fna FONDO NACIONAL DEL AHORRO	**INFORME DE SEGUIMIENTO Y DE EVALUACIÓN CONTRACTUAL**	**Código: GLC-CONT-FO-016**
	PROCESO DE CONTRATACIÓN	**Versión: 2**

INFORME No 3 **FACTURA No**

No. DE ACEPTACIÓN: 1000061238

FECHA		
08	05	2026
dd	mm	aaaa

1. GENERALIDADES DEL CONTRATO

CONTRATO No 22 (Número de Contrato) **DE** 2026 (Año de suscripción) **TIPO DE CONTRATO** PRESTACION DE SERVICIO (Prestación de servicios, interventoría, consultoría, Convenio)

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

CONTRATISTA RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S. - GRUPO REINCAR S.A.S. (Escriba el nombre o razón social del contratista)

TIPO DE INTERVENTORÍA Y/O SUPERVISIÓN: **INDIVIDUAL** [X] **COLEGIADA** [ ]

INTERVENTOR Y/O SUPERVISOR (E) GABRIEL ERNESTO FUENTES AGUILAR (Escriba nombre del supervisor o interventor del contrato) — (Escriba nombre del supervisor o interventor del contrato)

APOYO SUPERVISIÓN JULLY ALEXANDRA GARCIA AGUDELO (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

Prestar los servicios de gestión y recuperación de la cartera del Fondo Nacional del Ahorro S.A., a nivel nacional, en las etapas preventiva y administrativa, incluyendo la cartera titularizada y la ejecución de campañas especiales de créditos.

DEPENDENCIA EJECUCIÓN CONTRATO GERENCIA DE COBRANZAS Y BRDPR (Indique el nombre de la dependencia responsable del contrato)

PLAZO DE EJECUCIÓN DEL CONTRATO 12 MESES (Indique en este espacio el número de días o de meses para ejecutar el contrato)

FECHA DE INICIACIÓN DEL CONTRATO 3 (Día) **DE** 2 (Mes) **DE** 2026 (Año)

FECHA DE TERMINACIÓN DEL CONTRATO 2 (Día) **DE** 2 (Mes) **DE** 2027 (Año)

REGISTRO PRESUPUESTAL No. **5400002203**

VALOR DEL CONTRATO

DOS MIL SEISCIENTOS MILLONES SETENTA Y SEIS MIL TRESCIENTOS OCHO PESOS M/CTE ($2.600.076.308), incluido el IVA y demás impuestos, tasas, gravámenes y contribuciones establecidos por las autoridades nacionales, departamentales, distritales o municipales, aplicables a los costos directos e indirectos generados con ocasión de la celebración, ejecución y/o liquidación del contrato.

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

PRÓRROGAS	
No.	**PLAZO**

ADICIONES		
No.	**VALOR**	**RP**

SUSPENSIONES		
No	**DESDE**	**HASTA**

2. INFORMACIÓN DE EJECUCIÓN PRESUPUESTAL

DESCRIPCIÓN	VALOR	PORCENTAJE
Valor Inicial del Contrato	$ 2,600,076,308	**100.0%**
Adiciones	$ -	**0.0%**
VALOR TOTAL DEL CONTRATO	**$ 2,600,076,308**	**100.0%**
Valor ejecutado antes del presente pago	$ 571,701,909	**22.0%**
Valor del pago aprobado con el presente informe	$ 390,889,933	**15.0%**
VALOR TOTAL EJECUTADO	**$ 962,591,842**	**37.0%**
Porcentaje de ejecución presupuestal programado a la fecha		
DIFERENCIA EN LA EJECUCIÓN PRESUPUESTAL DEL CONTRATO		**37.0%**

OBSERVACIONES

3. DESCRIPCION ACTIVIDADES

Porcentaje de ejecución de actividades proyectado a la fecha	**37.0%**
Porcentaje de ejecución de actividades realizado a la fecha	**37.0%**
DIFERENCIA EN LA EJECUCIÓN DE ACTIVIDADES DEL CONTRATO	**0.0%**

**Nota: Esta información es diligenciada únicamente 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

4. CONCEPTO SUPERVISOR O INTERVENTOR

Facturación reparto del mes de abril 2026; en los terminos estipulados en el objeto del presente contrato.

5. EVALUACIÓN CONTRATISTA (Escala de 0 - 5)

EVALUACIÓN PARCIAL	
Cumplimiento del contrato	**4**
Plazos	**5**
Aspectos administrativos	**5**

6. CERTIFICACIÓN PARA PAGO

EL SUSCRITO GERENTE DE COBRANZAS Y BRDPR (E) EN SU CONDICIÓN DE SUPERVISOR DEL CONTRATO No. 22 de 2026

CERTIFICA:

Que RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S. - GRUPO REINCAR S.A.S., identificado con NIT. No.900.405.236-5, entregó un informe de las actividades desarrolladas desde Bucaramanga - Santander en el período correspondiente a abril 2026, dando de esta manera cumplimiento a las obligaciones contenidas en el Contrato de prestacion de servicio No.22 de fecha 30 de enero de 2026.

7. CERTIFICACIÓN DE CUMPLIMIENTO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL

DIEGO ENRIQUE GONZALEZ RAMIREZ identificado con cédula de ciudadanía número 1.098.642.487 expedida en Bucaramanga actuando en calidad de Gerente General, y SANDRA MILENA CARRILLO BLANCO identificada con la cédula de ciudadanía numero 1.095.530.320 expedida en Jordán, Santander, actuando en calidad de Revisora Fiscal, de la Sociedad GRUPO REINCAR S.A.S con Nit 900405236-5 certifican:

Que la sociedad GRUPO REINCAR S.A.S realiza de manera oportuna el pago de aportes al sistema de Seguridad Social y Parafiscales la oficina principal de Bucaramanga, y sedes en Cúcuta, Manizales y Bogotá, de acuerdo con lo contemplado en la ley 21 de 1982, la ley 100 de 1993 y la ley 797 de 2003.

De acuerdo con el Artículo 50 de la Ley 789 de 2002 la sociedad se encuentra en situación de cumplimiento con las obligaciones del sistema de seguridad social y parafiscales y en los últimos 6 meses ha cumplido el pago de estos aportes. La sociedad de igual forma viene cumpliendo con la cuota de aprendices que estableció la misma normatividad.

Que a la fecha de la certificación no tiene deudas contraídas por dichos conceptos de meses anteriores al que actualmente se viene causando.

Expide la certificacion el 7 de mayo de 2026, en cumplimiento de la normatividad legal para efectos de contratación con el estado y particulares.

ANEXOS PRESENTE INFORME

ANEXO		No FOLIOS	DESCRIPCIÓN
Anexo Técnico	☐		
Certificado pago Seguridad Social	X	1	Certificado de Seguridad Social y Parafiscales
Informes del Contratista	X	18	Informes de Gestion Mensual
Certificado (Revisor fiscal o RL) o planillas de pago de parafiscales	☐		Certificado de Seguridad Social y Parafiscales
Certificación Bancaria	☐		
OTROS	X	157	Archivo de Liquidacion - Informe de supervision - Certificaciones especificaciones tecnicas y operativas, resolucion de facturacion, Rut, tarjeta profesional revisior fiscal

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

Ocho (día en letras) **(8)** (día en números) días del mes de **Mayo** (mes en letras) de **2026** (Año)

(Firma) Gabriel Ernesto Fuentes Aguilar — Firmado digitalmente por Gabriel Ernesto Fuentes Aguilar

(Nombre) GABRIEL ERNESTO FUENTES AGUILAR

(Firma)

(Nombre) NOMBRE SUPERVISIÓN

(Firma) Jully Alexandra Garcia Agudelo — Firmado digitalmente por Jully Alexandra Garcia Agudelo Fecha: 2026.05.08 16:47:36 -05'00'

(Nombre) JULLY ALEXANDRA GARCIA AGUDELO

(Firma)

(Nombre) NOMBRE INTERVENTOR

Estadística de datos	Cantidad
Registros transferidos	142

Cl.doc. : RE (Factura bruto) Documento normal

Reg.prelim.por	NTUIRAN	Contab.por	MRINCONZ		
Nº doc.	5100000930	Sociedad	1000	Ejercicio	2026
Fe.docum.	12.05.2026	Fecha contab.	12.05.2026	Período	05
Calc.impuestos	☑				
Referen.	2940				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202605130650896				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
1	31	1002007511	RECUPERADORA Y NORMA		W0	345,395,600-
2	86	2511950101	CXP PROVED EM/RF		W0	8,755,539
3	91	5130950103	SERVICIO COBRO ADMIN		W0	0
4	86	2511950101	CXP PROVED EM/RF		W0	46,835
5	91	5130950103	SERVICIO COBRO ADMIN		W0	0
6	86	2511950101	CXP PROVED EM/RF		W0	150,712,790
7	91	5130950103	SERVICIO COBRO ADMIN		W0	0
8	86	2511950101	CXP PROVED EM/RF		W0	40,177,749
9	91	5130950103	SERVICIO COBRO ADMIN		W0	0
10	86	2511950101	CXP PROVED EM/RF		W0	108,839
11	91	5130950103	SERVICIO COBRO ADMIN		W0	0
12	86	2511950101	CXP PROVED EM/RF		W0	2,242,162
13	91	5130950103	SERVICIO COBRO ADMIN		W0	0
14	86	2511950101	CXP PROVED EM/RF		W0	4,739,440
15	91	5130950103	SERVICIO COBRO ADMIN		W0	0
16	86	2511950101	CXP PROVED EM/RF		W0	7,960,202
17	91	5130950103	SERVICIO COBRO ADMIN		W0	0
18	86	2511950101	CXP PROVED EM/RF		W0	36,774,647
19	91	5130950103	SERVICIO COBRO ADMIN		W0	0
20	86	2511950101	CXP PROVED EM/RF		W0	1,696,876
21	91	5130950103	SERVICIO COBRO ADMIN		W0	0
22	86	2511950101	CXP PROVED EM/RF		W0	1,920,628
23	91	5130950103	SERVICIO COBRO ADMIN		W0	0
24	86	2511950101	CXP PROVED EM/RF		W0	147,148
25	91	5130950103	SERVICIO COBRO ADMIN		W0	0
26	86	2511950101	CXP PROVED EM/RF		W0	1,065,117
27	91	5130950103	SERVICIO COBRO ADMIN		W0	0
28	86	2511950101	CXP PROVED EM/RF		W0	582,461
29	91	5130950103	SERVICIO COBRO ADMIN		W0	0
30	86	2511950101	CXP PROVED EM/RF		W0	3,018,207
31	91	5130950103	SERVICIO COBRO ADMIN		W0	0
32	86	2511950101	CXP PROVED EM/RF		W0	2,334,035
33	91	5130950103	SERVICIO COBRO ADMIN		W0	0
34	86	2511950101	CXP PROVED EM/RF		W0	4,394,374
35	91	5130950103	SERVICIO COBRO ADMIN		W0	0
36	86	2511950101	CXP PROVED EM/RF		W0	1,190,898
37	91	5130950103	SERVICIO COBRO ADMIN		W0	0
38	86	2511950101	CXP PROVED EM/RF		W0	2,503,611
39	91	5130950103	SERVICIO COBRO ADMIN		W0	0
40	86	2511950101	CXP PROVED EM/RF		W0	3,953,677
41	91	5130950103	SERVICIO COBRO ADMIN		W0	0
42	86	2511950101	CXP PROVED EM/RF		W0	10,798,814
43	91	5130950103	SERVICIO COBRO ADMIN		W0	0
44	86	2511950101	CXP PROVED EM/RF		W0	7,725,004
45	91	5130950103	SERVICIO COBRO ADMIN		W0	0
46	86	2511950101	CXP PROVED EM/RF		W0	1,025,133
47	91	5130950103	SERVICIO COBRO ADMIN		W0	0
48	86	2511950101	CXP PROVED EM/RF		W0	651,300
49	91	5130950103	SERVICIO COBRO ADMIN		W0	0

Cl.doc. : RE (Factura bruto) Documento normal

Reg.prelim.por	NTUIRAN	Contab.por	MRINCONZ		
Nº doc.	5100000930	Sociedad	1000	Ejercicio	2026
Fe.docum.	12.05.2026	Fecha contab.	12.05.2026	Período	05
Calc.impuestos	☑				
Referen.	2940				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202605130650896				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
50	86	2511950101	CXP PROVED EM/RF		W0	1,784,466
51	91	5130950103	SERVICIO COBRO ADMIN		W0	0
52	86	2511950101	CXP PROVED EM/RF		W0	45,653
53	91	5130950103	SERVICIO COBRO ADMIN		W0	0
54	86	2511950101	CXP PROVED EM/RF		W0	547,964
55	91	5130950103	SERVICIO COBRO ADMIN		W0	0
56	86	2511950101	CXP PROVED EM/RF		W0	13,784,918
57	91	5130950103	SERVICIO COBRO ADMIN		W0	0
58	86	2511950101	CXP PROVED EM/RF		W0	4,345,424
59	91	5130950103	SERVICIO COBRO ADMIN		W0	0
60	86	2511950101	CXP PROVED EM/RF		W0	27,784,099
61	91	5130950103	SERVICIO COBRO ADMIN		W0	0
62	86	2511950101	CXP PROVED EM/RF		W0	5,323,226
63	91	5130950103	SERVICIO COBRO ADMIN		W0	0
64	86	2511950101	CXP PROVED EM/RF		W0	2,667,355
65	91	5130950103	SERVICIO COBRO ADMIN		W0	0
66	86	2511950101	CXP PROVED EM/RF		W0	2,223,738
67	91	5130950103	SERVICIO COBRO ADMIN		W0	0
68	86	2511950101	CXP PROVED EM/RF		W0	17,851,793
69	91	5130950103	SERVICIO COBRO ADMIN		W0	0
70	86	2511950101	CXP PROVED EM/RF		W0	525,409
71	91	5130950103	SERVICIO COBRO ADMIN		W0	0
72	86	2511950101	CXP PROVED EM/RF		W0	243,548
73	91	5130950103	SERVICIO COBRO ADMIN		W0	0
74	86	2511950101	CXP PROVED EM/RF		W0	154,821
75	91	5130950103	SERVICIO COBRO ADMIN		W0	0
76	86	2511950101	CXP PROVED EM/RF		W0	481
77	86	2511950101	CXP PROVED EM/RF		W0	59,051
78	91	5130950103	SERVICIO COBRO ADMIN		W0	0
79	86	2511950101	CXP PROVED EM/RF		W0	67,323
80	91	5130950103	SERVICIO COBRO ADMIN		W0	0
81	86	2511950101	CXP PROVED EM/RF		W0	45,801
82	91	5130950103	SERVICIO COBRO ADMIN		W0	0
83	86	2511950101	CXP PROVED EM/RF		W0	709,220
84	91	5130950103	SERVICIO COBRO ADMIN		W0	0
85	86	2511950101	CXP PROVED EM/RF		W0	6,111
86	91	5130950103	SERVICIO COBRO ADMIN		W0	0
87	86	2511950101	CXP PROVED EM/RF		W0	27,936
88	91	5130950103	SERVICIO COBRO ADMIN		W0	0
89	86	2511950101	CXP PROVED EM/RF		W0	50,684
90	91	5130950103	SERVICIO COBRO ADMIN		W0	0
91	86	2511950101	CXP PROVED EM/RF		W0	896,776
92	91	5130950103	SERVICIO COBRO ADMIN		W0	0
93	86	2511950101	CXP PROVED EM/RF		W0	1,581,621
94	91	5130950103	SERVICIO COBRO ADMIN		W0	0
95	86	2511950101	CXP PROVED EM/RF		W0	766,084
96	91	5130950103	SERVICIO COBRO ADMIN		W0	0
97	86	2511950101	CXP PROVED EM/RF		W0	2,778,283
98	91	5130950103	SERVICIO COBRO ADMIN		W0	0

Cl.doc. : RE (Factura bruto) Documento normal

Reg.prelim.por	NTUIRAN	Contab.por	MRINCONZ		
Nº doc.	5100000930	Sociedad	1000	Ejercicio	2026
Fe.docum.	12.05.2026	Fecha contab.	12.05.2026	Período	05
Calc.impuestos	☑				
Referen.	2940				
Moneda doc.	COP				
Txt.cab.doc.	02-2303-202605130650896				

Pos	CT	Cuenta	Texto breve cuenta	Asignación	II	Importe
99	86	2511950101	CXP PROVED EM/RF		W0	6,693,155
100	91	5130950103	SERVICIO COBRO ADMIN		W0	0
101	86	2511950101	CXP PROVED EM/RF		W0	96,175
102	91	5130950103	SERVICIO COBRO ADMIN		W0	0
103	86	2511950101	CXP PROVED EM/RF		W0	142,339
104	91	5130950103	SERVICIO COBRO ADMIN		W0	0
105	86	2511950101	CXP PROVED EM/RF		W0	186,416
106	91	5130950103	SERVICIO COBRO ADMIN		W0	0
107	86	2511950101	CXP PROVED EM/RF		W0	79,237
108	91	5130950103	SERVICIO COBRO ADMIN		W0	0
109	86	2511950101	CXP PROVED EM/RF		W0	199,200
110	91	5130950103	SERVICIO COBRO ADMIN		W0	0
111	86	2511950101	CXP PROVED EM/RF		W0	459,441
112	91	5130950103	SERVICIO COBRO ADMIN		W0	0
113	86	2511950101	CXP PROVED EM/RF		W0	96,175
114	91	5130950103	SERVICIO COBRO ADMIN		W0	0
115	86	2511950101	CXP PROVED EM/RF		W0	534,473
116	91	5130950103	SERVICIO COBRO ADMIN		W0	0
117	86	2511950101	CXP PROVED EM/RF		W0	267,079
118	91	5130950103	SERVICIO COBRO ADMIN		W0	0
119	86	2511950101	CXP PROVED EM/RF		W0	500,111
120	91	5130950103	SERVICIO COBRO ADMIN		W0	0
121	86	2511950101	CXP PROVED EM/RF		W0	34,521
122	91	5130950103	SERVICIO COBRO ADMIN		W0	0
123	86	2511950101	CXP PROVED EM/RF		W0	107,293
124	91	5130950103	SERVICIO COBRO ADMIN		W0	0
125	86	2511950101	CXP PROVED EM/RF		W0	177,924
126	91	5130950103	SERVICIO COBRO ADMIN		W0	0
127	86	2511950101	CXP PROVED EM/RF		W0	468,379
128	91	5130950103	SERVICIO COBRO ADMIN		W0	0
129	86	2511950101	CXP PROVED EM/RF		W0	254,329
130	91	5130950103	SERVICIO COBRO ADMIN		W0	0
131	86	2511950101	CXP PROVED EM/RF		W0	38,470
132	91	5130950103	SERVICIO COBRO ADMIN		W0	0
133	86	2511950101	CXP PROVED EM/RF		W0	164,459
134	91	5130950103	SERVICIO COBRO ADMIN		W0	0
135	86	2511950101	CXP PROVED EM/RF		W0	199,082
136	91	5130950103	SERVICIO COBRO ADMIN		W0	0
137	86	2511950101	CXP PROVED EM/RF		W0	668,323
138	91	5130950103	SERVICIO COBRO ADMIN		W0	0
139	86	2511950101	CXP PROVED EM/RF		W0	726,081
140	91	5130950103	SERVICIO COBRO ADMIN		W0	0
141	50	2519050401	HONORARIOS 11%			36,132,683-
142	50	2519053801	RTE IVA TARIFA GENER			9,361,650-

Reincar
Recuperadora integral de cartera

Grupo Reincar
NIT 900.405.236-5
Carrera 19 No.36 20
Tel: (607) 6978148
Bucaramanga - Colombia
contabilidad@reincar.com.co

Factura electrónica de venta
No. ELEC 2940

Señores	FONDO NACIONAL DEL AHORRO S.A.		
NIT	899.999.284-4	**Teléfono**	(601) 3810150
Dirección	CL 12 65 11	**Ciudad**	Bogotá - Colombia

Fecha y hora Factura	
Generación	12/05/2026, 11:37
Expedición	12/05/2026, 11:37
Vencimiento	11/06/2026

Ítem	Descripción	Cantidad	Vr. Unitario	Valor Impto.Rete.	Vr. Total	Vr. Bruto
1	HONORARIOS GESTIÓN ABRIL 2026 CÓDIGOS DE APROBACIÓN 1000061238 •Aplicación descuento ofertado 3% por valor de $12.089.379	1.00	328,478,935.29	36,132,682.88	354,757,250.12	328,478,935.29

Total items: 1

Valor en Letras: Trescientos cuarenta y cinco millones trescientos noventa y cinco mil seiscientos pesos m/cte con cuarenta y seis cent.

Forma de pago:
Crédito

Medio de pago:
Otro - Crédito - Cuota No. 001 vence el 2026-06-11 por $ 345,395,600.46

Total Bruto	328,478,935.29
IVA 19%	62,410,997.71
Retefuente 11% Honorarios	36,132,682.88
ReteIVA 15%	9,361,649.66
Total a Pagar	**345,395,600.46**

Observaciones: Cancelar en cuenta corriente del Banco de Bogotá 184197929

No practicar ICA en Bucaramanga debido a que somos Autorretenedores según Res. 1017 del 31 de mayo de 2021

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 18764099913569 aprobado en 20251008 prefijo ELEC desde el número 2794 al 3000 Vigencia: 12 Meses**
Responsable de IVA - Actividad Económica 8220 Actividades de centros de llamadas (call center) Tarifa
CUFE: a101deead2d96c08fdfc5ff0badb71294840f0316435e3b50ac3e99c662a5acaa4c153be430e154c0df42d3b28036d6e

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

Reincar
Recuperadora Integral de Cartera
NIT. 900.405.236-5

SI-2000523 SC-CER546357

Bucaramanga, 7 de mayo de 2026

Señores
A QUIEN INTERESE

Nosotros **DIEGO ENRIQUE GONZALEZ RAMIREZ** identificado con cédula de ciudadanía número 1.098.642.487 expedida en Bucaramanga actuando en calidad de GERENTE GENERAL, y **SANDRA MILENA CARRILLO BLANCO** identificada con la cédula de ciudadanía numero 1.095.530.320 expedida en Jordán, Santander, actuando en calidad de REVISORA FISCAL, de la Sociedad GRUPO REINCAR S.A.S con Nit 900405236-5 nos permitimos:

CERTIFICAR

Que la sociedad GRUPO REINCAR S.A.S realiza de manera oportuna el pago de aportes al sistema de Seguridad Social y Parafiscales la oficina principal de Bucaramanga, y sedes en Cúcuta, Manizales y Bogotá, de acuerdo con lo contemplado en la ley 21 de 1982, la ley 100 de 1993 y la ley 797 de 2003.
De acuerdo con el Artículo 50 de la Ley 789 de 2002 la sociedad se encuentra en situación de cumplimiento con las obligaciones del sistema de seguridad social y parafiscales y en los últimos 6 meses ha cumplido el pago de estos aportes. La sociedad de igual forma viene cumpliendo con la cuota de aprendices que estableció la misma normatividad.

Que a la fecha de esta certificación no tiene deudas contraídas por dichos conceptos de meses anteriores al que actualmente se viene causando.

Se expide en cumplimiento de la normatividad legal para efectos de contratación con el estado y particulares.

Cordialmente

DIEGO ENRIQUE GONZALEZ RAMIREZ
Gerente General

SANDRA MILENA CARRILLO BLANCO
Revisora Fiscal
T.P. 316730-T

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 02 Actualización

4. Número de formulario 141221151243

(415)7707212489984(8020) 000014122115124 3

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
900405236	5	Impuestos y Aduanas de Bucaramanga	4

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
RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

36. Nombre comercial	37. Sigla
	GRUPO REINCAR S.A.S.

UBICACIÓN

38. País	39. Departamento	40. Ciudad/Municipio
COLOMBIA 169	Santander 68	Bucaramanga 001

41. Dirección principal
CR 19 36 20 OF 501 ED CAMARA DE COMERCIO

42. Correo electrónico recuperadora@reincar.com.co

43. Código postal	44. Teléfono 1	45. Teléfono 2
	6076978148	

CLASIFICACIÓN

Actividad económica

Actividad principal		Actividad secundaria		Otras actividades			Ocupación	
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código	1	2	51. Código	52. Número establecimientos
8220	2011-01-04	6910	2011-01-04		4330	8219		3

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	14	42	48	52	55																			

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

Usuarios aduaneros

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

Exportadores

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

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

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2025-11-18 / 01:07:22PM

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

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre GONZALEZ RAMIREZ DIEGO ENRIQUE

985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario

001

Espacio reservado para la DIAN

4. Número de formulario: 141221151243

(415)7707212489984(8020) **000014122115124 3**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional		14. Buzón electrónico
9 0 0 4 0 5 2 3 6	5	Impuestos y Aduanas de Bucaramanga	4	

Características y formas de las organizaciones

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

Constitución, Registro y Última Reforma

Documento	1. Constitución	2. Reforma
71. Clase	0 4	0 1
72. Número		0 1 6
73. Fecha	2 0 1 1 0 1 0 3	2 0 2 1 0 4 0 5
74. Número de notaría		
75. Entidad de registro	0 3	0 3
76. Fecha de registro	2 0 1 1 0 1 0 4	2 0 2 1 0 4 1 3
77. No. Matrícula mercantil	0 5 1 9 7 4 8 2 1 6	0 5 1 9 7 4 8 2 1 6
78. Departamento	6 8	6 8
79. Ciudad/Municipio	5	5

Vigencia

80. Desde	2 0 1 1 0 1 0 3
81. Hasta	2 0 9 9 1 2 3 1

Composición del Capital

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

Entidad de vigilancia y control

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

Estado y Beneficio

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

Vinculación económica

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

97. Nombre o razón social de la matriz o controlante

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

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Representación

001

Espacio reservado para la DIAN

4. Número de formulario: 141221151243

(415)7707212489984(8020) **000014122115124 3**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 4 0 5 2 3 6	5	Impuestos y Aduanas de Bucaramanga	4

Representación

1

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL PRIN 1 8	2 0 1 1 0 1 0 4

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadaní 1 3	1 0 9 8 6 4 2 4 8 7		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
GONZALEZ	RAMREZ	DIEGO	ENRIQUE

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

2

98. Representación	99. Fecha inicio ejercicio representación
REPRS LEGAL SUPL 1 9	2 0 1 8 0 8 1 5

100. Tipo de documento	101. Número de identificación	102. DV	103. Número de tarjeta profesional
Cédula de Ciudadan 1 3	8 8 0 3 0 2 5 5		

104. Primer apellido	105. Segundo apellido	106. Primer nombre	107. Otros nombres
RAMOS	SOLANO	LEANDRO	ENRIQUE

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

3

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

4

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

5

98. Representación	99. Fecha inicio ejercicio representación

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

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

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

001

Espacio reservado para la DIAN

4. Número de formulario: 141221151243

(415)7707212489984(8020) **000014122115124 3**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 4 0 5 2 3 6	5	Impuestos y Aduanas de Bucaramanga	4

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

1

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad
Cédula de Ciudada 1 3	1 0 9 8 6 4 2 4 8 7		COLOMBIA 1 6 9

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres
GONZALEZ	RAMIREZ	DIEGO	ENRIQUE

119. Razón social

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

2

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad
Cédula de Ciudada 1 3	8 8 0 3 0 2 5 5		COLOMBIA 1 6 9

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres
RAMOS	SOLANO	LEANDRO	ENRIQUE

119. Razón social

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

3

111. Tipo de documento	112. Número de identificación	113. DV	114. Nacionalidad
Cédula de Ciudada 1 3	5 4 7 7 5 9 3		COLOMBIA 1 6 9

115. Primer apellido	116. Segundo apellido	117. Primer nombre	118. Otros nombres
BAUTISTA	FLOREZ	ROLANDO	

119. Razón social

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

4

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

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

119. Razón social

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

5

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

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

119. Razón social

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

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Revisor Fiscal y Contador

001

Espacio reservado para la DIAN

4. Número de formulario: 141221151243

(415)7707212489984(8020) **000014122115124 3**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 4 0 5 2 3 6	5	Impuestos y Aduanas de Bucaramanga	4

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 9 5 5 3 0 3 2 0	2	3 1 6 7 3 0 T

128. Primer apellido	129. Segundo apellido	130. Primer nombre	131. Otros nombres
CARRILLO	BLANCO	SANDRA	MILENA

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

135. Fecha de nombramiento: 2 0 2 4 0 6 1 2

Revisor fiscal suplente

136. Tipo de documento	137. Número de identificación	138. DV	139. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	1 0 9 8 7 5 4 0 2 3	2	1 2 0 5 7 7 T

140. Primer apellido	141. Segundo apellido	142. Primer nombre	143. Otros nombres
GALVIS	RODRIGUEZ	INGRID	CAROLINA

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

147. Fecha de nombramiento: 2 0 2 4 0 6 1 2

Contador

148. Tipo de documento	149. Número de identificación	150. DV	151. Número de tarjeta profesional
Cédula de Ciudadanía 1 3	1 0 0 7 4 7 7 7 9 0	4	3 0 3 1 7 3

152. Primer apellido	153. Segundo apellido	154. Primer nombre	155. Otros nombres
REYES	VELASCO	GINETH	VIVIANA

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

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

COPIA CERTIFICADO
DOCUMENTO SIN COSTO

DIAN

Formulario del Registro Único Tributario
Establecimientos

001

Espacio reservado para la DIAN

4. Número de formulario: 141221151243

(415)7707212489984(8020) **000014122115124 3**

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
9 0 0 4 0 5 2 3 6	5	Impuestos y Aduanas de Bucaramanga 4	

Establecimientos, agencias, sucursales, oficinas, sedes o negocios entre otros

1

160. Tipo de establecimiento	161. Actividad económica
Establecimiento de comerci 0 2	Actividades de centros de llamadas (call center) 8 2 2 0

162. Nombre del establecimiento: RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

163. Departamento	164. Ciudad/Municipio
Santander 6 8	Bucaramanga 0 0 1

165. Dirección: CR 19 36 20 OF 501 ED CAMARA DE COMERCIO

166. Número de matrícula mercantil	167. Fecha de la matrícula mercantil
1 9 7 4 8 3	2 0 1 1 0 1 0 4
168. Teléfono	**169. Fecha de cierre**
6 0 7 6 9 7 8 1 4 8	

2

160. Tipo de establecimiento	161. Actividad económica
Establecimiento de comerci 0 2	Actividades de centros de llamadas (call center) 8 2 2 0

162. Nombre del establecimiento: RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

163. Departamento	164. Ciudad/Municipio
Bogotá D.C. 1 1	Bogotá, D.C. 0 0 1

165. Dirección: CL 30 A 6 22 ED SAN MARTIN OF 2703

166. Número de matrícula mercantil	167. Fecha de la matrícula mercantil
2 5 7 7 3 5 2	2 0 1 1 0 1 0 4
168. Teléfono	**169. Fecha de cierre**
6 0 1 7 9 4 8 4 8 4	

3

160. Tipo de establecimiento	161. Actividad económica
Establecimiento de comerci 0 2	Actividades de centros de llamadas (call center) 8 2 2 0

162. Nombre del establecimiento: RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

163. Departamento	164. Ciudad/Municipio
Norte de Santander 5 4	Cúcuta 0 0 1

165. Dirección: AV 5 12 62 OF 202 ED COLSEGUROS

166. Número de matrícula mercantil	167. Fecha de la matrícula mercantil
4 5 5 0 7 6	2 0 2 4 0 1 0 1
168. Teléfono	**169. Fecha de cierre**
6 0 7 5 9 5 6 5 1 2	

COPIA CERTIFICADO DOCUMENTO SIN COSTO

DIAN

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764081290454

(415)7707212489984(8020) 001876408129045 4

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
900405236	5				

11. Razón social

RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

12. Dirección seccional

Impuestos y Aduanas de Bucaramanga

Cód. 4

24. Dirección

CR 19 36 20 OF 501 ED CAMARA DE COMERCIO

25. País	26.Departamento	27. Municipio
Colombia	Santander	Bucaramanga

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

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

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

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

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

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

Firma del solicitante

Firma del funcionario autorizado

DIAN

2024-10-09 / 05:13:16 PM

Fecha Acuse de Recibo

Firmado

984. Apellidos y nombres

985. Cargo

989. Dependencia

990. Lugar administrativo SUBDIRECCION DE FACTURA ELECTRONICA Y SOLUCI

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

992. Área

993. Establecimiento

1001. Apellidos y nombres GONZALEZ RAMIREZ DIEGO ENRIQUE

1002. Tipo documento Cédula de Ciudadanía

1003. No. Identiflcación 1098642487 1004. DV 5

1005. Cod. Representación Representante Legal Principal

1006. Organización RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA

997. Fecha formalización 2024-10-09/17:13:16

AUTORIZADO

DIAN

Autorización Numeración de Facturación

1876

Espacio reservado para la DIAN

4. Número de formulario 18764081290454

(415)7707212489984(8020) 001876408129045 4

5. Número de Identificación Tributaria - NIT	6. DV	7. Primer apellido	8. Segundo apellido	9. Primer nombre	10. Otros nombres
900405236	5				

11. Razón social

RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S.

Rangos de numeración para autorizar, habilitar o inhabilitar

	29. Establecimiento	30. Modalidad	Cód.	31. Prefijo	32. Desde el número	33. Hasta el número	38. Vigencia	34. Tipo solicitud	Cód.
1	RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S. CR 19 36 20 ED CAMARA DE COMERCIO	FACTURA ELECTRÓNICA DE VENTA	4	ELEC	2,548	3,000	12	HABILITACIÓN	2
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									

AUTORIZADO

República de Colombia
Ministerio de Comercio, Industria y Turismo

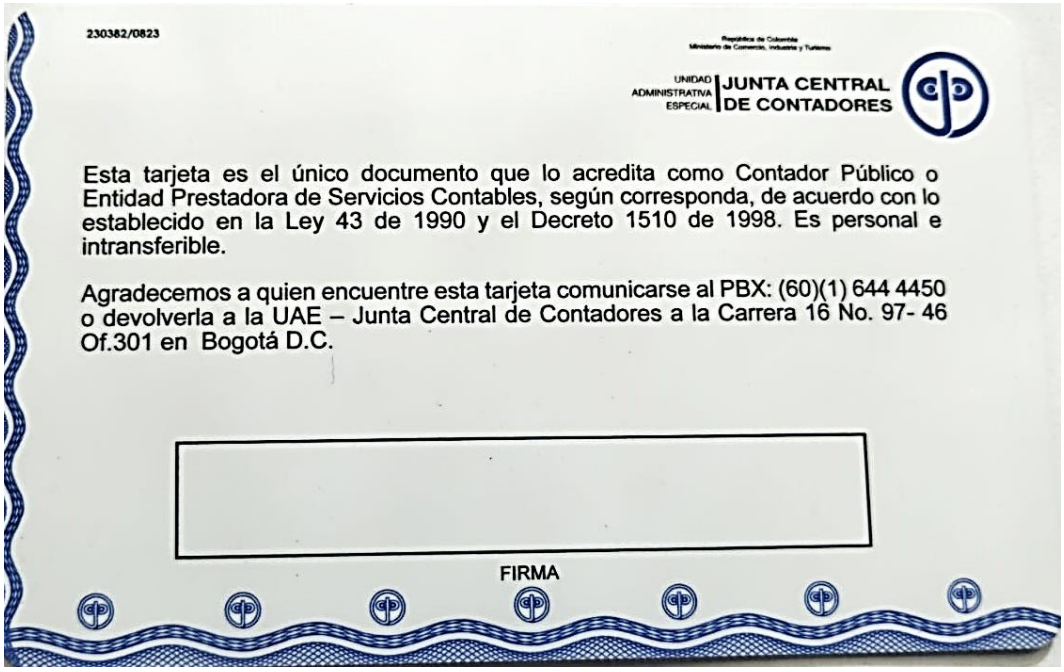
UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

316730-T

SANDRA MILENA
CARRILLO BLANCO
C.C. 1095530320
RES. INSCRIPCION 439 DEL 10/10/2023
CORPORACION UNIVERSITARIA REMINGTON

JOSE ORLANDO RAMIREZ ZULUAGA
DIRECTOR GENERAL

366539 372082



230382/0823

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

Esta tarjeta es el único documento que lo acredita como Contador Público o Entidad Prestadora de Servicios Contables, según corresponda, de acuerdo con lo establecido en la Ley 43 de 1990 y el Decreto 1510 de 1998. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (60)(1) 644 4450 o devolverla a la UAE – Junta Central de Contadores a la Carrera 16 No. 97- 46 Of.301 en Bogotá D.C.

FIRMA

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

NUMERO **1.098.642.487**

GONZALEZ RAMIREZ

APELLIDOS

DIEGO ENRIQUE

NOMBRES

FIRMA

INDICE DERECHO

FECHA DE NACIMIENTO **25-SEP-1987**

BUCARAMANGA
(SANTANDER)
LUGAR DE NACIMIENTO

1.80	**B+**	**M**
ESTATURA	G.S. RH	SEXO

28-SEP-2005 BUCARAMANGA
FECHA Y LUGAR DE EXPEDICION

REGISTRADOR NACIONAL
CARLOS ARIEL SÁNCHEZ TORRES

A-2700100-00119421-M-1098642487-20081101 0005149332A 1 24017924

INFORME DE SUPERVISION

CONTRATISTA	RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S. - GRUPO REINCAR S.A.S.
No. CONTRATO	FNA-022-2026
OBJETO	Prestar los servicios de gestión y recuperación de la cartera del Fondo Nacional del Ahorro S.A., a nivel nacional, en las etapas preventiva y administrativa, incluyendo la cartera titularizada y la ejecución de campañas especiales de créditos.
PERIODO DEL INFORME	6 al 30 de abril 2026
AVANCE FINANCIERO DEL CONTRATO	Valor del contrato: $2,600,076,308 Pagos realizados: $571,701,909 Pago gestión periodo del presente informe: $390,889,933 Porcentaje ejecutado: 37.02% Saldo del contrato: $1,637,484,466

ASIGNACION

Para el periodo del presente informe se realizó asignación de 10.442 obligaciones a Reincar en reparto administrativo y 20.278 en reparto preventivo, de acuerdo con los resultados obtenidos en el último trimestre de asignación por cada franja de mora, para la gestión de recuperación de cartera, asignación cargada en aplicativo de gestión asignado por el fondo, para inicio de las gestiones el 6 de abril de 2026, se realizó asignación de la cartera en todas las franjas de mora, buscando un impacto positivo en el indicador, para lo cual se solicitó intensificar la gestión en los montos altos para poder llegar más rápido a la cifra requerida, este aspecto se implementó en todas las franjas para impactar directamente el indicador con las metas de recuperación y deterioro, se solicitó focalizar la cartera dependiendo el tipo de vivienda VIS Y NO VIS. Los casos en UVR se mantuvieron en constante seguimiento, adicionalmente potencializar el ofrecimiento de negociación de las franjas altas que permitan generar un impacto positivo al indicador.

A continuación, se relaciona el reparto generado a la casa de cobro para su gestión.

