

18 de diciembre de 2025

INFORME 20 DE 2025

EVALUACIÓN A LA GESTIÓN RIESGO OPERACIONAL, PCN Y EVALUACIÓN RIESGO FRAUDE (NÚM. 4.4.2.4 PI, TI, CAP. IV SI CE 008 DE 2023 SFC/ RIESGOS FISCALES, NÚM. 4 GUÍA ADM. DEL RIESGO Y DISEÑO DE CONTROLES ENTIDADES PUB. V6 – DAFP) – (Periodo 01- 10-2024 al 30-09-2025)

TABLA DE CONTENIDO

1. OBJETIVO GENERAL	3
2. OBJETIVOS ESPECÍFICOS	3
3. ALCANCE	4
4. MARCO LEGAL	4
4.1. Normatividad Externa	4
4.2. Normatividad Interna	5
5. METODOLOGÍA	7
6. Desarrollo Procedimientos de Auditoría Gestión del Riesgo Operacional del 01-10-2024 al 30-09-2025	7
7. Riesgo Fraude (NÚM. 4.4.2.4 PI, TI, CAP. IV SI CE 008 DE 2023 SFC/ Riesgos Fiscales	25
8. Componente Plan de Continuidad del Negocio - PCN	28
9. SÍNTESIS	87
9.1. Síntesis Oportunidades de Mejora	87
a. Síntesis Recomendaciones	91
3. NIVEL DE PRIORIZACIÓN DE CRITICIDAD DE LOS HALLAZGOS	94
4. CONCLUSIONES	96

1. OBJETIVO GENERAL

Evaluar por parte de la Oficina de Control Interno (OFCIN) de la Caja Promotora de Vivienda Militar y de Policía (CPVMP), la efectividad y cumplimiento de cada una de las etapas y los elementos de la Gestión del Riesgo de Operacional, según lo establecido por la Superintendencia Financiera de Colombia (SFC) la normatividad aplicable en materia de Órdenes de Embargo (CE. 022 de 2018); Capítulo XXXI en la CBCF Sistema Integral de Administración de Riesgos (SIAR) estipulado en la CE. 018 del 2021 de la SFC en su Anexo 13 “metodología estándar para determinar el valor de la exposición al riesgo operacional de los establecimientos de crédito”. Realizando entre otras actividades, revisión del Registro de Eventos de Riesgo Operacional (RERO) informando los resultados de la auditoría, al Representante Legal y la OAGRI, revisión del cumplimiento del Anexo 1 “Método Estándar para determinar el Valor de la Exposición al Riesgo Operacional de los Establecimientos de Crédito” - VERRO (Capítulo XXIII en la CBCF (CE. 100 de 1995) y lo pertinente de la CE. 020 de 2019 (Relaciones Mínimas de Solvencia, Capítulo XIII-16 - Margen de Solvencia y otros Requerimientos de Patrimonio CBCF – CE. 100 de 1995); asimismo, el equipo auditor revisará el cumplimiento de las políticas internas en los procesos interrelacionados, de las dimensiones y políticas del Modelo Integrado de Planeación y Gestión (MIPG) establecidas en Manual Operativo del MIPG, versión 6 de diciembre de 2024 y lo pertinente para el Sistema de Control Interno (SCI) según lo requerido por la SFC en la Parte I, Título I, Capítulo IV Circular Externa 006 de 2025 – Superintendencia Financiera de Colombia “Por la cual se subroga el texto completo de la Circular Externa 029 de 2014 (Circular Básica Jurídica), las modificaciones realizadas a través de la CE. 008 de 2023 “Instrucciones relativas al Sistema de Control Interno de las Entidades Vigiladas”, así como las demás modificaciones y/o actualizaciones pertinentes.

2. OBJETIVOS ESPECÍFICOS

- Evaluar para el periodo entre el 01-10-2024 hasta el 30-09-2025 la efectividad y cumplimiento de cada una de las etapas y los elementos de la Gestión del Riesgo Operacional.
- Revisar los cálculos y reportes realizados pertinentes al VERRO según lo requerido en el Anexo 13 del Capítulo XXXI de la CE. 018 de 2021; revisando los aspectos evaluados en la auditoría anterior de la OFCIN en el Informe 25 de 2024.
- Realizar revisión periódica del RERO, e informar al Representante Legal sobre el cumplimiento de las condiciones señaladas en el marco normativo de la SFC Capítulo XXXI de la CE. 018 de 2021, Parte III, numeral 4.2.2.2.4
- Verificar el monitoreo por parte de la OAGRI del cumplimiento por parte de Caja Honor del numeral 4.5. (“reglas especiales en materia de órdenes de embargo”), del marco normativo de la SFC.
- Evaluar el cumplimiento de las políticas, procedimientos, estructura organizacional, y lineamientos generales que le permiten a la CPVMP, identificar, medir, controlar y monitorear los objetivos establecidos para la Gestión del Riesgo Operacional.
- Verificar las Matrices de Riesgos Operacionales de cada proceso, causas y controles de la Gestión de Riesgo Operacional actualizadas y aprobadas por la Junta Directiva para el periodo auditado.
- Velar por el oportuno flujo de información a la Junta Directiva y a la Alta Gerencia, verificando a través de muestras aleatorias de fechas, los reportes realizados por la OAGRI en las periodicidades establecidas normativamente.

- Observar los informes remitidos por la Revisoría Fiscal pertinentes a la Gestión del Riesgo Operacional según lo establecido en el numeral 3.6. del marco normativo de la SFC, verificando el dictamen de los Estados Financieros de la vigencia 2024.
- Verificar la efectividad en la gestión del riesgo de las políticas de Riesgos de Fraude de conformidad a la CE 008 de 2023 - SFC y Riesgos Fiscales - DAFP, el cumplimiento de las Políticas Antifraude, Anticorrupción, Antisoborno y fiscal, la implementación de controles a través de sus procedimientos, caracterizaciones, mapas de riesgos y actividades de capacitación en cumplimiento a los lineamientos establecidos por la SFC - DAFP y respecto al marco legal aplicable.

3. ALCANCE

Evaluar la efectividad y cumplimiento de las Etapas y Elementos de la Gestión del Riesgo Operacional para el periodo auditado entre el 01-10-2024 hasta el 30-09-2025, de acuerdo con el marco normativo vigente establecido por la SFC y las modificaciones de la implementación del Capítulo XXXI en la CBCF SIAR estipulado en la CE. 018 del 2021 de la SFC, verificando las políticas, procedimientos, estructura organizacional, los procesos interrelacionados, la implementación del Manual del SIAR, procedimientos y demás documentación pertinente, los registros pertinentes de Eventos de Riesgo Operacional (RERO) del periodo auditado bajo en anexo 13 de la CE. 018 de 2021 SIAR de la SFC y la normatividad aplicable en materia de Órdenes de Embargo (CE. 022 de 2018), lo pertinente al Anexo 1 VERRO, revisión de los requerimientos y/o comunicaciones con la SFC; verificando el cumplimiento de las políticas internas, de los procedimientos, de las dimensiones y políticas establecidas en Manual Operativo del MIPG, versión 6 de diciembre de 2024, controles en los procesos interrelacionados, estructura organizacional, los reportes realizados a Junta Directiva y la Alta Gerencia, entre otros requisitos normativos de la SFC y demás consideraciones impartidas por la CPVMP en los Manuales y demás documentación relacionada.

4. MARCO LEGAL

4.1. Normatividad Externa

- Capítulo XXXI en la Circular Básica Contable y Financiera (CBCF) Sistema Integral de Administración de Riesgos (SIAR) estipulado en la CE 018 del 22-09-2021 de la SFC.
- Capítulo II CBCF (CE 100 de 1995 y su modificación a través de CE 009 de 2022, CE 042 de 2020, CE 022 de 2020, CE 016 de 2019, CE 026 de 2017 y demás que lo actualicen y/o modifiquen) de la SFC.
- Ley 546 de 1999 del Congreso de Colombia – “por la cual se dictan normas en materia de vivienda, se señalan los objetivos y criterios generales a los cuales debe sujetarse el Gobierno Nacional para regular un sistema especializado para su financiación, se crean instrumentos de ahorro destinado a dicha financiación, se dictan medidas relacionadas con los impuestos y otros costos vinculados a la construcción y negociación de vivienda y se expiden otras disposiciones”.
- Ley 2157 de 2021 del Congreso de Colombia “modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del habeas data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”. – Ley Borrón y Cuenta Nueva.
- Decreto 739 de 02-07-2021 Ministerio de Vivienda, Ciudad y Territorio “por el cual se modifica el Decreto 1077 de 2015 en relación con las condiciones de asignación y operación del subsidio familiar de vivienda”.

- Decreto 1233 de 2020 Ministerio de Hacienda y Crédito Público "por el cual se modifica el Decreto 1068 de 2015 Decreto Único Reglamentario del Sector Hacienda y Crédito Público, en lo relacionado con la cobertura del Programa FRECH NO VIS".
- Estatuto Orgánico del Sistema Financiero (EOSF).
- Decreto 2555 de 2010, Decreto Único del Sistema Financiero, CE 100 de 1995 SFC Capítulos adicionales I, XIX, y XXV.
- Circular Externa 006 de 2025 – Superintendencia Financiera de Colombia “Por la cual se subroga el texto completo de la Circular Externa 029 de 2014 (Circular Básica Jurídica), por el texto jurídico que se expide por medio de la presente circular y Circular Externa 008 de 2023 – Superintendencia Financiera de Colombia “Instrucciones relativas al Sistema de Control Interno de las Entidades Vigiladas”.
- Ley 973 de 2005, reglamentación que modifica la normatividad por la cual fue creada la Caja Promotora de Vivienda Militar y de Policía
- Ley 87 de 1993 “por la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del estado y se dictan otras disposiciones”.
- Decreto 076 del 21-01-2022 “por medio del cual se modifica la estructura de la Caja Promotora de Vivienda Militar y de Policía”, modificando el Decreto 1900 de 2013 del 06-09-2013, dentro de los cuales se determinan las funciones de sus dependencias y se dictan otras disposiciones.
- Decreto 2636 de 2022 MDN “por el cual se adiciona la Subsección 2 a las Sección 1 del Título 2 de la Parte 6 del Libro 2 del Decreto 1070 de 2015 del Decreto Único Reglamentario del Sector Administrativo de Defensa, en lo relacionado con el ajuste del esquema vigente de Subsidios de Vivienda para los afiliados” de la CPVMP.
- Decreto 648 de 2017 “por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública”.
- Decreto 1499 de 2017 “por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015”.
- Ley 1952 de 2019 para lo concerniente en Conflicto de Interés.
- Ley 2195 de 2022, “por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones”, que modifica la Ley 1474 de 2011, Ley 1712 de 2014.
- Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG), versión 6 de diciembre de 2024.
- Norma ISO 27001:2022 Gestión de Seguridad de la Información.
- Resolución 7870 del 2022 “Política General de Seguridad y Privacidad de la Información para el Sector Defensa” MDN.
- Norma Internacionales de Auditoría NIA, Evaluación del riesgo y respuesta a los riesgos evaluados/control interno, NIA-402” consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios”, NIA-450 “evaluaciones de las incorrecciones identificadas durante la realización de la auditoría”, Evidencia de auditoría, NIA-500 “evidencia de auditoría” y NIA-530 “muestreo de auditoría”.
- Normas Internacionales Para el Ejercicio Profesional de la Auditoría Interna, Marco Internacional para la Práctica Profesional MIPP.

4.2. Normatividad Interna

- Resolución 084 de 2022, “por la cual se actualizan y unifican las disposiciones que regulan la estructura, funciones y siglas de las Áreas y Grupos Internos de Trabajo de la Caja Promotora de Vivienda Militar y de Policía y se dictan otras disposiciones”, deroga

la Resolución 079 de 2021 la cual derogó las Resoluciones 320 y 592 de 2018 y 241 de 2019 y las demás disposiciones que le sean contrarias Modificada por la Resolución 196 del 2022. / Modificada por la Resolución 068 de 2025.

- Acuerdo 01 del 29-01-2021, que modifica al Acuerdo 02 de 2016 y deroga al Acuerdo 01 de 2017, actualiza las disposiciones que regulan el funcionamiento del Comité Financiero y Comité de Riesgos de la CPVMP.
- Acuerdo 02 del 28-05-2021 “por el cual se establecen las condiciones generales y financieras del Crédito Hipotecario de la Caja Promotora de Vivienda Militar y de Policía y se dictan otras disposiciones” y Resolución 342 del 18-06-2021 (implementa el Acuerdo 02 de 2021).
- Acuerdo 05 de 2016 “por el cual se adopta el Estatuto Interno de la Caja Promotora de Vivienda Militar y de Policía”.
- Manual del Sistema Integrado de Administración de Riesgos (SIAR), Cod. GR-MA-010, versión 7 del 27/11/2025.
- Procedimiento etapas Gestión Riesgo de crédito, Cod. GR-PR-024, Versión 12 del 31/Oct/2025.
- Formato Solicitud de Producto de Créditos de Vivienda (Conocimiento del Cliente), Cod. GR-FM-018, Versión 22 del 31/Oct/2025.
- Procedimiento Seguimiento Inmuebles Entregados en Leasing Habitacional, Cod. AS-PR-008, Versión 10 del 31/Oct/2025.
- Manual de Seguridad de la Información y Ciberseguridad, Código: GR-MA-009, Versión 5 del 30/Sep/2025.
- Guía de Gestión de Incidentes de Ciberseguridad, Código: IT-GU-030, Versión 7 del 31/Oct/2025.
- Guía Gestión de Incidente de Seguridad de la Información, Código: GR-GU-023, Versión 11 del 31/Oct/2025.
- Guía Elaboración de Simulaciones de Crédito, Código: RE-GU-006, Versión 2 del 31/Oct/2025.
- Manual del Producto Crédito de Vivienda y Leasing Habitacional, Código: RE-MA-001, Versión 2 del 06/Jun/2025.
- Procedimiento Evaluación de Garantías para Créditos de Vivienda, Código: RE-PR-006, Versión 2 del 31/Oct/2025.
- Guía de Protocolo de Seguridad de la Información y Ciberseguridad para Trabajo a Distancia de código GR-GU-036 V6 - 31-10-2025
- Guía General Reporte de Eventos de Ciberseguridad al CCOC – CSIRT – COLCERT de código IT-GU-029 V9 - 31-10-2025
- Guía Gestión de Incidentes de Ciberseguridad de código IT-GU-030 V7 - 31-10-2025.
- Acuerdo De Confidencialidad Y Políticas De Seguridad De La Información Para La Etapa Pre Contractual de código GR-FM-034 V012 - 31-10-2025.
- Acuerdo de Confidencialidad y Políticas de Seguridad de la Información y Ciberseguridad para la Relación Contractual o Legal y Reglamentaria de código TH-FM-053 V25 - 31-10-2025.
- Formato Evaluaciones de Seguridad de la Información en Visitas a Proveedores de código GR-FM-027 V012 - 31-10-2025.
- Guía General Gestión De Eventos E Incidentes De Seguridad De La Información de código GR-GU-023 V11 - 31-10-2025.
- Manual de Gestión del Plan de Continuidad del Negocio – PCN de código GR-MA-008 V007 / 26-09-2025
- Plan de Recuperación ante Desastres – DRP de código IT-PL-003 V9 – 31-10-2025.

- Guía de Operación punto Alterno de Continuidad – PAC de código GR-GU-005 V16 – 31-10-2025

5. METODOLOGÍA

Según lo estipulado en el marco normativo de la SFC y lo documentado en la “Guía Evaluar Gestión del Riesgo Operacional y PCN” con código CI-GU-006, versión 019 del 31-10-2025, para el desarrollo de los objetivos de auditoría descritos, el equipo auditor realiza un requerimiento inicial de información a la OAGRI, que permite hacer un diagnóstico inicial del cumplimiento normativo de la Gestión de Riesgo Operacional, de Eventos de Riesgo Operacional (RERO) del periodo auditado bajo en anexo 13 de la CE. 018 de 2021 SIAR de la SFC y la normatividad aplicable en materia de Órdenes de Embargo (CE. 022 de 2018), lo pertinente al Anexo 1 VERRO; verificar el cumplimiento de las políticas internas establecidas para su gestión durante el periodo auditado a través de técnicas de muestreo aleatorio los reportes a la SFC, a la Alta Gerencia, los RERO, cumplimiento de los indicadores de Riesgo Operacional (disponibilidad, incidentes, Cumplimiento de Órdenes de Embargo, entre otros), informes de la Revisoría Fiscal, cumplimiento de la capacitación a los funcionarios y contratistas de la CPVMP.

6. Desarrollo Procedimientos de Auditoría Gestión del Riesgo Operacional del 01-10-2024 al 30-09-2025

La CPVMP es una Empresa Industrial y Comercial del Estado de carácter financiero del orden nacional, vigilada por la SFC, organizada como establecimiento de crédito, de naturaleza especial, dotada de personería jurídica, autonomía administrativa y capital independiente, vinculada al Ministerio de Defensa Nacional; para la presente auditoría el marco normativo de la SFC aplicable es el Capítulo XXXI, en la CBCF (CE 100 de 1995) SIAR y sus respectivos anexos, para lo pertinente a la Gestión del Riesgo Operacional.

La OFCIN desarrolló esta auditoría in situ y virtual (a través de herramientas colaborativas), cumpliendo satisfactoriamente con el objetivo, alcance, los tiempos, calidad del producto entregado; utilizando los medios proporcionados tales como: correo electrónico, aplicativos, chat corporativo (Teams) y FileServer, que permitieron verificar por el auditor, el adecuado funcionamiento en los procesos interrelacionados, muestreos aleatorios en el cumplimiento de reportes a la SFC y Alta Gerencia; asimismo, la elaboración del presente informe, traslado de resultados, comunicación con los procesos interrelacionados y entregas a la GERGE, sin que se hayan materializado riesgos, ni presentado inconvenientes de tipo material o afectación en la prestación del servicio del proceso de Auditoría y Control.

1.1. Verificación Informes Riesgo Operacional a la Junta Directiva y Comité de Riesgos

En la verificación de la OFCIN, durante el periodo auditado, se revisó el cumplimiento del Capítulo XXXI de la CE. 018 de 2021 y los anexos que le apliquen al Riesgo Operacional; evidenciando los informes trimestrales presentados a la JD, con los aspectos relevantes del RO y el pronunciamiento de los miembros de la JD en las actas correspondientes; los informes fueron presentados según lo establecido en el Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, con los siguientes aspectos relevantes:

Tabla 1. Verificación OFCIN, Informes Riesgo Operacional Periodo auditado 01-10-2024 a 30-09-2025

ASPECTO REVISADO	III TRIM 2025		
	IV TRIM 2024	II TRIM 2025	III TRIM 2025
Ajustes realizados al RO	Durante el trimestre se realizó la actualización de las matrices de riesgos de los procesos, con el fin de incluir un nuevo riesgo transversal, junto a las causas identificadas y los controles de mitigación, encaminados a fortalecer la supervisión de contratos.	Durante el trimestre se realizaron sesiones con Grupos de Expertos para revisar los riesgos por proceso, considerando insumos como hallazgos de auditoría, salidas no conformes, eventos reportados y proyectos en curso. No se identificó la necesidad de incorporar nuevos riesgos operacionales.	Durante el trimestre las matrices de riesgo se mantienen sin modificaciones, toda vez que no se identificó la necesidad de incorporar nuevos riesgos operacionales.
# RO y Perfil Riesgo Residual	71 RO, 2.72 puntos de riesgo residual, con nivel exposición bajo	71 RO, 2.75 puntos de riesgo residual, con nivel exposición bajo	71 RO, 2.75 puntos de riesgo residual, con nivel exposición bajo

ASPECTO REVISADO	IV TRIM 2024	I TRIM 2025	II TRIM 2025	III TRIM 2025
Número y afectación de Estado Resultados Integral Entidad	16 REROS, Uno de los eventos reportados afectó Estado de Resultados, correspondiente a la provisión inicial para un proceso jurídico por \$ 375.583.630. Durante el trimestre se reversaron \$ 2.501.159 por concepto de provisiones de procesos jurídicos.	20 REROS, Uno de los eventos reportados afectó el Estado de Resultados, correspondiente a la provisión inicial para un proceso jurídico por \$ 45.030.599. Durante el trimestre se registraron \$ 184.344.025 por concepto de recuperación de provisiones de litigios.	19 REROS, ninguno de los eventos reportados afectó Estado de Resultados	16 REROS, (4) eventos con afectación directa, de los cuales tres (3) corresponden a la constitución inicial de provisiones por procesos jurídicos, por un valor total, de \$ 141.680.944,09. El cuarto evento corresponde a un pago ordenado por juzgado, relacionado con un incidente de solidaridad en un proceso de alimentos, por \$ 1.423.500.
Capacitaciones	13 inducciones a funcionarios, contratistas. 370 funcionarios y colaboradores plan de capacitación. 350 funcionarios 3 contratistas 5 aprendices practicantes 12 enlaces Porcentaje participación 94,30%	14 inducciones a funcionarios y aprendices nuevos.	15 inducciones a funcionarios y aprendices nuevos. 398 funcionarios y colaboradores plan de capacitación. 347 funcionarios 18 contratistas 12 aprendices practicantes 21 enlaces Porcentaje participación 93,65%	11 inducciones a funcionarios nuevos.

1 RERO: Registro Evento Riesgo Operacional

ASPECTO REVISADO	IV TRIM 2024		I TRIM 2025		II TRIM 2025		III TRIM 2025	
	Indicador	RERO	Indicador	RERO	Indicador	RERO	Indicador	RERO
Incidentes	100 %	100 %	99.70%	100 %	99.70%	100 %	100 %	88,27%
Quejas (promedio trimestre)	5 por mes	2 por mes	99.70%	2 por mes	99.70%	4 por mes	6 por mes	6 por mes
Desempeño frecuencia Riesgo Operacional	91.55%	88.73%	88.73%	88.73%	88.73%	88.73%	92.96%	92.96%
Desempeño Probabilidad Impacto	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (1 riesgo) afectaron el Impacto. alcanzando 98,59% para este indicador.	De los 71 riesgos identificados, (2 riesgos) afectaron el Impacto. alcanzando 97,18% para este indicador.
Cumplimiento de Órdenes Embargo CE. 022 2018	Seguimiento de los siguientes indicadores: <ul style="list-style-type: none"> Durante el trimestre se recibieron 2.433 requerimientos judiciales, de los cuales 2.427 fueron atendidos en menos de 5 días (99,75 %), alcanzando el 100 % logrando la meta establecida 95 % Se radicaron 240 corresponden a pagos de depósitos judiciales, 	Seguimiento de los siguientes indicadores: <ul style="list-style-type: none"> Gestión de Embargos: Se recibieron 1.635 requerimientos judiciales, de los cuales 1.632 fueron atendidos en menos de 5 días (99,82 %), alcanzando el 100 % de cumplimiento de la meta establecida 	Seguimiento de los siguientes indicadores: <ul style="list-style-type: none"> Gestión de Embargos: Se recibieron 1.819 de 1.836 requerimientos judiciales en menos de 5 días (99,07 %), logrando la meta (95 %). Los 243 pagos se realizaron en menos de 3 días, alcanzando el 100 % de cumplimiento 	Seguimiento de los siguientes indicadores: <ul style="list-style-type: none"> Gestión de Embargos: Se atendieron 1.948 de 1.959 requerimientos judiciales en menos de 5 días (99,44 %), logrando la meta establecida (95 %). se radicaron 187 requerimientos judiciales de pago, de los cuales 185 fueron gestionados en un plazo menor a tres (3) días, y los dos (2) 				

ASPECTO REVISADO	IV TRIM 2024	I TRIM 2025	II TRIM 2025	III TRIM 2025
	los cuales en su totalidad se surtieron en un término menor a 3 días, alcanzando la meta establecida (100 %).	<p>para este indicador que es 95 %.</p> <ul style="list-style-type: none"> Se radicaron 147 corresponden a pagos de depósitos judiciales, los cuales en su totalidad se surtieron en un término menor a 3 días, alcanzando la meta establecida (100 %). 		<p>restantes se procesaron en un tiempo superior. Esto permitió alcanzar un cumplimiento del 98,93% frente a la meta establecida del 100%. Los dos casos que excedieron el plazo se debieron a que el funcionario responsable no realizó la tipificación correspondiente al día siguiente de recibir el requerimiento judicial.</p>

Fuente: Elaboración OFCIN, requerimiento de Información OAGRI, noviembre 2025.

Según lo analizado por el equipo auditor, se evidencia el cumplimiento de los Informes de Comité de Riesgos y JD, reportados por la OAGRI, según el numeral 3.3.2 literal a, del marco normativo vigente para el SIAR de la SFC.

1.2. Revisión Registro de Eventos de Riesgo Operacional (RERO)

Durante el periodo auditado, para el registro de los RERO, se encontraba vigente lo estipulado en el numeral 6.4.4 del Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, la Guía de Reporte General de Eventos de Riesgo código GR-GU-029, versión 010 del 31-10-2025, el Procedimiento Reporte y Registro de Eventos de Riesgo Operacional, con código GR-PR-019, versión 009 del 31-10-2025 y la Guía Aprobación de REROS en el Sistema de Información, código GR-GU-037, versión 005 del 31-10-2025; verificando para cada trimestre auditado, el grado de detalle de la información requerido por la SFC, incluido en el Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, según lo requerido por la SFC.

De acuerdo con lo anterior, para la clasificación de los RERO, el auditor verificó las categorías de acuerdo con el marco normativo de la SFC vigente durante el periodo auditado, observando el siguiente comportamiento por cada clasificación de riesgo:

CLASIFICACIÓN	IV TRIMESTRE 2024	I TRIMESTRE 2025	II TRIMESTRE 2025	III TRIMESTRE 2025	IV TRIMESTRE 2025
Infraestructura	0	0	2	0	0
Recurso Humano	5	7	5	5	0
fallas tecnológicas	2	3	6	3	0
ejecución y administración de procesos	8	4	4	1	1
eventos externos	1	6	3	4	1
TOTAL	16	20	20	13	2
Eventos que Afectaron Estado de Resultados Integral (ERI CPVMP)	1	0	0	2	2
Monto afectación ERI CPVMP	\$ 236,984,542.00	\$ -	\$ -	\$ 111,780,943.00	\$ 31,323,500.00

Figura 1. REROS periodo auditado. Fuente: elaboración propia OFCIN, cifras tomadas Informes Comité de Riesgos, requerimiento de información OAGRI del 01-10-2025.

En el siguiente anexo como papel de trabajo, el auditor realizó seguimiento a los RERO registrados en el periodo auditado por proceso, clasificación y seguimiento de los eventos y de aquellos que afectaron el Estado de Resultados Integral de la CPVMP:



Reporte eventos
oct 2024 a sep 2025.

Anexo 1: Seguimiento OFCIN RERO periodo auditado
Fuente: Elaboración propia OFCIN 11-12-2025

Para la verificación en referencia, la OFCIN cuenta con el perfil auditor del Sistema de Información de VIGIA RIESGOS; el cual cuenta con la Bondad de poder verificarlo indicado en Manual SIAR código GR-MA-010, versión 007 del 27-11-2025, numeral 6.8.1, para la revisión de la debida clasificación de los RERO y la verificación de la documentación pertinente.

De acuerdo con lo anterior, para la revisión de la debida clasificación de los RERO, la OFCIN realizó la verificación en Vigía Riesgos aplicando la práctica 2320 – 3 “Muestreo para Auditoría, emitido por el Instituto Internacional de Auditores Internos (TheIIA Global)”,

realizó una muestra correspondiente al 10% del total de RERO registrados por trimestre, con el siguiente análisis:

a) IV trimestre de 2024:

Figura 2. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Figura 3. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Se observa, debida clasificación requerida en el marco normativo de la SFC Capítulo XXXI de la CBCF CE 100 de 1995, Parte III, numeral 4.2.2.2.4; durante la prueba de recorrido con OAGRI fueron evidenciados los soportes y cargados, cumpliendo con lo

requerido en la Guía Aprobación de REROS en el Sistema de Información con código GR-GU-037, versión 005 del 31-10-2025, numeral 5.9.

b) I trimestre de 2025:

Figura 4. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Figura 5. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Se observa, debida clasificación requerida en el marco normativo de la SFC Capítulo XXXI de la CBCF CE 100 de 1995, Parte III, numeral 4.2.2.2.4; durante la prueba de recorrido con OAGRI fueron evidenciados los soportes y cargados, cumpliendo con lo requerido en la Guía Aprobación de REROS en el Sistema de Información con código GR-GU-037, versión 005 del 31-10-2025, numeral 5.9.

c) II trimestre de 2025:

Figura 6. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Figura 7. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Se observa, debida clasificación requerida en el marco normativo de la SFC Capítulo XXXI de la CBCF CE 100 de 1995, Parte III, numeral 4.2.2.2.4; durante la prueba de recorrido con OAGRI fueron evidenciados los soportes y cargados, cumpliendo con lo requerido en la Guía Aprobación de REROS en el Sistema de Información con código GR-GU-037, versión 005 del 31-10-2025, numeral 5.9.

d) III trimestre de 2025:

Figura 8. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Figura 9. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Se observa, debida clasificación requerida en el marco normativo de la SFC Capítulo XXXI de la CBCF CE 100 de 1995, Parte III, numeral 4.2.2.2.4; durante la prueba de recorrido con OAGRI fueron evidenciados los soportes y cargados, cumpliendo con lo requerido en la Guía Aprobación de REROS en el Sistema de Información con código GR-GU-037, versión 005 del 31-10-2025, numeral 5.9.

e) IV trimestre de 2025:

Figura 10. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Figura 11. Análisis grado de detalle VIGIA RIESGOS. Fuente: consulta perfil OAGRI, prueba de recorrido 21-11-2024.

Se observa, debida clasificación requerida en el marco normativo de la SFC Capítulo XXXI de la CBCF CE 100 de 1995, Parte III, numeral 4.2.2.2.4; durante la prueba de recorrido con OAGRI fueron evidenciados los soportes y cargados, cumpliendo con lo requerido en la Guía Aprobación de REROS en el Sistema de Información con código GR-GU-037, versión 005 del 31-10-2025, numeral 5.9.

De acuerdo con lo expuesto, la OFCIN realizó el seguimiento de los RERO del periodo auditado, analizando la muestra descrita, evidenciando la apropiada identificación,

recolección y tratamiento de los registros por parte de la OAGRI, cumpliendo con los requisitos de la SFC en el marco normativo.

Posteriormente la OFCIN realiza la validación de los REROS en el aplicativo Vigía Riesgos, en la lista de Riesgo Materializado de un periodo determinado en consulta, como se muestra a continuación, así:



Figura 12. Análisis REROS - VIGIA RIESGOS

Al darle clic en exportar a Excel, no deja descargar la información de esta manera, generando el siguiente error.



Figura 13. error en exportación REROS - VIGIA RIESGOS


Por lo anterior la OFCIN, realiza la siguiente:

Oportunidad de Mejora Correctiva 01:

La OFCIN recomienda a la OAGRI, Solicitar al proveedor del software la implementación de la funcionalidad exportación directa de los REROS en formato Excel para el perfil Auditor, lo anterior a que el software utilizado para la administración de riesgos no permite la exportación automática de los Reportes de Eventos de Riesgo Operacional (REROS) en formato Excel. Actualmente, Esta situación dificulta la obtención de evidencia confiable, compromete la trazabilidad de los datos y aumenta el esfuerzo requerido para validar la integridad de la información. Además, genera retrasos en la

revisión y análisis, lo que puede impedir el cumplimiento de los plazos establecidos por la normativa y reducir la efectividad del proceso de auditoría; lo anterior a que la CE. 018 de la SFC DEL 2021: exige mantener registros actualizados y trazables de los eventos de riesgo operacional, lo que implica contar con herramientas tecnológicas que faciliten la gestión y reporte, en prevención de los “R028 Fallas en el Reporte y Documentación de Riesgos” y “RSI050 No Disponibilidad de Herramientas”, así como lo reglamentado en la Dimensión 4 Evaluación de Resultados, establecida en Manual Operativo del MIPG, versión 6 de diciembre de 2024.

La OAGRI, ha adoptado un enfoque preventivo mediante el uso de herramientas de análisis y verificación. Este procedimiento permite asegurar que los procesos internos no incurran en omisiones relacionadas con el reporte de eventos de riesgo operacional (REROS), como se muestra a continuación.



The screenshot shows the 'CajaHONOR' web interface. On the left, there is a sidebar with 'Mis solicitudes' (My requests) and a list of requests including 'VALIDACION EQUIPO PCN' and 'Solicitud de permiso para instalar la consola de Service Manager' (SR632964). The main content area displays the details for SR632964, which is 'Cerrada' (Closed). It shows the description 'Solicitud de permiso para instalar la consola de Service Manager' and a list of actions: 'Registro asignado' and 'There was a status change for Service Request', both dated '4 días atrás' (4 days ago).

Figura 14. prueba de recorrido OAGRI, solicitud Service Manager

Figura 15. Prueba de recorrido OAGRI, solicitud Service Manager solicitud reporte PQR de Excel

Estos controles adicionales fortalecerán la gestión integral del Riesgo, reduciendo la probabilidad de incumplimientos regulatorios y contribuye a la transparencia y confiabilidad de la información reportada, generando mayor confianza en la administración del riesgo dentro de la entidad.

1.3. Cumplimiento marco normativo VERRO y Relación de Solvencia

En la verificación de la OFCIN, durante el periodo auditado, se revisó el cumplimiento de lo sustituida por el Capítulo XXXI CE. 018 de 2021 SIAR en su capítulo Anexo 13; lo requerido en la CE 020 de 2019 “Instrucciones relacionadas con el Margen de Solvencia y otros Requerimientos de Patrimonio de los Establecimientos de Crédito”, la transmisión del Formato 239 (Proforma F.1000-141 “Reporte de Información de Margen de Solvencia y Otros Requerimientos de Patrimonio y Declaración del Control de Ley Margen de Solvencia”).

