

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

INFORME No	45	FACTURA No	FECHA		
No. DE ACEPTACIÓN:		1000058966	16	12	25
			dd	mm	aaaa

1. GENERALIDADES DEL CONTRATO

CONTRATO No 173 **DE** 2023 **TIPO DE CONTRATO** 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 Juan Sebastián Cardenas Hernández
(Escriba nombre del supervisor o interventor del contrato) (Escriba nombre del supervisor o interventor del contrato)

APOYO SUPERVISIÓN Enrique Alfredo Arrazola Montes Jonathan Escobar Rodriguez
(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 Ciberseguridad 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 31 DE dic DE 2026
(Día) (Mes) (Año)

REGISTRO PRESUPUESTAL No. 5400001604 - 6200000102 - 5400001890 - 6200000115 - 5400002134

VALOR DEL CONTRATO

TREINTA Y SEIS MIL CUATROCIENTOS NOVENTA Y NUEVE MILLONES QUINIENTOS OCHENTA Y TRES MIL SEISCIENTOS DIEZ PESOS MONEDA CORRIENTE (\$36.499.583.610,00) M/CTE INCLUIDO IVA Y DEMÁS CONTRIBUCIONES A LAS QUE HAYA LUGAR.

ADICIÓN NRO. 1 DIECINUEVE MIL NOVECIENTOS VEINTIDOS MILLONES NOVECIENTOS OCHENTA Y SIETE MIL CUATROCIENTOS NOVENTA Y TRES PESOS MCTE (\$19.922.987.493)

ADICIÓN Nro. 2 DIECINUEVE MIL NOVECIENTOS SETENTA Y TRES MILLONES SEISCIENTOS TREINTA Y SIETE MIL DIEZ PESOS MCTE (\$19.973.637.010)

El valor del presente contrato es hasta la suma de SETENTA Y SEIS MIL TRESCIENTOS NOVENTA Y SEIS MILLONES DOSCIENTOS OCHO MIL CIENTO TRECE PESOS M/CTE (\$76.396.208.113,00)

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

PRÓRROGAS	
No.	PLAZO
1	12 meses

ADICIONES		
No.	VALOR	RP
1	\$ 19.922.987.493	5400001890
2	\$ 19.973.637.010	5400002134

SUSPENSIONES		
No	DESDE	HASTA

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	47,78%
Adición Nro. 1	\$ 19.922.987.493,00	26,08%
Adición Nro. 2	\$ 19.973.637.010,00	38,80%
VALOR TOTAL DEL CONTRATO	\$ 76.396.208.113,00	73,86%
Valor ejecutado antes del presente pago	\$ 51.474.843.637,00	67,38%
Valor del pago aprobado con el presente informe	\$ 272.973.255,00	0,36%
VALOR TOTAL EJECUTADO	\$ 51.747.816.892,00	67,74%
Porcentaje de ejecución presupuestal programado a la fecha		67,77%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,03%

OBSERVACIONES

Cuenta 45: Analisis de vulnerabilidades por demanda-Ethical Hacking por demanda - Ingeniería Social
Periodo 22-10-2025 al 21-11-2025
La diferencia en la ejecución Presupuestal se presenta por cobros de ANS en cuentas 3 y 4.

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

3. DESCRIPCION ACTIVIDADES

Porcentaje de ejecución de actividades proyectado a la fecha	100%
Porcentaje de ejecución de actividades realizado a la fecha	100%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CONTRATO	0%

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

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

SI ☐ NO ☒

*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 DOSCIENTOS SETENTA Y DOS MILLONES NOVECIENTOS SETENTA Y TRES MIL DOSCIENTOS CINCUENTA Y CINCO PESOS MCTE (\$ 272,973,255).

5. EVALUACIÓN CONTRATISTA (Escala de 0 - 5)

EVALUACION PARCIAL	
Cumplimiento del contrato	4
Plazos	4
Aspectos administrativos	4

6. CERTIFICACIÓN PARA PAGO

EL SUSCRITO GERENTE DE CIBERSEGURIDAD 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

DIECISEIS

16

días del mes de

DICIEMBRE

de

2025

(día en letras)

(día en números)

(mes en letras)

(Año)

Juan Sebastian Cardenas Hernández

**Gerente de Ciberseguridad y Aseguramiento Informatico
Supervisor CTO173-2023**

Revisó y aprobó: Enrique Alfredo Arrazola Montes - Jonathan Escobar Rodríguez Apoyos a la supervisión

Estadística de datos	Cantidad
Registros transferidos	6

Cl.doc. : RE (Factura bruto) Documento normal					
Reg.prelim.por		NTUIRAN	Contab.por		MRINCONZ
Nº doc.	5100002442	Sociedad	1000	Ejercicio	2025
Fe.docum.	17.12.2025	Fecha contab.	17.12.2025	Periodo	12
Calc.impuestos	☒				
Referen.	55				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202512181354132				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1003700788	CONSORCIO UNIDAD DE		W0	238,986,937-
2	86	2511950101	CXP PROVED EM/RF		W0	272,973,255
3	91	5130950401	CENTRO OPER SEG		W0	0
4	50	2519053801	RTE IVA TARIFA GENER			6,537,595-
5	50	2519054408	SERVICIOS 304 BOGOTA			2,215,901-
6	50	2519050401	HONORARIOS 11%			25,232,822-



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 55

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

Fecha y hora Factura	
Generación	17/12/2025, 13:24
Expedición	17/12/2025, 13:25
Vencimiento	16/01/2026

Ítem	Descripción	Cantidad	Valor desc.	Vr. Total
1	Análisis de vulnerabilidades por demanda-Ethical Hacking por demanda N° de aceptación 1000058966	1.00	0.00	244,047,580.00
2	Ingeniería Social N° de aceptación 1000058966	1.00	0.00	28,925,675.00

Total items: 2

Valor en Letras:

Doscientos setenta y dos millones novecientos setenta y tres mil doscientos cincuenta y cinco pesos m/cte

Forma de pago:

Crédito

Medio de pago:

Otro - Crédito - Cuota No. 001 vence el 2026-01-16 por \$ 272,973,255.00

Observaciones:

Distribución de ingreso:

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	229,389,289.92
IVA 19%	43,583,965.08
Total a Pagar	272,973,255.00

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: 57d354a0f6bc39922d177f1ce3a0629bfa52163f3aa39e1adb2ab8508e434edb7cdeb62d8da6a36aa06e126b0ef006a0

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 Diciembre 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 **MNEMO EVOLUTION & INTEGRATION SERVICES SA**, identificada con NIT 901.306.687-2, debidamente inscrito en la Cámara de Comercio de Bogotá D.C., luego de examinar de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico que la sucursal en mención **NO CUENTA CON PERSONAL VINCULADO EN COLOMBIA** por lo que no tiene obligaciones pendientes durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de presentación de la propuesta para el presente proceso de selección, por los conceptos de salud, pensiones, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002. Dada en Bogotá D.C., a los Once (11) días del mes de Diciembre de 2025.

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

HUMBERTO DE JESUS VELEZ CASTRO

C.C. 8.770.446 de Soledad – Atlántico

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

DATOS GENERALES DEL APORTANTE								
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Dirección	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
2025-10	2025-11	1940842585	9494863371	E	2025/11/21	2025/11/19	BANCO BBVA COLOMBIA S.A.	\$168,994,000

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 (92 Afiliados)																																																			

SUCURSAL: PRINCIPAL (92 Afiliados)

Página 2 de 6

33	CC	1026295259	BEJARANO QUIROGA ANDRES FELIPE							X							25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
34	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER														23020 1	30	MIN001	30	CCF24	30	14-25	30	0.522%	30		Si
35	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN														23030 1	30	EP5002	30	CCF24	30	14-25	30	0.522%	30		Si
36	CC	1122512867	CAMPOS MARTINEZ JUAN ALEJANDRO							X							23030 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
37	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID							X							23030 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
38	CC	80731020	DESALVADOR RESTREPO MARCELO														25-14	25	EP5017	25	CCF24	25	14-25	25	0.522%	25		Si
39	CC	80731020	DESALVADOR RESTREPO MARCELO								X						25-14	5	EP5017	5	CCF24	5	14-25	5	0.000%	5		Si
40	CC	1012976046	DIAZ MARIN CAMILO ARTURO							X							23030 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
41	CC	80102292	DIAZ TORRES CHRISTIAN ALEXANDER														23030 1	30	EP5008	30	CCF24	30	14-25	30	0.522%	30		Si
42	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER														25-14	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
43	CC	1001326677	GOMEZ PARRA CRISTIAN CAMILO							X							23020 1	30	EP5001	30	CCF24	30	14-25	30	0.522%	30		Si
44	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO														25-14	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
45	CC	1002811541	GRAJALES GUTIERREZ JESSICA ALEJANDRA														25-14	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
46	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN														23030 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
47	CC	1010840818	GUEVARA GUANCHA ERWIN SANTIAGO							X							25-14	30	EP5017	30	CCF24	30	14-25	30	0.522%	30		Si
48	CC	1082874657	GUEVARA RIZZO SANTIAGO							X							23030 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		Si
49	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES														23100 1	30	EP5005	30	CCF24	30	14-25	30	0.522%	30		No
50	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA														23030 1	22	EP5017	22	CCF24	22	14-25	22	0.522%	22		Si
51	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA								X						23030 1	8	EP5017	8	CCF24	8	14-25	8	0.000%	8		Si
52	CC	1099374748	LEAL GOMEZ DANIELA														23020 1	30	EP5037	30	CCF24	30	14-25	30	0.522%	30		Si
53	CC	1069769484	LOPEZ ZAMORA JUAN DAVID														23030 1	30	EP5002	30	CCF24	30	14-25	30	0.522%	30		Si

65	CC	1033801510	MONTALEGRE AMADO KESSICA YULIANA								X						230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
66	CC	1033711407	MURCIA TORRES JHON FREDY														230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
67	CC	1034660019	MURCIA CARVAJAL KAROL DANIELA														230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
68	CC	1011087203	MURCIA GUERRERO SAMUEL														230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
69	CC	1032479763	ORJUELA CALDERON PAULA NATALIA								X						231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
70	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER								X						230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
71	CC	1053328985	PAEZ CORTES LADY ZOLANYI								X						231001	26	EPS005	26	CCF24	26	14-25	26	0.522%	26		Si
72	CC	1053328985	PAEZ CORTES LADY ZOLANYI								X	X					231001	4	EPS005	4	CCF24	1	14-25	4	0.000%	1		Si
73	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN														231001	22	EPS017	22	CCF24	22	14-25	22	0.522%	22		Si
74	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN									X					231001	8	EPS017	8	CCF24	8	14-25	8	0.000%	8		Si
75	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO														230901	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
76	CC	1030618626	PINZON ROJAS ANDRES CAMILO														230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
77	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN								X						230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
78	CC	1019110870	RAMIREZ ALARCON CAMILO								X						230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
79	CC	1011096205	RIOS MONTAÑEZ DIEGO ALEXANDER														230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30		Si
80	CC	80218335	RIVEROS SALAMANCA ANDERSON														231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
81	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES	X							X					X	25-14	29	EPS010	29	CCF24	29	14-25	29	0.522%	29		Si
82	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES									X					25-14	1	EPS010	1	CCF24	0	14-25	1	0.000%	0		Si
83	CC	1003712217	RODRIGUEZ PENAGOS JOAN SEBASTIAN								X						230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
84	CC	1005012004	RODRIGUEZ CONDE MARIA FERNANDA														230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
85	CC	52505417	ROJAS PEÑA NILSA YAMILE														25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30		Si
86	CC	1030697447	ROJAS PEREZ VALENTINA								X						230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
87	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO														230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
88	CC	1034657947	SANTA HENAO DANNIEL								X						230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
89	CC	1000470126	SILVA BELTRAN JULIAN ANDRES								X						230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
90	CC	1003916380	SUAREZ BERDUGO SAMUEL ELIAS								X						230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
91	CC	1030539604	TAMAYO RIVERA FABIO ANDRES														230901	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
92	CC	1020808701	TIBADIUIZA CALDERON SEBASTIAN														231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
93	CC	1018408876	TOVAR LOZANO JAIRO DAVID														230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
94	CC	1014279176	URBANO ARDILA SEBASTIAN								X						25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
95	CC	80247522	YARGAS HINCAPIE CARLOS														25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
96	CC	1032424681	YARGAS HERRERA FERNANDO ARTURO														230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
97	CC	1075280531	YARGAS POLANIA JAIRO ALEXANDER														231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30		Si
98	CC	1014197302	VELASQUEZ RAMOS JOHAN SEBASTIAN														25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si

Página 5 de 6

DATOS GENERALES DEL APORTANTE										
Identificación	dv	Razon Social		Clase Aportante		Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS		B - MENOS DE 200 COTIZANTES		PRINCIPAL	CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION										
Periodo		Clave		Tipo	Fecha		Pago			
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor	
2025-10	2025-11	1940842585	9494863371	E	2025/11/21	2025/11/19	BANCO BBVA COLOMBIA S.A.	0	\$168,994,000	
RESUMEN DE PAGO										
RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR		
AFP (ADMINISTRADORAS: 5)				93	\$92,495,100	\$0	\$0	\$92,495,100		
COLFONDOS	231001	800,227,940	6	14	\$20,509,500	\$0	\$0	\$20,509,500		
COLPENSIONES	25-14	900,336,004	7	19	\$21,811,000	\$0	\$0	\$21,811,000		
PORVENIR	230301	800,224,808	8	36	\$24,744,900	\$0	\$0	\$24,744,900		
PROTECCION	230201	800,229,739	0	21	\$20,499,700	\$0	\$0	\$20,499,700		
SKANDIA	230901	800,253,055	2	3	\$4,930,000	\$0	\$0	\$4,930,000		
ARL (ADMINISTRADORAS: 1)				95	\$4,433,900	\$0	\$0	\$4,433,900		
COLMENA	14-25	800,226,175	3	95	\$4,433,900	\$0	\$0	\$4,433,900		
CCF (ADMINISTRADORAS: 2)				95	\$24,447,800	\$0	\$0	\$24,447,800		
COMFENALCO VALLE	CCF56	890,303,093	5	2	\$117,900	\$0	\$0	\$117,900		
COMPENSAR	CCF24	860,066,942	7	93	\$24,329,900	\$0	\$0	\$24,329,900		
EPS (ADMINISTRADORAS: 10)				95	\$39,046,700	\$0	\$0	\$39,046,700		
ALIANSAUD EPS (ANTES COLMEDICA)	EPS001	830,113,831	0	3	\$2,135,600	\$0	\$0	\$2,135,600		
CAPITAL SALUD	EPSC34	900,298,372	9	1	\$138,300	\$0	\$0	\$138,300		
COMPENSAR	EPS008	860,066,942	7	15	\$3,178,200	\$0	\$0	\$3,178,200		
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	3	\$378,400	\$0	\$0	\$378,400		
FAMISANAR	EPS017	830,003,564	7	10	\$1,905,800	\$0	\$0	\$1,905,800		
FOSYGA	MIN001	901,037,916	1	7	\$3,659,600	\$0	\$0	\$3,659,600		
FOSYGA RÉGIMEN DE EXCEPCIÓN	MIN002	901,037,916	1	1	\$220,000	\$0	\$0	\$220,000		
NUEVA E.P.S.	EPS037	900,156,264	2	5	\$749,600	\$0	\$0	\$749,600		
SALUD TOTAL	EPS002	800,130,907	4	9	\$3,122,100	\$0	\$0	\$3,122,100		
SANITAS	EPS005	800,251,440	6	41	\$23,559,100	\$0	\$0	\$23,559,100		
ICBF (ADMINISTRADORAS: 1)				10	\$5,142,400	\$0	\$0	\$5,142,400		
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	10	\$5,142,400	\$0	\$0	\$5,142,400		
SENA (ADMINISTRADORAS: 1)				10	\$3,428,100	\$0	\$0	\$3,428,100		
SENA	PASENA	899,999,034	1	10	\$3,428,100	\$0	\$0	\$3,428,100		
TOTAL				95	\$168,994,000	\$0	\$0	\$168,994,000		

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	Días Mora	Valor
2025-10	2025-11	1936964657	9494819980	E	2025/11/19	2025/11/18	BANCO DAVIVIENDA	0	\$90,510,800

LIQUIDACION DETALLADA DE APORTES																														
EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS		PARAFISCALES		
No.	Identificación	Nombre	ing	ret	de	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (61 Afiliados)																														
Centro de Trabajo: CENTRO TRABAJO 1 (60 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (60 Afiliados)																														
1	CC	53049489	ACERO PALOMARES IVONNE FARIDE	X																230301	22	EPS008	22	CCF24	22	14-25	22	0.522%	22	Si
2	CC	53049489	ACERO PALOMARES IVONNE FARIDE												X					230301	8	EPS008	8	CCF24	8	14-25	8	0.000%	8	Si
3	CC	11204846	AFANADOR TORRES FRANZ JOAO																	25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
4	CC	1032392540	ALDANA FLOREZ JUAN SEBASTIAN								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
5	CC	86055602	ALFEREZ MARTINEZ CARLOS FERNEY	X																231001	10	MIN001	10	CCF24	10	14-25	10	0.522%	10	Si
6	CC	1015425546	CAITA CORREA CHRISTIAM GERMAN																	25-14	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
7	CC	1015425546	CAITA CORREA CHRISTIAM GERMAN										X							25-14	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	Si
8	CC	1103101791	CANARIA ASCENCIO JEISON SMITH																	230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
9	CC	80772089	CARDENAS RAMOS ROGER DANIEL																	231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
10	CC	1023957330	CARDONA CASTRO JUAN SEBASTIAN																	230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
11	CC	1001346794	CASTELLANOS CRISTIANCHO YOAN NICOLAS																	230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
12	CC	1081728680	CHAVARRO MEDINA MARYI VANESA								X									230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
13	CC	1000850961	CHIPATECUA PINEDA JOSE STEVEN								X									25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
14	CC	1070981128	COLLAZOS FONSECA MATEO																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
15	CC	1018423823	CORTES GUTIERREZ ALFREDO ALEJANDRO																	230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
16	CC	80169118	COY FRANCO JOHAN MANUEL																	230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
17	CC	79619776	ENCISO ALARCON JOHN JAIRO																	231001	25	MIN001	25	CCF24	25	14-25	25	0.522%	25	Si
18	CC	79619776	ENCISO ALARCON JOHN JAIRO												X					231001	5	MIN001	5	CCF24	5	14-25	5	0.000%	5	Si
19	CC	79752133	GACHARNA GACHARNA FEDERICO	X																25-14	10	EPS005	10	CCF24	10	14-25	10	0.522%	10	Si
20	CC	1014209187	GALEANO FORTALECHE DIANA PATRICIA		X														X	25-14	19	EPS005	19	CCF24	19	14-25	19	0.522%	19	Si
21	CC	1000620156	GAMARRA SANCHEZ LEIDY CAROLINA									X								230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
22	CC	91180662	GARRIDO PRADA YEINSON ALBERTO																	230301	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
23	CC	80833507	GONZALEZ RODRIGUEZ WILLIAM IVAN		X						X								X	230301	20	EPS008	20	CCF24	20	14-25	20	0.522%	20	Si
24	CC	1012384194	HERRERA CARDENAS DANIEL FELIPE									X								230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si

25	CC	80048819	JARAMILLO RAMIREZ MIGUEL ANGEL																	25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
26	CC	52546926	JEREZ DUARTE MARIBEL	X																23030 1	10	EPS005	10	CCF24	10	14-25	10	0.522%	10		Si
27	CC	1024460422	JIMENEZ JIMENEZ BRAYAN STEVEN															X		25-14	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30		Si
28	CC	1193390038	LIZARAZO HERNANDEZ ANDREY JAVIER																	23020 1	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
29	CC	1016017636	MARTIN GONZALEZ GUSTAVO ADOLFO																	25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
30	CC	13871620	MARTINEZ CARREÑO HECTOR MANUEL															X		23090 1	3	EPS005	3	CCF24	3	14-25	3	0.000%	3		Si
31	CC	13871620	MARTINEZ CARREÑO HECTOR MANUEL																	23090 1	27	EPS005	27	CCF24	27	14-25	27	0.522%	27		Si
32	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																	23020 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30		Si
33	CC	1018453849	MERCHAN SANCHEZ LUISA FERNANDA															X		23030 1	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
34	CC	1032488654	MESA TORRES NICOLAS																	23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
35	CC	1030696891	MORALES CASTELLANOS BRAIAN DANIEL															X		23030 1	25	EPS017	25	CCF24	25	14-25	25	0.522%	25		Si
36	CC	1030696891	MORALES CASTELLANOS BRAIAN DANIEL															X		23030 1	5	EPS017	5	CCF24	5	14-25	5	0.000%	5		Si
37	CC	1023937645	MORENO DIAZ WENDY JOHANNA															X		23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
38	CC	1144066570	Ocampo Sanchez Angie Liliana															X		23030 1	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30		Si
39	CC	1000351714	OCHOA CASALLAS DIEGO ALEXANDER	X																25-14	4	EPS005	4	CCF24	4	14-25	4	0.522%	4		Si
40	CC	85435109	PAYARES IBAÑEZ JOSE MANUEL																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
41	CC	1001202777	Peña Acosta Stefanny																	23030 1	30	EPS008	30	CCF24	30	14-25	30	0.522%	30		Si
42	CC	1098647425	PEREZ MARTINEZ FRANCO JAVIER	X														X		23020 1	8	EPS005	8	CCF24	8	14-25	8	0.522%	8		Si
43	CC	80093909	PICO Carreño Mauro Javier																	25-14	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si
44	CC	1070971441	PINEDA Duarte Oscar Javier															X		23030 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30		Si

59	CC	79729048	URIBE RUIZ WILSON																X								25-14	3	MIN001	3	CCF24	3	14-25	3	0.000%	3	Si
60	CC	79729048	URIBE RUIZ WILSON																								25-14	27	MIN001	27	CCF24	27	14-25	27	0.522%	27	Si
61	CC	1031143384	URREGO BOLIVAR SANDRO JAVIER																X								23020 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
62	CC	1025142024	VALERO RICAURTE JOHAN STIF																X								23030 1	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	79627239	VARGAS RAMIREZ JHON MAURICIO																								25-14	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
64	CC	1015404947	VARGAS MARTINEZ JOSE DAVID																								23100 1	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
65	CC	80504200	VEGA CASTILLO DIEGO ANDRES																								25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
66	CC	1002559699	VEGA CORREDOR SERGIO LEONARDO																								23020 1	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
67	CC	1070307880	ZAMBRANO OSORIO OSCAR ANDRES																X								23020 1	30	EPS041	30	CCF24	30	14-25	30	0.522%	30	Si
68	CC	1035415884	ZAPATA QUIJANO OSWALDO JUAN																								23030 1	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	No
69	CC	1022438994	ZARAMA CAMPOS JUAN SEBASTIAN																X								23020 1	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																																					
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																																					
70	CC	1070917650	HERNANDEZ PEREZ YENNY FERNANDA																								23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
Total Afiliados(61)																																					

DATOS GENERALES DEL APORTANTE								
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 901447968	1	MNEMO CYBER SEC SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CL 99 10 19	BOGOTA-BOGOTA D.E.	5527210	Si
DATOS GENERALES DE LA LIQUIDACION								
Periodo		Clave		Tipo	Fecha		Pago	
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Valor
2025-10	2025-11	1936964657	9494819980	E	2025/11/19	2025/11/18	BANCO DAVIVIENDA	\$90,510,800
RESUMEN DE PAGO								
RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				61	\$56,066,700	\$0	\$0	\$56,066,700
COLFONDOS	231001	800,227,940	6	5	\$4,434,300	\$0	\$0	\$4,434,300
COLPENSIONES	25-14	900,336,004	7	17	\$20,023,600	\$0	\$0	\$20,023,600
PORVENIR	230301	800,224,808	8	25	\$19,527,100	\$0	\$0	\$19,527,100
PROTECCION	230201	800,229,739	0	12	\$10,095,700	\$0	\$0	\$10,095,700
SKANDIA	230901	800,253,055	2	2	\$1,986,000	\$0	\$0	\$1,986,000
ARL (ADMINISTRADORAS: 1)				61	\$1,800,000	\$0	\$0	\$1,800,000
COLMENA	14-25	800,226,175	3	61	\$1,800,000	\$0	\$0	\$1,800,000
CCF (ADMINISTRADORAS: 1)				61	\$13,606,400	\$0	\$0	\$13,606,400
COMPENSAR	CCF24	860,066,942	7	61	\$13,606,400	\$0	\$0	\$13,606,400
EPS (ADMINISTRADORAS: 9)				61	\$16,992,100	\$0	\$0	\$16,992,100
CAPITAL SALUD	EPSC34	900,298,372	9	2	\$265,600	\$0	\$0	\$265,600
COMPENSAR	EPS008	860,066,942	7	7	\$1,425,600	\$0	\$0	\$1,425,600
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	4	\$2,293,300	\$0	\$0	\$2,293,300
FAMISANAR	EPS017	830,003,564	7	14	\$2,928,100	\$0	\$0	\$2,928,100
FOSYGA	MIN001	901,037,916	1	4	\$1,046,800	\$0	\$0	\$1,046,800
NUEVA E.P.S.	EPS037	900,156,264	2	2	\$283,300	\$0	\$0	\$283,300
NUEVA EPS MOVILIDAD	EPS041	900,156,264	2	1	\$160,500	\$0	\$0	\$160,500
SALUD TOTAL	EPS002	800,130,907	4	10	\$3,833,600	\$0	\$0	\$3,833,600
SANITAS	EPS005	800,251,440	6	17	\$4,755,300	\$0	\$0	\$4,755,300
ICBF (ADMINISTRADORAS: 1)				3	\$1,227,400	\$0	\$0	\$1,227,400
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	3	\$1,227,400	\$0	\$0	\$1,227,400
SENA (ADMINISTRADORAS: 1)				3	\$818,200	\$0	\$0	\$818,200
SENA	PASENA	899,999,034	1	3	\$818,200	\$0	\$0	\$818,200
TOTAL				61	\$90,510,800	\$0	\$0	\$90,510,800

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

Acta N°	136/ 25-0844	Tema:	Reunión de revisión de ANS, contrato 173 de 2023, Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda– e ingeniería social del año 2025.
Fecha:	28/11/2025	Ubicación:	Virtual.
Hora inicio:	4:00 pm	Hora fin:	4:30 pm

Objetivo	Reunión de revisión de ANS, contrato 173-2023 para Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda– e ingeniería social del año 2025.		
PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	Dependencia	Cargo	¿Asistió?
Enrique Alfredo Arrazola	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 03	Si
Jonathan Escobar	Gerencia de Estrategia de TI y Aseguramiento Informático	Profesional 02	Si
María Camila Vargas	Mnemo	Apoyo a la Gerencia del Proyecto	Si
Cesar Orlando Pinto	Mnemo	Gerente de Proyecto Mnemo	Si

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

TEMAS TRATADOS

Revisión cumplimiento de ANS para los ejercicios de Análisis **de Vulnerabilidades por demanda – Ethical Hacking por demanda– e ingeniería social del año 2025**, contrato FNA-173-2023.