Franja	Saldo K.	Oblig.
B. DE 1 A 30	194,994,357,910	3048
C. DE 31 A 60	158,582,135,458	2434
D. DE 61 A 90	15,603,607,981	243
E. DE 91 A 120	52,144,406,839	830
F. DE 121 A 150	35,297,604,995	555
G. DE 151 A 360	29,833,633,492	471
H. DE 360 A 540	17,783,404,771	330
I. MAYOR A 540	64,162,878,373	949
J. CASTIGO	53,044,774,783	1582
Total general	**621,446,804,602**	**10442**

GESTIONES REALIZADA

En el transcurso del mes se realizó medición de rotación de cartera, spin rate y tipo de contacto realizado a la careta y estos fueron los resultados:

Rotación de cartera

CASA DE COBRO	REINCAR	Total general
04/25/2026	14	14
04/27/2026	1	1
04/28/2026	48	48
04/29/2026	15	15
04/30/2026	8297	8297
Total general	**8375**	**8375**

Spin Rate

CASA DE COBRO	D. 3 Gestion	E. 4. Gestion	F. Mas 4 Gestion	Total general
REINCAR	1	488	7886	8375
Total general	**1**	**488**	**7886**	**8375**

Tipo de contacto

	1-CONTACTO DIRECTO		2-CONTACTO CON TERCERO		3-SIN CONTACTO		Total Oblig.	Total %
CASA DE COBRO	Oblig.	%	Oblig.	%	Oblig.	%		
REINCAR	3740	44.66%	223	2.66%	4412	52.68%	8375	100.00%
Total general	**3740**	**44.66%**	**223**	**2.66%**	**4412**	**52.68%**	**8375**	**100.00%**

RESULTADOS OBTENIDOS

Con base al trabajo realizado por la casa de cobro, se obtuvieron los siguientes resultados de recuperación:

Etiquetas de fila	NORMALIZADO	RECUPERADO < 30	RECUPERADO > 30	MANTENIDO	DETERIORADO	Total general	CONTENCION	META	% EJECUCION	FALTANTE
REINCAR	**22.92%**	**4.48%**	**1.92%**	**27.86%**	**42.83%**	**100.00%**				
B. DE 1 A 30	38.69%	0.00%	0.00%	39.98%	21.32%	100.00%	78.68%	90.00%	87.42%	-11.32%
C. DE 31 A 60	17.23%	14.35%	0.00%	36.14%	32.28%	100.00%	67.72%	80.00%	84.65%	-12.28%
D. DE 61 A 90	19.15%	3.50%	5.83%	27.95%	43.56%	100.00%	56.44%	59.02%	95.63%	-2.58%
E. DE 91 A 120	13.06%	1.31%	9.80%	24.75%	51.08%	100.00%	48.92%	52.85%	92.57%	-3.93%
F. DE 121 A 150	17.96%	1.56%	10.29%	16.25%	53.94%	100.00%	46.06%	43.06%	106.96%	3.00%
G. DE 151 A 360	28.00%	1.24%	2.50%	0.00%	68.26%	100.00%	31.74%	10.37%	306.26%	21.38%
H. DE 360 A 540	6.49%	1.84%	1.71%	0.00%	89.95%	100.00%	10.05%	6.50%	154.68%	3.55%
I. MAYOR A 540	3.16%	0.16%	0.28%	0.00%	96.39%	100.00%	3.61%	6.00%	60.09%	-2.39%

LISTA DE VERIFICACION DE CUMPLIMIENTO DE OBLIGACIONES ESPECIFICAS

OBLIGACION	ACTIVIDADES DESARROLLADAS/ EVIDENCIA
1. Cumplir todas las obligaciones definidas y contenidas en el Anexo No. 1 - Requerimientos - Especificaciones Técnicas y Operativas del Servicio a Contratar y el Anexo No.5 Acuerdos de Niveles de Servicio.	Reincar aporta certificaciones de cumplimiento de los requerimientos
2. Recibir las obligaciones asignadas por el Fondo para la gestión de recuperación de cartera y gestionar por los medio o canales autorizados (telefónico, correo electrónico, sms, agentes virtuales)	Reincar realiza la recepción de la asignación del 6 de abril 2026 y realiza las gestiones de cobro a través de los canales autorizados dejando evidencia en el aplicativo de gestión asignado por el fondo **https://fna.adminfo.net/smartplus/**
3. Realizar la gestión de cobro preventivo, administrativo y cartera titularizada de las obligaciones crediticias hipotecarias, de leasing habitacional y consumo, que la Gerencia Cobranzas y BRDPR ordene (o quien haga sus veces).	Reincar realizo las gestiones de cobro correspondientes sobre las obligaciones asignadas, información registrada en el aplicativo de gestión asignado por el fondo
4. Realizar la gestión de cobro sobre las obligaciones asignadas en campañas especiales según las necesidades y estrategias dadas por la Gerencia de Cobranzas y BRDPR.	Para el periodo del presente informe no se asignaron campañas especiales
5. Asistir a las reuniones que convoque el Supervisor del contrato definido por el Fondo.	El proveedor asistió a las reuniones convocadas por el FNA de lo cual queda constancia en las actas de reunión
6. Mantener durante la ejecución del contrato el recurso humano, la infraestructura física y las demás condiciones presentadas en la oferta.	Reincar aporta certificaciones de cumplimiento de los requerimientos
7. No podrá subcontratar otras empresas para realizar la gestión objeto del contrato.	Durante el periodo del presente informe no se evidencia subcontratación
8. Celebrar acuerdos de confidencialidad con sus colaboradores sobre la información conocida para la ejecución del contrato y sobre las actividades desarrolladas. Por tanto, será responsable por la filtración que de esta información haga su personal. Dichos acuerdos deben reposar en la carpeta del contrato del personal y ser validado por el Supervisor del contrato antes de inicio de actividades.	Reincar aporta hojas de vida de los colaboradores donde se evidencia el acuerdo de confidencialidad
9. Instruir a sus colaboradores sobre la propiedad de la información que le entregue el Fondo Nacional del Ahorro S.A., así, como de los procedimientos y controles	Se evidencia el registro de las gestiones realizadas a las obligaciones asignada en el aplicativo de gestión designado por el fondo **https://fna.adminfo.net/smartplus/**

establecidos para el manejo de esta, para tales efectos el contratista registrará las actividades de cobranza en la herramienta de gestión asignada por el Fondo.	
10. Contar con protocolos de redes, servicios, aplicaciones, usuarios, equipos y todo lo que sea necesario para la ejecución del objeto del contrato	Reincar certifica capacidad operativa y de seguridad de la información
11. Dejar constancia documental de las gestiones realizadas para recuperación de cartera y de la información que se suministró a los deudores, así como de los compromisos y las condiciones que se establezcan dejando evidencia de que los clientes han conocido toda la información y la han aceptado, en la herramienta de gestión asignada por el Fondo.	Reincar deja evidencia de las gestiones realizadas a las obligaciones asignada en el aplicativo de gestión designado por el fondo y carga en esta los compromisos de pago **https://fna.adminfo.net/smartplus/**
12. Dejar evidencia documental en la herramienta de gestión cuando se realicen acuerdos de pago bajo las alternativas definidas por el Fondo (normalización, extinción, pago parcial de las cuotas mora, diferidos castigo, entre otros)	Reincar deja evidencia documental cargando los acuerdos de pago de alternativas de pago solicitadas por los clientes de las obligaciones asignadas en el aplicativo de gestión asignado por el fondo **https://fna.adminfo.net/smartplus/**
13. Informar al supervisor asignado por el Fondo Nacional del Ahorro S.A., de manera inmediata vía correo electrónico los pagos realizados por los deudores en los bancos comerciales con Convenio de Recaudo y Puntos de Pago de las empresas de giro habilitadas mediante convenio con el Fondo, los cuales no sean visualizados en la herramienta de gestión, para que sean aplicados a la obligación crediticia, en el evento en que no hayan sido aplicados oportunamente a las obligaciones y de los cuales tenga conocimiento el contratista.	En el periodo del presente informe no se presentaron reportes de pagos no aplicados a las obligaciones asignadas a Reincar
14. No dejar ningún tipo de mensajes con menores de edad, al momento de realizar la gestión de recuperación de cartera a un deudor.	No se evidenciaron gestiones de cobro realizadas de manera incorrecta en contravía de la obligación
15. Presentar mensualmente, o en el momento que sean requeridos por el supervisor del contrato definido por el Fondo, los informes de la gestión acorde con los parámetros establecidos, para su evaluación, desempeño y eficiencia.	Reincar suministro los informes requeridos por el fondo en los tiempos y condiciones solicitados
16. Grabar todas las llamadas realizadas por los clientes asignados para la recuperación de	Reincar certifica la grabación de las llamadas realizadas sobre las obligaciones asignadas en el

<table>
<tr><td>cartera a los centros de atención telefónica del contratista cuando consulten o actualicen su información.</td><td>periodo del presente informe se solicitaron grabaciones aleatorias para validación del cumplimiento</td></tr>
<tr><td>17. El contratista deberá ejecutar el objeto del contrato dentro de los siguientes horarios:
<table><tr><th>DÍAS</th><th>HORARIO</th></tr><tr><td>Lunes a viernes</td><td>De 7:00 AM a 7:00 PM</td></tr><tr><td>Sábados</td><td>De 8:00 AM a 3:00 PM</td></tr></table></td><td>Para asegurar el cumplimiento de esta obligación el fondo en el aplicativo de gestión presenta restricción horaria de acceso</td></tr>
</table>

CALIFICACION DE LA ACTIVIDAD CONTRACTUAL

CRITERIO	DESCRIPCIÓN	PORCENTAJE	PUNTAJE: DEL 1 AL 5
Efectividad en la recuperación de cartera	Medir de los resultados de recuperación. • Porcentaje de recuperación frente a la cartera asignada • Cumplimiento de metas de recaudo • Evolución mensual del recaudo • Recuperación según altura de mora (0–30, 31–60, 61-90, +90 días)	40%	4
Calidad de la gestión de cobro	Evaluar cómo se realiza la gestión, no solo cuánto se recupera. • Trazabilidad de las gestiones realizadas • Registro adecuado de llamadas, gestiones y acuerdos • Pertinencia y consistencia de las estrategias de cobro • Manejo adecuado del deudor (trato respetuoso, no abusivo)	20%	5
Gestión administrativa y reporte	Evaluar el soporte operativo del contrato. • Calidad y claridad de los informes • Oportunidad en la entrega de reportes • Consistencia de la información reportada • Atención a requerimientos del supervisor • Capacidad de respuesta ante observaciones	20%	5
Cumplimiento contractual	Determinar si el contratista cumple lo pactado en el contrato. • Cumplimiento de plazos y cronograma • Ejecución de las actividades contratadas • Entrega oportuna de informes y soportes • Uso adecuado de los canales y herramientas autorizadas	10%	5

	• Confidencialidad de la información y protección de datos		
Cumplimiento legal y normativo	Validar el cumplimiento para evitar riesgos jurídicos y reputacionales. • Cumplimiento de normas de protección de datos personales • Cumplimiento de normas de cobranza (consumidor financiero, habeas data, ley 2300) • Ausencia de quejas, sanciones o procesos legales	10%	5

APLICACIONES DE ACUERDOS DE NIVELES DE SERVICIO

<table>
<tr><th>ANS</th><th>PENALIDAD (SI/NO)</th><th>PORCENTAJE PENALIDAD</th><th>VALOR</th></tr>
<tr><td>Incumplimiento de las metas establecidas (sin incluir castigo)</td><td>SI</td><td><table><tr><th>FRANJA</th><th>PENALIDAD</th></tr><tr><td>Franja 1 – 30</td><td>0.5%</td></tr><tr><td>Franja 31 – 60</td><td>1%</td></tr><tr><td>Franja 61 – 90</td><td>1%</td></tr><tr><td>Franja 91 – 120</td><td>0.4%</td></tr><tr><td>Franja 121 – 150</td><td>0.4%</td></tr><tr><td>Franja 151 - 360</td><td>0.4%</td></tr><tr><td>Franjas >361</td><td>0.4%</td></tr><tr><td>TOTAL</td><td>3.70%</td></tr></table></td><td>$ 15,483,110</td></tr>
<tr><td>Tendrán un término de cuatro (4) días para realizar el primer barrido de gestión a toda la cartera asignada en busca de contactar al deudor</td><td>NO</td><td></td><td></td></tr>
<tr><td>Deberá como mínimo realizar cuatro (4) gestiones telefónicas a las obligaciones asignadas siempre y cuando presente mora</td><td>NO</td><td></td><td></td></tr>
<tr><td>No recibir quejas por mal trato o prácticas abusivas derivadas de la gestión de cobro realizada</td><td>NO</td><td></td><td></td></tr>
<tr><td>Deberá asegurar que la información registrada en la herramienta de gestión corresponda a la realidad de la gestión realizada o contacto con los clientes.</td><td>NO</td><td></td><td></td></tr>
</table>

Deberá asegurar que el personal cuente con el conocimiento necesarios para la prestación del servicio	NO		

***Dentro de la oferta económica presentada por el contratista, este oferto un descuento del 3% sobre el valor total de la factura el cual para el presente informe corresponde al valor de **$12,089,379**

Firma,

Gabriel Ernesto Fuentes Aguilar

Firmado digitalmente por Gabriel Ernesto Fuentes Aguilar

GABRIEL ERNESTO FUENTES AGUILAR
Gerente Cobranza y BRDPR (E)
Supervisor del contrato (E)

Proyecto: John Alexander Serna G. – Gcb-p06
Proyecto: Jully Alexandra Garcia A. – Gcb-p04

Descripción Funcional Aplicativo in house ReincarApp

Software principal el cual brinda a nuestros clientes toda la seguridad en cada uno de los procesos de recuperación de su cartera.

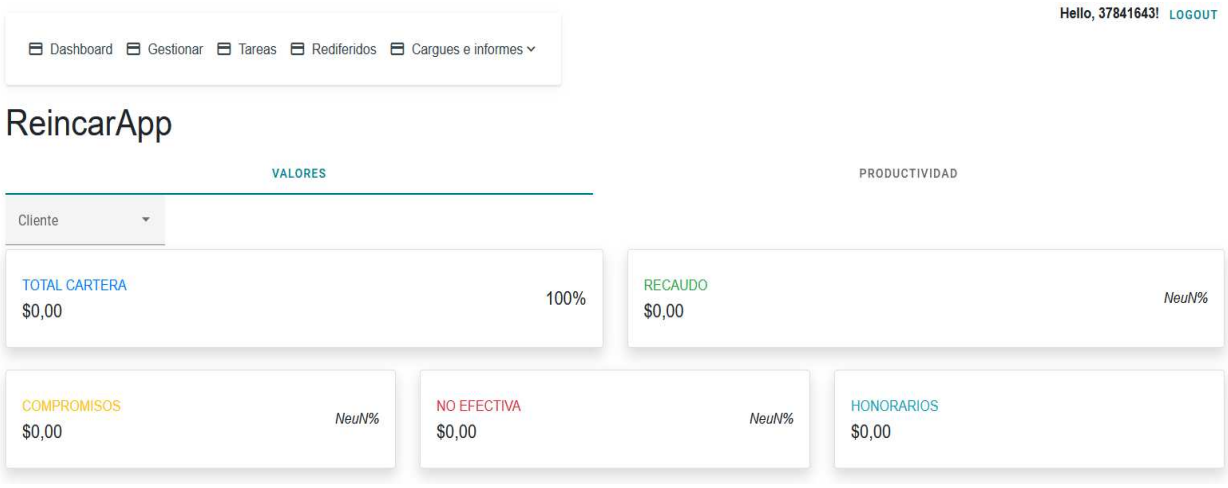
Con Reincarapp tenemos una segura y organizada administración de toda la información de cada cliente para la correcta gestión de cobranza a nivel pre jurídico y jurídico.

Un software practico y fácil de usar con campos parametrizables a las necesidades de cada cliente, robusto, veloz y escalable, y con un diseño visualmente amigable, el cual podemos administrar fácilmente desde la barra superior de herramientas en el cual tendremos el Dashboard, que es donde encontramos el resumen general de cómo se encuentra en ese momento la cartera de cada cliente.

También encontramos la herramienta Gestionar, que es donde vamos a realizar todos los procesos de cobranza con cada cliente.

Con la herramienta tareas, podemos ver los seguimientos y compromisos que se van creando conforme a los logros alcanzados por cada uno de nuestros asesores desde el Callcenter.

Con la herramienta cargue e informes podemos descargar informes detallados de cada uno de los procesos de cada cliente en la recuperación de cartera.



CONFIDENCIAL

POLÍTICA DE USOS DE MEDIOS TECNOLÓGICOS

GRUPO REINCAR

Recuperadora y Normalizadora integral de cartera.

1 OBJETO, FINALIDAD Y AMBITO DE APLICACIÓN

El presente documento tiene por objeto regular la utilización de los medios y recursos tecnológicos propiedad de la empresa puestos a disposición de los trabajadores, así como garantizar la seguridad de la información de los clientes, la propia y el rendimiento, fiabilidad y privacidad de las comunicaciones; preservar la privacidad y seguridad del personal y en general garantizar el cumplimiento efectivo de las actividades y demás tareas administrativas que emanan del ámbito estrictamente laboral.

Ambas partes son conscientes de la necesidad de utilización de las herramientas de las tecnologías de la información y las comunicaciones en el proceso laboral. Los usuarios de los recursos tecnológicos son responsables de no abusar en su utilización, de mantener el respeto a los derechos de los demás usuarios, por lo que manifiestan estar de acuerdo en el establecimiento de las normas que deben regir su utilización y someterse a su cumplimiento.

Este documento será de aplicación a todos los usuarios que tengan acceso a la utilización de los recursos tecnológicos propiedad de la empresa Grupo Reincar SAS. Dicho acceso incluye todos los sistemas de información propiedad de la empresa, los equipos informáticos (PC´s, portátiles, servidores), infraestructuras de comunicaciones, conexión a redes internas o externas, terminales, software, hardware, servicios telemáticos, infraestructura de redes, accesos a Internet y todos los recursos a los que tenga acceso el personal o usuario para el cumplimiento de tareas asignadas en el ámbito laboral.

1.1 Definiciones

Sistemas de comunicaciones: Abarcan sistemas de telefonía fija, móvil, telefonía IP, correo electrónico, sistemas de mensajería instantánea o cualquier otro medio electrónico que la Empresa pone a disposición de su personal para comunicarse en el ámbito laboral.

Recursos tecnológicos: Elementos que integran las Tecnologías de la Información y la Comunicación, tales como dispositivos electrónicos, software, hardware, cableado, nodos

CONFIDENCIAL

y acceso a redes públicas o privadas, servidores y en general toda la infraestructura utilizada por los sistemas de comunicación.

Política de uso: Conjunto de disposiciones que regulan la utilización aceptable de los recursos tecnológicos destinados al cumplimiento de los objetivos de la empresa y de la seguridad de la información.

Usuario o Empleado: Se refiere a todo el personal o recurso humano que utiliza dentro del ámbito laboral, los sistemas de comunicación y los recursos tecnológicos propiedad de la empresa.

Administrador de sistemas: Responsable de la gestión y administración de los equipos informáticos, así como de vigilar el estricto cumplimiento de la política de uso de medios tecnológicos.

Director Administrativo: Responsable de dirigir las medidas y acciones para el cumplimiento de la presente política, así como de resolver problemas e incidencias que emanen de la utilización de los recursos tecnológicos.

Posición de la empresa en cuanto al uso de herramientas y medios informáticos

Por el presente documento, la empresa establece la regulación del uso de los recursos tecnológicos a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal, los cuales quedan sujetos a esta política así como a los principios morales y éticos en la utilización de los recursos puestos a disposición del usuario para el desempeño de las actividades laborables.

Ambas partes reconocen que tienen conocimiento y asumen los compromisos, normas y reglamentos para el uso de los medios tecnológicos, tomando todas las medidas que correspondan para su estricto cumplimiento.

El uso inapropiado, abusivo, o que escape a los hábitos tolerados de los servicios de comunicación y de los medios tecnológicos será sancionado con la eliminación del acceso

CONFIDENCIAL

a los recursos, la aplicación de las sanciones disciplinarias derivadas por incumplimiento de los términos y condiciones que emanen de la relación laboral consignadas en el contrato de trabajo y por tanto de obligatorio cumplimiento, además de las sanciones legales establecidas en la normativa vigente aplicable.

La empresa podrá realizar las investigaciones y controles que resulten necesarios tanto de los equipos como de las herramientas facilitadas al usuario por parte de la empresa, lo que incluye entre otros el correo electrónico empresarial, dispositivos de tipo pda o blackberry, dentro del ámbito de potestades de control del empresario.

El control y acceso a los medios facilitados por la empresa, incluyendo los documentos generados por los mismos y las comunicaciones que partan de los mismos podrá ser llevado a cabo sin una justificación específica, de forma temporal o permanente, dada cuenta la naturaleza de dichos medios como herramientas de producción facilitadas por la empresa.

El control de estos medios se llevará a cabo sin dañar y sin atentar contra la dignidad o intimidad del usuario, dada cuenta del conocimiento que tiene éste del objeto y la existencia del presente control y fiscalización a la que los usuarios son sometidos.

Las finalidades genéricas de este control son las siguientes:

- **PROTECCIÓN DEL SISTEMA Y RED INFORMÁTICA Y DE LOS EQUIPOS QUE LO CONFORMAN, A FIN DE PROTEGER LA INTEGRIDAD DEL SISTEMA Y LA SEGURIDAD DE LA INFORMACIÓN.**
- **PREVENCIÓN DE LA RESPONSABILIDAD FRENTE A TERCEROS.**
- **COMPROBACIÓN DEL CUMPLIMIENTO DE LAS OBLIGACIONES LABORALES DEL USUARIO.**
- **COMPROBACIÓN DE LA EXISTENCIA O NO DEL USO ABUSIVO DE LOS MEDIOS TECNOLÓGICOS FACILITADOS POR LA EMPRESA PARA USOS**

CONFIDENCIAL

PERSONALES DURANTE EL HORARIO LABORAL.

Por tanto todos los contenidos, informaciones, ficheros almacenados en el mismo, incluida la información temporal, podrán ser accedidos por parte de la empresa o de los responsables designados al efecto.

El alcance de estos procedimientos de control o inspección se notificarán a todos los usuarios de tal forma que quede constancia pública de los mismos.

El presente documento plantea una serie de recomendaciones que regulan el adecuado uso y disponibilidad de los recursos informáticos, comprometiéndose la empresa a su difusión hacia todo el personal laboral. Los usuarios que de forma reiterada, deliberada o por negligencia los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se estimen oportunas.

1.2 Propiedad y especificaciones de los sistemas operativos

Los usuarios se comprometen a respetar la integridad de los recursos y sistemas de información a los que tengan acceso para el cumplimiento de las tareas dentro del ámbito exclusivamente laboral, quedando estrictamente prohibido llevar a cabo o facilitar a cualquier tercero la comisión de cualquiera de los siguientes supuestos:

- **ALTERAR DE FORMA TOTAL O PARCIAL LOS COMPONENTES HARDWARE, SOFTWARE Y LAS CONFIGURACIONES DE LOS SISTEMAS OPERATIVOS DE LOS EQUIPOS INFORMÁTICOS ASIGNADOS AL MISMO USUARIO O A OTROS USUARIOS, SIN LA DEBIDA AUTORIZACIÓN.**
- **UTILIZAR APLICACIONES INFORMÁTICAS QUE SATUREN LAS REDES, LOS SERVIDORES O QUE ENTORPEZCAN EL FUNCIONAMIENTO DE LOS EQUIPOS INFORMÁTICOS.**
- **HACER MODIFICACIONES DE PRIVILEGIOS O PERMISOS SIN AUTORIZACIÓN DEL ADMINISTRADOR DE SISTEMAS.**

CONFIDENCIAL

- **OCASIONAR DAÑOS FÍSICOS O LÓGICOS, POR MAL USO O NEGLIGENCIA DE LOS EQUIPOS INFORMÁTICOS, APLICACIONES, HERRAMIENTAS INFORMÁTICAS Y TODO DISPOSITIVO O MEDIO TECNOLÓGICO.**

- **DESARROLLAR O USAR INTENCIONAL O ACCIDENTALMENTE PROGRAMAS MALICIOSOS O ACCESOS A RECURSOS RESTRINGIDOS POR EL ADMINISTRADOR DE SISTEMAS.**

- **NO GUARDAR CON LA DEBIDA DILIGENCIA LAS CLAVES, CONTRASEÑAS, NOMBRES DE USUARIO O CUALESQUIERA OTROS IDENTIFICADORES QUE PUDIERAN FACILITARSE AL TRABAJADOR PARA UTILIZAR CUALQUIERA DE LAS HERRAMIENTAS, O PARA ACCEDER A LOS EQUIPOS O SISTEMAS DE LA EMPRESA.**

1.3 Acceso a los equipos

- **ACCESO DE LOS USUARIOS**

Todo acceso a los equipos y sistemas de información estará controlado y autorizado por el administrador de sistemas. Queda estrictamente prohibido para el usuario, intentar acceder a los sistemas o recursos a los que no tenga autorización expresa por parte del administrador de sistemas.

Los usuarios se obligan a respetar los derechos de terceros en los sistemas de uso compartido, comprometiéndose a no acceder a la información privada de otros usuarios, sin previa autorización. Así mismo, los usuarios se comprometen a no compartir ficheros o documentos de cualquier tipo con otros usuarios, sin implementar las medidas necesarias que garanticen la seguridad de la información y de los sistemas operativos. Toda suplantación de identidad será sancionada de acuerdo a la normativa vigente que resulte de aplicación.

Todo usuario autorizado tiene acceso a los sistemas informáticos mediante un nombre de

CONFIDENCIAL

usuario y contraseña personal e intransferible, comprometiéndose a tratarla con la máxima diligencia y confidencialidad, siendo el único responsable del buen uso de la misma. El titular autorizado será responsable único y directo de todo lo ejecutado en el sistema bajo su nombre de usuario y contraseña. Así mismo, quedan estrictamente prohibidos los intentos reiterados, por cualquier medio, para obtener el acceso a contraseñas de otros usuarios sin su consentimiento.

Queda prohibido divulgar por cualquier medio las claves de acceso a cualquiera de los servicios que se faciliten a los empleados. Todos los nombres de usuario, contraseñas, claves de acceso y demás identificadores facilitados al usuario tendrán el carácter de confidencial, resultando personales e intransferibles. Los usuarios se comprometen a dar aviso al administrador de sistemas y/o al Director Administrativo de forma inmediata de cualquier incidencia o anomalía detectada en los accesos a los sistemas de información o en la seguridad de los mismos.

Dejar un equipo sin bloqueo durante el brake, almuerzo, o pausas, es equivalente a no utilizar contraseña de acceso. Los asesores deben bloquear el equipo al momento de levantarse del puesto. Asimismo, debemos indicar al asesor que deben apagar los equipos al acabar la jornada laboral.

- **ACCESOS DEL ADMINISTRADOR DE SISTEMAS**

El administrador de sistemas se obliga a actuar con absoluta diligencia, guardando total confidencialidad sobre los datos, documentos, y demás informaciones a las que pudiere tener acceso en el ejercicio de sus tareas. A título ejemplificativo, pero no limitativo se pueden incluir los siguientes:

- **ACCESO A LOS EQUIPOS Y SISTEMAS DE INFORMACIÓN PARA LLEVAR A CABO TAREAS DE MANTENIMIENTO.**

- **ACCESO A LOS EQUIPOS, SISTEMAS DE INFORMACIÓN Y DOCUMENTOS ELECTRÓNICOS POR MOTIVOS DE SEGURIDAD.**

CONFIDENCIAL

- **AUTORIZAR LOS ACCESOS DE LOS USUARIOS A LOS SISTEMAS DE INFORMACIÓN QUE REQUIEREN PARA EL CUMPLIMIENTO DE SUS TAREAS, ASÍ COMO A LOS EQUIPOS INFORMÁTICOS, EN CONJUNTO CON EL DIRECTOR ADMINISTRATIVO.**

- **ACCESO A LOS EQUIPOS, REDES O SISTEMAS DE INFORMACIÓN POR INCIDENCIAS EN LA SEGURIDAD DE LA INFORMACIÓN.**

En cualquier caso, tanto el administrador de sistemas, auxiliares de sistemas como el Director Administrativo tienen el deber y la obligación de guardar con absoluta confidencialidad toda la información a la que tengan acceso para el cumplimiento de sus actividades, quedando estrictamente prohibido comunicarla o facilitarla, directa o indirectamente a ningún tercero.

2 ASIGNACIÓN DE ROLES, USUARIOS, CONTRASEÑAS Y ENTREGA DE IMPLEMENTOS

2.1 Existen 19 diecinueve tipos de roles en Grupo Reincar:

2.1.1 Líder TIC: acceso pleno a toda la información, aplicaciones, correo e internet.

2.1.2 Auxiliar TIC: acceso a las carpetas necesarias, aplicaciones, correo con restricciones e internet sin restricciones

2.1.3 Gerente: acceso a las carpetas solicitadas, aplicaciones, correo sin restricción e internet.

2.1.4 Director Administrativo y Financiero: acceso a las carpetas solicitadas, aplicaciones, correo sin restricción e internet.

2.1.5 Director Comercial: acceso a las carpetas solicitadas, aplicaciones, correo sin restricción e internet.

CONFIDENCIAL

2.1.6 Líder Capital Humano: acceso a las carpetas solicitadas, aplicaciones, correo sin restricción e internet.

2.1.7 Contador: acceso a las carpetas solicitadas, aplicaciones, correo sin restricción e internet.

2.1.8 Auditor: acceso mediante solicitud al administrador del sistema a carpetas necesarias para realizar el proceso de auditoría de la gestión de cobro, correo y paginas autorizadas a Internet. No tiene habilitado consola dos, paint, bloc de notas, click derecho, panel de control, propiedades del internet, discos extraíbles y unidades de cd.

2.1.9 Coordinador de cartera: accesos a las carpetas relacionadas con la cartera a su cargo, correo institucional sin restricciones, páginas web de consultas que no permitan la filtración de información. No debe tener habilitado: panel de control, discos extraíbles y unidades de cd

2.1.10 Coordinador de cartera avvillas: accesos a las carpetas relacionadas con la cartera a su cargo, correo institucional con restricciones, páginas web de consultas que no permitan la filtración de información. No debe tener habilitado: click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles y unidades de cd. Tiene acceso a la impresora.

2.1.11 Coordinador de cartera avvillas Bogotá: accesos a las carpetas relacionadas con la cartera a su cargo, correo institucional con restricciones, páginas web de consulta que no permitan la filtración. No debe tener habilitado: click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles y unidades de cd. Tiene acceso a la impresora.

2.1.12 Auxiliar administrativo: acceso a carpetas y páginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Acceso Correo electrónico e impresora. No debe tener habilitado click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles, unidades de cd, panel de control.

CONFIDENCIAL

2.1.13 Gestor: acceso a carpetas y páginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Ningún correo electrónico que no esté previamente autorizado por el coordinador, ni aplicaciones. No debe tener habilitado click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles, unidades de cd, panel de control, accesos a los discos locales e impresoras.

2.1.14 Gestor fna: acceso a carpetas y paginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Ningún correo electrónico ni aplicaciones. Debe tener restringido modificaciones en el panel de control, instalación de aplicativos discos extraíbles, unidades de cd e impresoras.

2.1.15 Gestor fna usuario local: acceso a carpetas y páginas web de consultas que autorice el coordinador y que no presenten riesgo de filtrado de información. Ningún correo electrónico ni aplicaciones. Tiene las restricciones configuradas de un usuario local estándar de Windows.

2.1.16 Gestor Banco Bogotá: acceso a carpetas y páginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Ningún correo electrónico que no esté previamente autorizado por el coordinador, ni aplicaciones. No debe tener habilitado click derecho, consola dos, bloc de notas propiedades del internet, discos extraíbles, unidades de cd, panel de control, accesos a los discos locales e impresoras.

NOTA: Las asesoras tienen habilitado paint ya que deben generar pantallazos para envío de propuestas fuera de políticas.

2.1.17 Abogado: accesos a las carpetas relacionadas con la cartera a su cargo, correo institucional, páginas web de consultas que no permitan la filtración de información. No debe tener habilitado: click derecho, paint, consola dos, bloc de notas, propiedades del internet, discos extraíbles y unidades de cd.

2.1.18 Auxiliar Operativo: acceso a carpetas y páginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Acceso a Correo

CONFIDENCIAL

electrónico. No debe tener habilitado click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles, unidades de cd, panel de control, accesos a los discos locales. Tiene habilitada la impresora.

2.1.19 Analista de datos: acceso a carpetas y páginas web de consulta que autorice el coordinador y que no presenten riesgo de filtrado de información. Acceso a Correo electrónico. No debe tener habilitado click derecho, paint, consola dos, bloc de notas propiedades del internet, discos extraíbles, unidades de cd, panel de control, accesos a los discos locales. Tiene acceso a la impresora.

2.2 Creación, modificación y eliminación de usuarios dentro del dominio:

La creación o modificación de un usuario para el acceso al servidor de dominio y de datos en las oficinas de Grupo Reincar SAS debe seguir los siguientes pasos:

1. El líder de área vía correo electrónico envía el formato GR-FR55 Formato de solicitud de usuario, debidamente diligenciado al área de TIC, señalando la cartera en la que el gestor se va a desempeñar e indicando las carpetas necesarias y que tipo de acceso si es solo de lectura o escritura, si es compartida con otros usuarios o si el acceso es privado solo para ese usuario y a que área necesita ingreso para la creación de la huella. Es necesario especificar si el nuevo usuario requiere acceso a alguna página web en particular y adjuntar el link para que el área de TIC evalúe las vulnerabilidades de seguridad de la información y apruebe de acuerdo a la política de seguridad de la información.

Al recibimiento del correo el área de TIC procede a realizar la creación del usuario, el cual debe estar compuesto por la inicial del primer nombre seguida por el primer apellido. Por ejemplo, lramos. al momento de crear el usuario el área de TIC debe revisar en la configuración del servidor que la opción de la cuenta: “el usuario debe realizar el cambio de contraseña en el siguiente cambio de sesión “quede activada, para que el funcionario realice el cambio de contraseña.

CONFIDENCIAL

El área de TIC debe garantizar que el usuario se cree de acuerdo a las normas de seguridad de información y a los perfiles creados en el punto anterior.

Las contraseñas deben cumplir con los requerimientos de complejidad que tiene Windows Serve de acuerdo a la política de contraseñas seguras contenido en el Manuel de políticas de seguridad de la información TC-IN02 Manual de Políticas de Seguridad de la Informaciónv9.

Cuando se presente el ingreso de un nuevo líder de área en la empresa el formato GR-FR55 Formato de Solicitud de Usuario será diligenciado por el área de Capital Humano.

Cabe mencionar que solo se realizara la creación de usuarios que tengan el formato GR-FR55 Formato Solicitud Usuariov1 diligenciado, sin importar que la solicitud sea realizada por los directivos.

Cuando un empleado salga a vacaciones o se encuentre incapacitado por más de 3 días, el jefe inmediato debe notificar mediante correo al líder TIC para la deshabilitación del usuario.

En caso de que se efectúe una terminación de contrato ya sea por despido o renuncia de cualquier colaborador el coordinador de cartera o jefe inmediato debe solicitar la eliminación del usuario vía correo electrónico al Líder de TIC mediante el Formato GR-FR55 Formato de creación modificación y eliminación de Usuario, cumpliendo con los criterios descritos en el formato.

La eliminación de la información se realizara a través de la herramienta hardwipe para garantizar que se realice el proceso de borrado seguro y se guardara evidencia en una carpeta del fileserver ubicada en la ruta \\192.168.2.252\tic´s\gestion de identidad de usuarios\eliminación de usuarios.

2.3 Creación de usuarios herramienta B2chat.

CONFIDENCIAL

La creación de un usuario para el ingreso a la herramienta B2chat debe seguir los siguientes pasos:

1. Solicitud vía correo electrónico por parte del coordinador de cartera al área de TIC para su respectiva creación, informando el tipo de cartera y que asesor tendrá acceso a la aplicación.

2. El área de TIC creará el usuario y la clave de ingreso a la herramienta.

3. El área de TIC se desplazará hasta el equipo del colaborador para ingresar las credenciales.

2.4 Creación de usuarios de VPN

La solicitud de creación de usuario de VPN se realiza al área de TIC a través del formato GR-FR55 Formato de creación modificación y eliminación de Usuario el cual debe ser diligenciado por el jefe inmediato al ingresar o al momento en que sea necesaria dicha configuración.

El área TIC realiza la creación de la VPN y la generación de las credenciales de acceso a través de la herramienta bitwarden para mayor seguridad.

2.5 Gestión de incidencias

Todas las incidencias en la utilización de los recursos y medios tecnológicos de la empresa, o que, por cualquier circunstancia, directa o indirecta que pueda comprometer la Seguridad de la Información, deberá ser notificada con la mayor brevedad que sea posible al director Administrativo y al líder TIC.

El líder TIC será el encargado de llevar a cabo un registro, diagnóstico y seguimiento de todas las incidencias comunicadas por los usuarios. Asimismo, deberá mantener actualizado el registro de incidencias donde se especificará el tipo de incidencia y la resolución de las mismas, comprobando periódicamente que las incidencias son resueltas

CONFIDENCIAL

y la Seguridad de la Información queda garantizada.

Se analizará si la falla realmente es una incidencia que afecte las propiedades de la seguridad de la información las cuales son la confidencialidad, disponibilidad e integridad.

Para el control particular de este tipo de incidencias se debe registra en el formato TC-FR04 Tratamiento de incidentes técnicos que afecten la seguridad y de acuerdo a la gravedad del hecho se debe generar una acción correctiva o preventiva a la cual se le debe hacer seguimiento mensual.

2.6 Seguridad, confidencialidad y protección de datos personales

Se regirá a partir de la política de protección de datos personales TC-IN03 política de protección de datos personales

2.7 Entrega implementos de sistemas.

Procedimiento entrega implementos de sistema

3 El responsable de TICS o asistente de TICS, entrega al colaborador el equipo de cómputo el cual debe tener los aplicativos a utilizar para la gestión según el cargo y las restricciones establecidas para el cumplimiento de la política de seguridad de la información, el área de TIC debe firmar el formato GR-FR26 Hoja de vida equipos.

4 Para la entrega de diadema, la persona quien recibe debe firmar el formato GR-FR06 Entrega de diademas. Y en el caso de entrega de celular, el colaborador debe fir mar el formato GR-FR14 CARTA DE ENTREGA CELULARES.

5 El asistente o responsable de TICS procede a escanear y posteriormente el documento físico queda guardado en las AZ.

3. UTILIZACIÓN DEL CORREO ELECTRÓNICO

3.1 USO DEL CORREO PERSONAL

El uso de cuentas de correo personales, basadas en acceso a web, tipo hotmail, yahoo, no podrán ser utilizadas bajo ninguna circunstancia. Las cuentas de correo corporativo serán autorizadas por el coordinador de cartera.

3.2 Uso del correo empresarial

El correo electrónico empresarial, las listas de distribución, los contactos, son herramientas cuyo objetivo principal es facilitar la comunicación corporativa exclusivamente en el ámbito laboral.