Siendo así, en el requerimiento de información, se verificó con OAGRI, el VERRO obtenido para el periodo auditado, las fuentes para la construcción del Formato 239, observando por el auditor, el siguiente comportamiento de las cuentas principales del Margen de Solvencia, junto con el reporte de transmisión a la SFC con “Validación de Información Correcta” para todo el periodo auditado:

VERIFICACIÓN FORMATO 239 - OFCIN

DECLARACIÓN DEL CONTROL DE LEY RELACIÓN DE LAS RELACIONES DE SOLVENCIA Y OTROS REQUERIMIENTOS DE PATRIMONIO

SUBCUENTA	CONCEPTO	VALOR PONDERADO										VERIFICACIÓN RESULTADO TRANSMISIÓN
		31/01/2025	28/02/2025	30/03/2025	30/04/2025	30/05/2025	30/06/2025	30/07/2025	30/08/2025			
020	Patrimonio Técnico	263.955.431,079.92	246.313.799.747.62	280.959.852.637.96	282.244.565.508.68	283.916.921.152.30	283.969.321.330.60	283.968.930.665.16	286.291.767.012.17			
30	Total Riesgo de Mercado	598,823,768.56	832,162,175.00	22,883,307,958.44	1,031,476,502.00	1,756,803,592.78	1,736,344,287.44	854,976,711.89	874,495,828.67			
040	Relación de Apalancamiento	3.07	2.84	3.21	3.19	3.19	3.17	3.11	3.1			
045	Relación de Solvencia Básica	12.91	12.02	13.45	13.75	13.81	13.81	13.84	13.97			
060	Relación de Solvencia Total	12.98	12.1	13.53	13.83	13.89	13.9	13.93	14.06			
	VERIFICACIÓN RESULTADO TRANSMISIÓN	Correcta	Por debajo de lo requerido	Correcta	Correcta	Correcta	Correcta	Correcta	Correcta			

Figura 16. Verificación OFCIN Formato 239, Riesgo Operacional, Relación de Apalancamiento y Relación de Solvencia Total – periodo auditado. Fuente: elaboración propia OFCIN, cifras tomadas requerimiento de información OAGRI del 02-10-2024.

Como fue evidenciado en la figura anterior, se observa que, para el periodo auditado, la relación de apalancamiento continua por debajo del 3 % que es lo requerido por la SFC en el numeral 2.1 “Relaciones mínimas de solvencia”, del Capítulo XIII-16 -Margen de Solvencia y otros requerimientos de patrimonio (CE 100 de 1995) de la SFC, asimismo la Relación de Solvencia Total se evidencia mayor al 9% de lo requerido en el mismo numeral.

La Entidad ha demostrado un desempeño sólido y consistente posterior a la relación de apalancamiento del mes de febrero de 2025, manteniendo niveles estables o superiores al 3%, en línea con lo indicado por la Superintendencia Financiera de Colombia (SFC). Este resultado refleja la adecuada gestión financiera y el compromiso con las recomendaciones emitidas por la Auditoría Interna, como lo es en la Recomendación 01 del informe 06 – 2025 y la Revisoría Fiscal, fortaleciendo la confianza en la solidez y sostenibilidad de la organización.

Al 30-09-2024, el auditor no observa respuestas y/o requerimientos adicionales de la SFC de lo expuesto. Siendo así, de acuerdo con lo evidenciado con las fuentes y el cálculo del VERRO, con los cálculos respectivos del Formato 239 (Proforma F.1000-141 “Reporte de Información de Margen de Solvencia y Otros Requerimientos de Patrimonio y Declaración del Control de Ley Margen de Solvencia) con los soportes de transmisiones correctos a la SFC, no se generan observaciones por parte de la OFCIN y se continuará con la revisión de su cumplimiento en las próximas auditorías a realizar.

Por su parte, el auditor en entrevista con la OAGRI del 05-12-2025, verificó el cumplimiento de lo requerido por la SFC para el cálculo del “Componente de Pérdida (CP)”, en el numeral 1.3.1.1 y numeral 1.3.1.2 del Anexo 13:

1.3.1.1. Las entidades solo podrán considerar las pérdidas operacionales históricas consignadas en su registro de eventos de pérdida de 10 años, siempre que los mismos cumplan la totalidad de los criterios generales y específicos para el “Registro de eventos de riesgo operacional de alta calidad” a que se refieren el subnumeral 4.2.2. de la Parte III del presente Capítulo y cuenten con la autorización previa de la SFC.

1.3.1.2. La entidad que demuestre ante la SFC que cuenta con un “Registro de eventos de riesgo operacional de alta calidad” que cumple con la totalidad de los criterios generales y específicos a que se refieren el subnumeral 4.2.2. de la Parte III del presente Capítulo, pero no cuenta con los registros de eventos de riesgo operacional de los últimos 10 años, podrá hacer uso de una base de 5 años para calcular el Componente de Pérdida (CP) para el cálculo del Indicador de Pérdida Interna (IPI), siempre que cuente con la autorización previa de la SFC.

Figura 17. Fuente: Capítulo XXXI CE 100 de 1995, Anexo 13 “Metodología Estándar para determinar el Valor de la Exposición al Riesgo Operacional de los Establecimientos De Crédito” – VERRO.

1.4. Documentación requerida Gestión Riesgo Operacional – RO

La revisión de la documentación controlada de la Gestión del Riesgo Operacional – RO es realizada por el equipo auditor de acuerdo con lo requerido por la SFC en el Capítulo XXXI (CE 018 de 2021) SIAR, parte I numeral 5, literal c), con las siguientes observaciones:

Tabla 2. Revisión OFCIN en Suite Visión – Documentación Controlada

#	Documento	Identificación Isolucion	Comentarios OFCIN
1	Manual SIAR	Código GR -MA-010, versión 007 del 27-11-2025.	- N/A
2	Guía Reporte General de Eventos de Riesgo	Código GR-GU-029, versión 010 del 31-10-2025.	- N/A
3	Guía Aprobación de REROS	Código GR-GU-037, versión 005 del 31-10-2025.	- N/A
4	Procedimiento Etapas Gestión de Riesgo Operacional	Código: GR-PR-002, versión: 009, del 31-10-2025.	- N/A
5	Procedimiento Reporte y Registro de Eventos de Riesgo Operacional	Código GR-PR-019, versión 009 del 31-10-2025.	- N/A
6	Procedimiento Grupo de Expertos	Código GR -PR-029 versión 005 del 31-10-2025.	- N/A

Fuente: elaboración propia OFCIN, revisión documentación Suite Visión, fecha de consulta 10-12-2025.

De acuerdo con lo anteriormente expuesto, la OFCIN no tiene ningún comentario.

1.5. Revisión aspectos adicionales para la Evaluación de la Gestión del Riesgo Operacional.

La revisión de las etapas y elementos de la Gestión del Riesgo Operacional se realiza por la OFCIN, de acuerdo con lo estipulado por la SFC en el Capítulo XXXI de la CE 100 de 1995 CE. 018 del 2021 SIAR, Parte I, numeral 3.5; revisando los siguientes:

1.5.1. Cumplimiento del marco normativo en materia de órdenes de embargo: se encuentra descrito en la parte II numeral 4.5 (Capítulo XXXI de la CE. 018 de 2021; según los mecanismos requeridos por la SFC con ocasión al Riesgo Legal generado en materia de órdenes de embargo, el auditor observa:

- Se encuentra documentado en el Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, numeral 6.6, la descripción de las herramientas tecnológicas y los sistemas de información necesarios para que los funcionarios reciban, procesen, acaten, atiendan y den respuesta a los mandatos judiciales y administrativos de forma completa, oportuna y conforme al procedimiento establecido en la ley, asimismo describiendo las Tablas de Retención Documental con las que cuenta la CPVMP.

- Para lo pertinente de la condición de inembargabilidad, el auditor observa en el Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, numeral 6.6.2, lo estipulado para los aportes de los Afiliados en la CPVMP y los excedentes registrados en la cuenta individual de los afiliados con condición de inembargables, salvo que se trate de embargo por pensiones alimenticias, de conformidad con las disposiciones legales vigentes sobre la materia.

- En el Manual SIAR descrito, numeral 6.6.3, la OFCIN evidencia las disposiciones para la capacitación permanentemente al recurso humano responsable de la atención de las Órdenes de Embargo y en el numeral 6.6.4 las acciones de la CVPMP, para garantizar los límites de inembargabilidad.

1.5.2. Matrices Riesgo Operacional y Actas Grupos de Expertos: en cumplimiento de lo requerido en el Manual SIAR, código GR-MA-010, versión 007 del 27-11-2025, numeral 6.3.2 y 6.3.3, el auditor evidenció las Actas de reuniones de Grupo de Expertos organizadas por OAGRI con los Líderes de Procesos, durante el periodo auditado.

Con relación a las Matrices de Riesgo de los procesos se evidencio el envío de 11 matrices de 18 procesos de la Entidad como se muestra a continuación, así:

Nombre	Modificado
Matriz RO Adm Ctas 20251.xlsx	El miércoles a las 1...
Matriz RO Credito 20251 V2 jun.xlsx	El miércoles a las 1...
Matriz RO Gest Estrategica 20251.xlsx	Ayer a las 16:50
Matriz RO Gest Financiera 2025.xlsx	Ayer a las 17:03
Matriz RO Gest Inform 20251.xlsx	Ayer a las 17:02
Matriz RO Gest SAC 20251.xlsx	Ayer a las 17:01
Matriz RO Gest Tal Hum 2025 v2.xlsx	Ayer a las 17:00
Matriz RO Gest Tesoreria 20251.xlsx	Ayer a las 16:56
Matriz RO Gest Tramite 20251.xlsx	Ayer a las 16:59
Matriz RO Riesgos 20251.xlsx	El miércoles a las 1...
Matriz RO Serv Administr. 20251.xlsx	Ayer a las 16:58

Figura 18. Matriz de Riesgos Procesos Caja Honor

Por lo anterior la OFCIN, realiza la siguiente:

Oportunidad de Mejora Correctiva 02:

La OFCIN recomienda a la OAGRI la actualización de las matrices de Riesgos, lo anterior a que se evidenció la no entrega completa de las matrices de Riesgo correspondientes a todos los procesos de la Entidad, lo que limita la identificación, evaluación y monitoreo integral de los riesgos institucionales, lo cual representa un incumplimiento frente a lo dispuesto en la Circular Externa 018 de 2021 de la Superintendencia Financiera de Colombia, que exige la implementación de un Sistema de Administración del Riesgo Operacional (SIAR) con procesos estructurados de identificación, medición, control y monitoreo del riesgo. Esta situación afecta la trazabilidad y la gestión integral del riesgo, por lo que se recomienda establecer mecanismos de control y seguimiento que garanticen la entrega completa y oportuna de dichas matrices. Lo anterior en prevención de los “R028 Fallas en el Reporte y Documentación de Riesgos” y “RSI050 No Disponibilidad de Herramientas”, así como lo reglamentado en la Dimensión 4 Evaluación de Resultados, establecida en Manual Operativo del MIPG, versión 6 de diciembre de 2024.

1.5.3. Capacitación: se revisó el desarrollo del Plan de Capacitación realizado al personal de Caja Honor por parte de la OAGRI, para el II semestre de 2024 y I semestre de 2025, en cumplimiento de lo requerido por la SFC en la parte I numeral 4.4 de la CE. 018 de la SFC del 2021 SIAR, evidenciando por el auditor la programación realizada, los resultados tabulados con las respuestas del personal evaluado, con el fin de determinar la eficacia de dichos programas; sin generar observaciones por el auditor.

7. Riesgo Fraude (NÚM. 4.4.2.4 PI, TI, CAP. IV SI CE 008 DE 2023 SFC/ Riesgos Fiscales

La gestión del riesgo de fraude en las entidades financieras constituye un pilar fundamental para garantizar la transparencia, la confianza del público y la estabilidad del sistema financiero. En atención a lo dispuesto en la **Circular Externa 008 de 2023** de la **Superintendencia Financiera de Colombia**, particularmente en el numeral **4.4.2.4 del Capítulo IV del Sistema Integral de Control Interno (SI)**, se establece la obligación de implementar políticas, procedimientos y controles orientados a prevenir, detectar y mitigar los riesgos asociados al fraude, tanto interno como externo.

El fraude financiero, entendido como cualquier acción deliberada para obtener un beneficio indebido mediante engaño, manipulación o abuso de confianza, representa una amenaza significativa para la integridad de las operaciones, la protección de los activos y la credibilidad institucional. Por ello, la normativa exige que las entidades adopten un enfoque integral que abarque:

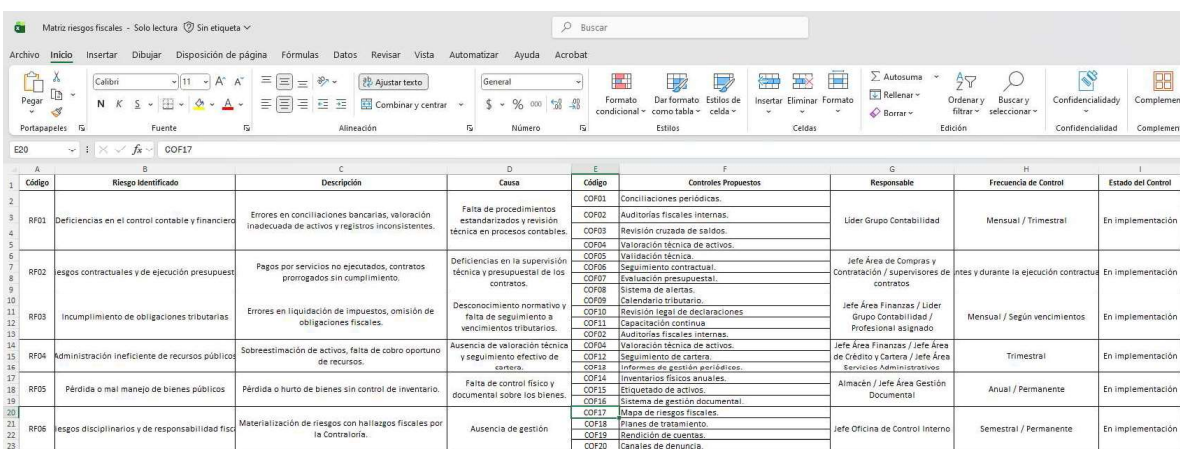
- **Identificación y evaluación del riesgo de fraude**, considerando factores internos (procesos, personal, tecnología) y externos (clientes, proveedores, entorno económico).

- **Diseño e implementación de controles preventivos y detectivos**, alineados con los principios del Sistema de Control Interno.
- **Monitoreo y reporte oportuno**, que permita una respuesta eficaz ante eventos o intentos de fraude.
- **Cultura organizacional basada en la ética y la transparencia**, promoviendo la participación activa de todos los niveles jerárquicos.

La gestión del riesgo de fraude reviste una importancia estratégica para las entidades financieras, ya que garantiza la protección de los recursos, la continuidad del negocio y la confianza de los grupos de interés. Prevenir y mitigar el fraude no solo responde a un mandato normativo, sino que constituye un elemento esencial para preservar la integridad del sistema financiero, reducir pérdidas económicas y salvaguardar la reputación institucional. Integrar la prevención del fraude en la estrategia corporativa fortalece la cultura organizacional basada en la ética y la transparencia, y asegura que los procesos internos y externos se desarrollen bajo estándares de control y supervisión que minimicen vulnerabilidades y riesgos.

Por lo anterior desde la OFCIN, se realiza la verificación de las acciones tomadas por parte del proceso de OAGRI, con relación al informe 24 del 2024, donde en prueba de recorrido presencial el día 05/12/2025, se indico *“El avance de plan de trabajo del informe 24 de 2024 sobre riesgos fiscales, tenemos los riesgos identificados para proponer a los líderes que los tendrán a cargo, para lo cual, se desarrollarán mesas de trabajo.”*

Tomando como evidencia los riesgos, así:



A	B	C	D	E	F	G	H	I
Código	Riesgo Identificado	Descripción	Causa	Código	Controles Propuestos	Responsable	Frecuencia de Control	Estado del Control
RF01	Deficiencias en el control contable y financiero	Error en conciliaciones bancarias, valoración inadecuada de activos y registros inconsistentes.	Falta de procedimientos estandarizados y revisión técnica en procesos contables.	COF01 COF02 COF03 COF04 COF05	Conciliaciones periódicas. Auditorías fiscales internas. Revisión cruzada de saldos. Valoración técnica de activos. Validación técnica.	Líder Grupo Contabilidad	Mensual / Trimestral	En implementación
RF02	riesgos contractuales y de ejecución presupuest	Pagos por servicios no ejecutados, contratos prorrogados sin cumplimiento.	Deficiencias en la supervisión técnica y presupuestal de los contratos.	COF06 COF07 COF08 COF09	Seguimiento contractual. Evaluación presupuestal. Sistema de alertas. Calendario tributario.	Jefe Área de Compras y Contratación / supervisores de contratos	antes y durante la ejecución contractual	En implementación
RF03	Incumplimiento de obligaciones tributarias	Error en liquidación de impuestos, omisión de obligaciones fiscales.	Desconocimiento normativo y vencimientos tributarios.	COF10 COF11 COF12	Revisión legal de declaraciones. Capacitación continua.	Jefe Área Finanzas / Líder Grupo Contabilidad / Profesional asignado	Mensual / Según vencimientos	En implementación
RF04	Administración ineficiente de recursos públicos	Sobreestimación de activos, falta de cobro oportuno de recursos.	Ausencia de valoración técnica y seguimiento efectivo de cartera.	COF13 COF14 COF15 COF16 COF17	Seguimiento de cartera. Informes de gestión periódicos. Inventarios fiscales anuales. Etiquetado de activos. Sistema de gestión documental.	Jefe Área Finanzas / Jefe Área de Crédito y Cartera / Jefe Área de Servicios Administrativos	Trimestral	En implementación
RF05	Pérdida o mal manejo de bienes públicos	Pérdida o hurto de bienes sin control de inventario.	Falta de control físico y documental sobre los bienes.	COF18 COF19 COF20	Mapa de riesgos fiscales. Planes de tratamiento. Rendición de cuentas. Canales de denuncia.	Almacén / Jefe Área Gestión Documental Jefe Oficina de Control Interno	Anual / Permanente	En implementación
RF06	riesgos disciplinarios y de responsabilidad fiscal	Materialización de riesgos con hallazgos fiscales por la Contraloría.	Ausencia de gestión				Semestral / Permanente	En implementación

Figura 19. Matriz Riesgos Fiscales que se llevarán a aprobación con los procesos por parte de la OAGRI, tomado de la prueba de recorrido.

Ejemplo matriz - Solo lectura Sin etiqueta

Archivo Inicio Insertar Dibujar Disposición de página Fórmulas Datos Revisar Vista Automatizar Ayuda Acrobat

Calibri 12 A⁺ A⁻ Ajustar texto General

Portapapeles Fuente Alineación Número Estilos Formato condicional Dar formato como tabla Estilos de celda Insertar Eliminar Formato Celdas Autosuma Rellenar Borrar

J15 =+F15*H15

Fuente	Riesgo Inherente	Código	Control	Zona de Riesgo Residual			Dependencia	Responsable del control	Recomendación
				Probabilidad	Impacto	Riesgo Residual			
4	BAJA	COF01	Conciliaciones periódicas.	1	4	4	Área Financiera	Líder Grupo Contabilidad	Implementar manuales contables y capacitaciones periódicas.
		COF02	Auditorías fiscales internas.	2	2	4	Oficina de Control Interno	Jefe Oficina Control Interno	
		COF03	Revisión cruzada de saldos.	4	2	8	Área Tesorería	Líder Grupo Pagaduría	
		COF04	Valoración técnica de activos.	1	2	2	Área Operaciones	Professional Back Office	
1	BAJA	COF05	Validación técnica.	3	1	3	Área de Compras y Contratación	Profesional asignado	Fortalecer la supervisión contractual con herramientas de seguimiento.
		COF06	Seguimiento contractual.	2	2	4	Área de Compras y Contratación	Profesional asignado	
		COF07	Evaluación presupuestal.	3	3	9	Área Financiera	Líder Grupo Presupuesto	
		COF08	Sistema de alertas.	2	3	6	Área Financiera	Líder Grupo Presupuesto	
4	#VALOR!	COF09	Calendario tributario.	3	3	9	Área Financiera	Líder Grupo Contabilidad	Establecer un sistema automatizado de alertas tributarias.
		COF10	Revisión legal de declaraciones.	2	2	4	Área Financiera	Líder Grupo Contabilidad	
		COF11	Capacitación continua.	3	3	9	Área Financiera	Líder Grupo Contabilidad	
		COF12	Auditorías fiscales internas.	3	2	6	Oficina de Control Interno	Jefe Oficina Control Interno	
3	#VALOR!	COF13	Seguimiento de cartera.	2	2	4	Área Crédito y Cartera	Líder Grupo Administración de Cartera	Realizar auditorías técnicas y seguimiento mensual de cartera.
		COF14	Inventarios físicos periódicos.	3	2	6	Área Crédito y Cartera	Jefe Área Crédito y Cartera	
3	#VALOR!	COF15	Inventarios físicos anuales.	2	2	4	Área Servicios Administrativos	Almacenista	Actualizar inventarios y digitalizar el control de activos.
		COF16	Etiquetado de activos.	2	2	4	Área Servicios Administrativos	Almacenista	
1	#VALOR!	COF17	Sistema de gestión documental.	1	2	2	Área Gestión Documental	Jefe Área Gestión Documental	Difundir el mapa de riesgos y promover la cultura de control fiscal.
		COF18	Mapa de riesgos fiscales.	2	1	2	Oficina Asesora de Gestión del Riesgo	Profesional asignado	
		COF19	Planes de tratamiento.	2	1	2	Oficina Asesora de Gestión del Riesgo	Profesional asignado	
		COF20	Rendición de cuentas.	3	1	3	Oficina Asesora de Planeación	Profesional asignado	
		COF20	Canales de denuncia.	2	2	4	Unidad de Control Disciplinario	Líder Unidad de Control Disciplinario	

Figura 20. Ejemplo Matriz Riesgos Fiscales que se llevarán a aprobación con los procesos por parte de la OAGRI, tomado de la prueba de recorrido.

Por lo anterior la OFCIN, realiza la siguiente:

Recomendación 01:

La OFCIN recomienda a la OAGRI implementar de manera integral las acciones definidas en el Plan de Mejoramiento derivado de la auditoría 24 del año 2024, que tiene como fecha de implementación el día 30/01/2026, lo anterior en atención a aprobación de los Riesgos de Fraude por la Junta Directiva en sesión de 29-04-2024 según Acta 5, y remitido a la OAGRI, mediante comunicado interno GERGE-359-01-2024070900078.

8. Componente Plan de Continuidad del Negocio – PCN

A través del repositorio de información implementado en SharePoint, con fecha 15 de octubre de 2025, la Oficina Asesora de Gestión del Riesgo Institucional – OAGRI dispuso la siguiente documentación relevante para el desarrollo de la auditoría:

DocumentosOAGRI > GRC > 2025 > Informes > Control

Nombre	Modificado
Punto #1 PAC	Hace 5 días
Punto #1 PCN	Hace 5 días
Punto #10 PAC	Hace 5 días
Punto #11 PCN	Hace 5 días
Punto #12 PCN	Hace 5 días
Punto #16 PCN	Hace 5 días
Punto #2 DRP	Hace 3 días
Punto #2 PAC	Hace 5 días
Punto #2 PCN	Hace 5 días
Punto #3 PCN	Hace 5 días
Punto #4 PAC	Hace 5 días
Punto #5 PCN	Hace 5 días
Punto #6 PAC	Hace 5 días
Punto #7 PCN	Hace 5 días
Punto #8 PAC	Hace 5 días
Punto #8 PCN	Hace 5 días
Punto #9 PCN	Hace 5 días
Documento Guía para acceso a carpetas.d...	Hace 3 días
Requerimiento de Información PCN PAC Y ...	Hace 4 días

Figura 21. Información suministrada por OAGRI – proceso de Auditoría
Fuente: OAGRI – SharePoint, link: 10 Octubre

Verificación de la información suministrada por la OAGRI:

1. Punto #1 PCN.

Relación de Riesgos que pueden afectar las operaciones del Negocio incluyendo: identificación de amenazas y vulnerabilidades, Valoración del riesgo, Controles existentes y evaluación de su efectividad, Documentación del análisis de riesgos y su relación con el BIA.

Respuesta: Se adjunta el documento Manual de gestión del PCN, dentro del cual se encuentra desarrollado en el capítulo de Gestión de Riesgos de Continuidad, la relación de los riesgos que pueden afectar las operaciones del Negocio, este capítulo toma como documento base para su elaboración, la matriz de continuidad, ambos documentos adjuntos en la carpeta Punto #1 PCN.

El proceso auditado suministró los siguientes archivos:



Figura 22. Archivos Req. Item 1 – Riesgos que afectan operaciones del Negocio
Fuente: OAGRI – SharePoint – link: [Punto #1 PCN](#)

- **Archivo Matriz_Riesgos_Continuidad_Completa.xlsx**

Contiene las pestañas RO Continuidad, Calificaciones, Controles Recomendados, OAGRI, OAINF, OAJUR, OAPLA, OFCIN, Vivienda y Mercadeo, Comunicaciones, Tramite, SAC, AOPER, Tesorería, Crédito y Cartera, Finanzas, Talento Humano, Gestión Documental, Servicios Administrativos y Control Disciplinario.

A continuación, se presenta una gráfica con los 17 procesos y la distribución completa de riesgos, ilustrados por colores para priorización de estos: **Rojo = Riesgos ALTO**, **Naranja = Riesgos MODERADO** y **Verde = Riesgos BAJO**:

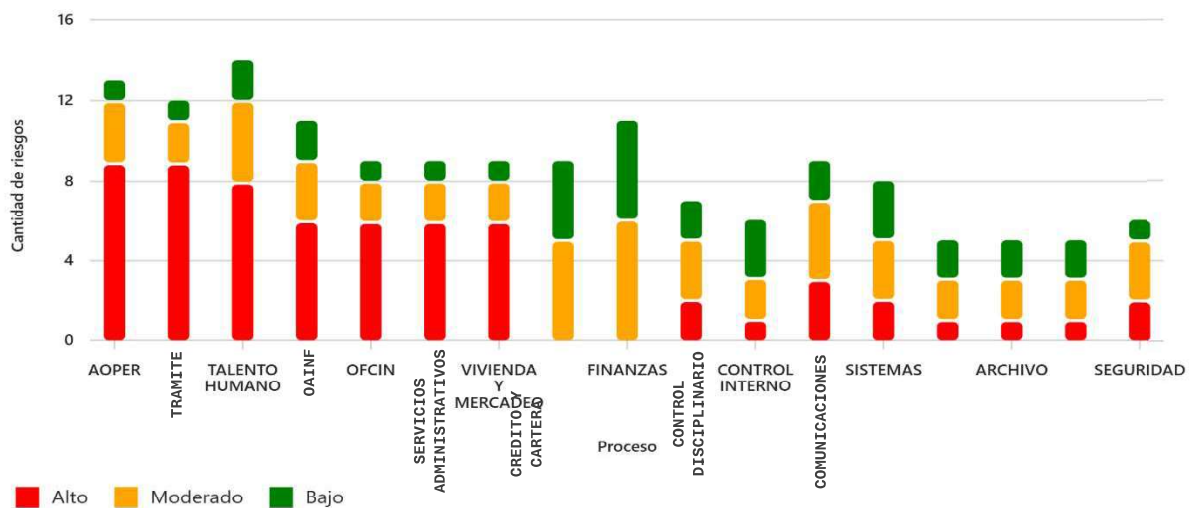


Figura 23. Distribución de Riesgos procesos Caja Honor
Fuente: OAGRI – Archivo Matriz_Riesgos_Continuidad_Completa.xlsx

De la gráfica anterior, se tienen las siguientes precisiones:

- AOPER y TRÁMITE son áreas críticas ya que presentan 9 riesgos altos cada uno.
- TALENTO HUMANO (8) Altos y OAINF, OFCIN, SERVICIOS ADMINISTRATIVOS, VIVIENDA Y MERCADEO (6 riesgos Altos cada uno), considerándose igualmente áreas críticas.
- CREDITO Y CARTERA y FINANZAS tienen predominancia de riesgos MODERADOS y BAJOS, lo que indica menor exposición crítica

En consecuencia, las áreas consideradas como críticas por presentar Riesgos Altos, requieren atención prioritaria en planes de continuidad y mejora de controles.

Por otra parte, en relación con el archivo **Matriz_Riesgos_Continuidad_Completa.xlsx**, una vez revisado su contenido, la OFCIN manifiesta inquietudes respecto a su carácter oficial y controlado, considerando necesario verificar la existencia de firmas de los responsables que respalden su autenticidad y validación formal. Adicionalmente, se observa que en dicha matriz no se encuentra incluido el **riesgo R074**, el cual sí está identificado como riesgo principal en el documento **GR-NA-MA-008 MANUAL PCN V7.docx**. Los temas antes citados, son importantes para garantizar la alineación entre dichos instrumentos de gestión de riesgos.

Ante la citada inquietud, el profesional universitario 01 encargado de la Gestión del Plan de Continuidad del Negocio – PCN en la Entidad, indica que el documento **Matriz_Riesgos_Continuidad_Completa.xlsx**, no es controlado y se adjuntó como apoyo o complemento de la información requerida por la OFCIN en el presente ítem.

- **Archivo GR-NA-MA-008 MANUAL PCN V7.docx**

Al consultar dicho documento se observa que corresponde a la versión 007 del 26-09-2025 compuesto por 31 páginas en donde en el numeral 4.6.2. Principales Riesgos de continuidad Identificados registra se indica que a través de la plataforma VIGIA, se identifican y clasifican sistemáticamente los riesgos de continuidad según su impacto, probabilidad y relación con procesos críticos, lo que permite trazar eventos, activar protocolos y fortalecer la capacidad institucional de respuesta. Estos riesgos, organizados por naturaleza y frecuencia, orientan estrategias de mitigación y controles que refuerzan la resiliencia y aseguran la continuidad operativa ante situaciones adversas.

Una vez la OFCIN analizó dicha información, se ha identificado una inconsistencia entre la matriz de riesgos, donde algunos se registran como 'RO', y la plataforma VIGIA RIESGO, donde aparecen como 'R'. Por lo que la OFCIN recomienda validar y unificar la nomenclatura utilizada para los riesgos, dado que dicha estandarización es clave para garantizar la coherencia en el registro, análisis y seguimiento de los riesgos institucionales.

2. En el Alcance el PCN – Identificación de procesos críticos (El PCN Incluye todas las áreas críticas de la Entidad). Favor relacionarlas.

Respuesta: Las áreas críticas se describen en el documento “Guía análisis de impacto al negocio (BIA)”, Se adjunta el documento Excel: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja “Punto #2” del Excel.

En el capítulo 3.3 del Manual de gestión del PCN, se establece que el alcance del Plan de Continuidad del Negocio (PCN) abarca todas las áreas de la Entidad, ya que promueve una cultura organizacional enfocada en la gestión del riesgo y la mejora continua. Este enfoque es fundamental para garantizar la sostenibilidad a largo plazo.

Asimismo, tras la verificación del documento MANUAL DE GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO, Código: GR-NA-MA-008, Versión 007 del 26-09-2025, en su ítem 3.3. se describe el Alcance del PCN, indicando que “la aplicación de los procedimientos y estrategias documentados en el Plan de Continuidad se extiende a todas

las oficinas, procesos y servicios de la Caja Promotora de Vivienda Militar y de Policía, garantizando la prestación del servicio ante cualquier escenario de interrupción además de contemplar lo siguiente:

- Ejecución procedimientos y estrategias documentadas en el PCN en todas las sedes de la Entidad, incluyendo la sede principal y puntos de atención regionales.
- Protección a las personas, la información y los activos tecnológicos y físicos de la Entidad.
- Implementación de una respuesta rápida y eficaz ante eventos disruptivos, minimizando el impacto sobre los procesos críticos.

Este alcance incluye la activación de planes de contingencia, recuperación ante desastres (DRP), uso del punto alerno de continuidad, gestión de crisis y la coordinación de equipos de trabajo especializados para asegurar la resiliencia institucional.”

3. Documentos del PCN: Documento oficial del Plan de Continuidad del Negocio, Política de Plan de Continuidad de Continuidad del Negocio, Planes de contingencia de los sistemas/aplicativos críticos, Procedimientos de activación, recuperación y restauración del plan, Registros de mantenimiento y actualización del PCN.

Respuesta: Se adjunta Manual de gestión del PCN (Documento Oficial PCN) en la carpeta Punto #1 PCN, en donde se enmarcan los siguientes capítulos:

- 3.4.3 Política de continuidad del negocio y recuperación ante desastres: Política del PCN.
- 4. PUESTA EN MARCHA DEL PCN: todo lo relacionado al despliegue del plan de continuidad).
- 5.1 Plan de Recuperación ante Desastres: Estrategia operativa de recuperación de sistemas.
- 6. MANTENIMIENTO Y ACTUALIZACIÓN DEL PCN: la gestión para la actualización de este.

La OFCIN procede a verificar los capítulos indicados por la OAGRI en su respuesta, extractando fundamentalmente lo que a continuación se cita de cada uno de los ítems en relación:

- ✓ Ítem 3.4.3. Política de continuidad del negocio y recuperación ante desastres, que establece principios y responsabilidades para asegurar la continuidad de operaciones críticas ante eventos disruptivos, garantizando servicios esenciales, protección de activos y recuperación oportuna. Aplica a todas las áreas, procesos críticos, infraestructura tecnológica, personal y proveedores estratégicos.
- ✓ Ítem 4. Puesta en marcha del PCN. Se activa como respuesta inmediata ante la declaración formal de una contingencia que afecta la operación normal de la Entidad. Igualmente, la OFCIN destaca el aspecto relacionado con la conformación de los diferentes comités en virtud del despliegue del PCN, tema que es fundamental para garantizar una gestión integral, coordinada y eficaz de la continuidad operativa ante situaciones de crisis o interrupciones.

