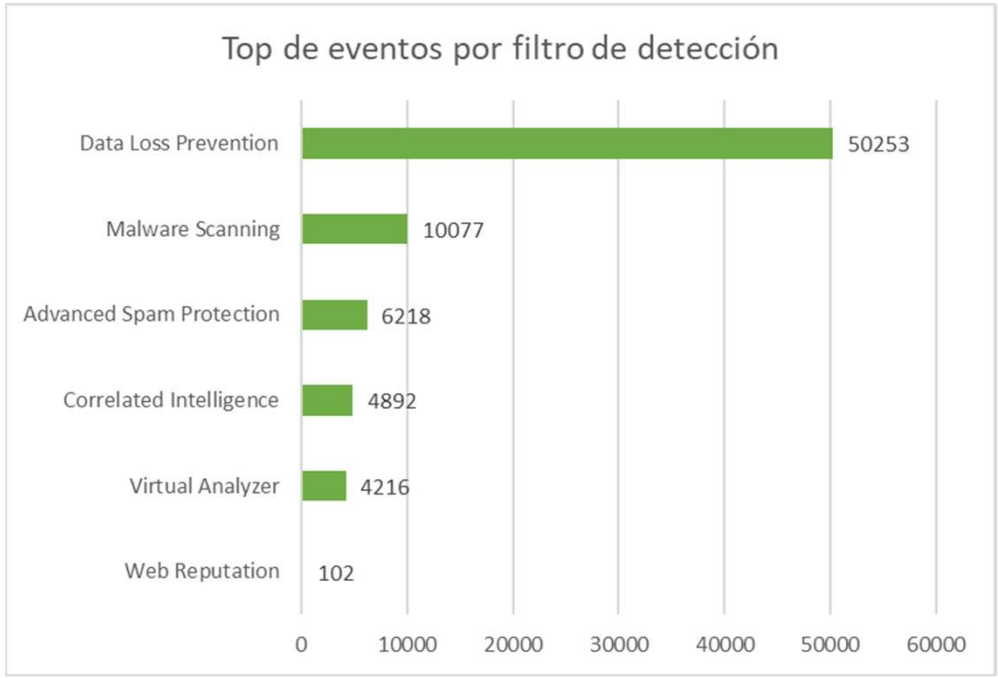
CASB Top de eventos por regla.

Para el periodo de **22 de noviembre al 21 de diciembre del 2024 se presentaron un total de 76942 eventos** registrados por la solución CASB, 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

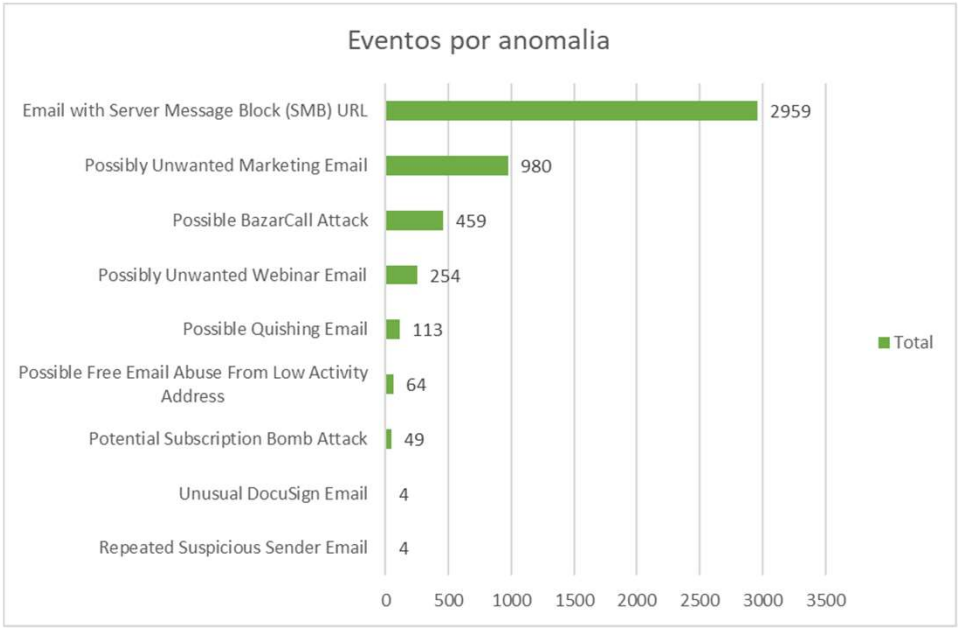
Dentro de los eventos la mayoría corresponden eventos de Data Loss Prevention, seguido de eventos de malware.



Estadísticas Generales de detección

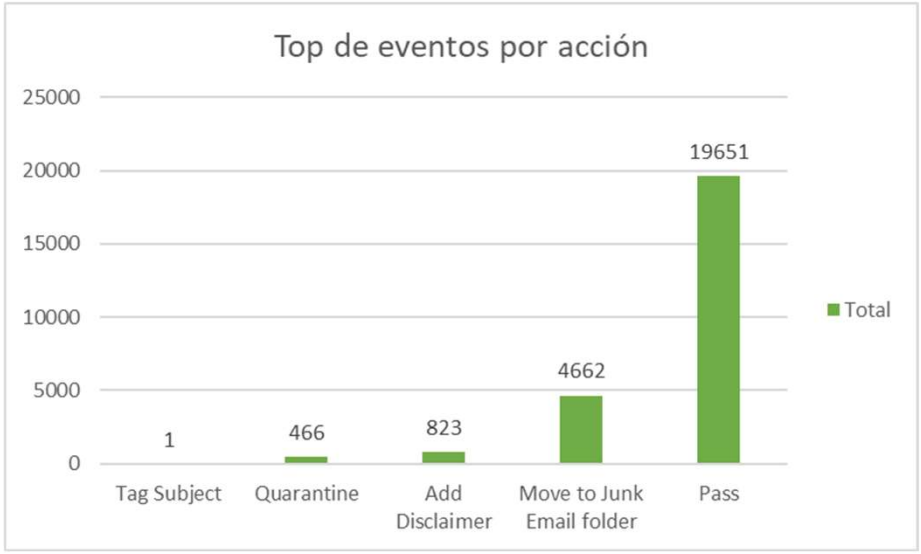
CASB Top de eventos por nombre de anomalía.