Las partes acuerdan que la utilización de los servicios de comunicación y difusión de la información quedará sujeta a las siguientes condiciones:

- **SOLO USUARIOS AUTORIZADOS PODRÁN TENER UNA CUENTA @REINCAR.COM.CO**
- **QUEDA PROHIBIDO LA UTILIZACIÓN DE LAS HERRAMIENTAS DE COMUNICACIÓN PARA USO PERSONAL. ASI MISMO, SE PROHÍBE EL ENVÍO DE CORREO ELECTRÓNICO CON MENSAJES OFENSIVOS, AMENAZANTES, CONTENIDO ILÍCITO O FRAUDULENTO.**
- **QUEDA PROHIBIDO LA UTILIZACIÓN DEL CORREO ELECTRÓNICO CON FINES LUCRATIVOS O COMERCIALES, PARA USO RECREATIVO O CUALQUIER OTRO QUE NO GUARDE RELACIÓN CON LA ACTIVIDAD LABORAL.**
- **SE PROHÍBE EL USO DEL CORREO PROFESIONAL PARA LA INSCRIPCIÓN A "NEWSLETTER", GRUPOS DE NOTICIAS, O SIMILARES QUE NO ESTÉN DIRECTAMENTE RELACIONADAS CON LA ACTIVIDAD PROFESIONAL**

CONFIDENCIAL

DESARROLLADA POR EL USUARIO Y QUE RESULTEN DE PLENA CONFIANZA.

- **LAS LISTAS DE DISTRIBUCIÓN DE CORREO SOLO PODRÁN SER UTILIZADAS PARA LOS FINES PROPIOS DE LA EMPRESA, Y NUNCA CON FINES PUBLICITARIOS, COMERCIALES O DE ÍNDOLE PERSONAL QUE NO VAYAN RELACIONADAS CON ACTIVIDADES PROPIAS DEL DESEMPEÑO LABORAL.**

- **ESTÁ PROHIBIDO ACCEDER SIN AUTORIZACIÓN A LAS COMUNICACIONES QUE CIRCULAN POR LA RED, ASÍ COMO SU MANIPULACIÓN, DESTRUCCIÓN Y APROPIACIÓN INDEBIDA.**

- **ESTÁ PROHIBIDO EL ENVIÓ DE CORREOS MASIVOS, LOS CORREOS SOLO DEBEN IR DIRIGIDOS A LA PERSONA INTERESADA, A EXCEPCIÓN DE CLIENTES QUE TENGAN MAS DE 2 CUENTAS DE CORREO.**

- **ESTA PROHIBIDO EL INTERCAMBIO DE ARCHIVOS CON INFORMACIÓN DE LOS DEUDORES ENTRE LOS COORDINADORES DE CARTERA Y LOS AUXILIARES ADMINISTRATIVOS.**

3.3 Estatus legal de los mensajes

Todos los mensajes enviados por correo electrónico corporativo deberán contener el aviso legal de conformidad con el Código Penal, que establece como delito al que para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento, se apodere de mensajes de correo electrónico, así como para aquel que descubriere, revelare o cediere datos reservados de personas jurídicas sin el consentimiento de sus representantes.

Asimismo, se deberá manifestar expresamente la obligación de abstenerse de un tratamiento no autorizado de la información, en caso de que el correo hubiese sido enviado por error a otro destinatario.

CONFIDENCIAL

3.4 Información que debe incluirse en el mensaje y firma

Todo correo electrónico emitido desde cualquier cuenta electrónica administrada por la empresa, deberá ser identificado bajo un título relacionado con el contenido e incluir la siguiente información:

- **RAZÓN SOCIAL DE LA ENTIDAD.**
- **NOMBRE COMPLETO DEL EMISOR.**
- **DIRECCIÓN.**
- **AVISO LEGAL.**

3.5 Uso de correo encriptado

Para el envío de información confidencial con los clientes es necesario el uso del correo cifrado para encriptar datos. Las políticas de cifrado de correos serán aplicadas y configuradas dependiendo del tipo de cartera.

3.6 Uso de correo electrónico masivo

Para el envío de correo masivo los coordinadores deben tener en cuenta lo siguiente:

1. Validación de los correos de los deudores registrados en el demográfico.

2. Confirmar la autorización del titular para envió de información en caso de que el correo electrónico se actualice en la gestión de cobro.

3. Está prohibido pegar en la plantilla información con datos diferentes a los requeridos por el deudor.

4. SEGURIDAD PERIMETRAL

La seguridad perimetral de la plataforma tecnológica es manejada a través de un firewall

CONFIDENCIAL

Microtik, en este dispositivo se configura y administra toda la red de datos, incluyendo la seguridad necesaria para evitar el acceso de intrusos.

El Microtik recibe el enlace del servicio de Internet UNE y lo distribuye a los Switches, los cuales se interconectan con los servidores y equipos de cómputo. El direccionamiento IP es entregado por el microtik.

4.1 RESTRICCIONES A LA NAVEGACIÓN POR INTERNET

Queda prohibida la utilización de la red para navegar por sitios de Internet para otros usos que no sean los permitidos para el desempeño de su actividad. Una lista con las direcciones (lista blanca) contendrá las direcciones url autorizadas.

La navegación por Internet utilizará hardware y software (microtik) adecuado para filtrar los accesos a los sitios que a consideración del administrador de sistemas sean inapropiados para la empresa, o innecesarios para la actividad laboral o que puedan presentar un riesgo a la seguridad de la información

La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del usuario emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación. Las cuales se contemplan en el contrato y reglamento interno de trabajo.

Está estrictamente prohibido el acceso a páginas con contenidos ilícitos, material pornográfico, de contenido racista, sexual, o cualquier material que atente contra la dignidad y los principios morales.

La administración del Mikrotik se realiza a través del software Winbox que se encuentra en la carpeta del servidor de archivos llamada instaladores. El usuario y clave para conectarse a este se encuentran en poder del director administrativo y el ing. de sistemas. Por medio de este firewall se regula el acceso a las páginas web de Bogotá y Bucaramanga.

CONFIDENCIAL

4.2 CONEXIONES VPN

El Microtik permite y administra la configuración de las conexiones de VPN entre las sedes, así como también las conexiones de VPN clientes y conexiones externas site to site.

4.3 BLOQUEO DE PUERTOS Y APLICACIONES

Desde el Microtik se realiza todo el bloqueo de puertos conocidos con el fin de evitar escaneos y posibles ataques a la red. También se realiza el bloqueo de aplicaciones como Team viewer y demás aplicaciones que permiten el acceso remoto a la red.

Este firewall cuenta con soporte técnico directamente con la empresa doctor Linux quien realizo la instalación y configuración.

Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven de la utilización de programas de intercambio de archivos, será sancionado por la legislación vigente aplicable, así como por las sanciones impuestas por incumplimiento en la relación laboral.

4.4 ANTIVIRUS

Los equipos de cómputo cuentan con antivirus licenciado Kaspersky Endpoint security cloud el cual les proporciona seguridad ya que incluye herramientas de ciberseguridad tales como:

Protección contra ransomware: protege el sistema de los cryptolockers y ransomware

Protección frente a amenazas de archivos, Internet y correos electrónicos: Libera el sistema corporativo del malware y las nuevas ciberamenazas avanzadas.

Cloud Discovery: Detecta y restringe el uso no autorizado de recursos en la nube, las redes sociales y las plataformas de mensajería.

Control web y de dispositivos. Controla qué sitios externos, unidades USB y redes Wi-Fi tengan acceso permitido.

CONFIDENCIAL

Data Discovery. Analiza qué datos se tiene almacenados en la nube para evitar la pérdida de datos corporativos.

Microsoft Office 365. Cuenta con protección completa para todas las aplicaciones integradas de Microsoft Office 365.

Endpoint Detection and Response. Responde a las ciberamenazas y combate los ataques complejos.

Análisis de IoC. Permite buscar proactivamente posibles amenazas en la infraestructura de TI.

Administración de parches. Mantiene todos los dispositivos, tanto locales como remotos, actualizados con los parches y las actualizaciones más recientes.

Para la administración del antivirus se tiene una plataforma centralizada lo que posibilita recopilar y detectar amenazas en cada uno de los equipos conectados dentro y fuera de la red de la empresa y de esta forma responder de manera oportuna.

Adicionalmente tenemos configurados unos informes que se generan de forma semanal sobre amenazas detectas y vulnerabilidades los cuales son enviados vía correo al responsable TICS para su respectiva revisión.

5. COPIAS DE SEGURIDAD

Se tiene un plan de copias de seguridad para las oficinas de Bucaramanga y Bogotá configurado de la siguiente manera:

5.1 Copia de seguridad disco externo de Bucaramanga: Esta copia de seguridad es de tipo diferencial y aloja toda la información de la empresa, se ejecuta de lunes a sábado a las 6:30 p.m. y se almacena en un disco externo de 2 TB, el cual permanece conectado al servidor. Cuando el disco se llena se procede a eliminar la información y a iniciar nuevamente la copia.

CONFIDENCIAL

5.2 Copia de seguridad servidor oficina Bucaramanga: Esta copia de seguridad es de tipo completa, se ejecuta de lunes a sábado desde las 5:30 pm hasta las 11:00 p.m. y se almacena en un disco interno del servidor de dominio. En esta copia no se guardan históricos de días anteriores.

5.3 Copia de seguridad disco externo sede Bogotá: Esta copia de seguridad es de tipo diferencial, se ejecuta de lunes a sábado a las 10:00 p.m. y se almacena en un disco externo de 1 TB, el cual permanece conectado al servidor en Bogotá. Cuando el disco se llena se procede a eliminar la información y a iniciar nuevamente la copia.

5.4 Copia de seguridad servidor oficina Bogotá: Esta copia de seguridad es de tipo completa, se ejecuta de lunes a sábado a las 8:00 pm y se almacena en un disco interno del servidor de dominio. En esta copia no se guardan históricos de días anteriores.

5.5 Copia seguridad Llamadas: Las llamadas de Bucaramanga se guardan en los discos duros de los servidores internos y también en un disco duro externo, esto con el fin de que si el servidor de llamadas presenta indisponibilidad podamos acceder a las grabaciones que sean requeridas por los clientes y el área de auditoría.

Las copias de seguridad de las llamadas se guardarán por 10 años. Una vez se llene un disco este debe ser retirado y guardado en la caja de seguridad.

Las copias de seguridad de las llamadas de la oficina de Bogotá se encuentran en los discos internos del servidor. Una vez se llena se almacena, se trasladan a un disco duro externo, se etiqueta por fecha y se resguarda bajo llave, cabe mencionar que este disco externo está bajo custodia del director Administrativo de la oficina de Bogota.

5.6 Copias de seguridad de las bases de datos: Esta copia de seguridad se realiza en un disco externo para el servidor de llamadas Issabel de forma automática y se realiza en horas de la noche quedando así la copia de la base de datos del día anterior, para el caso del servidor Reincarapp se realiza de forma manual y se aloja en un servidor de archivos en horas de la noche quedando así la copia de la base de datos del día anterior.

CONFIDENCIAL

De manera semestral se realiza la restauración de la base de datos del Reincarapp y como evidencia se genera un informe.

5.7 Copias de seguridad sistemas operativos: Esta copia de seguridad se realiza de manera automática todos los meses en los equipos de cómputo y de manera mensual el área de auditoria valida la restauración de los sistemas operativos.

5.8 Copia de seguridad disco externo resguardado fuera de la oficina Bucaramanga: En esta copia de seguridad se almacena toda la información administrativa utilizada en Grupo Reincar por medio de un disco duro externo, el cual es entregado al director administrativo para su respectivo alojamiento fuera de la oficina. No debe incluir información de los deudores.

El disco dispuesto para este backup está cifrado mediante BitLocker para proteger los datos del acceso no autorizado y la clave para descifrar el disco se encuentra custodiada por el responsable TIC.

El proceso se realiza de forma semestral de la siguiente manera:

Salida del disco externo copia de seguridad:

- Para la salida del disco se levanta un acta de reunión donde se deja constancia que el disco fue entregado por el responsable TIC al director Administrativo para su respectiva salida.
- El director Administrativo es el encargado de realizar el transporte del disco y dejarlo en el sitio de disposición final (caja fuerte) para su respectivo resguardo

Entrada del disco externo copia de seguridad:

- El ingreso del disco duro externo está asociado al acta de reunión firmada en la salida, con el fin tener evidencia que el disco fue entregado al responsable TIC de forma satisfactoria, en esta acta se deja un espacio de compromisos donde se

CONFIDENCIAL

registra la fecha y estado del disco al momento del ingreso

- Una vez recibido por el responsable TIC, el disco se aloja en el cuarto técnico y se conecta al equipo dispuesto para la realización de las copias de seguridad, se valida que el disco se encuentre cifrado y con la información que se había realizado en el backup anterior.

6. USO DE LAS BASES DE DATOS PROCEDIMIENTO DE ENTREGA Y BORRADO SEGURO.

Las bases de datos son asignadas por el Banco o Cliente y por medio de una ruta o VPN segura, correo electrónico encriptado o cd-DVD entregado personalmente con remisión o por medio de correo certificado.

Estos datos se albergan en una carpeta protegida en el servidor respectivo y se asignan los permisos necesarios para el coordinador encargado.

Si la asignación de la cartera es para un mes esta debe ser recibida en los primeros días y deberá ser borrada tan pronto se hayan confirmado los pagos y se haya recibido la nueva asignación.

Luego el coordinador designa a cada gestor los datos de las obligaciones generando un archivo único para cada gestor que debe estar guardado en una carpeta donde solo el coordinador y el gestor tengan acceso. Al cabo del mes estos archivos deben ser eliminados. Solo deben existir archivos del mes vigente.

Una vez al mes la auditoría de seguridad de la información buscará bases de meses anteriores para mantener el control sobre las bases vigentes.

En el caso en que se detecten daños en los discos duros, se procede a realizar el proceso de formateo de bajo nivel a través de la herramienta HDD Low Level Format De igual forma se realiza la destrucción física del disco utilizando un martillo y de esta forma garantizar que la información contenida allí sea irrecuperable.

CONFIDENCIAL

Cada vez que se borre información de los discos duros o la información que se encuentra almacenada en el servidor, se debe realizar por medio de la herramienta Hardwipe con el método de Gutmann para garantizar un borrado seguro, también se debe llevar un registro por medio de acta firmado por quienes participen en dicha eliminación.

7. PROHIBICIÓN DEL USO DE HERRAMIENTAS Y REDES P2P

El servidor de dominio debe estar programado para que no admita la instalación de ningún programa sin embargo queda estrictamente prohibida la instalación de cualquier tipo de programa P2P, o cualquier otra aplicación para el intercambio de archivos que saturen el ancho de banda de la conexión a Internet, impidiendo el acceso a los demás usuarios o entorpeciendo las conexiones a la Red.

Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven de la utilización de programas de intercambio de archivos, será sancionado por la legislación vigente aplicable, así como por las sanciones impuestas por incumplimiento en la relación laboral.

8. PROHIBICIÓN DE USO Y/O INGRESO DE EQUIPOS PERSONALES

Está prohibido el ingreso de equipos de cómputo, equipos celulares, tablets, relojes inteligentes, cámaras fotográficas y cualquier otro medio físico en el cual se pueda filtrar información al Call Center, con el fin de garantizar la seguridad de la información de los clientes.

El ingreso de estos equipos acarrea sanciones disciplinarias y legales las cuales están dispuestas en el reglamento interno de Grupo Reincar.

9. RESTRICCIONES Y POLÍTICA DE USO DE SOFTWARE DE MENSAJERÍA INSTANTANEA

No se podrá instalar ningún software de servicio telemático o de mensajería instantánea sin autorización expresa del personal directivo, o del administrador de sistemas en su caso.

CONFIDENCIAL

Queda expresamente prohibido utilizar lenguaje obsceno, agresivo, ofensivo o discriminatorio en el envío de comunicaciones a través de servicios de mensajería instantánea.

La utilización del servicio de mensajería instantánea será de uso exclusivo para el cumplimiento de las actividades relacionadas dentro del ámbito laboral, quedando prohibida la transferencia de ficheros, imágenes o cualquier comunicación no relacionada con la actividad laboral.

Por seguridad, no se deberán descargar por ningún motivo ficheros adjuntos provenientes de remitentes desconocidos.

Queda prohibida la utilización del correo electrónico con fines lucrativos o comerciales, para uso recreativo o cualquier otro que no guarde relación con la actividad laboral.

El usuario será responsable de todo daño ocasionado en los equipos informáticos y sistemas de información, por negligencia, violación, o mal uso de los servicios de mensajería instantánea.

El software que la empresa utiliza se encuentra ubicado en los servidores de Bogotá y Bucaramanga en la carpeta instaladores y es el siguiente:

- Sistema operativo: Windows Ultimate: licenciado por medio de stiker y licencias.
- Procesador de texto y hojas de cálculo: open office
- Visualizador de pdf: adobe reader
- Descompresor de archivos: 7zip.
- Explorador: mozila, chrome e internet explorer.
- Acceso remoto: team viewer controlado que debe estar controlado siempre por el firewall.

CONFIDENCIAL

- Softphone: eyebeam
- Antivirus: Kaspersky Endpoint security pro y Kaspersky cloud free
- Optimizador: CCLEANER

10. PROGRAMAS Y DISPOSITIVOS DE CONTROL Y MONITORIZACIÓN

El administrador de sistemas pondrá en funcionamiento herramientas de control automatizadas para analizar y detectar los usos y comportamientos indebidos o ilícitos en la red, no implicado dicho control violación a la privacidad o a la intimidad de los usuarios.

Por cuestiones de seguridad toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por la empresa, podrá ser monitoreada y sujeta a controles y reportes sobre su uso, brindando información como: usuario, fecha de accesos, hora de accesos, bytes transferidos, almacenamiento de ficheros, acceso a los servidores, sitios visitados, tiempo de navegación por la red, entre otros.

Para el control de los virus informáticos es necesario mantener el proxy en los equipos y eliminar cualquier acceso no autorizado y necesario direcciones web y mantener instalado y actualizado en los equipos el programa Kaspersky o Windows defender

11. USO DE EQUIPOS INFORMÁTICOS FUERA DE LA EMPRESA

Las entradas y salidas de los equipos informáticos necesarios para el desarrollo de las actividades de la empresa, serán autorizadas por el área de TIC o director Administrativo por medio de dos cartas, una dirigida a la portería del edificio para permitir la salida del equipo y otra firmada por el empleado la cual irá firmada por él y archivada en la hoja de vida.

En todo caso se debe revisar que los equipos que salgan de la oficina por ejemplo para brigadas o eventos no cuenten con ningún tipo de información.

El responsable TIC implementará las medidas necesarias para garantizar la integridad y

CONFIDENCIAL

seguridad de los equipos informáticos fuera de la empresa mediante directivas de seguridad y credenciales de acceso.

12. USO DE LAS IMPRESORAS

A las impresoras solo podrán tener acceso los coordinadores de cartera y el personal administrativo y operativo. Ningún gestor de cobranza podrá tener acceso a las impresoras.

13. USO DEL CONTROL DE ACCESO BIOMETRICO

Los controles de acceso biométrico serán administrados por el director administrativo, el ing. de sistemas y los gerentes de las oficinas en Bogotá y Bucaramanga. Cada gestor deberá grabar su huella dactilar de dedo índice y pulgar para acceder al área de call center. El sistema registra la hora de llegada y salida y muestra el tiempo dentro del call center. El gerente de la oficina de Bogotá y director administrativo de Bucaramanga deberá generarlos informes necesarios para realizar el seguimiento de puntualidad a los gestores.

14. ASISTENCIA TÉCNICA, ENTREGA Y MANTENIMIENTO DE EQUIPOS

14.1 Asistencia técnica

Los requerimientos técnicos deben ser solicitados por medio del vínculo:

https://docs.google.com/forms/d/e/1FAIpQLSdpyrC-PdWeWcfx06CCqw4I9CzCDDmFgtCs73PVf_yVTS5Jyw/viewform
llenando el formato que se despliega. Si el requerimiento es de urgencia se debe realizar la solicitud directa al responsable TIC quien le dará la prioridad del caso.

14.2 Entrega de equipos

Para la realización de entrega de equipos o cambio se deben seguir los siguientes pasos:

1. Se debe configurar el equipo con las restricciones de seguridad según la cartera que pertenezca y el perfil del usuario.

CONFIDENCIAL

2. Se debe diligenciar el formato TC-FR04 Lista de chequeo configuración equipos de cómputo el cual se encuentra en el link https://docs.google.com/forms/d/e/1FAIpQLSe8y77G_3aRmi8Ah74xzh1Z81_tV5Uei56rKopjsr-DDS66bA/viewform , con el fin de validar las restricciones y garantizar el cumplimiento de la seguridad de la información.

3. Se debe crear o actualizar la hoja de vida del equipo mediante formato GR-FR26 Hoja de vida equipos según sea el caso.

4. Se debe realizar carta de entrega de diadema GR-FR06 ENTREGA DE DIADEMAS y actualizar Hoja de vida de diademas GR-FR27.

5. Se debe validar el funcionamiento del equipo.

Cada vez que un equipo se restablezca a fabrica, se realice proceso de formateo o se le realice el cambio de asesor se deben seguir los pasos anteriores.

14.3 Mantenimiento preventivo y correctivo

El mantenimiento preventivo y correctivo de los sistemas de información es realizado por el ingeniero y auxiliares TIC que brindan soporte a la empresa. Para el caso de los mantenimientos preventivos se tiene un cronograma en Google donde aparece las fechas de los mantenimientos que se van a realizar en el año, garantizando el correcto funcionamiento de equipos y servidores.

En el caso de los mantenimientos correctivos se tienen equipos de respaldo que sirven de contingencia en caso de presentarse falla por hardware o software y se deba restablecer el equipo o una de sus partes deba ser reemplazada.

15. USO DE LAS LICENCIAS DE SOFTWARE

Los usuarios están obligados a respetar las condiciones de licencia y copyright del software instalado en los equipos informáticos, siendo responsables de su adecuada utilización.

CONFIDENCIAL

Todo software protegido por copyrights no podrá ser copiado, ni se podrá disponer de cualquier información protegida por los derechos de autor que esté en formato electrónico en el equipo de cualquiera de los usuarios.

Los usuarios serán responsables de todo software instalado en sus equipos sin autorización expresa del administrador de sistemas, así como de uso y en su caso, de los daños que causen a los equipos o sistemas de información que deriven de su uso o instalación.

Cualquier actividad que infrinja las leyes de la propiedad intelectual, incluyendo los derechos de autor, marcas o derechos registrados y el de su reproducción será sancionado por la normativa.

16. USO DE LOS FORMULARIOS DE GOOGLE

Para la consolidación de información del estado de la cartera a nivel general con la información de cada uno de los gestores, se puede utilizar la herramienta de formularios de google de la siguiente manera:

- Asignar al coordinador de cartera acceso y clave de usuario al correo reincarbogota@gmail.com y reincarbucaramanga@gmail.com respectivamente o si es necesario en otra ubicación o coordinación, solicitarlo al director administrativo. Estas cuentas solo deben ser consultadas por los Coordinadores de cartera y se rigen bajo todas las políticas de confidencialidad y seguridad de información.

- Dar acceso al link del formulario a los gestores y revisar que solo accedan a este y no a alguna otra extensión de google.

- Para encontrar los datos que subieron los gestores. Se debe buscar en la consola de administración de la cuenta la aplicación drive y en la carpeta Reporte Diario buscar el archivo de base de cálculo reporte de recuperación (Respuestas).

- Realizar la descarga e ingresar la información a la plantilla que resume la

CONFIDENCIAL

información por tipo de cartera.

- Analizar la información y/o enviar al Funcionario del cliente que solicita la información.

17. CONSECUENCIAS DERIVADAS DEL MAL USO DE LOS MEDIOS O RECURSOS TECNOLÓGICOS

Los usuarios se comprometen a colaborar con el administrador de sistema para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos.

Toda incidencia detectada en los equipos informáticos, así como en los sistemas de información, podrán derivar en la suspensión o restricción del acceso o uso de los servicios al usuario, así como la aplicación de las medidas que el Director Administrativo considere oportunas al incumplimiento de lo establecido en el presente documento, del contrato de trabajo y de la legislación laboral actual.

18. TRANSFERENCIA SEGURA DE ARCHIVOS FTP

En caso de que el cliente cuente con un servidor de transferencia de archivos FTP para el intercambio de información, se utilizará la herramienta WinSCP para llevar dicho intercambio. La configuración de la herramienta la realizará el área de Sistemas con la configuración y datos de acceso entregados por el cliente.

Una vez configurada la aplicación, se verifica el acceso a la carpeta compartida. Cabe resaltar que la seguridad del sitio FTP será manejada por el cliente, así como también los permisos para copiar y pegar información.

En el momento que el coordinador acceda al sitio será el responsable del manejo de la información contenida y deberá atender las recomendaciones informadas por el cliente.

19. TRABAJO REMOTO

CONFIDENCIAL

Debido a la pandemia presentada a nivel mundial por causa del virus COVID-19 se hizo necesario implementar la modalidad de trabajo en casa, dando cumplimiento a la política de seguridad de la información y garantizando el funcionamiento de los aplicativos necesarios para la gestión de cobro.

Para llevar a cabo esta implementación al asesor se le asignó el mismo equipo de cómputo que utilizaba en la oficina, de igual forma el Ing. De sistemas y los auxiliares antes de la entrega validaron que estuvieran activas las restricciones de seguridad en el equipo a través del formato TC-FR04 Lista de chequeo configuración equipos de cómputo.

La entrega e instalación de los equipos de cómputo en cada una de las casas de los asesores la realizaron los auxiliares técnicos. En el equipo se realizó la creación y configuración de la conexión virtual privada VPN con el fin de que el asesor estuviera conectado a la red interna y así poder acceder a la información y aplicativos necesarios para la gestión. Luego de realizar la instalación del equipo se entregó el formato TC-FR06 Entrega de equipos brigadas o teletrabajo el cual debía firmar el aseor, donde se especificaba la información del equipo de cómputo y se mencionan unas recomendaciones de seguridad de la información y las implicaciones en caso de no cumplirlas.

En caso de que el asesor presente falla en el equipo de cómputo debe reportarlo a través del link de incidencias para que el Ing. De sistemas o los auxiliares técnicos realicen la revisión a través de la herramienta Team Viewer, la cual tiene una configuración de seguridad para que solo el personal de sistemas pueda acceder a los equipos.

CONFIDENCIAL

En conjunto con el área de auditoria se realiza revisión mensual en los equipos para validar que las directivas de seguridad estén funcionando bien.

20. ACTUALIZACIONES DEL SISTEMA OPERATIVO

Las actualizaciones de los sistemas operativos tanto de equipos de cómputo como de servidores Windows se realizan a través de la plataforma del antivirus Kaspersky Endpoint Security Cloud Pro con una tarea programada que se ejecuta todos los sábados a las 8 a.m.

En caso de que un dispositivo protegido no está en línea a la hora programada, la instalación de la actualización se ejecutará tan pronto como el dispositivo vuelva a estar en línea.

En los momentos en que el equipo o servidor no este tomando la tarea enviada desde el agente del antivirus, estas actualizaciones deben realizarse manualmente siempre y cuando sean críticas, en caso contrario se debe revisar en la plataforma del antivirus la falla y si es necesario reportarla al proveedor y/o fabricante.

21. SEGURIDAD Y GRABACIONES AREAS SEGURAS

Para un mejor aseguramiento y control en la entrada y salida de personal a las instalaciones de GRUPO REINCAR se cuenta con un sistema de videovigilancia que permita monitorear en tiempo real las oficinas y áreas seguras con el fin de prevenir accesos no autorizados.

22. RESPONSABILIDADES DERIVADAS DEL INCUMPLIMIENTO DE LA POLÍTICA

El presente documento estará regulado por las leyes y normativas colombianas, en

CONFIDENCIAL

relación con protección de datos de carácter personal, propiedad intelectual y uso de herramientas telemáticas, así como la normativa aplicable dentro del ámbito laboral y toda la que pueda aparecer en un futuro.

Aprueban:

DIEGO ENRIQUE GONZALEZ RAMIREZ
C.C. 1.098.642.487 de Bucaramanga

Leandro Enrique Ramos Solano
Cc 88.030.255 de Pamplona

CONFIDENCIAL

FICHA TÉCNICA – PLATAFORMA CALL CENTER PREDICTIVO

1. Control Documental

Nombre del documento	Ficha Técnica – Plataforma Call Center Predictivo
Código	FT-CC-001
Versión	1.1
Fecha	03/10/2025
Elaboró	Jesús Fuentes
Revisó / Aprobó	Julian Pineda

2. Alcance

El presente documento describe las especificaciones técnicas de la Plataforma de Call Center IP Inbound/Outbound implementada, con el fin de evidenciar el cumplimiento de los requisitos técnicos establecidos para la operación del sistema en el marco de auditoría interna.

3. Descripción Técnica de la Solución

La solución consiste en la implementación de una Plataforma de Call Center IP basada en Issabel 5 con motor Asterisk versión 18.1G.0, bajo arquitectura cliente-servidor y administración vía interfaz web.

- ACD (Automatic Call Distribution) con gestión de colas y agentes dinámicos/estáticos.
- Grabación de llamadas y monitoreo en tiempo real.
- Reportes históricos y estadísticos.
- Gestión de usuarios, roles y perfiles con auditoría de acciones.
- Marcador predictivo (Predictive Dialer) para campañas outbound.
- Integración mediante SIP, AMI y AGI.

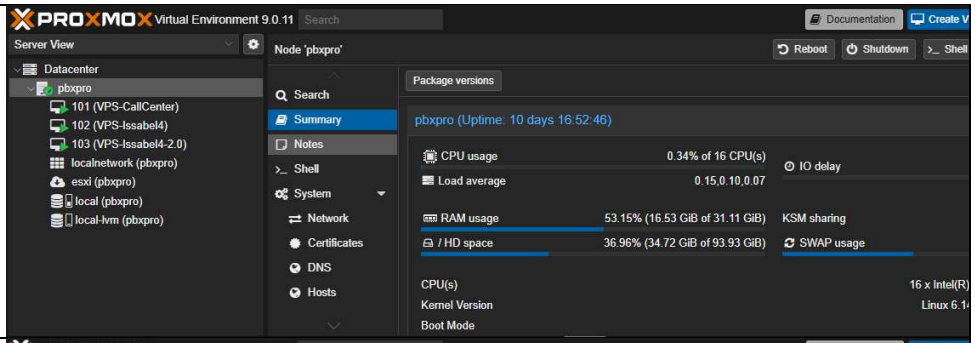
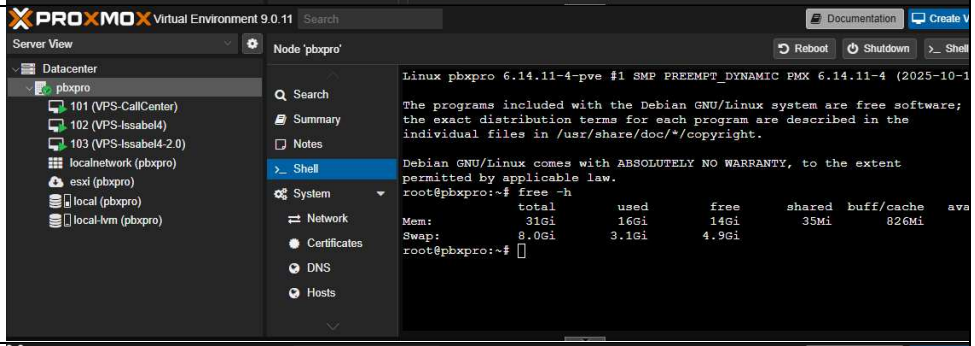
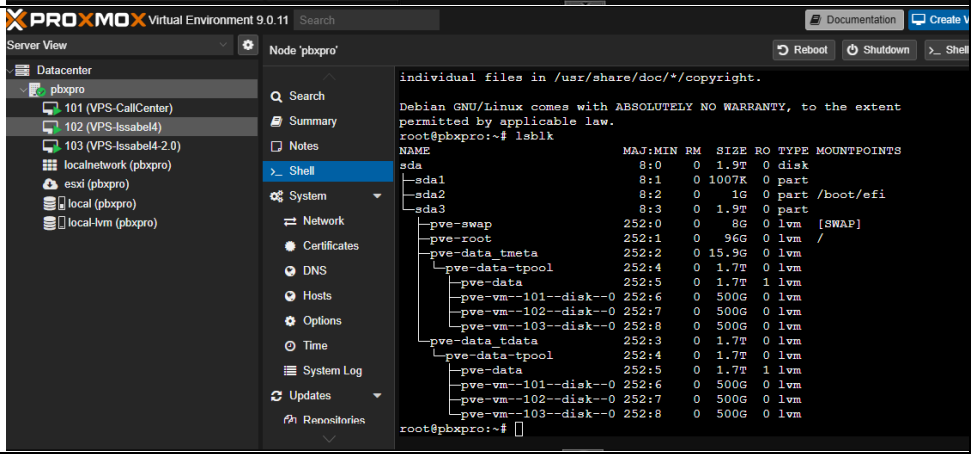
Ítem	Requisito	Descripción técnica (Issabel 5)
1	**Implementación de Plataforma Call Center IP Inbound/Outbound basada en Issabel 5, con software, cumpliendo arquitectura, telefonía, funcionalidades ACD, reportes, seguridad, escalabilidad, integraciones y soporte.**	Suministro, instalación, configuración y puesta en marcha de una **Plataforma de Call Center IP Inbound/Outbound** basada en **Issabel 5**, con motor de telefonía **Asterisk versión 18.1G.0** y soporte completo del protocolo **SIP (RFC 3261)**. La solución debe operar bajo una **arquitectura cliente-servidor**, disponiendo de **interfaz web** para la administración, operación y supervisión del sistema. La plataforma debe incluir **funcionalidades ACD (Automatic Call Distribution)** con gestión de colas, agentes dinámicos y estáticos, así como múltiples estrategias de distribución y enrutamiento de llamadas. Debe incorporar **grabación de llamadas**, monitoreo y **supervisión en tiempo real** para el control operativo. La solución debe proveer **reportes históricos y estadísticos**, orientados a la medición de la operación y el rendimiento del Call Center. En materia de seguridad, debe contemplar **gestión de usuarios, roles, perfiles y auditoría de acciones**. Los **requerimientos mínimos del servidor físico** son: procesador **Intel® Core™ i9-14900K**, con **8 núcleos físicos y 16 hilos de procesamiento**, **31 GB de memoria RAM**, **SSD de 1.9 TB de almacenamiento en discos SSD**, tarjeta Ethernet 1 GbE BASE-T **(1000 Mb/s Full Dúplex),** y plataforma de virtualización mediante **hipervisor**. La solución debe ser **escalable**, permitiendo la operación de múltiples agentes y múltiples colas de atención. Asimismo, debe incluir **marcación automática outbound** con **modo predictivo (Predictive Dialer)**, orientada a incrementar la productividad mediante discado automático de campañas y listas, detección de llamadas contestadas y no contestadas, gestión de reintentos y asignación automática de llamadas a agentes disponibles. Debe permitir la **parametrización de campañas** (horarios, ritmo/ratio de marcación, listas) y garantizar la **trazabilidad completa en los reportes**. La plataforma debe permitir **integración con sistemas CRM** y contar con mecanismos de integración y automatización propios de la telefonía, tales como **SIP, AMI y AGI**.Se requiere la provisión de **soporte técnico bajo esquema SLA 7x24**, así como **capacitación para administradores, supervisores y/o operadores**, incluyendo **transferencia de conocimiento** y **documentación completa de la configuración implementada**.

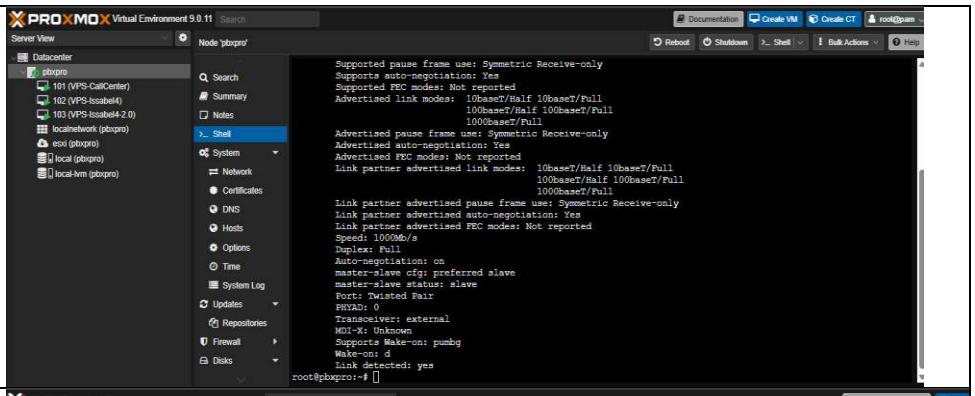
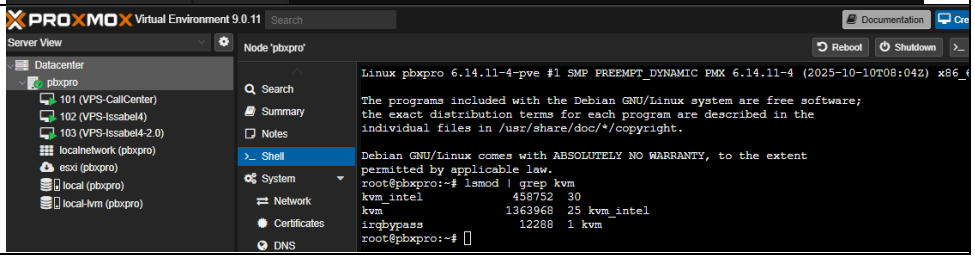
4. Infraestructura del Servidor

- Procesador: Intel® Core™ i9-14900K (8 núcleos físicos / 16 hilos).
- Memoria RAM: 31 GB.
- Almacenamiento: 1.9 TB en disco SSD (ROTA=0).
- Red: Tarjeta Ethernet 1 GbE BASE-T (1000 Mb/s Full Dúplex).
- Virtualización: Proxmox VE con hipervisor KVM (Intel VT-x habilitado).

5. Evidencias Técnicas

A continuación, se relacionan las evidencias técnicas obtenidas directamente desde el servidor Proxmox VE mediante comandos del sistema.