Estos comités permiten distribuir responsabilidades, facilitar la toma de decisiones informadas y asegurar que cada área clave de la organización esté representada en la planificación, ejecución y seguimiento de las estrategias de continuidad. Además, fomentan la cultura de prevención y resiliencia, fortaleciendo la capacidad institucional para responder de manera oportuna y eficiente ante cualquier eventualidad que pueda afectar el normal desarrollo de las actividades misionales. Entre los cuales se citan los componentes y descripción del Comité Directivo de Continuidad, el Nombre del Equipo, los Integrantes y Funciones de los Equipos de trabajo provisionales, así como la identificación de Partes Interesadas y la justificación de inclusión en el PCN. Por otra parte, teniendo en cuenta la **Oportunidad de Mejora Correctiva 1** registrada en la vigencia 2024 en el INFORME 25 DE 2024 EVALUACIÓN A LA GESTIÓN DEL RIESGO OPERACIONAL PERIODO AUDITADO DEL 01 DE JUNIO DE 2023 AL 30 DE SEPTIEMBRE DE 2024 que cita:

“La OFCIN recomienda a la OAGRI en coordinación con la OAPLA y demás procesos interrelacionados, efectuar la actualización del MANUAL DE GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO, Código GR-NA-MA-008 del 25-04-2023, frente a aspectos tales como:

- Exista coincidencia entre los numerales registrados en la Tabla de Contenido y los registrados en el cuerpo del documento, tema esencial para garantizar precisión, coherencia y profesionalismo en la presentación del documento, facilitando la navegación por el mismo, además de dar cumplimiento normativo.
- Se revise y actualice el capítulo de Marco Legal, especialmente de la SFC como Entidad reguladora, como es el caso de las Circulares Externas 038 de 2009 y CE 008 de 2023 (que aunque la circular no menciona explícitamente los PCN, al fortalecer el SCI se promueve una gestión más robusta de los riesgos operacional y la resiliencia organizacional, lo que contribuye indirectamente a la eficacia del PCN), por tanto, es importante que Caja Honor como Entidad vigilada por la SFC, mantenga actualizado el Plan de Continuidad del Negocio, asegurando la resiliencia y continuidad de sus operaciones frente a posibles interrupciones y de esta manera dar cumplimiento a las normativas establecidas.
- Incluir otros términos y definiciones clave para garantizar la comprensión de todos los involucrados como por ejemplo: Resiliencia Operacional, Interrupción, Evento Crítico, otros.
- Actualizar el capítulo relacionado con Marco de referencia interno puesto que los documentos allí citados actualmente se encuentran en otra versión: (GR-NA-MA-009, V4 del 28/ago./2024, GR-NA-MA-003_Manual_SARO_V17 ya no existe puesto que fue integrado en el Manual del Sistema Integral de Administración de Riesgos – SIAR, Cod. GR-NA-MA-010, V2 del 27/sep./2024), además de ser importante especificar el nombre preciso, código, versión y fecha de aprobación del documento “Matriz de Riesgo General de Talento Humano”, puesto que como tal no registra en el repositorio documental ISOLUCION.
- Complementar el capítulo de Marco de Referencia Interno con los demás documentos internos relacionados con el PCN.
- Incluir capítulo referente al Mantenimiento y Actualización del PCN, en donde se describan los procedimientos para revisar y actualizar el Plan, Criterios para incorporar cambios organizativos, tecnológicos o regulatorios, además del registro de versiones del PCN, temas relevantes para garantizar su funcionalidad frente a nuevos desafíos.
- Entre otros que consideren pertinentes.

Lo anterior, toda vez que el mantener el Manual del Plan de Continuidad del Negocio – PCN debidamente actualizado es fundamental para asegurar que sea funcional y verificar que la Entidad se encuentre preparada para afrontar cualquier situación imprevista, resguardando no solo los intereses de Caja Honor sino que además refuerza la capacidad de adaptación y recuperación asegurando la continuidad de operaciones en la Entidad, dando cumplimiento entre otros a lo dispuesto por la SFC en las Circulares Externas 038 de 2009 y CE 008 de 2023, además de las buenas prácticas de la Norma ISO 22301:2019, Norma ISO 27001:2013 Gestión de Seguridad de la Información Anexo A numeral 17. Aspectos de Seguridad de la Información de la Gestión de continuidad de Negocio y su actualización 2022, con el propósito de fortalecer el autocontrol como principio rector del Sistema de Control Interno en los procesos y dar cumplimiento de las Dimensiones de MIPG V6 de diciembre 2024 dimensiones 3ª Gestión con Valores para Resultado y 5ª Información y comunicación. Se observaron los R010 – Incumplimiento de Obligaciones Legales y/o Normativas Aplicables a la Entidad, el R029 – Fallas en la Administración PCN por CA029 – Falta de Actualización y Capacitación de los Procedimientos frente a la Normatividad”.

En consecuencia y una vez revisado el documento MANUAL DE GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO, Código: GR-NA-MA-008, Versión 007 del 26-09-2025, la OFCIN observó que el proceso auditado dio cumplimiento a las recomendaciones establecidas en la Oportunidad de Mejora No. 1 del Informe de Auditoría 2024, evidenciando su atención mediante la debida documentación de los aspectos objeto de dicha oportunidad de mejora; acción que refleja el compromiso del área con la mejora continua y el fortalecimiento de sus controles internos. No obstante, la OFCIN recomienda:

Recomendación No. 2.

La OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados fortalecer los siguientes apartados dentro del documento MANUAL DE GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO – PCN:

1. Apartado de **Indicadores de Desempeño**: incorporando ejemplos concretos de KPIs como el *Tiempo Objetivo de Recuperación (RTO)*, el *porcentaje de cumplimiento de pruebas de continuidad*, y el *número de incidentes gestionados conforme al plan*.
2. Apartado **Simulacros y Pruebas**, se sugiere incluir un plan anual estructurado que detalle la frecuencia, tipo de ejercicios (activación de equipos de respuesta, recuperación de sistemas, simulacros de evacuación), y responsables, lo cual facilitará el seguimiento y mejora continua.
3. Apartado **Integración con otros Sistemas**, se valora positivamente la articulación con el SGSI y la norma ISO 27001; sin embargo, se recomienda complementar esta sección con la *alineación al marco NIST*, especialmente al *NIST SP 800-34 Rev. 1*, que establece lineamientos para la continuidad del negocio y recuperación ante desastres, asegurando que exista evidencia documental de esta integración que respalden la coherencia entre los sistemas, como matrices de correspondencia, actas de reuniones conjuntas, o procedimientos compartidos, mapeos entre los controles del PCN y el NIST Cybersecurity Framework (CSF), así como con prácticas documentadas en gestión de incidentes, análisis de impacto al negocio (BIA) y planes de recuperación, entre otros.

Todo lo anterior contribuye al cumplimiento de normativas internacionales y a la minimización de riesgos operacional (interrupciones en procesos críticos), tecnológicos

(fallos en infraestructura o ciberataques) y reputacionales (pérdida de confianza de clientes o partes interesadas), fortaleciendo la capacidad de respuesta y recuperación de la entidad ante eventos disruptivos, fortaleciendo la resiliencia institucional.

4. Documento oficial de conformación del Comité de Continuidad el Negocio (CCN) y detalle de los roles y responsabilidades. Asimismo, si en la Entidad existen conformados otros comités relacionados con el PCN favor relacionarlos y suministrar la documentación pertinente.

Respuesta: Se adjunta en la carpeta Punto #2, la resolución 604 del 2019 en donde se detalla la conformación del comité directivo de continuidad y los equipos de apoyo como parte del Plan de Continuidad del Negocio, asimismo se adjunta la resolución 396 del 2025 que modifica la anterior. En el Manual de gestión del PCN en el capítulo 4.1 y 4.2 se detallan roles y responsabilidades para la operación en contingencia.

El proceso auditado suministra los siguientes archivos:

DocumentosOAGRI > GRC > 2025 > Informes > Control Inte

Nombre	Modificado
Resolucion 396 de 2025.pdf	15 de octubre
Resolucion 604 de 2019.pdf	15 de octubre

Figura 24. Archivos suministrados por OAGRI
Fuente: OAGRI – SharePoint – link: [Punto #2 PCN](#)

La información correspondiente al Objeto e Integración del Comité Directivo de Continuidad, se observa documentada en la Resolución 604 del 09-diciembre-2019 en el Título II Capítulo I Artículos 3 y 4, como se muestra a continuación:

**TITULO II
DE LA PUESTA EN MARCHA DEL PLAN DE CONTINUIDAD DEL NEGOCIO
CAPITULO I
COMITÉ DIRECTIVO DE CONTINUIDAD**

ARTÍCULO 3. – OBJETO DEL COMITÉ DIRECTIVO DE CONTINUIDAD. El Comité Directivo de Continuidad tiene por finalidad administrar y verificar los recursos necesarios para manejar las operaciones que deba realizar la Entidad ante un eventual escenario de crisis y/o contingencia.

ARTÍCULO 4. – INTEGRACIÓN. El Comité Directivo de Continuidad lo integran los siguientes funcionarios, quienes actúan con voz y voto:

1. Gerente General, quien lo presidirá.
2. Subgerente Financiero.
3. Subgerente de Atención al Afiliado y Operaciones
4. Subgerente Administrativo.
5. Subgerente de Vivienda y Proyectos.
6. Jefe Oficina Asesora Jurídica.
7. Jefe Oficina Asesora de Informática.

Figura 25. Resolución 604 del 09-diciembre-2019 en el Título II Capítulo I, Artículos 3 y 4
Fuente: Fuente: OAGRI – SharePoint – link: [Punto #2 PCN](#)

Ahora bien, teniendo en cuenta que la Resolución 396 del 26-sept. De 2025 modifica la Resolución 604 del 09 de diciembre de 2019, así:

RESUELVE:

Artículo 1. Modifíquese el artículo 17 de la Resolución 604 de 2019, el cual quedará así:

Artículo 17. MIEMBROS DEL EQUIPO DE SOPORTE TECNOLÓGICO. El Equipo de Soporte Tecnológico estará conformado por los siguientes servidores públicos:

1. Jefe Oficina Asesora de Informática, quien lo liderará.
2. Profesionales de la Oficina Asesora de Informática que tenga a cargo la administración de infraestructura informática de la Entidad.
3. Profesional de la Oficina Asesora de Informática que tenga a cargo la administración de la red de la Entidad.
4. Profesional de la Oficina Asesora de Informática que tenga a cargo la administración de la base de datos de la Entidad.
5. Profesional de la Oficina Asesora de Informática que tenga a cargo la administración de Ciberseguridad.
6. Ingenieros expertos en DRP y PCN.
7. Los líderes Técnicos de los Sistemas de Información Críticos establecidos en la Guía de Análisis de Impacto del Negocio.

La participación de los miembros en el Equipo de Soporte Tecnológico será obligatoria e indelegable.

Artículo 2. Modifíquese el artículo 24 de la Resolución 604 de 2019, el cual quedará así:

Artículo 24. MIEMBROS DEL EQUIPO DE SOPORTE DE COMUNICACIONES PARA ESCENARIOS DE CRISIS. El Equipo de Soporte de Comunicaciones para Escenarios de Crisis estará conformado por los siguientes funcionarios:

1. Jefe del Área de Asuntos Gerenciales y Proyectos.
2. Jefe Área de Comunicaciones.
3. Jefe Área de Vivienda
4. Profesional de la Oficina Asesora Jurídica.

La participación de los miembros en el Equipo de Soporte de Comunicaciones será obligatoria e indelegable, salvo en el caso del funcionario señalado en el numeral 4 cuya participación en todo caso será obligatoria.

Artículo 3. Deróguese el artículo 7° de la Resolución 026 de 2017 y modifíquese el artículo 26 de la Resolución 604 de 2019, el cual quedará así:

Artículo 26. UBICACIÓN DEL PUNTO ALTERNO DE CONTINUIDAD - PAC. El Punto Alternativo de Continuidad realizará su ejecución de manera remota, y tiene como función principal mantener activa la operación crítica del negocio para las partes interesadas, y garantizar que se cumplan los lineamientos establecidos en el Plan de Continuidad de Negocio.

Artículo 4. Modifíquese el artículo 27 de la Resolución 604 de 2019, el cual quedará así:

Artículo 27. SERVICIO QUE PRESTARÁ EL PUNTO ALTERNO DE CONTINUIDAD - PAC. El Punto Alternativo de Continuidad (PAC), prestará los siguientes servicios:

- a. **En el momento de la contingencia:** El Punto Alternativo de Continuidad (PAC) asegurará la continuidad operativa de la Entidad en situaciones de contingencia. Para ello, se activa la estrategia del trabajo remoto donde se ejecuten los lineamientos aplicables, asegurando la continuidad de los procesos críticos descritos en el análisis de impacto de negocio de la Entidad tras las interrupciones que se presenten, estos

lineamientos se desarrollarán de acuerdo con la Guía de Punto Alternativo de Continuidad establecido en el Plan de Continuidad de Negocio de Caja Honor.

- b. **En la operación normal del negocio:** El Punto Alternativo de Continuidad — PAC, se mantendrá en la operación normal del negocio, con la disponibilidad suficiente, las condiciones tecnológicas y administrativas necesarias hasta el momento en el que los equipos designados de manera provisional del PCN validen y garanticen la operación normal, lo que ponga fin a la contingencia con el objetivo de comenzar el retorno a la Sede Principal.

Artículo 5. Modifíquese el artículo 28 de la Resolución 604 de 2019, el cual quedará así:

Artículo 28. PERSONAL QUE INTEGRARÁ EL PUNTO ALTERNO DE CONTINUIDAD PAC. El Punto Alternativo de Continuidad – PAC, estará conformado por el personal que se nombrará o contratará de acuerdo con las necesidades administrativas y operativas, conforme a lo dispuesto en el Manual del Plan de Continuidad del Negocio, los cuales seguirán las órdenes de los líderes de los procesos críticos y demás directivos en caso de que se requiera de la Caja Promotora de Vivienda Militar y de Policía.

Artículo 6. Modifíquese el artículo 29 de la Resolución 604 de 2019, el cual quedará así:

Artículo 29. RECURSOS TECNOLÓGICOS. De acuerdo con los requerimientos que establezca el Líder del Plan de Continuidad, se deberán contar con los recursos técnicos y tecnológicos requeridos para la puesta en marcha de esta actividad, las cuales constarán de equipos de cómputo y coordinaciones a nivel de logística, exclusivamente para las actividades del Punto Alterno de Continuidad-PAC. La Oficina Asesora de Informática apoyará con las características tecnológicas tales como conexión segura VPN, usuarios con los accesos y permisos requeridos para la operación. El equipo de cómputo asignado deberá contar con los controles de seguridad de la información y ciberseguridad y demás elementos que sean indispensables para el desarrollo de las actividades del Punto Alterno de Continuidad-PAC, de acuerdo con el Plan de Continuidad de Negocio.

Artículo 7. VIGENCIA Y DEROGATORIAS. La presente Resolución rige a partir de la fecha de su expedición, modifica la Resolución 604 del 09 de diciembre de 2019 y deroga el artículo 7° de la Resolución 026 del 19 de enero de 2017, y las demás disposiciones que le sean contrarias.

Figura 26.. Resolución 396 del 26-sept. De 2025 – Resuelve
Fuente: Fuente: OAGRI – SharePoint – link: [Punto #2 PCN](#)

Teniendo en cuenta que, la Resolución 396 de 2025 no menciona explícitamente la figura del Comité de Continuidad del Negocio (CCN), resulta pertinente conservarlo como instancia organizacional estratégica. Es de anotar, que, en su lugar, dicha resolución contempla al *Equipo de Soporte de Comunicaciones para Crisis*, cuya función principal se centra en la gestión del mensaje institucional y la protección de la reputación organizacional durante situaciones críticas. No obstante, tras el análisis realizado por la OFCIN, se hace especial énfasis respecto a que el CCN cumple un rol más amplio y estratégico en la gestión de la continuidad operativa, en tanto que, abarca la planificación, activación y supervisión de los planes de continuidad del negocio. A continuación, se presenta una tabla comparativa que evidencia las diferencias funcionales entre ambas estructuras:

Tabla 3. Comparativo CCN vs. Equipo de Comunicaciones para Crisis

Aspecto	Comité de Continuidad del Negocio (CCN)	Equipo de Soporte de Comunicaciones para Crisis
Propósito principal	Garantizar la continuidad operativa de la organización ante eventos disruptivos.	Gestionar la comunicación interna y externa durante una crisis para proteger la reputación.
Enfoque	Estratégico y operativo: activación de planes, toma de decisiones, recuperación de procesos críticos.	Comunicacional y táctico: elaboración de mensajes, vocería, manejo de medios y redes sociales.
Composición típica	Alta dirección, líderes de TI, operaciones, seguridad, legal, recursos humanos, continuidad del negocio.	Comunicadores institucionales, voceros oficiales, PR, redes sociales, relaciones institucionales.
Responsabilidades clave	Activar el BCP, asignar recursos, coordinar recuperación, supervisar ejecución, evaluar lecciones aprendidas.	Redactar comunicados, coordinar vocería, gestionar crisis reputacional, mantener flujo informativo.
Participación en decisiones	Alta: toma decisiones críticas para la organización.	Media: ejecuta decisiones comunicacionales según lineamientos del CCN o Comité de Crisis.
Interacción con stakeholders externos	Limitada, salvo en casos estratégicos o regulatorios.	Alta: medios de comunicación, clientes, comunidad, empleados, autoridades.
Activación en crisis	Se activa al inicio de una crisis para liderar la respuesta organizacional.	Se activa inmediatamente para gestionar la narrativa y los canales de comunicación.
Duración de participación	Desde la planificación hasta la recuperación post-crisis.	Principalmente durante la fase de crisis y comunicación inicial.

Dependencia jerárquica	Reporta a la alta dirección o CEO.	Puede depender del área de comunicaciones, relaciones públicas o directamente del Comité de Crisis.
Capacitación requerida	Gestión de riesgos, continuidad del negocio, liderazgo en crisis.	Comunicación estratégica, manejo de crisis, vocería, medios digitales.
¿Puede haber miembros en común?	Sí, especialmente en organizaciones pequeñas o integradas.	Sí, pero con roles diferenciados según la función.

Fuente: OFCIN – Diseño Propio Ayuda IA

En consecuencia, la OFCIN realiza la presente precisión:

Recomendación No. 3.

Se recomienda a la OAGRI en coordinación con la Administración y los procesos de la Entidad, mantener el Comité de Continuidad del Negocio – CCN) como una instancia organizacional estratégica, dado que cumple funciones esenciales en la planificación, activación y supervisión de los planes de continuidad operativa, así como en la articulación entre los procesos durante situaciones críticas; esta recomendación surge del análisis realizado por la OFCIN, quien evidenció que el CCN desempeña un rol más amplio que el Equipo de Soporte de Comunicaciones para Crisis contemplado en la Resolución 396 de 2025, el cual se enfoca exclusivamente en la gestión del mensaje institucional y la protección de la reputación organizacional; aunque dicha resolución modifica la Resolución 604 de 2019 y omite la mención explícita del CCN, no prohíbe su existencia, lo que permite conservarlo como buena práctica alineada con estándares internacionales; en tanto que eliminar el CCN implicaría riesgos como la desarticulación operativa, pérdida de enfoque estratégico, debilitamiento de la gobernanza en continuidad, mayor exposición a impactos negativos y cumplimiento normativo parcial, afectando la capacidad institucional de respuesta ante eventos críticos, por el contrario, mantener el CCN aporta beneficios como una mayor capacidad de respuesta coordinada, fortalecimiento de la gobernanza en crisis, mejora en la toma de decisiones estratégicas, continuidad efectiva de procesos críticos y alineación con marcos internacionales de gestión de continuidad del negocio.

5. Documento Análisis de Impacto del Negocio – BIA actualizado

Respuesta: Se adjunta el documento GR-NA-GU-028 Guía Análisis del Impacto del Negocio_V007 en la carpeta Punto #3 PCN.

Una vez la OFCIN revisó el documento GR-NA-GU-028 Guía Análisis del Impacto del Negocio_V007 del 29-09-2023, se observó que presenta oportunidades de mejora relevantes en la estructuración del Plan de Continuidad del Negocio, en tanto que, no se evidenció una evaluación detallada de los procesos y subprocesos, lo cual limita la capacidad de identificar puntos críticos de operación. Asimismo, no presenta una vinculación explícita entre los procesos operativos y los aplicativos tecnológicos que los soportan, lo cual dificulta la identificación de dependencias críticas y la planificación efectiva de estrategias de recuperación tecnológica por proceso. Los tiempos de recuperación (Objetivo de Tiempo de Recuperación – RTO, Objetivo de Punto de Recuperación – RPO, Periodo Máximo Tolerable de Disrupción – MTPD y Tiempo de Recuperación Operativa – WRT) no reflejan actualizaciones basadas en simulacros recientes, lo que compromete la precisión de los escenarios de respuesta. Además, no se registra una clasificación formal de los servicios transversales críticos– ni se documenta la asignación de recurso– humanos mínimos requeridos para la continuidad de los procesos esenciales. Así las cosas, es de

vital importancia priorizar la actualización del Análisis de Impacto al Negocio (BIA) para mantener la efectividad del Plan de Continuidad del Negocio, ya que asegura que los procesos críticos, tecnologías y riesgos emergentes estén correctamente identificados en tanto que un BIA vigente facilita la toma de decisiones, reduce riesgos operacional y garantiza la coherencia con otros planes como el DRP y el PAC, fortaleciendo la resiliencia organizacional. Por lo anterior, la OFCIN se permite registrar las siguientes recomendaciones:

Oportunidad de Mejora Correctiva No.3.

La OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, priorizar la actualización del documento Guía Análisis del Impacto del Negocio con una frecuencia de revisión apropiada, acorde al contexto y los riesgos del negocio, incorporando entre otros aspectos como los que se detallan a continuación y establecer e implementar un cronograma formal de revisión anual y definir responsables para su mantenimiento:

1. Aspectos Generales:

- Para fortalecer la eficacia del Plan de Continuidad del Negocio (PCN), se recomienda implementar una estrategia de actualización continua mediante un cronograma de revisión semestral o anual del Análisis de Impacto al Negocio (BIA), con responsables claramente designados para su mantenimiento.
- Asegurar la integración y coherencia entre el BIA, el Plan de Recuperación ante Desastres (DRP) y el Punto Alterno de Continuidad (PAC), validando que los tiempos definidos en cada uno estén alineados.
- Para facilitar la priorización, se sugiere incorporar herramientas visuales como mapas de calor, diagramas de flujo y gráficos comparativos que evidencien la evolución de los tiempos de recuperación antes y después de los simulacros; documentando sistemáticamente los resultados de las pruebas, incluyendo lecciones aprendidas, y establecer un plan anual de simulacros.
- En cuanto a la gestión de terceros, es clave identificar proveedores críticos, evaluar sus propios planes de continuidad y verificar la alineación de sus BIA con el de CAJA HONOR.
- Incluir escenarios de riesgos emergentes como ciberataques, fallos en servicios en la nube o configuraciones erróneas de inteligencia artificial, evaluar la resiliencia digital de los procesos dependientes de tecnología, capacitar periódicamente a los responsables de procesos críticos y desarrollar un manual simplificado para los equipos operativos.
- Registrar en el control de cambios la actualización correspondiente del documento, toda vez que se observó que no ha sido actualizado desde la vigencia 2023.

2. Aspectos Específicos:

- En la sección de *Metodología*, se sugiere clarificar el marco de referencia utilizado, ya que actualmente no se evidencia una alineación explícita con normas reconocidas; además, es recomendable incluir una descripción más precisa de las fases del proceso y los responsables asignados, complementada con ejemplos de aplicación por proceso.
- En cuanto a la *Evaluación de criticidad*, se recomienda validar que los criterios de impacto estén alineados con los objetivos estratégicos de la organización, e

incorporar el impacto reputacional y el cumplimiento normativo como dimensiones independientes.

- Respecto a los *Aplicativos*, es necesario verificar que todos los sistemas listados cuenten con respaldo y planes de restauración documentados, así como identificar y registrar las dependencias tecnológicas entre ellos.
- En la sección de *Recursos mínimos*, se debe asegurar que los recursos definidos sean suficientes para operar desde un punto alternativo, incluyendo un inventario detallado de equipos y accesos requeridos.
- Para continuar con el fortalecimiento del plan, se recomienda integrar las observaciones antes citadas en una versión actualizada del Análisis de Impacto al Negocio (BIA), elaborar una presentación ejecutiva para la alta dirección y diseñar una plantilla editable que facilite futuras actualizaciones del plan.

Lo anterior, dado que se evidenció que el documento no ha sido actualizado desde la vigencia 2023, pese a que su revisión debe realizarse al menos de forma anual y cada vez que ocurran cambios significativos en la Entidad. Conforme a la norma ISO 22301, el BIA constituye un documento dinámico que requiere ajustes periódicos y no debe considerarse una actividad única, debiendo actualizarse tras incidentes relevantes, auditorías internas o modificaciones sustanciales en procesos, tecnología o estructura organizacional.

En este contexto, las acciones propuestas buscan garantizar el cumplimiento de normativas nacionales e internacionales aplicables a la gestión de continuidad del negocio, tales como la NTC ISO/IEC 22301, el Modelo Integrado de Planeación y Gestión (MIPG), y disposiciones regulatorias como la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1474 de 2011 en materia de transparencia y control institucional. Asimismo, se alinean con los requerimientos de la Superintendencia Financiera, que exige contar con planes de recuperación ante desastres, gestión de terceros y continuidad operativa. Es de anotar que, la implementación de estas medidas permite fortalecer la trazabilidad, la alineación entre componentes del PCN (BIA, DRP, PAC), y la capacidad de respuesta ante eventos disruptivos; minimizar riesgos operacionales, tecnológicos y reputacionales, tales como la pérdida de información crítica, la interrupción de servicios esenciales, el incumplimiento normativo y la exposición a ciberataques o fallos en servicios digitales. También contribuyen a mejorar la resiliencia organizacional, facilitar la toma de decisiones en escenarios de crisis, garantizar la continuidad de procesos críticos y generar confianza en los grupos de interés o partes interesadas. De igual forma, la incorporación de herramientas visuales, simulacros documentados, gestión de proveedores críticos y capacitación periódica refuerza la eficacia del PCN y su capacidad de adaptación frente a riesgos emergentes. Se observó el R029 – Fallas en la Gestión del Plan de Continuidad del Negocio (PCN), CA029 – Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad.

6. ¿Para la ejecución del PCN se han definido claramente los roles y responsabilidades de todos los involucrados? Adjuntar conformación del PCN indicando datos tales como: nombres y apellidos, Área o Dependencia, Cargo, Rol que ejerce en el PCN, Datos de Contacto y demás que considere pueden aportar para el ejercicio auditor.

Respuesta: Se adjunta el documento Excel: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #4" del

Excel en donde se enlista el personal que hace parte los equipos relacionados al PCN y DRP.

Mediante el archivo denominado Requerimiento de Información PCN PAC Y DRP.xlsx el proceso auditado suministró la siguiente información:

Tabla 4. Conformación Comité Directivo de Continuidad

Fuente: OAGRI – Archivo Requerimiento de Información PCN PAC Y DRP.xlsx – Hoja Punto #4

Tabla 5. Integrantes PCN

Fuente: OAGRI – Archivo Requerimiento de Información PCN PAC Y DRP.xlsx – Hoja Punto #4

De la información registrada en la Tabla 4, se evidenció que procesos y áreas estratégicas como Jurídica (Profesional de la Oficina Asesora Jurídica), Gestión del Riesgo (Profesional Especializado de la Oficina Asesora de Gestión del Riesgo), Proveedor de Data Center Claro (Administración de Red y Bases de Datos), Informática (Líderes técnicos de sistemas críticos) y procesos Misionales como Comunicaciones (Profesional Universitario del Área de Comunicaciones) no tienen plenamente identificado al funcionario que ejerce el rol dentro del Equipo de Administración de Crisis. Esta falta de definición compromete la capacidad de respuesta coordinada ante eventos disruptivos, especialmente en aspectos legales, tecnológicos, de gestión del riesgo y comunicación institucional; además de representar un incumplimiento de la norma técnica NTC ISO/IEC 22301, que exige la asignación clara de responsabilidades dentro del sistema de gestión de continuidad. Esta debilidad expone a la organización a riesgos como fallas en la toma de decisiones, pérdida de trazabilidad legal, interrupciones en la infraestructura tecnológica, y afectación reputacional por falta de comunicación efectiva. Se recomienda formalizar la designación de responsables en cada área crítica, documentarlos en el plan de continuidad, y asegurar que cuenten con la capacitación necesaria para actuar de manera oportuna y eficaz en escenarios de crisis.

7. Suministrar evidencias de la formación y capacitación suministrada al personal sobre sus funciones en el PCN y demás procedimientos de continuidad.

Respuesta: Se adjuntan los siguientes documentos en la carpeta Punto #5 PCN, acordes a las capacitaciones realizadas durante el periodo auditado (01-Octubre-2024 al 30-Sept-2025).

- CAPACITACION PCN MAYO 2025.pdf.
- CAPACITACION PCN SEPTIEMBRE 2025.pdf.

Así como también los listados de asistencia respectivos a dichas capacitaciones

- Informe de asistencia 8-05-25 PCN MAYO.
- Informe de asistencia 9-25-25 PCN SEPTIEMBRE.

En la carpeta mencionada se observan los siguientes archivos:





Nombre	Fecha de modificación
 CAPACITACION PCN MAYO 2025.pdf	20/10/2025 12:19 p. m.
 CAPACITACION PCN SEPTIEMBRE 2025.pdf	20/10/2025 12:19 p. m.
 Informe de asistencia 8-05-25 PCN MAYO.csv	20/10/2025 12:19 p. m.
 Informe de asistencia 9-25-25 PCN SEPTIEMBRE.csv	20/10/2025 12:19 p. m.

Figura 27. OAGRI – Evidencias Capacitación PCN



Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre


- Archivo CAPACITACION PCN MAYO 2025.pdf: contiene 22 slides con temas tales como Organigrama OAGRI Gestión de Seguridad de la Información, contexto histórico de la gestión de continuidad de negocio comenzó a enfocarse en la recuperación ante desastres, Definición de PCN, Objetivos del PCN, BENEFICIOS DE TENER UN PCN, Puesta en marcha: Comité Directivo de Continuidad, Equipos de trabajo durante el PCN, Estrategias para garantizar la operación, Objetivos DRP en Caja Honor, Objetivos PAC en Caja Honor, Análisis de impacto en el negocio (BIA), Cual es el rol del funcionario dentro del PCN?, TIPS Para garantizar tu conexión VPN.
- CAPACITACION PCN SEPTIEMBRE 2025.pdf: contiene 27 slides con temas tales como Plan de Continuidad del Negocio, Definición PCN, Cual es el rol del funcionario dentro del PCN?, Estrategias para garantizar la operación, ¿Cuál es la estrategia operativa para restaurar los servicios dentro del PCN? Cuya respuesta es Plan de recuperación de desastres (DRP), PRUEBA DRP & PAC II SEMESTRE 2025 (3 Y 4 de octubre 2025), Guía de Operación Flujo documental GR-NA-GU-038, TIPS Para garantizar tu conexión VPN, ¿Cuál es el código de la guía de operación del flujo 395? Cuya respuesta corresponde a GR-NA-GU-038, Actualización Res. 604 del 2019, Equipos de trabajo durante el PCN, Principales Actualizaciones, Actualización Manual PCN V7, Gestión PCN con proveedores y terceros, entre otros.
- Informe de asistencia 8-05-25 PCN MAYO.csv: contiene información de la asistencia de 211 participantes con duración de la reunión de 1 hora y 16 minutos.


De la información contenida en el presente archivo se tienen las siguientes precisiones:

- ✓ De acuerdo con el nombre del archivo se entiende que la capacitación fue realizada el 08-05-2025.
- ✓ En los campos *Hora de Inicio* se observa “8/05/25, 7:10:55 AM” y *Hora de Finalización* registra “8/05/25, 8:27:08 AM”
- ✓ No obstante, para cada asistente tanto la *Fecha de entrada* como la *Fecha de Salida* registra “4-05-2025”, lo cual no es concordante con las fechas antes citadas en el ítem anterior.
- Informe de asistencia 9-25-25 PCN SEPTIEMBRE.csv; contiene información de la asistencia de 237 participantes con duración de la reunión de 2 h 38 minutos. De la información contenida en el presente archivo se tienen las siguientes precisiones:
 - ✓ De acuerdo con el nombre del archivo se entiende que la capacitación fue realizada el 25-09-2025.
 - ✓ En los campos *Hora de Inicio* se observa “9/25/25, 7:15:31 AM” y *Hora de Finalización* registra “9/25/25, 9:54:25 AM”
 - ✓ Tanto en la *Fecha de entrada* como la *Fecha de Salida* registra “9/25/25”, tema que concuerda con las fechas registradas en el ítem anterior.

Si bien el proceso auditado suministró soportes que evidencian la realización de capacitaciones relacionadas con el Plan de Continuidad del Negocio – PCN, para la capacitación realizada en el primer semestre de 2025, no se identificó la aplicación de instrumentos de evaluación ni el análisis de los resultados obtenidos que permitieran determinar el nivel de comprensión, apropiación o percepción de los asistentes frente a la información impartida, lo que limita la trazabilidad del impacto formativo y dificulta la retroalimentación estratégica del proceso, considerando que la sensibilización efectiva sobre el PCN es un componente crítico para fortalecer la resiliencia organizacional y garantizar la respuesta oportuna ante eventos contingentes. Cabe destacar que, respecto a la capacitación realizada en el segundo semestre de 2025, la OAGRI, mediante comunicación electrónica del 06-11-2025, aportó soportes que evidencian el análisis de los resultados de evaluación y la definición de acciones orientadas al fortalecimiento de áreas que requieren mejora, en donde con fecha 17-10-72025 socializó el Material de Refuerzo – Guía Refuerzo Plan de Continuidad del Negocio, así:



Guía Refuerzo Plan de Continuidad del Negocio


- 1. Rol del Funcionario en el PCN** 



Conocer el Plan de Continuidad del Negocio (PCN) institucional implica entender a fondo las políticas, procedimientos y estrategias que la organización ha definido para garantizar la operación continua de sus procesos críticos ante eventos disruptivos.
- 2. Estrategias de Continuidad** 

 - ❖ **DRP (Plan de Recuperación de Desastres):** conjunto de procedimientos técnicos y operativos diseñados para restaurar la infraestructura tecnológica y los servicios críticos tras un evento disruptivo.
 - ❖ **PAC (Punto Alterno de Contingencia):** Estrategia de trabajo remoto que permite continuar operaciones en caso de indisponibilidad del sitio principal.



Fallover




Fallback


- 3. Gestión de Comunicación en Crisis** 

Se cuenta con el Árbol de llamadas y la Matriz de comunicación PCN que permiten una respuesta rápida, estructurada y coordinada ante desastres naturales, fallas tecnológicas o incidentes que comprometan la operación.


- 4. Actualización documental** 

 - ❖ **Manual PCN:** Ajuste estructural e inclusión de capítulos.
 - ❖ **Guía de operación PAC:** Lineamientos para operación en PAC.
 - ❖ **Resolución 604 del 2019:** Modificada mediante la Resolución 396 del 2025
 - ❖ **Plan de Crisis:** Estrategias de operación en escenarios de crisis.
- 5. Gestión con Proveedores y Terceros** 

Resaltar la importancia de la inclusión de cláusulas de continuidad, seguridad de la información, pruebas de vulnerabilidad y gestión de accesos por como parte de las obligaciones contractuales.