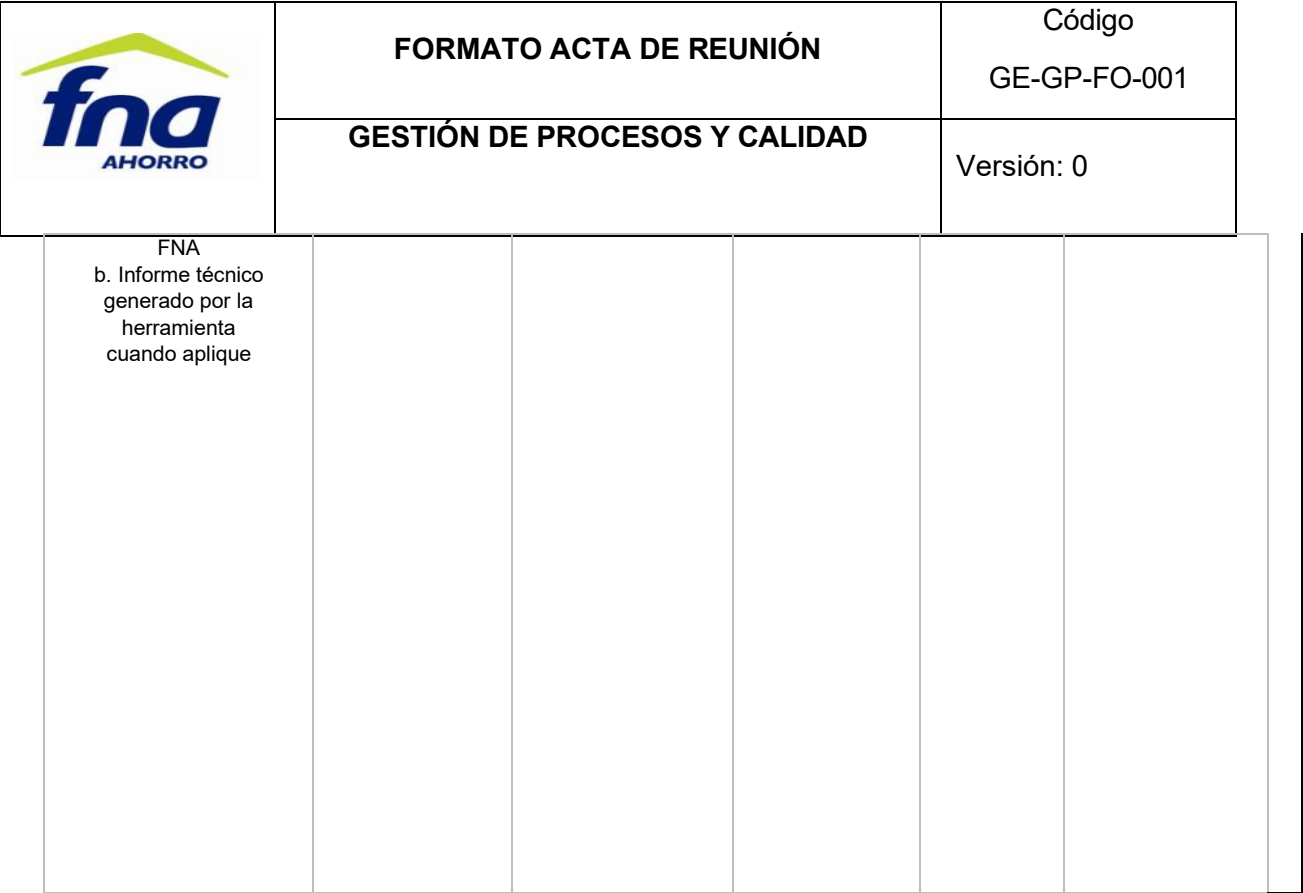
ACUERDO NIVELES DE SERVICIO

- GTGGTFO013 - ANS GENERALES UNIDAD DE CIBERSEGURIDAD (Servicios de Seguridad Integrados) V1

1. DOCUMENTACIÓN CONTRACTUAL

Se realiza la entrega de los informes de análisis de vulnerabilidades y ethical hacking por demanda , así mismo el del ejercicio de ingeniería social del año 2025.

2. Documentación Mensual o cuando se requiera					
Asegurar el cumplimiento de los procedimientos, políticas, normas y directrices establecidas por el FNA.					
Documentación Mensual	ANS Establecido	Número de incumplimientos	Compensación	Valor a Descontar	Observación
1.7.3 Informe ingeniería social (1 obligatorio al año), el cual debe contener como mínimo: a. Informe ejecutivo b. Informe técnico c. Metodología de ejecución de las pruebas 1.7.4 Informe de análisis de vulnerabilidades por demanda – Ethical hacking por demanda, el cual debe contener como mínimo: a.Formato Matriz de vulnerabilidades	Por cada 5 incumplimientos 0,5% del valor de la facturación mensual que se irán acumulando	0	0	0	Informes de ingeniería social enviados el 18 de noviembre, dentro del plazo del contrato correspondiente al año 2025. Informes de análisis de vulnerabilidades y ethical hacking por demanda, enviados en el transcurso del proyecto.



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

2. SISTEMA DE GESTIÓN DE CALIDAD

Se da cumplimiento al uso de los formatos y procedimientos del FNA.

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

3. CUMPLIMIENTO DEL CRONOGRAMA

Se da cumplimiento de este ítem de acuerdo con las siguientes observaciones y acuerdos entre las partes.

Ingeniería social: Se debe ejecutar al menos una vez al año. El ejercicio del año 2025 se ejecutó en los meses de octubre y noviembre del año 2025, lo cual da cumplimiento a las fechas de entrega dentro de los plazos del contrato. Así mismo se inició una vez se tuvo la aprobación de las gerencias de seguridad de la información y gerencia de ciberseguridad y aseguramiento informático y la entrega de los insumos por parte de FNA para iniciar las pruebas de ingeniería social.

Análisis de vulnerabilidades y ethical hacking por demanda: Estos ejercicios no tienen una fecha definida de entrega, dado a que son solicitudes que se escalan por parte de FNA durante todo el transcurso del contrato.

4. DETERMINACIÓN DEL VALOR A FACTURAR

Una vez verificados los conceptos por ANS, se define que el contratista CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA cumplió con el desarrollo del servicio dentro de las condiciones pactadas en el documento de GTGGTFO013 - ANS GENERALES UNIDAD DE CIBERSEGURIDAD (Servicios de Seguridad Integrados) V1, no se genera una Aplicación de Ans

		FORMATO ACTA DE REUNIÓN		Código GE-GP-FO-001	
		GESTIÓN DE PROCESOS Y CALIDAD		Versión: 0	
Descripción	Precio unitario IVA incluido	Aplicación ANS	Valor después de ANS	Valor total IVA incluido	Valor total IVA incluido
-Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda	205.082.000,00 COP	\$ 0,00	\$ 205.082.000,00	\$ 38.965.580,00	\$ 244.047.580,00
Ingeniería social	24.307.289,92 COP	\$ 0,00	\$ 24.307.289,92	\$ 4.618.385,08	\$ 28.925.675,00
TOTAL					\$ 272.973.255,00

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

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

ELABORÓ	APROBÓ
 Cesar Orlando Pinto Gerente de Proyecto Consortio Unidad de ciberseguridad	 Enrique Alfredo Arrázola Montes Profesional 03 Gerencia de ciberseguridad y Aseguramiento Informático
	APROBÓ
	 Jonathan Escobar Profesional universitario 2 Gerencia de ciberseguridad y Aseguramiento Informático



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

SUPERVISIÓN AL CONTRATO No. 173 de 2023
FONDO NACIONAL DEL AHORRO
Informe No. 45

-Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda y -Ejercicio de Ingeniería Social.

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

Bogotá, D.C. diciembre 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 Jefatura de la Gerencia de Estrategia TI y Aseguramiento Informático del FONDO NACIONAL DEL AHORRO, se realizó el seguimiento a las actividades conforme a lo establecido en el CTO 173 de 2023. El presente informe tiene como fin el análisis realizado en cuanto al cumplimiento del hito referente a Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda y 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

De acuerdo con lo establecido en el CTO 173 de 2023, se realiza el seguimiento, control y verificación del hito referente a Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda y Ejercicio de Ingeniería Social, donde se detalla lo siguiente:



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

ACTIVIDADES REALIZADAS

- a) Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda
Actividades solicitadas por demanda durante la ejecución contractual. Un solo pago por la vigencia del contrato.

Ejemplos solicitudes por demanda:

Re: Urgente - Solicitud Re-test de **Ethical** Hacking y Código Dinámico

 César Orlando Pinto González
Para  Jhoan David Agudelo Enciso;  Cristian Samir Acosta Fuentes
CC  Andrey Javier Lizarazo Hernández;  Andrés Tamayo Rivera
mar 18/11/2025 11:37 a.m.

 Este remitente co.pintogonzalez@mnemo.com es externo a la organización.
 Mensaje reenviado el 18/11/2025 11:40 a.m..

 Matriz de vulnerabilidades ACD FERP 2025.xlsx
681 KB

 Matriz de vulnerabilidades ACD Operaciones Reciprocas 2025.xlsx
290 KB

 Matriz de vulnerabilidades ACD FELE 2025.xlsx

Buenos días

Adjunto informes de los retest de los análisis de código solicitados.

Quedamos atentos a cualquier inquietud

Cordialmente

Cesar Orlando Pinto

Informe Ejercicio a **CCTV**

JE Jonathan Escobar Rodriguez

Para ☐ Seguridad de la Información; ☒ Leivi Dayana Cortes Bautista;
☒ Juan Carlos Martínez Carrillo

CC ☒ Juan Sebastian Cardenas Hernández; ☒ Cristian Samir Acosta Fuentes;
☒ Enrique Alfredo Arrazola Montes

vie 21/11/2025 11:53

 Informe_Simulacro_Ataque_Denegacion_Servicio (004).pdf
583 KB

 Minutograma.xlsx
67 KB

 EH - Red_Nueva_CCTV.xlsx

Buenas tardes,

Se envía el reporte del ejercicio realizado al **CCTV** implementado en el FNA:

- **EH – Red_Nueva CCTV** (documento con las vulnerabilidades encontradas en la primera revisión).
- **Minutograma** (proceso ejecutado para el ejercicio de evaluación del sistema).
- **Informe_Simulacro_Ataque_Denegación_Servicio (004)** (informe final del ejercicio realizado).

Re: Solicitud ETH y ACD

AT Andrés Tamayo Rivera <fa.tam>

Para ☒ Jhoan David Agudelo Enciso
CC ☒ Cristian Samir Acosta Fuentes; ☐ César Orlando Pinto González

 Este remitente fa.tamayorivera@mnemo.com es externo a la organización.

 Informe-EH atencion cl cliente - Asesores.xlsx
1 MB

 Informe-EH atencion cl cliente - Asesores - Administrador.pdf
2 MB

Buenas tardes,

Envío adjunto resultados del EH solicitado.

Quedo atento a sus comentarios.

Saludos.

El mié, 16 jul 2025 a las 16:09, Jhoan David Agudelo Enciso (<jhagudeloe@fna.gov.co>)

Buena tarde



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

RV: #FNA# INFORMES DE LOS 8 ACTIVOS ETHICAL HACKING CAJA GRIS 2025



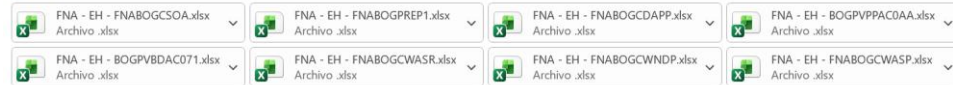
Cristian Samir Acosta Fuentes

Para Jhoan David Agudelo Enciso; Juan Carlos Martínez Carrillo
CC Seguridad de la Información

Responder Responder a todos Reenviar

jue 2/10/2025 3:45 p.m.

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.



FYI

De: César Orlando Pinto González <co.pintogonzalez@mnemo.com>

Enviado el: miércoles, 17 de septiembre de 2025 12:00 p. m.

Para: Cristian Samir Acosta Fuentes <cacosta@fna.gov.co>; Enrique Alfredo Arrazola Montes <Earrazola@fna.gov.co>

CC: Henry Vargas Hincapié <h.vargashincapie@mnemo.com>; Sergio Sanclemente <s.sanclemente@mnemo.com>; María Camila Vargas León <c.vargasleon@mnemo.com>; Juan Sebastian Cardenas Hernández <jcardenash@fna.gov.co>

Asunto: #FNA# INFORMES DE LOS 8 ACTIVOS ETHICAL HACKING CAJA GRIS 2025

Buen día ingenieros,

Adjunto a este correo los informes de los ejercicios de ethical hacking en modalidad de caja gris, realizados sobre los 8 activos que fueron enviados por parte de FNA, de un total de 15 posibles, según lo acordado en el acta de ANS #40 adjunta (FNA - 173 - Adición - Acta_Revisión ANS_40 01042025 licenciamiento ciberanalítica).

Los ejercicios se ejecutaron para dar cumplimiento a la fecha de entrega establecida antes del 30 de septiembre. A continuación, se detalla la lista de los 8 activos incluidos en los informes:

RV: #FNA# INFORMES DE LOS 8 ACTIVOS ETHICAL HACKING CAJA GRIS 2025



Cristian Samir Acosta Fuentes

Para Jhoan David Agudelo Enciso; Juan Carlos Martínez Carrillo
CC Seguridad de la Información

Responder Responder a todos Reenviar

jue 2/10/2025 3:46 p.m.

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.



De: César Orlando Pinto González <co.pintogonzalez@mnemo.com>

Enviado el: martes, 23 de septiembre de 2025 11:37 a. m.

Para: Cristian Samir Acosta Fuentes <cacosta@fna.gov.co>; Enrique Alfredo Arrazola Montes <Earrazola@fna.gov.co>

CC: Henry Vargas Hincapié <h.vargashincapie@mnemo.com>; Sergio Sanclemente <s.sanclemente@mnemo.com>; María Camila Vargas León <c.vargasleon@mnemo.com>; Juan Sebastian Cardenas Hernández <jcardenash@fna.gov.co>

Asunto: Re: #FNA# INFORMES DE LOS 8 ACTIVOS ETHICAL HACKING CAJA GRIS 2025

Buenos días ingenieros

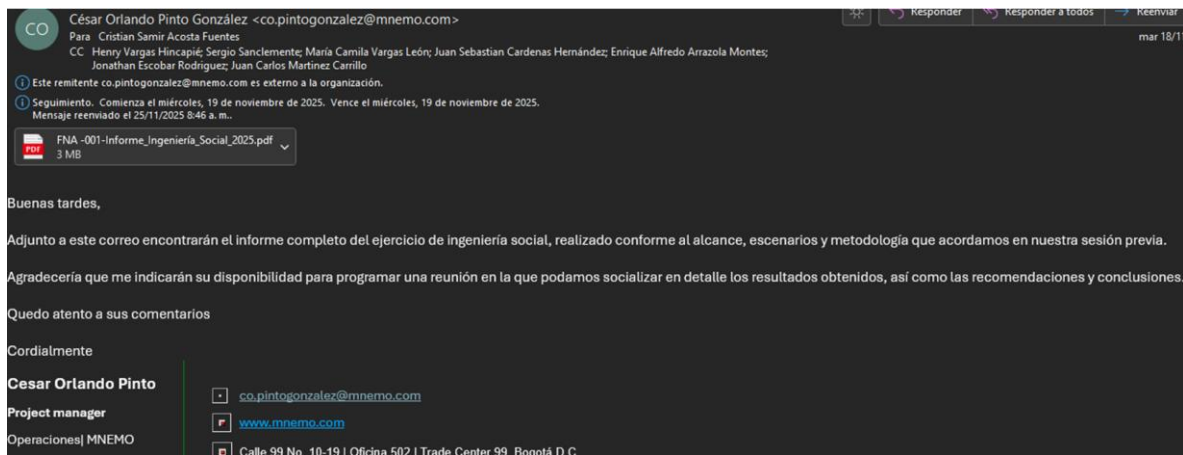
En presente correo adjunto el informe ejecutivo con el consolidado de los resultados de los ethical hacking caja gris realizado a los 8 activos relacionados por FNA.

Agradezco indicar un espacio para realizar la socialización respectiva.

Cordialmente

b) Ejercicio Ingeniería Social

- FNA -001-Informe_ ejecutivo_ Ingeniería_ Social_ 2025.PDF
- FNA -001-Informe_ Ingeniería_ Social_ 2025.PDF
- MNCO-SIG-25-0859_FNA#137_ Socialización_ IngSocial2025 rv DC.PDF



5.1 INFORMACIÓN DE AVANCE PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	\$ 36.499.583.610,00	47,78%
Adición Nro. 1	\$ 19.922.987.493,00	26,08%
Adición Nro. 2	\$ 19.973.637.010,00	38,80%
VALOR TOTAL DEL CONTRATO	\$ 76.396.208.113,00	73,86%
Valor ejecutado antes del presente pago	\$ 51.474.843.637,00	67,38%
Valor del pago aprobado con el presente informe	\$ 272.973.255,00	0,36%
VALOR TOTAL EJECUTADO	\$ 51.747.816.892,00	67,74%
Porcentaje de ejecución presupuestal programado a la fecha		67,77%
DIFERENCIA EN LA EJECUCION PRESUPUESTAL DEL CONTRATO		-0,03%

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 hito concerniente a Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda y Ejercicio de Ingeniería Social.

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

Porcentaje de ejecución proyectado	100%
Porcentaje de ejecución realizado	100%
DIFERENCIA EN LA EJECUCION DE ACTIVIDADES DEL CTO 173 de 2023	0%

6. NIVELES DE SERVICIO

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

7. VERIFICACIÓN DE ENTREGABLES

Por el desarrollo de las actividades ejecutadas en cuanto a Análisis de Vulnerabilidades por demanda – Ethical Hacking por demanda y Ejercicio de Ingeniería Social, 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 -001-Informe ejecutivo Ingeniería S	Bueno	Noviembre 2025	Ninguna

	ocial_2025.PDF			
	FNA -001- Informe_Ingeniería_So cial_2025.PDF	Bueno	Noviembre 2025	Ninguna
	MNCO-SIG-25- 0859_FNA#137_ Socialización_IngSocial 2025 rv DC.PDF	Bueno	Noviembre 2025	Ninguna
	FNA - EH Informe Ejecutivo EH.PDF	Bueno	Septiembre 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 **DOSCIENTOS SETENTA Y DOS MILLONES NOVECIENTOS SETENTA Y TRES MIL DOSCIENTOS CINCUENTA Y CINCO PESOS MCTE (\$ 272,973,255).**



**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 12 días del mes de diciembre de 2025.

JUAN SEBASTIAN CARDENAS
Gerente Estrategia TI y Aseguramiento
Informático
Supervisor CTO 173 de 2023

ENRIQUE A. ARRÁZOLA MONTES
Profesional 3
Apoyo supervisión CTO 173 de 2023

JONATHAN ESCOBAR RODRIGUEZ
Profesional Universitario 2
Apoyo a la Supervisión CTO 173 de 2023



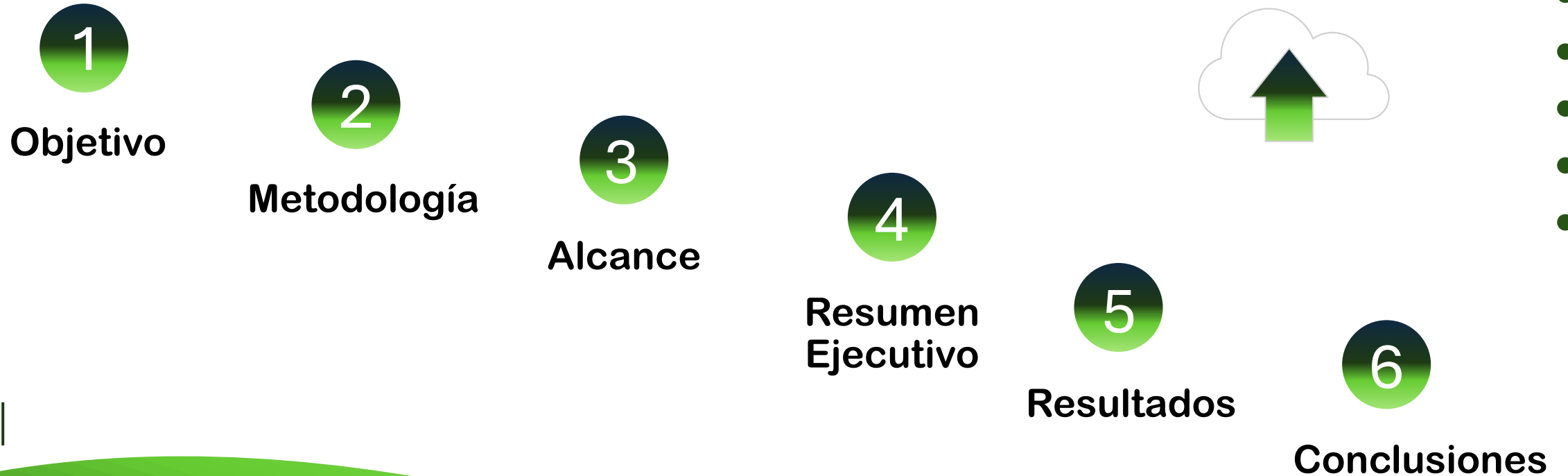
Presentación Ejecutiva

Ingenierías Sociales

Fondo Nacional del Ahorro

Noviembre 2025

Tabla de contenido



Objetivo

Evaluar, bajo autorización y en entorno controlado, la exposición de FNA frente a técnicas de ingeniería social con el fin de medir la susceptibilidad humana, validar la efectividad de los controles organizacionales (tecnológicos y procedimentales) y determinar el impacto potencial sobre la seguridad de la información.

Enfoque

- Analizar, simular y documentar intentos de manipulación a través de canales seleccionados (Acceso Físico, Quishing, Rogue AP, Vishing, Smishing, Phishing).
- Identificar y evidenciar brechas que puedan afectar **Confidencialidad, Integridad, Disponibilidad y No repudio** de la información.
- Medir métricas clave (tasa de clic/escaneo, divulgación de datos, cumplimiento de protocolos, reporte de incidentes) para estimar riesgo y efectividad de la respuesta.
- Proveer recomendaciones priorizadas para reducir el riesgo humano, fortalecer controles y orientar planes de concienciación y mejora continua.



Ingenierías sociales

Intrusión Física

Ingreso a instalaciones con pretextos, credenciales falsas o tailgating.

Quishing

QR que dirige a sitios falsos para robar datos o descargar malware.

Rogue AP

Wi-Fi falso que imita la red y captura tráfico/credenciales.

Ing. Físicas



Ing. Virtual

Vishing

Llamadas con pretextos para obtener información o forzar acciones.

Smishing

SMS con urgencia/enlaces falsos para robar credenciales u obtener datos.

Phishing

Envío de correo con portal falso para capturar credenciales u obtener datos.



INTRUSIÓN FÍSICA

RESULTADOS DEL EJERCICIO – Intrusión física

El auditor ingresa sin autorización aprovechando observación, interacción social y una falla en el control de accesos por medio de los siguientes puntos a destacar:

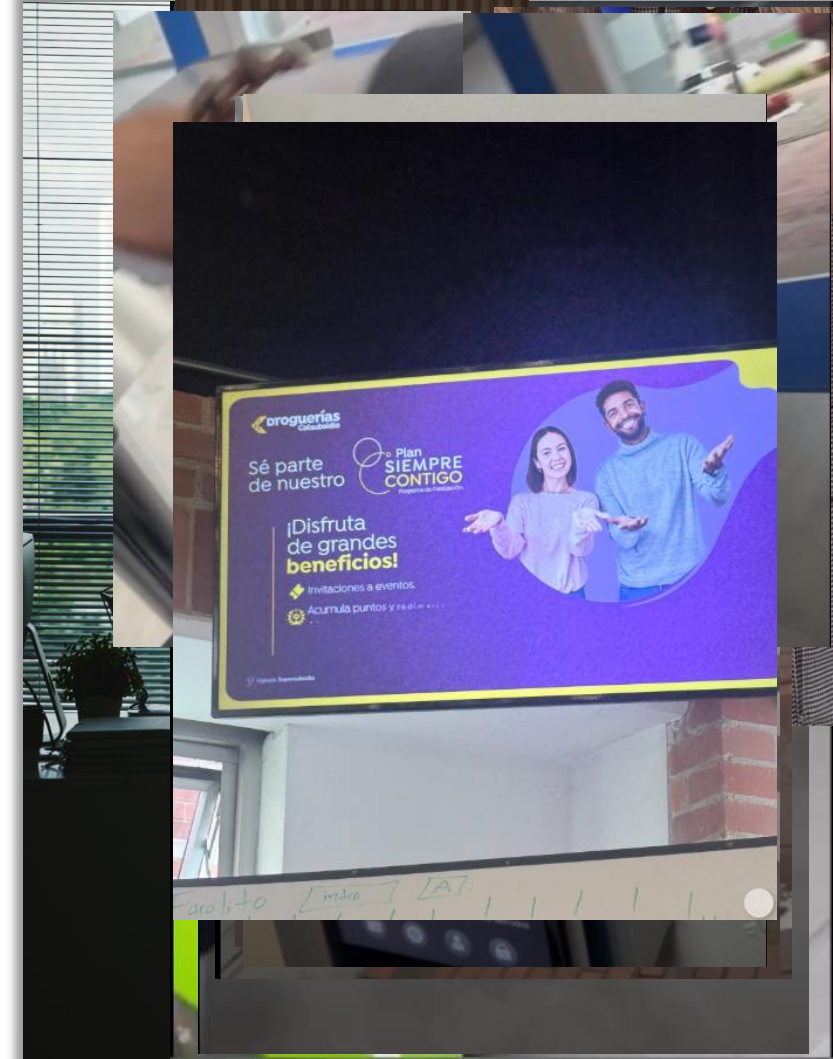
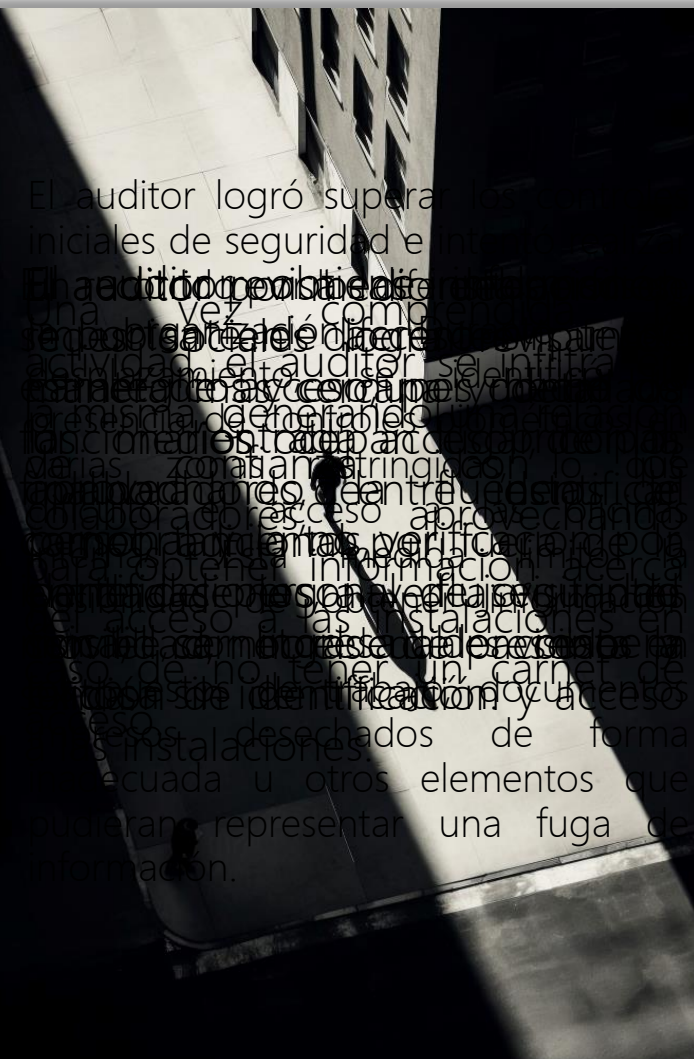
Observación del perímetro

Reconocimiento de carnets

Infiltración en evento

Acceso sin identificación

Movilidad interna



Tips

Verificación en Parqueadero

Actualmente el ingreso al parqueadero funciona con acceso biométrico, esto dificulta el acceso por esta entrada.



Eventos ≠ Vía Libre

En días de eventos, refuerza filtros: pre-registro y brazaletes únicos por sede.



Exige Carnet Siempre

No dejes pasar a nadie sin carnet visible y vigente (sin "se me quedó").



