INFORME

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL
III TRIMESTRE DE 2023

Bogotá, D.C., 17-10-2023

INTRODUCCIÓN

La Caja Promotora de Vivienda Militar y de Policía en adelante Caja Honor, por ser una Entidad Financiera de carácter especial, organizada como establecimiento de crédito, vigilada por la Superintendencia Financiera de Colombia, en adelante SFC, en desarrollo de su objeto social está expuesta al Riesgo Operacional, por lo que, en cumplimiento de las directrices impartidas por la SFC, adoptó un Sistema de Administración de Riesgo Operacional (SARO Circular Externa N°018 de 2021) el cual debe desarrollar, establecer, implementar y actualizar.

1 RIESGO OPERACIONAL

A corte del tercer trimestre de 2023 Caja Honor registra un total de **71** riesgos operacionales identificados al interior de los 17 procesos en las diferentes áreas, con una calificación del perfil de riesgo residual de **2,72**[1] puntos, manteniendo el nivel de exposición **Bajo** dada la efectividad de los controles y la cobertura de estos en relación con el riesgo Inherente.

Tabla 1. Nivel de exposición al riesgo - III Trimestre 2023

Concepto	Cantidad	Riesgo Inherente		Riesgo Residual	
Riesgos Operacionales	71	Riesgo Extremo	0	Riesgo Extremo	0
		Riesgo Alto	34	Riesgo Alto	0
		Riesgo Moderado	33	Riesgo Moderado	0
		Riesgo Bajo	4	Riesgo Bajo	71
Nivel de exposición al riesgo		**7,14**		**2,72**	

Fuente: Oficina Asesora de Gestión del Riesgo (2023).

1.1 Registro de Eventos de Riesgo Operacional (RERO):

Durante el tercer trimestre de 2023, se recibieron **34 RERO´s**, reportados por los procesos y analizados por la Oficina Asesora de Gestión del Riesgo en adelante OAGRI:

[1] Indicador Riesgo Bajo (promedio ponderado de la calificación de los 71 riesgos en una escala de 1 – 25).

1. Un RERO reportado como Ejecución y administración de procesos afectó estado de resultados en $ 2.500.000 debido a una condena en costas procesales.

2. Un RERO correspondiente a provisión por $ 225.719.054,33, para procesos con probabilidad de pérdida.

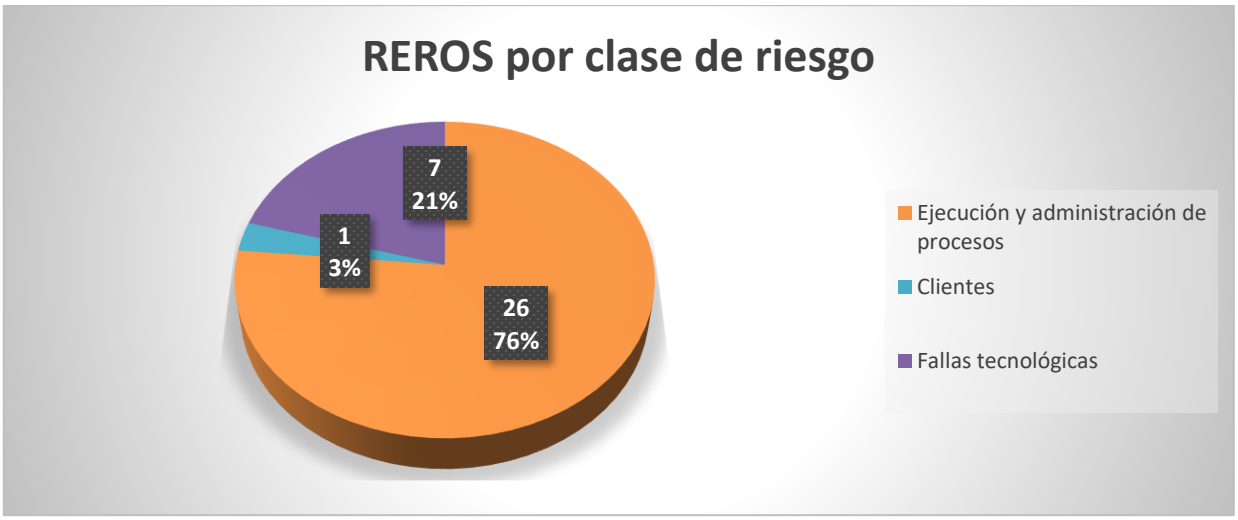

Figura 1. Fuente: Oficina Asesora de Gestión del Riesgo (2023).