Figura 28. Guía Refuerzo Plan de Continuidad del Negocio – socializada Email 17-10-2025
Fuente: OAGRI – Outlook – Correo Electrónico 06-11-2025

Durante la revisión se evidenció que el seguimiento y análisis de las capacitaciones impartidas, así como de las evaluaciones aplicadas a los colaboradores, no se realizó de manera integral para todas las actividades formativas, lo que limita la identificación de oportunidades de mejora y la implementación de acciones correctivas en casos de reprobación, lo cual afecta directamente la eficacia del programa de capacitación y el cumplimiento de los requisitos establecidos en la norma ISO 22301:2019, cláusula 7.2, y en el numeral 3.2.4 de la Circular Externa 006 de 2025 de la SFC.

Cabe resaltar que esta situación ya había sido identificada y documentada en el Informe 25 de 2024 – Evaluación a la Gestión del Riesgo Operacional, correspondiente al período auditado entre el 1 de junio de 2023 y el 30 de septiembre de 2024, en donde se incluyó la Recomendación 2. “La OFCIN recomienda a OAGRI, que una vez impartida la capacitación y aplicada la evaluación respectiva a los colaboradores de la Entidad, los resultados sean analizados de tal forma que se conozca si hubo comprensión del tema y apropiación del mismo, evaluar cuánto contenido fue asimilado y si los participantes están preparados para aplicar lo aprendido, análisis de la participación y compromiso, análisis de satisfacción de los participantes y en fin saber si la capacitación frente al tema de alta importancia para la Entidad como lo es el PCN, fue efectiva o si es necesario la aplicación de ajustes o recapitación. Lo anterior, con el objetivo de tender al fortalecimiento de la cultura organizacional, cumplimiento normativo y reducción de riesgos, entre otros aspectos”, la

cual para el desarrollo del presente ejercicio auditor aún no ha sido atendida, la OFCIN registra:

Oportunidad de Mejora Correctiva No. 4.

La OFCIN recomienda a la OAGRI en coordinación con los demás procesos interrelacionados implementar mecanismos de evaluación antes, durante y después de las capacitaciones relacionadas con el Plan de Continuidad del Negocio – PCN, que permitan medir el nivel de comprensión, apropiación y percepción de los asistentes, así como analizar los resultados obtenidos para identificar brechas de conocimiento, retroalimentar estratégicamente el proceso formativo y aplicar acciones correctivas cuando sea necesario; toda vez que durante la revisión del proceso de capacitación relacionado con el Plan de Continuidad del Negocio – PCN, se evidenció que, si bien se cuenta con soportes que demuestran la realización de actividades formativas, no se identificó la aplicación de instrumentos de evaluación ni el análisis de resultados que permitan determinar el nivel de comprensión, apropiación o percepción de la información por parte de los asistentes; lo que limita la trazabilidad del impacto formativo, dificulta la retroalimentación estratégica del proceso y restringe la implementación de acciones correctivas en caso de reprobación, afectando la eficacia del programa y el cumplimiento de los requisitos establecidos en la norma ISO 22301:2019, cláusula 7.2, y el numeral 3.2.4 de la CE 006 de 2025 de SFC. La ausencia de estos mecanismos incrementa el riesgo de desinformación del personal frente a sus roles en situaciones de contingencia, una respuesta ineficaz ante eventos disruptivos y la pérdida de continuidad operativa, comprometiendo la resiliencia organizacional. Se observó el R029 – FALLAS EN LA GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN).

8. ¿La Entidad cuenta con mecanismos que permitan verificar el conocimiento y preparación del personal en situaciones de crisis? Favor describir

Respuesta: Durante las capacitaciones realizadas en el periodo auditado, se relacionan temas acordes a la preparación del personal en situaciones de crisis, así como estrategias que se tienen para abordar las mismas, como resultado se adjuntan los siguientes resultados obtenidos de la capacitación realizada en el mes de mayo:

Tabla 6. Estadísticas proceso de Capacitación Situaciones de Crisis – Mayo de 2025

Estadísticas	
Asistieron a la Capacitación:	211
Realizaron la Capacitación	403
Personal:	442
Aprobaron:	354
No Aprobaron:	25
Porcentaje de participación:	91,18%
Tasa de aprobación:	87,84%
Puntuación media:	9,23

Fuente: OAGRI – Archivo Documento Guía para acceso a carpetas.docx

El análisis de los datos de capacitación presentados en la Tabla 6, revela una alta participación del personal, con un 91,18% de los colaboradores involucrados en el proceso formativo, lo que refleja un elevado nivel de compromiso institucional o una estrategia de convocatoria eficaz. No obstante, la OFCIN observó inconsistencias en los datos dado que las sumatorias no eran concordantes con el universo del personal, con fecha 11-11-2025

se llevó a cabo prueba de recorrido con el profesional responsable por parte de la OAGRI solicitando dar alcance a la información previamente suministrada, con lo que el proceso auditado realizó los ajustes pertinentes y allegó los soportes respectivos mediante email de la misma fecha, además de aclarar que la capacitación fue realizada vía Teams, así:

Tabla 7. Información Estadística Ajustada proceso de Capacitación Situaciones de Crisis – Mayo de 2025

Estadísticas	
Asistieron a la Capacitación:	211
Realizaron la Evaluación de la Capacitación:	403
Personal:	442
Aprobaron:	375
No Aprobaron:	28
Porcentaje de participación:	91,18%
Tasa de aprobación:	93,05%
Puntuación media:	9.23

Fuente: OAGRI – Outlook – Correo Electrónico 11-11-2025

En la Tabla 7 se presenta que el universo de personal de la Entidad corresponde a 442 colaboradores, de los cuales un total de 211 participaron en la capacitación virtual impartida a través de Microsoft Teams. No obstante, la evaluación fue completada por 403 personas, lo que indica que 192 colaboradores, aun sin asistir a la sesión virtual, accedieron al enlace de la evaluación y lograron realizarla. Asimismo, del total de participantes evaluados, 375 aprobaron, alcanzando una tasa de aprobación del 93,05%, mientras que 28 no lograron superar la prueba. La puntuación media obtenida fue de 9,23 sobre 10, lo que refleja una alta efectividad en la transferencia de conocimiento y un nivel significativo de satisfacción con la capacitación.

Sin embargo, se identifican áreas de mejora en la cobertura, dado que 39 personas no participaron en la capacitación, así como en el seguimiento a los 28 colaboradores que no aprobaron. Este análisis permitirá determinar si las causas están asociadas a la asistencia, el desempeño académico o factores técnicos, con el objetivo de fortalecer los procesos de formación, evaluación y acompañamiento en futuras jornadas.

Igualmente, la OAGRI suministró evidencias de la formación enfocada a preparación ante situaciones de crisis en la sensibilización del mes de septiembre, así:

Tabla 8. Estadísticas proceso de Capacitación Situaciones de Crisis – Septiembre de 2025

Asistieron a la Capacitación:	237
Realizaron la Capacitación:	401
Personal:	442
Aprobaron:	381
No Aprobaron:	19
Porcentaje de participación:	90,72%
Tasa de aprobación:	95,01%
Puntuación media:	95,81

Fuente: OAGRI – Archivo Documento Guía para acceso a carpetas.docx

Como se observa en la Tabla 8, la capacitación presentó una participación destacada del 90,72% del personal total (442 personas), con 401 colaboradores que completaron el proceso formativo. De los cuales, 381 aprobaron, alcanzaron una tasa de aprobación del 95,01%, respaldada por una puntuación media de 95,81, lo que evidencia un alto nivel de desempeño y efectividad en la estrategia de formación implementada. No obstante, la OFCIN observó inconsistencias en los datos dado que las sumatorias no eran concordantes con el universo del personal, con fecha 11-11-2025 se llevó a cabo prueba de recorrido

con el profesional responsable por parte de la OAGRI solicitando dar alcance a la información previamente suministrada, con lo que el proceso auditado realizó los ajustes pertinentes y allegó los soportes respectivos mediante email de la misma fecha, además de aclarar que la capacitación fue realizada vía Teams, así:

Tabla 9. Información Estadística Ajustada proceso de Capacitación Situaciones de Crisis – Sept. De 2025

Estadísticas	
Asistieron a la Capacitación:	237
Realizaron la Capacitación:	406
Personal:	440
Aprobaron:	386
No Aprobaron:	20
Porcentaje de participación:	92,27%
Tasa de aprobación:	95,07%
Puntuación media:	95,76

Fuente: OAGRI – Outlook – Correo Electrónico 11-11-2025

En la Tabla 9 se presenta que el universo de personal de la Entidad corresponde 440 colaboradores, de los cuales 237 asistieron a la capacitación virtual. Sin embargo, la evaluación fue completada por 406 personas, lo que evidencia que 169 colaboradores, aun sin asistir, accedieron al enlace de la evaluación. Del total evaluado, 386 aprobaron, alcanzando una tasa de aprobación del 95,07%, mientras que 20 no lograron superar la prueba. La puntuación media obtenida fue de 95,76 sobre 100, reflejando una alta efectividad en la transferencia de conocimiento y satisfacción con la capacitación. No obstante, se identifican oportunidades de mejora en la cobertura presencial y en el seguimiento a los participantes que no aprobaron, con el fin de analizar causas relacionadas con asistencia, rendimiento o factores técnicos, y fortalecer los procesos de formación y acompañamiento en futuras jornadas.

9. Informes de Ejecución y desarrollo de las últimas pruebas y simulacros de continuidad y contingencia efectuadas en la Entidad, en el cual se registre y detalle todo lo ocurrido durante el simulacro, seguimiento de eventos clave, tiempos de respuesta, acciones realizadas y desviaciones o problemas encontrados, captura de pantallas, grabaciones y demás que demuestren el desarrollo de las acciones.

Respuesta: Se adjunta el siguiente documento en la carpeta Punto #7 PCN:

- INFORME DRP-PRUEBA PAC MAYO 2025.pdf en donde se detalla la ejecución de la prueba DRP y PAC en los días 02 y 03 de mayo del 2025.

[Verificación Archivo INFORME DRP-PRUEBA PAC MAYO 2025.pdf](#)

Este archivo contiene un total de 15 folios correspondiente al INFORME PRUEBA TECNICA DRP / PUNTO ALTERNO DE CONTINUIDAD del 30-05-2025, en el cual se indica que las pruebas fueron desarrolladas durante los días 02 y 03 de mayo de 2025, cuyo objetivo principal fue “El objetivo de esta prueba fue validar la capacidad de Caja Honor para recuperar sus operaciones críticas en caso de un desastre, asegurando la continuidad del negocio” y con objetivos específicos:

- Verificar el cumplimiento del minutograma durante la prueba del DRP.

- Realizar en paralelo la ejecución de una prueba del Punto Alterno de Continuidad.
- Realizar el seguimiento a las evidencias tomadas por todo el personal que interviene en la prueba DRP y PAC. “

Igualmente, una vez revisado el informe citado, se observa que durante el ejercicio fueron probados tanto el Plan de recuperación de desastres – DRP, la cual se indicó en el informe que se “*declaró exitosa en vista de que fueron validados los procedimientos de failover y failback*” no obstante, es importante tener en cuenta que una prueba de Disaster Recovery Plan – DRP se considera exitosa cuando valida la capacidad de la organización para restaurar la operación crítica dentro de los parámetros definidos por el plan, más allá de ejecutar el failover y failback; siendo que el éxito implica cumplir los objetivos de recuperación (RTO y RPO), garantizar la integridad y disponibilidad de los datos y aplicaciones, y confirmar que los servicios esenciales funcionan correctamente en el entorno alternativo. Además, la prueba debe documentarse de forma completa, evidenciando tiempos, incidencias y acciones correctivas, asegurando que los procedimientos y roles se ejecutaron conforme a lo establecido. Solo bajo estos criterios se puede afirmar que el DRP es efectivo y que la continuidad del negocio está asegurada ante un evento disruptivo.

Por su parte, tras el análisis del informe de la prueba del Punto Alterno de Continuidad – PAC se evidencia la necesidad de fortalecer la preparación operativa y técnica para garantizar la efectividad del DRP, estableciendo acciones correctivas enfocadas en tres áreas críticas: gestión del personal, asegurando la disponibilidad y capacitación previa; validación técnica, mediante revisiones anticipadas de equipos y pruebas de conectividad VPN; y mejora de procedimientos, actualizando la documentación y estableciendo controles preventivos; medidas que permitirán reducir riesgos, optimizar tiempos de respuesta y asegurar la continuidad del negocio en escenarios de contingencia.

Dado lo anteriormente expuesto, la OFCIN precisa:

Recomendación No. 4.

La OFCIN recomienda a la OAGRI en coordinación con la OAINF que para garantizar la efectividad del Plan de Recuperación de Desastres (DRP) y del Punto Alterno de Continuidad (PAC), se implemente un enfoque integral que incluya la **validación** completa del DRP, asegurando que las pruebas no solo contemplen el failover y failback, sino también el cumplimiento de los objetivos de recuperación (RTO y RPO), la integridad de los datos y la operatividad de los servicios críticos en el entorno alternativo, conforme a los lineamientos de la **Ley 1523 de 2012 sobre Gestión del Riesgo de Desastres**, directrices de la Unidad Nacional para la Gestión del Riesgo de Desastres – **UNGRD** para continuidad operativa; **documentación exhaustiva**, registrando tiempos, incidencias y acciones correctivas, en cumplimiento con estándares como **ISO 22301:2019** sobre Sistemas de Gestión de Continuidad del Negocio; **fortalecimiento operativo y técnico del PAC**, mediante la capacitación previa del personal clave, revisiones anticipadas de equipos y pruebas de conectividad VPN, alineadas con las políticas de seguridad de la información (Ley 1581 de 2012 y Decreto 1377); y **actualización y control de procedimientos**, incorporando controles preventivos y ajustes derivados de las lecciones aprendidas, así como los lineamientos de la **Circular Externa 006 de 2025, Parte I, Título I, Capítulo VIII (Espacio Controlado de Pruebas – ECP)**, que exige la realización de pruebas periódicas y documentadas para garantizar la continuidad operativa y tecnológica, incluyendo escenarios de contingencia, validación de RTO y RPO, capacitación del personal y reporte

de resultados a la SFC. Lo anterior, con el objeto de minimizar riesgos asociados con la pérdida de datos críticos, fallas en la conectividad del PAC que impidan la operación remota, errores humanos por falta de capacitación, vulnerabilidades frente a ciberataques durante la contingencia y afectación reputacional y financiera por interrupciones prolongadas.

10. Informe de Resultados del Simulacro en el cual se registre el resultado del desempeño, si se cumplieron los objetivos planeados, métricas más relevantes, cumplimiento de los tiempos de recuperación RTO /RPO, Análisis de brechas, debilidades, fallos detectados con detalle de los puntos críticos, entre otros que considere importantes.

Respuesta: Se adjuntan los siguientes documentos en la carpeta Punto #8 PCN:

- Plan_prueba_DRP_Total_CajaHonor_2025.pdf: Detalla el alcance y resultados esperados de la prueba.
- Informe Ger prueba_DRP_Total_CajaHonor_02 y 03 mayo 2025.pdf: Informe ejecutivo de resultado de la prueba DRP.
- Informe Prueba DRP Total Caja Honor 02y03mayo2025.pdf: Informe detallado de la ejecución de la prueba DRP.

Documentos analizados en el ítem 7.

11. Documentos relacionados con el proceso de pruebas:
 - Árbol de Llamadas (Personal responsable indicando nombres, cargo y Rol en el simulacro, Nro. Contacto)
 - Minutograma del desarrollo de la prueba
 - Comunicados a partes interesadas
 - Alcance de la prueba
 - Descripción de Escenarios de la prueba
 - Evidencias de comunicación en todo el proceso de pruebas
 - Lista de todos los asistentes que participaron en el simulacro (funcionarios, terceros, otras partes interesadas), incluyendo roles y responsabilidades durante la prueba)
 - Otros

Respuesta: Se adjuntan los siguientes documentos en la carpeta Punto #9 PCN:

- Requerimiento de Información PCN PAC Y DRP.xlsx en la hoja "Punto #9" se encuentran roles y responsabilidades, datos de contacto de la prueba DRP.
- Árbol de Llamadas PCN.xlsx – Septiembre 2025.
- Informe Ger prueba_DRP_Total_CajaHonor_02 y 03 mayo 2025.pdf.
- Informe Prueba DRP Total Caja Honor 02y03mayo2025.pdf con resultados y análisis obtenidos.
- SIMULACRO – PLAN DE RECUPERACION ANTE DESASTRES (DRP) y PAC_: Comunicado emitido a funcionarios mencionando la indisponibilidad de servicios durante los días de la prueba.

Archivo Requerimiento de Información PCN PAC Y DRP.xlsx – Hoja Punto #9: contiene la relación del recurso humano tanto de Caja Honor como del proveedor CLARO responsable del DRP, así:

Tabla 10. Equipo Humano DRP – Entidades Caja Honor – Proveedor CLARO

Fuente: OAIGRI - Repositorio Documental – Link: 10 Octubre - Archivo Requerimiento de Información PCN PAC Y DRP.xlsx - Hoja Punto #9

En la Tabla 10 se presenta la estructura del recurso humano asignado al DRP, conformada por nueve profesionales del contratista CLARO con funciones específicas como Coordinador de Continuidad, Consultor DRP, especialistas en Bases de Datos, Infraestructura TI (Virtualización y Sistemas Operativos), Administración de Redes, Almacenamiento, DSD Premium, TSM Caja Honor y NOC-LAN. Por parte de Caja Honor, se cuenta con siete profesionales que desempeñan roles clave, entre ellos Líder DRP, Líder PCN, Ingeniero Profesional PCN, especialistas en Seguridad de la Información (Ethical Hacking), Ciberseguridad FW, Ciberseguridad e Infraestructura TI.

Así las cosas, en términos generales, el equipo antes descrito resulta adecuado para atender el DRP, ya que cuenta con perfiles esenciales en continuidad del negocio, administración de infraestructura, redes, almacenamiento, bases de datos y seguridad de la información, roles fundamentales para garantizar la recuperación y operación de los servicios críticos ante una contingencia. No obstante, su suficiencia depende de factores adicionales como la cobertura horaria 24/7 para respuesta inmediata, la experiencia y certificaciones en gestión de continuidad y recuperación (ISO 22301, ITIL, entre otras), así como la capacidad de coordinación y ejecución de pruebas periódicas que validen la efectividad del plan.

12. ¿En función de los cambios normativos, cambios en la Entidad, en la tecnología o en el entorno, Caja Honor tiene implementados procedimientos para revisar y mejorar el plan – PCN continuamente? Cuales, descríbelos.

Respuesta: Se encuentra actualizada la versión 7 del Manual de gestión del Plan de Continuidad del Negocio (PCN), la cual incorpora los cambios recientes derivados del proceso de revisión y mejora continua. En esta versión se destaca la inclusión del Capítulo 6. MANTENIMIENTO Y ACTUALIZACION DEL PCN, donde se documenta de manera estructurada el procedimiento para la actualización del plan.

Una vez la OFCIN revisó el documento GR-NA-MA-008 MANUAL PCN V7.docx, se observó la descripción del procedimiento para revisar y mejorar el plan – PCN continuamente, así:

6. MANTENIMIENTO Y ACTUALIZACION DEL PCN

Establecer los procedimientos y responsabilidades para el mantenimiento y la actualización continua del Plan de Continuidad del Negocio (PCN) garantizan su efectividad y relevancia ante cambios internos y externos. Debe ser revisado de manera periódica con el fin de actualizar su estructura cuando ocurran estos eventos:

- Cambios significativos en la estructura organizacional.
- Introducción de nuevas tecnologías o procesos.
- Cambios en la normativa legal o regulatoria.
- Resultados de pruebas y simulacros que indiquen la necesidad de ajustes.
- Incidentes reales que requieran la activación del PCN tras el registro de las lecciones aprendidas.

6.2 Procedimiento de Actualización

- **Recolección de Información:** Recopilar datos sobre cambios internos y externos que puedan afectar el PCN.
- **Evaluación de Impacto:** Analizar el impacto de los cambios identificados en los procesos críticos del negocio.
- **Revisión y Aprobación:** El Comité de Continuidad del Negocio revisará las propuestas de actualización y aprobará los cambios necesarios.
- **Comunicación:** Informar a todos los interesados sobre las actualizaciones realizadas en el PCN.
- **Documentación:** Actualizar todos los documentos relacionados con el PCN y asegurar su accesibilidad.
- **Pruebas y Simulacros:** Realizar pruebas y simulacros periódicos con su debida documentación, para evaluar la efectividad del PCN y la capacidad de respuesta de la organización.

6.3 Capacitación y Sensibilización

Proporcionar formación continua a los empleados sobre sus roles y responsabilidades en el PCN además de realizar campañas de concienciación para asegurar que todos los empleados comprendan la importancia del PCN y sepan cómo actuar en caso de una interrupción.

Figura 29. Procedimiento para revisar y mejorar el plan – PCN
Fuente: OAGRI – documento GR-NA-MA-008 MANUAL PCN V7.docx, pág. 32

No obstante, en lo que respecta a su implementación en la Entidad, este aspecto será objeto de revisión por parte de la OFCIN en el marco de futuros ejercicios de auditoría interna.

13. ¿Para el tema de comunicación y notificación, existen sistemas alternativos de comunicación en caso de falla en los canales habituales? Favor mencionarlos e indicar el documento en los que se encuentran registrados.

Respuesta: El documento Manual de gestión del PCN contiene los siguientes capítulos que detallan el proceso de comunicación en contingencias

- 4.3 identificación de partes interesadas
- 4.3.1 Comunicación con las partes interesadas

Adicionalmente se adjunta documento:

- **MATRIZ COMUNICACION PCN.xlsx**: consolida los escenarios clave de activación, los mensajes estratégicos, así como los canales, medios y frecuencias definidos para garantizar una gestión oportuna de la información durante situaciones de contingencia.

Tras el análisis realizado por la OFCIN se observó dentro del documento GR-NA-MA-008 MANUAL PCN V7.docx, páginas 14, 15 y 16 el tema correspondiente con partes interesadas y 8 pasos a seguir en caso de presentarse algún evento que generen una afectación operativa, tecnológica o reputacional en Caja Honor, incluyendo incidentes de ciberseguridad, fallas operativas, interrupciones de servicio y situaciones de crisis, así:

- Detección y clasificación del evento**
 - El evento se identifica por el Área responsable (Informática, Talento Humano, Comunicaciones, etc.).
 - Clasificado según su naturaleza: operativo, tecnológico, reputacional, entre otros.
- Activación del protocolo**
 - Se activa el protocolo correspondiente establecido en:
 - **PCN** para continuidad operativa.
 - **Manual de Comunicaciones** para gestión reputacional.
 - **Guía IT-NA-GU-029** para eventos de ciberseguridad.
- Identificación de partes interesadas**
 - Se consulta la matriz GE-NA-PI-02 para determinar los actores afectados.
 - Se prioriza según nivel de impacto y criticidad.
- Selección de canal de comunicación**
 - Se elige el canal más adecuado según el tipo de parte interesada (interno, externo, institucional).
 - Funcionarios: Intranet, Outlook, reuniones.
 - Afiliados: Portal institucional, redes sociales, puntos de atención.
 - Entes de control: correo institucional, comunicados oficiales.
- Redacción del mensaje**
 - El mensaje debe ser claro y de carácter institucional.
 - Debe incluir: descripción del evento, acciones tomadas, canales de atención y compromiso.
- Registro documental**
 - Todo mensaje enviado debe ser registrado en el sistema de gestión documental.
 - Se debe incluir fecha, canal, destinatario, contenido y responsable.
- Seguimiento y retroalimentación**
 - Se monitorea la recepción y respuesta de las partes interesadas.
 - Se documenta cualquier retroalimentación relevante.
- Escalamiento técnico (si aplica)**
 - En caso de eventos tecnológicos críticos, se reporta al:
 - **CCOC**: info@ccoc.mil.co
 - **COLCERT**: contacto@colcert.gov.co
 - **CSIRT**: csirtqob@mintic.gov.co, sopORTECC@mintic.gov.co

Figura 30. Partes interesadas y 8 pasos a seguir ante la presencia de eventos adversos
Fuente: OAGRI – documento GR-NA-MA-008 MANUAL PCN V7.docx, págs. 14, 15 y 16

Por su parte, en el documento MATRIZ COMUNICACION PCN.xlsx se consolida la información relacionada con los diferentes escenarios clave de activación para los Procesos (Gestión Informática, Gestión Administrativa, Gestión de Talento Humano, Gestión Estratégica), detallando para cada uno de ellos la Actividad específica, el Escenario de crisis, el tipo de Afectación, el Plan de Acción (Continuidad de Negocio), las Partes Interesadas, el Canal de comunicación y el Mensaje Recomendado. Sin embargo, es fundamental que esta matriz integre no solo la totalidad de los procesos de la Entidad, sino también las partes interesadas internas y externas, garantizando una visión integral y coordinada para la gestión de la comunicación en situaciones críticas; articulación que permite asegurar que todos los actores relevantes estén informados y alineados con las acciones definidas en el Plan de Continuidad del Negocio. Asimismo, el documento debe ser formalizado mediante la firma del responsable y del funcionario que lo proyectó, y posteriormente socializado en toda la organización, asegurando que los actores involucrados comprendan su alcance y aplicación, además la OFCIN hace especial énfasis respecto a que para garantizar la trazabilidad y la correcta administración del documento, éste debe contener la fecha de elaboración, el número de versión y un apartado de control de cambios, elementos que son esenciales para mantener la vigencia, identificar

actualizaciones y asegurar que la información utilizada sea la más reciente y validada. En consecuencia, la OFCIN precisa:

Oportunidad de Mejora Correctiva No. 5.

La OFCIN recomienda a la OAGRI, la actualización del documento MATRIZ COMUNICACIÓN PCN.xlsx integrando la totalidad de los procesos de la Entidad y partes interesadas internas y externas, asegurando una visión integral y coordinada para la gestión de comunicación en situaciones críticas. Asimismo, incorporar los elementos de control documental como fecha de elaboración, número de versión y control de cambios, conforme a las directrices del Sistema de Gestión Documental, además de ser importante la formalización del documento mediante las firmas correspondientes y garantizar su socialización en la Entidad y la alineación de la citada matriz con el Plan de Continuidad del Negocio (PCN), asegurando coherencia con los lineamientos normativos y las mejores prácticas. Lo anterior, toda vez que la OFCIN observó que el documento MATRIZ COMUNICACIÓN PCN.xlsx suministrado por la OAGRI, utilizado para la gestión de comunicación en escenarios críticos, no contempla la totalidad de los procesos de la Entidad, limitándose únicamente a Gestión Informática, Gestión Administrativa, Gestión de Talento Humano y Gestión Estratégica, situación que puede generar vacíos en la articulación y respuesta integral ante eventos disruptivos, afectando la efectividad del Plan de Continuidad del Negocio – PCN. De igual forma, se identificó la ausencia de la firma del responsable y del funcionario que lo proyectó, actas de socialización, control de cambios del documento que garantice la trazabilidad, transparencia e integridad, permitiendo identificar qué modificaciones se realizaron, quién las efectuó y en qué fecha, asegurando un historial claro para auditorías y revisiones. Además, de asegurar que la versión vigente sea la correcta, evitando el uso de información desactualizada y manteniendo la alineación con actualizaciones normativas o estratégicas y en el marco de documentos críticos como la matriz de comunicación del PCN, este control reduce riesgos operacionales al asegurar que todos los actores trabajen con información validada y actualizada. Lo anterior en aras de dar cumplimiento a la Política de Continuidad del Negocio y Procedimiento de Comunicación en Crisis, que establece la obligación de incluir todos los procesos institucionales en la matriz de comunicación, Ley 594 de 2000 (Ley General de Archivos) – Principios de organización y conservación documental, Ley 1712 de 2014 (Transparencia y acceso a la información pública), Modelo Integrado de Planeación y Gestión (MIPG) V.6 de 2024, Dimensión 5. Información y Comunicación – Lineamiento sobre gestión documental y trazabilidad, Norma Técnica Colombiana NTC ISO 22301 – Requisitos para la gestión de continuidad del negocio, incluyendo comunicación y control de la información, Políticas internas de gestión documental (control de cambios, versiones y trazabilidad), Circular Externa 006 de 2025 SFC - Planes de Continuidad del Negocio (PCN) y la matriz de comunicaciones en escenarios de crisis - Parte I – Instrucciones Generales, específicamente en el Capítulo relacionado con Gestión del Riesgo Operacional y Continuidad del Negocio. Se observó el R029 - Fallas en la Gestión del Plan de Continuidad del Negocio (PCN) por causas asociadas con CA029 - Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad.

14. Planeación simulacro de contingencia y continuidad vigencia 2025 (Detalle Objetivos del ejercicio, Escenario planteado, Lista de participantes y roles, Fecha y duración del simulacro, recursos tecnológicos (Infraestructura Tecnológica, Sistemas de Información, entre otros).

Respuesta: Se adjunta en la carpeta Punto #12 PCN los siguientes documentos

- Carpeta PLANEACION DRP-PAC con evidencias correspondientes a la planeación del simulacro DRP vigencia 2025.
- Documento Minutograma_Caja Honor_PruebaDRP_02y03mayo2025.xlsx se detalla la infraestructura en la hoja Direccionamiento_2025 y las aplicaciones en la hoja Aplicaciones_2025 y en la hoja Directorio se encuentra el listado de participantes.

Información suministrada por OAGRI:

Nombre	Fecha de modificación	Tipo	Tamaño
PLANEACION DRP-PAC	20/10/2025 12:19 p. m.	Carpeta de archivos	
Minutograma_Caja Honor_PruebaDRP_0...	20/10/2025 12:19 p. m.	Documento Adob...	221 KB

Figura 31. Documento Guía para acceso a carpetas.docx - Punto #12 PCN

Fuente: OAGRI – Información contenida en carpeta Punto #12 PCN

Carpeta PLANEACION DRP-PAC: contiene 12 archivos correspondientes a comunicaciones realizadas mediante correo electrónico, en su mayoría emitidas por del profesional de la OAGRI responsable del PCN; en donde informa sobre actividades relacionadas en virtud del desarrollo de las pruebas de continuidad DRP / PAC programadas para primer semestre de 2025, como se muestra a continuación:

Documento suministrado	Descripción
DRP Portal web y Portal financiero.msg	<p>Correo del 23-04-2025:</p> <p>DRP Portal web y Portal financiero</p> <p>Clara Rojas Cruz Gomez Pablo Steven Nieto Chao CC: EDU ARDENDI ANDRÉS MORALES, ISSAC OSAR PARRAGA, Dayi Nairo Gomez W Helo Ig Chica, Buenos tardes</p> <p>Para continuar con la entrega enviada los parámetros de los eventos DRP que se registran levantar los datos en el localizador de los registros de producción estos son la URL. Se recomienda utilizar los mismos IP y los mismos nombres de los registros para que sea un éxito en el PCN.</p> <p>Ver documento Ver foto</p> <p>Portal web Institucional</p>
CLIENTE __ DRP - CAJA HONOR __ SESIÓN TÉCNICA 2.msg	<p>Correo del 21-04-2025:</p> <p>CLIENTE DRP - CAJA HONOR SESIÓN TÉCNICA 2</p> <p>Para el momento de la prueba de continuidad de los servicios de la Caja Honor se realizará una sesión técnica para explicar los procedimientos a seguir y los roles de cada uno de los participantes.</p> <p>Microsoft Teams Ver detalles</p> <p>Únase a la reunión ahora</p> <p>El día: jueves, 20 de abril de 2025 El tiempo: 12:00 PM - 12:30 PM Código de reunión: 9223666666</p> <p>Móstrame un diagnóstico de problemas</p> <p>Clase de capacitación para el desarrollo de pruebas de continuidad de los servicios de la Caja Honor</p> <p>El día: jueves, 20 de abril de 2025 El tiempo: 12:00 PM - 12:30 PM Código de reunión: 9223666666</p> <p>Para registrarse en esta reunión: Clic aquí para ir a la reunión</p>
CLIENTE __ DRP - CAJA HONOR __ SESIÓN TÉCNICA 3.msg	<p>Correo del 24-04-2025</p> <p>CLIENTE DRP - CAJA HONOR SESIÓN TÉCNICA 3</p> <p>Para el momento de la prueba de continuidad de los servicios de la Caja Honor se realizará una sesión técnica para explicar los procedimientos a seguir y los roles de cada uno de los participantes.</p> <p>Microsoft Teams Ver detalles</p> <p>Únase a la reunión ahora</p> <p>El día: jueves, 24 de abril de 2025 El tiempo: 12:00 PM - 12:30 PM Código de reunión: 9223666666</p> <p>Móstrame un diagnóstico de problemas</p> <p>Clase de capacitación para el desarrollo de pruebas de continuidad de los servicios de la Caja Honor</p> <p>El día: jueves, 24 de abril de 2025 El tiempo: 12:00 PM - 12:30 PM Código de reunión: 9223666666</p> <p>Para registrarse en esta reunión: Clic aquí para ir a la reunión</p>
DRP Portal web y Portal financiero.msg	<p>Correo del 23-04-2025:</p> <p>DRP Portal web y Portal financiero</p> <p>Clara Rojas Cruz Gomez Pablo Steven Nieto Chao CC: EDU ARDENDI ANDRÉS MORALES, ISSAC OSAR PARRAGA, Dayi Nairo Gomez W Helo Ig Chica, Buenos tardes</p> <p>Para continuar con la entrega enviada los parámetros de los eventos DRP que se registran levantar los datos en el localizador de los registros de producción estos son la URL. Se recomienda utilizar los mismos IP y los mismos nombres de los registros para que sea un éxito en el PCN.</p> <p>Ver documento Ver foto</p> <p>Portal web Institucional</p> <p>Continuando...</p>

PRUEBA PUNTO ALTERNO DE CONTINUIDAD SÁBADO 03 DE MAYO...msg	Correo del 02-05-2025
RE_CLIENTE __ DRP - CAJA HONOR __ SESIÓN 2.msg	Correo del 11-03-2025: RE CLIENTE 2 DRP - CAJA HONOR 2 SESIÓN 2
RE_CLIENTE __ DRP - CAJA HONOR __ SESIÓN 3.msg	Correo del 21-03-2025:
RE_CLIENTE __ DRP - CAJA HONOR __ SESIÓN 4.msg	Correo del 28-03-2025
RE_CLIENTE __ DRP - CAJA HONOR __ SESIÓN 5.msg	Correo 04-04-2025
RE_CLIENTE __ DRP - CAJA HONOR __ SESIÓN 6.msg	Correo 11-04-2025
RE_SIMULACRO TECNICO - Plan de recuperación de desastres (DRP) _ PAC.msg	Correo 01-05-2025
RV_CLIENTE __ DRP - CAJA HONOR __ SESIÓN TÉCNICA 1.msg	Correo de 21-04-2025
Simulacro DRP - PAC Caja Honor Mayo 2025.msg	Correo de 01-05-2025

Figura 32. Comunicaciones en virtud de desarrollo de continuidad DRP / PAC primer semestre de 2025.
Fuente: OAGRI - Repositorio Documental – Link: 10 Octubre – Carpeta Punto #12 PCN – Subcarpeta PLANEACION DRP-PAC

Lo anterior, refleja la gestión proactiva de la Entidad en la socialización con las partes interesadas respecto a las actividades de pruebas del Plan de Recuperación ante Desastres

(DRP) y del Plan de Continuidad del Negocio (PAC), asegurando la comprensión de objetivos, alcances y resultados. Esta práctica fortalece la resiliencia operativa, fomenta la mitigación de riesgos tecnológicos y garantiza el cumplimiento de las políticas de seguridad de la información, contribuyendo a la mejora continua y a la alineación estratégica entre las áreas involucradas.