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 **logistica@sumicorp.com y mailer-daemon@googlemail.com**

Top de remitentes clasificados como SPAM	
Sender	**#Eventos**
"camacol comunicaciones"<dircomunicaciones@camacol.info>	63
"locatel colombia"<newsletter@locatelnews.com>	65
<postmaster@outlook.com>	78
"bodytech"<contacto@social.bodytech.com.co>	79
"articulo20"<cybernoticias@articulo20.net.co>	81
"isabel de zalvadora"<isabel.muller@zalvadora.com>	87
"bbva"<info@email.bbva.com.co>	92
"noticieroficial"<boletin@noticieroficial.com>	104
"mail delivery subsystem"<mailer-daemon@googlemail.com>	241
"direccion logistica"<logistica@sumicorp.com>	352

CASB Top de cuentas como origen de Phishing.

En el top de correos remitentes de phishing esta la cuenta **alertasynotificaciones[@]notificacionesbancolombia[.]com y dianisjulieth[.]07@hotmail.com**

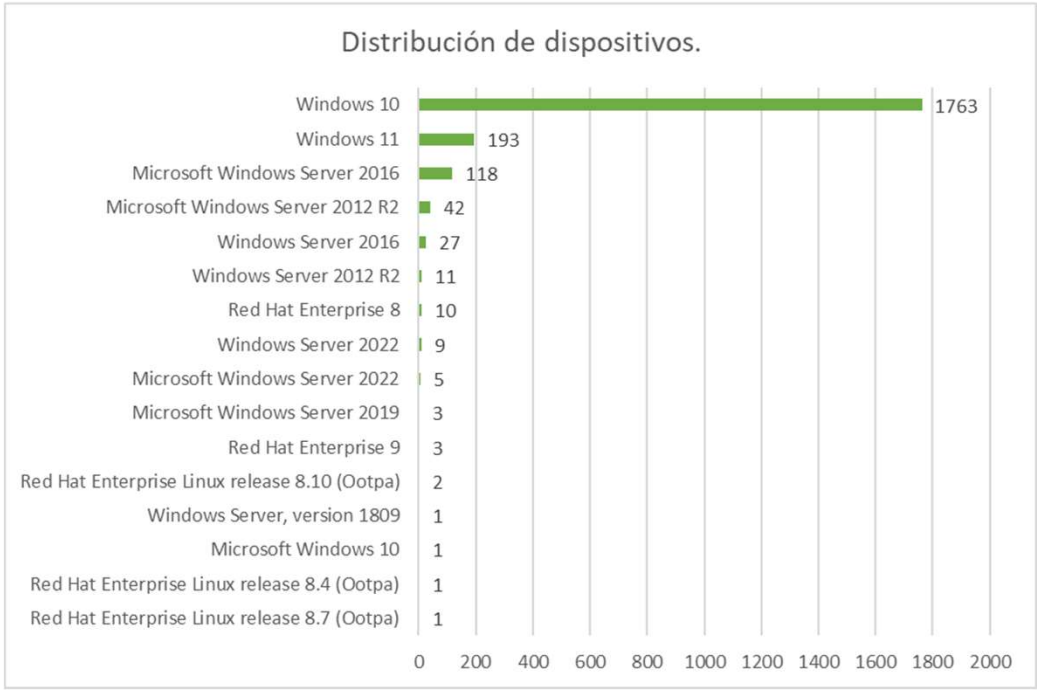
Correos clasificados como Phishing	
Etiquetas de fila	**Cuenta de Sender**
"marleyn arrazola cuesta"<marleyn27@hotmail.com>	1
"msr.marain llitch"<matt.cornall@dediserve.com>	1
"audisis ltda."<audisismercadeo@109603002.mailchimpapp.com>	1
"qysbkblhj"<garderie.loisirs@vinon-sur-verdon.fr>	1
"camilo andrés barrera riaño"<camianbarri@hotmail.com>	1
"servicio de entrega de correo"<postmaster@tie.cl>	1
"laura garcia"<laurags100191@gmail.com>	1
"united nations compensation fund"<mrsma2020@gmail.com>	1
"viviana suarez"<viviana6@icloud.com>	1
"alfredo humberto moreno"<alfredohumberto7@icloud.com>	1
<facilweb@solucionesnavarro.com>	2
"bancolombia"<tusinformes@tubienestarfinanciero.infobancolombia.com>	3
"dianis cantillo"<dianisjulieth.07@hotmail.com>	4
"alertas y notificaciones"<alertasynotificaciones@notificacionesbancolombia.com>	75
Total general	94

Estadísticas Generales de detección

Licenciamiento

A continuación, se relaciona el informe de 2190 dispositivos instalados en el periodo que comprende el periodo de 22 de noviembre al 21 de diciembre del 2024 .

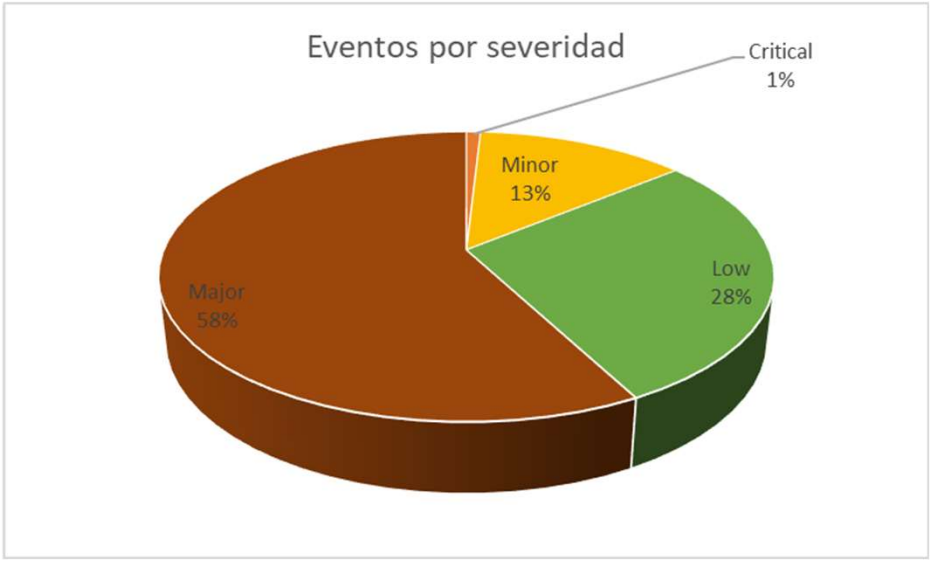
Licenciamiento



Estadísticas Generales de detección

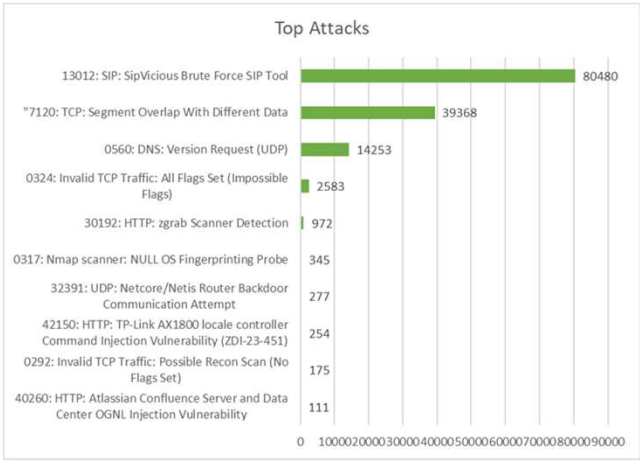
Top de ataques detectados IPS

Durante el periodo analizado del periodo **de 22 de noviembre al 21 de diciembre del 2024** , se encuentra el siguiente TOP de Eventos identificados por el IPS. Del total de los **139716** eventos, en su mayoría con clasificación **major con el 58 %** de los eventos.