Acompañamiento Obligatorio

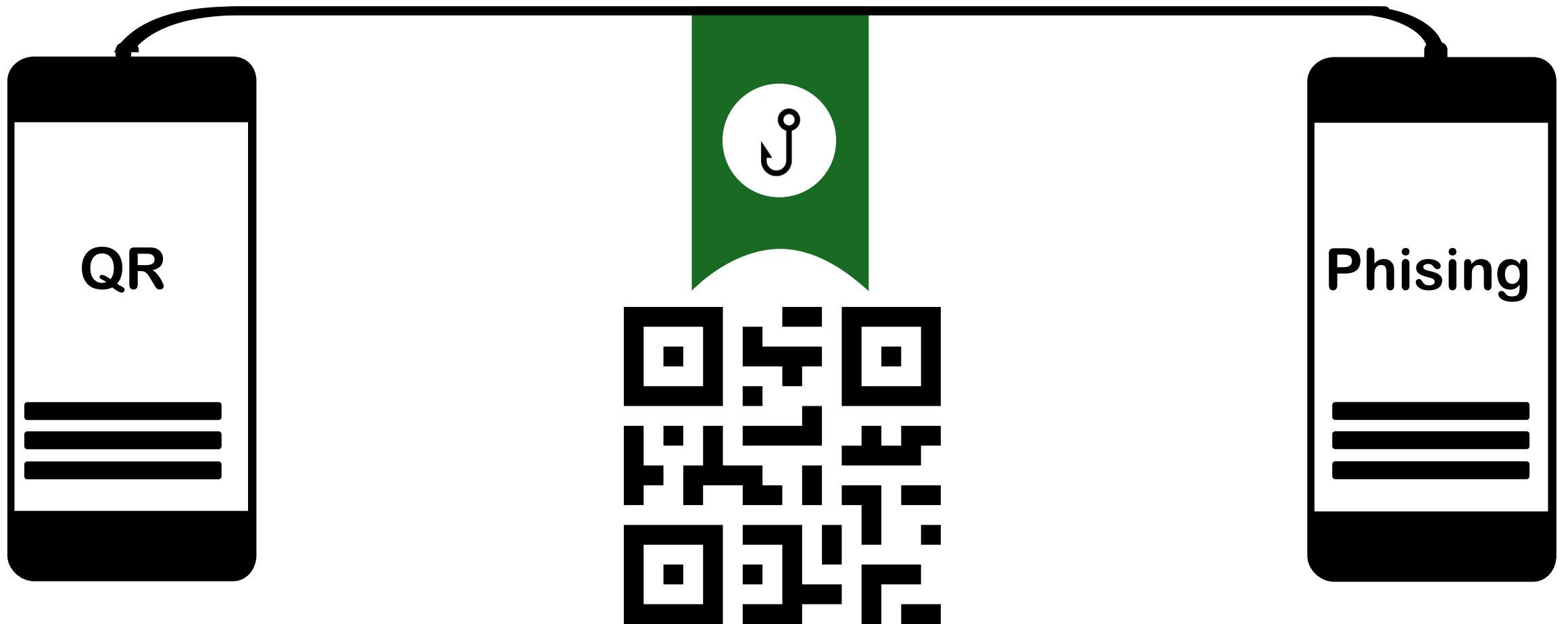
Visitantes y "proveedores" prestar especial atención; sin rondas libres por pisos.



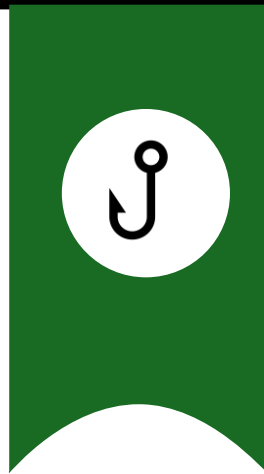
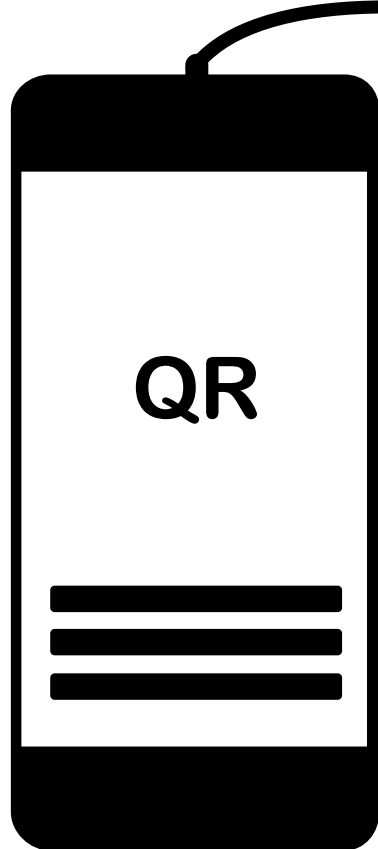
Reporte Inmediato

Si ves a alguien sin distintivo o en zona inusual, repórtalo antes de "ayudarlo".

Quishing

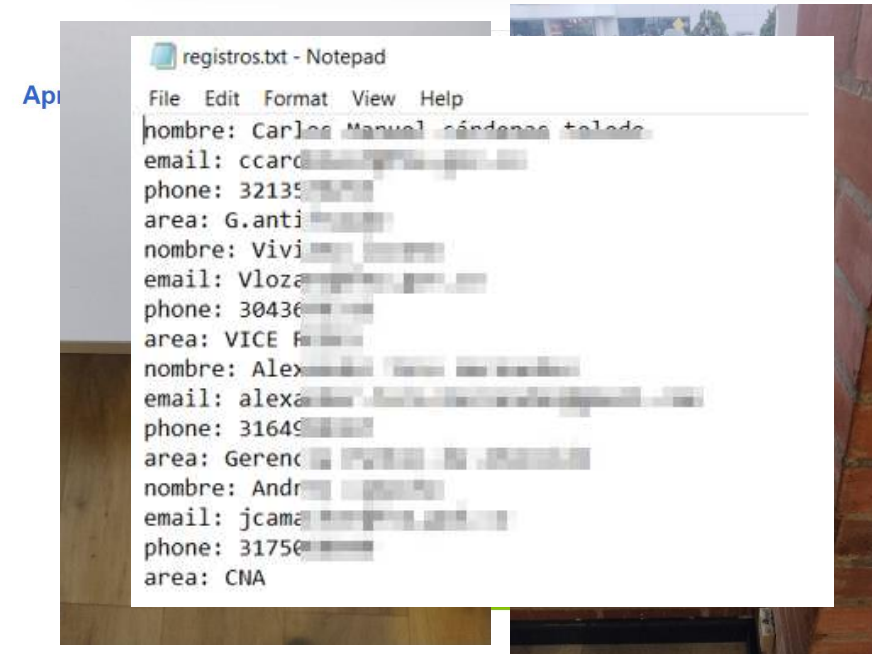


Desarrollo del Quishing



Idea

Se estructura la idea,
se compra el
dominio, ajuste de
página web, etc.



Tips

Desconfía de Avisos Nuevos

Carteles "corporativos" sin sello/folio oficial son sospechosos.

Valida el Dominio Antes

Escanéalo y revisa el URL: dominio exacto, HTTPS y subdominios legítimos



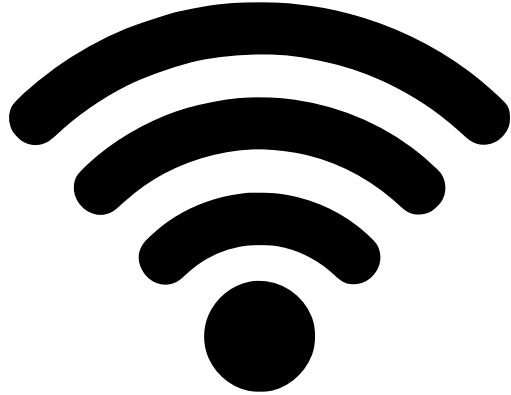
Retiro y Reporte

Si el QR no está autorizado, retíralo y notifica a seguridad.

No Escanees por Urgencia

Actualizaciones críticas no se piden por QR en áreas comunes.

Rogue AP | WiFi



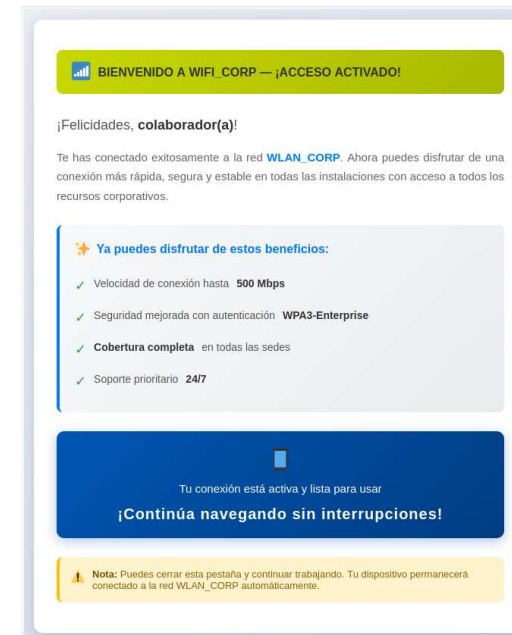
WLAN_CORP

La actividad de **Rogue AP** consistió en la **creación** de una **red WiFi** falsa que simulaba ser una nueva red legítima del Fondo Nacional del Ahorro. Para su ejecución, se elaboró un comunicado informando sobre la supuesta **apertura** de una nueva red inalámbrica denominada '**WLAN_CORP**', con el fin de inducir a los usuarios a conectarse a ella.

FLUJO ROGUE AP



El correo simulaba ser un **comunicado oficial** de la organización acerca de una nueva red WiFi Corporativa.

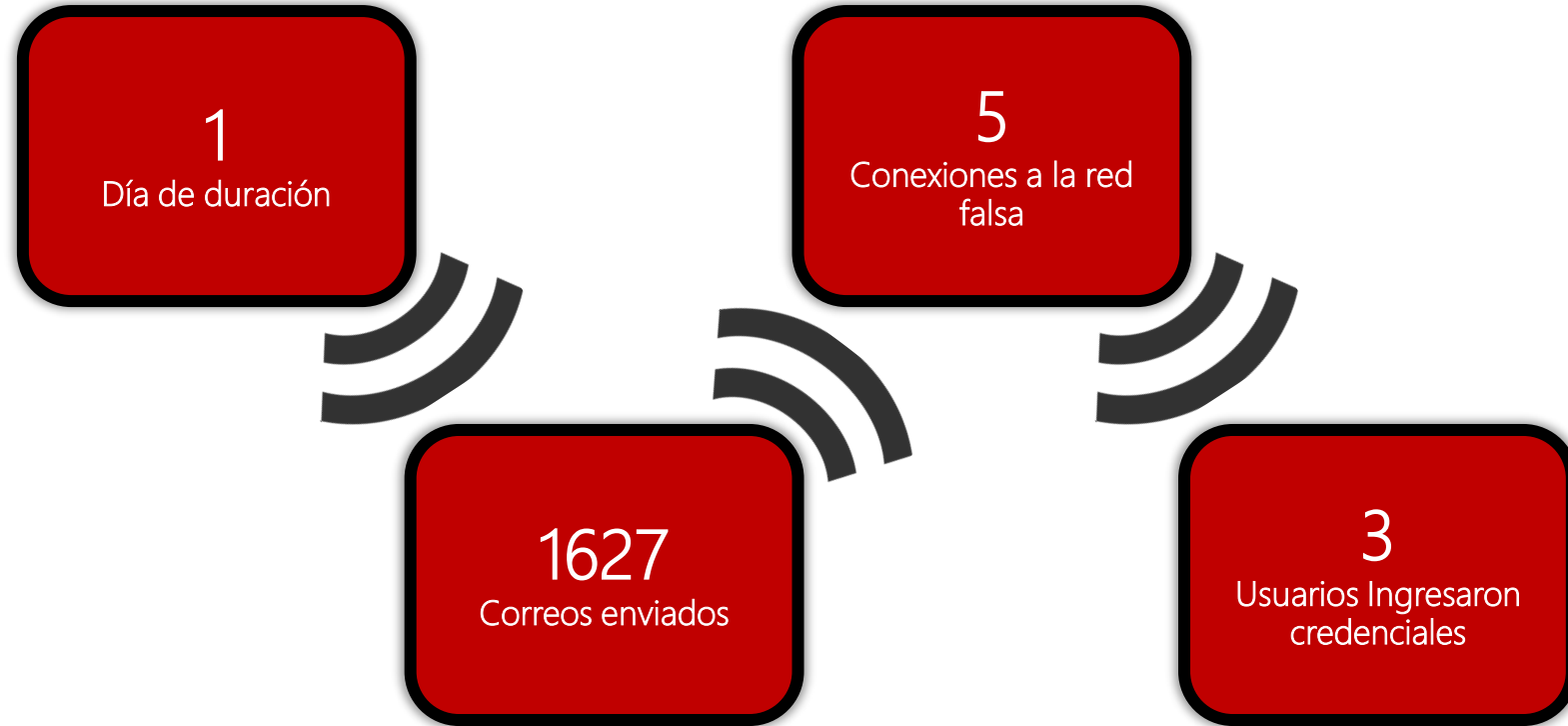


Al conectarse a la red WiFi, se despliega un **portal cautivo** solicitando **usuario** y **contraseña** de red, es de aclarar que se utilizo una plantilla muy similar al login del portal educativo **aprende**, esto para generar confianza entre los colaboradores.

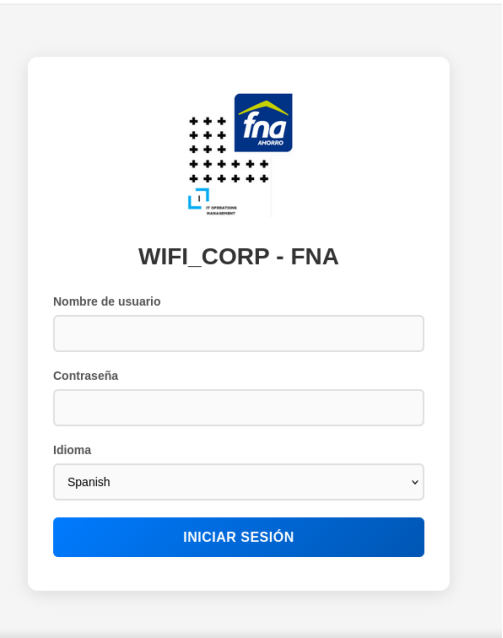
Rogue AP – Información General



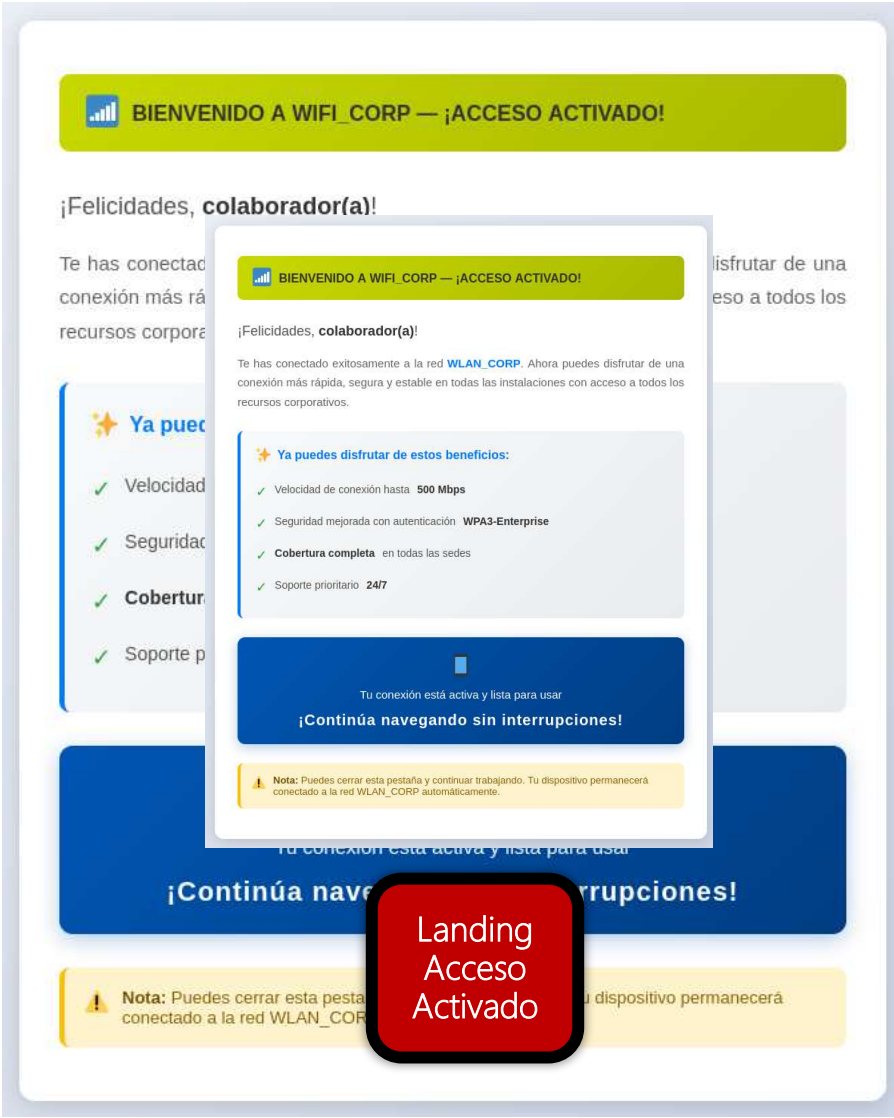
WLAN_CORP



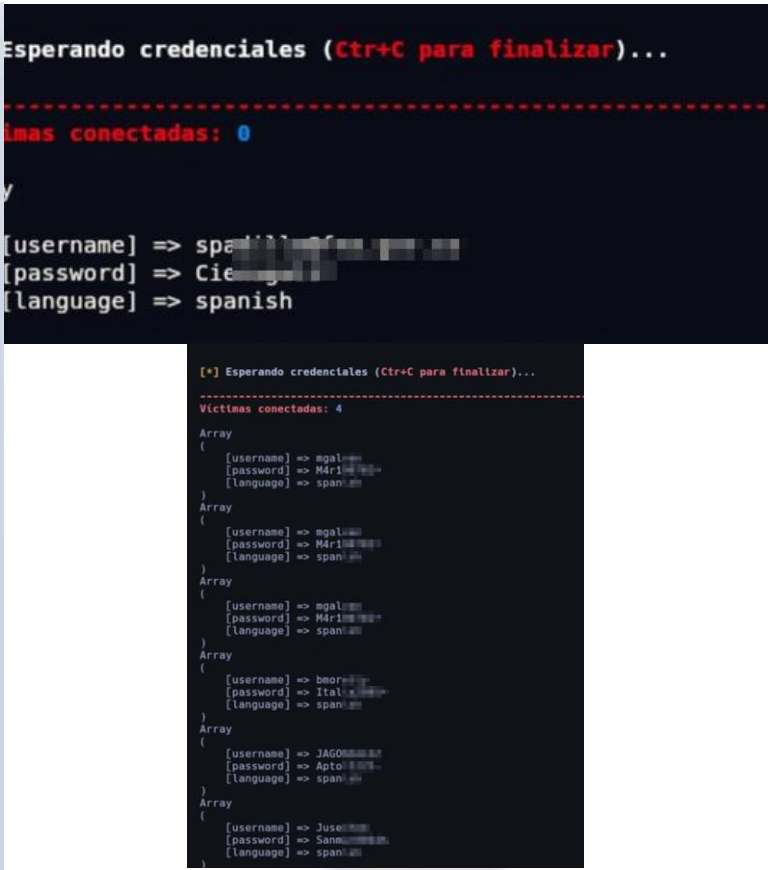
RESULTADOS DEL EJERCICIO - Evidencias



Landing
page
usado



Landing
Acceso
Activado



Captura
de data



Tips

1

Verifica el SSID

Conéctate sólo a nombres publicados en intranet; evita "corporativa-guest"

2

Cuidado con Portales

Si el portal pide credenciales de AD, revisa que el dominio/URL sea oficial.

3

Correos de "Nueva Red"

Mensajes desde dominios parecidos (fna-qov.co) son señal de fraude.

4

Doble Chequeo

Ante dudas, llama a TI; no introduces credenciales para "probar".

5

Reglas

Validar si los controles de Spam están activos.

Ingenierías sociales

Intrusión Física

Ingreso a instalaciones con pretextos, credenciales falsas o tailgating.

Quishing

QR que dirige a sitios falsos para robar datos o descargar malware.

Rogue AP

Wi-Fi falso que imita la red y captura tráfico/credenciales.

Ing. Físicas



Ing. Virtual

Vishing

Llamadas con pretextos para obtener información o forzar acciones.

Smishing

SMS con urgencia/enlaces falsos para robar credenciales u obtener datos.

Phishing

Envío de correo con portal falso para capturar credenciales u obtener datos.



Vishing

Desarrollo del Vishing



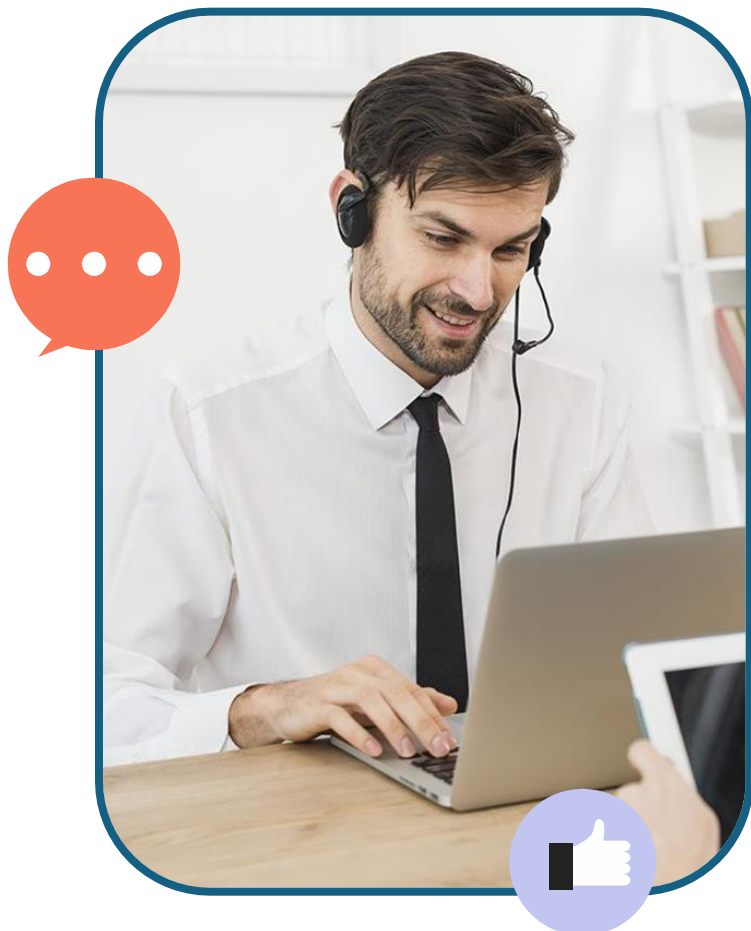
Llamada simulada

"¡Buenos días/tardes, [Nombre del Empleado FNA]! Mi nombre es [Hackercito] y le estoy contactando en nombre de Ktronix, aliado comercial del Fondo Nacional del Ahorro. Antes de continuar, le informo que esta llamada puede ser grabada y monitoreada con fines de control de calidad y verificación de la información. ¿Tiene un par de minutos para atenderme?"

✅ Gracias, le comento que, como parte de un programa de bienestar desarrollado en alianza entre Ktronix y el Fondo Nacional del Ahorro, usted ha sido seleccionado(a) para acceder a un bono especial de descuento aplicable en la renovación de electrodomésticos, productos de tecnología y artículos para el hogar. Este beneficio aplica únicamente para los afiliados a cajas de compensación como Cafam o Colsubsidio, y tiene como objetivo apoyar a las familias en la actualización de sus equipos esenciales para el hogar, brindando acceso a productos con garantía, respaldo y precios preferenciales. La iniciativa busca facilitar la renovación de sus dispositivos del hogar, promover el bienestar familiar y generar ahorros significativos para los afiliados. Para continuar, ¿quiere que le explique cómo reclamarlo por teléfono o prefiere recibir la información por su correo?

Opción Correo: Perfecto, podría indicarme su correo institucional y le enviaremos a su correo la información y así se informe de cómo obtener el beneficio. Muchas gracias por su tiempo. En los próximos minutos recibirá el correo oficial con las instrucciones detalladas de cómo obtener el beneficio junto con el proceso para redimirlo en Ktronix, ya sea de manera presencial en tienda o a través de la plataforma virtual. Agradecemos nuevamente su atención y le deseamos un excelente día.

❌ "Perfecto, comprendo que ahora no sea un buen momento. ¿Podría indicarme un horario en el que podamos volver a comunicarnos? Gracias por su atención me comunico más tarde, feliz día."



Resultados del ejercicio



Llamadas
realizadas

40

Nombre	Correo	Número Telé	ID	Nombre completo	Num. De identificación	Correo electrónico	Número de celular	Dependencia/area	Observaciones
LOPEZ CARDENAS JUAN PABLO	jplopezc@fna.gov.co	3,103E+09	1			tuapa_1984@gmail.com			Pidió seguir el proceso por correo porque está muy ocupado
MORA ARTURO VANESSA NATALI	vmoraa@fna.gov.co	3115584756	2						Número temporalmente suspendido
ORTIZ PUENTES CHRISTIAN DAVID	cdortizp@fna.gov.co	3,213E+09	3	Cristian David Ortiz	1121715767	ortizpuentesdavid19@gmail.co	3212787337	Comercial	No contesta
GOMEZ GUTIERREZ ESTEFANYULIET	egomezg@fna.gov.co	3,046E+09	4			estefg01@hotmail.com			Pidió seguir el proceso por correo porque está muy ocupado
BUSTOS LEON LEYDI PAOLA	lbustosl@fna.gov.co	3,506E+09	5						Es de recursos humanos
CERVANTES OTALVAREZ MARLY SOFIA	mcervantes@fna.gov.co	3,107E+09	6						Es de recursos humanos y dijo que eso no era oficial
AHUMADA GOMEZ ALVARO ANDRES	aahumada@fna.gov.co	3,116E+09	7						No contesta
RODRIGUEZ JIMENEZ LEIDY JOHENY	lrodriguezj@fna.gov.co	3,228E+09	8			lrodriguezj@fna.gov.co			Pidió seguir el proceso por correo porque está muy ocupado
DIAZ RODRIGUEZ CAMILA ALEJANDRA	cdiazr@fna.gov.co	3,216E+09	9						No contesta
PINEDA BETANCOURT ANGELA MARIA	apinedab@fna.gov.co	3,177E+09	10						No contesta

datos

5

Nombre	Correo	Número Teléfono	ID	Nombre completo	Num. De identificación	Correo electrónico	Número de celular	Dependencia/area en la que trabaja	Observaciones
DIAZ LOPEZ MARIA ANGELICA	MdiazL@fna.gov.co	4458950/3112474201	1			ange8050@gmail.com			No contesto
RUBIANO VARGAS ANGELA MARIA	ARubiano@fna.gov.co	3112964719	2						mas tarde
ARAZO HERNANDEZ JAVIER ENRIQUE	Jarazo@fna.gov.co	3017666626	3						No contesto
PRIETO NARANJO DAVID ARMANDO	dprieto@fna.gov.co	3193816312	4						Es de seguridad TI y me colgo
QUINTERO ERIKA PAOLA	Equintero@fna.gov.co	301579114	5						Falta un numero
SILVA CASTELLANOS JUAN ANDRES	jsilvac@fna.gov.co	3153934616	6						No contesto
RAMIREZ GALAN JUAN CARLOS	jcamirez@fna.gov.co	3106666219-9356851	7						No quiere bono
FRAILE SANCHEZ DUVAN ANDRES	dfraile@fna.gov.co	3187942101-9014909	8						No contesto
DELGADO RIVERA LUIS ALBERTO	ldelgador@fna.gov.co	3503346578	9						No contesto
NAJAS MAHECHA NIDYA	Nnajas@fna.gov.co	3105521492	10						No contesto

Octubre

Campaña



Tips

Premios y Bonos

= Señal

Ktronix/Colsubsidio-Cafam/caja no piden datos sensibles por teléfono.