Archivo Minutograma Caja Honor PruebaDRP_02y03mayo2025.pdf: contiene el registro del Minutograma de Ejecución de Actividades, correspondiente al formato Código AE3.16-F36, versión 14-feb-2014, suministrado por el proveedor CLARO, en el que se detallan 231 actividades organizadas por fases: Preparación (viernes 02 de mayo de 2025) con 7 actividades; Failover de comunicaciones (viernes 02 de mayo) con 6 actividades; Prueba de conectividad hacia el CAN (viernes 02 de mayo) con 3 actividades; Preparación (sábado 03 de mayo) con 8 actividades; Failover de aplicaciones y bases de datos (sábado 03 de mayo) con 33 actividades; Activación de bases de datos y aplicaciones en ambiente alterno CAN (inicio del RTO) con 71 actividades; Prueba de funcionalidad desde CAN (sábado 03 de mayo) con 6 actividades; Failback (CAN - TRIARA productivo) con 27 actividades; Activación de bases de datos y aplicaciones en TRIARA (retorno a la normalidad) con 64 actividades y Actividades de verificación en TRIARA productivo con 6 actividades.

Asimismo, en el documento Minutograma Caja Honor PruebaDRP_02y03mayo2025.pdf se observa el registro correspondiente al Plan de Retorno cuya duración conforme a los datos consignados en la figura 5, fue de 5 horas y 5 minutos, como se ilustra a continuación:

MINUTOGRAMA PLAN DE RETORNO							
Actividad	Control	Duracion	Inicio	Fin	Descripción	Responsable	Resultado-Encargado
4	C1	0:30	17:10	17:40	Se cancela actividad de DRP.	Lider DRP	
13	C2	0:10	19:40	19:50	Realizar rollback de las actividades 8 - 12	Lider DRP	
18	C3	0:05	20:40	20:45	Se cancela actividad de DRP.	Lider DRP/Redes	
24	C4	0:05	7:55	8:00	Se cancela actividad de DRP.	Lider DRP/Redes	
26	C5	1:15	8:05	9:20	Se cancela actividad de DRP.	Lider DRP/Redes	
111	C6	1:00	14:55	15:55	Realizar rollback de las actividades FailOver donde se diagnostique la falla	Lider DRP/Redes	
112	C7	1:00	14:55	15:55	Realizar rollback de las actividades FileOver donde se diagnostique la falla	Lider DRP/Redes/Virtualización (William Cruz/Almacenamiento)	
187	C8	1:00	21:27	22:27	Realizar rollback de las actividades Failback donde se diagnostique la falla	Lider DRP/Redes	
188	C9	1:00	21:27	22:27	Realizar rollback de las actividades Fileback donde se diagnostique la falla	Lider DRP/Redes/Virtualización (William Cruz/Almacenamiento)	

Figura 33. Comunicaciones en virtud de desarrollo de continuidad DRP / PAC primer semestre de 2025
Fuente: OAGRI - Archivo Minutograma Caja Honor PruebaDRP_02y03mayo2025.pdf

Por su parte, la OFCIN hace énfasis respecto a que la correcta documentación de estas actividades es fundamental en el contexto del desarrollo de simulacros de PCN, DRP y PAC, ya que permite evidenciar la trazabilidad, validar el cumplimiento de los procedimientos y garantizar la mejora continua.

Realizando la siguiente precisión:

Recomendación No. 5.

La OFCIN recomienda a la OAGRI, en coordinación con la OAINF y demás procesos interrelacionados, garantizar que:

- 1) Garantizar que la gestión del minutograma en el marco de las pruebas de continuidad no se limite al registro efectuado por el proveedor sino que la Entidad documente sus propias observaciones y realice la conciliación entre ambos registros antes de emitir el informe final, asegurando consistencia, integridad, transparencia

y confiabilidad en la evaluación del ejercicio, así como la alineación estratégica con la gestión de continuidad.

- 2) Dado que el minutograma constituye un registro oficial del ejercicio de simulacro, es fundamental (considerado una buena práctica) que dicho documento (Minutograma_Caja Honor_PruebaDRP_02y03mayo2025.pdf) incluya la fecha de realización y la firma del responsable, aspectos que otorgan validez y autenticidad del registro, siendo indispensables para auditorías internas y externas, así como para el cumplimiento de estándares internacionales como ISO 22301. Estos datos permiten verificar la correcta ejecución del simulacro, identificar responsables y asegurar que el documento constituye evidencia válida del ejercicio. La ausencia de esta información compromete la confiabilidad del registro y dificulta la gestión documental en procesos de continuidad del negocio y recuperación ante desastres. Lo anterior, toda vez que se evidenció que el documento identificado con Código AE3.16-F36, versión 14-feb-2014, generado por el proveedor CLARO no contiene estos datos esenciales.
- 3) Verificar la correcta paginación del documento, dado que, aunque contiene un total de 25 páginas, tanto la primera como la última presentan la leyenda “Pág. 1 de 1”, lo cual no corresponde con la numeración real y puede generar inconsistencias en la gestión documental. Lo anterior, en tanto que se observó que el archivo en formato PDF presenta un total de 25 páginas; sin embargo, tanto en la primera como en la última página se indica “Página 1 de 1”, lo que genera inconsistencias en la numeración y dificulta la trazabilidad del contenido.

Lo anterior, con el propósito de contribuir al cumplimiento normativo y a la mitigación de riesgos asociados a la vulneración de disposiciones como la Circular Externa 006 de 2025 de la Superintendencia Financiera de Colombia (SFC), Capítulo de Gestión del Riesgo Operacional y de Continuidad del Negocio, Numeral 4.2.2, que exige evidencias documentadas de pruebas y validación de planes de recuperación y continuidad; la Dimensión 5 – Información y Comunicación del Modelo Integrado de Planeación y Gestión (MIPG) V.6 de 2024, que garantiza la gestión documental y el acceso a la información; y estándares internacionales como ISO 22301 (Gestión de Continuidad del Negocio) e ISO/IEC 27001 (Seguridad de la Información). El incumplimiento de estas directrices puede generar riesgos significativos, tales como brechas en la trazabilidad, ausencia de evidencia para auditorías, sanciones regulatorias, pérdida de confianza de los grupos de interés y debilitamiento de la resiliencia organizacional.

15. Evidencias del presupuesto asignado para el PCN vigencia 2025 (Detalle de su ejecución)

Respuesta: Para el periodo auditado (01-Octubre-2024 al 30-Sept-2025, se adjunta la siguiente información correspondiente al presupuesto asignado para el PCN.

Tabla 11. Presupuesto Plan de Continuidad del Negocio – PCN Vigencia 2025

CTO 071/2022 MANOS EXPERTAS PCN	Pagos realizados	Saldo pendiente
\$ 170,635,810	\$ 42,658,953	\$127,976,857

Fuente: OAGRI – Archivo Documento Guía para acceso a carpetas.docx – Punto 13.

Así las cosas, la OFCIN con fecha 12-11-2025 consulto en la herramienta Seven-ERP el resumen del registro presupuestal para el rubro 0231107 Plan de continuidad del negocio, obteniendo la información que a continuación se presenta, en donde se evidencia el presupuesto para la vigencia 2025 y la ejecución de este:

CAJA PROMOTORA DE VIVIENDA MILITAR Y DE POLICIA											
RESUMEN MENSUAL DE REGISTROS PRESUPUESTALES POR RUBRO											
AÑO 2025 - MES INICIAL 1.- MES FINAL 11											
T Op.	Número	Fecha	RUBRO	Tercero	Descripción	Est.	Clase	Valor	Saldo		
RUBRO	0231107	2025	1	0231107	800153993 COMUNICACION CELULAR S.A	Otrosí 1 Cto.71-2022 - Servicio de Manos Expertas PARA PCN - EL ARRENDAMIENTO DE INSTALACIONES PARA DATACENTER PRINCIPAL, DOTADA CON SERVICIOS DE COMUNICACIONES AL TERCERO S. COPORTE ADMINISTRACION DE INFRAESTRUCTURA TECNOLÓGICA, INCLUYENDO LOS SERVICIOS DE MANOS EXPERTAS PARA DE Radicado: 116-01-2024031900446	A	COM	170.635.810.00	127.976.857.00	
TOTAL REGISTROS									170,635,810.00	127,976,857.00	
TOTAL RUBRO									0231107	170,635,810.00	127,976,857.00

Figura 34. Presupuesto asignado y ejecutado Plan de Continuidad vigencia 2025 Fuente: Herramienta Seven-ERP – consultado 12-11-2025

Como se observa en la figura 34, para el Plan de Continuidad del Negocio se asignó el Rubro presupuestal **0231107** con un presupuesto de **\$170.635.810**, en donde a la fecha de la presente consulta se observó un saldo de **\$127.976.857**, lo que indica que se han realizado pagos por valor de **\$42,658,953**, tal como se observa en la siguiente figura 34, en donde el pago se registra a nombre del Tercero Comunicación Celular S.A. COMCEL S.A., así:

Valor	Tipo Op	Nombre	Tipo Operación	Tercero	Nombre Tercero	Número	Fecha	Año	Mes	Día	Tipo de	Descripción	Est
170636000	3001	SOLICITUD PRESUPUESTO GASTOS	0	TERCERO NULO	TERCERO NULO	48	02/01/2025	2025	1	2	S	DESAGREGACION PRESUPUESTO VIGENCIA 2024 SEGUN RESOLUCION NA TA	A
170636000	3002	APROBACION PRESUPUESTO GASTOS	0	TERCERO NULO	TERCERO NULO	48	02/01/2025	2025	1	2	A	DESAGREGACION PRESUPUESTO VIGENCIA 2025 SEGUN RESOLUCION NA TA	A
170636810	3003	CUENTAS POR PAGAR CDPS	800153993	COMUNICACION CELULAR S.A COMCEL S.A	COMUNICACION CELULAR S.A COMCEL S.A	36	02/01/2025	2025	1	2	D	Otrosí 1 Cto.71-2022 - Servicio de Manos Expertas PARA PCN - EL ARRENDAMIE U	A
170636810	3004	CUENTAS POR PAGAR CDPS	800153993	COMUNICACION CELULAR S.A COMCEL S.A	COMUNICACION CELULAR S.A COMCEL S.A	36	02/01/2025	2025	1	2	F	Otrosí 1 Cto.71-2022 - Servicio de Manos Expertas PARA PCN - EL ARRENDAMIE U	A
42559953	3017	OBLIGACION PRESUPUESTAL	800153993	COMUNICACION CELULAR S.A COMCEL S.A	COMUNICACION CELULAR S.A COMCEL S.A	101466	30/07/2025	2025	7	30	0	Cto.71-2022-EL ARRENDAMIENTO DE INSTALACIONES PARA DATACENTER F U	A
42559953	2980	PAGOS TRANSFERENCIA (CREDITO)	800153993	COMUNICACION CELULAR S.A COMCEL S.A	COMUNICACION CELULAR S.A COMCEL S.A	103412	31/07/2025	2025	7	31	6	PAGO - Cto.71-2022-EL ARRENDAMIENTO DE INSTALACIONES PARA DATACE A	A

Figura 35. Movimiento Presupuestal Plan de Continuidad del Negocio vigencia 2025 Fuente. Aplicativo SEVEN-ERP

Igualmente, con fecha 13-11-2025 la OFCIN consultó el gestor documental Dodo Docs el flujo 127-EXPEDIENTE CONTRATOS-PROVEEDORES, observando el contrato 71-2022 y Otrosí No. 1 al citado contrato, con los siguientes datos:

Contrato 71-2022		Otrosí 1 Contrato 71-2022	
13	Plazo del contrato:	30 meses.	Adición del presente otrosí:
13	Lugar de ejecución del contrato:	El Proveedor prestará el servicio objeto del contrato en las instalaciones de la Caja Promotora de Vivienda Militar y de Policía, ubicada en la Carrera 54 No. 26 – 54 CAN de Bogotá, D.C y en las instalaciones del proveedor.	\$2.950.817.190 COP IVA incluido, compuesto por: 1. Servicio Datacenter: DOS MIL SETECIENTOS OCHENTA MILLONES CIENTO OCHENTA Y UN MIL TRESCIENTOS OCHENTA PESOS M/CTE (\$2.780.181.380). 2. Servicio de Manos Expertas: CIENTO SETENTA MILLONES SEISCIENTOS TREINTA Y CINCO MIL OCHOCIENTOS DIEZ PESOS M/CTE (\$170.635.810).
14	Valor del contrato:	\$ 2.950.817.190 COP IVA incluido de acuerdo con las ofertas allegadas. El presente contrato está compuesto por: 1. Servicio Datacenter: DOS MIL SETECIENTOS OCHENTA MILLONES CIENTO OCHENTA Y UN MIL TRESCIENTOS OCHENTA PESOS M/CTE (\$2.780.181.380). 2. Servicio de Manos Expertas: CIENTO SETENTA MILLONES SEISCIENTOS TREINTA Y CINCO MIL OCHOCIENTOS DIEZ PESOS M/CTE (\$170.635.810).	Prórroga del presente otrosí: 30 meses
			Número de disponibilidad presupuestal para la Adición del presente otrosí: 36304 del 4 de abril de 2024

Figura 36. Contrato 71-2022 y Otrosí No. 1 Cto. 71-2022 – Proveedor COMUNICACIÓN CELULAR S.A. COMCEL S.A.

Fuente: Gestor Documental Dodo Docs - flujo 127-Expediente Contratos-Proveedores

La OFCIN hace especial énfasis respecto a que la adecuada ejecución del presupuesto asignado al Plan de Continuidad del Negocio (PCN) es de vital importancia para garantizar la capacidad de la Entidad de responder de manera efectiva ante cualquier contingencia, asegurando la continuidad operativa y la protección de sus recursos estratégicos y reputación institucional. Asimismo, permite dar cumplimiento a los requerimientos normativos aplicables, fortaleciendo la resiliencia organizacional frente a interrupciones o

escenarios de crisis y mitigando impactos en procesos críticos. Un PCN debidamente financiado posibilita la implementación de medidas orientadas a salvaguardar activos esenciales como infraestructura, tecnologías de información y capital humano, evidenciando el compromiso con la gestión del riesgo y la sostenibilidad operativa, lo que genera confianza entre afiliados, clientes, colaboradores, proveedores y demás partes interesadas.

16. Registro de eventos de riesgo ocurridos durante el periodo objeto de la presente auditoría (01-Octubre-2024 al 30-Sept-2025) y documentados en VIGIA o herramienta tecnológica dispuesta para tal efecto.

Respuesta: Para el periodo auditado (01-Octubre-2024 al 30-Sept-2025) no se registró ningún evento de riesgo correspondiente al PCN.

Es de anotar que este tema fue evaluado por el auditor de Riesgo Operacional en el numeral 1.2. del presente informe.

17. Relación de personal con trabajo en casa o remoto durante el periodo objeto de la presente auditoría (01-Octubre-2024 al 30-Sept-2025).

Respuesta: Se adjunta el documento Excel: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #15" del Excel en donde se detalla el listado del personal con trabajo en casa durante el periodo auditado (01-Octubre-2024 al 30-Sept-2025).

Revisado la hoja electrónica denominada Punto #15 del archivo Requerimiento de Información PCN PAC Y DRP.xlsx se observa la siguiente información:

Figura 37. Relación de personal con trabajo en casa o remoto periodo (01-Octubre-2024 al 30-Sept-2025)
Fuente: OAGRI - Archivo Requerimiento de Información PCN PAC Y DRP.xlsx - Punto #15

Como se ilustra en la Figura 37, se observa un total de 35 colaboradores con trabajo en casa correspondiente a la vigencia 2025 y 10 colaboradores en 2024. Así las cosas, mantener actualizado el inventario de colaboradores con trabajo en casa o remoto debidamente autorizado es fundamental para garantizar la trazabilidad, el cumplimiento normativo y la correcta asignación de recursos tecnológicos y de seguridad por lo que la OFCIN recomienda:

Recomendación No. 6.

La OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados, establecer un proceso de actualización periódica (trimestral) del inventario de colaboradores con trabajo en casa o remoto, utilizando herramientas de gestión centralizada que permitan validar la autorización vigente y la correlación con los recursos asignados (equipos, accesos y licencias). Adicionalmente, se sugiere implementar indicadores de variación anual para anticipar necesidades tecnológicas y de seguridad alineados con estándares de ISO 27001, incluyendo autenticación multifactor, cifrado, VPN segura y gestión del ciclo de vida de activos, considerando el incremento observado en la vigencia 2025 (35 colaboradores) frente a 2024 (10 colaboradores). Este control preventivo contribuye a la continuidad operativa, la mitigación de riesgos y la optimización de costos asociados a la modalidad remota, información que es fundamental para la toma de decisiones por parte de la Entidad respecto de la implementación de modalidades laborales como trabajo remoto o híbrido conforme a la normativa vigente.

18. Relación de VPN implementadas en la Entidad durante el periodo evaluado (01-10-2024 al 30-09-2025), adjuntando el respectivo formato de Acuerdo de Confidencialidad para uso de dispositivos, redes sociales y trabajo a distancia.

Respuesta: Se adjunta lo siguiente en la carpeta Punto #16 PCN:

- Reporte Solicitudes VPN FLUJO 395 (01-Octubre-2024 al 30-Sept-2025).xlsx con el personal que realizo la respectiva solicitud mediante el flujo 395 vía Dodo-docs cuyo radicado se puede consultar en la herramienta Dodo-docs.

Tras el análisis de la información registrada en el archivo Reporte Solicitudes VPN FLUJO 395 (01-Octubre-2024 al 30-Sept-2025).xlsx, se observó un total de 783 registros de VPN implementadas durante el periodo objeto del presente ejercicio auditor, como se muestra en la siguiente tabla:

Tabla 12. Relación flujos documentales 395 – Implementación VPN

Dependencia	Tipo de equipo	Cant.
ALMACÉN	Portátil	4
ÁREA DE ASUNTOS GERENCIALES Y PROTOCOLO	Portátil	1
ÁREA DE ATENCIÓN CONSUMIDOR FINANCIERO	Equipo de escritorio	2
	Portátil	16
ÁREA DE COMPRAS Y CONTRATACIÓN	Equipo de escritorio	2
	Portátil	18
ÁREA DE COMUNICACIONES	Equipo de escritorio	5
	Portátil	3
ÁREA DE CREDITO Y CARTERA	Portátil	2
ÁREA DE FINANZAS	Portátil	3
ÁREA DE GESTIÓN DOCUMENTAL	Portátil	2
ÁREA DE OPERACIONES - BACK OFFICE	Portátil	4
ÁREA DE SERVICIOS ADMINISTRATIVOS	Equipo de escritorio	1
	Portátil	11
ÁREA DE TALENTO HUMANO	Equipo de escritorio	1
	Portátil	19
ÁREA DE TESORERÍA - FRONT OFFICE	Portátil	2
ÁREA DE VIVIENDA	Portátil	5
ÁREA SERVICIO AL AFILIADO	Portátil	16
GERENCIA GENERAL	Portátil	4
GRUPO ADMINISTRACIÓN CUENTAS INDIVIDUALES Y CESANTÍAS	Equipo de escritorio	4
	Portátil	3
GRUPO ADMINISTRACIÓN DE CRÉDITO Y CARTERA	Portátil	5
GRUPO APOYO JURÍDICO	Portátil	8
GRUPO APOYO TÉCNICO	Portátil	4

Dependencia	Tipo de equipo	Cant.
GRUPO ASUNTOS JURÍDICOS DE OPERACIONES	Equipo de escritorio	4
	Portátil	3
GRUPO ATENCIÓN VIRTUAL AL AFILIADO	Celular	2
	Portátil	21
GRUPO DE CONTABILIDAD	Portátil	38
GRUPO DE MERCADEO	Equipo de escritorio	4
	Portátil	25
GRUPO DE NEGOCIACIÓN	Portátil	5
GRUPO DE PAGADURÍA	Portátil	13
GRUPO DE PRESUPUESTO	Equipo de escritorio	1
	Portátil	13
GRUPO DE SERVICIOS GENERALES	Portátil	12
GRUPO FONDO DE SOLIDARIDAD Y ATENCIÓN VETERANOS	Equipo de escritorio	1
	Portátil	12
GRUPO GESTIÓN DE NOVEDADES	Equipo de escritorio	2
	Portátil	6
GRUPO GESTIÓN Y APOYO AL SERVICIO	Portátil	10
GRUPO ORIGINACIÓN DE CRÉDITO	Portátil	5
GRUPO VERIFICACIÓN DE IDENTIFICACIÓN SEGURIDAD DOCUMENTAL Y PREVENCIÓN	Portátil	1
OFICINA ASESORA DE GESTIÓN DEL RIESGO - MIDDLE OFFICE	Equipo de escritorio	4
	Portátil	17
OFICINA ASESORA DE INFORMÁTICA	Celular	1
	Equipo de escritorio	36
OFICINA ASESORA DE PLANEACIÓN	Portátil	54
	Portátil	7
OFICINA ASESORA JURÍDICA	Equipo de escritorio	1
OFICINA DE CONTROL INTERNO	Portátil	2
	Equipo de escritorio	1
OFICINA DE ENLACE DE LA ARMADA NACIONAL	Portátil	38
	Portátil	17
OFICINA DE ENLACE DE LA FUERZA AÉREA	Portátil	3
OFICINA DE ENLACE DE LA POLICÍA NACIONAL	Portátil	16
OFICINA DE ENLACE DEL EJÉRCITO	Portátil	23
PUNTO DE ATENCIÓN AL AFILIADO BARRANQUILLA	Portátil	24
PUNTO DE ATENCIÓN AL AFILIADO BUCARAMANGA	Equipo de escritorio	1
	Portátil	22
PUNTO DE ATENCIÓN AL AFILIADO CALI	Celular	2
	Equipo de escritorio	2
PUNTO DE ATENCIÓN AL AFILIADO FLORENCIA	Portátil	48
	Equipo de escritorio	1
PUNTO DE ATENCIÓN AL AFILIADO IBAGUÉ	Portátil	19
	Portátil	38
PUNTO DE ATENCIÓN AL AFILIADO MEDELLÍN	Celular	1
	Equipo de escritorio	3
PUNTO DE ATENCIÓN MOVIL BOGOTÁ	Portátil	43
	Portátil	2
PUNTO DE ATENCIÓN MOVIL BOGOTÁ	Portátil	1
PUNTO DE ATENCIÓN MOVIL NACIONAL	Portátil	4
SEDE PRINCIPAL - BOGOTÁ	Portátil	12
SUBGERENCIA ADMINISTRATIVA	Portátil	2
SUBGERENCIA DE ATENCIÓN AL AFILIADO Y OPERACIONES	Portátil	4
SUBGERENCIA FINANCIERA	Equipo de escritorio	1
	Portátil	7
UCODI JUZGAMIENTO	Portátil	1
UNIDAD DE CONTROL DISCIPLINARIO INTERNO	Portátil	2
Total general		783

Fuente: OAGRI – Archivo Reporte Solicitudes VPN FLUJO 395 (01-Octubre-2024 al 30-Sept-2025).xlsx

Por su parte, la OFCIN procedió a realizar cruce de información entre los datos contenidos en los archivos Requerimiento de Información PCN PAC Y DRP.xlsx - Punto #15 Vs Reporte Solicitudes VPN FLUJO 395 (01-Octubre-2024 al 30-Sept-2025).xlsx, en donde como resultado, se identificó que los registros del personal que se detallan a continuación no presentan correspondencia entre ambos reportes, con las siguientes observaciones:

Figura 38. Relación de personal con trabajo en casa – Inconsistencias

Fuente: Cruce de información archivos Requerimiento de Información PCN PAC Y DRP.xlsx – Punto #15 Vs Reporte Solicitudes VPN FLUJO 395 (01-Octubre-2024 al 30-Sept-2025).xlsx

En consecuencia, la OFCIN hace especial énfasis respecto a que es fundamental mantener un estricto seguimiento al inventario del personal que trabaja en casa y cuenta con VPN implementada, asegurando que el formato de solicitud respectivo se encuentre actualizado. Este control permite garantizar la trazabilidad de los equipos asignados, prevenir riesgos de seguridad informática, evitar accesos no autorizados y cumplir con las políticas corporativas de protección de información. Además, una gestión rigurosa del inventario facilita la identificación de incidencias, la planificación de mantenimientos y la toma de decisiones oportunas ante cambios en la infraestructura tecnológica, toda vez que como se indicó en la Figura 38, los registros que no cruzaron corresponden a errores en el documento de identidad y un colaborador que actualmente se encuentra en licencia de maternidad.

Punto Alternativo de Continuidad del Negocio – PAC

1. Manual operativo del PAC

Respuesta: Se adjunta el documento GR-NA-GU-005 Guía Operación PAC v15 en la carpeta Punto #1 PAC.

Una vez la OFCIN verificó el documento GR-NA.GU-005 Guía Operación PAC v15, se identificó:

3. Procesos Críticos en Caja Honor:

Tabla 13. Procesos Críticos en Caja Honor

No.	Proceso	Concepto
1	Gestión del Riesgo	La gestión del riesgo es crítica debido a la necesidad de controlar y monitorear aspectos como SARLAFT (Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo), SIAR (Sistema Integral de Administración de Riesgos), Ciberseguridad y Seguridad de la información. Estos controles son esenciales para proteger la integridad y continuidad de las operaciones.
2	Gestión Informática	Los procesos informáticos son el soporte fundamental de todos los servicios de la entidad. Sin una gestión informática eficiente, la entidad no podría operar ni prestar servicios a sus usuarios.
3	Gestión del Trámite	Mantener la operación activa en todos los puntos de atención es vital para la prestación del servicio a nivel nacional. El incumplimiento de los tiempos de MTPD (Periodo de tiempo máximo tolerable de interrupción), podría resultar en sanciones legales y económicas, afectando la reputación y la operatividad de la entidad.
4	Gestión de Tesorería	La gestión de tesorería es crucial para coordinar la rentabilidad, monitorear los mercados financieros, estructurar el portafolio de inversiones y proyectar el flujo de caja. El incumplimiento de los tiempos establecidos puede causar pérdidas económicas significativas
5	Administración de Cuentas	El manejo adecuado de los subsidios y la gestión de las novedades de las cuentas de los afiliados es esencial para evitar sanciones legales y jurídicas. Una administración ineficiente podría tener consecuencias graves para la entidad y sus afiliados.

Fuente: GR-NA-GU-005 Guía Operación PAC v15- Pág. 4

Tal como se evidencia en la Tabla 13, de los 18 procesos que conforman la estructura organizacional de Caja Honor, se identificaron como críticos cinco (5) procesos, de los cuales, dos corresponden a procesos estratégicos: Gestión del Riesgo y Gestión Informática; y tres a procesos misionales: Gestión del Trámite, Gestión de Tesorería y Administración de Cuentas. Acorde a la información documentada en la guía en mención, dicha clasificación se fundamenta en criterios como el impacto potencial sobre la continuidad del negocio, la dependencia tecnológica y la criticidad en la prestación de los servicios institucionales.

En consecuencia, y considerando que la Entidad ha adoptado el trabajo a distancia como estrategia dentro del Punto Alterno de Continuidad – PAC, cuyo enfoque es garantizar la operación ante eventos que comprometan el funcionamiento normal, la OFCIN precisa:

Recomendación No. 7.

La OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados, incorporar en la guía GR-GU-005 “*GUÍA DE OPERACIÓN PUNTO ALTERNO DE CONTINUIDAD – PAC, V16 – 31-10-2025*”, la normativa aplicable para la modalidad de teletrabajo (mixta, híbrida, autónoma o móvil), como lo es la Ley 1221 de 2008, el Decreto 884 de 2012 (compilado en el Decreto 1072 de 2015) y el Decreto 1227 de 2022; además de la Normativa de gestión de continuidad NTC-ISO/IEC 22301, que establece los lineamientos para la gestión de continuidad del negocio, definiendo procedimientos, roles, comités y documentación requerida para la activación del PAC. Lo anterior, toda vez que la incorporación de la normativa citada es esencial porque asegura que la estrategia de trabajo a distancia y la activación del Punto Alterno de Continuidad (PAC) se realicen bajo un marco legal y técnico que garantice el cumplimiento regulatorio, la protección de derechos laborales y la alineación con estándares internacionales. Esto permite minimizar riesgos como sanciones por incumplimiento normativo, vulnerabilidades operativas y tecnológicas, pérdida de información, descoordinación en la activación del PAC, afectación de la continuidad del negocio y exposición a riesgos reputacionales y financieros; dando cumplimiento a lo estipulado en la Circular Externa 006 de 2025 Parte I – Título I, Capítulo I: Organización y Numeral 1.2 – Documentación requerida y Numeral 1.3 – Especificidad en constitución de entidades; adicionalmente con MIPG v6 de 2024, Dimensión 1. Dirección estratégica y planeación que formaliza la estrategia de trabajo remoto dentro del PAC, alineada con el direccionamiento institucional y Dimensión 5 – Información y Comunicación. Lo anterior, en aras de fortalecer la gobernanza, la trazabilidad y la resiliencia institucional frente a eventos críticos.

Por otra parte, es de precisar que, considerando la decisión institucional de migrar la documentación controlada desde la herramienta ISOLUCION hacia la plataforma SVE, se informa que el documento GR-NA-GU-005 *Guía Operación PAC v15*, suministrado por el proceso auditado, se encontraba en el repositorio ISOLUCION con el código GR-NA-GU-005. No obstante, dicho documento fue actualizado en la plataforma SVE bajo el código GR-GU-005, versión 016, con fecha 31-10-2025.

2. Procedimientos detallados para la activación del PAC, Plan de transición entre sede principal y PAC, Registro de Pruebas, Evaluación de riesgos específicos del PAC.

Respuesta: Se adjunta el siguiente documento en la carpeta Punto #2 PAC:

- Carpeta PLANEACION PRUEBA PAC con los documentos pertinentes.

Se observa la siguiente documentación suministrada por la OAGRI en le repositorio de información dispuesto para la presente auditoría, así:

Nombre	Fecha de modificación
Correos	20/10/2025 12:19 p. m.
Análisis DOFA del Punto Alterno de Continuidad.pdf	20/10/2025 12:19 p. m.
INFORME PRUEBA PAC 22 DE MAYO 2025.pdf	20/10/2025 12:19 p. m.
MEMORANDO PAC 2025.docx	20/10/2025 12:19 p. m.
PREPARACION PRUEBA PAC - Informe de asistencia 5-19-25.csv	20/10/2025 12:19 p. m.
SIMULACRO TECNICO - Plan de recuperación de desastres (DRP) _ PAC - Informe de asistencia 4-30-25.csv	20/10/2025 12:19 p. m.

Figura 39. Procedimientos detallados para la activación del PAC

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre – Carpeta Punto #2 PAC

Carpeta Correos: contiene 4 emails, así:

- Archivo PERSONAL PRUEBA PAC_.msg: correspondiente a mensaje del 21-05-2025 emanado del profesional de la OAGRI responsable del PAC informando a Talento Humano el listado del personal que el jueves 22/05/2025 se encontrará ejecutando sus labores desde casa, quienes realizaron el flujo 395 para la solicitud de la VPN y movilización de equipo con el fin de realizar la conexión.
- Archivo PREPARACION PRUEBA PAC.msg: correspondiente al mensaje del 16-05-2025 mediante el cual el profesional de la OAGRI responsable del PAC, convocó reunión respecto a “coordinaciones previas a la prueba del PAC que se llevará a cabo el jueves 22 de mayo”
- Archivo PRUEBA PAC 22 DE MAYO 2025.msg: correspondiente al mensaje del 14-05-2025 mediante el cual el profesional de la OAGRI responsable del PAC, realizó la invitación para participar en la prueba del PAC que se llevará a cabo el **jueves 22 de mayo**.
- Archivo RECEPCIÓN DE INFORMES PAC 2025.msg: correspondiente al mensaje del 26-05-2025 mediante el cual el profesional de la OAGRI responsable del PAC “la fecha para el envío del informe por parte de cada uno de ustedes, quienes **participaron** en la prueba del PAC, es el **martes 27/05/2025**.”