TOP DE ATAQUES IPS

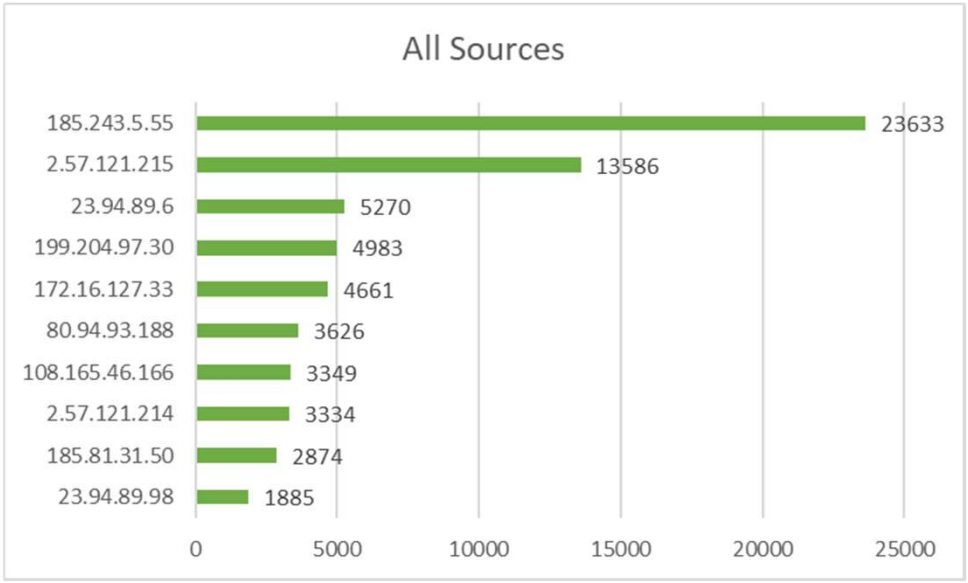
En el top de ataques se encuentra la regla **13012: SIP: SipVicious Brute Force SIP Tool**, por el uso de herramientas SIPVICIOUS para realizar intentos de ataque por fuerza bruta, este evento registra 80482 eventos del total. En segundo lugar se encuentra la regla **7120: TCP: Segment Overlap With Different 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

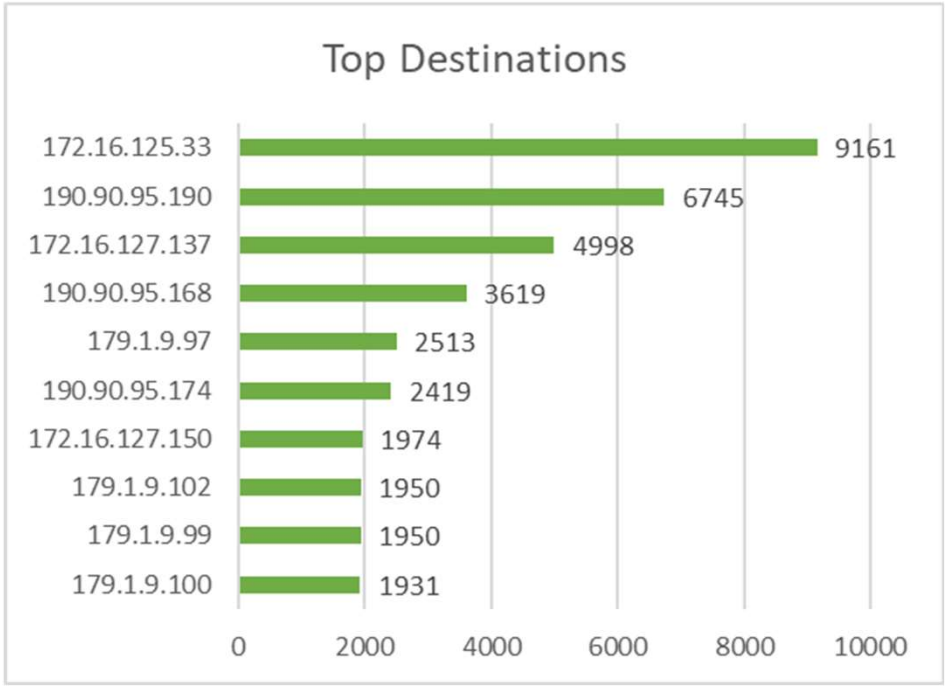
Top de origen.

A continuación se muestra el top de IP de **origen 185.243.5.55** de **Polonia** con **23633** eventos.



Top Destinos.

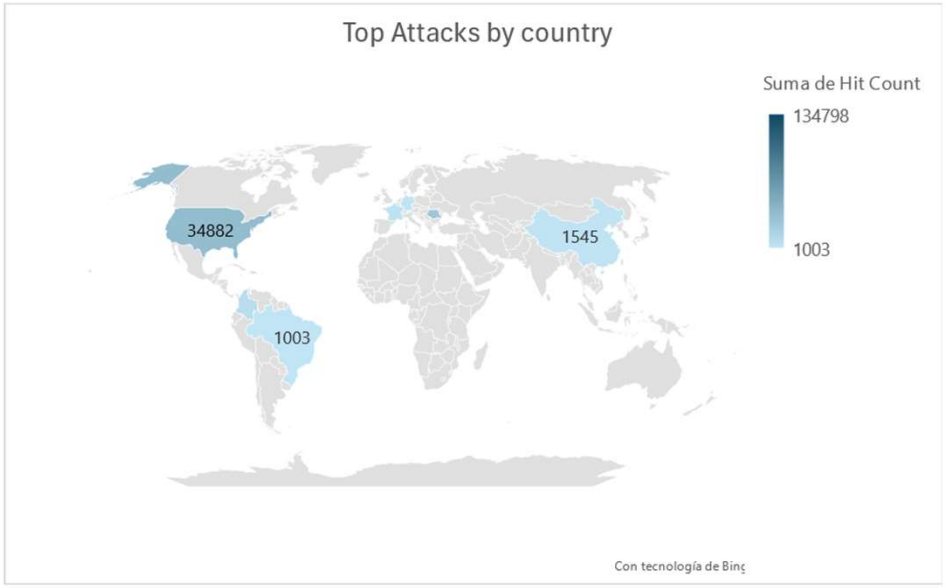
En el top de destino se encuentra la dirección IP **172.16.125.33, con 9161** registros.