Corta y Verifica

Finaliza la llamada y devuelve por números oficiales.

No Dictes Datos

Nunca entregues cédula, correo o códigos en llamada no iniciada por ti



Grabación y Folio

Solicita número de caso y canal oficial para continuar por escrito.

Comparte el Indicador

Si suena a "bono único", "última oportunidad", es presión típica de fraude.

Validar el número

Comprobar por diferentes medios si el número es legítimo.

Smishing



Desarrollo del Smishing

Beneficios Colsubsidio 2025 FNA

2

Bienestar FNA: Colsubsidio y FNA amplían tus beneficios. Ingresas para conocer los nuevos convenios y bonos exclusivos %Portafalso%.

40

2

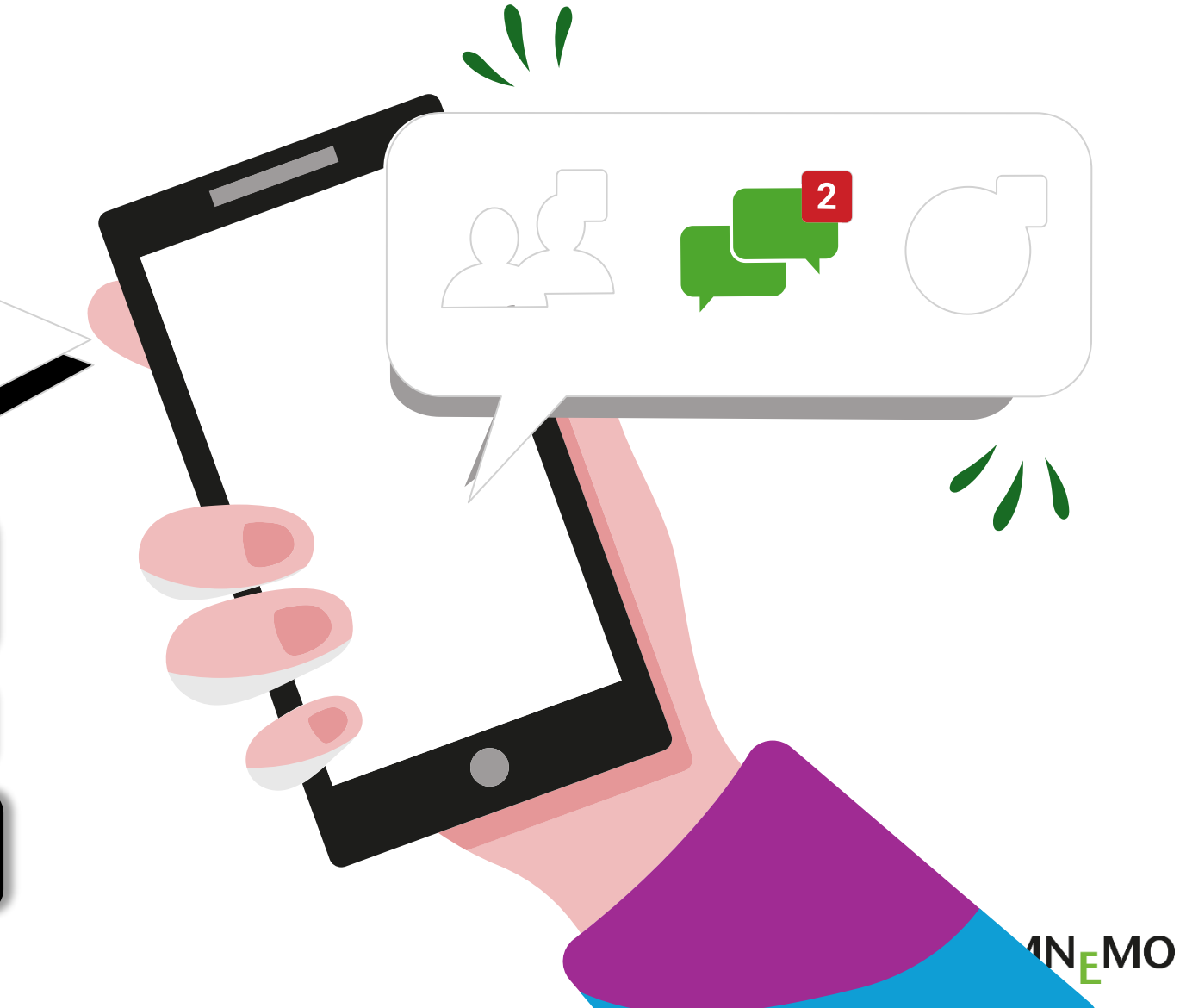
22 – 23
Oct.

SMS enviados

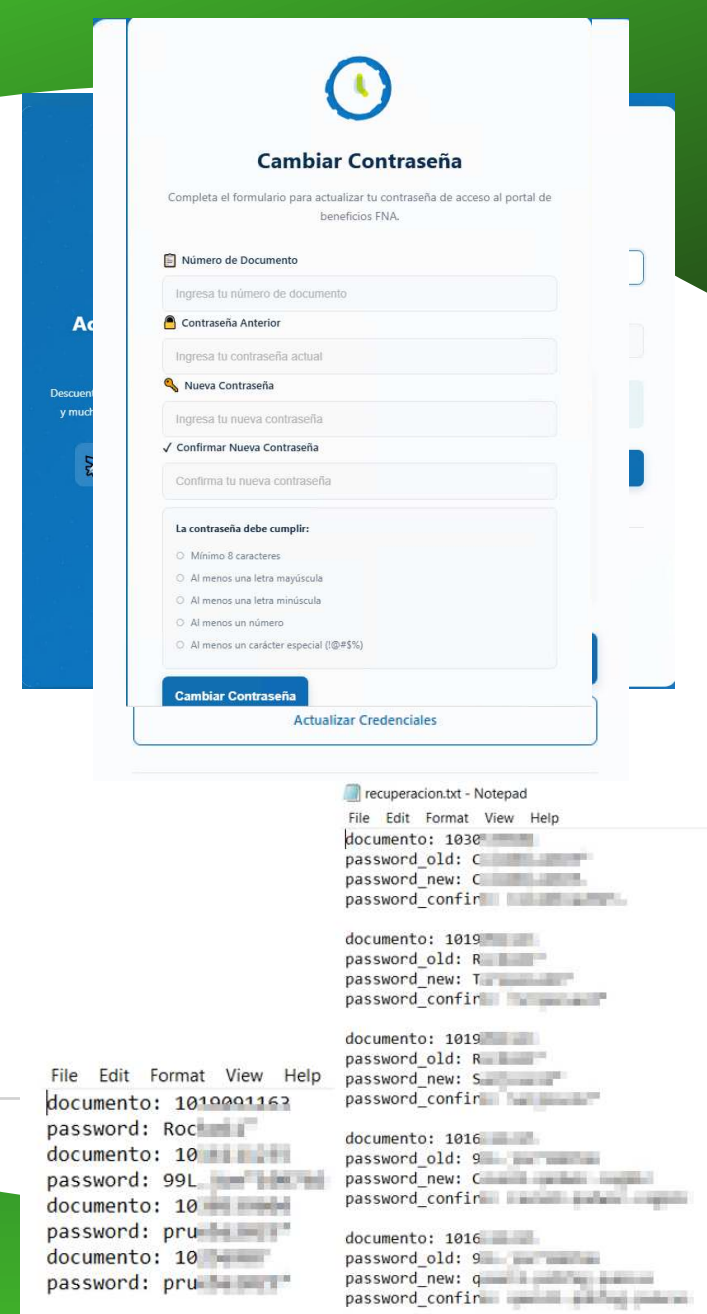
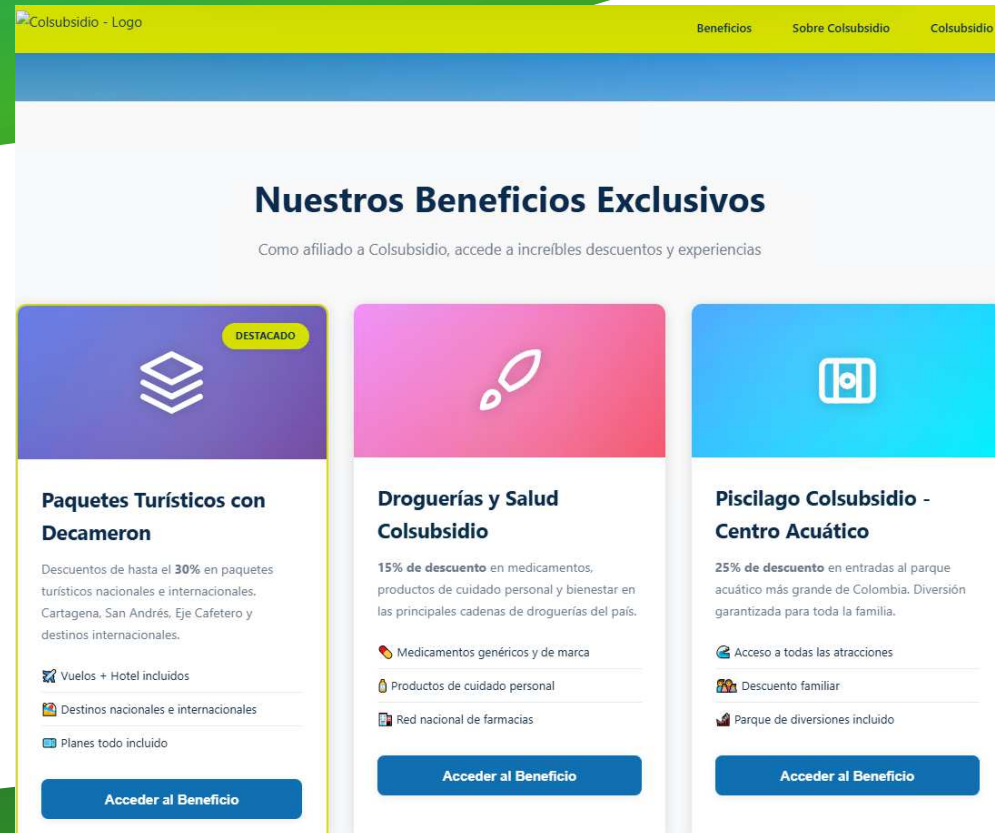
Víctimas

Duración campaña

En este tipo de actividades solo se puede contabilizar las personas que registraron datos, ya que la actividad se realiza con formularios de Personalizados.



Evidencias



Tips



Phishing 1 – Verify

Para los ejercicios de ingeniería social, que implicaba el envío de correos electrónicos, se utilizó el dominio **"fna-qov.co"** y el correo utilizado en esta primer ejercicio es **"verify@fna-qov.co"** que podrían crear confusión entre los trabajadores del Fondo Nacional del Ahorro.



verify@fna-qov.co



El contenido del correo electrónico fue diseñado para **simular** una campaña de aviso de expiración de contraseña en el portal de Verify.

SERVICIO DE NOTIFICACIÓN AUTOGESTIÓN DE USUARIOS VERIFY

EXPIRACIÓN DE CONTRASEÑA

Señor(a) usuario(a)

Se informa que su contraseña caducará en **1 día**, es necesario que realice el cambio de contraseña a través del módulo de [Autogestión de usuarios](#).

Para acceder al portal de autogestión de usuarios, de clic [AQUÍ](#).

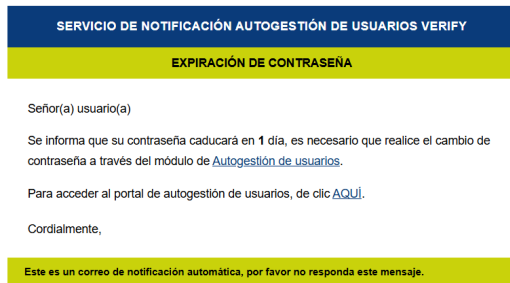
Cordialmente,

Este es un correo de notificación automática, por favor no responda este mensaje.

1
Buzón creado

FLUJO PHISHING

El portal de inicio de sesión simulaba la página de **Verify**



El correo simulaba ser un comunicado oficial de la organización.



ingresar el usuario de red la contraseña, continuaba en un nuevo portal, este direccionaba al portal principal del FNA.

RESULTADOS DEL EJERCICIO – Información General

El riesgo de un ataque de phishing comienza cuando un funcionario de la organización abre un correo electrónico desconocido, accede al enlace adjunto e ingresa al portal compartiendo sus credenciales.



#	Usuario	Intentos	Nivel de Riesgo
1	ggomezr@fna.gov.co	3	Alto
2	mfperezr@fna.gov.co	3	Alto
3	jargote	3	Alto
4	appena	3	Alto
5	jecastro@fna.gov.co	2	Medio
6	1012380313	2	Medio
7	jprieto@fna.gov.co	2	Medio
8	39424919	2	Medio
9	kpenuela@fna.gov.co	2	Medio
10	sgordillo@fna.gov.co	2	Medio
11	ykramirez	1	Bajo
12	apperez@fna.gov.co	1	Bajo
13	srninon@fna.gov.co	1	Bajo
14	caolarte	1	Bajo
15	overgara@fna.gov.co	1	Bajo
16	jmhernandezc@fna.gov.co	1	Bajo

27 -29

Oct

Duración de la
campaña

32%

Abrieron el correo

20,8%

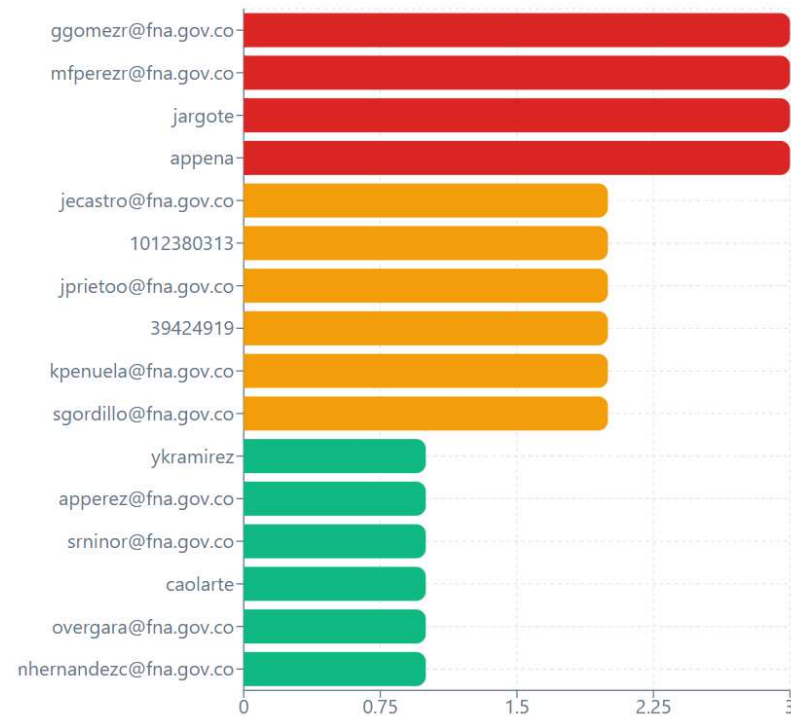
Dieron clic en el
correo

7,11%

Enviaron datos

RESULTADOS DEL EJERCICIO – Información General

Cantidad de eventos totales



RESULTADOS DEL EJERCICIO - Evidencias

registros.txt - Notepad

File Edit Format View Help

username: ykra...
password: Med...
username: jeca...
password: Cami...
username: jeca...
password: Cami...
username: appe...
password: Tasl...
username: 1012...
password: Luna...
username: 1012...
password: Luna...
username: jpri...
password: Jyor...
username: srni...
password: Gre...
username: jpri...
password: Jyor...
username: caol...
password: L1s4...
username: 3942...
password: Nicc...
username: 3942...
password: Nicc...
username: ggon...
password: Sari...
username: ggon...
password: Sari...
username: ggon...



registros.txt - Notepad

File Edit Format View Help

username: ykra
password: Medel
username: jeca
password: Cami
username: jeca
password: Cami
username: appe
password: Tasl
username: 1012
password: Luna
username: 1012
password: Luna
username: jpra
password: Jyor
username: srna
password: Gred
username: jpra
password: Jyor
username: caol
password: L1s4
username: 3942
password: Nico
username: 3942
password: Nico
username: ggon
password: Sari
username: ggon
password: Sari
username: ggon

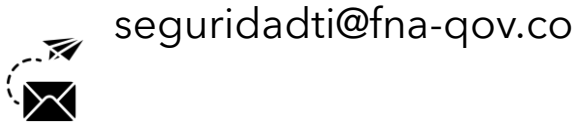
10
Usuarios
Reincidentes

10
Usuarios
Reincidentes

2	username: jecastr password: Camila2
4	username: jecastr password: Camila2 username: 101238 password: Luna*0 username: 101238 password: Luna*0
6	username: jprietoc password: Jyorky19 username: jprietoc password: Jyorky19
8	username: 394249 password: Nicolas username: 394249 password: Nicolas
9	username: ggomez password: Sarita5 username: ggomez password: Sarita5 username: ggomez password: Sarita5
10	username: kpenue password: Samytili username: kpenue password: Samytili
13	username: mfpere password: Praga1v username: mfpere password: Praga1v username: mfpere password: Praga1v
14	username: sgordill password: Camilo2 username: sgordill password: Camilo2
15	username: JARGO password: C0mput username: jargote password: C0mput username: jargote password: C0mput
16	username: appena password: juLIA19 username: appena

Phishing 2 – Vencimiento de Credenciales

Para el segundo ejercicio de Phishing se utilizo el subdominio “**seguridadti@fna-qov.co**” se realiza de está manera, por si algún colaborador reporta el correo o el propio Microsoft lo detecta como phishing.



El contenido del correo electrónico fue diseñado para **simular** un recordatorio de vencimiento de credenciales, y se esperar el accionar de los colaboradores que recibieron esta campaña.

PORTAL DE EDUCACIÓN VIRTUAL — FONDO NACIONAL DEL AHORRO

RECORDATORIO DE VENCIMIENTO DE CREDENCIALES

Te informamos que tu contraseña del **Portal de Educación Virtual del FNA** caducará en **1 día** día(s). Para mantener el acceso a tus cursos y certificaciones, te invitamos a actualizarla cuanto antes.

[Ir al Portal de Educación Virtual](#)

¿Olvidaste tu contraseña?

Restablécela desde [este enlace seguro](#).

Si no realizas el cambio a tiempo, por seguridad tu acceso podría quedar temporalmente bloqueado hasta completar el restablecimiento.

Cordialmente,

Equipo de Educación Virtual — FNA

Este es un correo automático, por favor no respondas a este mensaje. ¿Necesitas ayuda? Contáctanos: Mesa de ayuda.

1

Buzones creados

FLUJO PHISHING

PORTAL DE EDUCACIÓN VIRTUAL — FONDO NACIONAL DEL AHORRO

RECORDATORIO DE VENCIMIENTO DE CREDENCIAL

Te informamos que tu contraseña del **Portal de Educación Virtual** vencerá en **1 día** día(s). Para mantener el acceso a tus cursos y certificaciones, actualízala cuanto antes.

Ir al Portal de Educación Virtual

¿Olvidaste tu contraseña?

Restablécela desde [este enlace seguro](#).

Si no realizas el cambio a tiempo, por seguridad tu acceso podría bloquearse hasta completar el restablecimiento.

Cordialmente,
Equipo de Educación Virtual — FNA

Este es un correo automático, por favor no respondas a este mensaje. ¿Contactarnos: Mesa de ayuda.



Estamos en Mantenimiento

Plataforma de Educación Virtual FNA

Actualmente estamos realizando mejoras en nuestra plataforma para brindarte un mejor servicio. Nuestro equipo técnico está trabajando para que puedas acceder lo antes posible.

Disculpa las molestias ocasionadas.

Tiempo estimado
Próximamente

Soporte técnico
seguridadti@fna-qov.co

Volver al sitio principal

Fondo Nacional del Ahorro © 2025
Para mayor información visita www.fna.gov.co

Fondo Nacional del Ahorro

aprende.bti - Notepad

File Edit Format View Help

email: hivel
password: 10
email: ccast
password: C
email: maldi
password: m
email: lgalv
password:
email: Hcall
password:
email: Vorti
password: 16
email:
password:
email: ralf
password: B
email: sgar
password:
email: eguic
password: 16
email: bqui
password: 16
email: ylop
password: Ju
email: drolo
password: 16
email: ylop
password: Ju
email: llope
password: 8
email: hngar
password: 16
email: ARDB

El correo simulaba una **notificación oficial** de la organización por un correo electrónico no autorizado a la cuenta.

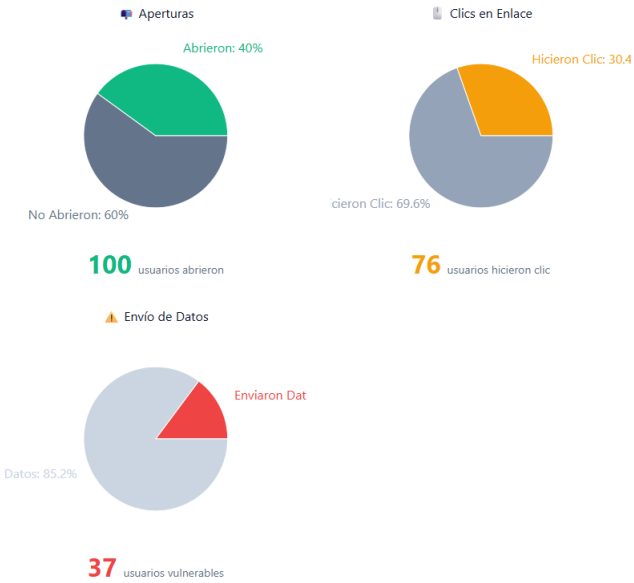
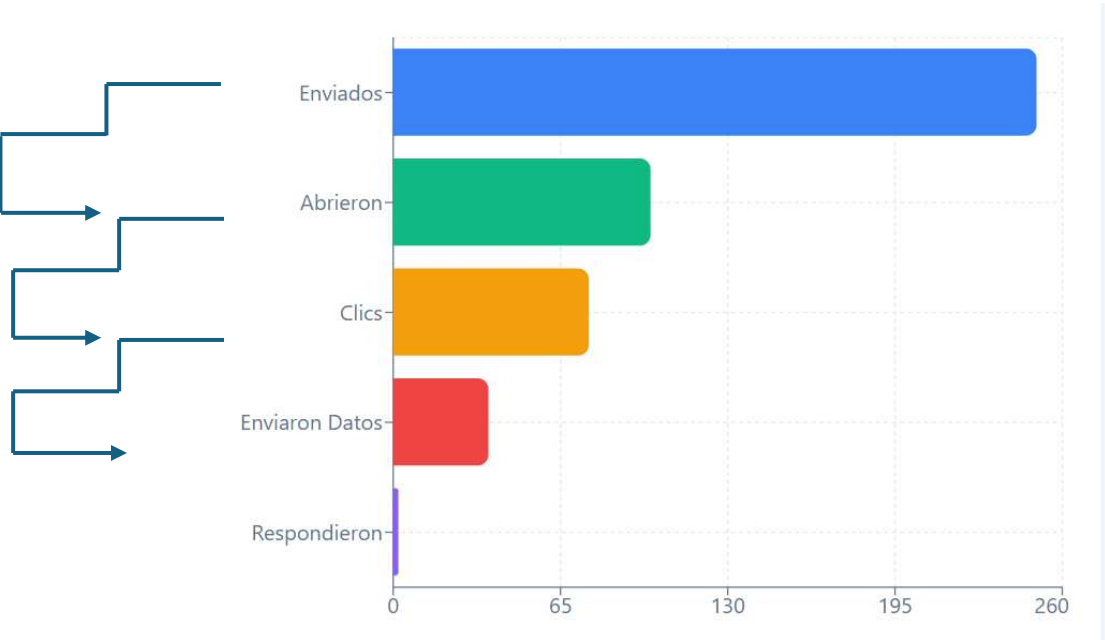
El correo simulaba una credencial actual o la contraseña conocida, y escribir dos caracteres de la nueva contraseña, el portal de Educación Virtual. De esta forma, se logra acceder al portal tanto las contraseñas actuales como las futuras, así como el correo de password utilizado por el colaborador.

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.

MNEMO

RESULTADOS DEL EJERCICIO – Información General

El riesgo de un ataque de phishing comienza cuando un funcionario de la organización abre un correo electrónico desconocido, accede al enlace adjunto e ingresa al portal compartiendo sus credenciales.



27 - 29
Oct
Duración de la
campaña

40%
Abrieron el correo

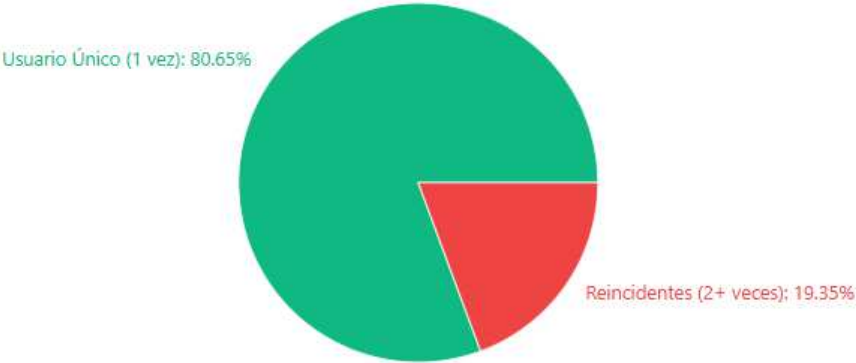
30,4%
Dieron clic en el
correo

14,8%
Enviaron datos

0,8%
Respondieron
Mensaje

RESULTADOS DEL EJERCICIO – Información General

Distribución: Únicos vs Reincidentes



80.65%

Usuarios Sin Reincidencia

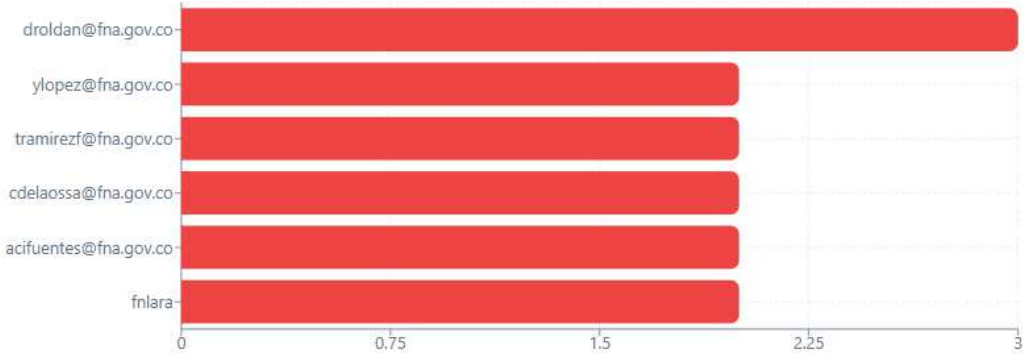
25 usuarios ingresaron datos una sola vez

19.35%

Usuarios Reincidentes

6 usuarios intentaron 2 o más veces

Análisis de Usuarios Reincidentes



#	Usuario	Intentos	Posiciones en Lista	Nivel de Riesgo
1	drolan@fna.gov.co	3	#11, #17, #32	CRÍTICO
2	ylopez@fna.gov.co	2	#9, #10	ALTO
3	tramirez@fna.gov.co	2	#16, #34	ALTO
4	cdelaossa@fna.gov.co	2	#23, #30	ALTO
5	acifuentes@fna.gov.co	2	#19, #31	ALTO
6	fnlara	2	#24, #25	ALTO

RESULTADOS DEL EJERCICIO - Evidencias

Y

Yesica Juli

Para: @ seguridad

CC: Monit

Buen dia

Pagina fr

De: seguric
Enviado el:
Asunto: Re

Algunos

L Lilia Maria Hernandez Cardenas<Lhernandezc@fna.gov.co>
Para: @ seguridad

Buenas tardes

No deja modificar la contraseña

Agradezco su atención

Cordial saludo,

Responder Responder a todos Reenviar
Lun 27/10/2025 14:13

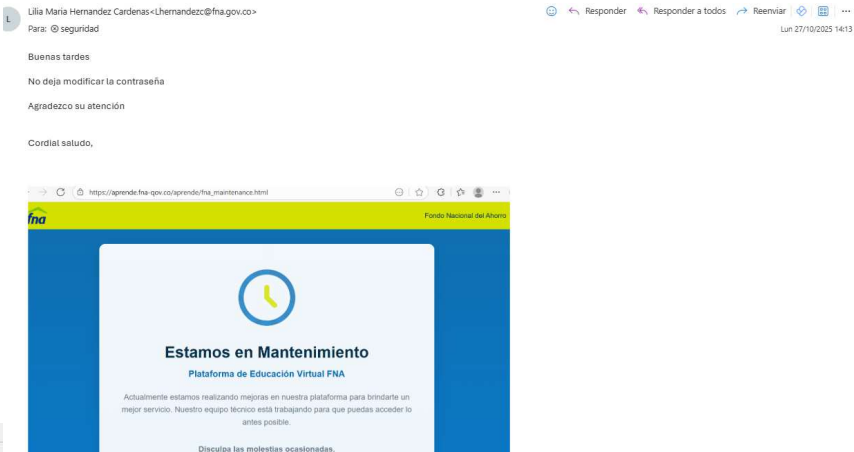
in 27/10/2025 9:37

@fna.gov.co>



fnlara
Posiciones: #24, #25

2 intentos



Tips



Recomendaciones

Capacitación continua con simulaciones reales

Programa permanente con sesiones breves y periódicas + simulaciones sorpresa en todos los canales (físico, QR, Wi-Fi, llamadas, SMS y correo).