Evidencia CPU	
Evidencia Memoria (free -h)	
Evidencia Almacenamiento (lsblk)	

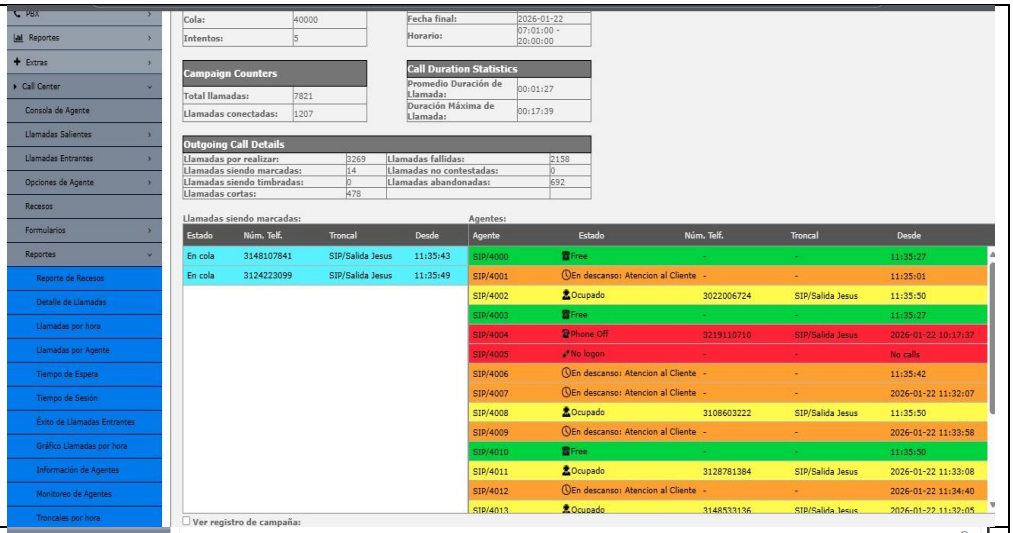
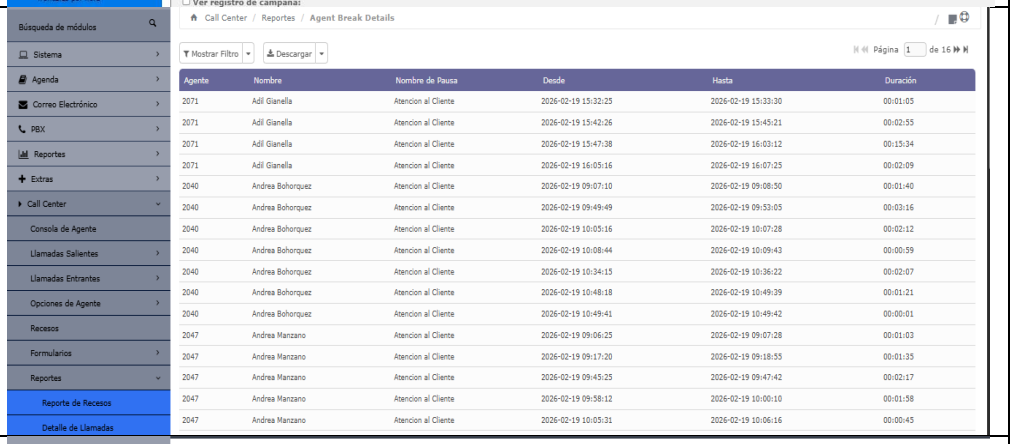
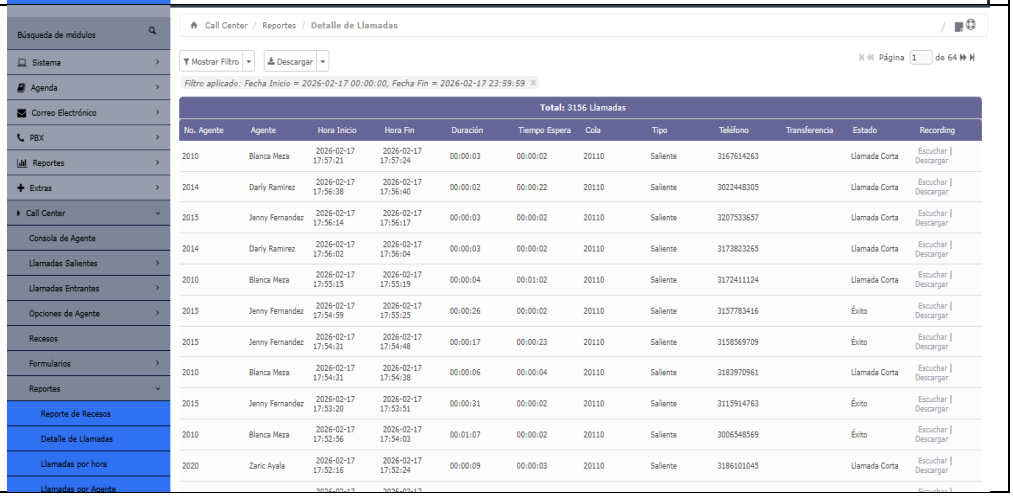
Evidencia Red (ethtool enp4s0)	
Evidencia Virtualización (lsmod | grep kvm)	

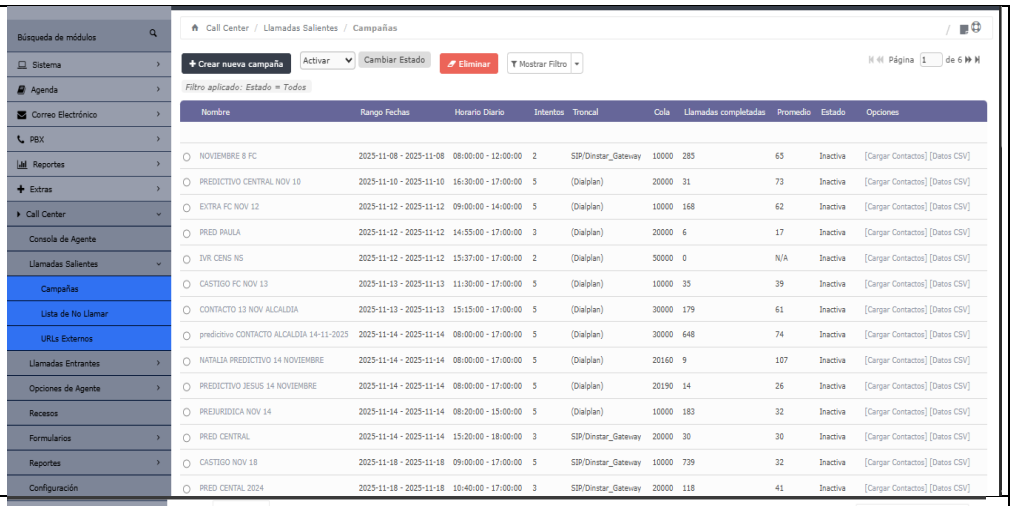
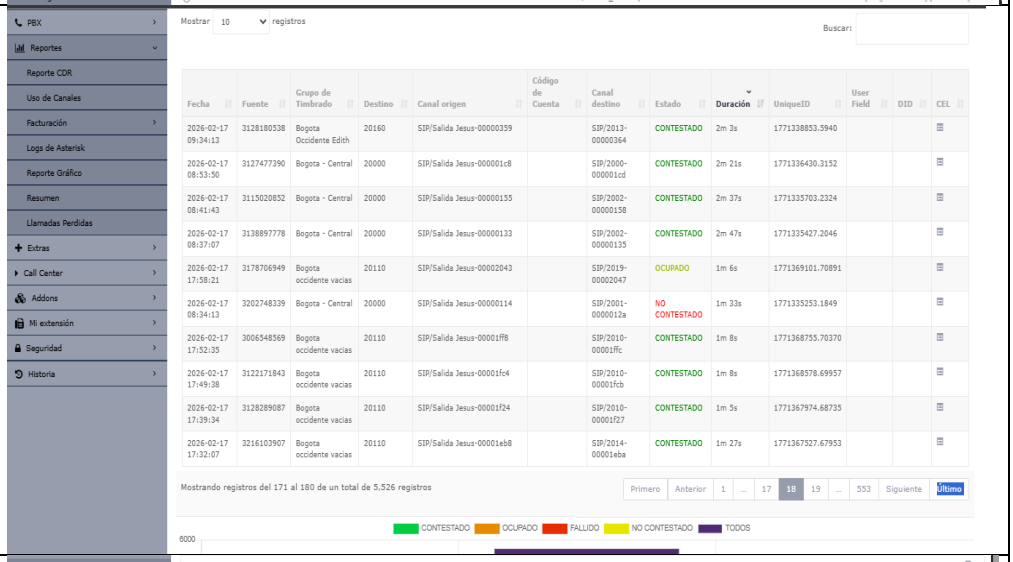
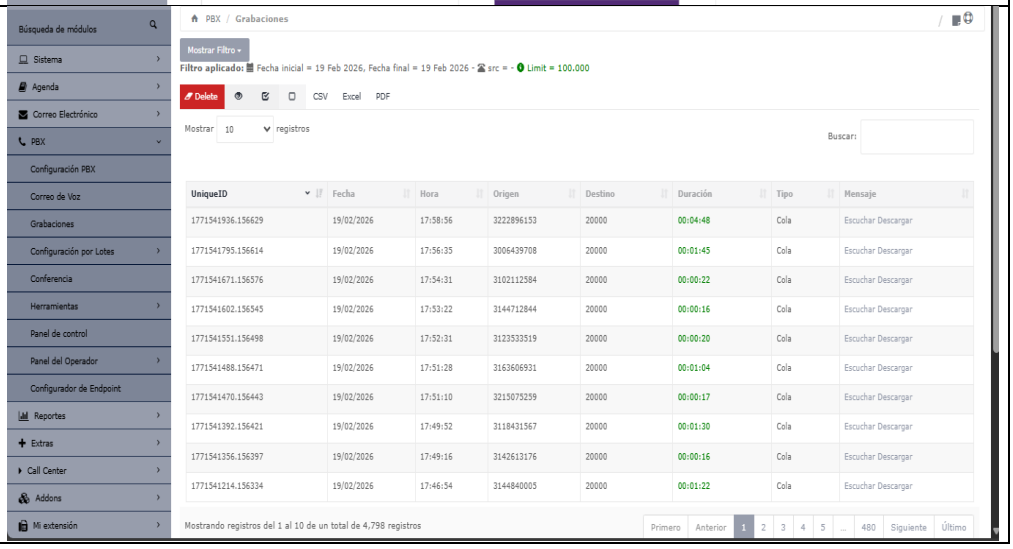
Matriz de Cumplimiento – Enfoque ISO 9001

La siguiente matriz documenta la verificación de cumplimiento de los requisitos técnicos bajo un enfoque de control y trazabilidad alineado con buenas prácticas de gestión de calidad (ISO 9001).

Requisito	Criterio de Verificación	Cumple (Sí/No)	Evidencia Objetiva	Responsable Verificación	Fecha Verificación	Observaciones
Procesador mínimo 8 núcleos	Validar salida comando lscpu	Sí	Captura lscpu – 8 núcleos físicos / 16 hilos	Jesús Fuentes	20/02/2026	Supera requerimiento mínimo
Memoria mínima 12 GB RAM	Validar salida free -h	Sí	Captura free -h – 31 GB RAM	Jesús Fuentes	20/02/2026	Capacidad superior al mínimo requerido
Almacenamiento mínimo 500 GB SSD	Validar lsblk (ROTA=0)	Sí	Captura lsblk – SSD 1.9 TB	Jesús Fuentes	20/02/2026	Disco sólido certificado
Tarjeta de red 1 GbE BASE-T	Validar ethtool enp4s0	Sí	Captura ethtool – 1000Mb/s Full Dúplex	Jesús Fuentes	20/02/2026	Cumple estándar solicitado
Hipervisor con virtualización habilitada	Validar lsmod | grep kvm	Sí	Captura KVM activo (kvm_intel)	Jesús Fuentes	20/02/2026	Virtualización por hardware habilitada

3. Evidencias Funcionales de la Plataforma

Módulo Call Center	
Módulo de monitoreo de Pausas por agente	
Modulo detalle de llamadas	

Módulo de campañas Marcador predictivo	
Modulo CDR	
Modulo grabación de llamadas	

6. Estado Operativo

La plataforma se encuentra en operación activa y estable, con monitoreo permanente de recursos (CPU, memoria y almacenamiento).

7. Validación y Firma

En constancia de lo anterior, se firma el presente documento para fines de auditoría interna.

_____

Jesús Guarguati Fuentes
Analista y Desarrollador de Sistemas de Información
Híbridos TI
Fecha: 03/10/2025

CERTIFICACION

REDES UPS Y PROTECCIONES E.U., Empresa dedicada al mantenimiento y comercialización de equipos de soporte y Protección eléctrica, así como a la implementación de soluciones de continuidad eléctrica para cargas críticas, ubicada en Bucaramanga y operando desde el año 2002, se permite certificar que:

La Empresa REINCAR LTDA es cliente nuestro desde el año 2015y cuenta con un sistema de REDUNDANCIA Y CONTINUIDAD ELECTRICA, conformado por los siguientes equipos:

- Suministro de Energía comercial por parte de la ESSA desde el transformador del edificio de la Camara de Comercio de Bucaramanga.
- Suministro de energía alterna desde la Planta de emergencia (sistema moto-generador) el cual es accionado mediante una transferencia automática para operar en caso de falla de la red comercial
- Soporte Eléctrico para las cargas críticas desde una UPS de 10 KVA instalada en el piso 5. Se trata de una UPS ONLINE, la cual impide que los equipos de cómputo y comunicaciones presenten apagado al realizarse la transferencia RED-PLANTA-RED gracias a su Banco de baterías interno.

La UPS es sometida a mantenimiento permanente ya que se realizan dos rutinas al año y el sistema eléctrico del edificio cuenta con el soporte de mantenimiento adecuado.

Atentamente:

REDES UPS Y PROTECCIONES E.U.
NIT: 804.014.290-7
FIRMA AUTORIZADA

DEPARTAMENTO TECNICO

REDES UPS Y PROTECCIONES E.U.

NIT 804.014.290-7

DoctorLinux.com
Soluciones TI que se adaptan a ti

No. OS2621280
Create: 27-01-2026 12:19:18

Informe Técnico de Incidencia

Status Cerrada Priority Contrato

Update 03-02-2026 11:33:29 Quote

Client GRUPO REINCAR S.A.S
Sr. Julian Pineda

Assigned to Jorge Enrique Baron Caceres
Ing. de Sistemas - CEO

Request Continuidad operacional Servidor Telefonia

Description REPORTE DE CONTINUIDAD Y FUNCIONAMIENTO DEL SISTEMA DE COMUNICACIONES

Solution 1. Objetivo del esquema de continuidad
Garantizar la disponibilidad del servicio de comunicaciones ante fallas del servidor principal, minimizando el impacto operativo y asegurando la conservación de la información crítica del sistema telefónico.

2. Arquitectura implementada (No Clúster)
Reincar cuenta con una arquitectura de continuidad operativa basada en redundancia lógica, compuesta por:
-Dos (2) servidores Issabel independientes
-Ambos servidores cuentan con:
*La misma configuración funcional
*Extensiones, troncales y parámetros operativos equivalentes
*Capacidad de operación autónoma
Este esquema permite mantener el servicio activo aun cuando uno de los servidores presente fallas.

3. Mecanismo de continuidad del servicio
-El Servidor Issabel Principal opera como plataforma activa.
-En caso de:
*Falla del sistema
*Mantenimiento correctivo
*Incidente imprevisto

Los usuarios son redirigidos y se conectan manualmente al servidor Issabel Secundario, garantizando la continuidad del servicio de llamadas. Este procedimiento evita interrupciones prolongadas y permite restablecer la operación en minutos.

4. Gestión y protección de audios (grabaciones)
-Cada servidor realiza:
*Copias de seguridad incrementales diarias de los audios de llamadas
*Estas copias se almacenan en un disco dedicado interno asignado exclusivamente para respaldos

-Adicionalmente:
*Se ejecutan copias manuales externas periódicas, como medida adicional de protección ante

eventos críticos.
Este esquema asegura la preservación histórica de grabaciones, incluso ante fallas de hardware o sistema.

5. Respaldo de configuración del sistema
Cada servidor Issabel mantiene:
-Copias de seguridad de su propia configuración, incluyendo:
*Parámetros del sistema
*Configuración de extensiones
*Troncales
*Reglas y servicios asociados

Estas copias permiten:
-Restauraciones rápidas
-Reemplazo de hardware
-Recuperación ante incidentes mayores

6. Beneficios del esquema implementado

 Alta disponibilidad operativa
 Reducción del riesgo de indisponibilidad del servicio
 Protección de grabaciones y datos críticos
 Recuperación rápida ante fallas
 Independencia de los servidores (no punto único de falla)

7. Conclusión

El esquema de continuidad implementado en Reincar proporciona una infraestructura robusta y confiable, diseñada para mantener la operación del sistema de comunicaciones aun ante fallas del servidor principal, respaldando tanto la información como la continuidad del servicio, conforme a buenas prácticas de infraestructura tecnológica.

_____	_____	**Elaboró:**
Firma del Cliente	Técnico de Doctor Linux Ltda	Jorge Enrique Baron Caceres Ing. de Sistemas - CEO

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cumple con:

Realizar mensualmente las pruebas de contingencia de acuerdo a TC-IN09 Estructura de plan de continuidad del negocio, validando pruebas del Sistema eléctrico, pruebas del sistema telefónico.

DIEGO ENRIQUE GONZALEZ
Gerente General

INFORME AUDITORIA SEGURIDAD DE LA INFORMACIÓN

1. **ALCANCE:** Esta auditoria aplica a todos los procesos de grupo de Reincar en la ciudad de Bucaramanga, con relación a la medición y cumplimiento de la seguridad de la información conforme a lo estipulado en la política.

a) **FECHA DE VERIFICACIÓN:** Diciembre 2025

b) **INTEGRANTES:** Liliana Vega – Auditor Interno

Julián Pineda – Líder TIC

1.1. OBJETIVO DE LA VERIFICACIÓN: Garantizar el cumplimiento y medición de los objetivos de la política de seguridad de la información en grupo Reincar, por medio de las revisiones a cada punto de la misma y dar a conocer los hallazgos encontrados.

1.1. ACTIVIDADES DESARROLLADAS.

1.1.1. Revisión de las restricciones de seguridad de la información en los computadores de grupo Reincar

1.1.2. Revisión formato registro de entrada y salida de las instalaciones de Grupo Reincar y cámaras.

1.1.3. Revisión de las copias de seguridad generadas en la ciudad de Bucaramanga.

1.1.4. Revisión de resguardo de los documentos físicos.

1.1.5. Revisión puestos de trabajo de los gestores ningún elemento que infrinja con la seguridad de la información, (celular -lápiz-lapicero-hoja).

1.1.6. Revisión aleatoria de las carpetas de los asesores tanto en la red como en la papelera de reciclaje.

1.1.7. Validar que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

1.1.8. Validación de plan de contingencia de grupo Reincar mes de Diciembre 2025.

1.1.9. Revisión de solución a las incidencias del área de Sistemas del mes de Diciembre 2025.

1.1.10. Confirmación de restricciones en los correos corporativos.

1.1.11 Revisión de las comunicaciones del B2CHAT y garantizando el cumplimiento a la política de tratamiento de datos y seguridad de la información.

2. DESCRIPCION DE HALLAZGOS

2.1.1 POLITICA SEGURIDAD DE LA INFORMACIÓN

Banco de Bogotá, Avvillas Bucaramanga, Cens - Veolia, Financiera Comultrasan – Toyota Financial Services, Fondo Nacional del Ahorro, Alcaldía, Lilipink, y se confirmó los siguientes bloqueos:

- Equipo Celular
- Memorias USB
- Unidad DVD
- Símbolo de sistema (cmd), Notas rápidas, y WordPad
- Impresoras
- Detención de redes automática
- Escritorio remoto
- Opciones de Internet Explorer
- Powershell
- Disco local C, D
- Panel de control

- Bluetooth
- carpetas no autorizadas.
- Páginas de internet no autorizadas.
- Paint
- Revisión puestos de trabajo (celular -lápiz-lapicero-hoja)
- Revisión aleatoria de las carpetas de los asesores tanto en la red como en la papelera de reciclaje
- Validar que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

Se revisó la hoja de cálculo del link y se evidencia los registros de los equipos nuevos en el siguiente link: https://docs.google.com/forms/d/e/1FAIpQLSe8y77G_3aRmi8Ah74xzh1Z81_tV5Uei56rKopjsr-DDS66bA/viewform y se puede validar en la hoja de respuestas https://docs.google.com/spreadsheets/d/14ax2Hd3qNohk1h0ez-jUDQqoZxFBuKjK5drSfVwTKwA/edit#gid=1841321568

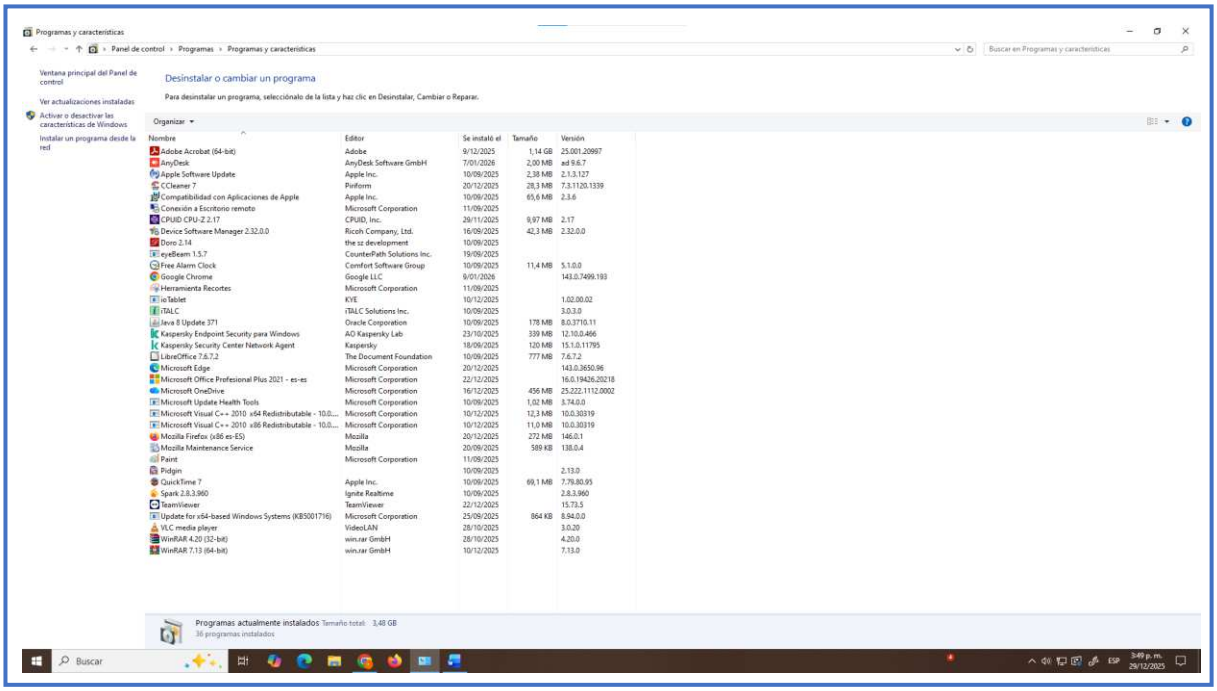
2.1.2 ACCESO FÍSICO Y ÁREAS SEGURAS

Por medio del registro de las grabaciones de las cámaras, se valida el ingreso el 03 de diciembre en Bucaramanga al señor Cesar Barrera identificado con Cédula de Ciudadanía: 5634933 ingreso a las 2:11 p.m. y salida 2: 30 p.m., se confirma registro de la cámara de seguridad el cual coincide con el registro de formato de ingreso. Así mismo se valida ingresos no autorizados a las áreas seguras de la empresa.

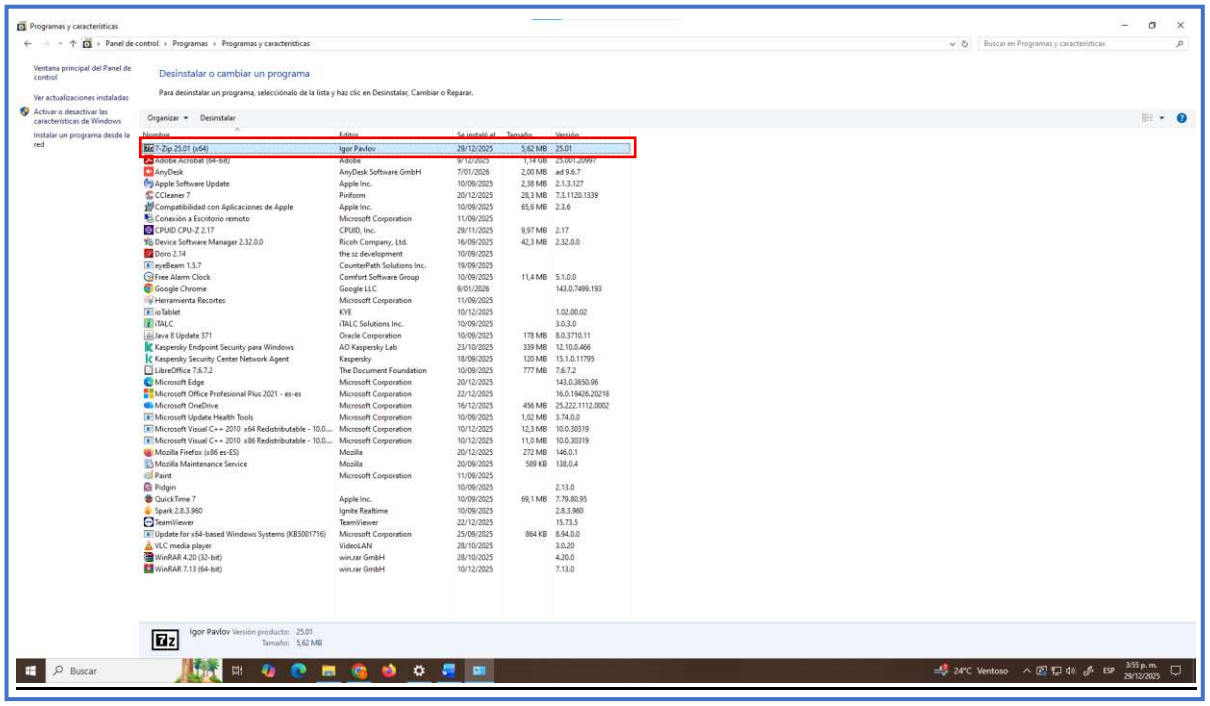
2.1.3 AUDITORIA A SISTEMAS OPERATIVOS

Para realizar la auditoría de los sistemas operativos, nos apoyamos de los puntos de restauración que tienen configurado los equipos de cómputo, se dispone de un equipo al cual se le realizan modificaciones posteriores al punto de restauración, posteriormente para ejecutar el proceso de revisión, el equipo de cómputo es restaurado a su versión anterior y se verifica tenga los programas iniciales junto con las restricciones de seguridad.

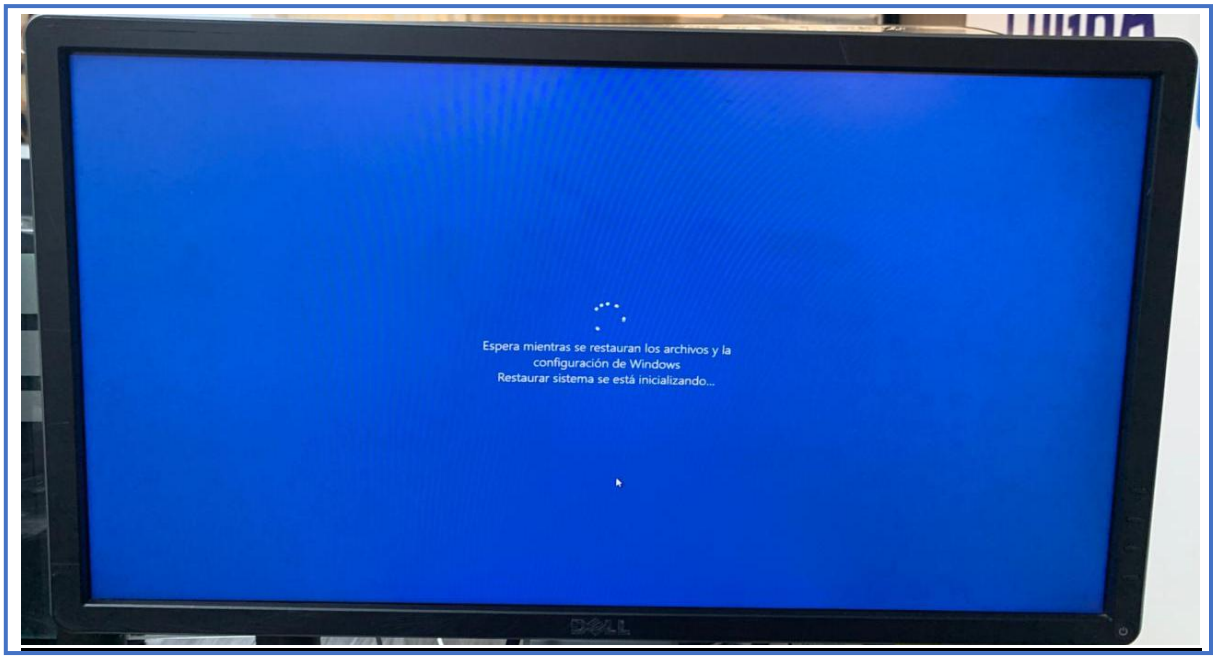
Evidencia 1. Programas iniciales del equipo



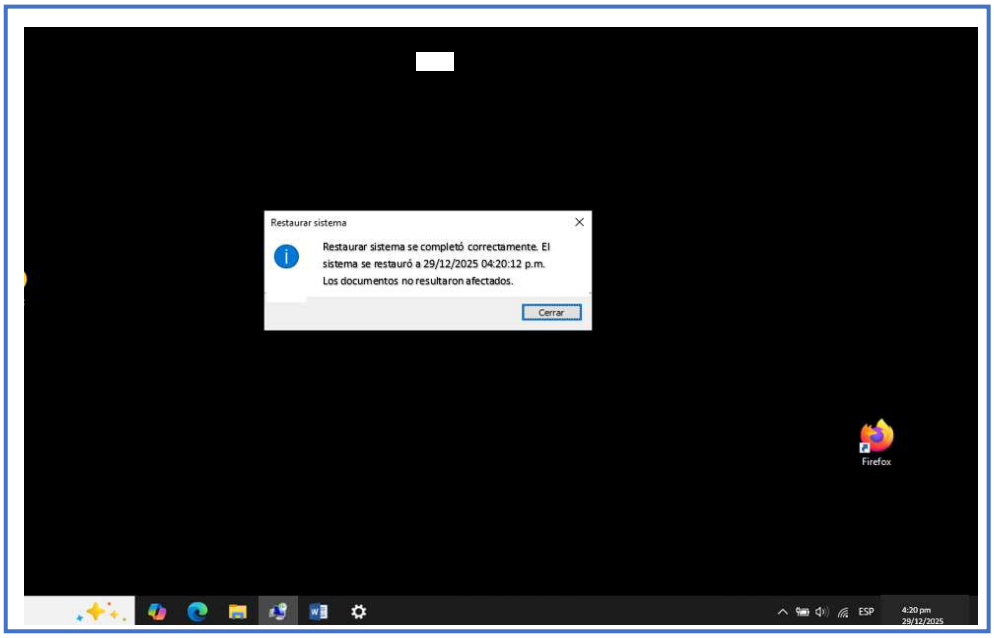
Evidencia 2. Instalación en el aplicativo 7zip



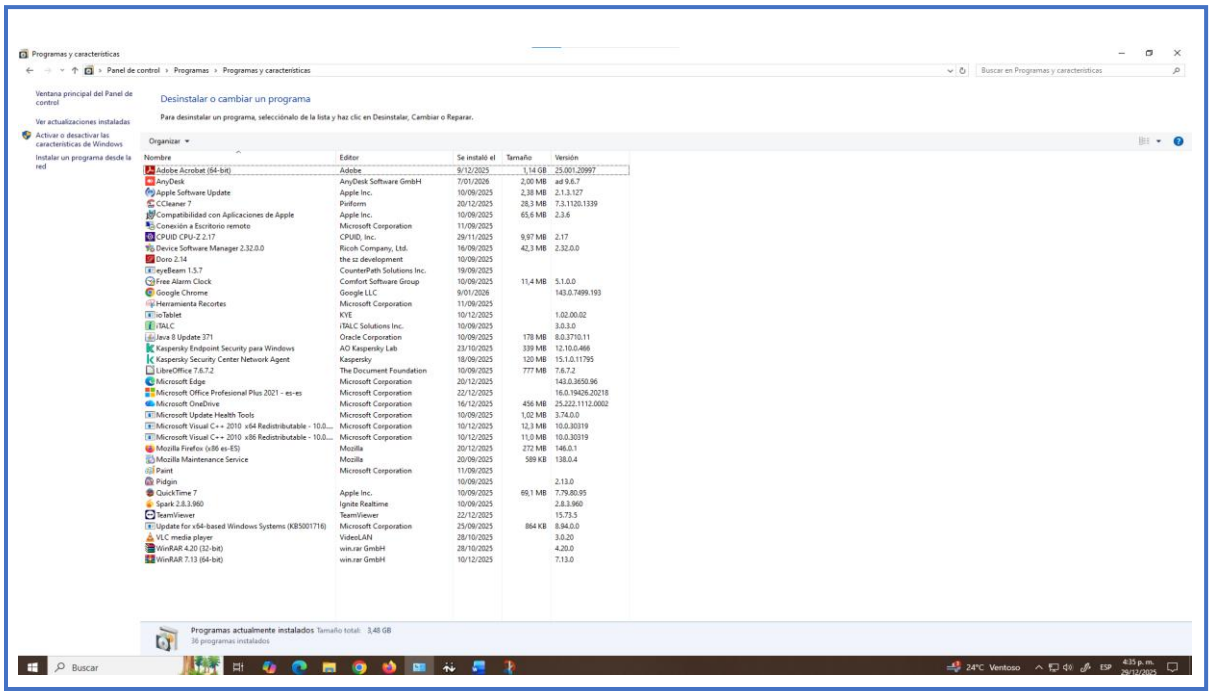
Evidencia 3. Ejecución proceso de restauración



Evidencia 4. Finalización proceso de restauración



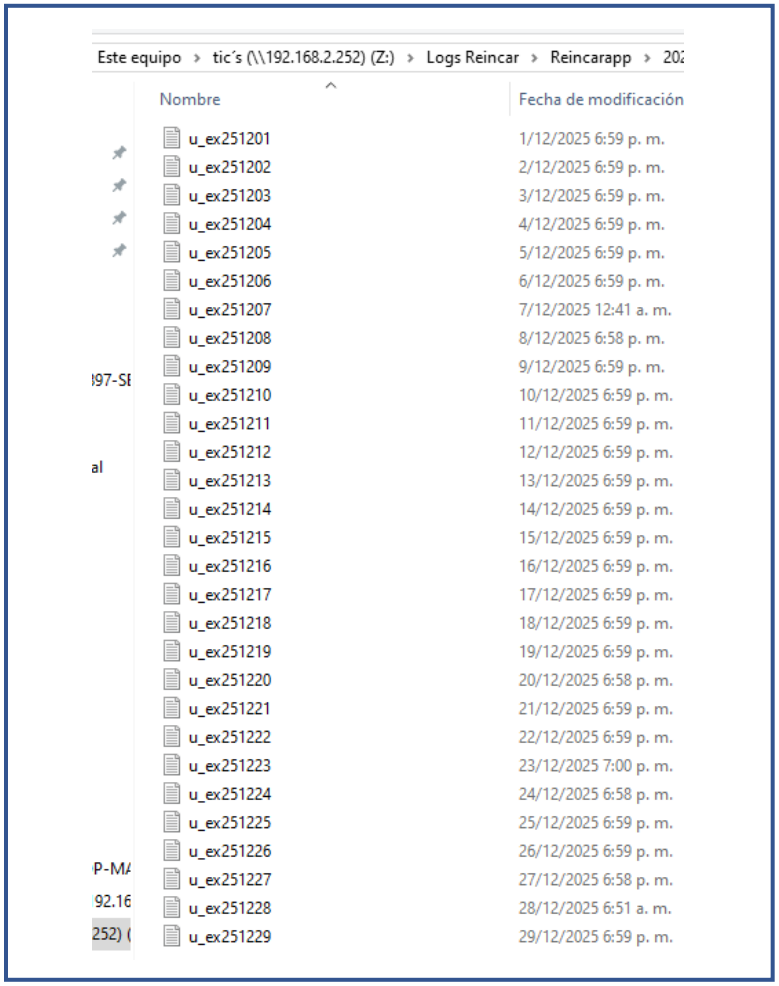
Evidencia 5. Validación programas instalados luego de la restauración



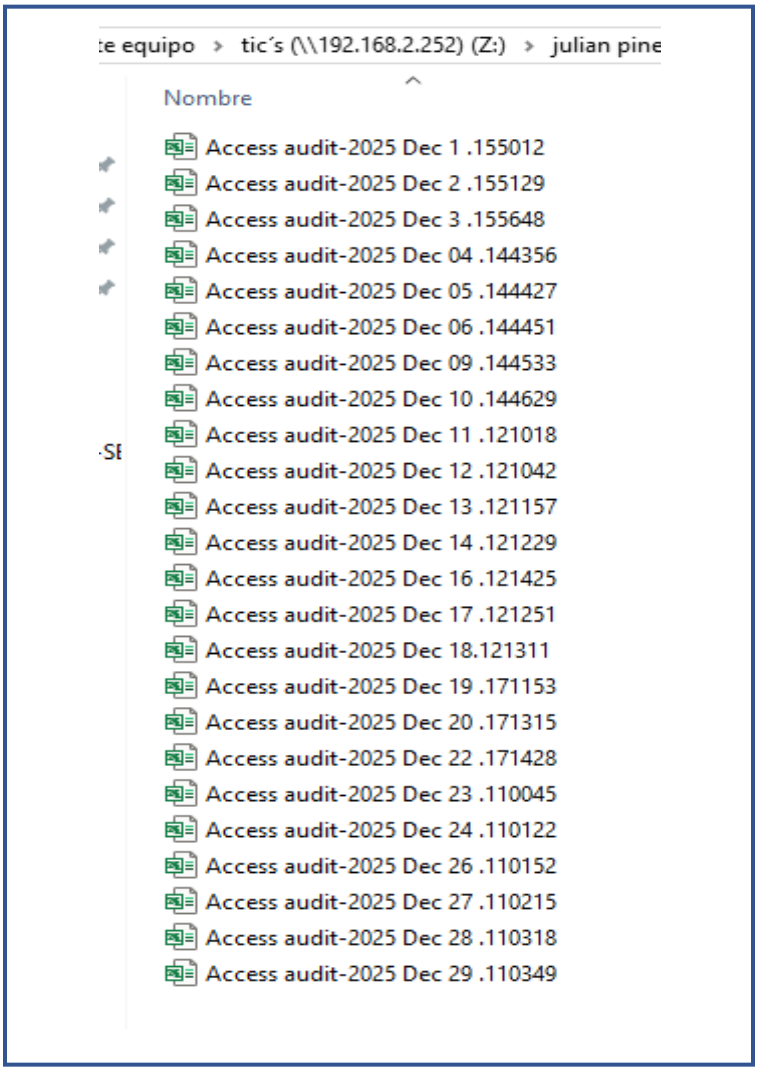
2.1.4 REVISIÓN DE LOGS EN LOS SERVIDORES

Como oportunidad de mejora resultado de la Auditoria de Icontec sobre ISO 27001 Seguridad de la Información, se debe ingresar a los servidores de dominio de archivos ReincarApp – Isabell y validar que los logs estén activos y revisar los eventos generados con el fin de detectar posibles anomalías.