*Este documento que les solicito es un informe de las actividades detalladas que cada uno realizo el día de la prueba del PAC con las evidencias respectivas, adicional al **Excel** que se les envió para el registro del acceso a los aplicativos.*

*De igual manera, amablemente les solicito a todos, diligenciar el siguiente **formulario** que será de gran ayuda para futuras planeaciones de esta prueba*

<https://forms.office.com/Pages/ResponsePage.aspx?id=UvKHjzH2mkWd3796nRuEo3JAyexisfFGkemClktTgqJURTEwOV04VzZONFVRN0FaWDZHVVR0U1FDTy4U>

- Archivo SEGUNDA PRUEBA PAC 22 DE MAYO.msg: correspondiente al mensaje del 14-05-2025 mediante el cual el profesional de la OAGRI responsable del PAC, realizó la invitación para participar en la prueba del PAC que se llevará a cabo el **jueves 22 de mayo**.
- Archivo Análisis DOFA del Punto Alterno de Continuidad.pdf: contiene la siguiente matriz:

Análisis DOFA del Punto Alterno de Continuidad

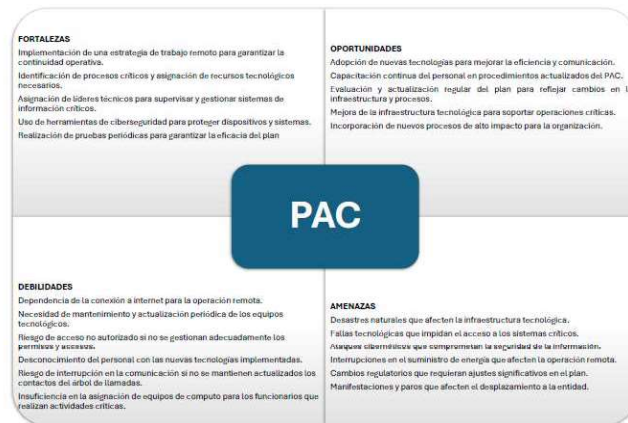


Figura 40. Análisis DOFA PAC Caja Honor
Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre - Carpeta Punto #2 PAC – Archivo Análisis DOFA del Punto Alterno de Continuidad.pdf

Una vez la OFCIN realizó el análisis de la información contenida en la matriz presentada en la Figura 40, se observó que el PAC cuenta con una estructura sólida gracias a sus fortalezas en trabajo remoto, identificación de procesos críticos y medidas de ciberseguridad, lo que le permite responder ante contingencias. Sin embargo, la dependencia tecnológica y la falta de actualización del personal y equipos representan riesgos internos que pueden afectar la continuidad operativa. Externamente, las amenazas como desastres naturales, ataques cibernéticos y cambios regulatorios exigen una preparación constante para evitar interrupciones significativas.

Por su parte, las oportunidades identificadas, como la adopción de nuevas tecnologías y la capacitación continua, son claves para reducir vulnerabilidades y aumentar la resiliencia. Si se aprovechan adecuadamente, permitirán transformar las debilidades en ventajas competitivas y mitigar el impacto de las amenazas.

- Archivo INFORME PRUEBA PAC 22 DE MAYO 2025.pdf: documento titulado **INFORME**

EJECUCIÓN PRUEBA PAC 22 DE MAYO 2025 de fecha 30/05/2025, cuyo objetivo general registra *“El objetivo principal de esta prueba es realizar la validación, funcionamiento, y eficacia de la estrategia de trabajo remoto para garantizar la continuidad de las actividades críticas de la Entidad, ante escenarios que afecten la operación o que impidan el acceso*

físico a las instalaciones, de igual manera se documentan los resultados de la prueba del Punto Alterno de Continuidad (PAC) realizada por parte de los funcionarios pertenecientes a esta estrategia de continuidad del negocio”, contiene 10 folios firmado por el ingeniero responsable del PCN, sin embargo, no se evidencia la firma correspondiente a la revisión por parte del Jefe de la OAGRI, situación importante dado que la validación por dicha instancia es requisito para garantizar la conformidad y el cumplimiento de los lineamientos establecidos.

Tras el análisis del documento realizado por la OFCIN, se observa que en la prueba del Punto Alterno de Continuidad (PAC) se validó la conectividad segura mediante VPN y RDP, lo que garantiza la continuidad operativa ante contingencias. La participación activa de los funcionarios y la coordinación técnica fueron factores críticos para el éxito, evidenciando la importancia de mantener procesos claros y comunicación efectiva. Para fortalecer esta estrategia, se recomienda priorizar la integración completa de aplicativos como LSI y Bloomberg a través de VPN, eliminando dependencias de acceso remoto que puedan generar vulnerabilidades o retrasos. Asimismo, se sugiere mantener el enfoque por fases en la implementación del incremento de personal, asegurando que la capacitación y asignación se realicen con base en criterios objetivos de carga operativa y competencias. Finalmente, es clave establecer un plan de pruebas periódicas que incluya validación funcional de todos los aplicativos y monitoreo de desempeño, garantizando la mejora continua y la resiliencia del negocio.

- Archivo MEMORANDO PAC 2025.docx: contiene 4 folios mediante el cual la OAGRI informa a las diferentes áreas y Grupos de la Entidad respecto de la Ejecución prueba Punto Alterno de Continuidad, con programación de la realización de una prueba técnica el jueves 22 de mayo de 2025 dentro de la jornada laboral. Se observa documento sin firma de quien lo emite, aspecto fundamental para asegurar su autenticidad y responsabilidad, evitando dudas sobre su origen y garantizando respaldo legal y administrativo dentro de la Entidad, además de que puede llegar a afectar la transparencia y la confianza en los procesos internos.
- PREPARACION PRUEBA PAC – Informe de asistencia 5-19-25.csv: correspondiente a la lista de asistencia de 23 participantes a la actividad titulada PREPARACION PRUEBA PAC con Hora de Inicio: 5/19/25, 9:47:42 AM y Hora de finalización: 5/19/25, 10:30:04 AM.
- SIMULACRO TECNICO – Plan de recuperación de desastres (DRP) _ PAC – Informe de asistencia 4-30-25.csv: correspondiente a la lista de asistencia de 30 participantes a la actividad titulada SIMULACRO TECNICO – Plan de recuperación de desastres (DRP) / PAC con Hora de inicio: 4/30/25, 3:56:02 PM y Hora de finalización: 4/30/25, 5:23:41 PM.

Tras la revisión de los documentos “PREPARACIÓN PRUEBA PAC – Informe de asistencia 19-05-2025.csv” y “SIMULACRO TÉCNICO – Plan de Recuperación de Desastres (DRP) _ PAC – Informe de asistencia 30-04-2025.csv”, se identificó una inconsistencia en la secuencia cronológica de las actividades, dado que la preparación del simulacro figura con fecha 19/05/2025, mientras que la ejecución aparece registrada el 30/04/2025, lo que

resulta incongruente con el orden lógico del proceso. Esta incongruencia podría deberse a errores en la documentación o en la carga de datos, afectando la trazabilidad y confiabilidad del informe; por lo tanto, se recomienda validar las fechas reales y corregir los registros para garantizar coherencia y consistencia en futuras pruebas del Plan de Recuperación ante Desastres (DRP).

3. Relación del recurso humano designado para tal efecto en cada uno de los procesos críticos de la Entidad, indicando datos tales como: Nombre del Proceso Crítico, Identificación del colaborador, Nombres y Apellidos, Área o Dependencia, Cargo, Número de Contacto y Correo Electrónico.

Respuesta: Se adjunta el documento: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #3 PAC" del Excel.

Tras el análisis de la información contenida en el archivo Requerimiento de Información PCN PAC Y DRP.xlsx, Hoja Electrónica Punto #3 PAC, se observó un total de 47 colaboradores distribuidos en los procesos que a continuación se presentan:

Tabla 14. Relación Personal PAC

PROCESO	CANT.
AOPER -BACK OFFICE	3
ARACF	6
ARTES	2
ASERA	1
GAJUO	3
GAVIA	4
GCICE	5
GENOV	2
GGASE	4
GUCON	1
GUPAG	3
OAGRI	6
OAINF	5
PUNTOS MOVILES	2
Total general	47

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre – Archivo Requerimiento de Información PCN PAC Y DRP.xlsx , Hoja Electrónica Punto #3 PAC

Es de anotar que mayor detalle de los campos reportados en el archivo Requerimiento de Información PCN PAC Y DRP.xlsx, Hoja Electrónica Punto #3 PAC se puede observar en el siguiente documento :



Requerimiento de Información PCN PA

Teniendo en cuenta la información relacionada en el archivo Requerimiento de Información PCN PAC Y DRP.xlsx, Hoja Electrónica Punto #3 PAC, en donde se evidencian los 17

equipos que se relaciona a continuación, que se encuentran pendientes de la actualización del sistemas Operativo:

Tabla 15. Relación Equipos de Cómputo sin actualización del Sistema Operativo

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre – Archivo Requerimiento de Información PCN PAC Y DRP.xlsx , Hoja Electrónica Punto #3 PAC

Asimismo, en la Oficina de Control Interno, existen los siguientes equipos de cómputo que requieren la actualización del sistema operativo, pasando de Windows 10 a Windows 11, conforme a los lineamientos establecidos, así:

Tabla 16. Relación Equipos de Cómputo OFCIN. Pendiente de actualización del Sistema Operativo

Fuente: Revisión OFCIN - Diseño Propio – consultado 19-11-2025

La OFCIN hace especial énfasis respecto de la actualización del SO en los equipos de la Entidad y en especial las máquinas dispuestas para temas de Continuidad del Negocio, en tanto que, actualizar de **Windows 10 a Windows 11** es esencial para garantizar seguridad, productividad y continuidad operativa, pues, Windows 10 dejó de recibir soporte en octubre

de 2025, lo que incrementa riesgos de vulnerabilidad y falta de parches críticos; por su parte, Windows 11 ofrece mejoras como TPM 2.0, autenticación biométrica y cifrado avanzado, además de optimización para hardware moderno y una interfaz más intuitiva que potencia la productividad. Mantener sistemas actualizados evita obsolescencia y asegura compatibilidad con aplicaciones y servicios estratégicos.

En materia de Continuidad del Negocio, la actualización a Windows 11 contribuye significativamente a la reducción de riesgos operacional, incrementa la resiliencia frente a fallos y optimiza los procesos de recuperación en entornos híbridos y en la nube. Además, asegura el cumplimiento de normativas internacionales como ISO 22301, garantizando soporte técnico adecuado en escenarios de contingencia. Considerando que el soporte oficial para Windows 10 ha finalizado y que en la Entidad aún persiste un número considerable de equipos sin actualizar, la OFCIN precisa:

Oportunidad de Mejora Correctiva No. 6.

La OFCIN recomienda a la OAINF en coordinación con la OAGRI y demás procesos interrelacionados implementar un cronograma acelerado y estructurado por fases para culminar el proceso de actualización del sistema operativo en los equipos de Caja Honor, para lo cual se sugiere la inclusión de aspectos tales como los que a continuación se relacionan:

- Fase 1 (inmediata): Inventario completo y pruebas de compatibilidad en todos los equipos pendientes.
- Fase 2 (próximos 2 meses): Migración prioritaria de equipos críticos y capacitación del personal.
- Fase 3 (máximo 3 meses): Finalizar la actualización del 100% de los equipos, validando el Plan de Continuidad y asegurando la operación sin interrupciones.

Asimismo, realizar la Actualización de la política interna incluyendo la obligación de mantener soporte activo, definir plazos máximos de migración y detallar roles de control y seguimiento; además de realizar la Capacitación del personal de TI y auditoría interna sobre la importancia del ciclo de vida del software operativo, el riesgo regulatorio asociado a sistemas sin soporte, y los procedimientos de continuidad del negocio; acciones que permitirán cumplir con la normativa vigente, fortalecer la ciberseguridad y garantizar la continuidad operativa de la Entidad frente a incidentes tecnológicos.

Lo anterior, toda vez que se identificó que la Entidad mantiene un número significativo de equipos (22) aun operando con Windows 10, sistema operativo que perdió soporte oficial el 14 de octubre de 2025, situación que representa un incumplimiento de la política interna de actualización que exige soporte activo y parches al día y de estándares internacionales de continuidad operativa y ciberseguridad, tales como ISO 22301 (cláusulas 6 y 7 relativas a la planificación del BCMS - Sistema de Gestión de Continuidad del Negocio, gestión de riesgos, asignación de recursos y mantenimiento del sistema y la cláusula 8, que exige controles operacionales para asegurar la continuidad frente a incidentes tecnológicos críticos al no aplicar mitigaciones para sistemas obsoletos en un entorno de continuidad del negocio), además del incumplimiento de la norma ISO/IEC 27001:2022 numerales A.8.8 (Vulnerabilidades), al no identificar ni corregir vulnerabilidades técnicas; A.5.10 (Malware), al dejar los sistemas expuestos a amenazas conocidas; A.8.32 (Gestión de cambios), por no implementar cambios formales en sistemas operativos; Cláusula 8 (Operación), al omitir la ejecución de controles operacionales esenciales; y Cláusula 10 (Mejora), al no garantizar

la actualización continua del ISMS - Sistema de Gestión de Seguridad de la Información - SGSI. En consecuencia, se observó el RSI008 - ERROR EN EL USO, CSI045 - FALTA DE CONCIENCIA ACERCA DE LA SEGURIDAD, R029 - FFALLAS EN LA GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN), CA029 - FALTA DE ACTUALIZACIÓN Y CAPACITACION DE LOS PROCEDIMIENTOS FRENTE A LA NORMATIVIDAD.

Posteriormente, en prueba de recorrido con la OAINF, se requirió mediante correo electrónico del 19-11-2025 el suministro del inventario actualizado de equipos de cómputo (servidores y equipos de usuarios finales) que aún no han completado la migración del sistema operativo Windows 10 a Windows 11. En respuesta al presente requerimiento de información, la OAINF con fecha 24-11-2025 suministró documento denominado Informe Windows 11.pdf el cual contiene 5 folios en donde se informa que del total de 688 máquinas activas en la Entidad, 429 se han migrado a Windows 11. Es decir, faltaría un total 259 máquinas por efectuarse la actualización del SO. Mayor detalle se puede observar en el archivo que a continuación se adjunta:



Proyecto
actualización Windo'

4. Evidencias de capacitaciones

Respuesta: Se adjuntan evidencias de capacitaciones realizadas en el marco del Punto Alterno de Continuidad:

Figura 41. Evidencias capacitaciones realizadas en el marco del Punto Alterno de Continuidad
Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre - Archivo Documento Guía para acceso a carpetas.docx

Adicional se adjuntan los siguientes documentos en la carpeta Punto #4 PAC como registro de asistencia a las preparaciones previas a las pruebas del PAC realizadas en el periodo auditado:

- SIMULACRO TECNICO - Plan de recuperación de desastres (DRP) _ PAC - Informe de asistencia 4-30-25.xlsx.
- PREPARACION PRUEBA PAC - Informe de asistencia 5-19-25.xlsx.

Tras la revisión de la OFCIN en consulta al repositorio documental – Link: 10 Octubre - Carpeta Punto #4 PAC se observa la siguiente información:

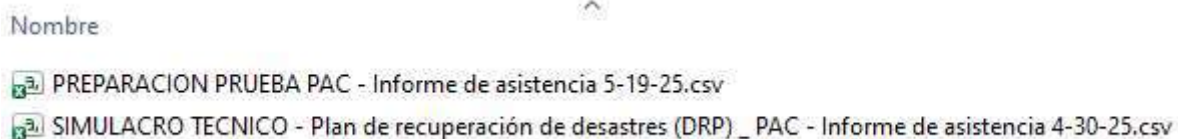


Figura 41. Análisis DOFA PAC Caja Honor

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre - Carpeta Punto #4 PAC

Archivo PREPARACION PRUEBA PAC - Informe de asistencia 5-19-25.xlsx: correspondiente a la lista de asistencia de 23 participantes a la reunión titulada PREPARACION PRUEBA PAC llevada a cabo Hora de inicio 5/19/25, 9:47:42 AM y Hora de finalización 5/19/25, 10:30:04 AM.

Archivo SIMULACRO TECNICO - Plan de recuperación de desastres (DRP) _ PAC - Informe de asistencia 4-30-25.xlsx: correspondiente a la lista de asistencia de 30 participantes a la reunión titulada SIMULACRO TECNICO - Plan de recuperación de desastres (DRP) / PAC llevada a cabo Hora de inicio 4/30/25, 3:56:02 PM y Hora de finalización 4/30/25, 5:23:41 PM.

Una vez analizada la información contenida en los archivos antes citados, se observa que acorde a la información registrada en la tabla 12 del presente informe, para el proceso PAC se cuenta con un total de 47 colaboradores asignados; sin embargo, en las capacitaciones realizadas los días 30 de abril y 19 de mayo se registró la asistencia de únicamente 30 y 23 participantes, respectivamente. Esta situación evidencia una brecha significativa en la cobertura de formación; lo que puede conllevar riesgos operacionales por la falta de capacitación completa y en un momento dado generar errores en la ejecución del proceso PAC, afectando la eficiencia y calidad del servicio; Riesgo de cumplimiento por el incumplimiento de los planes de formación establecidos con posible derivación de observaciones durante auditorías internas o externas; Riesgo reputacional por una baja preparación del personal lo que puede impactar negativamente la percepción de control y gestión dentro de la organización. Por lo anterior, la OFCIN precisa:

Recomendación No. 8.

La OFCIN recomienda a la OAGRI, en coordinación con los procesos interrelacionados, implementar acciones que garanticen la participación del 100% del personal asignado al proceso PAC y, en general, a las actividades de Continuidad del Negocio en todas las capacitaciones impartidas para el fortalecimiento y desarrollo de los simulacros de continuidad, estableciendo un plan de seguimiento y control de asistencia, reforzar la comunicación sobre la obligatoriedad de las capacitaciones, programar sesiones adicionales que aseguren la cobertura total del personal y evaluar mecanismos de registro y reporte que permitan evidenciar la participación efectiva en las actividades de formación. Lo anterior teniendo en cuenta que en el proceso PAC se cuenta con 47 colaboradores

asignados; sin embargo, en las capacitaciones realizadas los días 30 de abril y 19 de mayo se registró la asistencia de únicamente 30 y 23 participantes, respectivamente, lo que evidencia una brecha significativa en la cobertura de formación. En consecuencia, la falta de cobertura en la capacitación vulnera los principios establecidos en la ISO 22301:2019, específicamente la Cláusula 7.2 – Competencia, que exige que el personal sea competente para desempeñar su rol en la continuidad del negocio, y la Cláusula 8.4 – Ejercicios y pruebas, que requiere simulacros con personal capacitado para garantizar la eficacia del Sistema de Gestión de Continuidad del Negocio – BCMS; situación que puede generar riesgos operacional, por deficiencias en la ejecución de simulacros; de cumplimiento, por posibles hallazgos en auditorías internas o externas; y reputacional, por una percepción negativa sobre la preparación institucional ante incidentes.

5. Relación de Equipos de Cómputo destinados para el PAC indicando Placa de Inventario, responsable, SO instalado y proceso asignado.

Respuesta: Se adjunta el documento: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #3 PAC" del Excel.

Es de anotar que, para este ítem, la OAGRI suministró la misma información que la enviada para el ítem 3, por lo tanto, la OFCIN realizó el análisis respectivo en el Numeral 3 del componente **Punto Alternativo de Continuidad del Negocio – PAC.**

6. Relación de VPN implementadas para el PAC adjuntando copia de los formatos de solicitud VPN debidamente diligenciados, para cada uno de los colaboradores designados para el proceso PAC.

Respuesta:

- Se adjunta el documento: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #6 PAC" del Excel con la relación de flujos VPN solicitados.
- Se adjunta la carpeta FORMATOS VPN 395 con los Acuerdos de Confidencialidad para uso de dispositivos, redes sociales y trabajo a distancia del personal perteneciente al Punto Alternativo de Continuidad (PAC).

Una vez la OFCIN realizó el análisis de la información contenida en el archivo Requerimiento de Información PCN PAC Y DRP.xlsx, hoja "Punto #6 PAC" y consultado con fecha 19-11-2025 en el Gestor Documental cada uno de los 47 Radicados 395, se observó la información registrada en la siguiente tabla:

Tabla 17. Relación VPN implementadas para el PAC – Formatos Diligenciados

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre – archivo Requerimiento de Información PCN PAC Y DRP.xlsx, hoja "Punto #6 PAC

Como se evidencia en la Tabla 17, los Radicados 395-01-2025041000366 y 395-01-2025052700519 se encuentran vencidos, los radicados 395-01-2025051900480 y 395-01-2025060400562 presentan nombres cruzados o no correspondientes. Igualmente, del total

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá **601 755 7070**
Línea gratuita nacional **01 8000 185 570**
www.cajahonor.gov.co - **contactenos@cajahonor.gov.co**
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

de los 47 radicados, 8 de ellos no especifican exclusividad para temas de continuidad del negocio, siendo una medida esencial para garantizar la disponibilidad inmediata y la operatividad segura en escenarios de contingencia. Estos dispositivos deben permanecer reservados y configurados con las herramientas, accesos y controles requeridos para trabajo remoto puesto que es la estrategia establecida en la Entidad para el PAC, evitando su uso en actividades cotidianas que puedan comprometer su integridad, seguridad o disponibilidad; en donde esta práctica asegura el cumplimiento de los objetivos del plan, reduce riesgos operacionales y fortalece la capacidad de respuesta ante interrupciones.

7. Medidas y controles de seguridad y ciberseguridad implementados en la operación para la protección de datos y sistemas críticos (conectividad, acceso a aplicativos, autenticación de usuarios, firewalls, cifrado de información, etc.) que garanticen la seguridad de la información procesada mediante la estrategia de trabajo remoto.

Respuesta:

Medidas y controles de seguridad y ciberseguridad para acceso remoto mediante VPN

Con el fin de garantizar la seguridad de la información y la continuidad operativa en entornos de trabajo remoto, se establecen las siguientes medidas y controles aplicables al acceso por VPN:

Seguridad de dispositivos:

- Cifrado de disco con PGP en equipos portátiles para proteger la confidencialidad de la información almacenada.
- Agente antimalware obligatorio en equipos remotos como requisito previo para establecer conexión.
- Agente de prevención de fuga de datos (DLP) instalado en los dispositivos remotos como condición para el acceso.
- Restricción de puertos USB para evitar extracción no autorizada de información.

Control de conexión VPN:

- Agente VPN con políticas de cumplimiento, reglas de conexión y control de navegación.
- Conexión automática en redes públicas para garantizar el uso seguro de la VPN en entornos no confiables.
- Redundancia en conexiones mediante servicios en la nube para asegurar disponibilidad.
- Prevención de fugas de DNS: la aplicación solo permite solicitudes DNS a través del servidor especificado en la interfaz VPN.
- Autenticación multifactor (MFA) con Azure AD obligatoria para el establecimiento de la conexión VPN.
- Monitoreo continuo de conexiones VPN para detectar accesos no autorizados o comportamientos anómalos.
- Políticas de acceso condicional basadas en factores como ubicación geográfica, tipo de dispositivo o comportamiento inusual.

- Verificación continua si el equipo cumple con requisitos de seguridad (antimalware, DLP, Firewall activo, agente actualizado) antes de permitir la conexión y durante la misma.
- Envío de eventos de VPN (Autenticaciones Azure – Entra ID) a plataforma de monitoreo centralizada para correlación y respuesta ante incidentes SIEM.

Control de acceso y aplicaciones

- Reglas de firewall, inspección de tráfico por dispositivo IPS y políticas VPN para limitar el acceso a aplicaciones según perfil del usuario y control de tráfico no autorizado o anómalo.
- Acceso específico a aplicativos mediante autenticación SSO (Single Sign-On) (Intranet, Isolución, Service Manager, etc.) o login dedicado, con control de roles por aplicación (DODO-DOCS, GA2, Dialogo, etc.).

Gestión de dispositivos y sistemas

- Políticas de grupo (GPO) para aplicar configuraciones de seguridad en los equipos (bloqueo de pantalla, políticas de contraseñas, bloqueos por intentos fallidos, mínimo privilegio, etc.).
- Firewall local activado, despliegue de parches de actualización y seguridad del sistema operativo.
- Restricciones de privilegios administrativos y validación de que los dispositivos estén autorizados y unidos al dominio, restricción/control de sistemas operativos (Linux, MAC, Android, IOS)
- Uso de Configuration Manager para soporte, control y gestión centralizada de dispositivos por parte de la mesa de ayuda.

Procedimientos y cumplimiento

- Formatos de solicitud para conexión VPN, guía de protocolos de seguridad de la información y ciberseguridad, autorizaciones de conexión y retiro de equipos de la entidad, alistamiento de equipos gestionados por la mesa de ayuda.
- Acuerdo de confidencialidad y acatamiento de políticas de seguridad de la información y ciberseguridad firmado por los usuarios que acceden remotamente.
- Protección contra phishing y spam, incluyendo restricciones en el envío de correos electrónicos externos.
- Con apoyo de OAGRI, campañas de concientización y simulacros para fortalecer la cultura de seguridad entre los usuarios remotos.

Tras el análisis de la respuesta suministrada por la OAGRI, la OFCIN observa que el proceso demuestra un alto grado de madurez en la implementación de controles de seguridad y ciberseguridad para trabajo remoto, cumpliendo con buenas prácticas internacionales (VPN segura, MFA, cifrado, monitoreo, políticas de acceso condicional). Sin embargo, se recomienda fortalecer la validación continua de la efectividad de los controles, la gestión proactiva de vulnerabilidades y la formalización de pruebas periódicas y planes específicos de respuesta ante incidentes para garantizar la resiliencia y la mejora continua.

8. Favor suministrar documento oficial que describa el procedimiento para el acceso remoto a servidores.

Respuesta: Se adjunta en la carpeta Punto #8 PAC el documento: GR-NA-GU-036 Protocolo SICI Trabajo a Distancia V4.doc

El documento “Guía de Protocolo de Seguridad de la Información y Ciberseguridad para Trabajo a Distancia” es esencial puesto que establece un marco normativo y operativo orientado a garantizar la protección de los activos de información en entornos de trabajo a distancia y su contenido se estructura en directrices que buscan mitigar riesgos asociados a la pérdida, alteración o divulgación no autorizada de datos, así como prevenir incidentes de ciberseguridad derivados del uso de tecnologías fuera del perímetro corporativo.

Así las cosas, una vez revisado el documento GR-NA-GU-036 Protocolo SICI Trabajo a Distancia V4.doc se considera Importante incorporar en el marco normativo las disposiciones establecidas por la Ley de Protección de Datos Personales, garantizando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. En relación con el manejo de datos, se debe especificar el uso exclusivo de herramientas corporativas aprobadas para la transferencia y almacenamiento de archivos, evitando plataformas no autorizadas como aplicaciones de mensajería instantánea o correos electrónicos personales. Para asegurar la eficacia del protocolo en entornos de trabajo remoto, se requiere la ejecución de revisiones periódicas orientadas a verificar el cumplimiento de las políticas, identificar desviaciones y evaluar la efectividad de los controles implementados. Asimismo, es indispensable mantener una actualización continua frente a nuevas amenazas, vulnerabilidades y tecnologías emergentes, alineando las prácticas con estándares internacionales y normativas vigentes. La gestión del riesgo debe ser sistemática, complementada con pruebas de penetración y simulaciones de ataques que permitan detectar brechas antes de su explotación. Estos mecanismos fortalecen la postura de seguridad organizacional y consolidan una cultura orientada a la resiliencia y la mejora continua.

Por otra parte, es de precisar que, considerando la decisión institucional de migrar la documentación controlada desde la herramienta ISOLUCION hacia la plataforma SVE, se informa que el documento GR-NA-GU-036 Protocolo SICI Trabajo a Distancia V4, suministrado por el proceso auditado, se encontraba en el repositorio ISOLUCION con el código GR-NA-GU-036. No obstante, dicho documento fue actualizado en la plataforma SVE bajo el código GR-GU-036 V6 del 31-10-2025.

9. Capacidad Operacional y Soporte: Relacione los procesos críticos que pueden ser soportados con el PAC y cuales son críticos para la continuidad, sistemas de respaldo (UPS, almacenamiento redundante, etc., Duración de la operación evaluando por cuanto tiempo el PAC puede sostener las operaciones críticas).

Respuesta:

En cuanto a lo relacionado con el sistema de respaldo se indica el soporte establecido de la siguiente manera:

Sistemas de Respaldo:

- Para garantizar la continuidad de los procesos anteriores, el PAC contempla:
- UPS (Uninterruptible Power Supply): Dos UPS Marca VERTIV de 60 Kva cada una (Actúan como principal y Respaldo). Autonomía: 15 minutos a tope de carga.
- Baterías: 3 bancos de 24 unidades cada uno. (72 unidades por cada UPS).
Soporta Infraestructura tecnológica.

- Almacenamiento redundante: RAID (Redundant Array of Independent Disks).
- SAN/NAS con replicación en sitio alterno.
- Servidores en alta disponibilidad: Clústeres de servidores.
- virtualización con failover automático.
- Respaldos automáticos y fuera de sitio: Copias diarias/semanales/mensuales sitio principal.
- Pruebas periódicas de restauración. (Trimestral)
- Redundancia de red y conectividad: Enlaces principales y backups para CAN y Sedes a Nivel nacional

Si bien el proceso auditado describe los sistemas de respaldo implementados por la Entidad, no identifica cuáles son críticos ni establece su relación con el Plan de Continuidad del Negocio; tampoco precisa qué procesos críticos pueden ser soportados mediante dicho plan ni el tiempo estimado durante el cual el PAC garantiza la operación de estas actividades. Esta información es esencial para evaluar la capacidad real de la Entidad frente a contingencias y determinar la suficiencia y efectividad de las estrategias de continuidad y recuperación definidas. En consecuencia, se sugiere que la Entidad documente de forma clara y completa la relación entre los sistemas de respaldo y los procesos críticos definidos en el Plan de Continuidad del Negocio.

10. Pruebas o simulacros del PAC realizados durante el periodo auditado, adjuntando informe que registre fecha de la prueba, resultados del simulacro, lecciones aprendidas indicando los inconvenientes detectados en simulacros anteriores y acciones correctivas implementadas para mejorar el desempeño del PAC, medidas de seguridad implementadas.

Respuesta: Se adjunta en la carpeta Punto #10 PAC, el documento INFORME PRUEBA PAC 22 DE MAYO 2025.pdf donde se detalla lo solicitado.

Archivo INFORME PRUEBA PAC 22 DE MAYO 2025.pdf: contiene 10 folios correspondiente al documento de fecha 30/05/2025 emitido por la jefatura OAGRI con **Asunto: Prueba Punto Alterno de Continuidad** el cual fue previamente analizado en el punto 2 del componente PAC.

11. Indicadores de desempeño del PAC, Registro de incidentes reales gestionados desde el PAC.

Respuesta: Se adjunta el documento: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #11 PAC" del Excel, la relación de incidentes reales se encuentra descritos en el documento INFORME PRUEBA PAC 22 DE MAYO 2025.pdf.

Una vez la OFCIN revisó la información contenida en el archivo Requerimiento de Información PCN PAC Y DRP.xlsx, hoja Punto #11 PAC, se observó la documentación de los siguientes indicadores:

Tabla 18. Indicadores de desempeño del PAC

Indicador	Métrica Clave	Responsable	Periodicidad	Meta	Estado Actual
Funcionarios conectados en prueba PAC	% de conexión efectiva	OAGRI	Semestral	≥ 80% conectividad	39 funcionarios conectados, acceso exitoso
Tiempo de respuesta árbol de llamadas / N° Personas árbol de llamadas por área.	Tiempo promedio por nivel	OAGRI	Semestral	≤ 2 minutos	Cumplido (< 2 min)
Incidentes técnicos en pruebas PAC / N° aplicativos a los que se acceden	N° de incidentes documentados	Oficina Informática /OAGRI	Semestral	≤ 20	17 incidentes

Fuente: OAGRI – Repositorio Documental – Link: 10 Octubre – archivo Requerimiento de Información PCN PAC Y DRP.xlsx, hoja Punto #11 PAC

Si bien, el proceso auditado suministro información relacionada con los Indicadores de desempeño del PAC, registrados en la Tabla 18, éstos proporcionan información valiosa sobre la participación y la eficiencia operativa durante los ejercicios del Plan Alterno de Continuidad (PAC). Sin embargo, su alcance es limitado, ya que no permiten evaluar la capacidad real de recuperación ni la madurez del plan frente a una contingencia, situación que puede generar brechas en la toma de decisiones estratégicas y en el cumplimiento de estándares internacionales como ISO 22301. Por lo anterior, la OFCIN precisa:

Recomendación No. 9.

La OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, ampliar e implementar el conjunto de indicadores incorporando métricas que midan la Cobertura y Preparación (porcentaje de procesos críticos con plan probado y personal entrenado), la Eficacia de Recuperación (tiempo de activación del plan – RTO y cumplimiento del objetivo de punto de recuperación – RPO) y la Mejora Continua (hallazgos en simulacros y acciones correctivas implementadas). Esta ampliación permitirá contar con una visión integral del desempeño del PAC, fortaleciendo la resiliencia organizacional y asegurando que las pruebas no solo midan participación, sino también efectividad y alineación con los objetivos estratégicos. Así las cosas, minimizar la materialización de riesgos asociados a la falta de visibilidad sobre la capacidad de recuperación, lo que puede ocasionar tiempos prolongados de interrupción; incumplimiento normativo, que podría derivar en posibles sanciones y afectación reputacional y financiera, al no garantizar la continuidad de procesos críticos.

Por otra parte, con relación al Registro de incidentes reales gestionados desde el PAC, una vez consultado el documento INFORME PRUEBA PAC 22 DE MAYO 2025.pdf, se observó el numeral “5. Resumen de Incidentes Reportados”, con la siguiente información:

Tabla 19. Registro incidentes reportados Prueba PAC

Fuente: OAGRI - Repositorio Documental – Link: 10 Octubre - archivo INFORME PRUEBA PAC 22 DE MAYO 2025.pdf, numeral “5. Resumen de Incidentes Reportados”

Como se observa en la tabla 19, se identificaron 17 incidentes individuales, asociados principalmente a conectividad de red, acceso a sistemas institucionales y desempeño de aplicaciones críticas, en donde todos los casos fueron atendidos y resueltos oportunamente por el Ing. Coordinador de la actividad del PAC y la mesa de ayuda, garantizando la continuidad operativa y evitando afectaciones significativas en el servicio.

No obstante, teniendo en cuenta que el registro de incidentes suministrado, únicamente contempla el usuario que reporta, la descripción y el tipo de incidente, limita la trazabilidad y dificulta la identificación de patrones recurrentes, lo que incrementa el riesgo de reincidencia y afecta la capacidad de respuesta ante incidentes críticos. En consecuencia la OFCIN precisa:

Recomendación No. 10.

La OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, que para garantizar la integridad del proceso gestión de incidentes y la capacidad de análisis, se implemente un formato que incluya, como mínimo, los siguientes campos: ID del incidente, fecha y hora, descripción detallada, categoría, impacto, estado, responsable, tiempo de resolución, acciones correctivas y observaciones; información que permite evaluar el desempeño, medir el cumplimiento de los SLA - Acuerdo de Nivel de Servicio y generar reportes confiables para auditorías y mejora continua; pues mantener un registro incompleto limita la trazabilidad y dificulta la identificación de patrones recurrentes, lo que incrementa el riesgo de reincidencia y afecta la capacidad de respuesta ante incidentes críticos; lo que puede derivar en hallazgos y vulneración de normativas aplicables, particularmente la Circular Externa 008 De 2018 , numeral 2.3.4 (Capítulo I, Título II), que exige soporte documental completo para operaciones y eventos, y la Circular Básica Jurídica 006/25, Parte I – Instrucciones Generales, que establece la obligación de mantener procesos internos documentados y trazables. El incumplimiento de estas disposiciones expone a la Entidad a sanciones y pérdida de confianza, mientras que un registro robusto fortalece la gobernabilidad y la resiliencia operativa, en línea con las mejores prácticas de ITIL 4 y la norma ISO/IEC 27001 (Anexo A.16).

12. Plan de actualizaciones regulares del PAC en función de los cambios en la Entidad, la tecnología o en el entorno externo.

Respuesta: Actualmente, se está en proceso de aumento de personal, lo cual responde a la necesidad de asegurar el funcionamiento óptimo del PAC, esto se encuentra justificado en la realización de solicitudes formales a los procesos, fundamentada en la necesidad de garantizar la eficiencia y la continuidad operativa en situaciones de contingencia, así como en la creciente demanda de los servicios, lo que impacta las actividades críticas de la Entidad. Los nuevos funcionarios tendrán las siguientes responsabilidades:

- Carga de Trabajo.
- Mejora en la Eficiencia Operativa.
- Cumplimiento de Normativas y Procedimientos.

Cronograma de Implementación:

Para llevar a cabo la implementación de esta solicitud de manera efectiva, se propone el siguiente cronograma con el fin de ejecutar la totalidad de la ampliación del personal para futuras pruebas del PAC.

- Planificación y Aprobación.
- Definición de los perfiles y requisitos para los nuevos funcionarios.
- Configuración de equipos de cómputo con los requerimientos técnicos especificados e implementación de nuevo agente VPN Harmony SASE.
- Se incluye en el plan de compras del próximo año la adquisición de equipos de cómputo necesarios para este fin.
- Capacitación de los nuevos funcionarios.
- Evaluación y Ajustes.

Tras el análisis de la información suministrada por el proceso auditado, la OFCIN observó que se viene realizando gestión respecto al aumento de personal para el PAC; sin embargo, respecto del Plan de actualizaciones regulares del PAC, la OFCIN precisa:

Recomendación No. 11.

La OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, complementar el Plan de actualizaciones del PAC con datos tales como: Frecuencia y metodología de las actualizaciones, Responsables del seguimiento y ejecución, Procedimiento para identificar cambios internos, tecnológicos o externos, Mecanismos de validación y pruebas posteriores a cada actualización y Plan de comunicación y capacitación tras cada actualización. Lo anterior, en aras de dar cumplimiento a las buenas prácticas establecidas en marcos como ITIL y normas ISO 27001, minimizando la generación de riesgos operacional (interrupción del servicio), de seguridad (vulnerabilidades no detectadas), de cumplimiento (sanciones por normativa) y reputacionales (pérdida de confianza).

Por su parte, la OFCIN, con fecha 27-11-2025 procedió a consultar la herramienta SVE – Opción Menú “Documentos”, descargando la *Guía de Operación Punto Alterno de Continuidad – PAC* (Cód. GR-NA-GU-05, versión 015 del 20-09-2025, y una vez la OFCIN verificó dicha *Guía* se observó que la misma contiene un total de 14 páginas, en donde se tienen las siguientes precisiones:

- Considerando lo establecido en el numeral 3.2 “Recursos tecnológicos necesarios” de la *Guía de Operación Punto Alterno de Continuidad – PAC* (Cód. GR-NA-GU-05,

versión 015 del 20-09-2025), el cual indica que “se requiere que los funcionarios cuenten con un equipo de cómputo distinto al asignado en la entidad”, resulta prioritario garantizar que el inventario de equipos destinados para este propósito se mantenga completamente actualizado. Dichos equipos deben conservarse en condiciones óptimas de funcionamiento, de manera que estén disponibles y operativos en el momento en que se active el proceso PAC.

- De igual forma, con base a lo señalado en la citada Guía, donde se indica que “es necesario que todos los funcionarios designados para el despliegue del Punto Alterno de Continuidad dispongan de acceso a un proveedor de internet que cumpla con las características tecnológicas adecuadas para la conexión VPN, garantizando el acceso a los sistemas de información”, es indispensable que dicho documento especifique de manera clara y detallada cuáles son las características tecnológicas requeridas para asegurar una conexión VPN segura y eficiente.

Por otra parte, es de precisar que, nuevamente con fecha 01-12-2025, la OFCIN realizó una consulta en la herramienta SVE, observando que el documento *Guía de Operación Punto Alterno de Continuidad – PAC* (Cód. GR-NA-GU-05, versión 015 del 20-09-2025, fue actualizado bajo el nuevo código *GR-GU-005*, versión 016, del 31-10-2025, compuesto por 18 páginas.

Plan de Recuperación de Desastres – DRP

1. Documentación actualizada del Plan de Recuperación de Desastres incluyendo Procedimientos de respaldo y restauración de datos, Alcance del DRP (qué sistemas, procesos y ubicaciones cubre), Objetivos del DRP, incluyendo RTO (Recovery Time Objective) y RPO (Recovery Point Objective).

Respuesta: Se adjunta los documentos en la carpeta Punto #1 DRP

En la ubicación informada por el proceso auditado se observó:



Figura 42. Documentación DRP

Fuente: OAGRI - Repositorio Documental – Link: 10 Octubre - archivo

El documento suministrado por la OAGRI denominado IT-NA-PL-003_V8_6354_1 .docx corresponde al PLAN DE RECUPERACIÓN ANTE DESASTRES DRP, Cod. IT-NA-PL-003 V 008 de Fecha aprobación: 27-10-2025 con un total de 25 folios.

Igualmente, la OFCIN con fecha 01-12-2025 procedió a verificar en la plataforma SVE el documento PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP, observando que el mismo fue nuevamente actualizado bajo el Cod. IT-PL-003 V9 del 31-10-2025, evidenciando que se compone de 27 páginas, del cual se tienen las siguientes observaciones:

- Numeral 2. Alcance, eliminar párrafo repetido: “Restablecer y recuperar la operación en el menor tiempo posible ante un posible escenario que la coloque en riesgo, garantizando la continuidad de la operación en la Entidad, además de comprobar que la infraestructura tecnológica y el recurso humano se efectivos y eficiente.”
- Complementar el documento PLAN DE RECUPERACIÓN ANTE DESASTRES DRP, Cod. IT-PL-003 V9 del 31-10-2025 con la normativa actualizada de la Superintendencia Financiera de Colombia, como por ejemplo, entre otras, la Circular Básica Jurídica (C.E. 006 de 2025), la cual establece que las entidades vigiladas deben incorporar en sus planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) la operación en ambientes tecnológicos, incluyendo servicios en la nube. La normativa exige definir parámetros como RTO y RPO, implementar mecanismos de respaldo y cifrado, garantizar independencia lógica o física de la información, y establecer estrategias de migración ante interrupciones. Asimismo, los contratos con proveedores deben contemplar cláusulas sobre disponibilidad, tiempos de recuperación y borrado seguro de datos, complementadas con pruebas periódicas que aseguren la efectividad del DRP y la continuidad operativa.
- Asimismo, es de alta prioridad mantener actualizado el documento PLAN DE RECUPERACIÓN ANTE DESASTRES DRP, Cod. IT-PL-003 V9 del 31-10-2025 con información crítica que garantice la continuidad operativa, incluyendo el inventario de activos tecnológicos, aplicaciones y sistemas esenciales, parámetros de recuperación (RTO y RPO), procedimientos de activación y contingencia, datos de proveedores y acuerdos de nivel de servicio, ubicación y características del sitio alternativo, plan de comunicaciones, políticas de respaldo y resultados de pruebas. Esta actualización permanente asegura que los recursos, procesos y responsabilidades estén alineados con los requerimientos regulatorios y las mejores prácticas de gestión de riesgos, Para lo cual se sugiere la siguiente ficha en la cual se debe registrar la información pertinente:

Tabla 20. Componentes del Plan de Recuperación ante Desastres que deben actualizarse continuamente

Elemento	Descripción	Última actualización	Responsable
Inventario de activos	Equipos, servidores, dispositivos de red, software y versiones.		
Aplicaciones críticas	Lista de sistemas esenciales y sus dependencias.		
Parámetros RTO/RPO	Tiempos y puntos de recuperación definidos por proceso crítico.		
Procedimientos de contingencia	Pasos para activar el DRP y roles asignados.		
Proveedores y contratos	Contactos, SLA, cláusulas de continuidad y recuperación.		
Sitio alternativo	Ubicación, capacidad, conectividad y seguridad física.		
Plan de comunicaciones	Canales, protocolos y contactos actualizados del personal clave.		
Respaldos y medios	Políticas de backup, ubicación, frecuencia y pruebas de restauración.		
Pruebas del DRP	Cronograma, resultados y acciones correctivas.		
Cumplimiento normativo	Referencias a circulares SFC y regulaciones aplicables.		

Fuente: OFCIN – Diseño Propio

La presente observación se formula considerando que, en lo referente a los aplicativos, Isolución ya no debe incluirse en el inventario, dado que esta herramienta fue incorporada dentro de la Suite Visión Empresarial. Adicionalmente, tal como se indicó previamente, resulta indispensable proceder con la actualización normativa correspondiente.

2. Adjuntar evidencias de pruebas y simulacros realizados frente al Plan de respaldo de datos y recuperación ante desastres durante el periodo evaluado incluyendo (fechas, resultados, lecciones aprendidas).

Respuesta: Se adjuntan los siguientes documentos en la carpeta Punto #2 DRP:

- Informe Ger prueba_DRP_Total_CajaHonor_02 y 03 mayo 2025.pdf.
- Informe Prueba DRP Total Caja Honor 02y03mayo2025.pdf.

Se evidenciaron los siguientes documentos en la carpeta indicada en la respuesta de la OAGRI:



Nombre	Fecha de modificación
 Informe Ger prueba_DRP_Total_CajaHonor_02 y 03 mayo 2025.pdf	20/10/2025 12:19 p. m.
 Informe Prueba DRP Total Caja Honor 02y03mayo2025.pdf	20/10/2025 12:19 p. m.

Figura 43. Archivos carpeta Punto #2 DRP OAGRI - Repositorio Documental – Link: 10 Octubre - carpeta Punto #2 DRP

Archivo Informe Ger prueba DRP Total CajaHonor 02 y 03 mayo 2025.pdf: correspondiente a la presentación compuesta por 15 diapositivas, elaborada en virtud de la Prueba Técnica de Plan de Recuperación ante Desastres (DRP) ejecutada los días 02 y 03 de mayo de 2025, indicando que el ejercicio consistió en la simulación de un escenario de indisponibilidad de la infraestructura principal ubicada en Triara, realizando la conmutación de los servicios hacia el Data Center alternativo localizado en la sede de Caja Honor del CAN“. No obstante, se observó que el alcance de la prueba no contempló replicación inversa lo cual es de gran importancia, ya que permite validar no solo la capacidad de conmutación hacia el sitio alternativo (failover), sino también el retorno seguro al sitio principal (failback) sin pérdida de datos ni afectación de la operación. Este proceso garantiza la integridad y consistencia de la información generada durante la contingencia, reduce riesgos operacionales asociados a la reintegración de servicios y asegura el cumplimiento de estándares internacionales de continuidad (como ISO 22301), que exigen pruebas completas de recuperación. Adicionalmente, la replicación inversa contribuye a optimizar los tiempos de recuperación (RTO) y los puntos de recuperación (RPO), fortaleciendo la resiliencia tecnológica de la organización.

Adicionalmente, es de señalar que, dado a que la información registrada en el presente archivo respecto a los tiempos de recuperación total no resulta completamente precisa, con fecha 06-11-2025 se realizó una mesa de trabajo con el responsable de los temas de continuidad en la Entidad, remitiendo comunicación mediante correo electrónico de la misma fecha, solicitando la aclaración correspondiente y el alcance necesario sobre dicho aspecto.

Dado lo anteriormente expuesto, la OFCIN precisa:

Recomendación No. 12.

NIT: 860021967 - 7

Centro de Contacto al Ciudadano CCC en Bogotá 601 755 7070
Línea gratuita nacional 01 8000 185 570
www.cajahonor.gov.co - contactenos@cajahonor.gov.co
Carrera 54 No. 26-54 - Bogotá D.C. Colombia

BIENESTAR Y EXCELENCIA

La OFCIN recomienda a la OAGRI, en coordinación con OAINF y demás procesos interrelacionados, que en futuros ejercicios de simulacro del DRP se incorpore la ejecución de la replicación inversa (failback), la validación de la sincronización a nivel de almacenamiento y la precisión en los tiempos de recuperación documentados, toda vez que estas acciones son esenciales para garantizar la integridad y consistencia de los datos durante todo el ciclo de recuperación, así como para establecer mecanismos robustos que permitan registrar de manera confiable los RTO y RPO alcanzados, en cumplimiento de la norma ISO 22301:2019 (cláusula 8.4) y los lineamientos regulatorios de la SFC, particularmente lo dispuesto en la Circular Externa 007 de 2018, numeral 4.1.7 sobre pruebas del plan de continuidad y en la Circular Externa 008 de 2018, que modifica numerales como 1.2.2.1.2.7 y 2.3.4.1.3, relacionados con seguridad y calidad en la operación, en donde su implementación contribuirá a mitigar riesgos operacionales y regulatorios, fortaleciendo la resiliencia tecnológica de la organización.

Lo anterior se fundamenta en que, durante la revisión del informe de la prueba DRP realizada los días 02 y 03 de mayo de 2025, se evidenció que el alcance no contempló la replicación inversa ni la validación de sincronización, prácticas indispensables para asegurar el retorno seguro al sitio principal sin pérdida de datos ni afectación de la operación. Esta omisión contraviene lo dispuesto en la ISO 22301:2019, cláusula 8.4, y las buenas prácticas nacionales que exigen la definición y verificación de RTO y RPO. Adicionalmente, se observó falta de precisión en los tiempos de recuperación documentados, lo que limita la confiabilidad de los indicadores críticos y puede generar impactos significativos como pérdida de integridad de datos, interrupciones prolongadas, sanciones por incumplimiento normativo y deterioro reputacional frente a clientes y entes reguladores.

Archivo Informe Prueba DRP Total Caja Honor 02y03mayo2025.pdf: contiene la misma información del archivo denominado Informe Ger prueba_DRP_Total_CajaHonor_02 y 03 mayo 2025.pdf, con 15 páginas.

3. Lista de responsables del DRP y sus funciones específicas, Contactos de emergencia y cadena de mando en caso de desastre, Evidencia de capacitación y simulacros realizados por el personal involucrado.

Respuesta: Se adjunta el documento: Requerimiento de Información PCN PAC Y DRP.xlsx cuya respuesta a este punto, se encuentra detallado en la hoja "Punto #9" del Excel con la relación de flujos VPN solicitados.

Nota. Información previamente validada en el ítem 9 del componente PCN, Tabla 8.

4. Relaciona a detalle los recursos de plataforma tecnológica con los que cuenta la Entidad para Procedimiento Plan de Recuperación de Desastres Informáticos DRP, Inventario de activos críticos (servidores, aplicaciones, redes). Sistemas de respaldo y recuperación (on-premise, nube, híbridos). Ubicación de sitios alternos o centros de datos secundarios, Controles de acceso y seguridad en los sistemas de recuperación.

Respuesta:

Ciberseguridad:

El Plan de Recuperación de Desastres contempla una arquitectura tecnológica robusta, distribuida y redundante, orientada a garantizar la continuidad operativa, la protección de la información y la rápida recuperación ante eventos críticos. Entre los principales recursos y aplicaciones se incluyen:

Seguridad perimetral y detección de amenazas

- **Plataforma de protección perimetral FIREWALL** con arquitectura redundante en clústeres de alta disponibilidad (2 appliances), implementados tanto en los centros de datos CAN como TRIARA.
- **Sistema de prevención y detección de intrusos (IPS/IDS)** con redundancia ZPHA, compuesto por 2 appliances distribuidos en CAN y TRIARA.
- **Servicio de protección antimalware para endpoints**, basado en tecnología en la nube, que garantiza defensa activa contra amenazas tanto en servidores como equipos de cómputo.
- **Servicio de VPN basado en nube**, que permite acceso remoto seguro con políticas de autenticación y cifrado.
- **Plataforma de detección de fuga de datos (DLP)** con servidores de análisis en CAN y TRIARA, y agentes locales instalados en los endpoints para monitoreo y control en tiempo real.
- **Servicios de protección para portales web** mediante tecnología WAF (Web Application Firewall) basada en nube.
- **Servicio de certificados digitales** para portales web, que garantiza la autenticidad y cifrado de las comunicaciones.
- **Plataforma SIEM (Security Information and Event Management)** para centralización de eventos, correlación de alertas y respuesta ante incidentes, con cobertura en dispositivos y servidores ubicados en CAN y TRIARA.
- **Servicio de protección contra phishing y spam**, basado en nube, que filtra correos maliciosos y previene ataques de ingeniería social.
- **Copias de respaldo de configuraciones (Backups, Snapshots)** de políticas y consolas de administración de dispositivos de ciberseguridad, resguardadas en cintas, servidores y appliances.

Tras la revisión realizada por la OFCIN en el marco del Plan de Recuperación ante Desastres (DRP), se verificó que la organización cuenta con una infraestructura robusta orientada a la seguridad perimetral y la detección de amenazas, incluyendo firewalls en arquitectura redundante, sistemas IPS/IDS, plataformas DLP, WAF, SIEM y servicios antimalware en nube. Sin embargo, para garantizar la continuidad operativa y el cumplimiento de los objetivos de RTO y RPO, la OFCIN precisa:

Recomendación No. 13.

La OFCIN recomienda a la OAGRI, en coordinación con la OAINF, fortalecer la arquitectura tecnológica del Plan de Recuperación ante Desastres (DRP) mediante la incorporación de replicación de almacenamiento entre sitios, clústeres de alta disponibilidad, enlaces de red redundantes, mecanismos de orquestación para recuperación automatizada y copias de

seguridad aisladas (air-gapped) para mitigar riesgos como ransomware, además, se debe garantizar la sincronización de políticas de seguridad, certificados digitales y gestión de identidades en entornos alternos, junto con monitoreo centralizado y pruebas periódicas del DRP; de forma tal que se dé cumplimiento a la normativa del SFC, mediante directrices institucionales que definen los RTO y RPO como parte del marco de continuidad operacional en ambientes críticos, alineación con la ISO 27001:2022, que exige un plan de recuperación documentado e implementado para proteger la disponibilidad de la información crítica, y la ISO/IEC 27031, que define lineamientos para desarrollar capacidades de continuidad TIC alineadas con la gestión de riesgos. Adicionalmente, acatando lineamientos de la Ley 1523 de 2012, que establece “la gestión del riesgo incorpora prevención, atención y recuperación de desastres”; el Decreto 2157 de 2017, que obliga a “diseñar e implementar las medidas de reducción del riesgo y planes de emergencia y contingencia que serán de su obligatorio cumplimiento”; el Decreto 338 de 2022, que ordena “establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital. Lo anterior, con el objeto de mitigar riesgos como pérdida crítica de datos, interrupciones prolongadas, incumplimiento normativo, sanciones por parte de la SFC e impactos reputacionales, además de fortalecer la resiliencia tecnológica y garantizar la continuidad operativa de la Entidad.

6. Indicadores de desempeño del DRP, Mecanismos de revisión periódica del plan, Registro de incidentes reales y cómo se gestionaron que evidencien el control y seguimiento del DRP.

Respuesta: Actualmente, la Entidad no cuenta con indicadores de desempeño formalizados para el Plan de Recuperación ante Desastres (DRP), sin embargo, estos elementos se encuentran en proceso de elaboración en conjunto con el proveedor CLARO, como parte del fortalecimiento del PCN.

Dada la respuesta emitida por la OAGRI frente a este ítem, en donde se aclara que “*la Entidad no cuenta con indicadores de desempeño formalizados para el Plan de Recuperación ante Desastres (DRP)*”, la OFCIN recomienda:

Oportunidad de Mejora Correctiva No. 7.

La OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados, formalizar e integrar de manera prioritaria los indicadores RTO, RPO, porcentaje de pruebas exitosas en el DRP, Disponibilidad de recursos críticos; además de establecer un cronograma de revisión periódica y mantener un registro detallado de incidentes reales y su respuesta. Con ello, se fortalece el cumplimiento normativo, se mejora la capacidad de respuesta y se garantiza una gestión basada en datos que proteja la continuidad operativa y la confianza institucional. La adopción de estos elementos no solo facilitará la evaluación objetiva del desempeño del DRP, sino que también permitirá identificar brechas, optimizar procesos y garantizar la resiliencia operativa frente a eventos disruptivos. Adicionalmente, se sugiere establecer un cronograma de pruebas que aseguren la actualización continua del plan, así como la integración de estos indicadores en los reportes de gestión del PCN, para fortalecer la toma de decisiones basada en datos y cumplir con estándares de mejores prácticas en continuidad del negocio. Lo anterior, toda vez que se identificó que la Entidad no dispone de indicadores de desempeño formalizados para el Plan de Recuperación ante Desastres (DRP), lo cual transgrede los lineamientos de gestión del riesgo de la Superintendencia Financiera de Colombia (SFC), y su inclusión en

la Circular Básica Contable y Financiera (CBCF), especialmente en los Capítulos relacionados con Gobierno Corporativo y Administración del Riesgo Operacional, que implican la obligación de mantener sistemas robustos de continuidad del negocio y recuperación ante desastres. Asimismo, la carencia de indicadores de desempeño como RTO, RPO y porcentaje de pruebas exitosas impide cumplir con las expectativas prudenciales definidas por la SFC, así como con las mejores prácticas estipuladas en normas internacionales como la ISO 22301:2019, cláusula 9, que exige el monitoreo y revisión continua del desempeño del Sistema de Gestión de Continuidad del Negocio. En consecuencia, puede generar impactos reputacionales, sanciones regulatorias, pérdidas operativas y financieras, y una disminución significativa en la resiliencia institucional. Se observó el R062 - INDISPONIBILIDAD DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI) CA062 - FALLAS EN LA INFRAESTRUCTURA DEL DATACENTER ALTERNO, RSI077 - DENEGACION DE SERVICIOS POR CIBERATAQUES CSI078 - FALTA DE MECANISMOS DE MONITOREO ESTABLECIDOS PARA LAS BRECHAS DE SEGURIDAD.

9. SÍNTESIS

9.1. Síntesis Oportunidades de Mejora

Tabla 21. Consolidado Oportunidades de Mejora

#	OPORTUNIDADES DE MEJORA	CRITICIDAD	PLAZO OM
1	Oportunidad de Mejora Correctiva No. 1: La OFCIN recomienda a la OAGRI, Solicitar al proveedor del software la implementación de la funcionalidad exportación directa de los REROS en formato Excel para el perfil Auditor, lo anterior a que el software utilizado para la administración de riesgos no permite la exportación automática de los Reportes de Eventos de Riesgo Operacional (REROS) en formato Excel. Actualmente, Esta situación dificulta la obtención de evidencia confiable, compromete la trazabilidad de los datos y aumenta el esfuerzo requerido para validar la integridad de la información. Además, genera retrasos en la revisión y análisis, lo que puede impedir el cumplimiento de los plazos establecidos por la normativa y reducir la efectividad del proceso de auditoría; lo anterior a que la CE. 018 de la SFC DEL 2021: exige mantener registros actualizados y trazables de los eventos de riesgo operacional, lo que implica contar con herramientas tecnológicas que faciliten la gestión y reporte, en prevención de los “R028 Fallas en el Reporte y Documentación de Riesgos” y “RSI050 No Disponibilidad de Herramientas”, así como lo reglamentado en la Dimensión 4 Evaluación de Resultados, establecida en Manual Operativo del MIPG, versión 6 de diciembre de 2024.	Moderado	Debe estar implementada en un periodo no mayor a 9 meses.
2	Oportunidad de Mejora Correctiva No. 2: la OFCIN recomienda a la OAGRI la actualización de las matrices de Riesgos, lo anterior a que se evidenció la no entrega completa de las matrices de Riesgo correspondientes a todos los procesos de la Entidad, lo que limita la identificación, evaluación y monitoreo integral de los riesgos institucionales, lo cual representa un incumplimiento frente a lo dispuesto en la Circular Externa 018 de 2021 de la Superintendencia Financiera de Colombia, que exige la implementación de un Sistema de Administración del Riesgo Operacional (SIAR) con procesos estructurados de identificación, medición, control y monitoreo del riesgo. Esta situación afecta la trazabilidad y la gestión integral del riesgo, por lo que se recomienda establecer mecanismos de control y seguimiento que garanticen la entrega completa y oportuna de dichas matrices. Lo anterior en prevención de los “R028 Fallas en el Reporte y Documentación de Riesgos” y “RSI050 No Disponibilidad de Herramientas”, así como lo reglamentado en la Dimensión 4 Evaluación de Resultados, establecida en Manual Operativo del MIPG, versión 6 de diciembre de 2024.	Moderado	Debe estar implementada en un periodo no mayor a 9 meses.
	Oportunidad de Mejora Correctiva No.3: la OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, priorizar la actualización del documento Guía Análisis del Impacto del Negocio con una frecuencia de revisión apropiada, acorde al contexto y los riesgos del negocio, incorporando entre otros aspectos como los que se detallan a continuación y establecer e implementar un cronograma formal de revisión anual y definir responsables para su mantenimiento: 1. <u>Aspectos Generales:</u>		

3

- Para fortalecer la eficacia del Plan de Continuidad del Negocio (PCN), se recomienda implementar una estrategia de actualización continua mediante un cronograma de revisión semestral o anual del Análisis de Impacto al Negocio (BIA), con responsables claramente designados para su mantenimiento.
 - Asegurar la integración y coherencia entre el BIA, el Plan de Recuperación ante Desastres (DRP) y el Punto Alterno de Continuidad (PAC), validando que los tiempos definidos en cada uno estén alineados.
 - Para facilitar la priorización, se sugiere incorporar herramientas visuales como mapas de calor, diagramas de flujo y gráficos comparativos que evidencien la evolución de los tiempos de recuperación antes y después de los simulacros; documentando sistemáticamente los resultados de las pruebas, incluyendo lecciones aprendidas, y establecer un plan anual de simulacros.
 - En cuanto a la gestión de terceros, es clave identificar proveedores críticos, evaluar sus propios planes de continuidad y verificar la alineación de sus BIA con el de CAJA HONOR.
 - Incluir escenarios de riesgos emergentes como ciberataques, fallos en servicios en la nube o configuraciones erróneas de inteligencia artificial, evaluar la resiliencia digital de los procesos dependientes de tecnología, capacitar periódicamente a los responsables de procesos críticos y desarrollar un manual simplificado para los equipos operativos.
 - Registrar en el control de cambios la actualización correspondiente del documento, toda vez que se observó que no ha sido actualizado desde la vigencia 2023.
2. Aspectos Específicos:
- En la sección de *Metodología*, se sugiere clarificar el marco de referencia utilizado, ya que actualmente no se evidencia una alineación explícita con normas reconocidas; además, es recomendable incluir una descripción más precisa de las fases del proceso y los responsables asignados, complementada con ejemplos de aplicación por proceso.
 - En cuanto a la *Evaluación de criticidad*, se recomienda validar que los criterios de impacto estén alineados con los objetivos estratégicos de la organización, e incorporar el impacto reputacional y el cumplimiento normativo como dimensiones independientes.
 - Respecto a los *Aplicativos*, es necesario verificar que todos los sistemas listados cuenten con respaldo y planes de restauración documentados, así como identificar y registrar las dependencias tecnológicas entre ellos.
 - En la sección de *Recursos mínimos*, se debe asegurar que los recursos definidos sean suficientes para operar desde un punto alternativo, incluyendo un inventario detallado de equipos y accesos requeridos.
 - Para continuar con el fortalecimiento del plan, se recomienda integrar las observaciones antes citadas en una versión actualizada del Análisis de Impacto al Negocio (BIA), elaborar una presentación ejecutiva para la alta dirección y diseñar una plantilla editable que facilite futuras actualizaciones del plan.

Mayor

Debe estar implementada en un periodo no mayor a 6 meses

Lo anterior, dado que se evidenció que el documento no ha sido actualizado desde la vigencia 2023, pese a que su revisión debe realizarse al menos de forma anual y cada vez que ocurran cambios significativos en la Entidad. Conforme a la norma ISO 22301, el BIA constituye un documento dinámico que requiere ajustes periódicos y no debe considerarse una actividad única, debiendo actualizarse tras incidentes relevantes, auditorías internas o modificaciones sustanciales en procesos, tecnología o estructura organizacional.

En este contexto, las acciones propuestas buscan garantizar el cumplimiento de normativas nacionales e internacionales aplicables a la gestión de continuidad del negocio, tales como la NTC ISO/IEC 22301, el Modelo Integrado de Planeación y Gestión (MIPG), y disposiciones regulatorias como la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1474 de 2011 en materia de transparencia y control institucional. Asimismo, se alinean con los requerimientos de la Superintendencia Financiera, que exige contar con planes de recuperación ante desastres, gestión de terceros y continuidad operativa. Es de anotar que, la implementación de estas medidas permite fortalecer la trazabilidad, la alineación entre componentes del PCN (BIA, DRP, PAC), y la capacidad de respuesta ante eventos disruptivos; minimizar riesgos operacionales, tecnológicos y reputacionales, tales como la pérdida de información crítica, la interrupción de servicios esenciales, el incumplimiento normativo y la exposición a ciberataques o fallos en servicios digitales. También contribuyen a mejorar la resiliencia organizacional, facilitar la toma de decisiones en escenarios de crisis, garantizar la continuidad de procesos críticos y generar confianza en los grupos de interés o partes interesadas. De igual forma, la

	<p>incorporación de herramientas visuales, simulacros documentados, gestión de proveedores críticos y capacitación periódica refuerza la eficacia del PCN y su capacidad de adaptación frente a riesgos emergentes. Se observó el R029 - Fallas en la Gestión del Plan de Continuidad del Negocio (PCN), CA029 - Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad.</p>		
4	<p>Oportunidad de Mejora Correctiva No. 4: la OFCIN recomienda a la OAGRI en coordinación con los demás procesos interrelacionados implementar mecanismos de evaluación antes, durante y después de las capacitaciones relacionadas con el Plan de Continuidad del Negocio - PCN, que permitan medir el nivel de comprensión, apropiación y percepción de los asistentes, así como analizar los resultados obtenidos para identificar brechas de conocimiento, retroalimentar estratégicamente el proceso formativo y aplicar acciones correctivas cuando sea necesario; toda vez que durante la revisión del proceso de capacitación relacionado con el Plan de Continuidad del Negocio - PCN, se evidenció que, si bien se cuenta con soportes que demuestran la realización de actividades formativas, no se identificó la aplicación de instrumentos de evaluación ni el análisis de resultados que permitan determinar el nivel de comprensión, apropiación o percepción de la información por parte de los asistentes; lo que limita la trazabilidad del impacto formativo, dificulta la retroalimentación estratégica del proceso y restringe la implementación de acciones correctivas en caso de reprobación, afectando la eficacia del programa y el cumplimiento de los requisitos establecidos en la norma ISO 22301:2019, cláusula 7.2, y el numeral 3.2.4 de la CE 006 de 2025. La ausencia de estos mecanismos incrementa el riesgo de desinformación del personal frente a sus roles en situaciones de contingencia, una respuesta ineficaz ante eventos disruptivos y la pérdida de continuidad operativa, comprometiendo la resiliencia organizacional. Se observó el R029 - FALLAS EN LA GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN).</p>	Moderado	Debe estar implementada en un periodo no mayor a 9 meses.
5	<p>Oportunidad de Mejora Correctiva No. 5: la OFCIN recomienda a la OAGRI, la actualización del documento MATRIZ COMUNICACIÓN PCN.xlsx integrando la totalidad de los procesos de la Entidad y partes interesadas internas y externas, asegurando una visión integral y coordinada para la gestión de comunicación en situaciones críticas. Asimismo, incorporar los elementos de control documental como fecha de elaboración, número de versión y control de cambios, conforme a las directrices del Sistema de Gestión Documental, además de ser importante la formalización del documento mediante las firmas correspondientes y garantizar su socialización en la Entidad y la alineación de la citada matriz con el Plan de Continuidad del Negocio (PCN), asegurando coherencia con los lineamientos normativos y las mejores prácticas. Lo anterior, toda vez que la OFCIN observó que el documento MATRIZ COMUNICACIÓN PCN.xlsx suministrado por la OAGRI, utilizado para la gestión de comunicación en escenarios críticos, no contempla la totalidad de los procesos de la Entidad, limitándose únicamente a Gestión Informática, Gestión Administrativa, Gestión de Talento Humano y Gestión Estratégica, situación que puede generar vacíos en la articulación y respuesta integral ante eventos disruptivos, afectando la efectividad del Plan de Continuidad del Negocio – PCN. De igual forma, se identificó la ausencia de la firma del responsable y del funcionario que lo proyectó, actas de socialización, control de cambios del documento que garantice la trazabilidad, transparencia e integridad, permitiendo identificar qué modificaciones se realizaron, quién las efectuó y en qué fecha, asegurando un historial claro para auditorías y revisiones. Además, de asegurar que la versión vigente sea la correcta, evitando el uso de información desactualizada y manteniendo la alineación con actualizaciones normativas o estratégicas y en el marco de documentos críticos como la matriz de comunicación del PCN, este control reduce riesgos operacionales al asegurar que todos los actores trabajen con información validada y actualizada. Lo anterior en aras de dar cumplimiento a la Política de Continuidad del Negocio y Procedimiento de Comunicación en Crisis, que establece la obligación de incluir todos los procesos institucionales en la matriz de comunicación, Ley 594 de 2000 (Ley General de Archivos) – Principios de organización y conservación documental, Ley 1712 de 2014 (Transparencia y acceso a la información pública), Modelo Integrado de Planeación y Gestión (MIPG) V.6 de 2024, Dimensión 5. Información y Comunicación – Lineamiento sobre gestión documental y trazabilidad, Norma Técnica Colombiana NTC ISO 22301 – Requisitos para la gestión de continuidad del negocio, incluyendo comunicación y control de la información, Políticas internas de gestión documental (control de cambios, versiones y trazabilidad), Circular Externa 006 de 2025 - Planes de Continuidad del Negocio (PCN) y la matriz de comunicaciones en escenarios de crisis - Parte I – Instrucciones Generales, específicamente en el Capítulo relacionado con Gestión del Riesgo Operacional y Continuidad del Negocio. Se observó el R029 - Fallas en la Gestión del Plan de Continuidad del Negocio (PCN) por causas asociadas con CA029 - Falta de Actualización y Capacitación de los Procedimientos Frente a la Normatividad.</p>	Moderado	Debe estar implementada en un periodo no mayor a 9 meses.