Verificación múltiple

Cualquier solicitud sensible (credenciales, datos, pagos, cambios) debe confirmarse por un canal alternativo oficial (Teams/intranet/teléfono corporativo) antes de actuar.



Canales “oficiales” visibles y bloqueos preventivos

Publicar y mantener un catálogo de dominios, correos, números y SSID legítimos; registrar lookalikes, aplicar SPF/DMARC/DKIM estrictos y bloquear dominios/QR/SSID similares.

MFA Obligatorio

MFA obligatorio, además utilizar gestores de contraseñas, bloqueo de enlaces en correo sospechosos, filtrado DNS/URL y para Wi-Fi; principio de mínimo privilegio para limitar el impacto.

MN_EMO

Ingeniería Social
Intrusión física | Qhishing | Rogue AP |
Vishing | Smishing | Phishing
Fondo Nacional del Ahorro

Versión 1.0

ÍNDICE

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

5 Resumen..... 7

 5.1 Matriz de riesgos 8

 5.2 Metodología: cómo calculamos la probabilidad (%) 8

6 Intrusión física..... 9

 6.1 Objetivo 9

 6.2 Impacto..... 9

 6.3 Propuesta..... 9

 6.4 Desarrollo del escenario 9

 6.5 Resultados obtenidos 10

 6.6 Evidencias 11

 6.7 Recomendaciones..... 13

7 Qhishing 14

 7.1 Objetivo 14

 7.2 Impacto..... 14

 7.3 Propuesta..... 14

 7.4 Desarrollo del escenario 15

 7.5 Resultados obtenidos 15

 7.6 Evidencias 16

 7.7 Recomendaciones..... 19

8 Rogue AP 20

 8.1 Objetivo 20

 8.2 Impacto..... 20

 8.3 Propuesta..... 20

 8.4 Desarrollo del escenario 21

 8.5 Resultados obtenidos 21

 8.6 Evidencias 22

 8.7 Recomendaciones..... 24

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha:24 Sept 2025

1 / 47

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

9	Vishing.....	24
9.1	Objetivo	24
9.2	Impacto.....	24
9.3	Propuesta.....	24
9.4	Desarrollo del escenario	25
9.5	Resultados obtenidos	25
9.6	Evidencias	26
9.7	Recomendaciones.....	26
10	Smishing.....	27
10.1	Objetivo	27
10.2	Impacto.....	27
10.3	Propuesta.....	28
10.4	Desarrollo del escenario	28
10.5	Resultados obtenidos	29
10.6	Evidencias	29
10.7	Recomendaciones.....	31
11	Phishing.....	33
11.1	Objetivo	33
11.2	Impacto.....	33
11.3	Phishing 1 - Propuesta	33
11.4	Phishing 1 - Desarrollo del escenario	33
11.5	Phishing 1 - Resultados obtenidos.....	34
11.6	Evidencias	35
11.7	Phishing 2 - Propuesta	37
11.8	Phishing 2 - Desarrollo del escenario	38
11.9	Phishing 2 - Resultados obtenidos.....	38
11.10	Evidencias.....	39
11.11	Recomendaciones	41
12	Conclusiones	43
13	Anexo I: Conceptos y Definiciones.....	45
13.1	Usuarios comprometidos con credencial en texto plano.....	47

1 Hoja de información general

Proyecto	Ingeniería Social
Entidad	Fondo Nacional del Ahorro
Título	Informe de Ingeniería Social
Versión	1.0
Fecha de validación	30/10/2025
Fichero	FNA-002-Informe_Ingeniería_Social_v1.0
Resumen	El presente documento plasma los resultados obtenidos después de llevar a cabo el ejercicio de Ingeniería Social sobre la compañía Fondo Nacional del Ahorro.

Control de ediciones

Versión	Fecha de validación	Responsable	Cambios
1.0	30/10/2025	Equipo auditoría	Primera versión del entregable

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

3 / 47

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

2 Introducción y objetivos

El Fondo Nacional del Ahorro, es una entidad financiera del Estado colombiano, creada para administrar las cesantías y fomentar el ahorro de los trabajadores del país. Su objetivo principal es facilitar que los colombianos, especialmente aquellos que destinan sus cesantías o ahorros en esta institución, puedan acceder a créditos de vivienda y educación en condiciones favorables.

El presente documento detalla los resultados de los ejercicios realizados, proporcionando a el Fondo Nacional del Ahorro una visión del actuar de los colaboradores frente a diferentes escenarios de ingeniería social. Asimismo, se incluyen recomendaciones específicas para evitar ser víctima de este tipo de ataques que ponen a prueba el comportamiento humano y mejorar la reacción de sus colaboradores ante estos.

Objetivos Específicos del Análisis de Seguridad

1. Evaluar, bajo autorización y en entorno controlado, la exposición del Fondo Nacional de Ahorro frente a técnicas de ingeniería social con el fin de medir la susceptibilidad humana, validar la efectividad de los controles organizacionales (tecnológicos y procedimentales) y determinar el impacto potencial sobre la seguridad de la información.
2. Analizar, simular y documentar intentos de manipulación a través de canales seleccionados (Acceso Físico, Quishing, Rogue AP, Vishing, Smishing, Phishing).
3. Identificar y evidenciar brechas que puedan afectar Confidencialidad, Integridad, Disponibilidad y No repudio de la información.
4. Medir métricas clave (tasa de clic/escaneo, divulgación de datos, cumplimiento de protocolos, reporte de incidentes) para estimar riesgo y efectividad de la respuesta.
5. Proveer recomendaciones priorizadas para reducir el riesgo humano, fortalecer controles y orientar planes de concienciación y mejora continua.

3 Estructura del documento

A continuación, se presenta la estructura de este documento, resumiendo los aspectos clave de cada apartado tal y como fueron desarrollados:

- ✓ **Hoja de información general**
Identifica proyecto, entidad, versión, fecha de validación y propósito del informe, junto con el **control de ediciones** para trazabilidad de cambios.
- ✓ **Introducción y objetivos**
Contextualiza y define los objetivos específicos de la evaluación: medir susceptibilidad humana, validar controles organizacionales y priorizar mejoras basadas en evidencia.
- ✓ **Alcance del trabajo realizado**
Delimita el **alcance** (4 ejercicios de ingeniería social y un escenario de acceso físico), detalla **tipo de pruebas** (sociales físicas/virtuales) y **tipo de análisis** (caja negra/gris, origen externo/interno, pruebas híbridas). Establece supuestos y limitaciones.
- ✓ **Resumen**
Presenta los resultados consolidados en tabla (fechas, población evaluada y usuarios comprometidos por ejercicio) y prepara la lectura de los capítulos operativos.
- ✓ **Matriz de riesgos y metodología de cálculo**
Incluye la **matriz Probabilidad × Impacto** con la ubicación de cada vector (Intrusión física, Quishing, Rogue AP, Vishing, Smishing, Phishing 1 y 2) y la **fórmula** utilizada para calcular probabilidad (**usuarios comprometidos / usuarios evaluados × 100**), junto con notas de interpretación (p. ej., tracking parcial en Phishing 2, 0% en Quishing).
- ✓ **Capítulos por ejercicio (detalle operativo)**
Cada vector mantiene una estructura homogénea para facilitar comparación y trazabilidad:
 - **Objetivo e Impacto.**
 - **Propuesta** (elegida y decisiones de diseño).
 - **Desarrollo del escenario** en fases: *Preparación y permisos → Implementación técnica → Producción y despliegue → Operación, monitoreo y cierre.*
 - **Resultados obtenidos** (con tabla de síntesis y/o evidencias).
 - **Recomendaciones** específicas por vector.
El capítulo **Phishing** separa **Phishing 1** y **Phishing 2** con sus propias plantillas, métricas y evidencias, e incorpora conclusiones específicas.
- ✓ **Detalle de vulnerabilidades**
Recopila hallazgos que requieren cierre o seguimiento, alineados con los vectores evaluados y su impacto potencial.
- ✓ **Anexos y glosario**
Incluye **conceptos y definiciones** (términos de ingeniería social y seguridad) y anexos de soporte (p. ej., análisis de servicios/red, tablas de usuarios comprometidos), para estandarizar lenguaje y reforzar la verificabilidad del informe.

4 Alcance del trabajo realizado

4.1 Alcance del trabajo

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

Ejercicios	Para cumplir con el objetivo antes mencionado, se consideran todos los siguientes escenarios de ingeniería social sobre la compañía: 1. Intrusión física 2. Qhishing 3. Rogue AP 4. Vishing 5. Smishing 6. Phishing (x2)
Tipo de pruebas	Se realizaron pruebas de ingeniería social enfocadas en componentes sociales físicos y virtuales, así como dos ejercicios de phishing. Estas pruebas simulaban ataques de ingeniería social reales mediante tácticas y técnicas empleadas por adversarios sofisticados, con el propósito de obtener información interna de la compañía y sus colaboradores.
Tipo de análisis	El análisis de las ingenierías sociales se clasificó así: por conocimiento previo, se trabajó en coordinación para logística con el cliente. Por nivel de intrusión, se recorrió el ciclo enumeración → prueba de intrusión → explotación → post-explotación. Por origen de las pruebas, hubo externas (correo, SMS, llamadas) e internas (despliegues en sitio y acceso físico), con casos mixtos cuando aplicó (Rogue AP). Por tipo de pruebas, fueron híbridas, combinando automáticas y manuales (guiones, pretextos, presencia en sedes).

5 Resumen

El ejercicio de ingeniería social realizado para el Fondo Nacional del Ahorro se llevó a cabo en varias fases, que incluyeron:

- Propuesta de ejercicios de ingeniería social
- Plan de trabajo para los ejercicios seleccionados
- Ajustes de plan de trabajo en conjunto
- Despliegue
- Recolección y análisis de información
- Redacción de informes

La siguiente tabla muestra los datos más relevantes de cada uno de los ejercicios realizados:

Ejercicio	Fecha despliegue	Usuarios para evaluar	Usuarios comprometidos
Intrusión física	17/10/2025	Sede Principal	Sede Principal
Qhishing	17/10/2025 - 20/10/2025	Usuarios de la sede principal	4 (4 escaneos, 4 datos reales)
Rogue AP	06/11/2025	448 (correo; sede Salitre, varios pisos)	1 (credencial)
Vishing	25/08/2025 - 29/08/2025	40 llamadas	4 personas suministraron correo / 1 persona suministro datos completos
Smishing	22/10/2025 - 23/10/2025	80 SMS	2
Phishing 1	27/10/2025 - 29/10/2025	250 correos	16
Phishing 2	27/10/2025 - 29/10/2025	250 correos	37
Total	-	1.801 (sin contar Intrusión física ni Quishing)	61

Tabla 1. Cantidad de vulnerabilidades

5.1 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 ingenierías sociales ejecutadas.

I M P A C T O	BAJO	Quishing (0.00%)		
		Acceso Físico (0.00%)		
	MEDIO	Smishing (2.5%)	Vishing (12.5%)	
	ALTO	Rogue AP (0.22%)	Phishing 1 - Verify (6,4%)	Phishing 2 – Portal Aprende (14.8%)
		BAJA	MEDIA	ALTA

PROBABILIDAD DE OCURRENCIA

Tabla 2. Matriz de riesgos

5.2 Metodología: cómo calculamos la probabilidad (%)

Definición operativa: la probabilidad se calcula como el porcentaje de usuarios comprometidos sobre los usuarios evaluados en cada ejercicio.

Fórmula: Probabilidad (%) = (Usuarios comprometidos / Usuarios evaluados) × 100

- **Phishing 1:** 16/250 = 6,4%
- **Phishing 2:** 37/250 = 14,8%
- **Smishing:** 2/80 = 2,5%
- **Vishing:** 5/40 = 12,5%
- **Rogue AP:** 1/448 ≈ 0,22%
- **Quishing:** 4/N (sin datos reales) = 0% → Probabilidad Baja y Impacto Bajo en esta ronda

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

8 / 47

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

6 Intrusión física

6.1 Objetivo

El propósito de las pruebas de intrusión física, en el contexto de la ingeniería social, es evaluar la seguridad de las instalaciones físicas de una organización y la susceptibilidad de los empleados a ser engañados o manipulados. Estas pruebas buscan identificar vulnerabilidades en los accesos físicos, los controles de seguridad y el comportamiento del personal ante situaciones sospechosas.

6.2 Impacto

La intrusión confirmada demuestra que un adversario podría acceder a áreas internas, observar y fotografiar material sensible (dispositivos, planos de evacuación, equipos, material con logos corporativos), y reconocer rutas/controles para ataques posteriores. El riesgo compuesto incluye: fuga de información (potencial documentación, avistamiento de listados de inscripción a actividades), fraude (uso de logos en materiales institucionales), sabotaje o apropiación de dispositivos potencialmente no custodiados, y amenaza a la integridad de las personas si el intruso se aproxima a zonas críticas. La confianza social (deportiva/colaborativa) y el estrés operativo en horas punta facilitaron el *bypass* de controles de identidad.

6.3 Propuesta

Propuesta elegida y justificación

Se ejecutará un intento de acceso físico controlado en la sede principal, empleando un carnet de visitante que fue suplantado previamente. Este escenario fue seleccionado porque el control de acceso para visitantes se basa únicamente en la validación visual del carnet, a diferencia del acceso del personal que requiere tarjeta electrónica; por tanto, representa un vector realista para evaluar controles físicos y procedimientos de verificación.

Diseño de pretextos y decisiones clave

- Pretexto 1 (entrada principal): ingreso ordinario con el flujo general. Resultado: Se aprovechó el momento de afluencia media de personal para ingresar de manera simultánea al flujo de usuarios. El vigilante de acceso permitió el paso tras una verificación visual rápida del carné falso, sin realizar validaciones adicionales.
- Pretexto 2 (entrada de vehículos): “dejé el carnet dentro”. Decisión clave: inducir duda y aprovechar la presión por fila de vehículos. Resultado: No se consiguió el acceso, ya que el control de ingreso al área funciona mediante biometría, lo que impidió la entrada sin la validación correspondiente.
- Técnicas internas: *tailgating* para desplazarse por distintos pisos, observación cercana de elementos con identidad institucional (carnets, cordones, señales) y documentación (fotográfica) de hallazgos visibles. Resultado: no se logro acceder gracias a los controles actuales de seguridad física.

6.4 Desarrollo del escenario

Fase 1. Preparación y permisos

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

9 / 47

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

Se realizó reconocimiento externo de la sede (Principal) para mapeo de puntos de acceso, flujos de ingreso, rutinas visibles y artefactos de identificación (colores de cordones, formatos de carnet, señalética de visitantes).

Fase 2. Implementación técnica (logística de intrusión)

Se definieron pretextos y orden de intentos: primero la entrada principal, después la entrada de vehículos (mencionada por el primer filtro). Se preparó material mínimo de mimetización (carnet de visitante). Se establecieron límites: no forzar cerraduras ni violentar dispositivos; no interactuar con sistemas TI; no incurrir en coerción. Se planificó la toma de evidencia fotográfica únicamente de información expuesta (a la vista).

Fase 3. Producción y despliegue físico

Intento 1 (entrada principal): acceso gracias al carnet de visitante falsificado (control no funcionó). Ya en interior, se ejecutó *tailgating* para moverse entre varios pisos (4 pisos) y recopilar evidencia fotográfica (potencial documentación expuesta, dispositivos, material con logos/identificadores, planos de evacuación), sin embargo, no fue posible ya que en cada edificio el acceso ahora es con biometría.

Intento 2 (entrada vehículos): el auditor invocó el pretexto “carnet adentro” en horario de alto flujo. Se percibió duda del personal de seguridad, sin embargo, no permitió el ingreso ya que requiere acceso por biometría.

Fase 4. Operación, monitoreo y cierre

No se logró el acceso, gracias al control de biometría actualmente implementado en los puntos de ingreso vehicular. Este mecanismo refuerza significativamente la seguridad física, al asegurar que solo personal autorizado pueda acceder, incluso ante intentos de suplantación o pretextos sociales.

6.5 Resultados obtenidos

Duración de la actividad: 1 día (30 de septiembre 2025).

Indicadores operativos (derivados del relato):

- **Intentos de ingreso:** 2
 - **Principal:** **aceptado** (*bypass* por pretexto + presión).
 - **Vehículos:** **rechazado** (control efectivo).
- **Tasa de éxito de intrusión (por intento):** $1/2 = 50\%$.
- **Técnicas empleadas:** **pretexting**, **mimetización**, **tailgating**.
- **Evidencia recolectada (categorías):** no se logró recolectar evidencia gracias a los controles de biometría.
- **Salida:** sin verificación adicional de identidad (o con verificación no estricta).

Tabla de síntesis

Métrica	Valor
Sede	Principal
Puntos de acceso evaluados	Principal (permitido) / Vehicular (denegado)
Método de bypass	Pretexto “carnet falso” + flujo medio
Evidencia	Fotos de ingreso a la sede
Tasa de éxito (por intento)	50% (1 de 2)
Acompañamiento a No-Credencial	Insuficiente
Duración	1 día (30 de Septiembre)

Tabla 3. Síntesis intrusión física

6.6 Evidencias

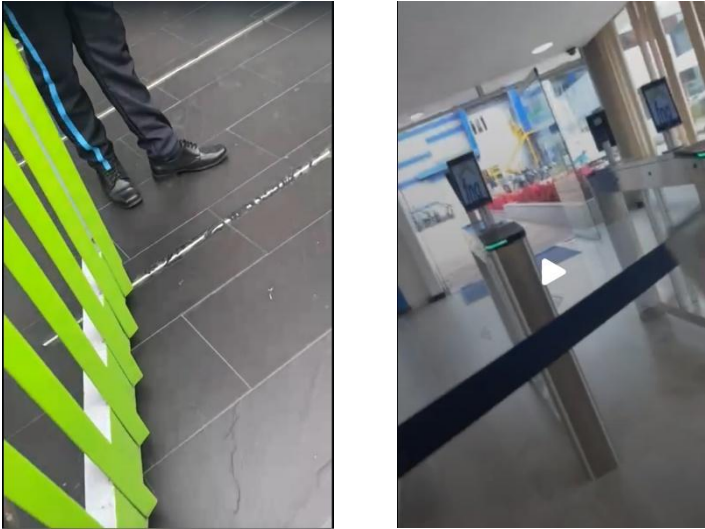


Ilustración 1. Detección de puntos de acceso

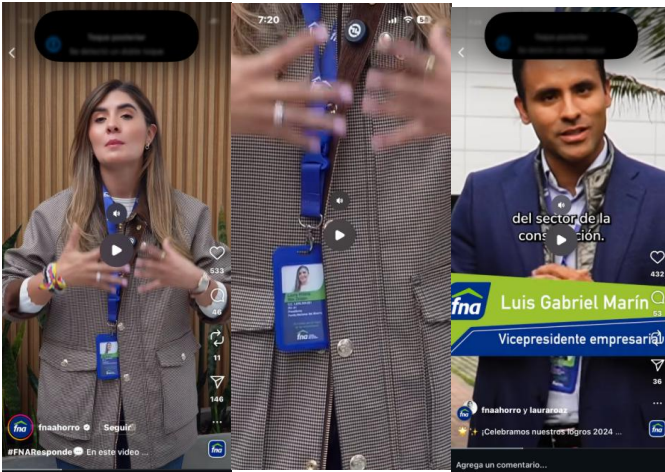


Ilustración 2. Identificación de carnet y porte de cordones corporativos

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

11 / 47

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



Ilustración 3. Ingreso a pisos internos

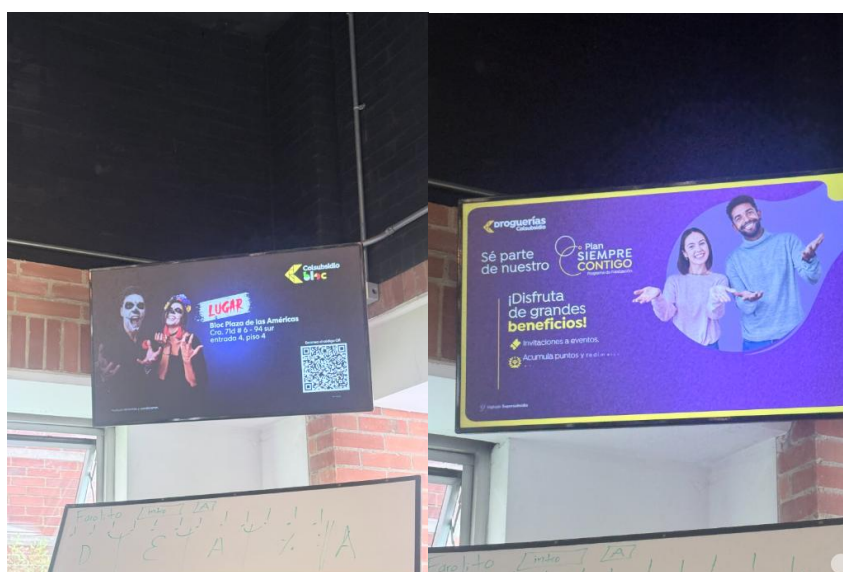


Ilustración 4. Ingreso casino interno

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

12 / 47

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

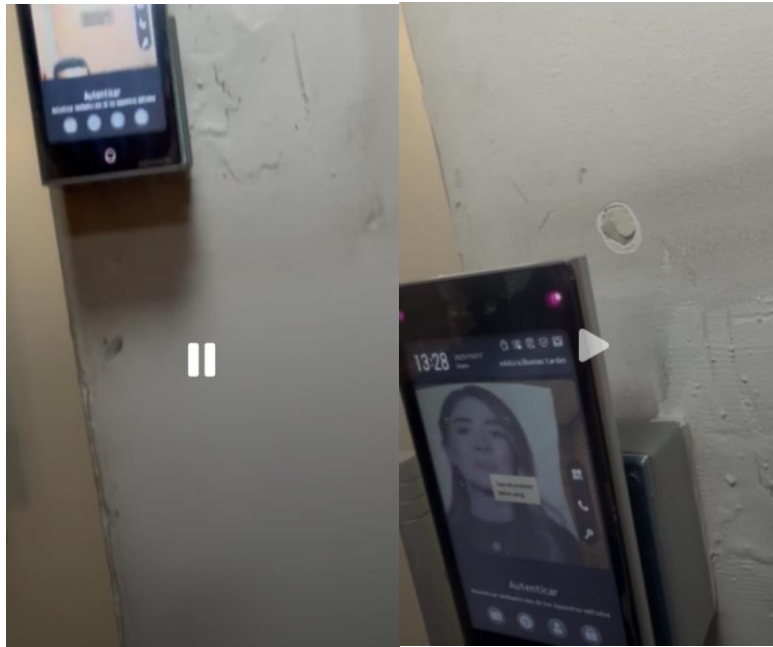


Ilustración 5. Intento de acceso a pisos.

6.7 Recomendaciones

- Siempre verificar en la entrada principal, el personal de control de acceso debe validar la identidad contra listas, incluso si viene en vehículo.
- En días de eventos, reforzar filtros como, pre-registro, brazaletes únicos por sede o exigencia estricta del uso de carné.
- Acompañamiento obligatorio para visitantes y proveedores.
- En caso de ver a una persona sospechosa sin distintivo o en una zona inusual realizar el reporte.

7 Qhishing

7.1 Objetivo

El objetivo principal de esta técnica es engañar a las víctimas para que revelen información personal sensible, como credenciales de inicio de sesión, datos bancarios o información de tarjetas de crédito, a través de códigos QR maliciosos. Se utilizan códigos QR manipulados que, al ser escaneados, dirigen a las víctimas a sitios web fraudulentos que imitan páginas legítimas, donde se les solicita que ingresen información confidencial.

7.2 Impacto

Las víctimas pueden verse comprometidas al ingresar sus credenciales o información personal en sitios web fraudulentos. Los atacantes pueden obtener acceso a cuentas, lo que les permite acceder a información confidencial. Los ataques exitosos pueden causar interrupciones en las operaciones normales de una organización, lo que afecta la productividad y el servicio al cliente.

7.3 Propuesta

Propuesta elegida y justificación.

Se consideraron tres propuestas, (beneficios por medio de un convenio con caja de compensación, Escanea y recibe un cupón digital de Amor y Amistad, Participa en la rifa de Halloween, escanea aquí.) finalmente gracias al ingreso físico y las pocas evidencias que se lograron tomar, nos dimos cuenta de que Colsubsidio es un aliado del FNA y presta varios beneficios a sus colaboradores incluyendo un casino interno, por esta razón se eligió **“Cupón de descuento en Casino Interno Colsubsidio”**.



Ilustración 6. Pieza para Qhishing

Diseño de plantillas y decisiones clave.

Se diseñó un portal web falso que replica la línea gráfica institucional del Fondo Nacional del Ahorro (FNA) e incorpora los logos de Colsubsidio, con el objetivo de simular una campaña legítima. El sitio promociona un

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

14 / 47

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

supuesto cupo de descuento en el casino interno, utilizando una paleta de colores y elementos visuales coherentes con la imagen corporativa de ambas entidades para aumentar su credibilidad.

El portal incluye imágenes atractivas de alimentos y un formulario de registro en el que se solicita a los usuarios ingresar sus datos personales con el fin de “participar” en la promoción. Este diseño busca evaluar la capacidad de los usuarios para identificar señales de fraude digital y medir su reacción ante un intento de ingeniería social tipo phishing.

7.4 Desarrollo del escenario

Fase 1. Preparación y permisos.

En coordinación con el cliente, se desarrolló la narrativa y se validó el diseño final. El cliente definió los lugares específicos donde se pegarían los QR, ubicaciones de alto tránsito (comedor, asesores, mesas cafetería OMA), preservando la naturalidad del entorno.

Fase 2. Implementación técnica.

Se desplegó el dominio parecido en hosting con certificado HTTPS. Las validaciones client/server reforzaron la apariencia de “beneficios oficiales” con funcionalidad de captura real de datos. El QR permitió observar picos de interacción por día.

Fase 3. Producción y despliegue físico.