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 de países

Top Attacks by country	
Etiquetas de fila	**Suma de Hit Count**
Brazil	1003
Germany	1199
China	1545
Taiwan	1624
France	2681
Colombia	6341
Romania	26351
Hong Kong	28391
Unknown	30781
United States	34882
Total general	134798

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.

- CASB, exclusión de dominio de Camacol de correos entrantes ya que se bloqueaba como SPAM.
- IPS, Antivirus, se asiste a las sesiones de auditorías de las soluciones de Trend Micro, dentro de la de Antivirus se encuentra algunos dispositivos que no tiene agente instalado, por lo que se hace seguimiento con mesa
- protección correo, Activación en modo de prueba del módulo de protección BEC, se envía información a seguridad de la información acerca de las alertas generadas.
- Se crea cambio para la solicitud de permisos, para la conexión de DDAN y V1, además de ZTNA Internet Access para su funcionamiento del módulo.
- IPS, validación de indicador de alerta en el servidor, se desactivan filtros que no hacen ningún match y que generan alto consumo de CPU, además se apagan las interfaces sin uso.
- Se evidencian un total de 1161 eventos de amenazas gestionados por Trend Micro, en su mayoría es por la detección por la regla Possible_Hifrm-6, se requiere validar los eventos para comprobar si son necesario excluirlos o son válidos.
- Se encontró el archivo Agent Dexon 5.1.3.222.exe, se requiere realizar seguimiento sobre el reporte del ejecutable en el dispositivo VGA-TCC-03-2331.
- Behavior Monitoring, se detectaron por este módulo el archivo TRAMITES.exe y Ahorro.exe estos se detectaron como archivos nuevos.
- Application Control, se encontró la ejecución de la aplicación Conda.exe, encontrada dentro de la lista de aplicaciones bloqueadas.
- El módulo de Device control, bloquea el uso no autorizado de dispositivos extraíbles, el usuario que mayor cantidad de eventos registra es aeguerrero con 16 registros.
- En el tipo de dispositivos que mayor cantidad de eventos registra, son dispositivos móviles.
- Dentro de las alertas más relevantes se encuentran las siguientes técnicas utilizadas, en las diferentes detecciones.
- Análisis inicial de compromiso: Técnicas relacionadas con phishing, archivos maliciosos y bypass de controles (e.g., MITRE.T1204.002, MITRE.T1548.002).
- Detección de persistencia y evasión: Abuso de DLL, herramientas legítimas, y manipulación de configuraciones (e.g., MITRE.T1574.001, XSAE.F3256).
- Movimiento lateral y exfiltración: Protocolo SMB y transferencias de archivos (e.g., MITRE.T1021.002, MITRE.T1105).
- XDR, En el top de eventos por nombre de acuerdo con el nombre de los archivos ejecutados, está el uso de la herramienta QuickAssist, para conexión remota, también el uso de MMC para administración de usuarios y la ejecución de Windows Powershell para desactivación de Windows Defender.
- XDR
    - Ejecución de comando sutil usn deletejournal /d /n c: y cipher /w:C:\, se escaló caso con administradores del servidor y se validó que correspondía a tareas

- administrativas, se recomienda el no uso del comando por borrado completo de información y no recomendado en entornos virtuales.
- 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.
- Domain Trust Discovery, está vinculado al intento de descubrimiento de relaciones de relaciones de confianza del dominio, este evento se genera por el despliegue de la herramienta Intune, de forma valida.
- El ultimo evento corresponde al acceso de la URL https://fulzzar[.]blogspot[.]com/favicon.ico, como pruebas realizadas por parte del administrador de DarkTrace.
- Se registran 4 eventos en el servidor FNABOGAPP015, por la regla de detección objetos embebidos en archivos. En específico, por el archivo 52 Informe de selecciÃ³n 023.pdf
- El módulo de Firewall de hosts ha sido activado en servidores, esto inicialmente en modo observación. De acuerdo a este módulo se generaron 3820 eventos, El evento que mayor cantidad de registros género es Retransmit, Ya se encuentra la mayoría de las reglas activas en modo bloqueo.
- 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.
- La mayoría de los eventos 3800 fueron bloqueados o denegados, los otros 20 fueron de auditoría.
- Los eventos que mayor cantidad de eventos registraron fueron los relacionados con los servicios de DNS y LDAP.
- El módulo de IPS de host en servidores se encuentra activo con el fin de identificar tráfico con comportamiento malicioso y vulnerabilidades de cara a la red. En el top de eventos se encuentra la regla: "Invalid Compression Denial of Service"
- 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, se requiere validar los servidores con las alertas.
- Inteligencia de amenazas se adicionan 93 reputaciones nuevas adicionadas por la integración con Threat Q, correspondientes a correos electrónicos y direcciones IP.
- Attack Surface Discovery, En el top de eventos, se registra los servidores bogpvpplp022, bogpvpplp015 y bogpvpplp019, con 86 vulnerabilidades y fallos en la configuración, con clasificación alta, es necesario mitigar las vulnerabilidades encontradas.
- Attack Surface Discovery, no se observa ninguna clasificación alta, la página con clasificación más alta es agendamiento.fna.gov.co.
- Para la cuenta de vigialdap tiene la mayor clasificación, se clasifica con riesgo alto, porque tiene bastantes permisos sobre la cuenta y porque tiene deshabilitada la opción de que la contraseña expire, entre otras vulnerabilidades.