1.2 Capacitaciones

La OAGRI brindó inducción sobre el Sistema de Administración del Riesgo Operacional (SARO) a un grupo de **14** funcionarios que ingresaron durante el trimestre a Caja Honor para los diferentes procesos.

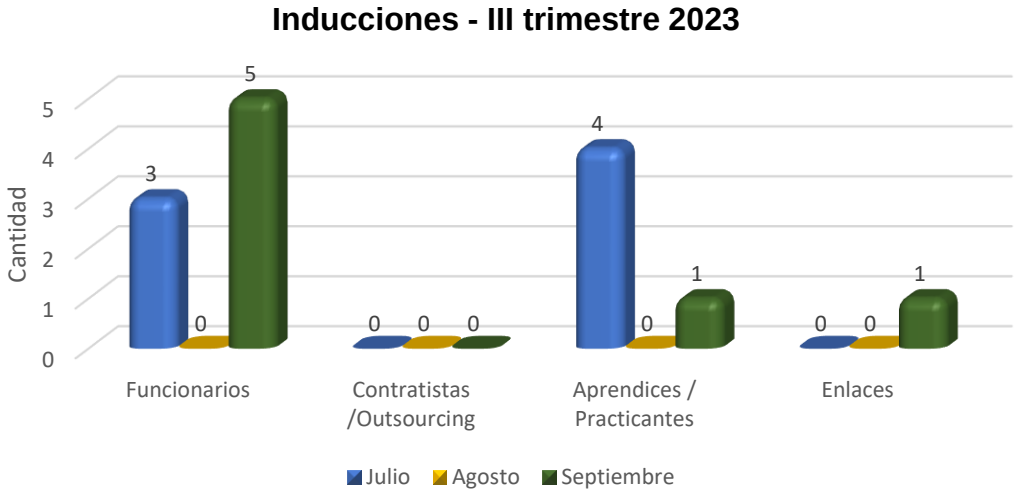

Figura 2. Fuente: Oficina Asesora de Gestión del Riesgo (2023).

En la inducción, la OAGRI efectuó una descripción general del SARO, enfatizando en la responsabilidad que cada funcionario adquiere al ingresar a la Entidad, con relación a los eventos de riesgo operacional que se puedan materializar en su proceso.

Asimismo, se realizó la capacitación virtual de SARO a 326 de 410 funcionarios (personal de planta, contratistas, aprendices SENA / practicantes universitarios y personal de las oficinas de enlace), quienes presentaron la evaluación de conocimiento.

Los funcionarios que por diferentes circunstancias (vacaciones, comisión, incapacidad, licencia o compromisos laborales) no desarrollaron la capacitación, la Oficina Asesora de Gestión del Riesgo gestionará la participación en la capacitación a través de la presentación de una nueva evaluación individual.