Se imprimieron 20 QR en alta calidad y se instalaron el 17 de octubre, dejando registro fotográfico. A lo largo de los días siguientes, se monitoreó el panel del QR y se consolidaron observaciones de seguridad local.

Fase 4. Operación, monitoreo y cierre.

Durante la ventana comprendida entre el 20 y el 21 de octubre de 2025, no se registraron reportes a través de ninguno de los canales de seguridad sobre la presencia de los códigos QR adheridos en la sede principal. Esto sugiere que el ejercicio se desarrolló sin alertas o incidentes visibles para el personal o los sistemas de monitoreo de la entidad.

7.5 Resultados obtenidos

Duración de la actividad: 17 de octubre – 21 de octubre.

Escaneos únicos: 4.

- Octubre: 4 escaneos únicos (todo el día 29/08).

El ejercicio confirma una exposición real ante escenarios de quishing (phishing mediante códigos QR), evidenciando la posibilidad de que empleados o visitantes interactúen con elementos maliciosos sin activar alertas internas. Las cifras obtenidas y la ausencia de reportes son suficientes para justificar la implementación de mejoras tanto en la señalética institucional como en los procedimientos de validación visual y física dentro de las instalaciones. Asimismo, se recomienda planificar futuras iteraciones del ejercicio con mayor nivel de instrumentación, como el uso de códigos QR, mecanismos de verificación autenticada o alertas internas automatizadas para fortalecer la detección temprana de este tipo de incidentes.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

15 / 47

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

Tabla de síntesis

Métrica	Valor
Sede puesta a prueba	1
Permanencia máxima	3 días
Ventana de campaña	17/10 – 21/10
Escaneos totales	4
Captura de datos real	4

Tabla 4. Síntesis Quishing

7.6 Evidencias

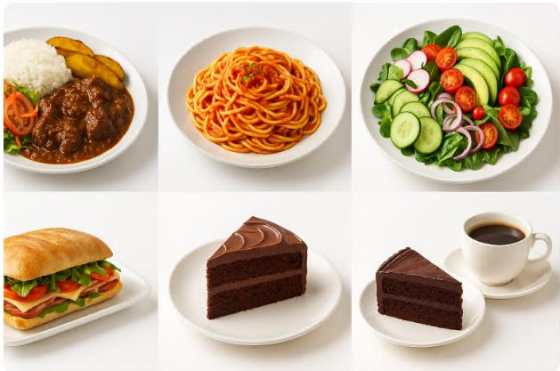
Se creó un portal web con temática de cupón de descuento, diseñado para simular una promoción institucional. El sitio incluía elementos visuales atractivos, como fotografías de alimentos, colores llamativos y logos institucionales simulados, con el fin de generar confianza y credibilidad ante el usuario.

Adicionalmente, se incorporó un formulario de registro donde se solicitaban datos básicos del participante, simulando un proceso legítimo de inscripción para reclamar el beneficio. Este diseño permitió evaluar el nivel de susceptibilidad de los usuarios ante sitios falsos que imitan campañas reales, así como analizar su comportamiento frente a solicitudes de información personal en contextos aparentemente seguros.

¡Colsubsidio y el Fondo Nacional del Ahorro te invita!

Aprovecha esta oportunidad única y participa para ganar un cupón del 30% de descuento.

¿Que esperas?, es válido solo por hoy en el Casino Zona C.



Regístrate y participa

Ilustración 7. página web



Regístrate y participa

Nombre Completo:

Correo Electrónico:

Teléfono:

Área:

Registrarme

Ilustración 8. formulario ajustado.



¡Registro Exitoso!

Tu registro ha sido procesado correctamente.

En breve enviaremos tu **cupón de descuento** al correo electrónico que registraste.

Salir

© Fondo Nacional del Ahorro - Convenio comedor Colsubsidio

Ilustración 9. Mensaje de registro exitoso.

Código QR creado

Se procede a generar un código QR, único para esta actividad.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

17 / 47

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



Ilustración 10. Código QR, generado para la actividad.



Ilustración 11. Plantilla final generada para distribuir en la sede.

Distribución de códigos QR en la sede principal, se tomaron evidencias de los códigos QR distribuidos en varios puntos de la sede.



Ilustración 12. Evidencias del despliegue de los códigos.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

18 / 47

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

Datos recopilados en nuestro servidor desplegado.



```
registros.txt - Notepad
File Edit Format View Help
nombre: Carlos Manuel Cárdenas Toledo
email: ccardenas@...
phone: 32135...
area: G.anti...
nombre: Vivian...
email: vloza...
phone: 30436...
area: VICE...
nombre: Alex...
email: alexa...
phone: 31645...
area: Gerenc...
nombre: Andre...
email: jcam...
phone: 3175...
area: CNA
```

Ilustración 13. Datos de login.

7.7 Recomendaciones

- Desconfiar de avisos nuevos que soliciten información, carteles corporativos sin sello/folio oficial o que no hayan sido notificados por canales oficiales suelen ser sospechosos.
- Realizar la validación del dominio al que se es redirigido al escanear un código QR, revisión de dominio y subdominio, uso de HTTPS.
- Retiro y reporte, si el QR o afiche no está autorizado, este debe ser retirado y notificado al área correspondiente.
- No realizar escaneos con urgencia, no es normal que actualizaciones críticas se soliciten a través de códigos QR en zonas comunes.
- Implementar una política QR corporativa. Toda pieza oficial debe incorporar folio/sello, un QR secundario de verificación que apunte a una página oficial (“¿Esta campaña es legítima?”) y, cuando sea viable, elementos antifraude (marca de agua/holograma). Esto genera una forma sencilla y visible de manera inmediata para identificar cualquier tipo de campaña no autorizada.
- Monitorear dominios lookalike/typosquatting, con alertas tempranas y bloqueos por DNS y HTTP en la infraestructura. Mantener HSTS, SPF/DKIM/DMARC y consistencia de certificados.
- Comunicar en canales oficiales que la entidad no solicita credenciales ni pagos por QR si es el caso. Capacitar trimestralmente a personal de atención y seguridad con un checklist práctico (folio, dominio, sellos, tono del mensaje, urgencia inusual entre otros).

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

19 / 47

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

8 Rogue AP

8.1 Objetivo

El objetivo de esta técnica engañar a los usuarios para que se conecten a una red Wi-Fi falsa que imita a una red legítima. Este tipo de ataque se basa en la creación de un punto de acceso Wi-Fi malicioso que se presenta como una red confiable, lo que permite al atacante interceptar el tráfico de datos y, potencialmente, robar información sensible de los usuarios conectados. Es importante mencionar que este ataque pretende evaluar el comportamiento de los usuarios, más no representa una evaluación sobre las redes Wi-Fi de la entidad, por lo que no debe confundirse con una auditoría a la red Wi-Fi.

8.2 Impacto

El éxito de este tipo de ataque podría causar acceso no autorizado a cuentas y servicios específicos de los usuarios conectados a la red maliciosa, robo de información personal al obtener credenciales de inicio de sesión, interceptación de comunicaciones, lo que puede resultar en exposición de información privada o manipulación de datos enviados o recibidos por la víctima. Por último, puede causar interrupciones en las operaciones normales de una organización, afectando la productividad y el servicio al cliente.

8.3 Propuesta

Propuesta elegida y justificación.

Se eligió anunciar por correo electrónico el despliegue de una “nueva red Wi-Fi corporativa” en la sede Principal. Esta narrativa tiene como objetivo mejorar la conectividad móvil dentro de las instalaciones del Fondo Nacional de Ahorro. De este modo, si un usuario se conecta al SSID similar a los utilizados en la sede, el portal cautivo solicita autenticación, pero luego muestra un mensaje de error de conectividad, la experiencia resulta normal y reduce la sospecha, mientras permite medir la propensión a entregar credenciales.

Diseño de plantillas y decisiones clave.

- **Remitentes verosímiles** bajo un dominio similar controlado se creó un buzón de correo para enviar este comunicado (comunicaciones@fna-qov.co).
- **Copy del correo** sobrio y corporativo (tono informativo, sin alarmismo), indicando que existe una nueva red corporativa.
- **SSID similar** alineado a convenciones internas (mismo estilo de nombre que los SSIDs legítimos; potencia/canales coherentes).
- **Portal cautivo** logos y colores corporativos; **formulario de usuario/contraseña de red**; tras el envío, **mensaje de “sin conexión a internet”** para enmascarar la captura y evitar múltiples reintentos visibles.
- **Salvaguardas éticas:** resguardo de cualquier contraseña capturada y comprobación si la credencial es correcta.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

20 / 47

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

8.4 Desarrollo del escenario

Fase 1. Preparación y permisos.

Aprobación del cliente del mensaje de correo, alcance técnico y límites. Habilitación de buzones bajo el dominio similar al del FNA.

Fase 2. Implementación técnica.

Despliegue del SSID **WLAN_CORP**. Vinculación del portal cautivo al SSID falso con validaciones mínimas y mensaje de error post-envío. Registro mínimo de eventos (intentos y envíos) sin retener información innecesaria.

Fase 3. Producción y despliegue físico.

Vector principal: correo electrónico (no se utilizó cartelería). Envío de 1,627 correos con el asunto ¡Nueva red Wi-Fi disponible para colaboradores! a las posibles víctimas elegidas con anterioridad. Instrumentación para medir tasas de apertura.

Fase 4. Operación, monitoreo y cierre.

Monitoreo de aperturas y de interacciones con SSID/portal. Resultado: 5 aperturas y 3 ingreso de credenciales. Al finalizar la actividad se apaga el SSID falso y se deshabilitan los buzones creados.

8.5 Resultados obtenidos

Duración de la actividad: 1 día (6 de noviembre de 2025)

Métrica equivalente del ejercicio:

- Correos enviados: 1,627
- Aperturas: 5 → tasa de apertura $\approx 0,3\%$
- Credenciales capturadas: 3
- Conversión sobre credenciales capturadas: $3/1,627 = 0,18\%$
- Conversión sobre aperturas: $5/1,627 = 0,30\%$

Este tipo de ejercicio puede dar una falsa sensación de seguridad si se evalúa solo como “porcentaje de caída” frente al total de correos enviados: $5/1,627 = 0,30\%$ ($\approx 0,30\%$). Con porcentajes tan bajos es fácil concluir que “estamos bien protegidos”; sin embargo, una sola credencial válida basta para que un atacante se conecte a la red Wi-Fi corporativa, enumere segmentos, servicios y dispositivos, realice movimientos laterales, pruebe reutilización de contraseñas y eleve privilegios. Además, esa misma credencial (sincronizada) puede habilitar la enumeración en Azure/Entra ID, consulta de grupos/roles, tanteo de aplicaciones SSO, y otros vectores de abuso. Por ello, no debe juzgarse el riesgo por el cociente “personas que cayeron / correos enviados”, sino por el impacto potencial de una credencial comprometida y la capacidad de contención (MFA, detección de accesos anómalos, rotación de credenciales).

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

21 / 47

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

Tabla de síntesis

Métrica	Valor
Sede objetivo	Sede Principal
Cobertura	Varios pisos
Canal de activación	Correo electrónico
Asunto del correo	¡Nueva red Wi-Fi disponible para colaboradores!
SSID desplegado	WLAN_CORP
Correos enviados	1627
Aperturas	5 (≈0,3%)
Credenciales capturadas	3
Técnicas coercitivas (deauth/jamming)	No utilizadas
Uso de credenciales	Ninguno (resguardo y reset)
Duración de la actividad	1 día (06/11/2025)

Tabla 5. Síntesis Rogue AP

8.6 Evidencias

Plantilla creada, la cual se envió mediante correo informando el despliegue de la nueva red WiFi.



Ilustración 14. Plantilla creada para el RogueAP

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

22 / 47

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

Primeras credenciales capturadas.

```
[*] Esperando credenciales (Ctrl+C para finalizar)...\n-----\nVictimas conectadas: 0\n\nArray\n(\n  [username] => spa[REDACTED]\n  [password] => Cie[REDACTED]\n  [language] => spanish\n)\n
```

Ilustración 15. Credenciales validas capturadas.

Credenciales ingresadas.

```
[*] Esperando credenciales (Ctrl+C para finalizar)...\n-----\nVictimas conectadas: 4\n\nArray\n(\n  [username] => mgal[REDACTED]\n  [password] => M4r1[REDACTED]\n  [language] => spanish\n)\n\nArray\n(\n  [username] => mgal[REDACTED]\n  [password] => M4r1[REDACTED]\n  [language] => spanish\n)\n\nArray\n(\n  [username] => mgal[REDACTED]\n  [password] => M4r1[REDACTED]\n  [language] => spanish\n)\n\nArray\n(\n  [username] => bmore[REDACTED]\n  [password] => Ital[REDACTED]\n  [language] => spanish\n)\n\nArray\n(\n  [username] => JAG0[REDACTED]\n  [password] => Apt0[REDACTED]\n  [language] => spanish\n)\n\nArray\n(\n  [username] => Juse[REDACTED]\n  [password] => Sana[REDACTED]\n  [language] => spanish\n)\n
```

Ilustración 16. Credenciales validas capturadas.

RF451386	Petición	En curso	FALLAS DE AGENTE TRENO MICRO
RF451380	Petición	En curso	REPORTE CORREO SOSPECHOSO
RF451482	Petición	En curso	¡NUEVA RED WI-FI DISPONIBLE PARA...
RF451484	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA ...
RF451482	Petición	En curso	VERIFICACIÓN DE CORREO
RF451488	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451489	Petición	En curso	REVISIÓN CORREO NO DESEADO
RF451496	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA ...
RF451492	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451498	Petición	En curso	REVISIÓN CORREO NO DESEADO
RF451501	Petición	En curso	¡NUEVA RED WI-FI DISPONIBLE PARA...
RF451504	Petición	En curso	REVISIÓN CORREO NO DESEADO
RF451508	Petición	En curso	CORREO SOSPECHOSO
RF451510	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451512	Petición	En curso	REPORTO EL CORREO ¡NUEVA RED ...
RF451513	Petición	En curso	CORREO MALICIOSO
RF451521	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451522	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA ...
RF451524	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA ...
RF451526	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA...
RF451522	Petición	En curso	VERIFICACIÓN DE CORREO
RF451529	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451530	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451534	Petición	En curso	NUEVA RED WI-FI DISPONIBLE PARA...
RF451536	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...
RF451543	Petición	En curso	¡NUEVA RED WI-FI DISPONIBLE PARA...
RF451542	Petición	En curso	VERIFICACIÓN DE CORREO
RF451546	Petición	En curso	RV: ¡NUEVA RED WI-FI DISPONIBLE P...

Ilustración 17. Casos creados por los usuarios.

8.7 Recomendaciones

- Verificar el SSID de las redes a las que se realizan conexiones, en caso de tener dudas consultar al personal encargado.
- Si se realiza la redirección a un portal en el que se solicitan credenciales, verificar que el dominio o URL sea oficial.
- Correos de “nueva red”, mensajes desde dominios similares al oficial son señal de fraude.

9 Vishing

9.1 Objetivo

Simular una campaña de Vishing (ingeniería social vía llamada telefónica) para evaluar la propensión de los colaboradores a entregar información personal ante un pretexto beneficioso. Se buscó medir: (1) tasas de contacto y respuesta, (2) capacidad de verificación frente a una llamada que aparenta legitimidad (mención de grabación, tono formal, marcas reconocidas), y (3) la conversión a divulgación de datos al ser invocados beneficios cotidianos (bonos para artículos del hogar).

9.2 Impacto

Si un atacante obtiene datos personales y de contacto (nombre completo, cédula, correo, teléfono y área), puede combinarlos para fraudes multi-canal (phishing dirigido, Smishing, reinicio de cuentas por ingeniería social, apropiación de identidad parcial), y/o como insumo para ataques de segunda etapa (apertura de *tickets* falsos, suplantación en canales internos, ataques a proveedores). Aunque la tasa de éxito no sea alta, basta un pequeño número de respuestas para habilitar movimientos posteriores con alto impacto (robo de información, intrusión, daño reputacional).

9.3 Propuesta

Propuesta elegida y justificación.

De tres guiones preparados, el cliente Fondo Nacional de Ahorro eligió el pretexto: suplantar a un trabajador del aliado Ktronix para comunicar un beneficio en alianza con las cajas de compensación Cafam-Colsubsidio. La atractividad del incentivo (bonos para electrodomésticos/artículos del hogar) aumenta la disposición a colaborar, al estar alineado con necesidades frecuentes y beneficios creíbles para colaboradores.

Diseño de plantillas y decisiones clave.

- Guion telefónico: saludo institucional, aviso de llamada grabada/monitoreada (señal de formalidad), explicación breve del beneficio aliado y solicitud explícita de consentimiento para continuar.
- Flujo de decisión: si el colaborador aceptaba el beneficio, se solicitaban datos personales (nombres, cédula, correo corporativo, celular, área).

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

24 / 47

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

- Manejo de objeciones: respuestas pautadas ante dudas de legitimidad (“podemos enviarle también la información a un correo...”), evitando coerción o presión del beneficio.
- Límites éticos: no solicitar credenciales, tokens ni información financiera; recolección mínima necesaria; resguardo y reporte al cliente.

9.4 Desarrollo del escenario

Fase 1. Preparación y permisos.

Se obtuvo autorización del cliente para el uso del pretexto de beneficios con marcas aliadas (Cafam-Colsubsidio y Ktronix) y para contactar a la muestra de 40 colaboradores. Se definieron límites (sin solicitudes de contraseñas ni movimientos financieros) y se aprobaron los scripts (apertura, beneficio, consentimiento, cierre). Se acordó un horario laboral para las llamadas.

Fase 2. Implementación técnica.

Se configuró la operación de llamadas (línea dedicada y registros mínimos), con guiones estandarizados y checklist de cumplimiento (verbalizar grabación, confirmar consentimiento, registrar únicamente los campos permitidos). Se definió el sistema de marcación y rotación de intentos para minimizar congestión e incrementar la tasa de respuesta sin generar molestia.

Fase 3. Producción y despliegue.

El canal fue 100% telefónico, sin material físico. Se realizaron 40 llamadas a la muestra aprobada, siguiendo el guion y tiempos de contacto establecidos. El tono buscó profesionalismo y familiaridad, remarcando la alianza entre Ktronix–Cafam–Colsubsidio como ancla de credibilidad.

Fase 4. Operación, monitoreo y cierre.

Durante la ventana del 29 al 31 de octubre de 2025, se registraron: 10 llamadas contestadas y 30 no contestadas. De las contestadas, 5 personas entregaron datos como el correo, 1 persona de las 5 entregó la mayoría de datos y 5 no brindaron información (rechazo, duda, personal de RH). Al cierre, se consolidaron métricas y se resguardaron los datos obtenidos para su gestión por el cliente (evaluación, notificación y acciones de concienciación).

9.5 Resultados obtenidos

Duración de la actividad: 3 días (29–31 de octubre de 2025)

Cálculos clave:

- **Tasa de contacto (contestación):** $10/40 = 25\%$ ($\approx 25\%$)
- **Tasa de éxito sobre el total llamado:** $5/40 = 12,5\%$ ($\approx 12,5\%$)
- **Conversión entre quienes contestaron:** $5/10 = 50\%$ ($\approx 50\%$)
- **Negativas/No entrega entre contestadas:** $5/10 = 50\%$ ($\approx 50\%$)
- **No contestadas:** $30/40 = 75\%$ ($\approx 75\%$)

Interpretación: aunque el **éxito global** (12,5%) pueda parecer moderado, la **conversión entre contactos efectivos** (50%) evidencia que el **pretexto** y el **guion** fueron persuasivos. Un atacante persistente, con mayor volumen o variaciones de narrativa, **podría escalar** los resultados.

Tabla de síntesis

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

25 / 47

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

Métrica	Valor
Ventana de campaña	29–31/10/2025
Muestra objetivo	40 colaboradores
Llamadas contestadas	10 (25%)
Llamadas no contestadas	30 (75%)
Entregas de datos	5
Tasa de éxito (sobre total)	12,5%
Conversión (sobre contestadas)	50%
Negativas/no entrega (sobre contestadas)	50%
Pretexto	Beneficio Ktronix–Cafam–Colsubsidio (bonos hogar)
Límites éticos	Sin credenciales/finanzas; recolección mínima; resguardo

Tabla 6. Síntesis Vishing

9.6 Evidencias

Evidencias de información obtenida.

Nombre	Correo	Número Tel	ID	Nombre completo	Num. De identificación	Correo electrónico	Número de celular	Dependencia/area	Observaciones
LOPEZ CARDENAS JUAN PABLO	jplopez@fna.gov.co	3.103E+09	1			tuapa_1984@gmail.com			Pidió seguir el proceso por correo porque está muy ocupado
MORA ARTURO VANESSA NATALI	vmora@fna.gov.co	3115584756	2						Número temporalmente suspendido
ORTIZ PUENTES CHRISTIAN DAVID	cdortiz@fna.gov.co	3.213E+09	3	Cristian David Ortiz	1121715767	ortizpuentesdavid19@gmail.co	3212787337	Comercial	No contesta
GOMEZ GUTIERREZ ESTEFANY YULIET	egomez@fna.gov.co	3.048E+09	4			estefg01@hotmail.com			Pidió seguir el proceso por correo porque está muy ocupado
BUSTOS LEON LEYDI PAOLA	lbustos@fna.gov.co	3.506E+09	5						Es de recursos humanos
CERVANTES OTALVAREZ MARLY SOFIA	mcervantes@fna.gov.co	3.107E+09	6						Pidió seguir el proceso por correo porque está muy ocupado
AHUMADA GOMEZ ALVARO ANDRES	aahumada@fna.gov.co	3.116E+09	7						Es de recursos humanos y dijo que eso no era oficial
RODRIGUEZ JIMENEZ LEIDY JOHENY	lrodriguez@fna.gov.co	3.228E+09	8			lrodriguezj@fna.gov.co			No contesta
DIAZ RODRIGUEZ CAMILA ALEJANDRA	cdiazr@fna.gov.co	3.216E+09	9						Pidió seguir el proceso por correo porque está muy ocupado
PINEDA BETANCOURT ANGELA MARIA	apineda@fna.gov.co	3.177E+09	10						No contesta

Ilustración 18. Evidencias 1

Nombre	Correo	Número Teléfono	ID	Nombre completo	Num. De identificación	Correo electrónico	Número de celular	Dependencia/area en la que trabaja	Observaciones
DIAZ LOPEZ MARIA ANGELICA	MdiazL@fna.gov.co	4458950/3112474201	1			ange8050@gmail.com			No contesto
RUBIANO VARGAS ANGELA MARIA	ARubiano@fna.gov.co	3112964719	2						mas tarde
ARAZO HERNANDEZ JAVIER ENRIQUE	Jarazo@fna.gov.co	5017666626	3						No contesto
PRIETO NARANJO DAVID ARMANDO	dprieto@fna.gov.co	3193816312	4						Es de seguridad TI y me colgo
QUINTERO ERIKA PAOLA	Equintero@fna.gov.co	501579114	5						Falta un numero
SILVA CASTELLANOS JUAN ANDRES	jsilvac@fna.gov.co	5153934616	6						No contesto
RAMIREZ GALAN JUAN CARLOS	jramirez@fna.gov.co	3106666219-9356851	7						No quiere bono
FRAILE SANCHEZ DUVAN ANDRES	dfraile@fna.gov.co	3187942101-9014908	8						No contesto
DELGADO RIVERA LUIS ALBERTO	ldelgador@fna.gov.co	3503346578	9						No contesto
NAJAS MAHECHA NIDYA	Nnajas@fna.gov.co	5105521492	10						No contesto

Ilustración 19. Evidencias 2

Grabaciones

- Para la revisión de evidencias del ejercicio de vishing, se debe acceder a la carpeta vishing/grabaciones y escuchar únicamente aquellas grabaciones en las que se haya logrado una interacción efectiva con los usuarios.

9.7 Recomendaciones

- En caso de recibir llamadas con asuntos asociados a premios y bonos, no entregar datos sensibles por vía telefónica.
- Corta y verifica, finalizar una llamada si se considera sospechosa y devolver la llamada a números telefónicos oficiales.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

26 / 47

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

- No entregar datos como cédula, correo o códigos en llamadas iniciadas por un tercero.
- Grabación y folio, solicita el número del caso y canal oficial para continuar por escrito.
- Comparte el indicador, las estafas suelen estar acompañadas de frases como “última oportunidad” o “bono único” para presionar al usuario y ponerlo en una posición de premura.
- Validar si el número telefónico origen es un canal oficial o legítimo.

10 Smishing

10.1 Objetivo

El objetivo de este ejercicio es evaluar la susceptibilidad de los colaboradores ante un mensaje SMS con apariencia corporativa, que simula provenir de una campaña oficial denominada “Beneficios Colsubsidio-FNA”. La prueba tiene como finalidad medir la tasa de respuesta, el nivel de interacción y la conversión hacia la entrega de datos sensibles, así como analizar la efectividad del pretexto empleado (beneficios y descuentos exclusivos).

El mensaje se redactó con un tono institucional y lenguaje persuasivo, e incluía un enlace que redirigía a un portal externo diseñado con elementos visuales de Colsubsidio y del Fondo Nacional del Ahorro, simulando una página legítima de beneficios corporativos. Una vez dentro, el portal mostraba una serie de supuestos beneficios (viajes, descuentos en farmacias, beneficios exclusivos, entre otros), tras lo cual solicitaba al usuario ingresar sus credenciales de acceso, sin embargo, al autenticarse les generaba un error y se daba la opción de recuperar las credenciales y así capturar mayor información. Tras la autenticación, el sistema generaba intencionalmente un error y ofrecía la opción de recuperar las credenciales, procedimiento que permitía recopilar información adicional del participante. Esta secuencia buscó evaluar la reacción natural de los usuarios ante un escenario de smishing y analizar hasta qué punto el pretexto y los pasos posteriores (error + recuperación) incrementan la probabilidad de entrega de datos sensibles.

Cabe resaltar que en ningún momento se especificó el tipo de credencial que debía usarse, dejando a criterio del participante la decisión sobre qué información ingresar. Esto permitió evaluar de manera más realista el comportamiento natural del usuario ante un escenario de ingeniería social de tipo smishing, observando su nivel de precaución, la atención a los indicadores de seguridad y su capacidad para identificar un intento de engaño digital.

10.2 Impacto

Si un atacante logra que el destinatario entregue datos por SMS (nombres, apellidos, correo corporativo, sede/área, teléfono, intereses), puede construir perfiles explotables para campañas posteriores: phishing dirigido, Smishing de segunda etapa, llamadas de Vishing con mayor credibilidad, o bypass de validaciones de identidad en mesas de ayuda. Incluso con una tasa de éxito baja, cada registro amplifica el alcance de futuros ataques, facilita la suplantación y deteriora la confianza en las comunicaciones corporativas.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

27 / 47

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

10.3 Propuesta

Propuesta elegida y justificación.

De 4 guiones propuestos (“Cambio de contraseña obligatorio Verify”, “Actividad inusual en cuenta corporativa”, “Convocatoria interna de talento y promociones 2025”, “Confirmación a jornada de salud”, “Aceptación de Política de Protección de Datos”) y (“Suplantación de voz Solicitud de información”). Finalmente, gracias a un primer reconocimiento durante la técnica de ingreso físico nos dimos cuenta en los monitores del casino interno que Colsubsidio ofrece varios beneficios a sus afiliados y se eligió “Beneficios Colsubsidio-FNA” por su alta similitud y atractividad (beneficios personales, baja fricción y percepción de legitimidad al provenir—aparentemente—de “Bienestar – Colsubsidio”).

Diseño de plantillas y decisiones clave.