- Attack Surface Discovery, la aplicación anyrun con clasificación media es la que mayor cantidad de visitas tiene.
- Attack Surface Discovery, en 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.
- IPS, Del total de los 139716 eventos, en su mayoría con clasificación major con el 58 % de los eventos.
- 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.
- IPS, el top de IP de origen 185.243.5.55 de Polonia con 23633 eventos.
- IPS, el top de destino se encuentra la dirección IP 172.16.125.33, con 9161 registros.
- IPS, En el top de eventos por país, se encuentra Estados unidos con mayor cantidad de registros, seguido de Hong Kong y Romania.
- CASB, se presentaron un total de 76942 eventos registrados por la solución CASB, 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 anomalías.
- CASB, En los eventos por nombre de anomalía, se encuentran correos con rutas compartidas, correos de marketing y correos relacionados con el malware Bazar.
- CASB, La cuenta que mayor cantidad de detecciones presenta es logistica@sumicorp.com y mailer-daemon@googlemail.com.
- CASB, En el top de correos remitentes de phishing esta la cuenta alertasynotificaciones[@]notificacionesbancolombia[.]com y dianisjulieth[.]07@hotmail.com.
- se relaciona el informe de 2190 dispositivos instalados en el periodo que comprende el periodo de 22 de noviembre al 21 de diciembre del 2024.

Informe de Consultoría

2024

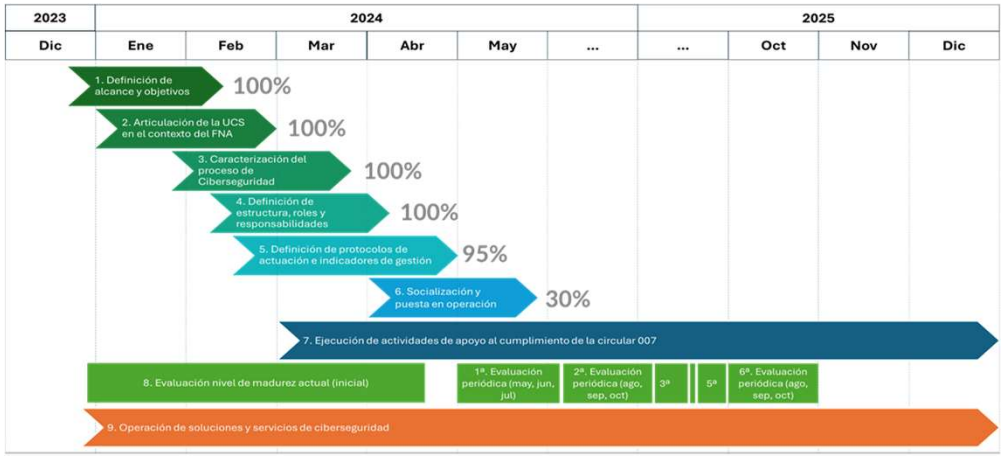
Objetivo

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

Alcance

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

Plan de implementación unidad de ciberseguridad



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

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

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

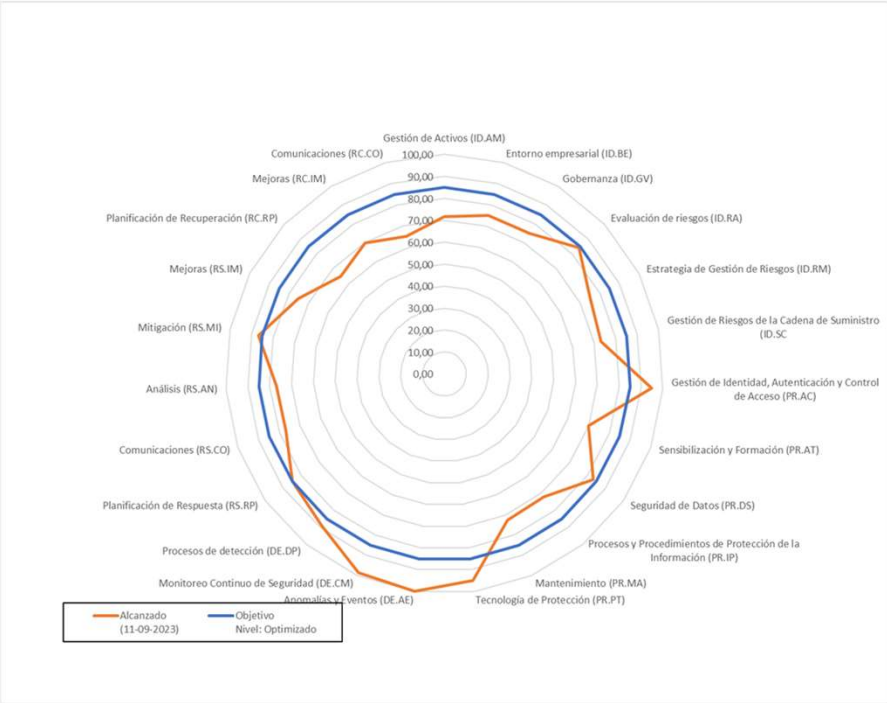
Se realiza el apoyo para la documentación de los catálogos de arquitectura empresarial de seguridad.

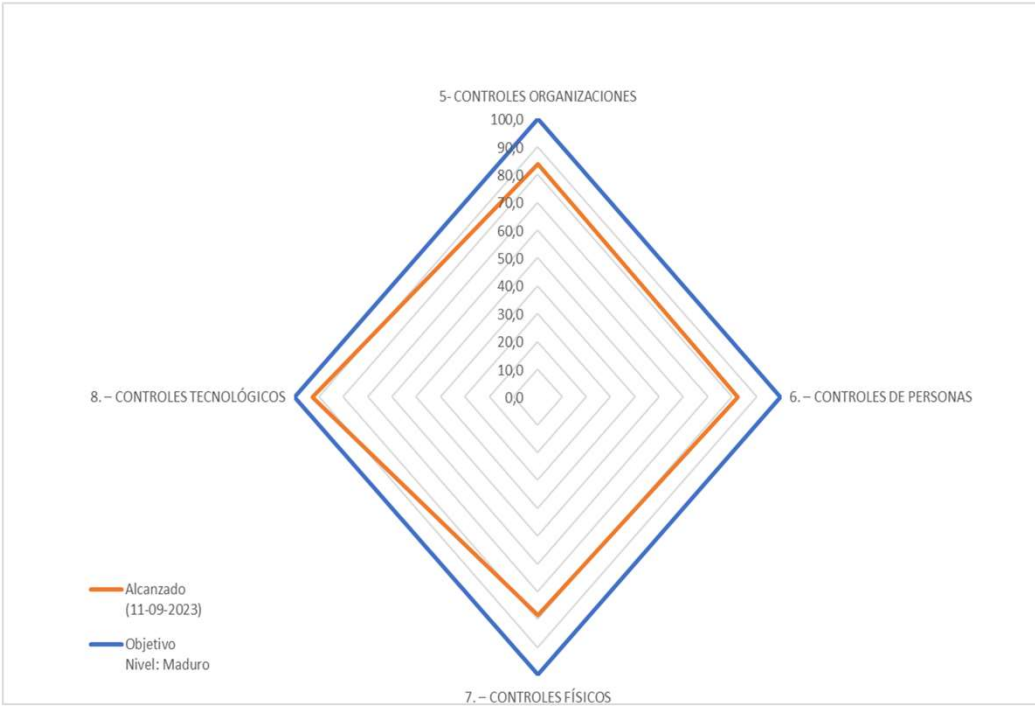
Plan de construcción de protocolos de actuación