Revisión de Logs generados por el servidor ReincarApp:



Revisión de Logs generados por el servidor Issabel:



2.1.5 COPIAS DE SEGURIDAD

Copias de seguridad Oficina Bucaramanga

copia disco externo Bucaramanga: J:\avvillas prejuridico 2025-12-19 17;30;09 (Diferencial)\JESSICA LEON\DICIEMBRE

copia servidor oficina Bogotá: E:\BackupDatosBmanga\avvillas_prejuri-dico\JESSICA LEON\DICIEMBRE

2.1.6 REVISIÓN DE AMENAZAS INTELIGENTES

El líder de TIC y el Auditor Interno se reúnen con periocidad mensual, para realizar la respectiva revisión a las amenazas identificadas, en esta fase se procesan los datos recopilados y se analizan para identificar patrones y tendencias (ver acta de registro).

2.1.7 SEGURIDAD DE LA INFORMACIÓN EN PUESTOS DE TRABAJO:

BANCO DE BOGOTÁ

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

Se solicitó al coordinador un acuerdo de pago **firmado** por el cliente se confirmó que esta custodiado en un lugar bajo llave.

AVVILLAS BUCARAMANGA

Se solicito a la coordinadora un acuerdo de pago aleatorio, informa y muestra que se envían por medio de correo electrónico.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

FONDO NACIONAL DEL AHORRRO

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

FINANCIERA COMULTRASAN

Se solicitó al coordinador un formato de visita correspondiente al mes, se confirmó que los documentos están en un lugar bajo seguridad.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

TOYOTA FINANCIAL SERVICES

Se solicitó al coordinador un formato de visita correspondiente al mes, se confirmó que los documentos están en un lugar bajo seguridad.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

CENS - VEOLIA

Se solicitó al coordinador un formato de visita correspondiente al mes, se confirmó que los documentos están en un lugar bajo seguridad.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

ALCALDIA

Se solicitó al coordinador un formato de visita correspondiente al mes, se confirmó que los documentos están en un lugar bajo seguridad.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

LILIPINK

Se solicitó al coordinador un formato de visita correspondiente al mes, se confirmó que los documentos están en un lugar bajo seguridad.

Se revisaron los puestos de trabajo de los gestores y no se encontraron celulares, ni elementos que infrinjan con la seguridad de la información(lápiz-lapicero-hoja).

Se confirmo que los acuerdos de pago se envían solo del correo del director.

2.1.8 ELIMINACIÓN DE INFORMACIÓN

AVVILLAS Bucaramanga

Se valida el equipo de la coordinación y no cuenta con bases de datos diferente al mes en curso.

Se revisan las carpetas de los asesores tanto en la red como en la papelera de reciclaje y se evidencia cumplimiento a la seguridad de la información, contando solo con la base del presente mes.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

BANCO DE BOGOTÁ

Se reviso la carpeta de todos los gestores y se evidencio cumplimiento a la seguridad de la información.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

FINANCIERA COMULTRASAN

No se encontró bases correspondientes a meses anteriores.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

TOYOTA FINANCIAL CENTER

No se encontró documentos correspondientes a meses anteriores.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

FONDO NACIONAL DEL AHORRO

No se encontró documentos correspondientes a meses anteriores.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

VEOLIA- CENS

No se encontró documentos correspondientes a meses anteriores.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

ALCALDIA

No se encontró documentos correspondientes a meses anteriores.

Se valida que el acceso al escritorio, documentos y descargas en los equipos de los gestores se encuentren bloqueados.

2.1.9 VALIDACIÓN PLAN CONTINGENCIA

Se realizó validación del Plan de Contingencia en el mes de Diciembre en la ciudad de Bucaramanga, se confirmó el correcto funcionamiento de los aplicativos de cobro usado por cada uno de las carteras del Grupo Reincar.

Las actas de validación del plan de contingencia están archivadas en:

\\192.168.2.251\auditoria\AUDITOR\AuditorInterno\AUDITORIAS\2024\PLAN CONTINGENCIA

2.1.10 VALIDACIÓN SOPORTE DE SISTEMAS

Se evidencia a la fecha 31 de Diciembre 2025 se han registrado 288 incidencias de las cuales 4 está pendiente y 2 están en blanco.

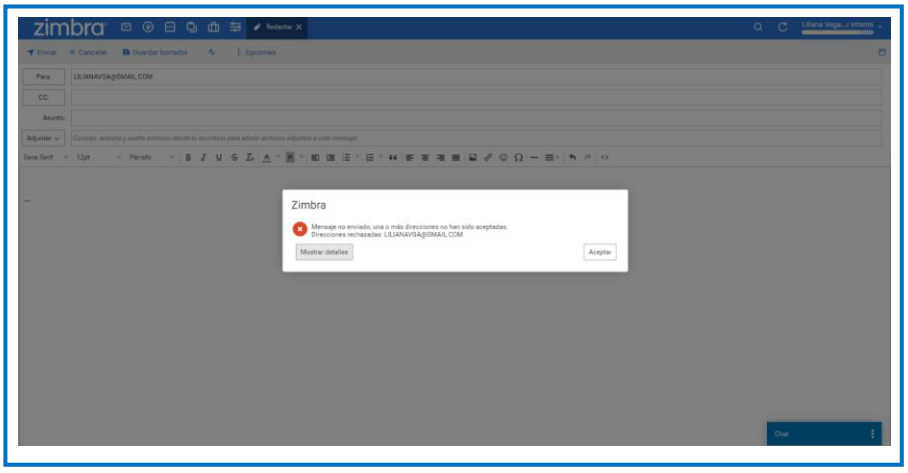
Cuenta de Indique la falla	Etiquetas de columna			
Etiquetas de fila	TERMINADO	PENDIENTE	(en blanco)	Total general
⊞Banco Bogotá	119			119
⊞Avvillas Bucaramanga	45	3		48
⊞Comultrasan	34	1	2	37
⊞FNA	22			22
⊞Cens	22			22
⊞IMPUESTOS BUC	13			13
⊞Auditoria	11			11
⊞Avvillas Bogota	8			8
⊞Toyota	3			3
⊞LILIPINK	3			3
⊞Administrativa	2			2
Total general	282	4	2	288

2.1.11 CORREO ELECTRONICO CORPORATIVO

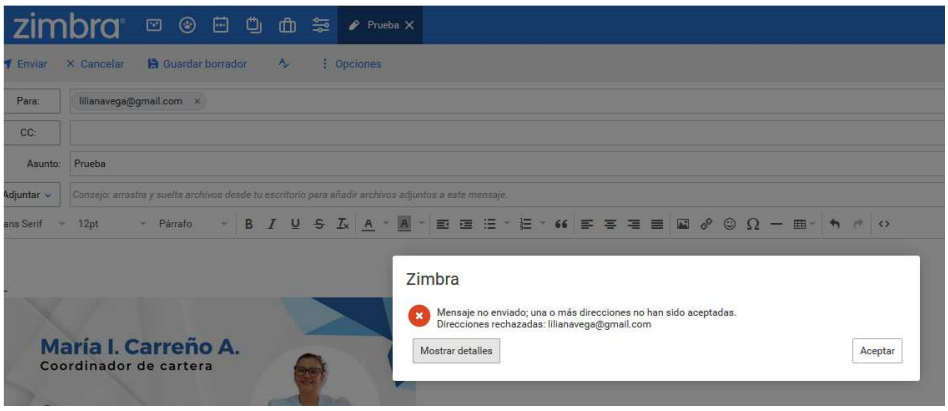
Se revisaron los correos electrónicos desde la plataforma web de administración del correo electrónico corporativo, en donde se puede ingresar y validar la información enviada y recibida de todos los colaboradores que tienen asignado al correo.

Se confirmo restricciones en los siguientes correos:

LILIANA VEGA– LÍDER AUDITOR INTERNO



MARÍA ISABEL CARREÑO–COORDINADOR AVVILLAS BUCARAMANGA



Se revisaron los correos de los coordinadores de las carteras de Banco de Bogotá, Avvillas Bucaramanga, Financiera Comultrasan, Veolia, CENS, Toyota Financial Services, Alcaldía y Lilipink se confirmó cumplimiento a la seguridad de la información en el envío y recepción de los correos.

2.1.12 Revisión plantillas de configuración segura de los servidores: esta revisión se realizará desde el área de Auditoría con una periocidad semestral.

2.1.13 WhatsApp y B2CHAT

Se revisaron las actas de las auditorías realizadas a Whatsapp y B2chat y el informe de monitoreo digital presentado en el mes de Diciembre 2025.

CONCLUSIÓN DE LA AUDITORIA:

- En la auditoría realizada se concluyó que se debe continuar con el seguimiento a los asesores en el tema de Seguridad de la Información, es importante estar en constante seguimiento.

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR da cumplimiento a las especificaciones tecnológicas exigidas en las circulares 048 y 052de la Superintendencia Financiera y las que reemplacen o modifiquen .

_____

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la Capacidad Física para adecuación de puestos de trabajo en caso de incremento de volúmenes de cartera y/o campañas especiales.

DIEGO ENRIQUE GONZALEZ
Gerente General

icontec ISO / IEC 27001 SI-2000523
icontec ISO 9001 SC-CER546357
IQNET

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la adecuación completa de los puestos de trabajo equipos de cómputo, dando cumplimiento a la Política de Seguridad de la Información, sin acceso a tener dispositivos de almacenamiento extraíbles.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la capacidad operativa para adaptar la gestión al teletrabajo y/o trabajo en casa (en las situaciones en que se amerite) con el cumplimiento todas las buenas prácticas de salud y seguridad del teletrabajo.

DIEGO ENRIQUE GONZALEZ
Gerente General

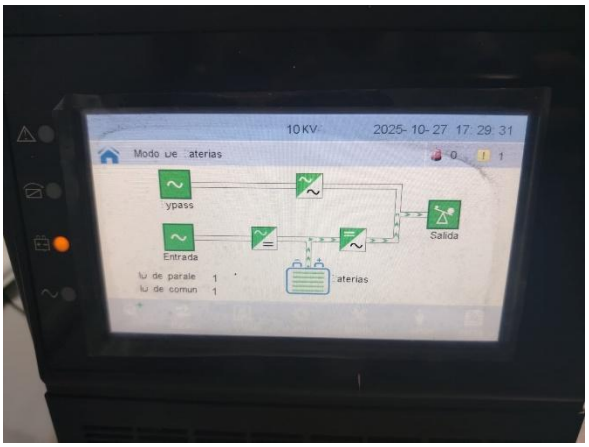
Reincar Recuperadora integral de cartera	**Acta de Validación de contingencias**	Código: TC-FR03
		Versión: 01

FECHA	DESCRIPCIÓN
OCTUBRE 2025	Realizar Plan de Contingencia mes de Octubre 2025 Grupo Reincar

ALCANCE: Aplica para todas las carteras del Grupo Reincar en relación con la validación de las amenazas que impidan gestionar cartera.

PLAN DE PRUEBAS

Tipo de prueba:	Revisión de todas las amenazas del Plan de Contingencia del Grupo Reincar.	
Objetivo:	Confirmar y garantizar el funcionamiento de la contingencia en Grupo Reincar.	
Integrantes:	**Nombre**	**Firma**
	Liliana Vega	Auditor Interno
	Julián Pineda	Responsable TIC
Fecha Programada:	Octubre 2025	
Escenario de Interrupción	Grupo Reincar Oficinas 501 y 1301	
Resultado esperado:	Continuidad del negocio cuando se presenten fallas que impidan gestionar cartera.	

Secuencia de pasos para la ejecución de la prueba:	**AMENAZA # 1 CORTE DEL SERVICIO DE LUZ (10 min)** • Se bajan los tacos e inmediatamente se confirmó funcionamiento de la UPS 10KVA  Se confirma que todos los computadores de Grupo Reincar continuaron encendidos.

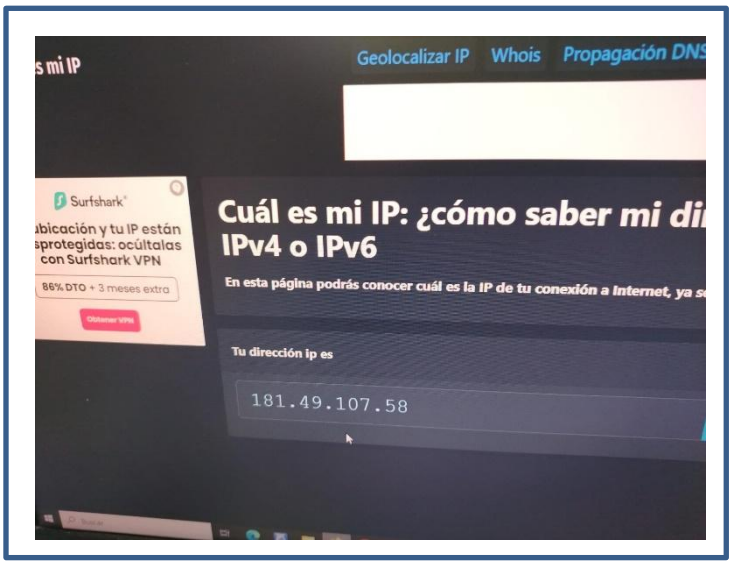
AMENAZA # 2 CORTE DEL SERVICIO DE LUZ (más 10 min)

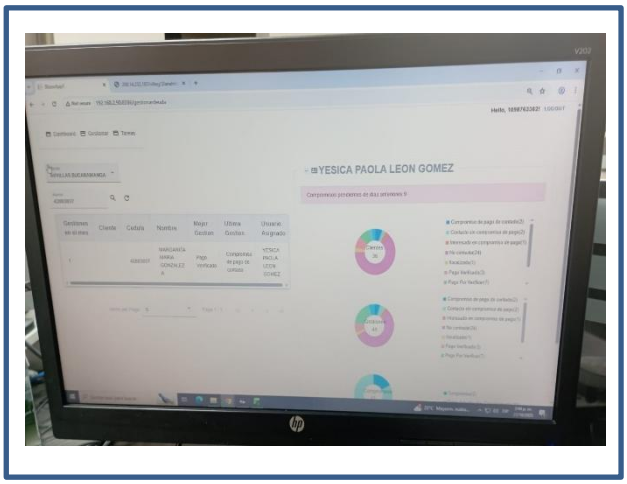
- Se confirma con el área administrativa y gestores de cada cartera que todos los computadores en uso continuaron encendidos.

AMENAZA # 3 CORTE DEL SERVICIO DE INTERNET

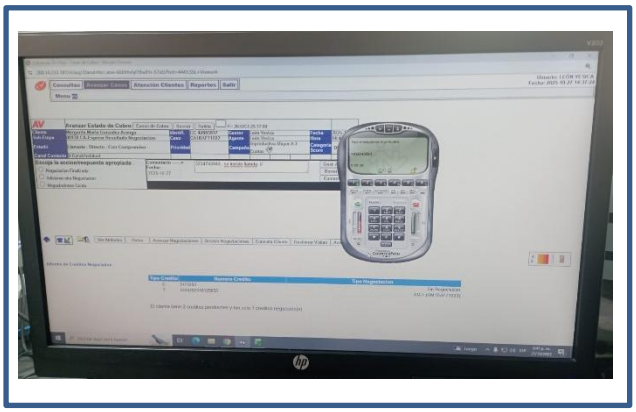
- Se desconectó el internet principal UNE, se conectó el de Claro e inmediatamente funcionó sin presentar dificultad.

Anexo soporte: IP pública servicio de CLARO y se valida acceso aplicativo REINCAR APP.

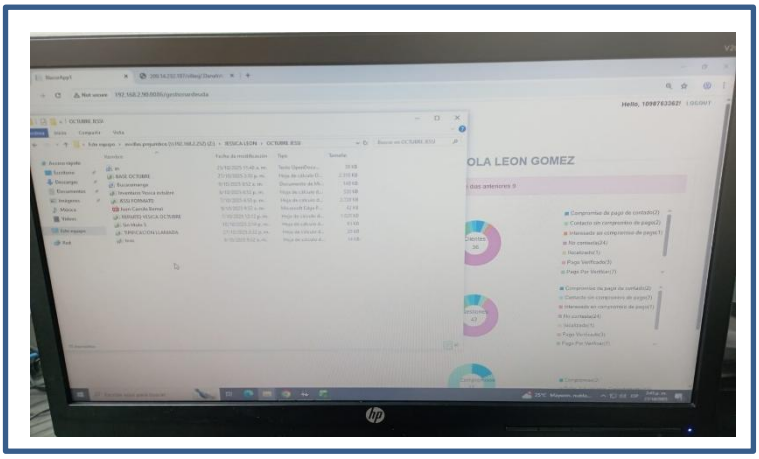




- Se valida el Ingreso al Eyebeam y al aplicativo y funciona correctamente:



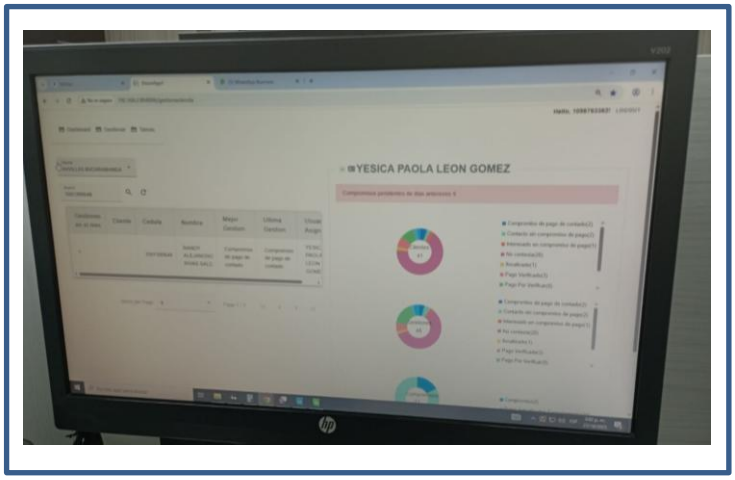
- Se valida que quedó que habilitado el acceso a la carpeta 216 de YESICA PAOLA LEON - CARTERA AVVILLAS BUCARAMANGA



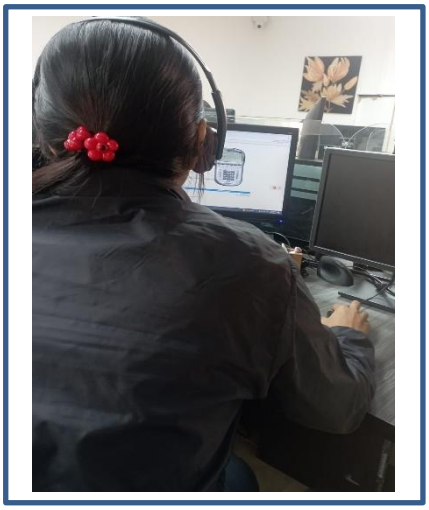
AMENAZA # 4 DAÑO DE COMPUTADOR

- Se realiza la prueba con el computador del gestor Yesica Paola Leon, sistemas realiza la configuración del equipo de respaldo para acceder a los aplicativos necesarios para continuar con la gestión de cobro y se constató que el asesor pudo continuar con sus actividades.

Ingresó al aplicativo REINCARAPP funcionando correctamente:



Ingreso al Eybeam funciona correctamente y al aplicativo:

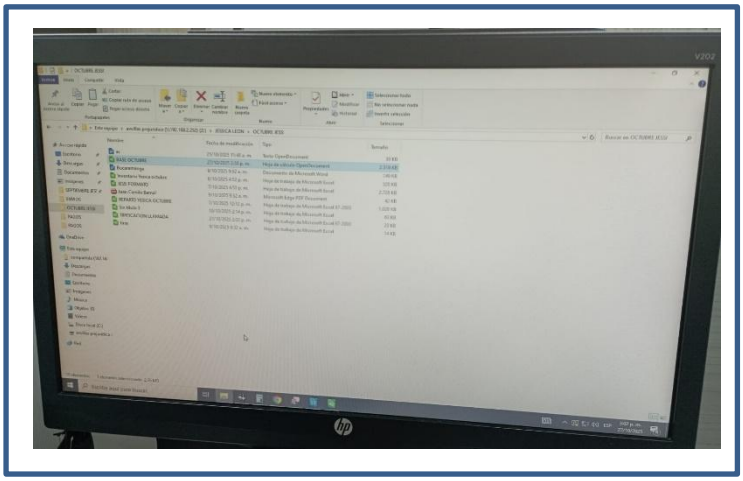


AMENAZA # 5 DAÑO DE SERVIDOR DE TELEFONIA

- Se activa extensión de respaldo en el aplicativo Eybeam en el equipo de la asesora Yesica Paola Leon ext. 215 – de la cartera AVVILLAS BUCARAMANGA y funciona correctamente y se evidencia que la llamada se encuentra en el servidor de respaldo IP://192.168.2.247.

AMENAZA # 6 DAÑO DE SERVIDOR DE DOMINIO

- La prueba se realiza con el gestor Yesica Leon ext. 215 – de la cartera de AVVILLAS BUCARAMANGA y se confirma ingreso a la carpeta personal y funciona correctamente y se evidencia que la llamada se encuentra en el servidor de respaldo IP://192.168.2.252



AMENAZA # 7 INCAPACIDAD DE GESTOR O COORDINADOR

Se valida con la coordinadora de la cartera AVVILLAS ingresa a la carpeta del asesor, organiza la base del asesor incapacitado según la estrategia planteada para el día y prioriza los compromisos de pago vigentes e incumplidos y los montos más altos de la base. Los datos son asignados a los demás asesores que están gestionando la cartera.

En caso de que la incapacidad sea del Coordinador de la Cartera, se realizó prueba con AVVILLAS, desde el área de TICS le habilitan los permisos al Coordinador Junior para que tenga acceso a la carpeta del Coordinador, con el fin de que se garantice la continuidad de la operación, logrando acceder a todos los aplicativos y que pueda descargar la información que envían del banco.

AMENAZA # 8 RETIRO PERMANENTE DE GESTOR O COORDINADOR

El Coordinador de cartera de AVVILLAS ingresa a la carpeta del asesor, organiza la base del asesor retirado según la estrategia planteada para el día y prioriza los compromisos de pago vigentes e incumplidos y los montos más altos de la base. Los datos son asignados a los asesores que están gestionando la cartera.

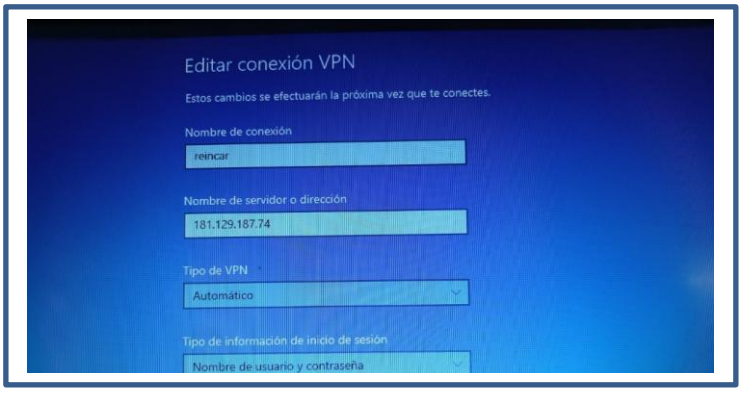
En caso de que el retiro permanente sea del Coordinador de la Cartera, se realizó prueba con AVVILLAS, desde el área de TICS le habiliten los permisos de la carpeta del Coordinador a la líder, con el fin de que se garantice la continuidad de la operación, de acuerdo a los requerimientos del cliente, mientras se inicia inmediatamente el proceso de selección y contratación para el cargo de Coordinador de Cartera.

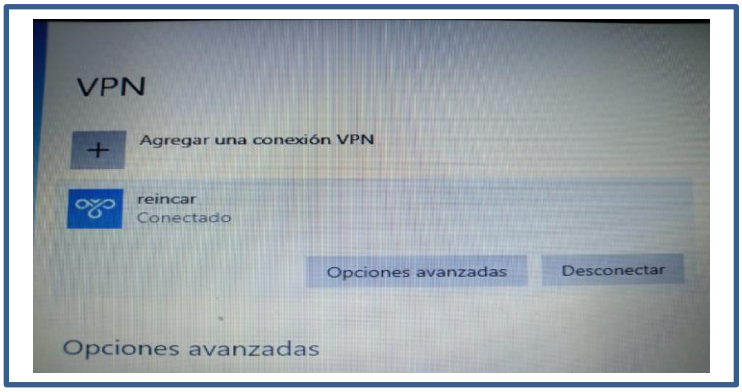
El Coordinador de cartera de AVVILLAS:

- ✓ ingresa a la carpeta del asesor
- ✓ organiza la base del asesor retirado según la estrategia planteada para el día
- ✓ prioriza los compromisos de pago vigentes e incumplidos y los montos más altos de la base
- ✓ los datos son asignados a los asesores que están gestionando la cartera.

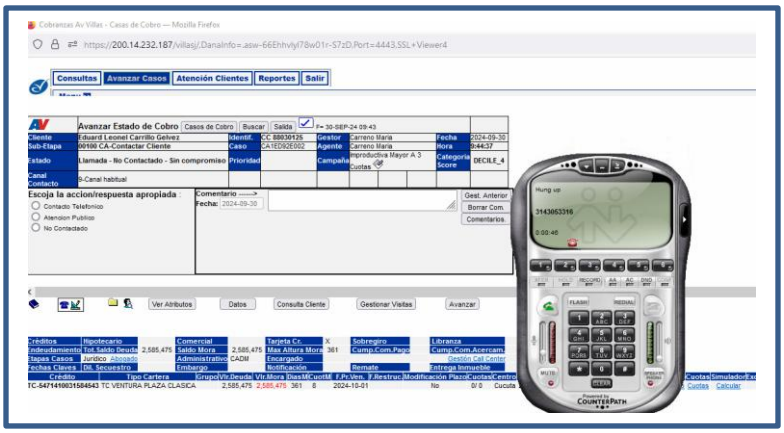
AMENAZA # 9 IMPOSIBILIDAD DE INGRESAR AL EDIFICIO PARA LABORAR POR ASONADA, INUNDACIÓN O DISTURBIO

Se realiza la prueba con la coordinadora de la cartera desde su lugar de residencia, está gestionando a través de la VPN y se evidencia que los aplicativos, llamadas y páginas autorizadas funcionan correctamente.

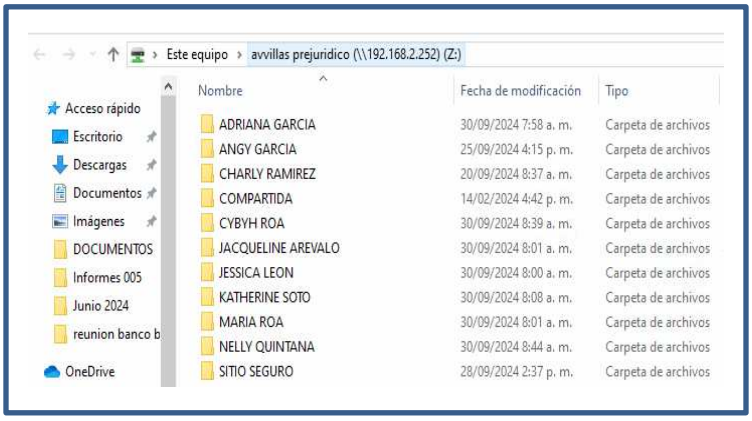
- Configuración y conexión de VPN
  - 

  - 

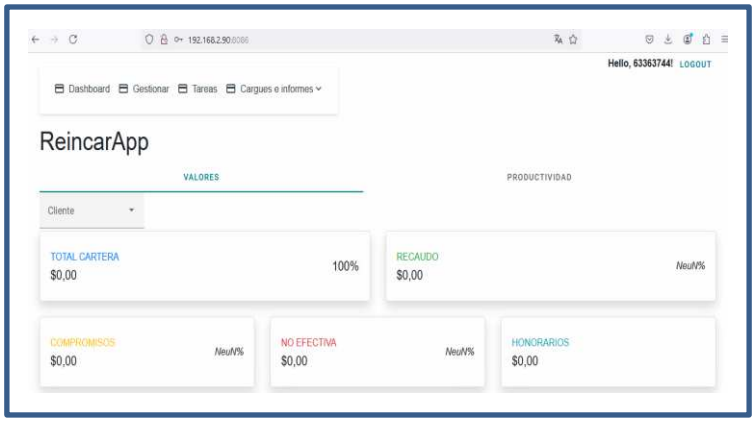
- Se valida acceso al aplicativo del Banco y Eyebeam



- Se valida acceso a la carpeta compartida



- Se valida acceso aplicativo Reincarapp

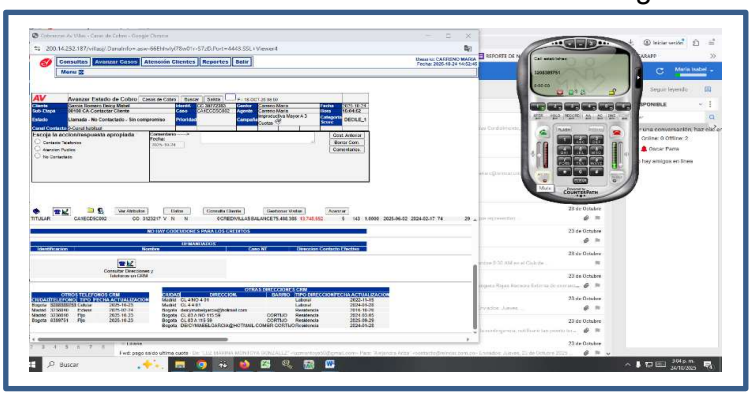


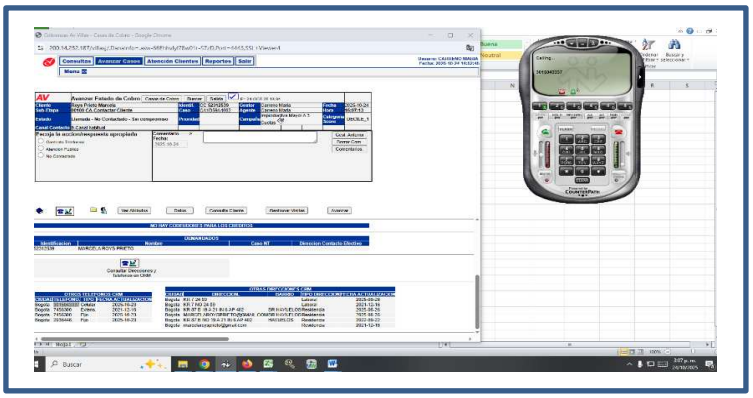
AMENAZA # 10 IMPOSIBILIDAD DE INGRESAR AL EDIFICIO PARA LABORAR POR PERDIDA TOTAL POR INCENDIO O TERREMOTO

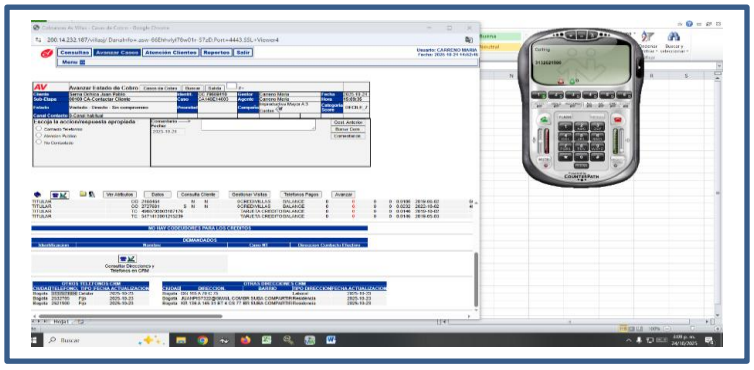
Gestión desde Bucaramanga cartera oficina Bogotá

1. Se ingreso a la base a gestionar.

2. Se ingreso al aplicativo syscorp desde el equipo de la coordinadora ubicado en la oficina de Bucaramanga.







	AMENAZA # 11 DECLARACION DE AISLAMIENTO A NIVEL NACIONAL POR PANDEMIA El centro alterno de gestión para todas las carteras sería el hogar de los empleados que tengan internet en sus hogares. La alternativa técnica es segura a través de una VPN por la cual el gestor accede por medio del computador asignado por la empresa a las carpetas del servidor y a la información de los aplicativos, así como al sistema de telefonía tal como si estuviera en la oficina con las mismas condiciones de seguridad. **AMENAZA # 12 FALLA EN EL SERVIDOR REINCARAPP** Se realiza la prueba con cada coordinador de la cartera AVVILLAS, colocan la plantilla de gestiones masivas en la carpeta compartida para que el asesor registre la información de las gestiones telefónicas. Una vez solucionado el inconveniente con el servidor el coordinador procede a subir la plantilla masivamente al servidor Reincarapp. **AMENAZA # 13 IMPEDIMENTO PARA LA REALIZACIÓN DE MONITOREO.** No es posible ingresar al servidor de llamadas y descargar las grabaciones, el Auditor procede a activar la contingencia informando al Líder de TIC. Como las llamadas quedan guardadas en un disco duro que se encuentra en el servidor de llamadas principal, en caso de no poder descargar la llamada se saca el disco duro del servidor y se conecta al computador del auditor para la realización de los monitoreos. Como opción adicional, también se realiza monitoreo de llamada en línea. Se evidencia como resultado con éxito que se logró acceder a la descarga de las llamadas y realizar los monitoreos asignados en el cronograma de actividades, adicional se realizó el ejercicio de escucha en línea.

	AMENAZA # 14 DAÑO AIRE ACONDICIONADO CUARTO DE DATOS. ▪ Temperatura tomada en el cuarto técnico utilizando el aire acondicionado de respaldo
Resultado obtenido:	Resultado exitoso
Fecha ejecución:	Octubre 2025
Anexos:	Fotografías en cada amenaza

Conclusiones:	• En la amenaza 1 y 2 ***CORTE DEL SERVICIO DE LUZ*** se confirma que todos los computadores de Grupo Reincar continuaron encendidos una vez se bajaron los tacos y entro en funcionamiento la UPS. • En la amenaza 3 ***CORTE SERVICIO DE INTERNET*** se desconectó el internet principal UNE, se conectó el de Claro e inmediatamente funciono el de Claro sin presentar dificultad. Se validó acceso al aplicativo Reincarapp y se valida el ingreso al Eybeam funcionando correctamente, también quedo habilitado el acceso a la carpeta de la cartera. En la amenaza 4 ***DAÑO EN COMPUTADOR*** se constató que el asesor pudo continuar con las gestiones, una vez sistemas realizó la configuración del equipo de respaldo para acceder a los aplicativos y demás • En la amenaza 5 **DAÑO DE SERVICOR DE TELEFONÍA** funciona correctamente el Isabell realizando sin inconveniente la gestión telefónica al titular y se evidencia que la llamada se encuentra en el servidor de respaldo IP://192.168.2.120, una vez fue activada en el aplicativo Eybeam. • En la amenaza 6 **DAÑO DE SERVIDOR DE DOMINIO** se confirma ingreso a la carpeta personal del asesor. • En la amenaza 7 **INCAPACIDAD DE GESTOR O COORDINADOR** Se logró garantizar la continuidad de la operación si un gestor se incapacita o incluso si el coordinador es quien se incapacita. • En la amenaza **8 RETIRO PERMANENTE DE GESTOR O COORDINADOR** se logró garantizar la continuidad de la operación si un gestor se retira inesperadamente o incluso si el coordinador es quien se retira. • **AMENAZA # 12 FALLA EN EL SERVIDOR REINCARAPP** se confirma que la prueba se realizó con total éxito. • **AMENAZA # 13 IMPEDIMENTO PARA LA REALIZACIÓN DE MONITOREO** se logró acceder a la descarga de las llamadas y realizar los monitoreos. • **AMENAZA # 14 DAÑO DE AIRE ACONDICIONADO CUARTO DE DATOS** Se confirma que el aire acondicionado mantiene una temperatura adecuada y funciona de manera óptima.

Genera acción	**Si**		**Acción correctiva**		**Número de la acción**	
	No	**x**	**Acción de mejora**			

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la capacidad operativa para ejecutar el contrato a nivel nacional, conforme a las necesidades del servicio del Fondo Nacional del Ahorrro.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR dispone de los medios idóneos para grabar las comunicaciones al 100% e indexarlas por número telefónico, ext, fecha y hora, desde el que se realiza la llamada, estas grabaciones son almacenadas hasta la finalización del contrato y por un periodo de 3 años más una vez finalizado el mismo y remitidas al Fondo Nacional del Ahorro si este las solicitare.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR mantiene actualiza la información suministrada por los afiliados diariamente tanto en el aplicativo interno Reincarapp como en la herramienta de gestión asignada por el Fondo Nacional del Ahorro - Adminfo, la cual es de total confiabilidad.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR suministra las Líneas telefónicas de atención a usuarios tanto de entrada como de salida de llamadas.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con una Política de Seguridad de la Información TC- PR05 alineada a los requisitos de la norma ISO 2701:2022, garantizando estricto cumplimiento liderado por el Oficial de Seguridad de la Información.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el Antivirus Kaspersky Endpoint Cloud Security Pro, garantizando mecanismos de protección contra virus informáticos, Malware, Spyware, entre otros tipos de código malicioso, el cual se encuentra especificado en el TC-IN01 Política de Uso de Medios Tecnológicos # 4.4.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con herramientas y procedimientos de borrado seguro de datos para el caso de cambios de equipos que contengan información del Fondo Nacional del Ahorro y posterior a la finalización del contrato, migración de datos a otras plataformas, aplicado a todos los ambientes de trabajo con que se cuente (desarrollo, pruebas, producción), el cual se encuentra especificado en el TC-IN01 Procedimiento de Uso de Medios Tecnológicos # 6.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con una Matriz de Riesgos de Seguridad de la Información, que se identifican mediante una metodología de análisis de riesgos donde se valoran los riesgos asociados a la pérdida o fuga de información.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la Cláusula de Confidencialidad tanto para empleados como para terceras partes.

_____

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cumple con las leyes, normativas y regulación colombiana asociada con la protección de la información y los datos personales (Decreto 1377 – Ley 1581), cuenta con un Programa Integral de Protección de Datos Personales GR-PR11 y una Política de Protección de Datos Personales TC-IN03.