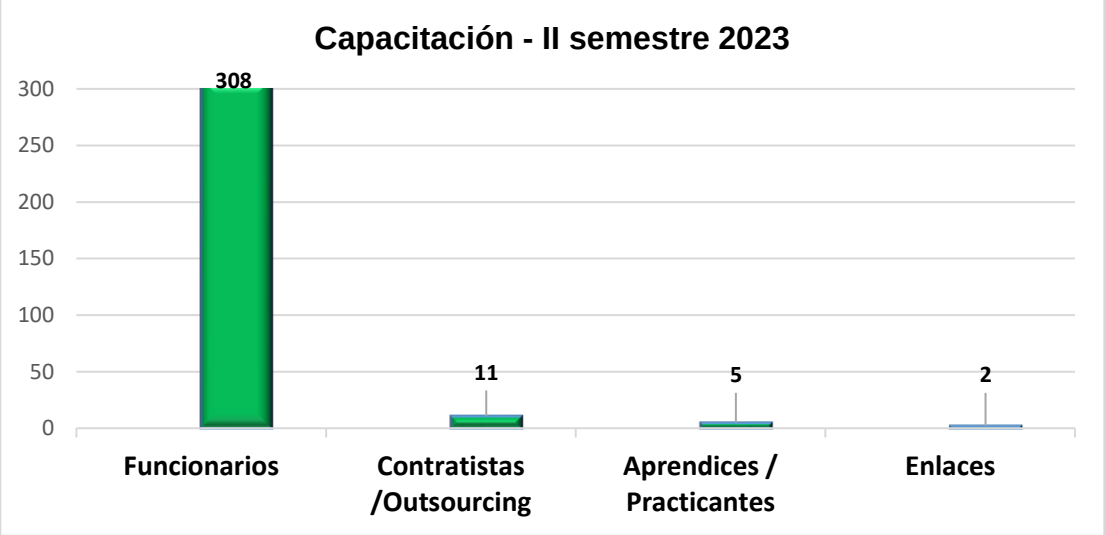

Figura 3. Fuente: Oficina Asesora de Gestión del Riesgo (2023).

1.3 Seguimiento Indicadores de Riesgo Operacional

Conforme con lo establecido en el Manual SARO, la OAGRI recibió la información necesaria para realizar el seguimiento de los indicadores de Riesgo Operacional definidos en este, así:

1.3.1 Indicador de Disponibilidad:

Este indicador alcanzó la meta al **100 %** durante este trimestre, con un promedio de disponibilidad de **99,75 %** en la sede principal y los puntos de atención. *(Información remitida por la Oficina Asesora de Informática).*

1.3.2 Indicador de Registro de Eventos de Riesgo Operacional (RERO):

El indicador de registro de eventos de riesgo alcanzó el **100 %**, debido a la gestión de los diferentes usuarios de los procesos, el acompañamiento de la OAGRI mediante la Guía GR-NA-GU-029 (Reporte general de eventos de riesgo) y para que los usuarios reporten situaciones que puedan traducirse en posibles eventos de riesgo operacional y que la OAGRI evalúa y analiza para confirmarlos como RERO´s o descartarlos.

1.3.3 Incidentes:

El indicador alcanzó el **89,16 %** de la meta establecida para el tercer trimestre, con la atención de incidentes en menos de 4 horas al **88,89 %**

Tabla 2. Incidentes III trimestre de 2023

Mes	Incidentes	Inferior a 4H	Indicador	Cumplimiento
Julio	11	11	100%	100%
Agosto	14	14	100%	100%
Septiembre	18	12	66,67%	66,67%
Total	43	37	88,89%	89,16%

Fuente: Oficina Asesora de Informática (2023).

1.3.4 Quejas:

El indicador alcanzó la meta en un **100 %,** donde el promedio de quejas durante el trimestre fue de **7** quejas por mes.

Tabla 3. Quejas III trimestre de 2023

Mes	Quejas
Julio	3
Agosto	8
Septiembre	10
Total	21

Fuente: Área de Atención Consumidor Financiero (2023).

Adicionalmente, se informa que las 21 quejas recibidas se analizaron y se determinó la favorabilidad de la siguiente manera:

Tabla 4. Favorabilidad de las quejas III trimestre de 2023

Tema	Cantidad	Favorabilidad	
	Quejas	Entidad	Consumidor financiero
Indebida atención del funcionario	11	2	9
Inconformidad con la información	6	3	3
Inconformidad con el servicio	4	3	1

Fuente: Área de Atención Consumidor Financiero (2023).

1.3.5 Desempeño Frecuencia Riesgo Operacional:

El indicador alcanzó el **100 %** de cumplimiento, dado que la frecuencia de Riesgo Operacional (RO) se ubicó en **87,32 %** de acuerdo con la meta establecida en la escala de calificación de Riesgo Operacional.

El indicador de probabilidad – impacto, registró que, de los **71** riesgos identificados:

- El **12,68 %** afectó la probabilidad de ocurrencia (nueve riesgos).
- El **2,82 %** (dos riesgos) afectaron el impacto.

Dejando como resultado un cumplimiento del **97,18 %** para este indicador.

1.3.6 Cumplimiento de órdenes de embargo[2]:

1.3.6.1 Gestión de embargos: durante el tercer trimestre se recibieron 1.604 requerimientos judiciales, los cuales 1.593 fueron atendidos en menos de 5 días, alcanzando el **99,31** % de cumplimiento de la meta establecida para este indicador**.**

1.3.6.2 Pago depósitos judiciales: de los 1.604 requerimientos judiciales recibidos, 145 corresponden a pagos de depósitos judiciales, los cuales en su totalidad se surtieron en un término menor a 3 días, alcanzando la meta para este indicador en un **100 %.**

[2] Informe Órdenes Judiciales de Embargo, Grupo Asuntos Jurídicos de Operaciones, octubre de 2023.