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

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

Evaluación inicial del nivel de madurez - GAP





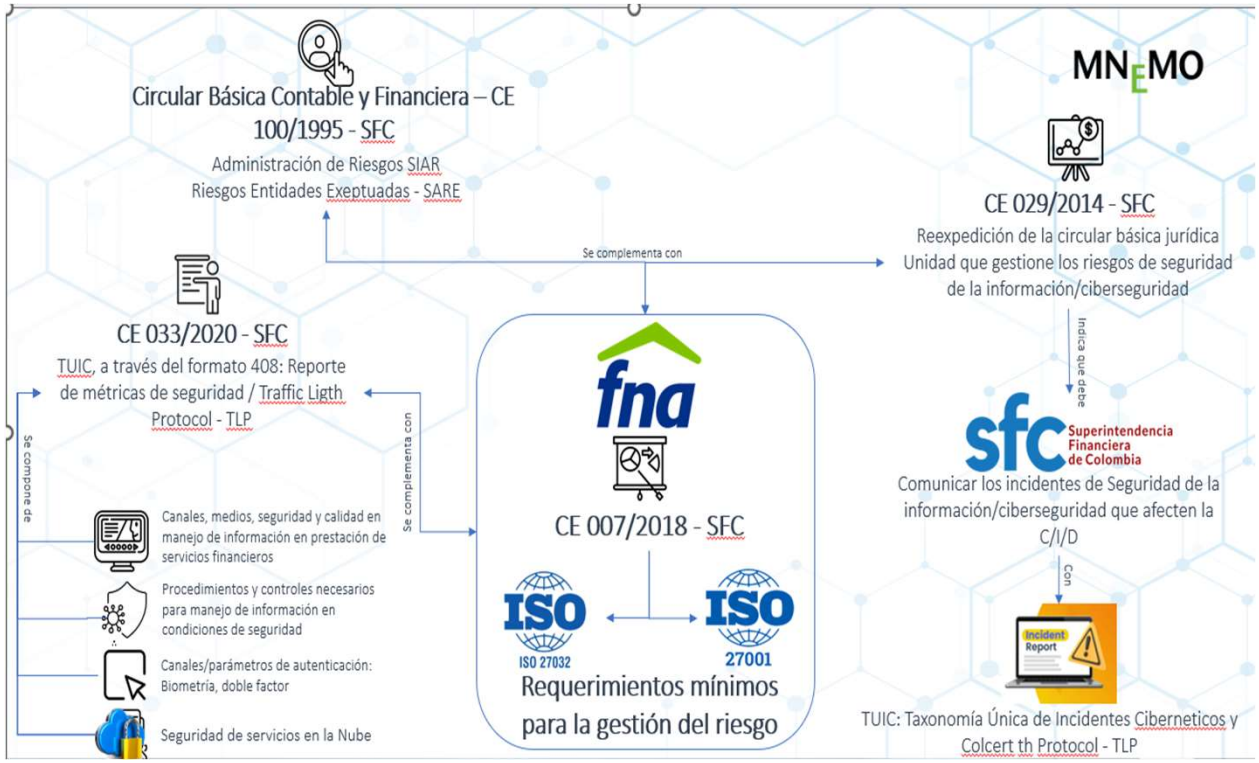
Construcción del modelo de análisis de nivel de madurez con base en marcos de referencia reconocidos como NIST, COBIT e ISO 27001.

Diseño preliminar de tableros de control



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

Apoyo al cumplimiento de la circular 007



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

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

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

CYBER SEC

PRE FACTURA

No. C-2-26

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

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2025-01-20

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

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

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
1	Administración y soporte de la plataforma XDR	1.00	3,326,000.00	3,957,940.00	0.00
2	Administración y soporte de la plataforma SOAR	1.00	14,627,000.00	17,406,130.00	0.00
3	Administración y soporte de la plataforma THREAT INTELLIGENCE	1.00	27,797,000.00	33,078,430.00	0.00
4	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	1.00	55,994,000.00	66,632,860.00	0.00
5	Administración y soporte Servicio de MONITOREO DE DNS	1.00	52,083,000.00	61,978,770.00	0.00
6	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	1.00	8,279,000.00	9,852,010.00	0.00
7	Administración y soporte de la plataforma CIBERDEFENSA	1.00	5,874,000.00	6,990,060.00	0.00
8	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	1.00	8,406,000.00	10,003,140.00	0.00
9	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	1.00	23,451,000.00	27,906,690.00	0.00
10	Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (IAM)	1.00	26,449,000.00	31,474,310.00	0.00

Total Bruto	226,286,000.00
Subtotal	226,286,000.00
IVA 19%	42,994,340.00
Total a Pagar	269,280,340.00

SUMA EN LETRAS: Doscientos sesenta y nueve millones doscientos ochenta mil trescientos cuarenta 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 Net Cash

BBVA Colombia
NIT 860.003.020-1
Certifica

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

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

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

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



Firma autorizada
BBVA Colombia

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14932552929

(415)7707212489984(8020) 000001493255292 9

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 4 4 7 9 6 8	1	Impuestos de Bogotá 3 2	

IDENTIFICACIÓN

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

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

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

35. Razón social
MNEMO CYBER SEC S.A.S

36. Nombre comercial	37. Sigla

UBICACIÓN

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

41. Dirección principal
CL 99 NO 10 19 OF 502

42. Correo electrónico j.parra@mnemo.com

43. Código postal	44. Teléfono 1	45. Teléfono 2
	6 9 1 3 1 3 3	

CLASIFICACIÓN

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

Responsabilidades, Calidades y Atributos

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

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

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

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

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

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2023 - 07 - 30 / 23 : 41: 33

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

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre VELEZ CASTRO HUMBERTO DE JESUS

985. Cargo Representante Legal Suplente Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 14932552929

(415)7707212489984(8020) **000001493255292 9**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 4 4 7 9 6 8	1	Impuestos de Bogotá 3 2	

Características y formas de las organizaciones

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

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 4	
72. Número		
73. Fecha	2 0 2 0 1 2 2 8	
74. Número de notaría		
75. Entidad de registro	0 3	
76. Fecha de registro	2 0 2 0 1 2 2 9	
77. No. Matrícula mercantil	0 3 3 2 0 4 4 3	
78. Departamento	1 1	
79. Ciudad/Municipio	4	
Vigencia		
80. Desde	2 0 2 0 1 2 2 8	
81. Hasta	2 0 9 9 1 2 3 1	