6	<p>Oportunidad de Mejora Correctiva No. 6: la OFCIN recomienda a la OAINF en coordinación con la OAGRI y demás procesos interrelacionados implementar un cronograma acelerado y estructurado por fases para culminar el proceso de actualización del sistema operativo en los equipos de Caja Honor, para lo cual se sugiere la inclusión de aspectos tales como los que a continuación se relacionan:</p> <ul style="list-style-type: none"> • Fase 1 (inmediata): Inventario completo y pruebas de compatibilidad en todos los equipos pendientes. • Fase 2 (próximos 2 meses): Migración prioritaria de equipos críticos y capacitación del personal. • Fase 3 (máximo 3 meses): Finalizar la actualización del 100% de los equipos, validando el Plan de Continuidad y asegurando la operación sin interrupciones. <p>Asimismo, realizar la Actualización de la política interna incluyendo la obligación de mantener soporte activo, definir plazos máximos de migración y detallar roles de control y seguimiento; además de realizar la Capacitación del personal de TI y auditoría interna sobre la importancia del ciclo de vida del software operativo, el riesgo regulatorio asociado a sistemas sin soporte, y los procedimientos de continuidad del negocio; acciones permitirán cumplir con la normativa vigente, fortalecer la ciberseguridad y garantizar la continuidad operativa de la Entidad frente a incidentes tecnológicos.</p> <p>Lo anterior, toda vez que se identificó que la Entidad mantiene un número significativo de equipos (22) aun operando con Windows 10, sistema operativo que perdió soporte oficial el 14 de octubre de 2025, situación que representa un incumplimiento de la política interna de actualización que exige soporte activo y parches al día y de estándares internacionales de continuidad operativa y ciberseguridad, tales como ISO 22301 (cláusulas 6 y 7 relativas a la planificación del BCMS - Sistema de Gestión de Continuidad del Negocio, gestión de riesgos, asignación de recursos y mantenimiento del sistema y la cláusula 8, que exige controles operacionales para asegurar la continuidad frente a incidentes tecnológicos críticos al no aplicar mitigaciones para sistemas obsoletos en un entorno de continuidad del negocio), además del incumplimiento de la norma ISO/IEC 27001:2022 numerales A.8.8 (Vulnerabilidades), al no identificar ni corregir vulnerabilidades técnicas; A.5.10 (Malware), al dejar los sistemas expuestos a amenazas conocidas; A.8.32 (Gestión de cambios), por no implementar cambios formales en sistemas operativos; Cláusula 8 (Operación), al omitir la ejecución de controles operacionales esenciales; y Cláusula 10 (Mejora), al no garantizar la actualización continua del ISMS - Sistema de Gestión de Seguridad de la Información - SGSI. En consecuencia, se observó el RSI008 - ERROR EN EL USO, CSI045 - FALTA DE CONCIENCIA ACERCA DE LA SEGURIDAD, R029 - FFALLAS EN LA GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO (PCN), CA029 - FALTA DE ACTUALIZACIÓN Y CAPACITACION DE LOS PROCEDIMIENTOS FRENTE A LA NORMATIVIDAD.</p>	Mayor	Debe estar implementada en un periodo no mayor a 6 meses
7	<p>Oportunidad de Mejora Correctiva No. 7: la OFCIN recomienda a la OAGRI en coordinación con la OAINF y demás procesos interrelacionados, formalizar e integrar de manera prioritaria los indicadores RTO, RPO, porcentaje de pruebas exitosas en el DRP, Disponibilidad de recursos críticos; además de establecer un cronograma de revisión periódica y mantener un registro detallado de incidentes reales y su respuesta. Con ello, se fortalece el cumplimiento normativo, se mejora la capacidad de respuesta y se garantiza una gestión basada en datos que proteja la continuidad operativa y la confianza institucional. La adopción de estos elementos no solo facilitará la evaluación objetiva del desempeño del DRP, sino que también permitirá identificar brechas, optimizar procesos y garantizar la resiliencia operativa frente a eventos disruptivos. Adicionalmente, se sugiere establecer un cronograma de pruebas que aseguren la actualización continua del plan, así como la integración de estos indicadores en los reportes de gestión del PCN, para fortalecer la toma de decisiones basada en datos y cumplir con estándares de mejores prácticas en continuidad del negocio. Lo anterior, toda vez que se identificó que la Entidad no dispone de indicadores de desempeño formalizados para el Plan de Recuperación ante Desastres (DRP), lo cual transgrede los lineamientos de gestión del riesgo de la Superintendencia Financiera de Colombia (SFC), y su inclusión en la Circular Básica Contable y Financiera (CBCF), especialmente en los Capítulos relacionados con Gobierno Corporativo y Administración del Riesgo Operacional, que implican la obligación de mantener sistemas robustos de continuidad del negocio y recuperación ante desastres. Asimismo, la carencia de indicadores de desempeño como RTO, RPO y porcentaje de pruebas exitosas impide cumplir con las expectativas prudenciales definidas por la SFC, así como con las mejores prácticas estipuladas en normas internacionales como la ISO 22301:2019, cláusula 9, que exige el monitoreo y revisión continua del desempeño del Sistema de Gestión de Continuidad del Negocio. En consecuencia, puede generar impactos reputacionales, sanciones regulatorias, pérdidas operativas y financieras, y una disminución significativa en la</p>	Moderado	Debe estar implementada en un periodo no mayor a 9 meses.

resiliencia institucional. Se observó el R062 - INDISPONIBILIDAD DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI) CA062 - FALLAS EN LA INFRAESTRUCTURA DEL DATACENTER ALTERNO, RSI077 - DENEGACION DE SERVICIOS POR CIBERATAQUES CSI078 - FALTA DE MECANISMOS DE MONITOREO ESTABLECIDOS PARA LAS BRECHAS DE SEGURIDAD.

Fuente: elaboración propia OFCIN, diciembre 2025.

a. Síntesis Recomendaciones

Tabla 22 Consolidado Recomendaciones

#	RECOMENDACIONES
1	Recomendación No. 1: la OFCIN recomienda a la OAGRI implementar de manera integral las acciones definidas en el Plan de Mejoramiento derivado de la auditoría 24 del año 2024, que tiene como fecha de implementación el día 30/01/2026, lo anterior en atención a aprobación de los Riesgos de Fraude por la Junta Directiva en sesión de 29-04-2024 según Acta 5, y remitido a la OAGRI, mediante comunicado interno GERGE-359-01-2024070900078.
2	Recomendación No. 2: la OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados fortalecer los siguientes apartados dentro del documento MANUAL DE GESTIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO – PCN: 1. Apartado de Indicadores de Desempeño: incorporando ejemplos concretos de KPIs como el <i>Tiempo Objetivo de Recuperación (RTO)</i> , el <i>porcentaje de cumplimiento de pruebas de continuidad</i> , y el <i>número de incidentes gestionados conforme al plan</i> . 2. Apartado Simulacros y Pruebas , se sugiere incluir un plan anual estructurado que detalle la frecuencia, tipo de ejercicios (activación de equipos de respuesta, recuperación de sistemas, simulacros de evacuación), y responsables, lo cual facilitará el seguimiento y mejora continua. 3. Apartado Integración con otros Sistemas , se valora positivamente la articulación con el SGSI y la norma ISO 27001; sin embargo, se recomienda complementar esta sección con la <i>alineación al marco NIST</i> , especialmente al <i>NIST SP 800-34 Rev. 1</i> , que establece lineamientos para la continuidad del negocio y recuperación ante desastres, asegurando que exista evidencia documental de esta integración que respalden la coherencia entre los sistemas, como matrices de correspondencia, actas de reuniones conjuntas, o procedimientos compartidos, mapeos entre los controles del PCN y el NIST Cybersecurity Framework (CSF), así como con prácticas documentadas en gestión de incidentes, análisis de impacto al negocio (BIA) y planes de recuperación, entre otros.
3	Recomendación No. 3: se recomienda a la OAGRI en coordinación con la Administración y los procesos de la Entidad, mantener el Comité de Continuidad del Negocio - CCN) como una instancia organizacional estratégica, dado que cumple funciones esenciales en la planificación, activación y supervisión de los planes de continuidad operativa, así como en la articulación entre los procesos durante situaciones críticas; esta recomendación surge del análisis realizado por la OFCIN, quien evidenció que el CCN desempeña un rol más amplio que el Equipo de Soporte de Comunicaciones para Crisis contemplado en la Resolución 396 de 2025, el cual se enfoca exclusivamente en la gestión del mensaje institucional y la protección de la reputación organizacional; aunque dicha resolución modifica la Resolución 604 de 2019 y omite la mención explícita del CCN, no prohíbe su existencia, lo que permite conservarlo como buena práctica alineada con estándares internacionales; en tanto que eliminar el CCN implicaría riesgos como la desarticulación operativa, pérdida de enfoque estratégico, debilitamiento de la gobernanza en continuidad, mayor exposición a impactos negativos y cumplimiento normativo parcial, afectando la capacidad institucional de respuesta ante eventos críticos, por el contrario, mantener el CCN aporta beneficios como una mayor capacidad de respuesta coordinada, fortalecimiento de la gobernanza en crisis, mejora en la toma de decisiones estratégicas, continuidad efectiva de procesos críticos y alineación con marcos internacionales de gestión de continuidad del negocio.
4	Recomendación No. 4: la OFCIN recomienda a la OAGRI en coordinación con la OAINF que para garantizar la efectividad del Plan de Recuperación de Desastres (DRP) y del Punto Alterno de Continuidad (PAC), se implemente un enfoque integral que incluya la validación completa del DRP, asegurando que las pruebas no solo contemplen el failover y failback, sino también el cumplimiento de los objetivos de recuperación (RTO y RPO), la integridad de los datos y la operatividad de los servicios críticos en el entorno alterno, conforme a los lineamientos de la Ley 1523 de 2012 sobre Gestión del Riesgo de Desastres , directrices de la Unidad Nacional para la Gestión del Riesgo de Desastres - UNGRD para continuidad operativa; documentación exhaustiva , registrando tiempos, incidencias y acciones correctivas, en cumplimiento con estándares como ISO 22301:2019 sobre Sistemas de Gestión de Continuidad del Negocio; fortalecimiento operativo y técnico del PAC , mediante la capacitación previa del personal clave, revisiones anticipadas de equipos y pruebas de conectividad VPN, alineadas con las políticas de seguridad de la información (Ley 1581 de 2012 y Decreto 1377); y actualización y control de procedimientos , incorporando controles preventivos y ajustes derivados de las lecciones aprendidas, así como los lineamientos de la Circular Externa 006 de 2025, Parte I, Título I, Capítulo VIII (Espacio Controlado de Pruebas - ECP) , que exige la realización de pruebas periódicas y documentadas para garantizar la continuidad operativa y tecnológica, incluyendo escenarios de contingencia, validación de RTO y RPO, capacitación del personal y reporte de resultados a la SFC. Lo anterior, con el objeto de minimizar riesgos asociados con la pérdida de datos críticos, fallas en la conectividad del PAC que impidan la operación remota, errores humanos por falta de capacitación, vulnerabilidades frente a ciberataques durante la contingencia y afectación reputacional y financiera por interrupciones prolongadas.
5	Recomendación No. 5: la OFCIN recomienda a la OAGRI, en coordinación con la OAINF y demás procesos interrelacionados, garantizar que:

	<ol style="list-style-type: none"> 1) Garantizar que la gestión del minutograma en el marco de las pruebas de continuidad no se limite al registro efectuado por el proveedor sino que la Entidad documente sus propias observaciones y realice la conciliación entre ambos registros antes de emitir el informe final, asegurando consistencia, integridad, transparencia y confiabilidad en la evaluación del ejercicio, así como la alineación estratégica con la gestión de continuidad. 2) Dado que el minutograma constituye un registro oficial del ejercicio de simulacro, es fundamental (considerado una buena práctica) que dicho documento (Minutograma_Caja Honor_PruebaDRP_02y03mayo2025.pdf) incluya la fecha de realización y la firma del responsable, aspectos que otorgan validez y autenticidad del registro, siendo indispensables para auditorías internas y externas, así como para el cumplimiento de estándares internacionales como ISO 22301. Estos datos permiten verificar la correcta ejecución del simulacro, identificar responsables y asegurar que el documento constituye evidencia válida del ejercicio. La ausencia de esta información compromete la confiabilidad del registro y dificulta la gestión documental en procesos de continuidad del negocio y recuperación ante desastres. Lo anterior, toda vez que se evidenció que el documento identificado con Código AE3.16-F36, versión 14-feb-2014, generado por el proveedor CLARO no contiene estos datos esenciales. 3) Verificar la correcta paginación del documento, dado que, aunque contiene un total de 25 páginas, tanto la primera como la última presentan la leyenda “Pág. 1 de 1”, lo cual no corresponde con la numeración real y puede generar inconsistencias en la gestión documental. Lo anterior, en tanto que se observó que el archivo en formato PDF presenta un total de 25 páginas; sin embargo, tanto en la primera como en la última página se indica “Página 1 de 1”, lo que genera inconsistencias en la numeración y dificulta la trazabilidad del contenido. <p>Lo anterior, con el propósito de contribuir al cumplimiento normativo y a la mitigación de riesgos asociados a la vulneración de disposiciones como la Circular Externa 006 de 2025 de la Superintendencia Financiera de Colombia (SFC), Capítulo de Gestión del Riesgo Operacional y de Continuidad del Negocio, Numeral 4.2.2, que exige evidencias documentadas de pruebas y validación de planes de recuperación y continuidad; la Dimensión 5 – Información y Comunicación del Modelo Integrado de Planeación y Gestión (MIPG) V.6 de 2024, que garantiza la gestión documental y el acceso a la información; y estándares internacionales como ISO 22301 (Gestión de Continuidad del Negocio) e ISO/IEC 27001 (Seguridad de la Información). El incumplimiento de estas directrices puede generar riesgos significativos, tales como brechas en la trazabilidad, ausencia de evidencia para auditorías, sanciones regulatorias, pérdida de confianza de los grupos de interés y debilitamiento de la resiliencia organizacional.</p>
6	<p>Recomendación No. 6: la OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados, establecer un proceso de actualización periódica (trimestral) del inventario de colaboradores con trabajo en casa o remoto, utilizando herramientas de gestión centralizada que permitan validar la autorización vigente y la correlación con los recursos asignados (equipos, accesos y licencias). Adicionalmente, se sugiere implementar indicadores de variación anual para anticipar necesidades tecnológicas y de seguridad alineados con estándares de ISO 27001, incluyendo autenticación multifactor, cifrado, VPN segura y gestión del ciclo de vida de activos, considerando el incremento observado en la vigencia 2025 (35 colaboradores) frente a 2024 (10 colaboradores). Este control preventivo contribuye a la continuidad operativa, la mitigación de riesgos y la optimización de costos asociados a la modalidad remota, información que es fundamental para la toma de decisiones por parte de la Entidad respecto de la implementación de modalidades laborales como trabajo remoto o híbrido conforme a la normativa vigente.</p>
7	<p>Recomendación No. 7: la OFCIN recomienda a la OAGRI en coordinación con procesos interrelacionados, incorporar en la guía GR-GU-005 “GUÍA DE OPERACIÓN PUNTO ALTERNO DE CONTINUIDAD – PAC, V16 – 31-10-2025”, la normativa aplicable para la modalidad de teletrabajo (mixta, híbrida, autónoma o móvil), como lo es la Ley 1221 de 2008, el Decreto 884 de 2012 (compilado en el Decreto 1072 de 2015) y el Decreto 1227 de 2022; además de la Normativa de gestión de continuidad NTC-ISO/IEC 22301, que establece los lineamientos para la gestión de continuidad del negocio, definiendo procedimientos, roles, comités y documentación requerida para la activación del PAC. Lo anterior, toda vez que la incorporación de la normativa citada es esencial porque asegura que la estrategia de trabajo a distancia y la activación del Punto Alterno de Continuidad (PAC) se realicen bajo un marco legal y técnico que garantice el cumplimiento regulatorio, la protección de derechos laborales y la alineación con estándares internacionales. Esto permite minimizar riesgos como sanciones por incumplimiento normativo, vulnerabilidades operativas y tecnológicas, pérdida de información, descoordinación en la activación del PAC, afectación de la continuidad del negocio y exposición a riesgos reputacionales y financieros; dando cumplimiento a lo estipulado en la Circular Externa 006 de 2025 Parte I – Título I, Capítulo I: Organización y Numeral 1.2 – Documentación requerida y Numeral 1.3 – Especificidad en constitución de entidades; adicionalmente con MIPG v6 de 2024, Dimensión 1. Dirección estratégica y planeación que formaliza la estrategia de trabajo remoto dentro del PAC, alineada con el direccionamiento institucional y Dimensión 5 – Información y Comunicación. Lo anterior, en aras de fortalecer la gobernanza, la trazabilidad y la resiliencia institucional frente a eventos críticos.</p>
8	<p>Recomendación No. 8: la OFCIN recomienda a la OAGRI, en coordinación con los procesos interrelacionados, implementar acciones que garanticen la participación del 100% del personal asignado al proceso PAC y, en general, a las actividades de Continuidad del Negocio en todas las capacitaciones impartidas para el fortalecimiento y desarrollo de los simulacros de continuidad, estableciendo un plan de seguimiento y control de asistencia, reforzar la comunicación sobre la obligatoriedad de las capacitaciones, programar sesiones adicionales que aseguren la cobertura total del personal y evaluar mecanismos de registro y reporte que permitan evidenciar la participación efectiva en las actividades de formación. Lo anterior teniendo en cuenta que en el proceso PAC se cuenta con 47 colaboradores asignados; sin embargo, en las capacitaciones realizadas los días 30 de abril y 19 de mayo se registró la asistencia de únicamente 30 y 23 participantes, respectivamente, lo que evidencia una brecha significativa en la cobertura de formación. En consecuencia, la falta de cobertura en la capacitación vulnera los principios establecidos en la ISO 22301:2019, específicamente la Cláusula 7.2 – Competencia, que exige que el personal sea competente para desempeñar su rol en la continuidad del negocio, y la Cláusula 8.4 – Ejercicios y pruebas, que requiere simulacros con personal capacitado para garantizar la eficacia del Sistema de Gestión de Continuidad del Negocio – BCMS; situación que puede generar riesgos operacionales, por deficiencias en la ejecución de simulacros; de cumplimiento, por posibles hallazgos en auditorías internas o externas; y reputacional, por una percepción negativa sobre la preparación institucional ante incidentes.</p>

9	<p>Recomendación No. 9: la OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, ampliar e implementar el conjunto de indicadores incorporando métricas que midan la Cobertura y Preparación (porcentaje de procesos críticos con plan probado y personal entrenado), la Eficacia de Recuperación (tiempo de activación del plan – RTO y cumplimiento del objetivo de punto de recuperación – RPO) y la Mejora Continua (hallazgos en simulacros y acciones correctivas implementadas). Esta ampliación permitirá contar con una visión integral del desempeño del PAC, fortaleciendo la resiliencia organizacional y asegurando que las pruebas no solo midan participación, sino también efectividad y alineación con los objetivos estratégicos. Así las cosas, minimizar la materialización de riesgos asociados a la falta de visibilidad sobre la capacidad de recuperación, lo que puede ocasionar tiempos prolongados de interrupción; incumplimiento normativo, que podría derivar en posibles sanciones y afectación reputacional y financiera, al no garantizar la continuidad de procesos críticos.</p>
10	<p>Recomendación No. 10: la OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, que para garantizar la integridad del proceso gestión de incidentes y la capacidad de análisis, se implemente un formato que incluya, como mínimo, los siguientes campos: <i>ID del incidente, fecha y hora, descripción detallada, categoría, impacto, estado, responsable, tiempo de resolución, acciones correctivas y observaciones</i>; información que permite evaluar el desempeño, medir el cumplimiento de los SLA - Acuerdo de Nivel de Servicio y generar reportes confiables para auditorías y mejora continua; pues mantener un registro incompleto limita la trazabilidad y dificulta la identificación de patrones recurrentes, lo que incrementa el riesgo de reincidencia y afecta la capacidad de respuesta ante incidentes críticos; lo que puede derivar en hallazgos y vulneración de normativas aplicables, particularmente la Circular Externa 008 de 2018, numeral 2.3.4 (Capítulo I, Título II), que exige soporte documental completo para operaciones y eventos, y la Circular Básica Jurídica 006/25, Parte I – Instrucciones Generales, que establece la obligación de mantener procesos internos documentados y trazables. El incumplimiento de estas disposiciones expone a la Entidad a sanciones y pérdida de confianza, mientras que un registro robusto fortalece la gobernabilidad y la resiliencia operativa, en línea con las mejores prácticas de ITIL 4 y la norma ISO/IEC 27001 (Anexo A.16).</p>
11	<p>Recomendación No. 11: la OFCIN recomienda a la OAGRI en coordinación con los procesos interrelacionados, complementar el Plan de actualizaciones del PAC con datos tales como Frecuencia y metodología de las actualizaciones, Responsables del seguimiento y ejecución, Procedimiento para identificar cambios internos, tecnológicos o externos, Mecanismos de validación y pruebas posteriores a cada actualización y Plan de comunicación y capacitación tras cada actualización. Lo anterior, en aras de dar cumplimiento a las buenas prácticas establecidas en marcos como ITIL y normas ISO 27001, minimizando la generación de riesgos operacionales (interrupción del servicio), de seguridad (vulnerabilidades no detectadas), de cumplimiento (sanciones por normativa) y reputacionales (pérdida de confianza).</p>
12	<p>Recomendación No. 12: la OFCIN recomienda a la OAGRI, en coordinación con OAINF y demás procesos interrelacionados, que en futuros ejercicios de simulacro del DRP se incorpore la ejecución de la replicación inversa (failback), la validación de la sincronización a nivel de almacenamiento y la precisión en los tiempos de recuperación documentados, toda vez que estas acciones son esenciales para garantizar la integridad y consistencia de los datos durante todo el ciclo de recuperación, así como para establecer mecanismos robustos que permitan registrar de manera confiable los RTO y RPO alcanzados, en cumplimiento de la norma ISO 22301:2019 (cláusula 8.4) y los lineamientos regulatorios de la SFC, particularmente lo dispuesto en la Circular Externa 007 de 2018, numeral 4.1.7 sobre pruebas del plan de continuidad y en la Circular Externa 008 de 2018, que modifica numerales como 1.2.2.1.2.7 y 2.3.4.1.3, relacionados con seguridad y calidad en la operación, en donde su implementación contribuirá a mitigar riesgos operacionales y regulatorios, fortaleciendo la resiliencia tecnológica de la organización.</p> <p>Lo anterior se fundamenta en que, durante la revisión del informe de la prueba DRP realizada los días 02 y 03 de mayo de 2025, se evidenció que el alcance no contempló la replicación inversa ni la validación de sincronización, prácticas indispensables para asegurar el retorno seguro al sitio principal sin pérdida de datos ni afectación de la operación. Esta omisión contraviene lo dispuesto en la ISO 22301:2019, cláusula 8.4, y las buenas prácticas nacionales que exigen la definición y verificación de RTO y RPO. Adicionalmente, se observó falta de precisión en los tiempos de recuperación documentados, lo que limita la confiabilidad de los indicadores críticos y puede generar impactos significativos como pérdida de integridad de datos, interrupciones prolongadas, sanciones por incumplimiento normativo y deterioro reputacional frente a clientes y entes reguladores.</p>
13	<p>Recomendación No. 13: la OFCIN recomienda a la OAGRI, en coordinación con la OAINF, fortalecer la arquitectura tecnológica del Plan de Recuperación ante Desastres (DRP) mediante la incorporación de replicación de almacenamiento entre sitios, clústeres de alta disponibilidad, enlaces de red redundantes, mecanismos de orquestación para recuperación automatizada y copias de seguridad aisladas (air-gapped) para mitigar riesgos como ransomware, además, se debe garantizar la sincronización de políticas de seguridad, certificados digitales y gestión de identidades en entornos alternos, junto con monitoreo centralizado y pruebas periódicas del DRP; de forma tal que se dé cumplimiento a la normativa del SFC, mediante directrices institucionales que definen los RTO y RPO como parte del marco de continuidad operacional en ambientes críticos, alineación con la ISO 27001:2022, que exige un plan de recuperación documentado e implementado para proteger la disponibilidad de la información crítica, y la ISO/IEC 27031, que define lineamientos para desarrollar capacidades de continuidad TIC alineadas con la gestión de riesgos. Adicionalmente, acatando lineamientos de la Ley 1523 de 2012, que establece “la gestión del riesgo incorpora prevención, atención y recuperación de desastres”; el Decreto 2157 de 2017, que obliga a “diseñar e implementar las medidas de reducción del riesgo y planes de emergencia y contingencia que serán de su obligatorio cumplimiento”; el Decreto 338 de 2022, que ordena “establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital. Lo anterior, con el objeto de mitigar riesgos como pérdida crítica de datos, interrupciones prolongadas, incumplimiento normativo, sanciones por parte de la SFC e impactos reputacionales, además de fortalecer la resiliencia tecnológica y garantizar la continuidad operativa de la Entidad.</p>

Fuente: elaboración propia OFCIN, diciembre 2025.

3. NIVEL DE PRIORIZACIÓN DE CRITICIDAD DE LOS HALLAZGOS

Criterios de Criticidad		
5	Crítico	de 23 a 30
4	Mayor	de 18 a 22
3	Moderado	de 13 a 17
2	Menor	de 9 a 12
1	Mínimo	de 6 a 8

De acuerdo con la expedición de la CE 008 de 2023 de la SFC, en sus numerales 4.2.3.1 de las Funciones del Comité de Auditoría respecto del ambiente de control, 4.5.3.3 y 4.5.4.2 de las Funciones de la Auditoría Interna respecto de las actividades de control y de información y comunicación respectivamente, se realizó la creación de la metodología de la Criticidad de los Hallazgos para la OFCIN en cumplimiento a la mencionada Circular y la presentación de esta en los informes y al Comité de Auditoría.

Por esta razón, para la evaluación de la criticidad de los hallazgos, hemos adoptado una metodología estructurada que permite una clasificación precisa y objetiva de cada hallazgo y se basa en una combinación de factores cuantitativos y cualitativos diseñados para evaluar el impacto potencial de cada hallazgo en las operaciones y la salud organizacional de la entidad, observando lo siguiente:



Matriz
Criticidad_RO y PCN

Fuente: OFCIN, Matriz Priorización Criticidad de los Hallazgos.

Este análisis se divide en segmentos, cada uno correspondiente a un nivel de criticidad: Crítico, Mayor, Moderado, Menor, Mínimo. Para cada categoría, se discuten los hallazgos específicos, sus implicaciones potenciales y las recomendaciones adecuadas.

Crítico

Son aquellos que presentan un riesgo inminente a la viabilidad financiera, legal o reputacional de la Entidad. Requieren atención inmediata debido a su potencial para provocar consecuencias severas.

Acciones Recomendadas: Implementación urgente de medidas correctivas, revisión de políticas y fortalecimiento de los controles internos.

Mayor

Los hallazgos 'Mayores' son serios, pero no tan inmediatos o amenazantes como los críticos; sin embargo, pueden deteriorar la eficiencia operativa y la conformidad normativa si no se tratan a tiempo.

En el marco de esta auditoría se evidenciaron los siguientes hallazgos en esta categoría:

- Deficiencias en controles internos que no han causado pérdidas inmediatas pero que presentan riesgos potenciales altos.

Acciones Recomendadas: Revisión y mejora de los procesos y controles afectados dentro de un plazo definido.

Moderado

Los hallazgos 'Moderados' implican problemas que poseen un impacto limitado en las operaciones y que pueden ser resueltos con ajustes menores en los procedimientos o controles existentes. Se evidenciaron los siguientes hallazgos en esta categoría:

- Inconsistencias en reportes internos que no afectan los resultados financieros globales.

Acciones Recomendadas: Ajustes en los procesos de reporte y capacitación adicional para el personal relevante.

Menor

Estos hallazgos tienen un impacto bajo y generalmente son de naturaleza operativa o de conformidad que requieren mejoras mínimas. Se evidenciaron los siguientes hallazgos en esta categoría:

- Pequeños errores en la documentación que no tienen efectos financieros o legales significativos.

Acciones Recomendadas: Correcciones simples y directas para mejorar la documentación o los procedimientos operativos.

Mínimo

Los hallazgos de 'Mínimo' impacto son esencialmente observaciones que no requieren acciones inmediatas pero que deben ser monitorizadas para evitar que escalen. En el marco de esta auditoría se evidenciaron los siguientes hallazgos en esta categoría:

Desviaciones menores de las mejores prácticas que no afectan el cumplimiento ni la eficacia operativa.

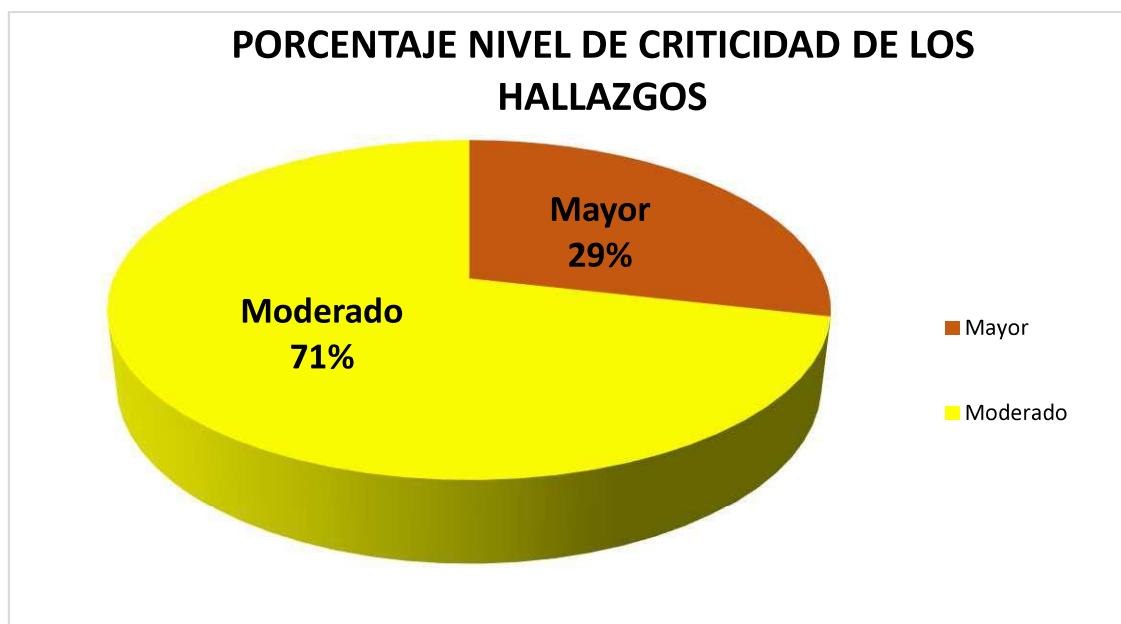


Figura 49. Fuente: Matriz Priorización Criticidad de los Hallazgos OFCIN

El gráfico de "Porcentaje Nivel de Criticidad de los Hallazgos" ofrece una visión clara y concisa sobre la distribución de los hallazgos auditados en función de su criticidad. Este análisis es fundamental para que la junta directiva evidencie la gravedad y urgencia de las acciones requeridas.

Moderados (71%): Constituyendo la mayoría de los hallazgos, los de nivel moderado indican problemas que, aunque necesitan ser abordados para mejorar los procesos y la eficiencia, no presentan un riesgo inmediato para la operatividad o la conformidad organizacional. Estos hallazgos ofrecen oportunidades significativas para mejoras proactivas y preventivas en las operaciones.

Mayor (29%): Este hallazgo, representa un riesgo importante para la Entidad, el cual requieren una acción rápida y una atención cercana para su pronta solución.

4. CONCLUSIONES

- Con el desarrollo de la presente auditoría, la OFCIN busca garantizar que las acciones de continuidad estén alineadas con los objetivos institucionales, promoviendo una cultura preventiva y asegurando la sostenibilidad del negocio frente a eventos disruptivos, en tanto que la auditoría del Plan de Continuidad del Negocio aporta un valor estratégico al identificar brechas y oportunidades de mejora que fortalecen la resiliencia organizacional. Este proceso no solo asegura el cumplimiento normativo, sino que también optimiza la capacidad de respuesta ante incidentes, reduciendo riesgos financieros y reputacionales, y generando confianza entre clientes, proveedores y demás partes interesadas.
- Entre otros aspectos, se resalta la necesidad de mantener actualizados documentos clave como el Análisis de Impacto al Negocio (BIA), base para definir prioridades y tiempos de recuperación; además de la implementar indicadores de desempeño en el Plan de Recuperación ante Desastres (DRP), permitiendo medir la efectividad de las estrategias y garantizar la mejora continua.
- Asimismo, teniendo en cuenta que la Oficina de Control Interno ejerce una supervisión independiente sobre la implementación y efectividad de los planes de continuidad del negocio, en donde su rol en los simulacros consiste en verificar el cumplimiento de políticas y procedimientos, evaluar la pertinencia de los controles aplicados, identificar desviaciones frente a los estándares definidos y emitir recomendaciones orientadas a la mejora continua, asegurando que los ejercicios no solo se ejecuten conforme a lo planeado, sino que también contribuyan a la transparencia, la mitigación de riesgos y la resiliencia institucional; es de vital importancia que se otorguen oportunamente los accesos requeridos, ya que la falta de estos limita la capacidad de supervisión independiente, impide la validación

objetiva de los resultados y genera riesgos asociados a decisiones basadas en información incompleta.

Cordialmente,

Original Firmado

MARTHA CECILIA MORA CORREA
Jefe Oficina de Control Interno

Original Firmado

Elaboró: Cpt. Jonathan Arley Peña Morales
Auditor Oficina de Control Interno

Original Firmado

Ing. Flor Alba Roncancio Gachancipá
Auditor Oficina de Control Interno