- Texto del SMS: “Beneficios Colsubsidio: Colsubsidio y FNA amplían tus beneficios. Ingresar para conocer los nuevos convenios y bonos exclusivos **%Enlace al portal falso%.**”
- Formularios de login de sesión con identidad visual similar (colores/logos Colsubsidio) solicitando: Número de Documento y Contraseña. En cuanto a la opción de recuperación de contraseña se solicita, número de documento, contraseña anterior y contraseña nueva.
- Tono sobrio y positivo, evitando urgencia excesiva y sin pedir credenciales ni datos financieros.
- Medición: El envío de datos a nuestro servidor de comando y control nos permitió obtener la medición de cuantos usuarios ingresaron los datos tanto en el formulario de inicio de sesión y recuperación.

10.4 Desarrollo del escenario

Fase 1. Preparación y permisos.

Se acordó con el cliente la lista de números a contactar y el alcance del ejercicio (no solicitar ni información sensible más allá de los campos definidos). Se validó el texto final del SMS y la maquetación del formulario para que reflejara identidad corporativa sin inducir a transacciones o cambios de seguridad.

Fase 2. Implementación técnica.

Se preparó el portal con los formularios y campos obligatorios y mensajes de confirmación neutros. Se configuró el enlace para ser incluido en el SMS. No se activaron funciones analíticas avanzadas; se priorizó similitud visual y flujo simple.

Fase 3. Producción y despliegue.

No hubo despliegue físico. El canal fue 100% SMS. Se enviaron 80 mensajes a la población definida, manteniendo horarios laborales y cuidando el remitente (texto simple, encabezado “Beneficios Colsubsidio”) para maximizar la lectura y minimizar sospechas por estilo.

Fase 4. Operación, monitoreo y cierre.

Se monitoreó exclusivamente el diligenciamiento de los formularios (datos enviados). Dado que era nuestra única manera de tomar métricas, la conversión efectiva se midió por datos registrados. Al cierre, se consolidaron resultados y se resguardó la información para tratamiento por el cliente (concienciación y acciones internas). No se reutilizaron los datos.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

28 / 47

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

10.5 Resultados obtenidos

Duración de la actividad: 22–23 de octubre 2025

Cálculos clave:

- Mensajes enviados: 40
- Formularios con datos recibidos: 2
- Tasa de conversión sobre enviados: $2/40 = 5\%$

Evitar falsa seguridad por porcentaje: aunque 5% parezca bajo, cada registro habilita ataques posteriores mejor orientados. Con persistencia, refuerzos de narrativa o incentivos, un actor malicioso podría escalar la tasa o usar esta base como semilla para campañas multicanal (correo/WhatsApp/llamadas).

Tabla de síntesis

Métrica	Valor
Ventana de campaña	22-23/10/2025
Canal	SMS (smishing)
Guion elegido	Beneficios Colsubsidio
Mensajes enviados	40
Formularios recibidos	2
Conversión (sobre enviados)	5%
Analítica de clics	No disponible (Únicamente datos capturados)
Datos solicitados	Número de Documento y Contraseña, contraseña anterior y contraseña nueva
Límites éticos	Datos financieros; recolección mínima; resguardo

Tabla 7. Síntesis Smishing

10.6 Evidencias



Ilustración 20. Mensaje de prueba

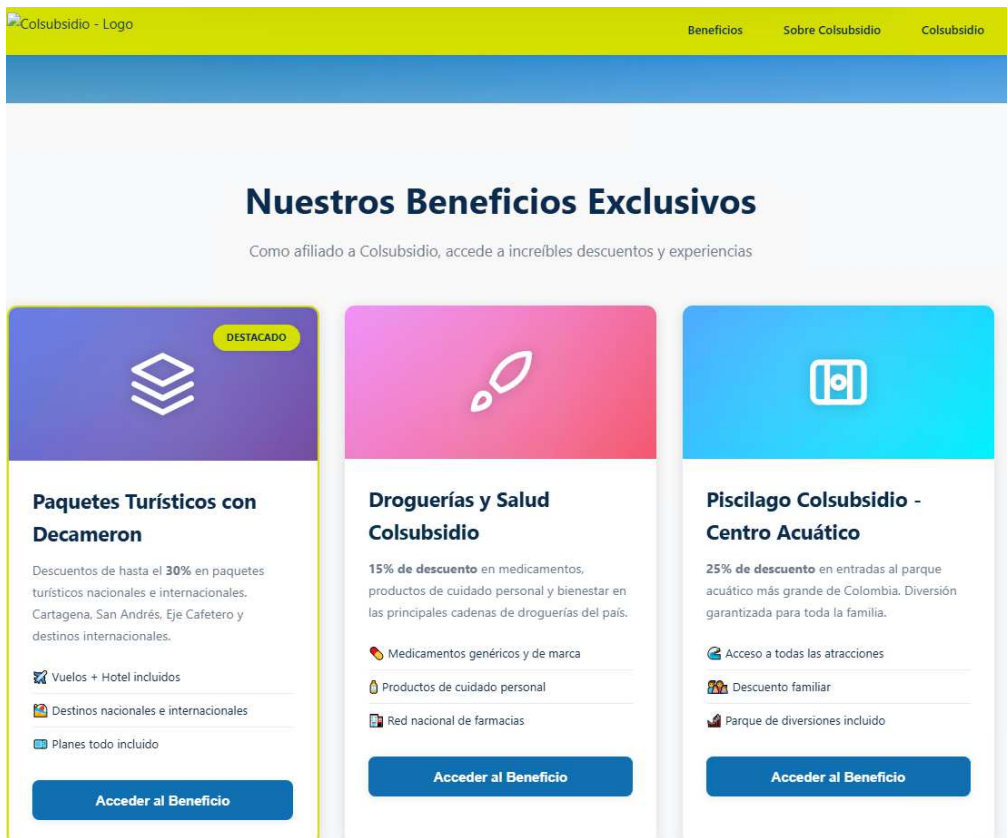


Ilustración 21. Portal falso de beneficios.

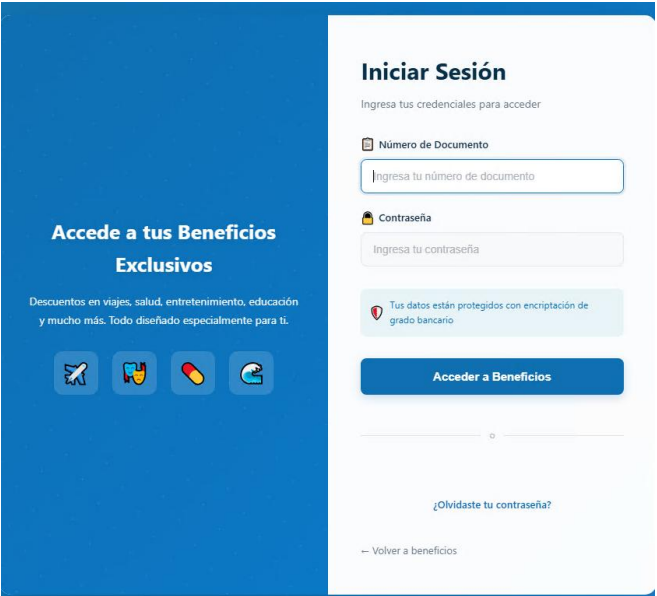


Ilustración 22. Formulario de acceso



Ilustración 23. Formulario 2 – recuperación de contraseña

Datos registrados

```
recuperacion.txt - Notepad
File Edit Format View Help
documento: 1030
password_old: 
password_new: 
password_confirm: 

documento: 1019
password_old: R
password_new: T
password_confirm: 

documento: 1019
password_old: R
password_new: S
password_confirm: 

documento: 10
password: Roc
documento: 10
password: 99L
documento: 10
password: pru
documento: 10
password: pru

documento: 1016
password_old: 9
password_new: q
password_confirm: 

documento: 1016
password_old: 9
password_new: q
password_confirm: 
```

Ilustración 24. Datos registrados

10.7 Recomendaciones

- No abras enlaces a formularios o encuestas si llegan por un SMS no solicitado.

- No completar formularios con datos personales si estos fueron remitidos por enlaces SMS.
- Realizar la confirmación a través de canales oficiales, consultar al área encargada sobre el contenido del SMS recibido.
- Reportar y eliminar, reenviar el mensaje al área encargada de la seguridad y eliminarlo para evitar accesos por error.

11 Phishing

11.1 Objetivo

Las pruebas de phishing consisten en simulaciones controladas para evaluar la capacidad de sus empleados para reconocer y reaccionar ante intentos de fraude a través de correos electrónicos o mensajes. En esta el atacante busca emular comunicaciones internas o campañas que atraigan la atención de las víctimas, con el objetivo de que estos entreguen información sensible, además estos son enviados desde un dominio que aparenta ser de confianza.

11.2 Impacto

Robo de identidad, la información obtenida a través de phishing puede ser utilizada para suplantar la identidad de una persona, además podría permitir la exfiltración de información, si se logran obtener credenciales de acceso, un atacante podría utilizarlas para obtener información confidencial, en consecuencia, la organización puede perder tiempo y recursos en la gestión de incidentes de seguridad, afectando su operatividad.

11.3 Phishing 1 - Propuesta

Propuesta elegida y justificación.

Se optó por utilizar el señuelo “**Aviso de expiración de contraseña**” debido a su alta verosimilitud y efectividad en contextos corporativos. Este tipo de mensajes es habitual en las organizaciones, ya que busca generar en el usuario la sensación de urgencia y la obligación de actualizar sus credenciales para mantener el acceso a los sistemas internos. El incentivo principal la posible expiración de la contraseña induce un estado de alerta, pues el usuario percibe que, de no actuar de inmediato, podría perder acceso a las aplicaciones y recursos esenciales para su trabajo diario. Esta estrategia resulta especialmente eficaz para evaluar la respuesta ante correos con apariencia legítima y un alto nivel de presión temporal.

Diseño de plantillas y decisiones clave.

- Dominio y subdominio similar: se registró el dominio fna-qov.co por su cercanía fonética/visual al dominio real y el subdominio verify.fna-qov.co.
Remitente/buzón (Microsoft 365) para mayor legitimidad:
verify@fna-qov.co.
- Correo: identidad visual de FNA (colores, logo, firma institucional), tono formal.
- Landing (login similar): clon de aplicación Verify (Autogestión de Usuarios) para disparar confianza del formulario.
- TLS/HTTPS: certificado válido para el dominio similar (icono de candado) como señal de “sitio seguro”.
- XAMP: plataforma de orquestación del portal público instalado en el servidor de comando y control (recolección de datos).

11.4 Phishing 1 - Desarrollo del escenario

Fase 1. Preparación y permisos.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

33 / 47

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

Se obtuvo aprobación del cliente para usar dominio muy similar al oficial, de igual manera se clonó el formulario de login de la aplicación Verify de IBM y se crearon buzones Microsoft 365 desde donde se envían los correos. Se definió el alcance ético, el periodo de envíos y las métricas a recolectar. Se acordaron pruebas de envío con los sistemas de acceso del cliente para minimizar bloqueos.

Fase 2. Implementación técnica.

Se adquirió y configuró el dominio fna-qov.co con TLS y subdominios necesarios; se clonó el formulario de Verify IBM (fuente: imágenes desde internet) y se desarrolló el formulario de login. Se creó el buzón en Microsoft 365 para firmar y distribuir envíos, evitando patrones que gatillen detecciones antispam. Se creó una plantilla de correo con el asunto, cuerpo y enlace adjunto.

Fase 3. Producción y despliegue físico.

No hubo material físico. El canal fue exclusivamente correo electrónico. Se realizaron pruebas de envío (cliente + equipo) para validar: plantilla del correo, resolución del dominio, certificado TLS, flujos de clic → login Verify → y registro de eventos en el servidor de comando y control.

Fase 4. Operación, monitoreo y cierre.

Se lanzó la campaña, se monitorearon métricas en tiempo real y se aplicaron pequeños ajustes de remitentes para sostener la entregabilidad. Al cierre, se consolidaron eventos únicos y la actividad por hora, se resguardaron datos y se preparó el reporte ejecutivo.

11.5 Phishing 1 - Resultados obtenidos

Ventana de actividad: 27 –29 de octubre de 2025

Población objetivo (enviados únicos): 250

- **Métricas principales (sobre enviados únicos)**
- **Aperturas:** 80 → **32%**
- **Clics en enlace:** 52 → **20,8%**
- **Envíos de datos:** 16 → **7,11%**
- **No abrieron:** 170 → **68%**
- **No hicieron clic:** 198 → **79,2%**
- **No enviaron datos:** 234 → **93,6%**
- **Mensajes Respondidos:** 0 → **0%**
- **Usuarios Reincidentes:** 10 → **4%**

Tabla de síntesis

Métrica	Valor
Ventana de campaña	27–29/10/2025
Enviados (únicos)	250
Aperturas	80 (32%)
Clics / “Escaneos únicos”	52 (20,8%)
Envíos de datos	16 (7,11%)
Dominio lookalike	fna-qov.co (con TLS)
Landings	Formulario login Verify IBM

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

34 / 47

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

Buzones M365 usados	verify@fna-qov.co
---------------------	-------------------

Tabla 8. Síntesis Phishing 1

11.6 Evidencias

A continuación, se muestra, lo desarrollos realizados para llevar a cabo la primera actividad de phishing 1.

SERVICIO DE NOTIFICACIÓN AUTOGESTIÓN DE USUARIOS VERIFY

EXPIRACIÓN DE CONTRASEÑA

Señor(a) usuario(a)

Se informa que su contraseña caducará en **1 día**, es necesario que realice el cambio de contraseña a través del módulo de [Autogestión de usuarios](#).

Para acceder al portal de autogestión de usuarios, de clic [AQUÍ](#).

Cordialmente,

Este es un correo de notificación automática, por favor no responda este mensaje.

Ilustración 25. Plantilla desarrollada.

Se procede a clonar el portal centralizado para las autenticaciones corporativas, el portal en mención es Verify, en este portal se aplican ciertos ajustes para guardar todos los datos ingresados, y ser utilizados posteriormente.



Security Verify Governance
Identity Manager

ID de usuario

Contraseña

Iniciar sesión

[¿Ha olvidado su contraseña?](#) | [Necesita ayuda?](#)

Español - Español

Inicie la sesión en Identity Manager Service Center para llevar a cabo las actividades siguientes:

Gestionar acceso

Gestionar actividades

Ver solicitudes

Gestionar perfiles

Más información

Ilustración 26. Login desarrollado

La siguiente imagen podemos observar la cantidad de correos enviados, de igual manera la cantidad de personas que abrieron el correo y el total de personas que dieron clic en la plantilla desarrollada, finalmente podemos observar la cantidad de personas que llenaron el formulario, en donde se les solicitaba hasta subir la hoja de vida, si deseaban participar en los ascensos disponibles en la compañía.

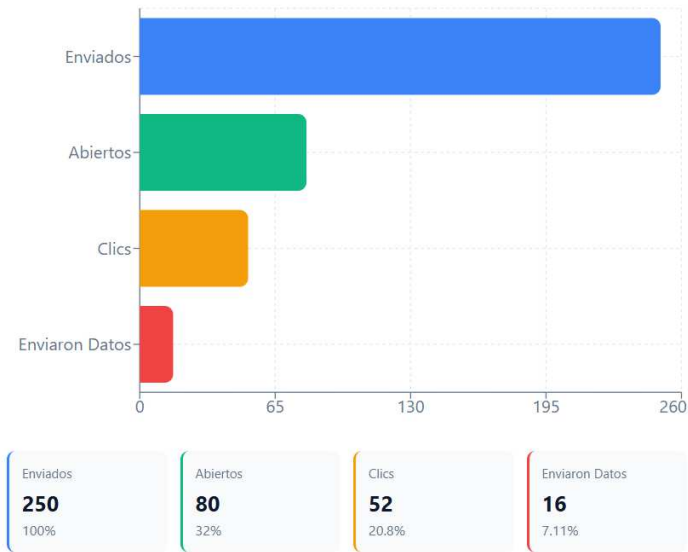


Ilustración 27. Estadísticas de los correos.

Aquí se ve de manera grafica la distribución de aperturas frente al primer phishing.

 Distribución de Aperturas

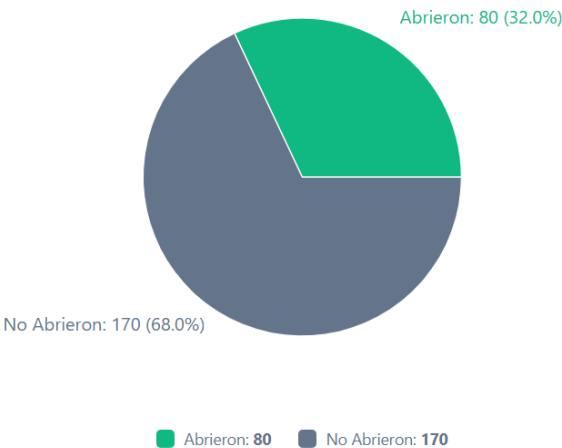


Ilustración 28. Distribución de Aperturas.



Ilustración 29. Top de usuarios con más envíos de información.

11.7 Phishing 2 - Propuesta

Propuesta elegida y justificación.

Se seleccionó la propuesta “Recordatorio de vencimiento de credenciales” por su alto nivel de realismo y coherencia con las comunicaciones internas habituales en entornos corporativos. Este tipo de mensaje replica con precisión los avisos legítimos que notifican la expiración de contraseñas, lo que incrementa su credibilidad. Además, el componente emocional asociado al temor de perder el acceso a las cuentas o afectar la continuidad laboral actúa como un detonante psicológico que incentiva al usuario a abrir el mensaje y hacer clic en el enlace. Esta dinámica permite evaluar de manera más precisa el nivel de conciencia y reacción del usuario ante un escenario verosímil de ingeniería social, observando si logra identificar la falsedad del mensaje o si avanza hasta la entrega de información sensible.

Diseño de plantillas y decisiones clave.

- Dominio y subdominio: se utilizó el dominio similar al original y se creó un subdominio aprende.fna-qov.co (nota: en la lista de buzones aparece “seguridadti@fna-qov.co”; teniendo en cuenta que la forma original es fna.gov.co).
- Correo: logos y colores de FNA; detalle de hora/país inusual; pie de página “Equipo de Educación Virtual — FNA”.
- Landing clonado: portal con estilos corporativos para maximizar familiaridad y reducir fricción cognitiva antes de la captura.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

37 / 47

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

- Infra & Recolección de datos: TLS/HTTPS, buzones M365 para remitentes, y plataforma Xampp: (plataforma de orquestación del portal público instalado en el servidor de comando y control (recolección de datos).

11.8 Phishing 2 - Desarrollo del escenario

Fase 1. Preparación y permisos.

Aprobación del cliente para usar subdominio de seguridadti, plantilla con alarma de vencimiento de credenciales, y clon visual de portal. Se definieron límites (sin coerción, sin solicitar datos financieros) y se hicieron pruebas de entregabilidad.

Fase 2. Implementación técnica.

Se creó el subdominio seguridadti@fna-qov.co con certificado https, se cargó la plantilla de correo y la *landing* clonada, y se configuraron buzones de Microsoft 365 para envío.

Fase 3. Producción y despliegue físico.

Se preparó el lote de 250 destinatarios. El canal fue exclusivamente correo electrónico. Se realizaron pruebas de envío (cliente + equipo) para validar: plantilla del correo, resolución del dominio, certificado TLS, flujos de clic → login portal educativo aprende → y registro de eventos en el servidor de comando y control.

Fase 4. Operación, monitoreo y cierre.

Se lanzó la campaña con segundo lote, se monitorearon métricas en tiempo real y se aplicaron pequeños ajustes de remitentes para sostener la entregabilidad. Al cierre, se consolidaron eventos únicos y la actividad por hora, se resguardaron datos y se preparó el reporte ejecutivo.

11.9 Phishing 2 - Resultados obtenidos

Ventana de actividad: 27 –29 de octubre de 2025

Enviados totales: 250

- Métricas principales (sobre enviados únicos)
- Aperturas: 100 → 40%
- Clics en enlace: 76 → 30,4%
- Envíos de datos: 37 → 14,8%
- No abrieron: 150 → 60%
- No hicieron clic: 174 → 69,6%
- No enviaron datos: 213 → 85,2%
- Mensajes Respondidos: 2 → 0,8%

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

38 / 47

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

Métrica	Valor
Ventana de campaña	27/10 – 29/10/2025
Enviados totales	250
Aperturas	100 (40%)
Clics / “Escaneos únicos”	76 (30,4%)
Envíos de datos	37 (14,8%)
Buzones remitentes	seguridadti
Subdominio	seguridadti.fna-qov.co
TLS/HTTPS	Sí

Tabla 9. Síntesis Phishing 2

11.10 Evidencias

PORTAL DE EDUCACIÓN VIRTUAL — FONDO NACIONAL DEL AHORRO

RECORDATORIO DE VENCIMIENTO DE CREDENCIALES

Te informamos que tu contraseña del **Portal de Educación Virtual del FNA** caducará en **1 día** día(s). Para mantener el acceso a tus cursos y certificaciones, te invitamos a actualizarla cuanto antes.

Ir al Portal de Educación Virtual

¿Olvidaste tu contraseña?

Restabícela desde [este enlace seguro](#).

Si no realizas el cambio a tiempo, por seguridad tu acceso podría quedar temporalmente bloqueado hasta completar el restablecimiento.

Cordialmente,

Equipo de Educación Virtual — FNA

Este es un correo automático, por favor no respondas a este mensaje. ¿Necesitas ayuda? Contáctanos: [Mesa de ayuda](#).

Ilustración 30. Plantilla diseñada para el phishing 2

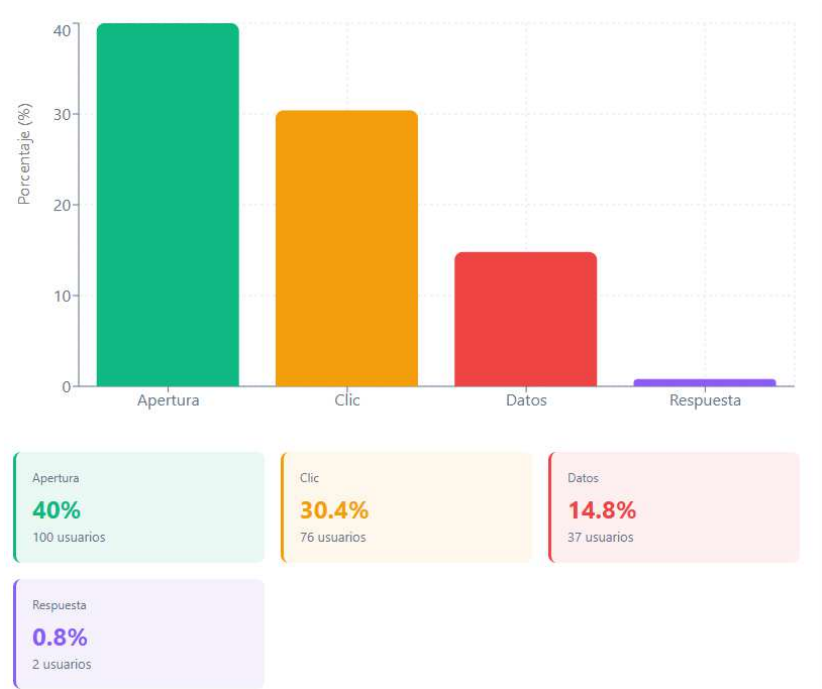


Ilustración 31. Estadísticas de correos abiertos, clic, envío de información y respuestas.

● Distribución: Únicos vs Reincidentes

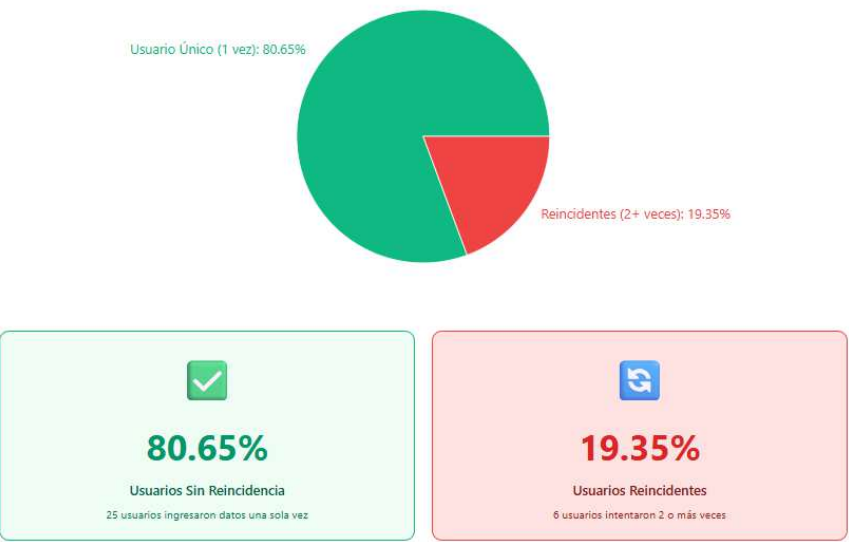


Ilustración 32. Distribución usuarios únicos vs reincidentes.



Ilustración 33. Evidencia de información capturada.

Número	Categoría	Fecha de entrega	Prioridad	Estado	Título
RF452060	Escritorio	27/10/2025 18:104 -	Baja	Closed	VERIFICACIÓN DE CORREO
RF452061	Escritorio	27/10/2025 18:124 -	Baja	Closed	VERIFICACIÓN DE CORREO
RF452094	Escritorio	28/10/2025 9:294 -	Baja	Closed	CONFIRMACIÓN DE CORREO
RF452098	Escritorio	28/10/2025 9:344 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452102	Escritorio	28/10/2025 9:384 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452105	Escritorio	28/10/2025 9:424 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452106	Escritorio	28/10/2025 9:444 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452108	Escritorio	28/10/2025 9:524 -	Baja	Closed	CORREO SOSPECHOSO
RF452111	Escritorio	28/10/2025 9:564 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452113	Escritorio	28/10/2025 10:004 -	Baja	Closed	RECORDATORIO VENCIMIENTO DE CREDENCIALES
RF452270	Escritorio	28/10/2025 16:164 -	Baja	Closed	VERIFICACIÓN DE CORREO
RF453018	Escritorio	4/11/2025 14:104 -	Baja	Closed	CORREO FRAUDULENTO. - INSTRUCCIONES PARA ACCEDER A TU BONO - KTRONIX
RF453070	Escritorio	4/11/2025 16:134 -	Baja	Closed	CORREO SOSPECHOSO

Ilustración 34. Evidencia casos creados por los usuarios.

11.11 Recomendaciones

- Revisar URL, dominio y subdominio letra por letra (sin lookalikes). No usar acortadores ni dominios “gemelos”.
- Las alertas reales no solicitan el cambio de contraseña a través de un enlace de correo electrónico, lo mejor es ir directamente al portal oficial.
- Realizar la revisión del remitente, expandirla en caso de ser necesario, verificar el correo completo, (dominio exacto, no parecido). Sospechar si falla SPF/DKIM o si responde a un buzón externo.
- Los correos con mensajes de urgencia, amenazas de bloqueo o pérdida de cuenta, incentivos suelen estar asociados a fraudes, por lo que se debe prestar especial atención a estos.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

41 / 47

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

- En caso de duda, consultar con el personal encargado usando los canales oficiales.