Composición del Capital

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

Entidad de vigilancia y control

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

Estado y Beneficio

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

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 14932552929

(415)7707212489984(8020) **000001493255292 9**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 4 4 7 9 6 8	1	Impuestos de Bogotá 3 2	

Representación

1

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

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

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

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

2

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

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

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

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 14932552929

(415)7707212489984(8020) **000001493255292 9**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 4 4 7 9 6 8	1	Impuestos de Bogotá 3 2	

Revisor Fiscal y Contador

Revisor fiscal principal

124. Tipo de documento	125. Número de identificación	126. DV	127. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	1 0 1 8 4 0 8 8 7 6		2 3 2 3 2 5 T

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
TOVAR	LOZANO	JAIRO	DAVID

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

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

Revisor fiscal suplente

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

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

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

147. Fecha de nombramiento

Contador

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

152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
PINZON	ROJAS	ANDRES	CAMILO

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14933306804

(415)7707212489984(8020) 000001493330680 4

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 3 0 6 6 8 7	2	Impuestos de Bogotá 3 2	

IDENTIFICACIÓN

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

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

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

35. Razón social
MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

36. Nombre comercial	37. Sigla

UBICACIÓN

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

41. Dirección principal
CL 99 10 19 OF 502

42. Correo electrónico Jc.aponte@mnemo.com

43. Código postal	44. Teléfono 1	45. Teléfono 2
	6 9 1 3 1 3 3	3 1 0 3 2 4 3 4 7 5

CLASIFICACIÓN

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

Responsabilidades, Calidades y Atributos

53. Código: 5 7 1 4 4 2 4 8 5 5

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

Usuarios aduaneros	Exportadores
54. Código (1 2 3 4 5 6 7 8 9 10 / 11 12 13 14 15 16 17 18 19 20)	55. Forma 56. Tipo; Servicio 1 2 3; 57. Modo; 58. CPC

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

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2023 - 07 - 31 / 16 : 56: 19

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

Sin perjuicio de las verificaciones que la DIAN realice.
Firma autorizada:

984. Nombre PARRA GAMBOA JOHN JAIRO
985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 14933306804

(415)7707212489984(8020) **000001493330680 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 3 0 6 6 8 7	2	Impuestos de Bogotá 3 2	

Características y formas de las organizaciones

62. Naturaleza	2	63. Formas asociativas	9 9	64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio	1

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 5	
72. Número		
73. Fecha	2 0 1 9 0 7 2 6	
74. Número de notaría	6 5	
75. Entidad de registro	0 3	
76. Fecha de registro	2 0 1 9 0 7 2 6	
77. No. Matrícula mercantil	0 0 0 3 1 4 4 6 0 3	
78. Departamento	1 1	
79. Ciudad/Municipio	0 0 1	
Vigencia		
80. Desde	2 0 1 9 0 7 2 6	
81. Hasta	9 9 9 9 1 2 3 1	

Composición del Capital

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

Entidad de vigilancia y control

88. Entidad de vigilancia y control

Estado y Beneficio

Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV
1	4 9	2 0 1 9 0 7 2 6		-
2	8 1	2 0 1 9 0 7 2 6		-
3		Año Mes Día		-
4		Año Mes Día		-
5		Año Mes Día		-

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 14933306804

(415)7707212489984(8020) 000001493330680 4

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 3 0 6 6 8 7	2	Impuestos de Bogotá 3 2	

Representación

1

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

2

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

3

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

4

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

5

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 14933306804

(415)7707212489984(8020) **000001493330680 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 3 0 6 6 8 7	2	Impuestos de Bogotá 3 2	

Revisor Fiscal y Contador

Revisor fiscal principal

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

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
VELEZ	CASTRO	HUMBERTO	DE JESUS

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

135. Fecha de nombramiento: 2 0 2 1 0 2 1 5

Revisor fiscal suplente

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

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

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

147. Fecha de nombramiento:

Contador

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

152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
TOVAR	LOZANO	JAIRO	DAVID

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

159. Fecha de nombramiento: 2 0 2 1 0 6 0 1

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14908474061

(415)7707212489984(8020) 000001490847406 1

5. Número de Identificación Tributaria (NIT)	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	27. Fecha expedición
Persona jurídica 1			

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

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

35. Razón social
MNEMO COLOMBIA SAS

36. Nombre comercial	37. Sigla

UBICACIÓN

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

41. Dirección principal
CL 99 10 19 OF 502

42. Correo electrónico recepcion.colombia@mnemo.com

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

CLASIFICACIÓN

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

Responsabilidades, Calidades y Atributos

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

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

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

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

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

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2023 - 04 - 14 / 10 : 02: 37

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

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre VELEZ CASTRO HUMBERTO DE JESUS

985. Cargo Representante Legal Suplente Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 14908474061

(415)7707212489984(8020) **000001490847406 1**

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

Características y formas de las organizaciones

62. Naturaleza	2	63. Formas asociativas	1 2	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	0 4
72. Número		
73. Fecha	2 0 1 0 1 1 1 2	2 0 1 3 0 4 1 8
74. Número de notaría		
75. Entidad de registro	0 3	0 3
76. Fecha de registro	2 0 1 0 1 1 1 9	2 0 1 3 0 7 0 9
77. No. Matrícula mercantil	0 2 0 4 5 1 6 2	0 2 0 4 5 1 6 2
78. Departamento	1 1	1 1
79. Ciudad/Municipio	4	4
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	91. Número de Identificación Tributaria (NIT)	92. DV
1	8 0	2 0 1 6 0 1 0 1		-
2		Año Mes Día		-
3		Año Mes Día		-
4		Año Mes Día		-
5		Año Mes Día		-

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 14908474061

(415)7707212489984(8020) **000001490847406 1**

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

Representación

1

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL PRIN 1 8	2 0 1 7 0 8 2 9

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

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

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

2

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL SUPL 1 9	2 0 2 2 0 1 1 7

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

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

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 14908474061

(415)7707212489984(8020) **000001490847406 1**

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

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

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

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

Revisor fiscal suplente

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

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

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

147. Fecha de nombramiento

Contador

148. Tipo de documento	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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14972953384

(415)7707212489984(8020) 000001497295338 4

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 7 8 1 6 2 5	1	Impuestos de Bogotá 3 2	