_____

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con un área de Capacitación y Formación quien brinda a sus empleados, formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, en relación con la seguridad de la información.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el TC-IN02 Manual de Seguridad de la Información y el TC-IN11 Seguridad física y áreas seguras, donde se identifican los controles de acceso en las instalaciones donde se ejecuta la operación del Fondo Nacional del Ahorro.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el TC-IN02 Manual de Seguridad de la Información #5,4, donde se identifican los procedimientos para retirar los derechos de acceso de todos los empleados a la información y a los servicios de procesamiento de información una vez se finalice su relación contractual.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR establece, documenta y revisa políticas y procedimientos de control de acceso físico a sus instalaciones y centros de procesamiento, contando con el TC-IN02 Manual de Seguridad de la Información # 5.9.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR establece, documenta y revisa políticas y procedimientos de control de acceso lógico, contando en el TC-IN02 Manual de Seguridad de la Información # 5.6 con la Política de Control de Acceso Lógico.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con una Política de Gestión de Contraseñas TC-IN02 Manual de Seguridad de la Información # 5.7, con el objetivo de evitar el uso de claves compartidas, genéricas o para grupos.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el TC-PR03 Procedimiento Gestión de eventos e incidentes de Seguridad de la Información, el cual nos permite detectar, evaluar y analizar cualquier incidente de Seguridad de la Información, así mismo recuperarnos ante un incidentes de seguridad de la información.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con una política TC-IN01 Política de uso de Medios Tecnológicos, para el manejo y uso adecuado de correo electrónico literal 3.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el TC-IN02 Manual de Seguridad de la Información #5.1, donde se identifica la política y un estándar para el manejo de dispositivos móviles (IPAD Tablet, PDA, Netbooks, Phablet, teléfonos), para el uso de la aplicación ADMINFO móvil.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con el TC-IN01 Política de uso de Medios Tecnológicos # 18, garantizando un intercambio seguro de información en caso de compartir información con el Fondo Nacional del Ahorro.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con la TC-IN01 Política de uso de Medios Tecnológicos # 5, la cual especifica la ejecución de las copias de respaldo de la información y la indicación del tiempo de retención de estas.

DIEGO ENRIQUE GONZALEZ
Gerente General

Reincar
Recuperadora Integral de Cartera
NIT. 900.405.236-5

SI-2000523 SC-CER546357

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con un área de Calidad consolidada, en la que se realizan monitoreos permanentemente a los asesores tanto en línea como monitoreo en piso, validando estructura evaluativa, logrando identificar oportunidades de mejora e implementando los planes de acción. Adicionalmente contamos con herramientas tecnológicas que permiten la detección de vulnerabilidades y amenazas de ciberseguridad.

Así mismo manejamos el formato TC-FR07 Tratamiento de incidentes técnicos que afecten la seguridad, cualquier incidente deben reportarlo inmediatamente por el link: https://docs.google.com/forms/d/e/1FAIpQLScHrN-9JG8D2TeHlrJAFP5fx1VxdbRTcSGupKEwEabAYWg11Q/viewform

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR cuenta con un Software legal ReincarApp en el cual se dejan los registros diarios de todas las gestiones.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR no desarrolla software propio, se cuenta con el TC- FR18 Formato para proveedores de requerimientos para desarrollo seguro de software y control de cambios en los diferentes ambientes.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que en REINCAR se realiza el análisis de Vulnerabilidades anualmente incluida la prueba de Ethical Hacking.

DIEGO ENRIQUE GONZALEZ
Gerente General

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **“Confidencial”**.

El presente documento es propiedad de Reincar y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Reincar

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno de Reincar y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

TABLA DE CONTENIDO

INTRODUCCIÓN **2**

DATOS ESPECÍFICOS DE LA PRUEBA 2

INFORME EJECUTIVO **3**

VULNERABILIDADES: **6**

1. Certificado TLS 6
2. Divulgación de información en encabezados HTTP 7
3. Validación inadecuada de intentos fallidos de inicio de sesión 9
4. Protección inadecuada de cookies 10
5. Ausencia de cabeceras de seguridad 12
6. Divulgación de información 13

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Aplicación Issabel

INTRODUCCIÓN

Reincar es una empresa constituida desde el 2010 por socios expertos en el sector de cobranzas, que nació como una respuesta a la necesidad de mejorar los procesos de cobranza y atención al cliente, brindado un mejor servicio, entendiendo las necesidades de nuestros clientes con una correcta asesoría que permita una efectiva recuperación en corto tiempo.

DATOS ESPECÍFICOS DE LA PRUEBA

A continuación se mencionan los datos relacionados a la planeación del proyecto:

Datos Básicos	
ID proyecto	Aplicación Issabel-2025-04
Fecha Ejecución	Fri Apr 04 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Hora Ejecución Inicial	8:00 a.m (hora colombia)
Hora Ejecución Final	6:00 p.m (hora colombia)
País	Colombia
Datos Específicos de la prueba	
Tipo de Prueba	Caja negra
Descripción del tipo de prueba	Pentesting
Origen de la prueba	Internas
Tipo de Activo	Aplicación web

Tabla 1 - Datos específicos de la prueba

Las pruebas de la auditoría se han realizado sobre los siguientes activos:

Activo	**Descripción**
Aplicación Issabel	Aplicación de PBX

Tabla 2 - Activos a auditar dentro del alcance

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

INFORME EJECUTIVO

Tras la auditoría realizada se muestra una tabla informativa clasificando las vulnerabilidades encontradas:

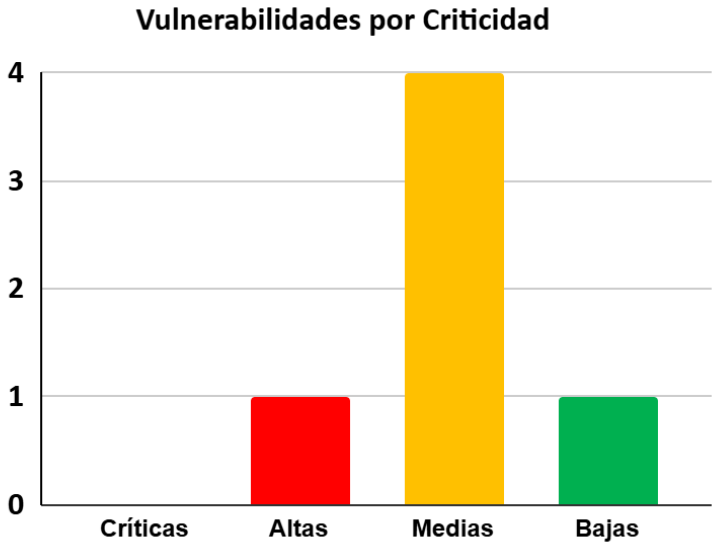


Ilustración 1 - Vulnerabilidades encontradas por criticidad.

Y cuyo cuadro resumen es:

Vulnerabilidades	Número	Criticidad	Estado
Certificado TLS	1	High	**Activa**
Divulgación de información en encabezados HTTP	1	Low	**Activa**
Dependencia de componente vulnerable	1	Medium	**Activa**
Validación inadecuada de intentos fallidos de inicio de sesión	1	Medium	**Activa**
Protección inadecuada de cookies	1	Medium	**Activa**
Ausencia de cabeceras de seguridad	1	Medium	**Activa**
Divulgación de información	1	Medium	**Activa**

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Tabla 3 - Número de vulnerabilidades y su criticidad.

VULNERABILIDADES:

1. Certificado TLS

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**High**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Certificado TLS

Descripción

TLS (o SSL) ayuda a proteger la confidencialidad e integridad de la información en tránsito entre el navegador y el servidor, y proporciona autenticación de la identidad del servidor. Para cumplir con este propósito, el servidor debe presentar un certificado TLS que sea válido para el nombre de host del servidor, emitido por una autoridad de confianza y válido para la fecha actual. Si no se cumple alguno de estos requisitos, las conexiones TLS al servidor no proporcionarán la protección completa para la que se diseñó TLS.

Cabe señalar que existen varios ataques contra TLS en general, y en el contexto de las conexiones web HTTPS en particular. Es posible que un atacante determinado y en una posición adecuada comprometa las conexiones TLS sin detección del usuario, incluso cuando se utiliza un certificado TLS válido.

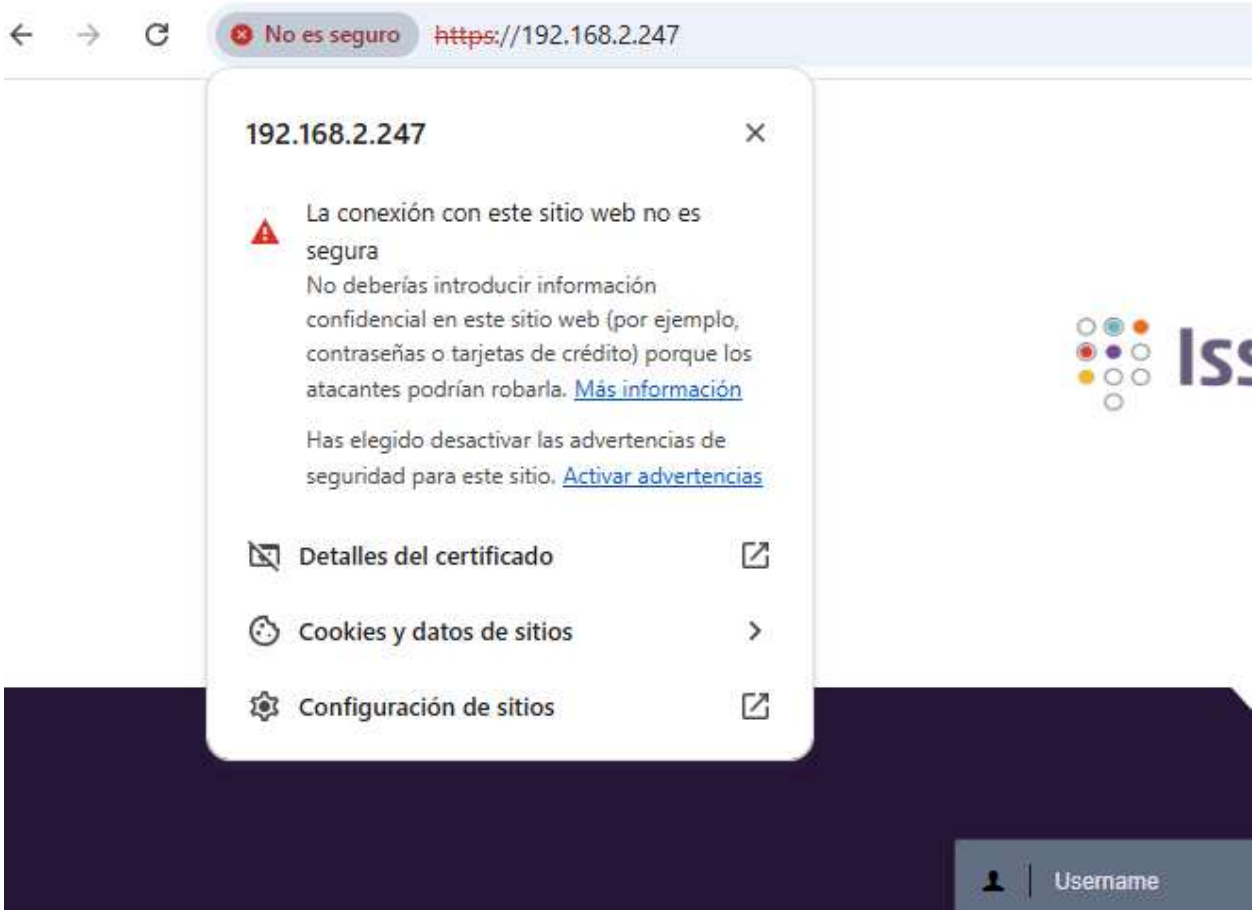
Se identifica que los certificado instalados para la aplicaciòn ISSABEL están vencidos por lo cual la comunicación cliente servidor es insegura

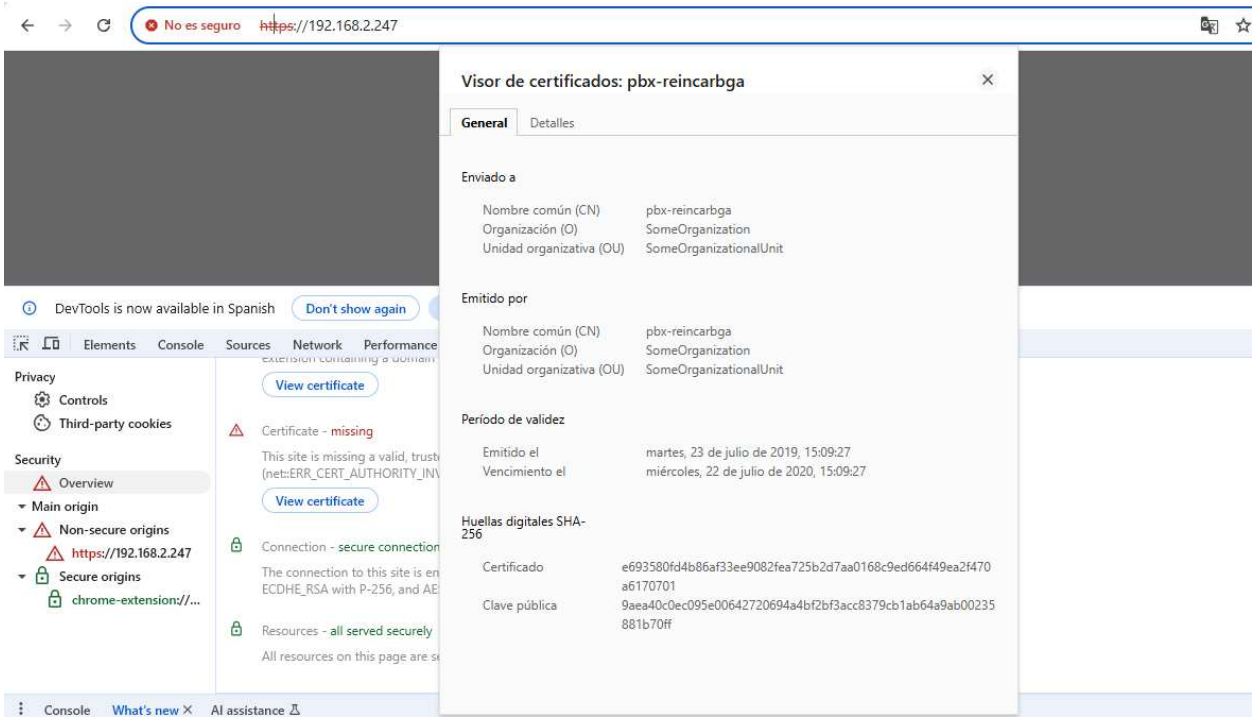
Impacto

Cabe señalar que existen varios ataques contra TLS en general, y en el contexto de las conexiones web HTTPS en particular. Es posible que un atacante determinado y en una posición adecuada comprometa las conexiones TLS sin detección del usuario, incluso cuando se utiliza un certificado TLS válido

Explotación / Descubrimiento

Se identifica que el certificado TLS está vencido





Mitigación / Solución

- Se debe solo hacer uso del protocolo TLS en las versiones 1.2 y 1.3, adicional, se debe evitar el uso de algoritmos de cifrado como DES, 3DES,CBC

Referencias

- https://wiki.mozilla.org/Security/Server_Side_TLS

2. Divulgación de información en encabezados HTTP

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Low**
Categoría	Web
Prueba	Manual

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Plataforma	Web

Tabla - Divulgación de información en encabezados HTTP

Descripción

Los encabezados HTTP son un gran refuerzo para la seguridad web con una fácil implementación. Los encabezados de respuesta HTTP adecuados pueden ayudar a prevenir vulnerabilidades de seguridad como Cross-Site Scripting, Clickjacking, divulgación de información y más.

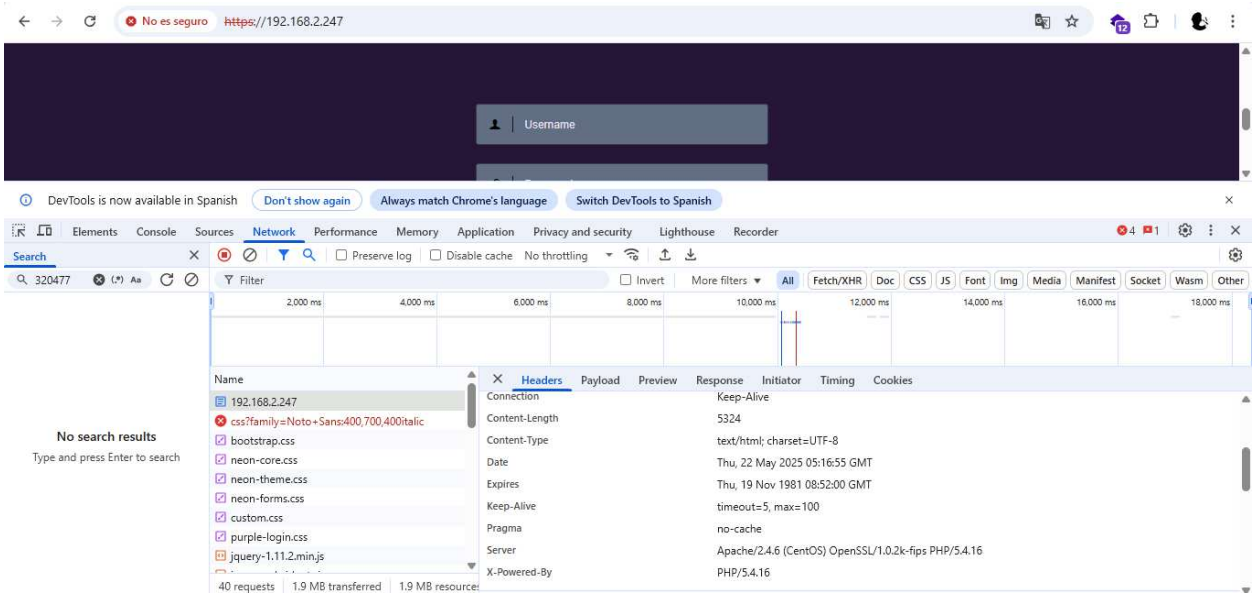
Se identifica la divulgación del servidor web en las respuesta del servidor de ISSABEL

Impacto

El Server Encabezado describe el software utilizado por el servidor de origen que manejó la solicitud, es decir, el servidor que generó la respuesta.

Explotación / Descubrimiento

Evidencia de la respuesta de la versión de apache



Mitigación / Solución

- Elimine este encabezado o establezca valores no informativos. Server: webserver

Referencias

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#server

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

1. Dependencia de componente vulnerable

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Dependencia de componente vulnerable

Descripción

El uso de componentes de terceros puede introducir una variedad de vulnerabilidades basadas en DOM, inyecciones u otras.

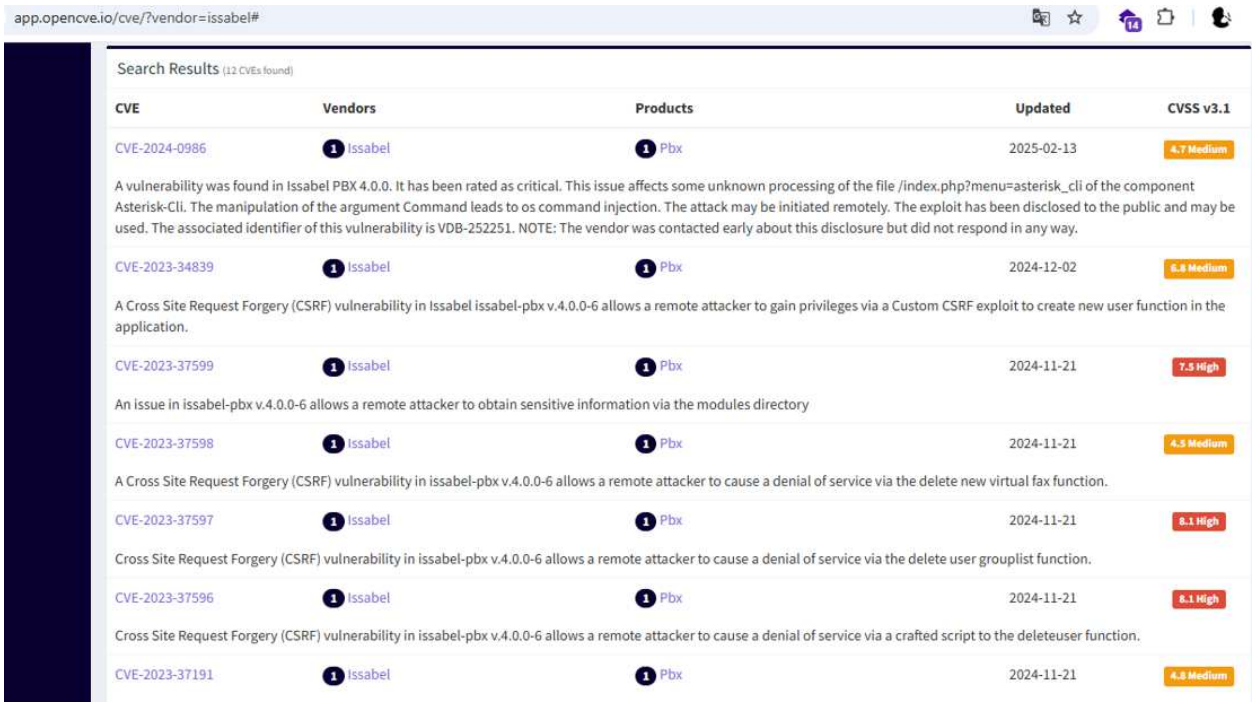
Se identifica múltiples vulnerabilidades públicas en la versión de Issabel actual, sin embargo, la vulnerabilidad más crítica no fue posible explotarla ya que no se cuenta con la versión de asterisk que es vulnerable, adicional por el nivel de exposición del activo (red interna) las vulnerabilidades bajan de severidad considerablemente.

Impacto

Algunas vulnerabilidades del software pueden llevar a acceso no autorizado del servidorl, por lo que recomendamos aplicar todas las actualizaciones de seguridad disponibles independientemente.

Explotación / Descubrimiento

Vulnerabilidades públicas que se verificaron durante el ejercicio



Mitigación / Solución

- Actualizar a la version mas reciente de Issabel

Referencias

- https://cwe.mitre.org/data/definitions/1104.html

3. Validación inadecuada de intentos fallidos de inicio de sesión

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Plataforma	Web

Tabla - Validación inadecuada de intentos fallidos de inicio de sesión

Descripción

Esta vulnerabilidad se produce cuando un sistema no implementa medidas para limitar el número de intentos de inicio de sesión fallidos que un usuario puede realizar antes de bloquear su cuenta o tomar otras medidas de seguridad. Si un sistema no tiene estas medidas, un atacante podría utilizar herramientas automatizadas para probar una gran cantidad de combinaciones de nombre de usuario y contraseña hasta que encuentre la combinación correcta.

No se evidencia un control anti automatización en el login de la aplicación ISSABEL

Impacto

La validación inadecuada de intentos fallidos de inicio de sesión puede tener graves consecuencias para la seguridad de los sistemas y las cuentas de usuario.

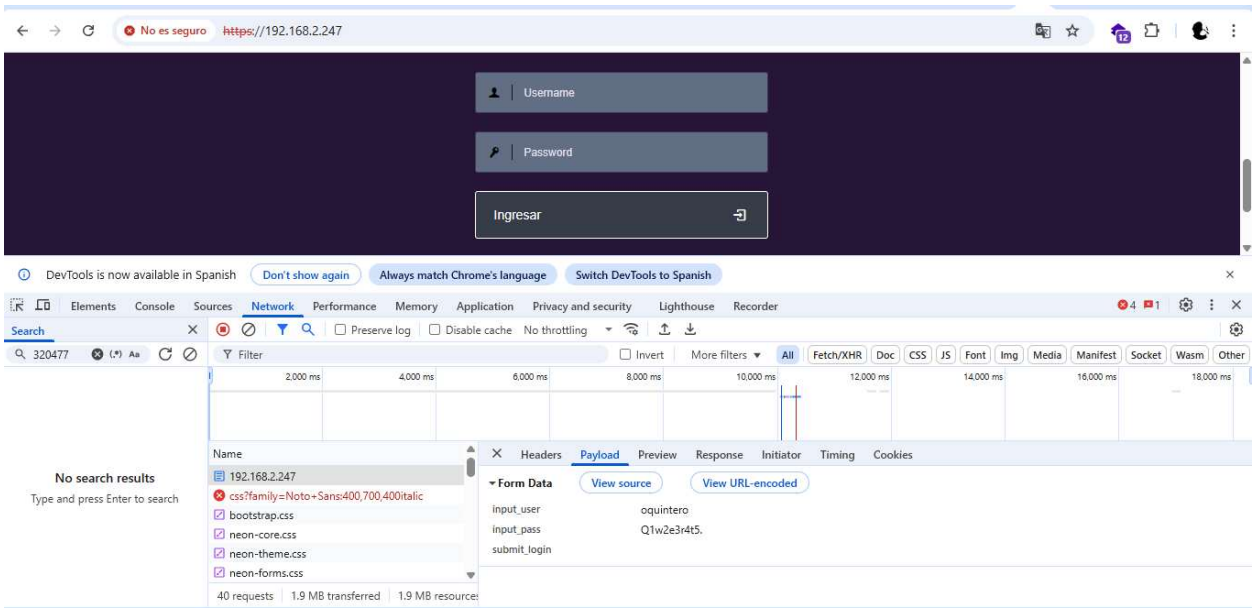
Acceso no autorizado: Si un atacante puede realizar intentos de inicio de sesión fallidos ilimitados, podría eventualmente adivinar la contraseña correcta y acceder a una cuenta sin autorización.

Robo de datos: Una vez que un atacante tiene acceso a una cuenta, puede robar datos sensibles o confidenciales, como información financiera, información personal o datos empresariales.

Explotación / Descubrimiento

No se evidencia la implementación de captcha

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD



Mitigación / Solución

- Para prevenir la vulnerabilidad de la validación inadecuada de intentos fallidos de inicio de sesión, los mecanismos de autenticación deben implementar medidas de seguridad adecuadas, como el bloqueo de la cuenta después de un número determinado de intentos fallidos, la implementación de un tiempo de espera después de varios intentos fallidos y la implementación de herramientas de protección contra ataques de fuerza bruta, como el captcha o los sistemas de prueba de trabajo.

Referencias

- NIST Special Publication 800-63B: Digital Identity Guidelines: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

  OWASP Cheat Sheet Series: Authentication: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#Lockout_Brute_Force_Defenses

  Microsoft Docs: Best practices for preventing DoS attacks: https://docs.microsoft.com/en-us/azure/architecture/patterns/prevention/denial-of-service-prevention

4. Protección inadecuada de cookies

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Protección inadecuada de cookies

Descripción

Se ha evidenciado que las banderas httponly y secure no se están implementando en el envío de las cookies entre cliente y servidor. La bandera httponly garantiza que en un ataque XSS no pueda ser obtenida la cookie en mención, por otro lado, la cabecera secure asegura que la cookie solo pueda ser enviada cuando el tráfico entre cliente y servidor se da a través de HTTPS.

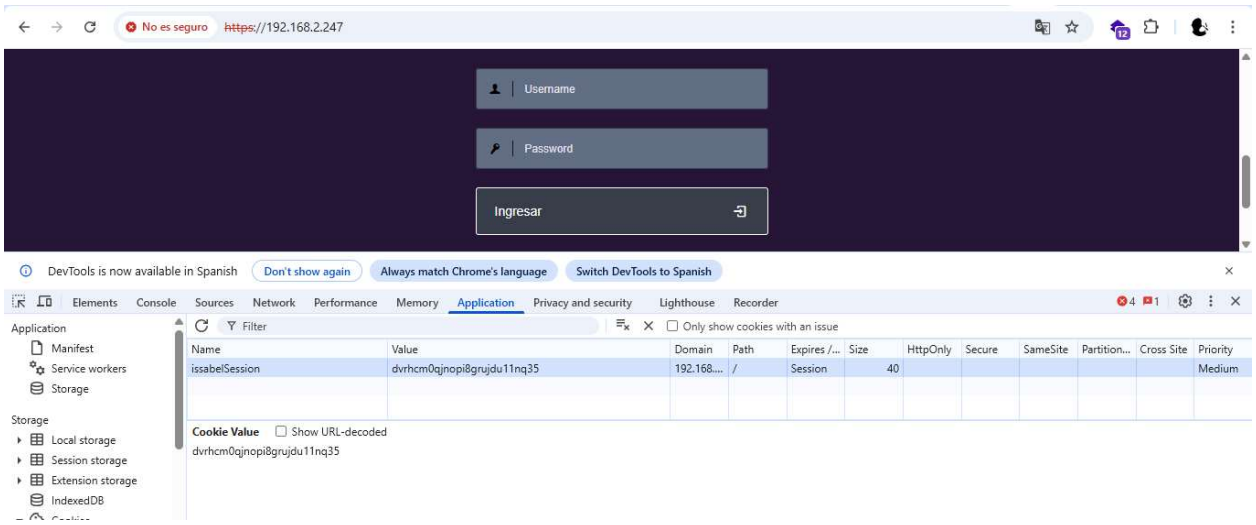
Se identifica que la aplicaciòn ISSABEL no asegura de forma adecuada sus cookies de sesiòn

Impacto

El no implementar las banderas en las cookies mencionadas podría causar que si un atacante lanza exitosamente un ataque de hombre en el medio o de XSS pueda acceder a las cookies y de esta manera comprometer y secuestrar la sesión del usuario víctima.

Explotación / Descubrimiento

Cookies sin atributo HTTPOnly y Secure



Mitigación / Solución

- Establecer el uso de las banderas mencionadas (HttpOnly y Secure) en las cookies enviadas entre cliente y servidor de la siguiente manera:

  Set-Cookie: <<cookie>>; Expires=<<fecha de expiración>>; Secure; HttpOnly

Referencias

- https://resources.infosecinstitute.com/topic/securing-cookies-httponly-secure-flags/

5. Ausencia de cabeceras de seguridad

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual
Plataforma	Web

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Tabla - Ausencia de cabeceras de seguridad

Descripción

No se presentan cabeceras de seguridad que evitan diferentes ataques a la aplicación, tales como Content-Security-Policy, Strict-Tranport-Security, X-Content-Type-Options, X-Frame-Options, entre otras

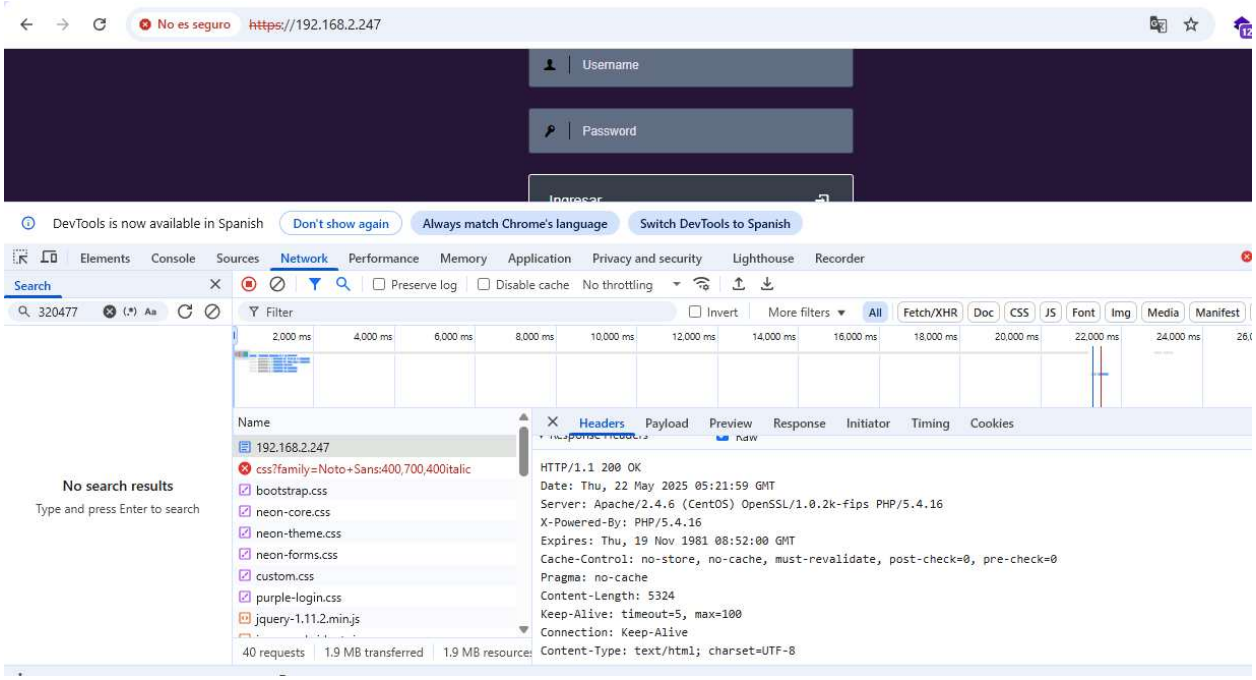
Se identifica que ISSABEL no implementa las cabeceras de seguridad HTTP

Impacto

Permite la ejecución de diferentes ataques como incrustar el sitio en otro, degradar la conexión pasando de HTTPS a HTTP, entre otros.

Explotación / Descubrimiento

Evidencia de la implementación de cabeceras HTTP



Mitigación / Solución

- Agregar las cabeceras de seguridad requeridas.

Referencias

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

6. Divulgación de información

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.247
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Divulgación de información

Descripción

La divulgación de información, también conocida como fuga de información, es cuando un sitio web revela involuntariamente información confidencial a sus usuarios. Dependiendo del contexto, los sitios web pueden filtrar todo tipo de información a un atacante potencial, que incluye: Datos sobre otros usuarios, como nombres de usuario o información financiera Datos comerciales o empresariales sensibles Detalles técnicos sobre el sitio web y su infraestructura

Se identifica rutas en el servidor que permiten la consulta de carpetas de la aplicaciòn ISSABEL

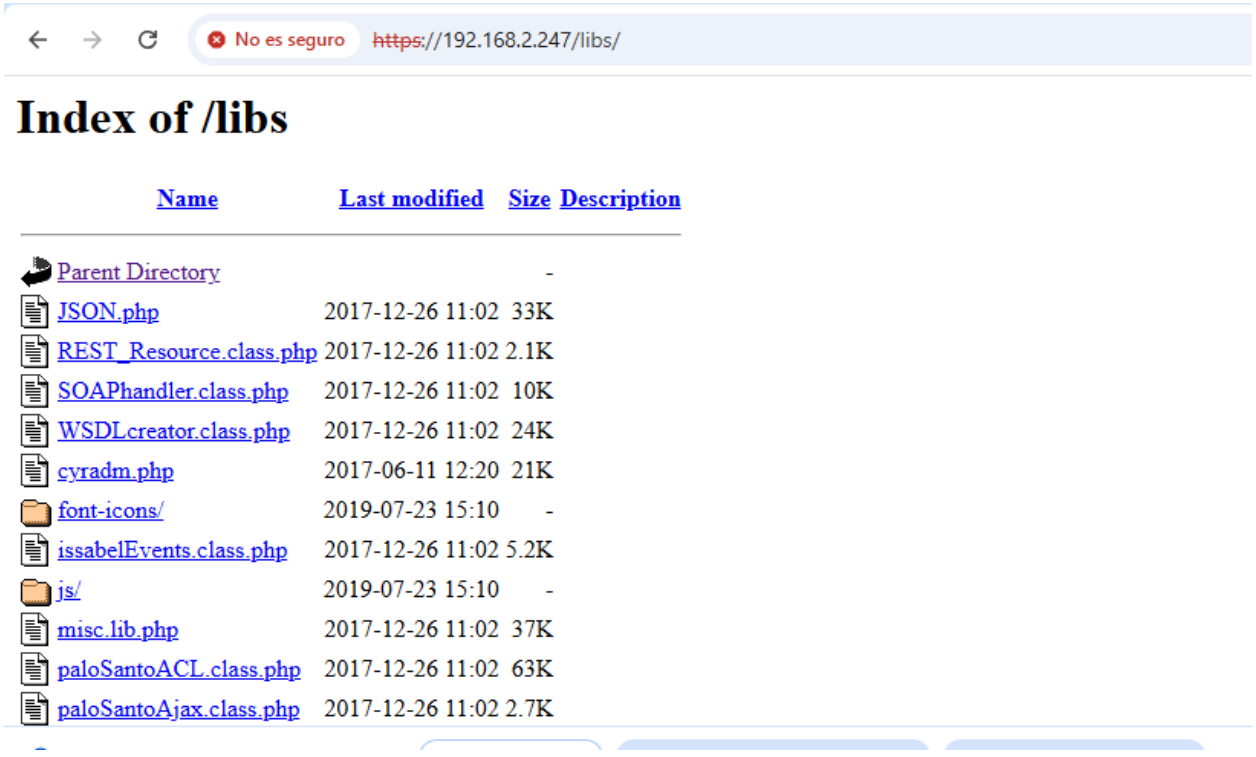
Impacto

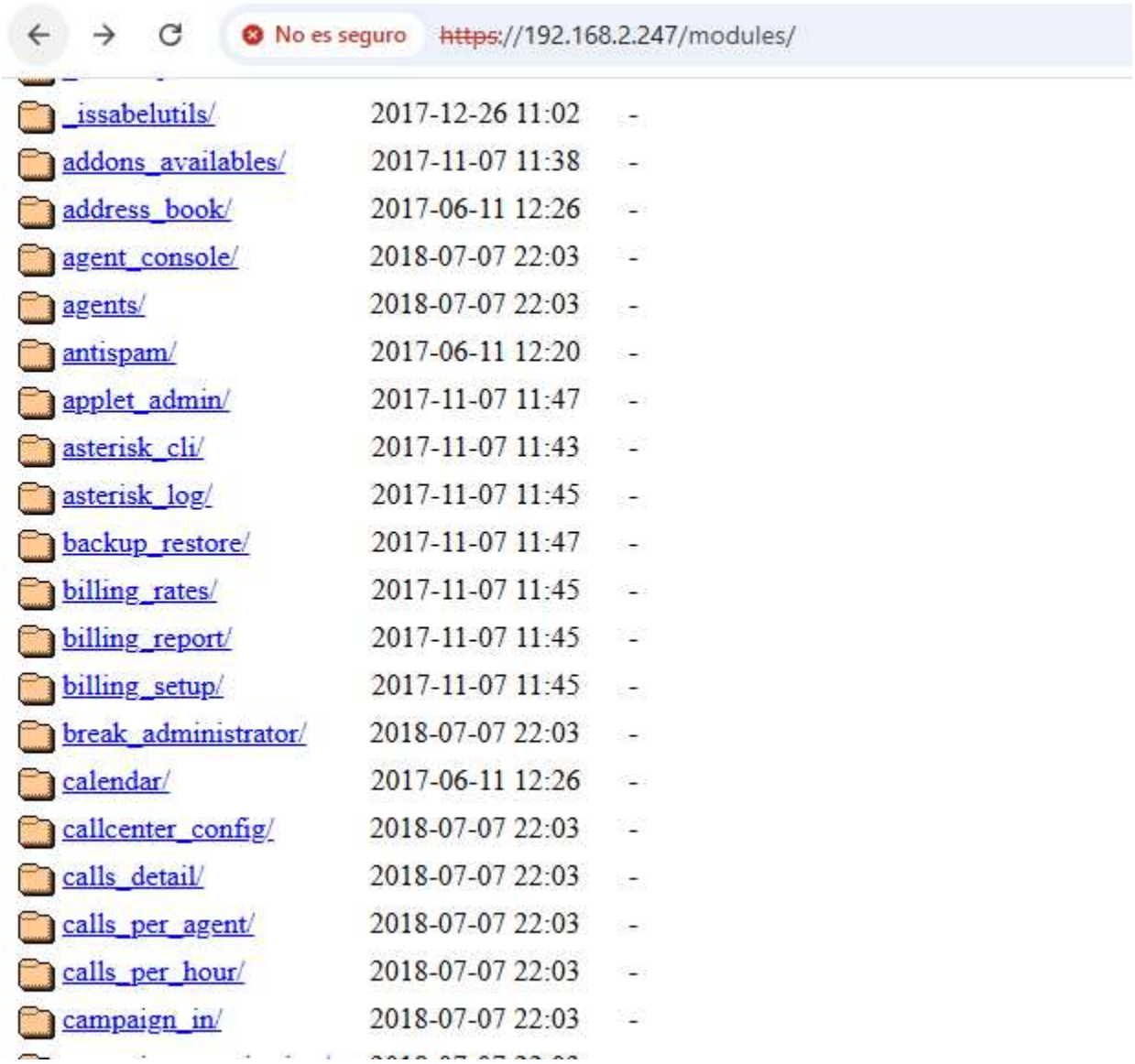
Vulnerabilidades de divulgación de información En esta sección, explicaremos los conceptos básicos de las vulnerabilidades de divulgación de información y describiremos cómo puede encontrarlas y explotarlas. También ofreceremos orientación sobre cómo puede evitar las vulnerabilidades de divulgación de información en sus propios sitios web. infografía de divulgación de información Aprender a encontrar y explotar la divulgación de información es una habilidad vital para cualquier probador. Es probable que lo encuentre regularmente y, una vez que sepa cómo explotarlo de manera efectiva, puede ayudarlo a mejorar la eficiencia de sus pruebas y permitirle encontrar errores adicionales de alta gravedad. laboratorios Si ya está familiarizado con los conceptos básicos detrás de las vulnerabilidades de divulgación de información y solo quiere practicar cómo explotarlas en algunos objetivos realistas y deliberadamente vulnerables, puede acceder a todos los laboratorios de este tema desde el siguiente enlace. Ver todos los laboratorios de divulgación de información ¿Qué es la

divulgación de información? La divulgación de información, también conocida como fuga de información, es cuando un sitio web revela involuntariamente información confidencial a sus usuarios. Dependiendo del contexto, los sitios web pueden filtrar todo tipo de información a un atacante potencial, que incluye: Datos sobre otros usuarios, como nombres de usuario o información financiera Datos comerciales o empresariales sensibles Detalles técnicos sobre el sitio web y su infraestructura Los peligros de filtrar datos confidenciales de usuarios o empresas son bastante obvios, pero la divulgación de información técnica a veces puede ser igual de grave. Aunque parte de esta información tendrá un uso limitado, puede ser potencialmente un punto de partida para exponer una superficie de ataque adicional, que puede contener otras vulnerabilidades interesantes. El conocimiento que puede recopilar podría incluso proporcionar la pieza faltante del rompecabezas cuando intenta construir ataques complejos de alta gravedad.