12 Conclusiones

- **Phishing 1 (Aviso de expiración de contraseña)** — El ejercicio evidenció un **nivel medio de susceptibilidad** ante correos con apariencia institucional y mensajes asociados a la **gestión de contraseñas**. Aunque el porcentaje de aperturas (32 %) indica curiosidad moderada, el **20,8 % de clics en el enlace** demuestra que una parte significativa de los usuarios aún confía en notificaciones aparentemente legítimas, sobre todo cuando implican urgencia o pérdida de acceso. La tasa reducida de **envío de datos (7,11 %)** refleja un grado básico de precaución en los usuarios, sin embargo, el resultado confirma la **necesidad de reforzar las campañas de concientización** enfocadas en identificar correos de expiración falsos y verificar siempre las fuentes antes de interactuar.
- **Phishing 2 (Recordatorio de vencimiento de credenciales)** — El segundo ejercicio obtuvo un **mayor nivel de interacción**, con **40 % de aperturas y 30,4 % de clics**, lo que demuestra que los mensajes con **alto realismo y tono corporativo coherente** generan una percepción de legitimidad aún más fuerte entre los usuarios.
El incremento en el **envío de datos (14,8 %)** evidencia que el componente emocional de pérdida de acceso es altamente efectivo para inducir acción inmediata, incluso sin verificar autenticidad. Estos resultados permiten concluir que los empleados son **más vulnerables a mensajes que imitan comunicaciones internas reales**, por lo que se recomienda **reforzar las capacitaciones en ingeniería social**, implementar **alertas visuales en el correo corporativo**, y fomentar la **cultura de reporte inmediato** ante mensajes sospechosos.
- **Smishing (Cambio de contraseña obligatorio Verify)** — El ejercicio de smishing demostró que los mensajes con **temáticas de beneficios personales y convenios corporativos** continúan siendo altamente efectivos para captar la atención de los usuarios, principalmente por su tono positivo, bajo nivel de fricción y apariencia de legitimidad.

Aunque el número de envíos fue reducido (40 mensajes), la obtención de **2 formularios con datos diligenciados (5%)** confirma que una fracción de los participantes respondió de manera impulsiva ante estímulos de tipo **“beneficio o recompensa”**, sin validar la autenticidad del remitente o el dominio del enlace.
Estos resultados reflejan una **tendencia de vulnerabilidad emocional**, en la que el deseo de obtener ventajas inmediatas supera la verificación racional del mensaje. Por tanto, se recomienda reforzar la **concientización sobre el smishing** mediante talleres prácticos y simulaciones periódicas, destacando la importancia de **no interactuar con enlaces recibidos por SMS o mensajería instantánea**, y de validar toda comunicación institucional a través de los canales oficiales del Fondo Nacional del Ahorro o de Colsubsidio.
- **Vishing (Beneficio Colsubsidio–Cafam–Ktronix)** — El ejercicio de vishing permitió evidenciar la eficacia de los ataques de ingeniería social basados en comunicación directa y tono institucional, especialmente cuando el mensaje simula provenir de un aliado o programa de beneficios corporativos. De los contactos realizados, el **25 % respondió la llamada**, y dentro de este grupo, la **mitad (50 %) accedió**

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

43 / 47

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

a **compartir información personal básica**, lo que representa una **tasa de éxito general del 12,5 %** sobre el total de intentos.

Estos resultados demuestran que **la interacción verbal incrementa el nivel de confianza del usuario**, reduciendo su percepción de riesgo y aumentando la probabilidad de divulgación de datos, aun cuando se evita cualquier presión explícita o solicitud de credenciales.

El ejercicio reafirma la necesidad de **reforzar la capacitación del personal frente a intentos de suplantación telefónica**, promoviendo el uso de **protocolos de verificación de identidad**, la **denuncia inmediata de llamadas sospechosas** y la **desconfianza ante beneficios o premios no solicitados**.

- **Rogue AP (SSID WLAN_CORP)** — Una contraseña capturada no es un número pequeño, es una brecha abierta: La captura de una credencial, aunque única, habilita el acceso a la red Wi-Fi, enumeración interna y posibles pivotes hacia Azure/Entra u otros servicios. Este ejercicio demuestra que el riesgo se mide por impacto, no solo por porcentaje. La remediación prioritaria es migrar a EAP-TLS (certificados de dispositivo), desplegar WIDS/WIPS para detectar AP falsos y comunicar de forma recurrente el listado oficial de SSIDs junto con la política de conexión segura.
- **Quishing (QR en zonas comunes)** — El ejercicio de Qhishing evidenció que los mensajes que involucran **beneficios tangibles y de fácil acceso, especialmente cuando se asocian a aliados institucionales reconocidos como Colsubsidio**, resultan altamente atractivos para los usuarios. A pesar del número limitado de escaneos (4 durante la jornada del 29 de octubre), el hecho de que se registraran interacciones demuestra que la **inserción de códigos QR en espacios físicos** (como carteles o monitores internos) constituye un vector viable de ingeniería social en entornos laborales.
- **Acceso físico (Sede Principal)** — El ejercicio de ingreso físico permitió comprobar que los **controles de verificación visual y de acompañamiento a visitantes** continúan representando un punto crítico en la seguridad perimetral. Durante la simulación se realizaron dos intentos de acceso, de los cuales **uno resultó exitoso (50 % de efectividad)** mediante la combinación de **pretexting, mimetización y tailgating**, evidenciando que el **factor humano** puede ser explotado para evadir protocolos físicos incluso en presencia de procedimientos establecidos. El ingreso logrado se basó en la **presión contextual y la aparente formalidad del pretexto**, lo cual generó una respuesta de confianza por parte del personal de recepción.

Aunque no se logró la recolección de evidencia sensible gracias a la existencia de **controles biométricos en áreas internas**, el ejercicio demuestra la **necesidad de fortalecer la cultura de verificación de identidad**, estandarizar los **procedimientos de validación de carnés y acompañamiento de visitantes**, e incorporar **entrenamientos prácticos para el personal de seguridad y recepción** orientados a detectar tácticas de suplantación o manipulación psicológica.

13 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.
<i>Risk</i>	Sistema de puntuación propio de Mnemo basado en estándares oficiales, como CVSS, para medir el riesgo que tiene una vulnerabilidad detectada para una entidad.

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

Documento: FNA-002-Informe_Ingeniería_Social_v1.0

Fecha: 24 Sept 2025

45 / 47

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

<i>Ingeniería social</i>	Conjunto de técnicas que se enfocan en personas y procesos para influenciar decisiones y conductas (confianza, urgencia, autoridad, curiosidad) con el fin de obtener información, acceso o acciones que favorezcan al atacante.
<i>Pretexting (pretexto)</i>	Construcción de una historia creíble (rol, contexto, evento) para legitimar una solicitud o presencia.
<i>Impersonation (suplantación)</i>	Hacerse pasar por una persona/rol (directivo, soporte, proveedor) mediante señales de identidad (voz, apariencia, correo, foto, firma).
<i>Phishing (email)</i>	Engaño por correo con enlaces/adjuntos a sitios o cargas maliciosas para capturar credenciales/datos o desplegar <i>malware</i> .
<i>Smishing (SMS)</i>	Phishing por mensaje de texto con enlace/CTA a formularios o sitios no oficiales.
<i>Vishing (voz/llamada)</i>	Llamadas con pretextos (beneficios, soporte, seguridad) para obtener datos o inducir acciones.
<i>Whishing (WhatsApp)</i>	Phishing por mensajería instantánea (texto, audio, voz clonada) desde números/identidades verosímiles.
<i>Quishing (QR phishing)</i>	Uso de códigos QR que llevan a dominios <i>lookalike</i> para captura de datos o descarga de apps.
<i>Rogue AP (punto de acceso falso)</i>	Red Wi-Fi que imita a la corporativa; suele usar portal cautivo para robar credenciales o forzar sesiones inseguras.
<i>Acceso físico / Tailgating / Piggybacking</i>	Intrusión presencial por seguimiento a personal autorizado o aprovechando picos de flujo y validaciones laxas.

Tabla 10 - Conceptos y definiciones

13.1 Usuarios comprometidos con credencial en texto plano

Usuarios víctimas	Ingeniería social
16	Phishing 1 - Aviso de expiración de contraseña
37	Phishing 2 - Recordatorio de vencimiento de credenciales
1	Vishing - Beneficio Colsubsidio-Cafam-Ktronix
2	Smishing - Beneficios Colsubsidio
3	Rogue AP - SSID "WLAN_CORP"
4	Quishing (QR phishing)
-	Acceso físico (intrusión en sede; no aplica conteo de "usuarios")

Tabla 11. Cantidad de usuarios que cayeron en las ingenierías sociales

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

Acta N°	137 MNCO-SIG-25-0859	Tema:	Socialización de informe de ejercicio de ingeniería social para el año 2025	
Fecha:	24/11/2025	Ubicación:	Virtual	
Hora inicio:	11:00 am	Hora fin:	12:00 pm	
Objetivo		Presentar el avance de la estructuración y operación de la unidad de ciberseguridad e identificar las barreras que actualmente se presentan en el proyecto a corte del 21/11/2025.		
PARTICIPANTES CONVOCADOS A LA REUNIÓN				
Nombre completo		Dependencia	Cargo	¿Asistió?
Leivi Dayana Cortes		Gerencia de seguridad de la información FNA	Gerente de seguridad de la información FNA	Si
Juan Carlos Martinez		Gerencia de seguridad de la información FNA	Profesional 4	Si
Enrique Arrazola		Gerencia de ciberseguridad y aseguramiento informático FNA	Profesional 3	Si
Cristian Samir Acosta		Gerencia de ciberseguridad y aseguramiento informático FNA	Analista de gestión	Si
Andres Tamayo		Consortio unidad de ciberseguridad FNA	Auditor tecnico	Si
Cesar Orlando Pinto		Consortio unidad de ciberseguridad FNA	Gerente de proyecto	Si

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

Se inicia la reunión mencionando el objetivo principal de la reunión y del ejercicio de ingeniería social ejecutado por consorcio unidad de ciberseguridad.

- Objetivo reunión: Socializar los resultados del ejercicio de ingeniería social, para que se tomen las medidas y remediaciones por parte de FNA.

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

- Objetivo ejercicio: Evaluar, bajo autorización y en entorno controlado, la exposición de FNA frente a técnicas de ingeniería social con el fin de medir la susceptibilidad humana, validar la efectividad de los controles organizacionales (tecnológicos y procedimentales) y determinar el

Dentro del ejercicio de ingeniería social se realizaron los escenarios de:

Ing. Físicas:

- Intrusión Física
- Quishing
- Rogue AP

Ing. Virtual

- Vishing
- Smishing
- Phishing

DESARROLLO

Descrito en presentación anexa que se enviara a FNA una vez finalizada la sesión como informe ejecutivo y entregable del ejercicio de ingeniería social

Recomendaciones:

- Capacitación continua con simulaciones reales
- Canales “oficiales”visibles y bloqueos preventivos
- MFA Obligatorio
- Verificación múltiple

2. RESUMEN DE LOS ACUERDOS (Registrar claramente los acuerdos de la reunión)

- Se acuerda enviar el anexo con el detalle de los usuarios que cayeron en las diferentes metodologías y escenarios del ejercicio de ingeniería social

3. COMPROMISOS PACTADOS

DESCRIPCIÓN	RESPONSABLE (s)	FECHA PROPUESTA PARA LA EJECUCIÓN DEL COMPROMISO
Envío de anexo con el detalle de datos y usuarios que cayeron en los ejercicios	Consortio unidad de ciberseguridad	27/11/2025

	FORMATO ACTA DE REUNIÓN	Código GE-GP-FO-001
	GESTION DE PROCESOS Y CALIDAD	Versión: 1

APROBÓ	APROBÓ
 Cesar Orlando Pinto Gerente de Proyecto Consortio unidad de ciberseguridad FNA	 Cristian Samir Analista de gestión Gerencia de ciberseguridad y aseguramiento informático FNA
 Fabio Andres Tamayo Auditor Tecnico Consortio unidad de ciberseguridad FNA	 Leivi Dayana Cortes Gerente de seguridad de la información Gerencia de seguridad de la información FNA
 Juan Carlos Martinez Profesional 4 Gerencia de seguridad de la información FNA	



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

PRE FACTURA
No. C-2-49

Para :	Fondo Nacional de Ahorro SA
Nit :	899.999.284-4
Fecha :	2025-12-02

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	Analisis de vulnerabilidades por demanda- Ethical Hacking por demanda	1.00	205,082,000.00	244,047,580.00	0.00
2	Ingeniería Social	1.00	24,307,289.92	28,925,675.00	0.00

Total Bruto	229,389,290.00
Subtotal	229,389,290.00
IVA 19%	43,583,965.00
Total a Pagar	272,973,255.00

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

Valor en Letras: Doscientos setenta y dos mil novecientos setenta y tres mil doscientos veinticinco pesos mcte

Distribucción de ingreso:
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 **5 de noviembre del 2025**.

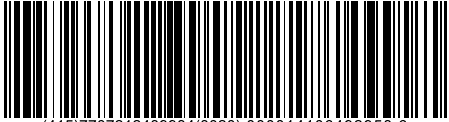
Para trámites de nómina, legales, internacionales y otros, también puedes usar las siguientes opciones de números de cuenta:

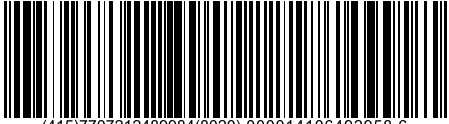
Cuenta de 10 dígitos:**0136002901**

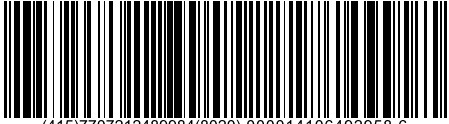
Cuenta de 16 dígitos:**0136000200002901**

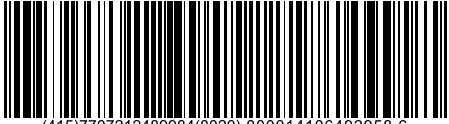
Cuenta de 20 dígitos:**00130136000200002901**

Firma autorizada
BBVA Colombia

DIAN		Formulario del Registro Único Tributario				001	
2. Concepto 02 Actualización				4. Número de formulario 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	
IDENTIFICACIÓN							
24. Tipo de contribuyente		25. Tipo de documento		26. Número de Identificación			
Persona jurídica		1					
Lugar de expedición		28. País		29. Departamento		30. Ciudad/Municipio	
31. Primer apellido		32. Segundo apellido		33. Primer nombre		34. Otros nombres	
35. Razón social							
MNEMO CYBER SEC S.A.S							
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 NO 10 19 OF 502							
42. Correo electrónico j.parra@mnemo.com							
43. Código postal		44. Teléfono 1		45. Teléfono 2			
1 1 0 1 1 1		6 9 1 3 1 3 3					
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 0, 1 2, 2 9		6 2 0 2		2 0 2 0, 1 2, 2 9	
Responsabilidades, Calidades y Atributos							
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26							
53. Código 5 7 1 4 4 2 4 8 5 2 5 5							
05- Impto. renta y compl. régimen ordinar							
07- Retención en la fuente a título de rent							
14- Informante de exogena							
42- Obligado a llevar contabilidad							
48 - Impuesto sobre las ventas - IVA							
52 - Facturador electrónico							
55 - Informante de Beneficiarios Finales							
Usuarios aduaneros				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.				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 141064929586		
 (415)7707212489984(8020) 000014106492958 6					
5. Número de Identificación Tributaria (NIT) 9 0 1 4 4 7 9 6 8 1		6. DV 1		12. Dirección seccional Impuestos de Bogotá	
		14. Buzón electrónico 3 2			
Características y formas de las organizaciones					
62. Naturaleza 2		63. Formas asociativas 1 2		64. Entidades o institutos de derecho público de orden nacional, departamental, municipal y descentralizados	
65. Fondos		66. Cooperativas		67. Sociedades y organismos extranjeros	
68. Sin personería jurídica		69. Otras organizaciones no clasificadas		70. Beneficio 1	
Constitución, Registro y Última Reforma			Composición del Capital		
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					
				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	
Contador	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. Concepto02Actualización

4. Número de formulario141064925838

5. Número de Identificación Tributaria (NIT)9003961761

6. DV1

12. Dirección seccionalImpuestos de Bogotá

14. Buzón electrónico32

IDENTIFICACIÓN

24. Tipo de contribuyentePersona jurídica1

25. Tipo de documento

26. Número de Identificación

Lugar de expedición28. País

29. Departamento

30. Ciudad/Municipio

31. Primer apellido

32. Segundo apellido

33. Primer nombre

34. Otros nombres

35. Razón socialMNEMO COLOMBIA SAS

36. Nombre comercial

37. Sigla

UBICACIÓN

38. PaísCOLOMBIA169

39. DepartamentoBogotá D.C.11

40. Ciudad/MunicipioBogotá, D.C.001

41. Dirección principalCL 99 10 19 OF 502

42. Correo electrónicorecepcion.colombia@mnemo.com

43. Código postal110111

44. Teléfono 13183835117

45. Teléfono 2575527210

CLASIFICACIÓN

Actividad económica

Ocupación

Actividad principal

Actividad secundaria

Otras actividades

51. Código

52. Número establecimientos

46. Código6201

47. Fecha inicio actividad20101112

48. Código6202

49. Fecha inicio actividad20101112

50. Código12098551

Responsabilidades, Calidades y Atributos

53. Código57910141819264142485255

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. Código23

55. Forma

56. Tipo

Servicio

1

2

3

57. Modo

58. CPC

59. AnexosSI NOX

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.

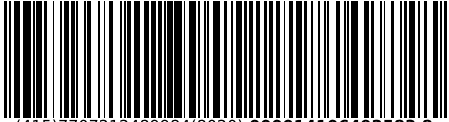
Sin perjuicio de las verificaciones que la DIAN realice.

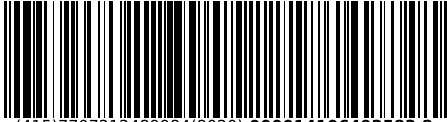
Firma autorizada:

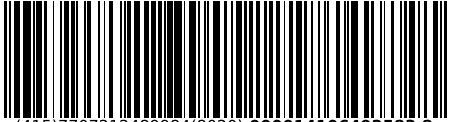
984. NombreVELEZ CASTRO HUMBERTO DE JESUS

985. CargoRepresentante Legal Suplente Certificado

Fecha generación documento PDF: 05-02-2025 05:39:39PM

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		
			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	
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					

DIAN		Formulario del Registro Único Tributario Representación				001	
Espacio reservado para la DIAN				Página 3 de 4 Hoja 3			
				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				99. Fecha inicio ejercicio representación 2 0 1 7 0 8 2 9			
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 7			
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 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		
Contador	140. Primer apellido		141. Segundo apellido		142. Primer nombre		143. Otros nombres
	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada		
	147. Fecha de nombramiento						
	148. Tipo de documento		149. Número de identificación		150. DV 151. Número de tarjeta profesional		
Contador	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6		2 3 2 3 2 5 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. Concepto02Actualización

4. Número de formulario141064931180

(415)7707212489984(8020)0000141064931180

5. Número de Identificación Tributaria (NIT)90130668726. DV212. Dirección seccionalImpuestos de Bogotá14. Buzón electrónico32

IDENTIFICACIÓN

24. Tipo de contribuyentePersona jurídica1

25. Tipo de documento

26. Número de Identificación

Lugar de expedición28. País

29. Departamento

30. Ciudad/Municipio

31. Primer apellido

32. Segundo apellido

33. Primer nombre

34. Otros nombres

35. Razón socialMNEMO EVOLUTION & INTEGRATION SERVICES S.A.

36. Nombre comercial

37. Sigla

UBICACIÓN

38. PaísCOLOMBIA169

39. DepartamentoBogotá D.C.11

40. Ciudad/MunicipioBogotá, D.C.001

41. Dirección principalCL 99 10 19 OF 502

42. Correo electrónicoJc.aponte@mnemo.com

43. Código postal110111

44. Teléfono 16913133

45. Teléfono 23103243475

CLASIFICACIÓN

Actividad económica

Actividad principal

46. Código47. Fecha inicio actividad

620120190702

Actividad secundaria

48. Código49. Fecha inicio actividad

620220190702

Otras actividades

50. Código12

6209

Ocupación

51. Código

52. Número establecimientos

Responsabilidades, Calidades y Atributos

53. Código5714424855

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

54. Código

11121314151617181920

Exportadores

55. Forma56. Tipo

Servicio123

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. AnexosSI[]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:

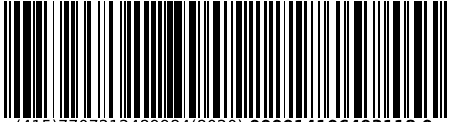
Sin perjuicio de las verificaciones que la DIAN realice.

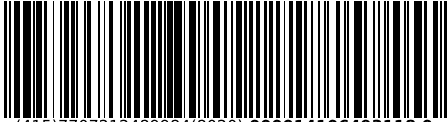
Firma autorizada:

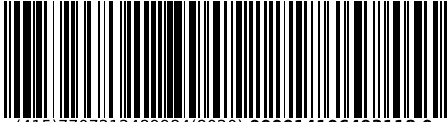
984. NombrePARRA GAMBOA JOHN JAIRO

985. CargoRepresentante legal Certificado

Fecha generación documento PDF: 05-02-2025 05:41:03PM

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 2		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					
72. Número					
73. Fecha 2 0 1 9 0 7 2 6					
74. Número de notaría 6 5					
75. Entidad de registro 0 3					
76. Fecha de registro 2 0 1 9 0 7 2 6					
77. No. Matrícula mercantil 0 0 0 3 1 4 4 6 0 3					
78. Departamento 1 1					
79. Ciudad/Municipio 0 0 1					
Vigencia					
80. Desde 2 0 1 9 0 7 2 6					
81. Hasta 9 9 9 9 1 2 3 1					
				82. Nacional 0 %	
				83. Nacional público 0 . 0 %	
				84. Nacional privado 0 . 0 %	
				85. Extranjero 1 0 0 %	
				86. Extranjero público 0 . 0 %	
				87. Extranjero privado 1 0 0 . 0 %	
Entidad de vigilancia y control					
88. Entidad de vigilancia y control					
Estado y Beneficio					
Item	89. Estado actual	90. Fecha cambio de estado	91. Número de Identificación Tributaria (NIT)	92. DV	
1	4 9	2 0 1 9 0 7 2 6		-	
2	8 1	2 0 1 9 0 7 2 6		-	
3				-	
4				-	
5				-	
Vinculación económica					
93. Vinculación económica	94. Nombre del grupo económico y/o empresarial			95. Número de Identificación Tributaria (NIT) de la Matriz o Controlante	
97. Nombre o razón social de la matriz o controlante				96. DV.	
170. Número de identificación tributaria otorgado en el exterior		171. País		172. Número de identificación tributaria sociedad o natural del exterior con EP	
173. Nombre o razón social de la sociedad o natural del exterior con EP					

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

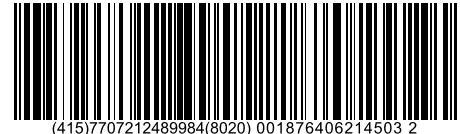
DIAN		Formulario del Registro Único Tributario Revisor Fiscal y Contador				001	
Espacio reservado para la DIAN				Página 4 de 4 Hoja 5			
				4. Número de formulario 141064931180			
 (415)7707212489984(8020) 000014106493118 0							
5. Número de Identificación Tributaria (NIT)		6. DV		12. Dirección seccional		14. Buzón electrónico	
9 0 1 3 0 6 6 8 7		2		Impuestos de Bogotá		3 2	
Revisor Fiscal y Contador							
Revisor fiscal principal	124. Tipo de documento		125. Número de identificación		126. DV 127. Número de tarjeta profesional		
	Cédula de Ciudadanía 1 3		8 7 7 0 4 4 6		6 1 0 6 1		
	128. Primer apellido		129. Segundo apellido		130. Primer nombre		131. Otros nombres
	VELEZ		CASTRO		HUMBERTO		DE JESUS
Revisor fiscal suplente	132. Número de Identificación Tributaria (NIT)		133. DV		134. Sociedad o firma designada		
	135. Fecha de nombramiento						
	2 0 2 1 0 2 1 5						
	136. Tipo de documento		137. Número de identificación		138. DV		139. Número de tarjeta profesional
Contador	140. Primer apellido		141. Segundo apellido		142. Primer nombre		143. Otros nombres
	144. Número de Identificación Tributaria (NIT)		145. DV		146. Sociedad o firma designada		
	147. Fecha de nombramiento						
	148. Tipo de documento		149. Número de identificación		150. DV		151. Número de tarjeta profesional
Contador	Cédula de Ciudadanía 1 3		1 0 1 8 4 0 8 8 7 6				2 3 2 3 2 5
	152. Primer apellido		153. Segundo apellido		154. Primer nombre		155. Otros nombres
	TOVAR		LOZANO		JAIRO		DAVID
	156. Número de Identificación Tributaria (NIT)		157. DV		158. Sociedad o firma designada		
159. Fecha de nombramiento							
2 0 2 1 0 6 0 1							

Espacio reservado para la DIAN



4. Número de formulario

18764062145032



(415)7707212489984(8020) 001876406214503 2

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

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

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

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

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

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

Firma del funcionario autorizado

Firma del solicitante



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

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

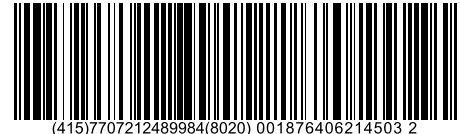
997. Fecha formalización 2 0 2 3 - 1 2 - 1 8 / 1 5 : 1 2 : 2 7

Espacio reservado para la DIAN



4. Número de formulario

18764062145032



(415)7707212489984(8020) 001876406214503 2

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

11. Razón social

CONSORCIO UNIDAD DE CIBERSEGURIDAD FNA

Rangos de numeración para autorizar, habilitar o inhabilitar

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



Bogotá, 02 de Diciembre de 2025

Señores

FONDO NACIONAL DEL AHORRO SA

Ciudad.

REF: CIRCULAR 042 DE 2012

Respetados señores:

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

Agradecemos la atención a la presente,

Cordialmente,

HUMBERTO DE JESUS VELEZ CASTRO
Representante legal
MNENO COLOMBIA SAS

División de Presupuesto

Documento de Pago

N° ORDEN DE PAGO	5300687874	FECHA DE CONTABILIZACIÓN	17.12.2025
N° DE REFERENCIA	55	FECHA DE PAGO	30.12.2025

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

PROVEEDOR	CONSORCIO UNIDAD DE CIBERSEGURIDAD	N° IDENTIFICACION	9017816251
BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE		
N° IDENTIFICACION	9017816251	TIPO DE IDENTIFICACION	NIT
FORMA DE PAGO	PAGO ELECTRÓNICO	CIUDAD	BOGOTÁ
N° DE CUENTA	0136002901	BANCO	BANCO BBVA
TIPO DE CUENTA	CUENTA DE AHORROS	INFORME N°	CTO 173-20
N° FACTURA PROVEEDOR	FE55 RAD 02-2303-202512181354132		

OBSERVACIONES:	FE55 RAD 02-2303-202512181354132.pl1009
----------------	---

INFORMACIÓN PRESUPUESTAL						
SOLPED	N° PEDIDO	POS	NÚMERO DE CONTRATO	LERF	RE-L	VALOR
20001368	6200000115	00010	CTO 173 DE 2023	1000055442	5105632112	272.973.255
AFECTACIÓN PEDIDO						272.973.255
DETALLE DE LA ORDEN DE PAGO						
VALOR TOTAL FAC.	272.973.255,00					
DESCUENTOS	33.986.318,00					
NOTAS CRÉDITOS	0,00					
VALOR A PAGAR	238.986.937,00					

Gerencia Tesorería

Documento de Pago

No. ORDEN DE PAGO	55	FECHA DE CONTABILIZACION	30-dic-25
No. DOCUMENTO DE PAGO	5300687874	FECHA DE DOCUMENTO	30-dic-25
		FECHA DE COMPENSACION	30-dic-25
PROPUESTA	56083	FECHA DE LA PROPUESTA	30-dic-25

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

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

BENEFICIARIO DEL PAGO			
NOMBRE COMPLETO	CONSORCIO UNIDAD DE CIBERSEGURIDAD		
No. IDENTIFICACIÓN	9017816251	TIPO DE IDENTIFICACIÓN	25
NOMBRE:	CONSORCIO UNIDAD DE		
OBSERVACIONES:	FE55 RAD 02-2303-202512181354132		
NÚMERO DE CUENTA	2511050101	TIPO DE CUENTA	CUENTA DE AHORROS
BANCO	BV02		
VIA DE PAGO	T		
VALOR NETO A CANCELAR	238.986.937		

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	5300687874	55	238.986.937	FE55 RAD 02-2303-202512181354132	6200000115	CTO 173 DE 2023