2 PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)

Durante el tercer trimestre se llevaron a cabo las siguientes actividades en cumplimiento de los controles de las normas ISO[3] y a los requerimientos de la Superintendencia Financiera de Colombia:

2.1 Simulacro de Plan de recuperación de desastre – DRP[4]

El escenario definido para el desarrollo del simulacro es la pérdida de conexión por falla o interrupción del Data Center Principal, que obliga a pasar toda la operación al Data Center Alterno.

Para el desarrollo de esta actividad se llevaron a cabo reuniones con el grupo de manos expertas y los ingenieros de Caja Honor, con el objetivo de coordinar, verificar y realizar cualquier adecuación de las herramientas tecnológicas y definir los tiempos de reacción en cada actividad, así como el apoyo necesario en cualquiera de las fases definidas en el minutograma.

Se dio prioridad a los portales y página web por los tiempos requeridos para el paso de un Data Center al otro, se continuó con los aplicativos, servidores, redes, base de datos y la implementación de los controles de Seguridad de la Información y Ciberseguridad en la Entidad, obteniendo un éxito de 100 % en cada una de las etapas programadas.

2.1.1 Día 1 del simulacro de DRP - 4 de agosto de 2023

- ✓ Verificación del grupo de ingenieros.
- ✓ Revisión de puestos de trabajo, conectividad, correcto funcionamiento de los sistemas y herramientas tecnológicas de la Entidad.
- ✓ Inicio del proceso de backup[5] que contempla una duración aproximada entre 6 y 8 horas, esta actividad se llevó a cabo sin ningún inconveniente.

2.1.2 Dia 2 de simulacro de DRP – 5 de agosto de 2023

- ✓ Verificación de la conectividad de los ingenieros al aplicativo Teams.
- ✓ Análisis y verificación del estado de restauración de backup; una vez comprobado su perfecto estado, se inicia el procedimiento de desacople de los sistemas del Data Center Principal.
- ✓ Verificación y acople de los sistemas y herramientas de tecnología en el Data Center Alterno

[3] Normas ISO: son documentos que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo.
[4] DRP, sigla del inglés Disaster Recovery Plan (Plan de recuperación ante desastres).
[5] Backup: Copia de seguridad de los datos realizada en un soporte de almacenamiento adecuado

En el desarrollo de estas actividades se redujeron los tiempos de desactivación de los sistemas y restauración de los aplicativos y herramientas en el Data Center Alterno, así como el retorno de la operación al Data Center Principal, obteniendo un resultado del 100 % de éxito.

2.2 Simulacro de Ciberseguridad

De conformidad con lo establecido en la Circular Externa 007/2018 de la SFC, en su requerimiento del numeral 4.1.7 “Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos”, se efectuó una simulación de ataque en un equipo suministrado por la Entidad para tal fin.

Para el desarrollo de esta actividad los ingenieros de ciberseguridad y de Hacking[6] Ético, en coordinación con el ingeniero del PCN programaron todos los recursos y requerimientos necesarios para esta actividad, que se llevó de manera simultánea con el simulacro de DRP, con el objetivo de verificar y garantizar que todas las etapas programadas cuenten con los Controles de Seguridad de la Información y Ciberseguridad garantizando la protección de los perímetros de Vlans[7] (redes de área local virtuales), servidores e internet, contra ataques informáticos y protección contra programas malignos. Este ejercicio tuvo una efectividad del 100 %.

2.3 Punto Alterno de Continuidad- PAC

La Gerencia General aprobó el cambio de estrategia del Punto Alterno de Continuidad - PAC, la cual en adelante se llevará a cabo como trabajo remoto; por lo anterior, para validar la nueva estrategia se realizó la prueba del PAC en el tercer trimestre, para esto, se coordinó con las diferentes dependencias la definición del personal que participó, la asignación de los recursos y la definición de los procedimientos para garantizar la operación y los controles de Seguridad de la Información y Ciberseguridad.