Explotación / Descubrimiento

Evidencia de los directorios de ISSABEL





Mitigación / Solución

- Evitar por completo la divulgación de información es complicado debido a la gran variedad de formas en que puede ocurrir. Sin embargo, existen algunas mejores prácticas generales que puede seguir para minimizar el riesgo de que este tipo de vulnerabilidades se introduzcan en sus propios sitios web. Asegúrese de que todos los

involucrados en la producción del sitio web sean plenamente conscientes de qué información se considera confidencial. A veces, la información aparentemente inofensiva puede ser mucho más útil para un atacante de lo que la gente cree. Resaltar estos peligros puede ayudar a garantizar que su organización maneje de manera más segura la información confidencial en general.

Referencias

- https://portswigger.net/web-security/information-disclosure

3. ANEXOS

3.1. Anexo 1 - Referencias

Metodologías

Como base para la realización de servicios de Seguridad, y más concretamente las auditorías de seguridad, Hacking ético y pentesting, los auditores utilizan varias metodologías y estándares internacionalmente difundidos y reconocidos como son:

OWASP (*Open Web Application Security Project*) – Guía de realización de pruebas de seguridad en aplicaciones Web.

- http://www.owasp.org/

Nomenclatura

CPE (Common Platform Enumeration) es el listado de tipos de plataformas y sistemas que permite identificar unívocamente un sistema específico con su versión y detalles

- https://nvd.nist.gov/cpe.cfm

CVE (Common Vulnerabilities and Exposures), ***CWE*** (Common Weakness Enumeration) y ***CAPEC*** (Common Attack Pattern Enumeration and Classification) son listas de vulnerabilidades específicas o tipos de vulnerabilidades genéricas que tiene por objeto proporcionar nombres comunes a los problemas conocidos públicamente.

- http://www.cve.mitre.org/
- http://cwe.mitre.org/
- http://capec.mitre.org/

Con el objeto de crear una valoración objetiva de las vulnerabilidades, se utiliza el sistema de valoración de vulnerabilidades definido en CVSS.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

El ***CVSS*** (Common Vulnerability Scoring System), es el sistema que define la métrica para poder medir y establecer el valor numérico del impacto de una vulnerabilidad en un sistema. Vector CVSS que contienen las cifras de base tienen la siguiente forma:

- (AV:[L,A,N]/AC:[H,M,L]/Au:[N,S,M]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C])

Las letras entre paréntesis representan los valores posibles de una métrica CVSS. Exactamente una opción se debe seleccionar para cada conjunto de corchetes. Las letras fuera de los corchetes son obligatorias y deben incluirse a fin de crear un vector CVSS válido. Cada letra o un par de letras es una abreviatura o de un valor de métrica en valor CVSS.

- Métricas: AV = Vector de Acceso (L = acceso local, A = Red adyacente, N = Internet)
- Métricas: AC = Complejidad de Acceso (H = Alta, M = Mediano, L = Bajo)
- Métricas: Au = Autenticación (N= No requerido, S = Un sistema, M = Múltiples sistemas)
- Métricas: C = Impacto a la Confidencialidad (N = No, P = Parcial, C = Completa)
- Métricas: I = Impacto a la Integridad (N = No, P = Parcial, C = Completa)
- Métricas: A = Impacto a la Disponibilidad (N = No, P = Parcial, C = Completa)

http://nvd.nist.gov/cvss.cfm?version=2

Para establecer las clasificaciones de impacto, se sigue como base la recomendación de la NVD, Base de Datos Nacional de Vulnerabilidades, en base a los resultados de los CVSS:

- La vulnerabilidad etiquetada de '**Crítica**' tiene un CVSS base de puntuación entre 9.6 y 10.0.
- La vulnerabilidad etiquetada de '**Alta**' tiene un CVSS base de puntuación entre 7.0 y 9.5.
- La vulnerabilidad etiquetada de '**Media**' tiene un CVSS base de puntuación entre 4.0 y 6.9.
- La vulnerabilidad etiquetada de '**Baja**' tiene un CVSS base de puntuación entre 0.1 y 3.9.
- La vulnerabilidad etiquetada de '**Información**' tiene un CVSS base de puntuación de 0.0.

Definiciones

Vulnerabilidad: Un error, falla, debilidad, o la exposición de una aplicación, sistema, dispositivo o servicio que podría dar lugar a un incumplimiento de la confidencialidad, integridad o disponibilidad.

Amenaza: La frecuencia o probabilidad de que un hecho dañoso se produzca.

Riesgo: Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.

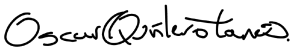
INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Activo: Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La empresa asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

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 adecuado.



Oscar Arnulfo Quintero Torres
Máster en ciberseguridad

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **“Confidencial”**.

El presente documento es propiedad de Reincar y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Reincar

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno de Reincar y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

TABLA DE CONTENIDO

INTRODUCCIÓN **3**

DATOS ESPECÍFICOS DE LA PRUEBA 3

INFORME EJECUTIVO **4**

VULNERABILIDADES: **5**

1. Comunicación insegura por HTTP 5

2. Validación inadecuada de los datos de entrada que ingresan los usuarios en la aplicación 6

3. Ausencia de cabeceras de seguridad 9

4. Protección inadecuada de cookies 10

5. Validación inadecuada de intentos fallidos de inicio de sesión 12

3. ANEXOS **14**

3.1. Anexo 1 - Referencias 14

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Aplicación ReincarApp

INTRODUCCIÓN

Reincar es una empresa constituida desde el 2010 por socios expertos en el sector de cobranzas, que nació como una respuesta a la necesidad de mejorar los procesos de cobranza y atención al cliente, brindado un mejor servicio, entendiendo las necesidades de nuestros clientes con una correcta asesoría que permita una efectiva recuperación en corto tiempo.

DATOS ESPECÍFICOS DE LA PRUEBA

A continuación se mencionan los datos relacionados a la planeación del proyecto:

Datos Básicos	
ID proyecto	Aplicación ReincarApp-2025-04
Fecha Ejecución	Fri Apr 04 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Hora Ejecución Inicial	8:00 a.m (hora colombia)
Hora Ejecución Final	6:00 p.m (hora colombia)
País	Colombia
Datos Específicos de la prueba	
Tipo de Prueba	Caja Negra
Descripción del tipo de prueba	Pentesting
Origen de la prueba	Internas
Tipo de Activo	Aplicación web

Tabla 1 - Datos específicos de la prueba

Las pruebas de la auditoría se han realizado sobre los siguientes activos:

Activo	**Descripción**
Aplicación ReincarApp	Aplicación de cartera reincarAPP

Tabla 2 - Activos a auditar dentro del alcance

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

INFORME EJECUTIVO

Tras la auditoría realizada se muestra una tabla informativa clasificando las vulnerabilidades encontradas:

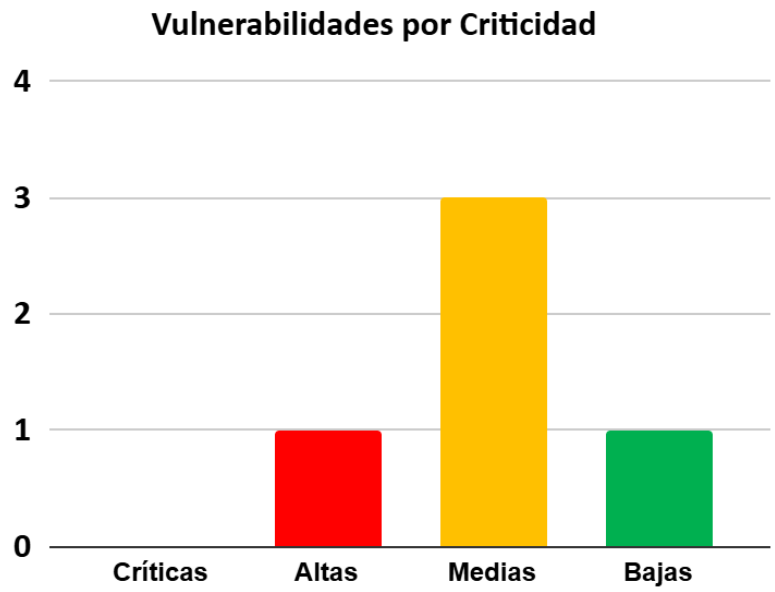


Ilustración 1 - Vulnerabilidades encontradas por criticidad.

Y cuyo cuadro resumen es:

Vulnerabilidades	Número	Criticidad	Estado
Comunicación insegura por HTTP	1	High	Activa
Validación inadecuada de los datos de entrada que ingresan los usuarios en la aplicación (XSS Persistente)	1	Low	Activa
Ausencia de cabeceras de seguridad	1	Medium	Activa
Protección inadecuada de cookies	1	Medium	Activa
Validación inadecuada de intentos fallidos de inicio de sesión	1	Medium	Activa

Tabla 3 - Número de vulnerabilidades y su criticidad.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

VULNERABILIDADES:

1. Comunicación insegura por HTTP

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	http://192.168.2.17:8088/
Datos	
Criticidad	**High**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Comunicación insegura por HTTP

Descripción

La comunicación no presenta cifrado a nivel de transporte, enviando la comunicación por HTTP y no HTTPS

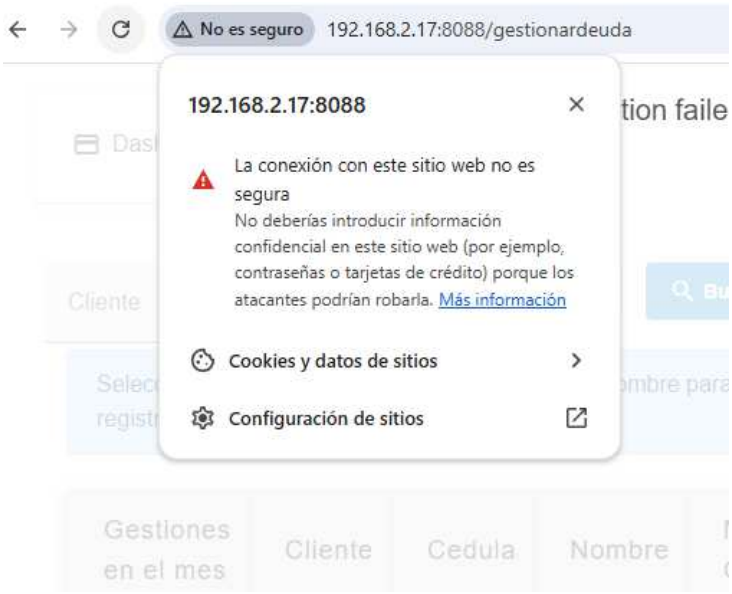
Durante la actividad se logra identificar que existen varias cabeceras de seguridad ausentes.

Impacto

La comunicación puede ser capturada y visualizada por un externo sin autorización de acceder a la información.

Explotación / Descubrimiento

Se identifica que ReincarAPP no hace uso del protocolo HTTPS por lo cual la comunicación puede ser susceptible a captura de tráfico en texto plano



Mitigación / Solución

- Utilizar comunicación HTTPS y redireccionar la comunicación del puerto 80 al 443.

Referencias

- https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

2. Validación inadecuada de los datos de entrada que ingresan los usuarios en la aplicación

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	http://192.168.2.17:8088/
Datos	
Criticidad	**Low**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Validación inadecuada de los datos de entrada que ingresan los usuarios en la aplicación

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Descripción

Los atacantes pueden aprovechar esta vulnerabilidad para inyectar código malicioso en una página web que luego se almacena en la base de datos de la aplicación, y se muestra cada vez que se carga la página web afectada.

Se identifica que la aplicación no sanitiza las entradas del usuario, aunque no se logra llevar la debilidad a una vulnerabilidad puntal es una mala práctica aceptar caracteres especiales en las entradas del usuario

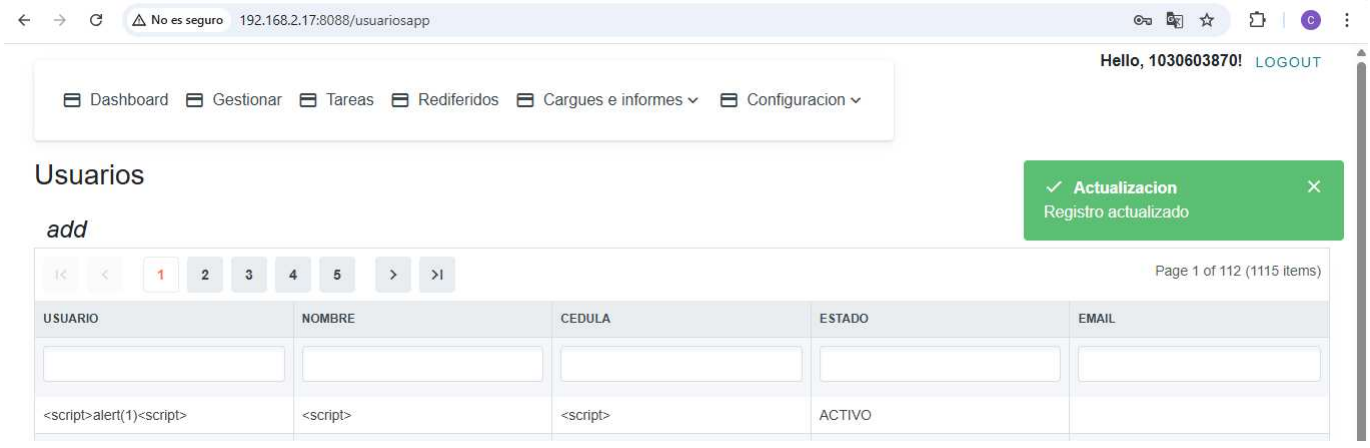
Impacto

La inyección de código malicioso puede ser utilizada para realizar diversas acciones maliciosas, como robar credenciales de usuario, realizar ataques de phishing, redirigir al usuario a un sitio web malicioso o incluso tomar el control total de la sesión del usuario.

El ataque XSS Persistente se diferencia del XSS Reflejado (Reflected Cross-Site Scripting) en que este último no almacena el código malicioso en la base de datos de la aplicación, sino que lo devuelve directamente al usuario a través de la respuesta HTTP. El XSS Persistente, por otro lado, tiene un impacto más duradero ya que el código malicioso se almacena en la base de datos de la aplicación y puede ser ejecutado cada vez que la página web es visitada.

Explotación / Descubrimiento

Se ingresan caracteres especiales como < en la creación de un usuario, aunque no se materializa a algún ataque ya que cuando se creo el usuario luego no permitió el ingreso puede deberse a que en login si hay sanitización



Mitigación / Solución

- Para prevenir los ataques XSS Persistente (Cross-Site Scripting Persistente), se deben implementar las siguientes medidas de seguridad:

  Validación adecuada de la entrada de usuario: Es importante validar la entrada de usuario en todas las áreas de la aplicación web que aceptan entrada del usuario, como formularios y campos de búsqueda. Se deben rechazar las entradas que contengan caracteres no permitidos o sospechosos, como caracteres especiales y etiquetas HTML.

  Sanitización de datos de entrada: Además de la validación de la entrada de usuario, también es importante sanitizar los datos de entrada para evitar la ejecución de código malicioso. Esto implica eliminar cualquier característica que pueda ser interpretada como código malicioso, como etiquetas HTML, JavaScript y otros códigos de scripting.

Referencias

- Aquí están algunas referencias útiles para obtener más información sobre la sanitización de entradas y la implementación de cabeceras de seguridad HTTP para prevenir los ataques XSS:

  OWASP (Open Web Application Security Project) es una organización sin fines de lucro dedicada a mejorar la seguridad de software. Ofrece una guía práctica sobre cómo prevenir los ataques XSS, que incluye información sobre la sanitización de entradas y la implementación de cabeceras de seguridad HTTP: https://owasp.org/www-community/attacks/xss/

  Mozilla Developer Network (MDN) es una plataforma de documentación de Mozilla que ofrece una guía práctica sobre cómo prevenir los ataques XSS mediante la sanitización de entradas: https://developer.mozilla.org/en-US/docs/Web/Security/Cross_Site_Scripting/Preventing_XSS_attacks

3. Ausencia de cabeceras de seguridad

Descripción

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	192.168.2.17:8088
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Automática
Plataforma	Web

Tabla - Ausencia de cabeceras de seguridad

Descripción

No se presentan cabeceras de seguridad que evitan diferentes ataques a la aplicación, tales como Content-Security-Policy, Strict-Tranport-Security, X-Content-Type-Options, X-Frame-Options, entre otras

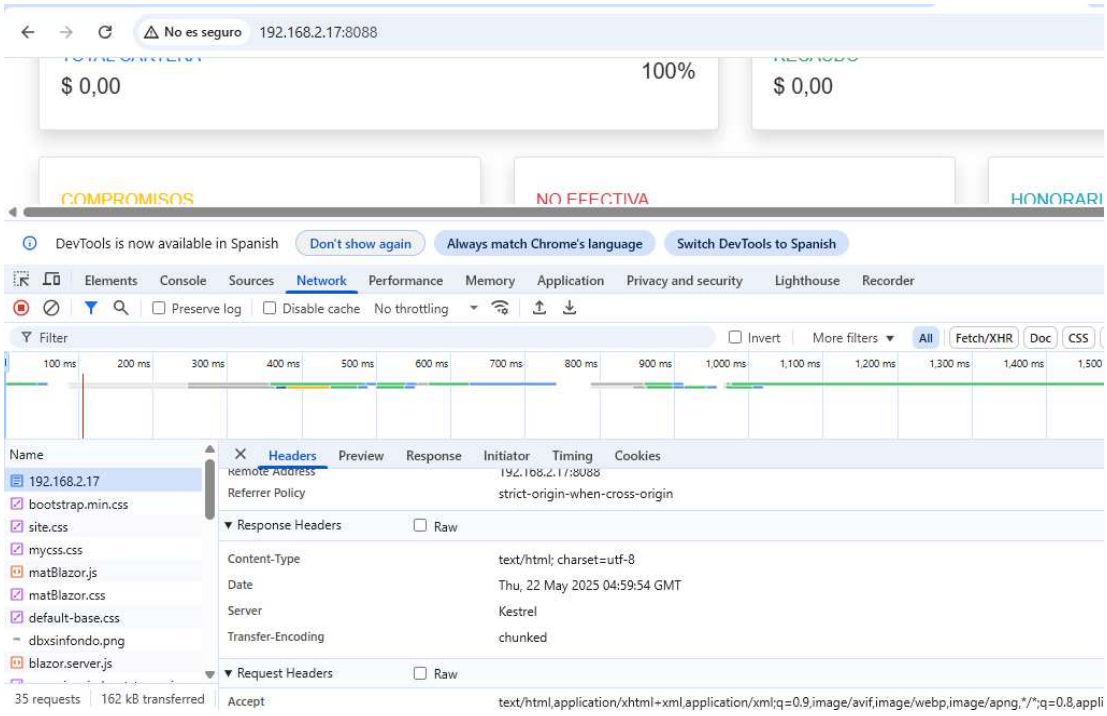
Se evidencia que Reincar APP no hace uso de las cabeceras de seguridad

Impacto

Permite la ejecución de diferentes ataques como incrustar el sitio en otro, degradar la conexión pasando de HTTPS a HTTP, entre otros.

Explotación / Descubrimiento

Se evidencia que la aplicación no entrega las cabeceras de seguridad HTTP, lo que permite realizar embebidos de la aplicación en otras paginas, no forzar el tráfico por HTTPS entre otras características de seguridad que aportan las cabeceras



Mitigación / Solución

- Agregar las cabeceras de seguridad requeridas.

Referencias

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

4. Protección inadecuada de cookies

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	http://192.168.2.17:8088/
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Manual
Plataforma	Web

Tabla - Protección inadecuada de cookies

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Descripción

Se ha evidenciado que las banderas httponly y "secure no se están implementando en el envío de las cookies entre cliente y servidor. La bandera httponly garantiza que en un ataque XSS no pueda ser obtenida la cookie en mención, por otro lado, la cabecera secure asegura que la cookie solo pueda ser enviada cuando el tráfico entre cliente y servidor se da a través de HTTPS.

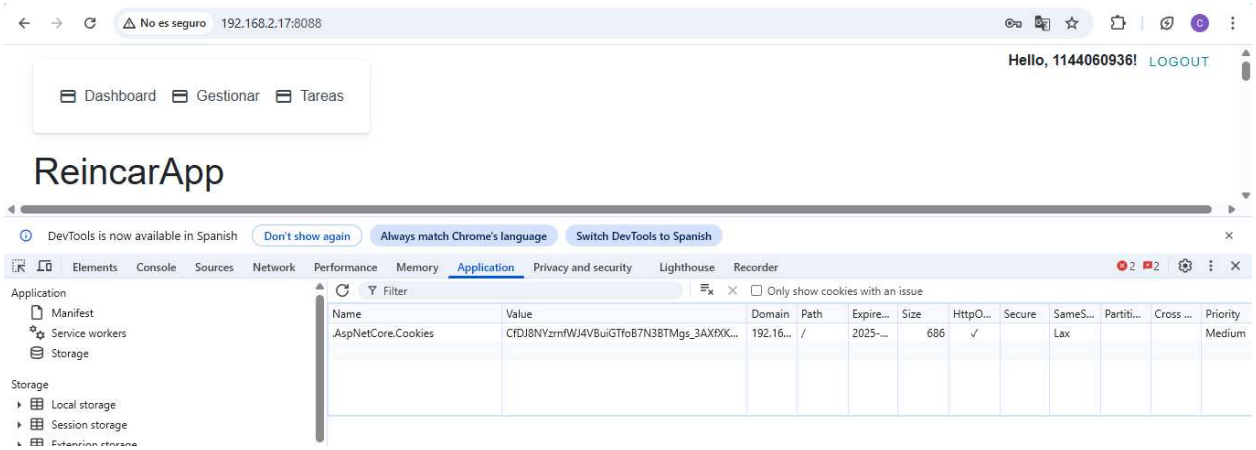
Se identifica que Reincar App no hace uso de los atributos de seguridad en las Cookies

Impacto

El no implementar las banderas en las cookies mencionadas podría causar que si un atacante lanza exitosamente un ataque de hombre en el medio o de XSS pueda acceder a las cookies y de esta manera comprometer y secuestrar la sesión del usuario víctima.

Explotación / Descubrimiento

Se evidencia la ausencia de aseguramiento en las Cookies de la aplicación, estas previenen el robo de Cookies frente a ataques de XSS si se llegasen a presentar



Mitigación / Solución

- Establecer el uso de las banderas mencionadas (HttpOnly y Secure) en las cookies enviadas entre cliente y servidor de la siguiente manera:

  Set-Cookie: <<cookie>>; Expires=<<fecha de expiración>>; Secure; HttpOnly

Referencias

- https://resources.infosecinstitute.com/topic/securing-cookies-httponly-secure-flags/

5. Validación inadecuada de intentos fallidos de inicio de sesión

Descripción	
Estado	**Activa**
Fecha de descubrimiento	Wed Apr 02 2025 23:00:00 GMT-0500 (Colombia Standard Time)
Activo	
Activo 1	http://192.168.2.17:8088/
Datos	
Criticidad	**Medium**
Categoría	Web
Prueba	Automática
Plataforma	Web

Tabla - Validación inadecuada de intentos fallidos de inicio de sesión

Descripción

Esta vulnerabilidad se produce cuando un sistema no implementa medidas para limitar el número de intentos de inicio de sesión fallidos que un usuario puede realizar antes de bloquear su cuenta o tomar otras medidas de seguridad. Si un sistema no tiene estas medidas, un atacante podría utilizar herramientas automatizadas para probar una gran cantidad de combinaciones de nombre de usuario y contraseña hasta que encuentre la combinación correcta.

Se identifica que ReincarApp no cuenta con un mecanismo anti automatización en el login, lo que permite realizar ataques de fuerza bruta

Impacto

La validación inadecuada de intentos fallidos de inicio de sesión puede tener graves consecuencias para la seguridad de los sistemas y las cuentas de usuario.

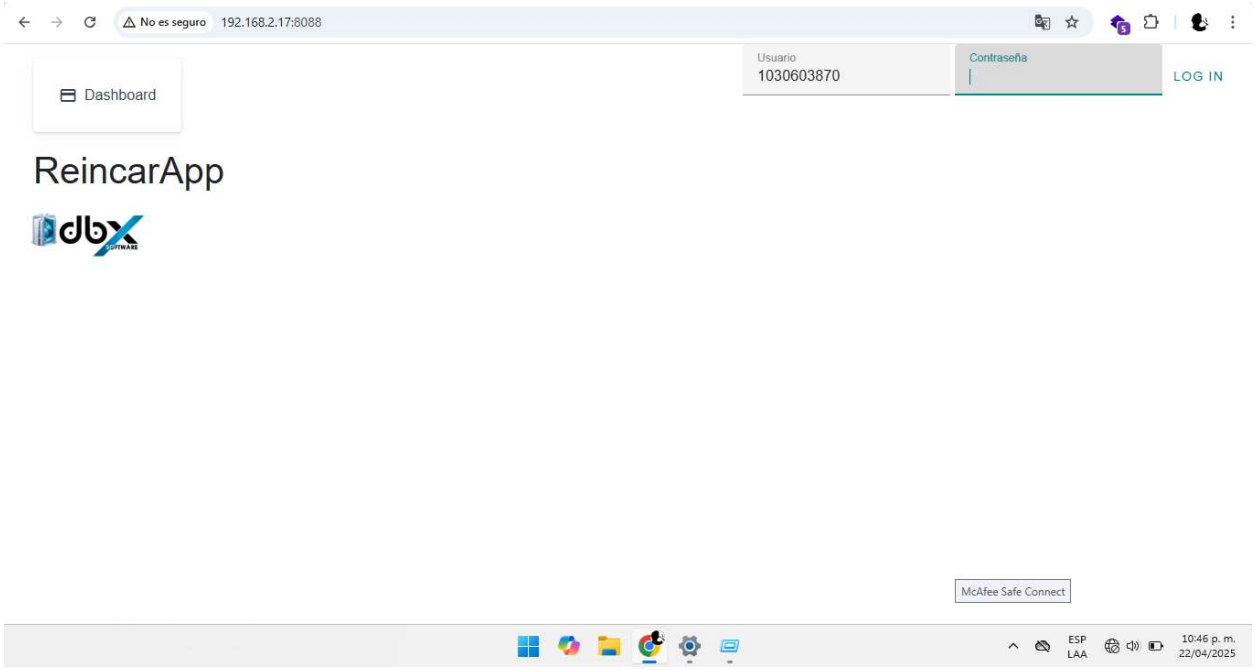
Acceso no autorizado: Si un atacante puede realizar intentos de inicio de sesión fallidos ilimitados, podría eventualmente adivinar la contraseña correcta y acceder a una cuenta sin autorización.

Robo de datos: Una vez que un atacante tiene acceso a una cuenta, puede robar datos sensibles o confidenciales, como información financiera, información personal o datos empresariales.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

Explotación / Descubrimiento

La ausencia de un control frente a la automatización o intentos fallidos de Login, permiten que el riesgo de ataques de fuerza bruta puedan tener una probabilidad de éxito mayor



Mitigación / Solución

- Para prevenir la vulnerabilidad de la validación inadecuada de intentos fallidos de inicio de sesión, los mecanismos de autenticación deben implementar medidas de seguridad adecuadas, como el bloqueo de la cuenta después de un número determinado de intentos fallidos, la implementación de un tiempo de espera después de varios intentos fallidos y la implementación de herramientas de protección contra ataques de fuerza bruta, como el captcha o los sistemas de prueba de trabajo.

Referencias

- NIST Special Publication 800-63B: Digital Identity Guidelines: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

  OWASP Cheat Sheet Series: Authentication: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#Lockout_Brute_Force_Defenses

3. ANEXOS

3.1. Anexo 1 - Referencias

Metodologías

Como base para la realización de servicios de Seguridad, y más concretamente las auditorías de seguridad, Hacking ético y pentesting, los auditores utilizan varias metodologías y estándares internacionalmente difundidos y reconocidos como son:

OWASP (*Open Web Application Security Project*) – Guía de realización de pruebas de seguridad en aplicaciones Web.

- http://www.owasp.org/

Nomenclatura

CPE (Common Platform Enumeration) es el listado de tipos de plataformas y sistemas que permite identificar unívocamente un sistema específico con su versión y detalles

- https://nvd.nist.gov/cpe.cfm

CVE (Common Vulnerabilities and Exposures), ***CWE*** (Common Weakness Enumeration) y ***CAPEC*** (Common Attack Pattern Enumeration and Classification) son listas de vulnerabilidades específicas o tipos de vulnerabilidades genéricas que tiene por objeto proporcionar nombres comunes a los problemas conocidos públicamente.

- http://www.cve.mitre.org/
- http://cwe.mitre.org/
- http://capec.mitre.org/

Con el objeto de crear una valoración objetiva de las vulnerabilidades, se utiliza el sistema de valoración de vulnerabilidades definido en CVSS.

El ***CVSS*** (Common Vulnerability Scoring System), es el sistema que define la métrica para poder medir y establecer el valor numérico del impacto de una vulnerabilidad en un sistema. Vector CVSS que contienen las cifras de base tienen la siguiente forma:

- (AV:[L,A,N]/AC:[H,M,L]/Au:[N,S,M]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C])

Las letras entre paréntesis representan los valores posibles de una métrica CVSS. Exactamente una opción se debe seleccionar para cada conjunto de corchetes. Las letras

fuera de los corchetes son obligatorias y deben incluirse a fin de crear un vector CVSS válido. Cada letra o un par de letras es una abreviatura o de un valor de métrica en valor CVSS.

- Métricas: AV = Vector de Acceso (L = acceso local, A = Red adyacente, N = Internet)
- Métricas: AC = Complejidad de Acceso (H = Alta, M = Mediano, L = Bajo)
- Métricas: Au = Autenticación (N= No requerido, S = Un sistema, M = Múltiples sistemas)
- Métricas: C = Impacto a la Confidencialidad (N = No, P = Parcial, C = Completa)
- Métricas: I = Impacto a la Integridad (N = No, P = Parcial, C = Completa)
- Métricas: A = Impacto a la Disponibilidad (N = No, P = Parcial, C = Completa)

http://nvd.nist.gov/cvss.cfm?version=2

Para establecer las clasificaciones de impacto, se sigue como base la recomendación de la NVD, Base de Datos Nacional de Vulnerabilidades, en base a los resultados de los CVSS:

- La vulnerabilidad etiquetada de '**Crítica**' tiene un CVSS base de puntuación entre 9.6 y 10.0.
- La vulnerabilidad etiquetada de '**Alta**' tiene un CVSS base de puntuación entre 7.0 y 9.5.
- La vulnerabilidad etiquetada de '**Media**' tiene un CVSS base de puntuación entre 4.0 y 6.9.
- La vulnerabilidad etiquetada de '**Baja**' tiene un CVSS base de puntuación entre 0.1 y 3.9.
- La vulnerabilidad etiquetada de '**Información**' tiene un CVSS base de puntuación de 0.0.

Definiciones

Vulnerabilidad: Un error, falla, debilidad, o la exposición de una aplicación, sistema, dispositivo o servicio que podría dar lugar a un incumplimiento de la confidencialidad, integridad o disponibilidad.

Amenaza: La frecuencia o probabilidad de que un hecho dañoso se produzca.

Riesgo: Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.

Activo: Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La empresa asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

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.

INFORME DE TEST – HALLAZGOS DE CIBERSEGURIDAD

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 adecuado.

Oscar Arnulfo Quintero Torres
Máster en ciberseguridad

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que en REINCAR contamos con el TC-IN09 Estructura de plan de continuidad del negocio y mensualmente se realiza la validación del plan de continuidad del negocio mediante el TC-IN05 Plan de Continuidad REINCAR.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que REINCAR da cumplimiento a los requisitos de calidad International Standard Organization ISO 27001.

DIEGO ENRIQUE GONZALEZ
Gerente General

Reincar
Recuperadora Integral de Cartera
NIT. 900.405.236-5

icontec ISO / IEC 27001 SI-2000523
icontec ISO 9001 SC-CER546357
IQNET

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que en REINCAR asegura que el personal no hará uso de dispositivos de almacenamiento dentro de las instalaciones en las cuales se ejecutará el contrato. Así mismo que se mantiene bloqueado el acceso a puertos USB, HDMI, Unidades de CD, DVD, Quemador, correos electrónicos y cualquier otro tipo que permita la extracción de información, en el sitio de operación de la cartera de FONDO NACIONAL DEL AHORRO, como se encuentra especificado en el Manual de Seguridad de la Información TC-IN02 #5.5 literal 1.

DIEGO ENRIQUE GONZALEZ
Gerente General

CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que en REINCAR se encuentra establecido que esta prohibido el ingreso y uso de celulares, tabletas, cámaras fotográficas en el sitio de operación de la cartera del Fondo Nacional del Ahorro, este lineamiento se encuentra definido en el TC-IN02 Manual de Seguridad de la Información Numeral 5.10 item 1.1.5

DIEGO ENRIQUE GONZALEZ
Gerente General

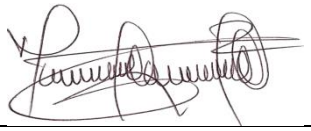
CERTIFICACIÓN

Yo, Diego Enrique González Ramírez, en mi calidad de Gerente General, certifico por medio de la presente que en REINCAR contamos con el TC-IN01 Política de uso de Medios Tecnológicos # 4, donde se describe la seguridad perimetral para la protección de la red.