IDENTIFICACIÓN

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

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

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

35. Razón social
CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

36. Nombre comercial	37. Sigla

UBICACIÓN

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

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

42. Correo electrónico r.rojasarias@mnemo.com

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

CLASIFICACIÓN

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

Responsabilidades, Calidades y Atributos

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

07- Retención en la fuente a título de rent
14- Informante de exogena
48 - Impuesto sobre las ventas - IVA
55 - Informante de Beneficiarios Finales

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

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

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

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2024 - 01 - 16 / 17 : 26: 47

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

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre VELEZ CASTRO HUMBERTO DE JESUS

985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 14972953384

(415)7707212489984(8020) **000001497295338 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 7 8 1 6 2 5	1	Impuestos de Bogotá 3 2	

Características y formas de las organizaciones

62. Naturaleza	2	63. Formas asociativas		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica	3	69. Otras organizaciones no clasificadas		70. Beneficio	1

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 2	
72. Número		
73. Fecha	2 0 2 3 1 1 2 3	
74. Número de notaría		
75. Entidad de registro	9 8	
76. Fecha de registro	2 0 2 3 1 2 1 3	
77. No. Matrícula mercantil		
78. Departamento	1 1	
79. Ciudad/Municipio	0 0 1	
Vigencia		
80. Desde	2 0 2 3 1 2 1 3	
81. Hasta	2 0 2 5 1 2 3 1	

Composición del Capital

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

Entidad de vigilancia y control

88. Entidad de vigilancia y control

Estado y Beneficio

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

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 14972953384

(415)7707212489984(8020) **000001497295338 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 7 8 1 6 2 5	1	Impuestos de Bogotá	3 2

Representación

1

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

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

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

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

2

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

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

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

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

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

001

Espacio reservado para la DIAN

4. Número de formulario: 14972953384

(415)7707212489984(8020) **000001497295338 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 7 8 1 6 2 5	1	Impuestos de Bogotá 3 2	

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

1

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

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres

119. Razón social: MNEMO CYBER SEC S.A.S

120. Valor capital del socio	121. % Participación	122. Fecha de ingreso	123. Fecha de retiro
	5 0	2 0 2 3 1 1 2 3	

2

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

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres

119. Razón social: MNEMO COLOMBIA SAS

120. Valor capital del socio	121. % Participación	122. Fecha de ingreso	123. Fecha de retiro
	4 9	2 0 2 3 1 1 2 3	

3

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

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres

119. Razón social: MNEMO EVOLUTION & INTEGRATION SERVICES S.A.

120. Valor capital del socio	121. % Participación	122. Fecha de ingreso	123. Fecha de retiro
	1	2 0 2 3 1 1 2 3	

4

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres

119. Razón social

120. Valor capital del socio	121. % Participación	122. Fecha de ingreso	123. Fecha de retiro

5

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres

119. Razón social

120. Valor capital del socio	121. % Participación	122. Fecha de ingreso	123. Fecha de retiro

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 14972953384

(415)7707212489984(8020) **000001497295338 4**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 1 7 8 1 6 2 5	1	Impuestos de Bogotá 3 2	

Revisor Fiscal y Contador

Revisor fiscal principal

124. Tipo de documento	125. Número de identificación	126. DV	127. Número de tarjeta profesional

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres

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

135. Fecha de nombramiento

Revisor fiscal suplente

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

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

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

147. Fecha de nombramiento

Contador

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

152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
PINZON	ROJAS	ANDRES	CAMILO

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

159. Fecha de nombramiento
2 0 2 3 1 1 0 8

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN
POR UNA COLOMBIA MÁS HONESTA

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764062145032

(415)7707212489984(8020) 001876406214503 2

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
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	26.Departamento	27. Municipio
Colombia	Bogotá D.C.	Bogotá, D.C.

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

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

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

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

AUTORIZADO

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

Firma del solicitante

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

Firma del funcionario autorizado

1001. Apellidos y nombres VELEZ CASTRO HUMBERTO DE JESUS
1002. Tipo documento Cédula de Ciudadanía
1003. No. Identiflcación 8770446 1004. DV 3
1005. Cod. Representación Representante Legal Principal
1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

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

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

DIAN
POR UNA COLOMBIA MÁS HONESTA

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764062145032

(415)7707212489984(8020) 001876406214503 2

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

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

Rangos de numeración para autorizar, habilitar o inhabilitar

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

AUTORIZADO

Bogotá, 05 de Febrero 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

División de Tesorería
Documento de Pago

No. ORDEN DE PAGO	34	**FECHA DE CONTABILIZACION**	11-mar-25
No. DOCUMENTO DE PAGO	5300180274	**FECHA DE DOCUMENTO**	11-mar-25
		FECHA DE COMPENSACION	11-mar-25
PROPUESTA	49498	**FECHA DE LA PROPUESTA**	11-mar-25

RESPONSABLE DEL PAGO

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

DATOS GENERALES

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

BENEFICIARIO DEL PAGO

NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSEGURIDAD		
No. IDENTIFICACIÓN	9017816251	**TIPO DE IDENTIFICACIÓN**	25
NOMBRE:	CONSORCIO UNIDAD DE		
OBSERVACIONES:	FE34 RAD 02-2303-202502250261353		
NÚMERO DE CUENTA	2501050101	**TIPO DE CUENTA**	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	252.725.256		

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	5300180274	34	252.725.256	FE34 RAD 02-2303-202502250261353	6200000102	CTO 173 DE 2023

División de Presupuesto
Documento de Pago

N° ORDEN DE PAGO	5300180274	**FECHA DE CONTABILIZACIÓN**	25.02.2025
N° DE REFERENCIA	34	**FECHA DE PAGO**	11.03.2025

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	FE34 RAD 02-2303-202502250261353		

OBSERVACIONES:

INFORMACIÓN PRESUPUESTAL

SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
20001186	6200000102	00090	CTO 173 DE 2023 .	1000049730	5105629989	37.036.370
20001186	6200000102	00010	CTO 173 DE 2023 .	1000048947	5105629989	162.859.830
20001186	6200000102	00080	CTO 173 DE 2023 .	1000048952	5105629989	27.906.690
20001186	6200000102	00030	CTO 173 DE 2023 .	1000051924	5105629989	31.474.310
20001186	6200000102	00010	CTO 173 DE 2023 .	1000048947	5105629989	10.003.140
					AFECTACIÓN PEDIDO	269.280.340

DETALLE DE LA ORDEN DE PAGO

VALOR TOTAL FAC.	269.280.340,00
DESCUENTOS	16.555.084,00
NOTAS CRÉDITOS	0,00
VALOR A PAGAR	252.725.256,00

Usuario: Jessebell Mejias
Fecha de impresión: 17.03.2025