2.3.1 Simulacro de Punto Alterno de Continuidad - PAC

Se llevó a cabo el 17 de agosto de 2023 aplicando la nueva estrategia de “trabajo remoto”, en la que se identificaron los procesos críticos de Caja Honor con los que se desarrolló la prueba, a su vez los líderes designaron el número de funcionarios que participaron en esta actividad, para lo que se hizo la entrega de equipos portátiles y se habilitaron los accesos por VPN[8]. Se realizaron las siguientes actividades:

1. Verificación de la conexión por VPN de todos los funcionarios.

[6] Hacking ético es el uso de habilidades y herramientas de hacking para evaluar la seguridad de un sistema informático o de una red, de manera legal y ética, con el objetivo de identificar y corregir posibles vulnerabilidades antes de que sean explotadas por hackers malintencionados
[7] VLANS (redes de área local virtuales)
[8] VPN o red privada virtual crea una conexión de red privada entre dispositivos a través de Internet se utiliza para transmitir datos de forma segura y anónima a través de redes públicas.

2. Mantener comunicación a través de Teams.
3. Validación de la adecuada conexión a los sistemas (aplicativos, base de datos, Sharepoint[9]).
4. Soporte y verificación de los controles de seguridad de la información y ciberseguridad.

El objetivo de esta actividad es garantizar la operación frente a un escenario que comprometa el acceso a las oficinas, esta actividad se llevó a cabo con una efectividad del 100 %.

2.4 Documentos del PCN

Durante este trimestre se actualizó el documento Guía de Análisis de Impacto de Negocio – BIA, con el fin de ajustar los valores de RPO[10] y RTO, se identifican procesos críticos y análisis de priorización de procesos.

2.5 Capacitación

Para este trimestre se realizó capacitación virtual de PCN dirigida a los funcionarios, la cual contó con una amplia participación:

Tabla 5. Capacitación PCN – III trimestre 2023

Mes	Funcionarios	Contratistas /Outsourcing	Aprendices / Practicantes	Enlaces	Total
Julio	256	12	7	2	277

Fuente: Oficina Asesora de Gestión del Riesgo (2023).

3 DOCUMENTOS Y PRONUNCIAMIENTOS EMANADOS DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Durante el trimestre de análisis se recibieron dos requerimientos de información por parte de la Delegatura para Riesgo Operacional y Ciberseguridad, con relación al nivel de madurez de la Gestión de Ciberseguridad mediante oficio radicado en la Entidad bajo el número 90-01-2023092500123 y con relación al Perfilamiento de Riesgo Cibernético el requerimiento bajo el radicado 90-01-2023092500124, se respondieron con radicado 03-01-20231011034039 con sus respectivos anexos.

De otro lado, se remitió el primer avance del plan de acción del seguimiento a las Instrucciones del Plan de Continuidad del Negocio, mediante radicado 03-01-20231009033692.

[9] SharePoint es una herramienta diseñada por Microsoft para la gestión documental y el trabajo en equipo.
[10] RPO es la pérdida real de datos entre la copia de seguridad y un incidente, el RTO es el tiempo que lleva solucionar el incidente antes de que todos los sistemas vuelvan a su normalidad.

4 CONCLUSIONES

La gestión del Riesgo Operacional está enfocada en la identificación y mitigación de riesgos que puedan generar pérdidas económicas por fallas en los procesos operativos o tecnológicos que afecten el desarrollo de la operación.

Durante el tercer trimestre de 2023, se evidenció el cumplimiento de las políticas establecidas en el Manual SARO; se dictaron inducciones al personal nuevo y capacitaciones al personal en general, el seguimiento y control de los eventos de riesgo operacional presentados y la medición de los indicadores, así como la gestión de la continuidad del negocio, de manera que se puede concluir que la Entidad mantiene el nivel de exposición al riesgo operacional en un nivel bajo.

Firmado por:
JOSE RAMIRO PAEZ OLARTE
2023/10/19 06:22:06
CC
80417277

JOSÉ RAMIRO PÁEZ OLARTE
Jefe de Oficina Asesora de Gestión del Riesgo

Elaboró:
Martha Patricia Reyes Gómez
Profesional Especializado – OAGRI

Elaboró:
Wilheim Erasto Cervantes Noguera
Profesional Especializado - OAGRI

Este documento ha sido realizado por los profesionales de la Oficina Asesora de Gestión del Riesgo de Caja Promotora de Vivienda Militar y de Policía. El uso de la información y cifras contenidas es exclusiva responsabilidad de cada usuario.