DIEGO ENRIQUE GONZALEZ
Gerente General

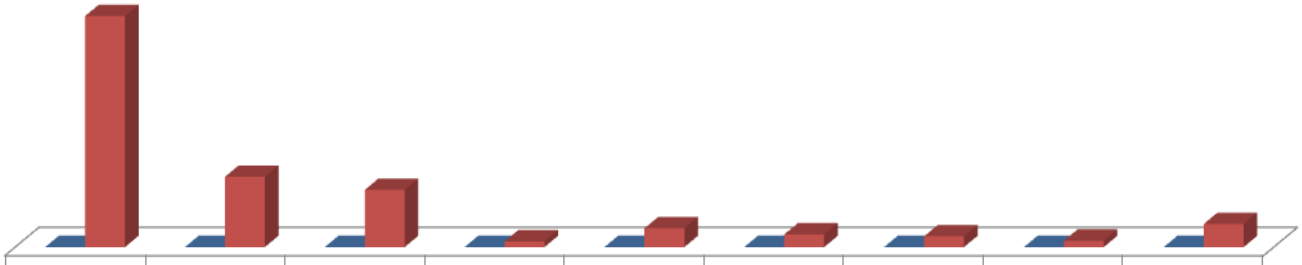
INFORME DE MEDICIÓN
REINCAR

TIPO DE ASIGNACION	DESCRIPCION ASIGNACION	PERIODO EJECUCION
*REPARTO ADMINISTRATIVA *REPARTO CASTIGO	**REPARTO ADMINISTRATRIVA:** 19.159 OBLIGACIONES POR $1.204.331.264.470 **REPARTO CASTIGO:** 1.582 OBLIGACIONES POR $53.044.774.783	ABRIL 2026

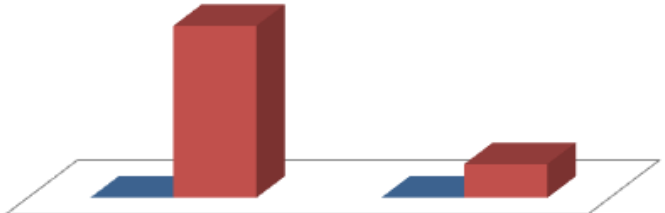
CASA DE COBRANZA	NOMBRE RESPONSABLE	FIRMA RESPONSABLE
REINCAR	MARIA ISABLE CHAVEZ PARRA	

1. ANALISIS DE LA CARTERA ENTREGADA VIA REPARTO Y/O CAMPAÑA ESPECIAL:

1.1. Descripción de la cartera por franja:



A. AL DIA	B. DE 1 A 30	C. DE 31 A 60	D. DE 61 A 90	E. DE 91 A 120	F. DE 121 A 150	G. DE 151 A 360	H. DE 360 A 540	I. MAYOR A 540
10.372	3.048	2.434	243	830	555	471	330	949
640.829.809.299	194.994.357.910	158.582.135.458	15.603.607.981	52.144.406.839	35.297.604.995	29.833.633.492	17.783.404.771	64.162.878.373

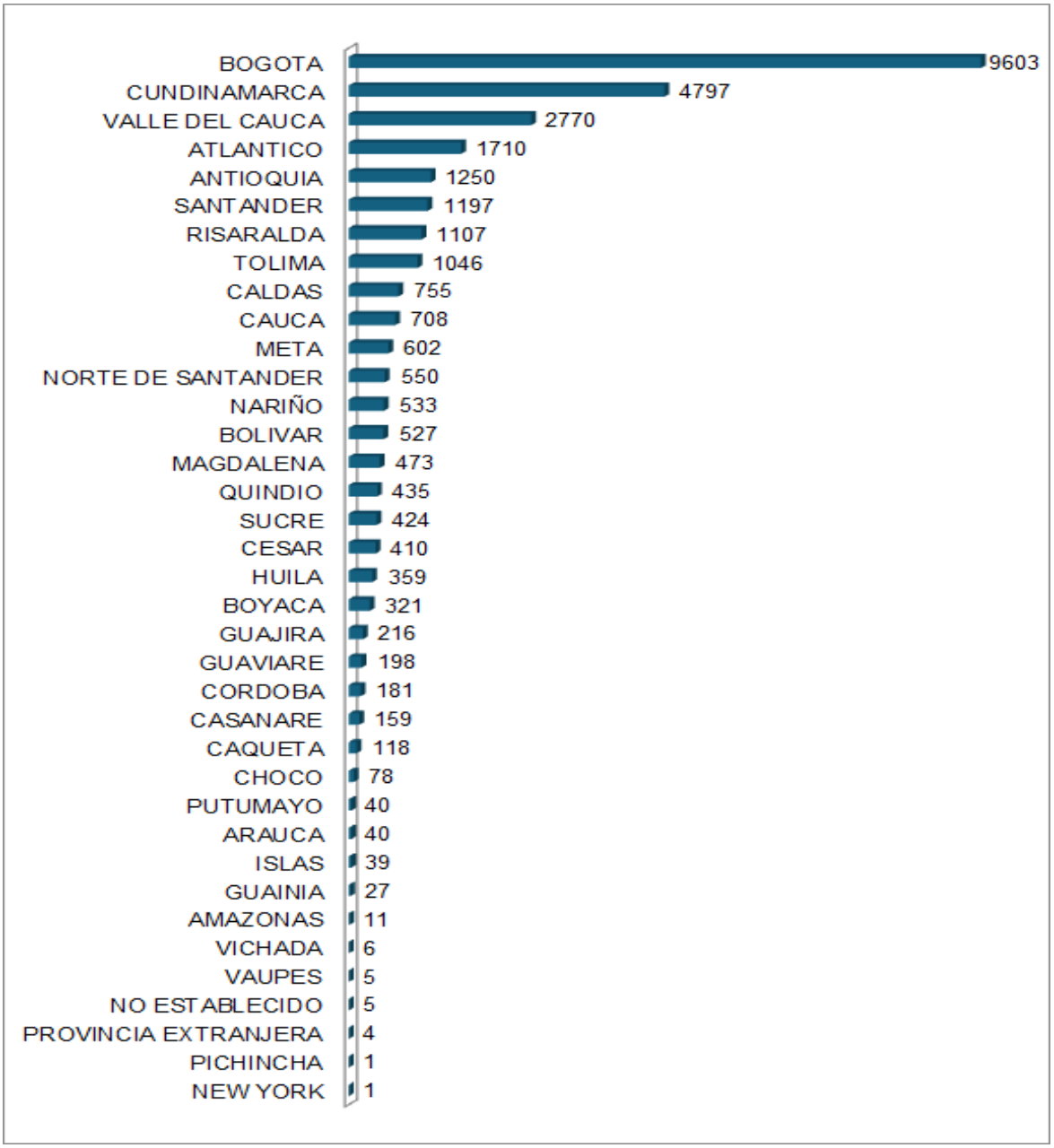


CASTIGO	DISPROYECTOS
1.415	167
44.366.383.545	8.678.391.237

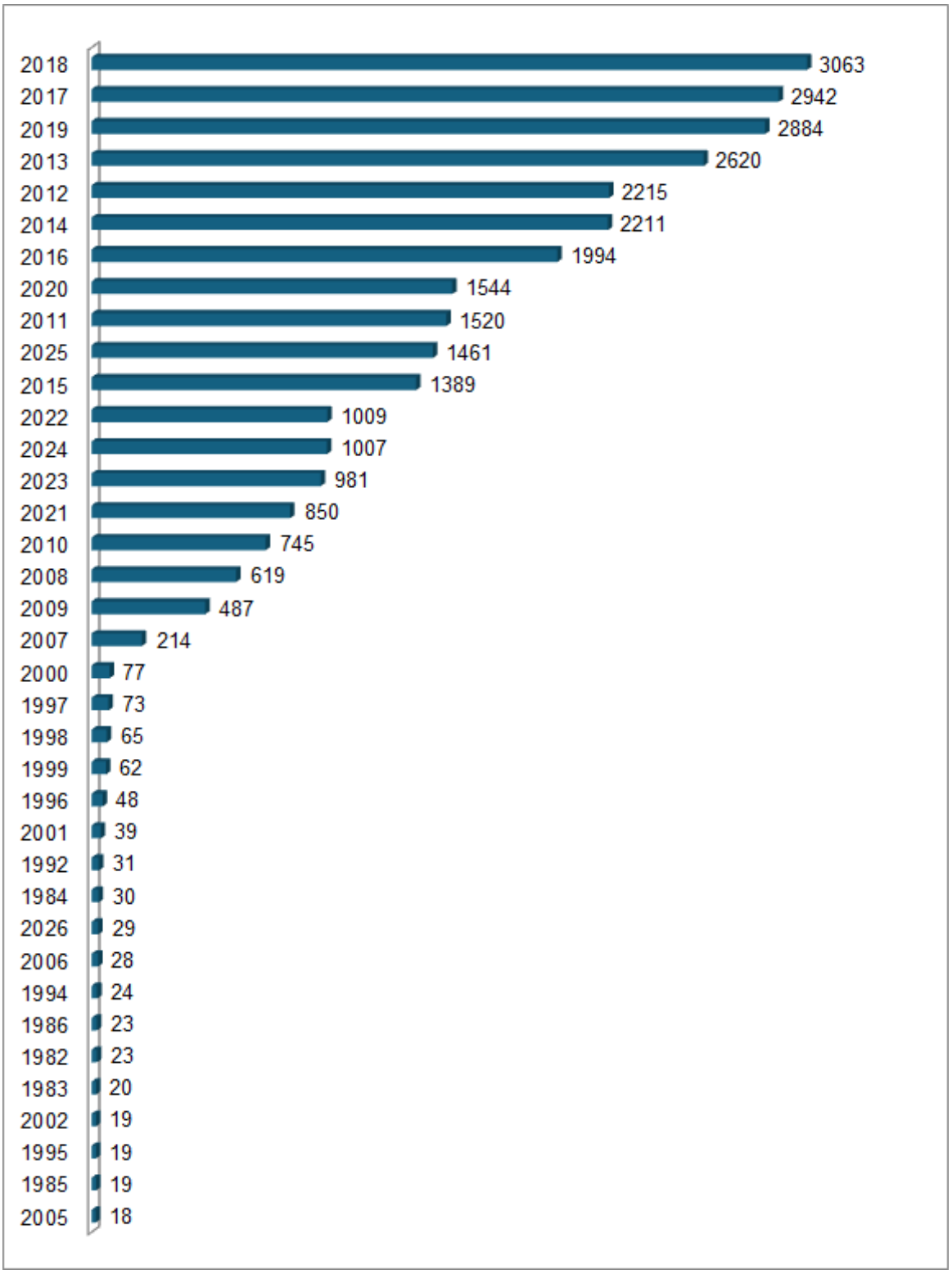
1.2. Distribución de la cartera por altura de mora

Se genero trabajo por bolsas de negociacion, en donde no se asigna cartera determinada a un gestor, todo depende de la negociaciones que cada gestor va realizando, se utiliza el marcador predictivo como herramienta de rotacion.

1.3. Descripción de la cartera por departamento



1.4. Descripción por cosecha



1.5. Descripción por línea de crédito

2. ANALISIS DE LA CAPACIDAD

2.1. Número de gestores asignados.

CANTIDAD	NOMBRE
1	INGRID XIMENA ALMEIDA QUINTERO
2	MARIA ELVIRA GONZALEZ BLANCO
3	JULY ALEJANDRA MORENO
4	JEIMY KATEHERINE VARGAS LAMUS
5	TATIANA DEL PILAR RANGEL LOPEZ
6	ZAYDITH YULIETH ALVAREZ MARTINEZ
7	JULIAN DAVID MOJICA MANTILLA
8	RONALD ANDRES BENITEZ BARCO
9	JUAN MANUEL IBARRA GARCIA
10	BAYRON DANIEL SANTOS TOLOZA
11	FERNEY ALFONSO LEON GARAVITO
12	MAYRA ALEJANDRA PARRA DUARTE
13	ANDREINA NAVARRO ARIZA
14	JONNATHAN JOSUE MARQUEZ FLOREZ
15	YALKIS YOHENIS PEREZ BRITO
16	MARIA JULIETH LUNA CAICEDO
17	LINDA MARCELA PEREZ GARNICA
18	DANA VALENTINA GARZON GOMEZ
19	RONALD DAVID GOMEZ
20	LUIS ENRIQUE HERNANDEZ HERNANDEZ
21	BRANYI JIMENEZ PARADA
22	PEDRO DAVID QUESADA SUAREZ
23	SILVANA LUZDEY HERNANDEZ MANOSALVA
24	LEIDY CAROLINA ULLOA GUALDRON
25	XIOMARA VANESA TIRIA PERDOMO

2.2. Meta diaria por gestor en número de contacto y en valor de recuperación.

FRANJA	GESTIONES DIARIAS	META % CONTACTO	META CONTACT DIARIO	META RECUPERACION DIARIA
B. DE 1 A 30	80	60%	48	536.981.420
C. DE 31 A 60		50%	40	60.623.220
D. DE 61 A 90		45%	36	99.773.161
E. DE 91 A 120		30%	24	44.153.937
F. DE 121 A 150				31.835.402
G. DE 151 A 360		20%	16	23.849.589
H. DE 360 A 540				5.343.531
I. MAYOR A 540				6.181.066
J. CASTIGO		10%	8	60.900.000

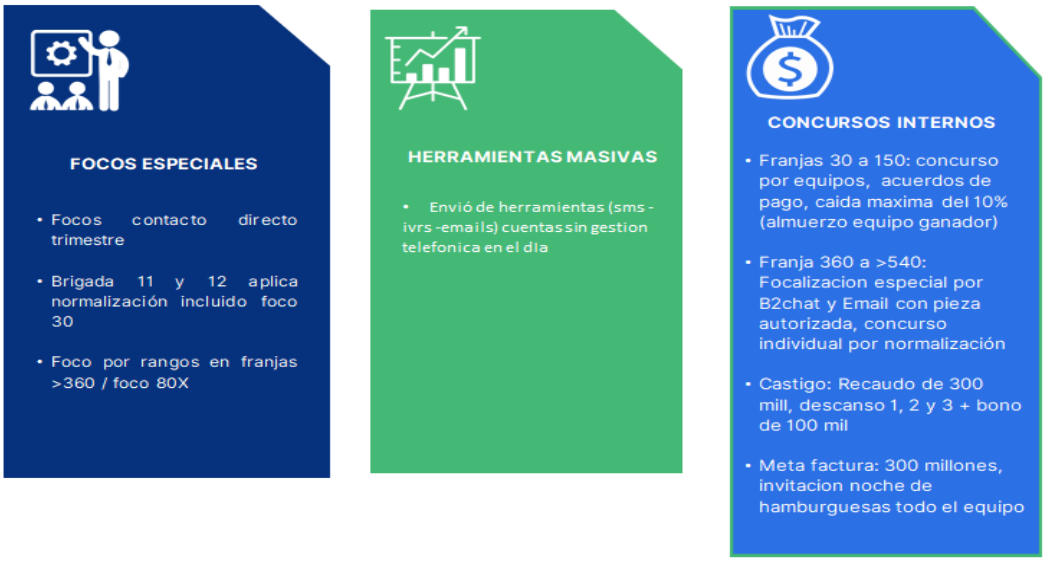
2.3. Cumplimiento de la meta por gestor, diaria, semanal y al final de la campaña.

ASESOR	META	HONRS ADMI	HONRS CAST	HOY	% META
BAYRON DANIEL SANTOS TOLOZA	10.755.157	14.520.395	3.244.476	17.764.871	165%
INGRID XIMENA ALMEIDA QUINTERO	10.730.921	19.431.711	408.833	19.840.543	185%
JEIMY KATHERINE VARGAS LAMUS	10.716.719	4.771.926	3.999.427	8.771.353	82%
JUAN MANUEL IBARRA GARCIA	10.691.184	7.561.642	19.045.415	26.607.056	249%
JULIAN DAVID MOJICA MANTILLA	10.767.462	6.301.656	4.880.269	11.181.924	104%
JULY ALEJANDRA MORENO	10.742.447	6.659.970	1.445.313	8.105.283	75%
MARIA ELVIRA GONZALEZ BLANCO	10.712.851	6.486.194	50.453.038	56.939.232	532%
RONALD ANDRES BENITEZ BARCO	10.733.935	2.362.204	5.305.403	7.667.607	71%
TATIANA DEL PILAR RANGEL LOPEZ	10.767.219	7.496.394	1.300.177	8.796.571	82%
PEDRO DAVID QUESADA SUAREZ	10.705.485	2.733.304	-	2.733.304	26%
MAYRA ALEJANDRA PARRA DUARTE	10.726.514	7.048.600	2.399.389	9.447.989	88%
FERNEY ALFONSO LEON GARAVITO	10.703.727	30.454.177	15.893.278	46.347.454	433%
JONNATHAN JOSUE MARQUEZ FLOREZ	10.698.435	13.823.651	5.395.102	19.218.753	180%
MARIA JULIETH LUNA CAICEDO	10.719.887	2.154.655	735.660	2.890.314	27%
LINDA MARCELA PEREZ GARNICA	10.727.987	8.482.674	294.024	8.776.698	82%
ANDREINA NAVARRO ARIZA	10.688.542	4.038.690	99.365	4.138.055	39%
DANA VALENTINA GARZON GOMEZ	10.686.808	12.379.332	-	12.379.332	116%
YALKIS YOHENIS PEREZ BRITO	10.716.360	2.249.453	8.035.231	10.284.684	96%
RONALD DAVID GOMEZ ALVARADO	10.680.517	2.107.512	-	2.107.512	20%
LUIS ENRIQUE HERNANDEZ HERNANDEZ	10.718.310	3.166.699	1.670.000	4.836.699	45%
SILVANA LUZDEY HERNANDEZ MANOSALVA	5.000.000	1.442.917	-	1.442.917	29%

2.4. Incentivos del mes por cumplimiento de metas.

ASESOR	HONORARIOS	INCENTIVO
MARIA ELVIRA GONZALEZ BLANCO	56.905.252	2.845.263
FERNEY ALFONSO LEON GARAVITO	45.933.369	2.296.668
JUAN MANUEL IBARRA GARCIA	26.370.574	1.318.529
INGRID XIMENA ALMEIDA QUINTERO	20.203.962	1.010.198
JONNATHAN JOSUE MARQUEZ FLOREZ	19.733.596	986.680
BAYRON DANIEL SANTOS TOLOZA	18.147.551	907.378
DANA VALENTINA GARZON GOMEZ	12.376.173	618.809
YALKIS YOHENIS PEREZ BRITO	12.069.952	603.498
JULIAN DAVID MOJICA MANTILLA	11.142.065	557.103
MAYRA ALEJANDRA PARRA DUARTE	9.026.077	-
TATIANA DEL PILAR RANGEL LOPEZ	8.741.337	-
LINDA MARCELA PEREZ GARNICA	8.719.233	-
JEIMY KATHERINE VARGAS LAMUS	8.335.784	-
JULY ALEJANDRA MORENO	8.153.781	-
RONALD ANDRES BENITEZ BARCO	7.919.459	-
LUIS ENRIQUE HERNANDEZ HERNANDEZ	4.778.831	-
ANDREINA NAVARRO ARIZA	4.081.732	-
MARIA JULIETH LUNA CAICEDO	2.883.678	-
PEDRO DAVID QUESADA SUAREZ	2.609.000	-
RONALD DAVID GOMEZ ALVARADO	2.152.143	-
SILVANA LUZDEY HERNANDEZ MANOSALVA	1.592.918	-
BRANYI IZAURA JIMENEZ PARADA	851.685	-

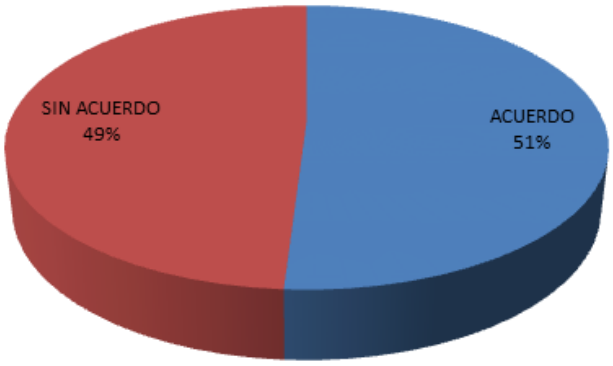
3. DESCRIPCION DE LA ESTRATEGIA



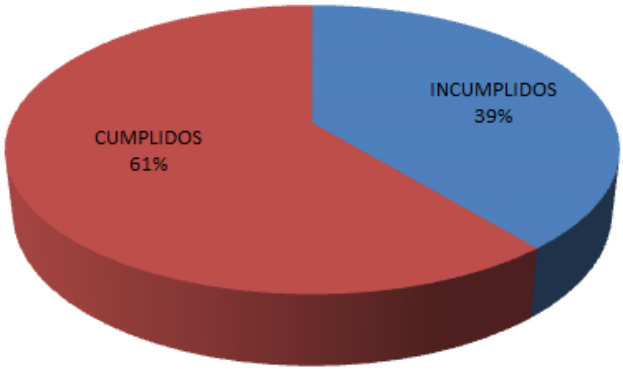
4. FACTORES DE MEDICION

4.1. EFECTIVIDAD EN EL CONTACTO TELEFÓNICO (Titular, Tercero Valido o Visita Efectiva):

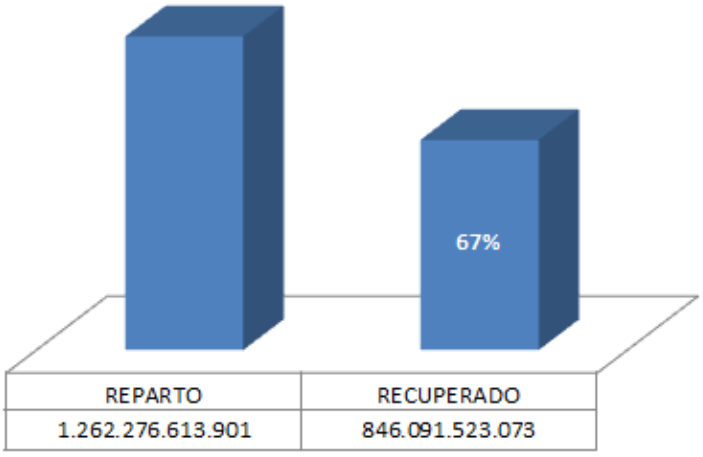
4.2. EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR:



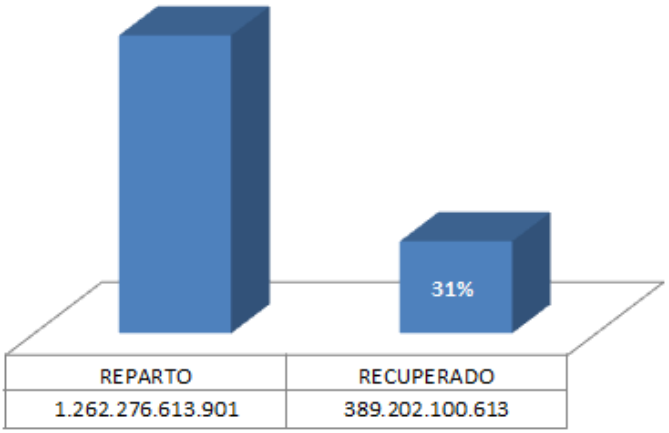
4.3. EFECTIVIDAD DE LOS COMPROMISOS O ACUERDOS DE PAGO:



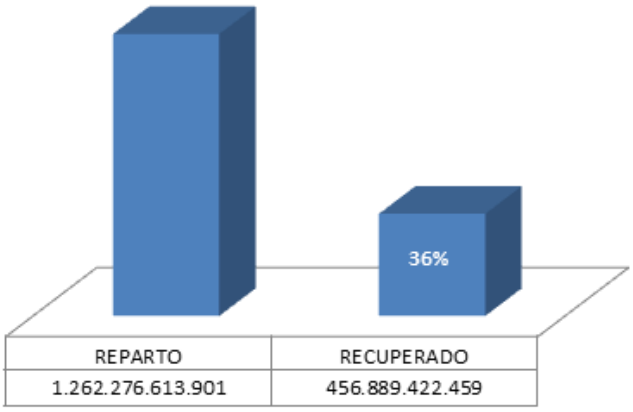
4.4. EFECTIVIDAD DE LA RECUPERACIÓN:



4.5. EFECTIVIDAD DE LA RECUPERACIÓN DE CRÉDITOS CONTACTADOS:



4.6. EFECTIVIDAD DE LA RECUPERACIÓN DE CRÉDITOS NO CONTACTADOS:



FACTORES DE MEDICIÓN

EFECTIVIDAD EN EL CONTACTO TELEFÓNICO (Titular , Tercero Valido o Visita Efectiva):

Total de créditos efectivamente contactados sobre el total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caídas - Ni Gestión Virtual).

EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR:

Total de promesas o acuerdos de pago generadas sobre el total de créditos efectivamente contactados

EFECTIVIDAD DE LOS COMPROMISOS O ACUERDOS DE PAGO:

Total de los compromisos o acuerdos efectivamente cumplidos parcial o totalmente, sobre el total de los compromisos o acuerdos de pago realizados (Factor Anterior).

EFECTIVIDAD DE LA RECUPERACIÓN:

Valor total recuperado parcial o totalmente, sobre el valor total de la mora asignada para cobro a inicio de mes. (No incluye recuperación por asignaciones diarias o refrescos por caídas)

EFECTIVIDAD DE LA RECUPERACIÓN DE CRÉDITOS CONTACTADOS:

Valor total recuperado parcial o totalmente, sobre el valor total de la mora asignada para cobro a inicio de mes. (No incluye recuperación por asignaciones diarias o refrescos por caídas) de los créditos contactados

EFECTIVIDAD DE LA RECUPERACIÓN DE CRÉDITOS NO CONTACTADOS:

Valor total recuperado parcial o totalmente, sobre el valor total de la mora asignada para cobro a inicio de mes. (No incluye recuperación por asignaciones diarias o refrescos por caídas) de los créditos no contactados.

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: > 540 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	3041	3048	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**3,041**	**3,048**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	295	3048	10%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**295**	**3,048**	**10%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	218	295	74%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**218**	**295**	**74%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	422,280,939	358,771,156	118%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**422,280,939**	**358,771,156**	**118%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	2746	3041	90%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**2,746**	**3,041**	**90%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	7	0%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**7**	**0%**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 31 Y 60 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	2433	2434	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**2,433**	**2,434**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	673	2434	28%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**673**	**2,434**	**28%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	376	673	56%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**376**	**673**	**56%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	582,480,318	791,726,711	74%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**582,480,318**	**791,726,711**	**74%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	1760	2433	72%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**1,760**	**2,433**	**72%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	1	0%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**1**	**0%**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 61 Y 90 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	243	243	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**243**	**243**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	56	243	23%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**56**	**243**	**23%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	31	56	55%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**31**	**56**	**55%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	66,875,936	96,108,720	70%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**66,875,936**	**96,108,720**	**70%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	187	243	77%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**187**	**243**	**77%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	0	#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**0**	**#¡DIV/0!**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 91 Y 120 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	830	830	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**830**	**830**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	197	830	24%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**197**	**830**	**24%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	123	197	62%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**123**	**197**	**62%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	259,718,955	455,156,487	57%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**259,718,955**	**455,156,487**	**57%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	633	830	76%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**633**	**830**	**76%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	0	#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**0**	**#¡DIV/0!**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 121 Y 150 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	555	555	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**555**	**555**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	147	555	26%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**147**	**555**	**26%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	100	147	68%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**100**	**147**	**68%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	263,673,142	448,272,343	59%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**263,673,142**	**448,272,343**	**59%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	408	555	74%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**408**	**555**	**74%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	0	#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**0**	**#¡DIV/0!**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 151 Y 360 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	470	471	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**470**	**471**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	143	471	30%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**143**	**471**	**30%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	112	143	78%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**112**	**143**	**78%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	404,927,077	741,307,730	55%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**404,927,077**	**741,307,730**	**55%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	327	470	70%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**327**	**470**	**70%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	0	1	0%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**0**	**1**	**0%**

MEDICIÓN CASAS DE COBRANZA
PERIODO:ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 361 Y 540 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	330	330	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**330**	**330**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	34	330	10%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**34**	**330**	**10%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	27	34	79%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**27**	**34**	**79%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	138,376,768	203,688,965	68%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**138,376,768**	**203,688,965**	**68%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	296	330	90%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**296**	**330**	**90%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	1	0	#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**1**	**0**	**#¡DIV/0!**

MEDICIÓN CASAS DE COBRANZA
PERIODO: ABRIL
CASA DE COBRANZA:REINCAR

RANGO DE MORA: ENTRE 1 Y 30 DIAS

PORCENTAJE DE EFECTIVIDAD EN EL CONTACTO TELEFÓNICO CON EL DEUDOR (en número de créditos)

Medición: Total de créditos efectivamente contactados (titular o tercero valido) sobre total de créditos asignados a inicio de mes para gestión de cobranza (No incluye asignaciones diarias o refrescos por caidas - Ni Gestión Virtual)

CASA DE COBRANZA - GESTOR	Total de Créditos Contactados	Total Créditos Asignados	%
Reincar	946	949	100%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**946**	**949**	**100%**

PORCENTAJE DE EFECTIVIDAD EN LA NEGOCIACIÓN CON EL DEUDOR (en número de créditos)

Medición: Total de compromisos generados sobre el total de créditos efectivamente contactados (titular o tercero valido)

CASA DE COBRANZA - GESTOR	Total Compromisos Generados	Total Créditos Asignados	%
Reincar	54	949	6%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**54**	**949**	**6%**

PORCENTAJE DE EFECTIVIDAD POR COMPROMISOS O ACUERDOS DE PAGO (en número de créditos)

Medicion: Total de los compromisos efectivamente cumplidos (parcial o totalmente) sobre el total de los compromisos pactados

CASA DE COBRANZA - GESTOR	Total Compromisos Cumplidos	Total Compromisos Pactados	%
Reincar	33	54	61%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**33**	**54**	**61%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS

Medición: Valor Total recuperado (parcial o totalmente) sobre el valor total de los créditos asignados para gestión al inicio de la campaña

CASA DE COBRANZA - GESTOR	Vr. Total Recuperado	Vr. Total Entregado para Recuperar	%
Reincar	790,871,730	1,182,009,753	67%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**790,871,730**	**1,182,009,753**	**67%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS CONTACTADOS

Medición: Porcentaje de créditos efectivamente contactados (titular o tercero valido) con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos Contactados	%
Reincar	892	946	94%
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**892**	**946**	**94%**

PORCENTAJE DE EFECTIVIDAD DE RECUPERACION EN PESOS DE LOS CRÉDITOS NO CONTACTADOS

Medición: Porcentaje de créditos NO contactados con pago parcial o total de la mora

CASA DE COBRANZA - GESTOR	Créditos con pago Total o Parcial	Total Créditos NO Contactados	%
Reincar	3	0	#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
			#¡DIV/0!
TOTALES	**3**	**0**	**#¡DIV/0!**

COBRADOR: RECUPERADORA Y NORMALIZADORA INTEGRAL DE CARTERA S.A.S. - GRUPO REINCAR S.A.S.
REPARTO: 6 DE ABRIL 2026
INFORME FINAL: 30 DE ABRIL 2026

VALOR RECUPERACIÓN

RANGO	AL DIA	1 A 30	31 A 60	61 A 90	91 A 120	121 A 150	151 A 360	360 A 540	MAYOR A 540
AL DIA	168,165,738	8,953,500	-	-	-	-	-	-	-
1 A 30	266,121,503	151,160,246	4,999,189	-	-	-	-	-	-
31 A 60	289,695,593	123,696,160	151,629,565	17,459,000	-	-	-	-	-
61 A 90	35,325,128	6,679,808	4,623,000	19,748,000	500,000	-	-	-	-
91 A 120	139,651,026	6,430,000	23,605,000	41,846,137	40,012,762	8,174,030	-	-	-
121 A 150	169,263,805	16,141,000	18,953,000	14,210,000	19,514,448	25,490,889	100,000	-	-
151 A 360	336,959,222	3,657,000	4,720,400	8,472,000	4,146,000	3,623,000	43,349,455	-	-
360 A 540	91,735,990	12,000,000	-	-	-	-	22,864,778	11,776,000	-
MAYOR A 540	726,504,348	-	-	-	-	-	-	16,918,500	47,448,882
Castigo									958,032,066

VALOR COMISIÓN

RANGO	AL DIA	1-30	31-60	61-90	91-120	121-150	151-180	360 A 540	MAYOR A 540	PLUS
AL DIA	1,244,426	-	-	-	-	-	-	-	-	-
1 A 30	3,220,070	982,542	-	-	-	-	-	-	-	-
31 A 60	6,634,029	1,570,941	1,061,407	-	-	-	-	-	-	-
61 A 90	1,257,575	160,315	55,938	124,412	-	-	-	-	-	-
91 A 120	8,323,201	230,837	590,125	548,184	268,086	-	-	-	-	-
121 A 150	13,507,252	920,037	665,250	333,935	265,396	173,338	-	-	-	-
151 A 360	37,537,257	273,178	249,709	316,853	128,526	80,431	494,184	-	-	3,615,776
360 A 540	11,035,840	1,034,400	-	-	-	-	521,317	136,602	-	-
MAYOR A 540	93,137,857	-	-	-	-	-	-	389,126	569,387	-
Castigo									159,991,355	-

RANGO	VALOR RECUPERADO	VALOR COMISIÓN
AL DIA	177,119,238	1,244,426
1 A 30	422,280,939	4,202,612
31 A 60	582,480,318	9,266,377
61 A 90	66,875,936	1,598,241
91 A 120	259,718,955	9,960,433
121 A 150	263,673,142	15,865,208
151 A 360	404,927,077	42,695,914
360 A 540	138,376,768	12,728,158
MAYOR A 540	790,871,730	94,096,370
Castigo	958,032,066	159,991,355
DESCUENTO ANS		13,011,016
TOTALES	**4,064,356,169**	**338,638,078**
	IVA	64,341,235
	TOTAL LIQUIDADO	**402,979,313**
DESCUENTO OFERTADO 3%		12,089,379
	TOTAL A PAGAR	**390,889,933**

APLICACIÓN ANS	VALOR DESCUENTO
INCUMPLIMIENTO META	15,483,110
PRIMERA GESTION	-
SPIN RATE	-
QUEJA MAL SERVICIO	-
CALIDAD INFORMACION APLICATIVO	-
CAPACITACION PERSONAL	-
TOTAL DESCUENTO	**15,483,110**
Antes de IVA	**13,011,016**

Elaboró: Jully Alexandra Garcia Agudelo - GCB - p04
Revisó: John Alexander Serna - GCB - p06
Aprobó: Gabriel Ernesto Fuentes Aguilar - GCB (E)

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

Acta N°		**Tema:**	SEGUIMIENTO CIFRAS REINCAR
Fecha:	15/04/2026	**Ubicación:**	TEAMS FNA
Hora inicio:	9:00 AM	**Hora fin:**	10:00 AM
Objetivo	VALIDAR ESTRATEGIAS Y PLANES DE TRABAJO PARA EL MES DE ABRIL 2026.		

PARTICIPANTES CONVOCADOS A LA REUNIÓN			
Nombre completo	**Dependencia**	**Cargo**	**¿Asistió?**
JOHN ALEXANDER SERNA	FNA	PROFESIONAL 6	SI
MARIA ISABEL CHAVEZ	REINCAR	COORDINADOR	SI
LEIDY ULLOA	REINCAR	LIDER	SI

1. TEMAS TRATADOS

ACTA DE COMITÉ – PLAN DE TRABAJO REINCAR ABRIL 2026

Fecha del comité: Abril 2026
Proyecto: Plan de Trabajo Operativo – Reincar
Tema: Seguimiento y ejecución de estrategias de recuperación de cartera
Área: Operaciones y Cobranza

1. OBJETIVO DEL COMITÉ

Realizar seguimiento al plan de trabajo definido para abril de 2026, enfocado en el fortalecimiento de la recuperación de cartera, control operativo, seguimiento a indicadores y priorización de cuentas estratégicas.

2. TEMAS DESARROLLADOS

2.1 Estrategia Foco 80/20

Se presentó una estrategia focalizada sobre cuentas de alto valor económico pertenecientes a franjas superiores a 60 días de mora, con el propósito de:

- Priorizar la recuperación de obligaciones representativas.
- Incrementar cumplimiento de metas de recaudo.
- Mejorar la contención de cartera crítica.
- Concentrar esfuerzos sobre clientes de mayor impacto financiero.

Se acordó realizar seguimiento permanente a los resultados obtenidos en esta estrategia.

2.2 Tablero de Seguimiento Operativo

Se definió la implementación de un esquema de seguimiento diario enfocado en:

- Socialización de resultados operativos.
- Publicación de ranking de desempeño entre casas y gestores.
- Seguimiento al cumplimiento de metas de honorarios.
- Monitoreo de indicadores de productividad.
- Control de ofrecimientos y negociaciones efectivas.

El comité resaltó la importancia de fortalecer la cultura de medición y competitividad operativa mediante tableros de control diarios.

3. ESTRATEGIAS OPERATIVAS

Durante la sesión se establecieron las siguientes líneas de acción:

Gestión estratégica

- Priorización de cuentas de mayor saldo.
- Seguimiento intensivo a cartera crítica.
- Control de cumplimiento de compromisos.

Gestión comercial y de negociación

- Fortalecimiento de ofrecimientos efectivos.
- Incremento de negociaciones aplicadas.
- Seguimiento a metas individuales y grupales.

Seguimiento operativo

- Evaluación permanente de indicadores.
- Comparativos de productividad.
- Medición de cumplimiento frente a recaudo proyectado.

4. OBJETIVOS DEL PLAN DE TRABAJO

El comité definió como objetivos principales:

1. Mejorar los niveles de recuperación.
2. Incrementar productividad operativa.
3. Priorizar gestión sobre cartera de alto impacto.
4. Fortalecer control y seguimiento diario.
5. Garantizar cumplimiento de metas de recaudo y honorarios.

5. COMPROMISOS

Compromiso	Responsable	Fecha
Ejecutar foco sobre cuentas de alto valor	Equipo Operativo	Abril 2026
Publicar tablero diario de resultados	Supervisión Operativa	Diario
Monitorear cumplimiento de indicadores	Coordinadores	Permanente
Fortalecer seguimiento a negociaciones	Equipo de Cobranza	Abril 2026
Realizar control de metas de honorarios	Dirección Operativa	Abril 2026

6. CONCLUSIONES

Se concluyó que el fortalecimiento del seguimiento operativo y la priorización estratégica de cartera permitirán mejorar los resultados de recuperación durante abril de 2026. Asimismo, se resaltó la importancia de mantener control diario sobre productividad, negociaciones y cumplimiento de metas.

7. CIERRE

Se da por finalizado el comité dejando aprobadas las estrategias operativas y los mecanismos de seguimiento definidos para el cumplimiento de los objetivos planteados en el plan de trabajo de abril 2026.

ELABORÓ	APROBÓ
JOHN ALEXANDER SERNA GARCIA JOHN ALEXANDER SERNA GARCIA PROFESIONAL 06 Gerencia de Cobranzas y Brdpr	

1. Resumen

Título de la reunión	SEGUIMIENTO ABRIL REINCAR
Participantes que asistieron	3
Hora de inicio	4/15/26, 8:55:34 AM
Hora de finalización	4/15/26, 9:23:37 AM
Duración de la reunión	28 min 3 s
Tiempo medio de asistencia	26 min 16 s

2. Participantes

Nombre	Primera entrada	Última salida	Duración de la reunión	Correo electrónico	Id. de participante (UPN)	Rol
John Alexander Serna Garcia	4/15/26, 8:56:05 AM	4/15/26, 9:23:37 AM	27 min 32 s	jsernag@fna.gov.co	jsernag@fna.gov.co	Organizador
Grupo reincar SAS	4/15/26, 8:56:16 AM	4/15/26, 9:23:23 AM	27 min 7 s			Moderador

3. Actividades de la reunión

Nombre	Hora de entrada	Hora de salida	Duración	Correo electrónico	Rol
John Alexander Serna Garcia	4/15/26, 8:56:05 AM	4/15/26, 9:23:37 AM	27 min 32 s	jsernag@fna.gov.co	Organizador
Grupo reincar SAS	4/15/26, 8:56:16 AM	4/15/26, 9:23:23 AM	27 min 7 s		Moderador

Gerencia Tesorería
Documento de Pago

N° Orden de Pago	2940	Fecha de Registro	22-may-26
N° Documento de Pago	5300334832	Fecha de Giro	22-may-26

RESPONSABLE DEL PAGO

Nombre Completo	RECUPERADORA Y NORMALIZADORA INTEGR		
Nª Identificación	9004052365	Tipo de Identificación	NIT
Concepto	ELEC2940 RAD 02-2303-202605130650896		
Observaciones			

BENEFICIARIO DEL PAGO

Nombre Completo	RECUPERADORA Y NORMALIZADORA INTEGR		
Nª Identificación	9004052365	Tipo de Identificación	NIT
Forma de Entrega	Pago Electrónico		
Ciudad de Entrega	BUCARAMANGA		
Numero de Cuenta	184197929	Tipo de Cuenta	Cuenta Corriente
Banco	BANCO DE BOGOTA		
Valor Bruto	$ 0		
Menos GMF	$ 0		
Vlr Neto a Cancelar	$ 345.395.600		

Uso interno de Tesoreria

Orden	59560	Fecha de la Propuesta	22-may-26

Información UVR

Valor Orden de Pago UVR	$	0
Valor Cotización UVR	$	0

Observaciones:

Nota: Los valores expresados en pesos para los retiros de cesantías, según la Ley 1955 de 2019 Artículos 224 y 225' y el reglamento de cesantías, serán liquidados con la cotización de la UVR del día de la aprobación de la orden de pago por parte del Fondo Nacional del Ahorro S.A.