N.º 42

EMPRESA NACIONAL PROMOTORA DEL DESARROLLO TERRITORIAL S.A

ASESORIA DE CONTROL INTERNO

INFORME FINAL EVALUACIÓN DE CUMPLIMIENTO DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS (SIAR)

PERIODO EVALUADO:
enero de 2026 a julio de 2026*

Elaborado:
Manuela Hernández Jaramillo, Contrato No. 20261144 – Auditor ACI
Carlos Eduardo Buitrago Cano, Contrato No. 20261190 – Auditor ACI

* El establecimiento de este periodo no limitaba la facultad de la Oficina Asesora de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados

CONTENIDO

INFORMACIÓN GENERAL:..... 3
DESARROLLO DEL INFORME: 3
OBJETIVO..... 3
ALCANCE..... 3
LIMITACION DEL ALCANCE..... 4
MARCO LEGAL..... 4
NOTAS 4
RESULTADOS DEL SEGUIMIENTO..... 5
CONCLUSIONES..... 72
RECOMENDACIONES 75

INFORMACIÓN GENERAL:

NOMBRE DEL INFORME:	Informe Final de Evaluación del Cumplimiento del Sistema Integral de Administración de Riesgos (SIAR)
TIPO DE INFORME:	Informe de Ley Circular Externa 018 de 2021 Capítulo XXXI - Sistema Integral de Administración de Riesgos (SIAR) de la Circular Básica Contable y Financiera - CBCF 100 de 1995
DESTINATARIOS:	Armando Vivas Salamanca Gerente Grupo Gestión de Riesgos
FUENTE DE INFORMACIÓN:	Grupo Gestión de Riesgos Sistema Integrado de Gestión Enterritorio S.A.
EMITIDO POR:	Orlando Correa Nuñez Asesor con funciones de Control Interno
AUDITORES:	Manuela Hernández Jaramillo Carlos Eduardo Buitrago Cano

DESARROLLO DEL INFORME:

OBJETIVO

Evaluar el Sistema Integral de Administración de Riesgos (SIAR) – Parte 2 implementado en ENTerritorio S.A, con el fin de verificar el cumplimiento de los requisitos normativos establecidos por la Superintendencia Financiera de Colombia, particularmente los previstos en la Circular Externa 018 de 2021, Capítulo XXXI – Sistema Integral de Administración de Riesgos (SIAR), de la Circular Básica Contable y Financiera (CBCF 100 de 1995), y en las disposiciones internas contenidas en manuales, procedimientos, circulares, guías e instructivos aplicables.

El resultado se informa al Gerente del Grupo de Riesgos para que sea comunicado a la Junta Directiva de ENTerritorio S.A.

ALCANCE

El presente seguimiento abarca el periodo comprendido entre enero a julio del 2026, frente al desarrollo específico de la implementación, seguimiento y funcionamiento del SIAR, considerando sus etapas, elementos y componentes según lo dispuesto en el Capítulo XXXI – Sistema Integral de Administración de Riesgos (SIAR), de la Circular Básica Contable y Financiera (CBCF 100 de 1995) y las disposiciones internas aplicables según el Sistema Integrado de Gestión de la Sociedad. Los sistemas objeto de evaluación fueron:

- Gestión de Riesgo de Liquidez.
- Gestión de Riesgo de Mercado.
- Gestión de Riesgo Operacional.
- Plan de Continuidad del Negocio.

- Sistema Gestión de Seguridad de la Información.

LIMITACION DEL ALCANCE

Para la ejecución del Informe Evaluación de Cumplimiento de las Etapas del Sistema Integral de Administración de Riesgos (SIAR); no se presentaron limitaciones al alcance.

MARCO LEGAL

- Normatividad Externa:
  - Circular Externa 018 de 2021 Capítulo XXXI - Sistema Integral de Administración de Riesgos (SIAR) de la Circular Básica Contable y Financiera - CBCF 100 de 1995).
  - Circular Externa 004 de 2026, con aplicabilidad (entrada en vigencia) desde el 1 de junio de 2026.

- Reglamentación y procedimientos Internos vigentes:
  - M-RI-08 Manual del Sistema Integral de Administración de Riesgos (SIAR).
  - M-RI-05 Manual de continuidad del negocio.
  - M-RI-03 Manual de gestión de riesgo operacionales.
  - M-RI-01 Manual de gestión de riesgos financieros.
  - M-RI-06 Manual políticas seguridad información.
  - P-RI-04 Medición y seguimiento de riesgo de mercado por el método interno y verificación del cumplimiento de límites de riesgo de mercado.
  - P-RI-05 Medición y transmisión diaria del riesgo de mercado por el método estándar.
  - P-RI-08 Monitoreo a la Valoración de Portafolios de Inversión
  - P-RI-09 Monitoreo a las Inversiones en Custodia.
  - P-RI-11 Monitoreo a la transmisión de reportes de composición del portafolio de inversiones.
  - P-RI-012 Gestión de Riesgo de Liquidez
  - P-FI-29 Financiamiento ante contingencia de liquidez.
  - P-FI-30 Flujo de Caja
  - G-RI-03 Guía para el diligenciamiento del Registro de Eventos de Riesgo Operacional
  - L-TH-01 Plan Prevención Atención Emergencias
  - P-RI-17 Pruebas al Plan de Continuidad del Negocio

NOTAS

1. La naturaleza de la labor de auditoría interna ejecutada por la Asesoría de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo, recursos y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

2. La evidencia recopilada para propósitos del seguimiento efectuado versa en información suministrada por el personal y/o colaboradores pertenecientes al proceso o actividad evaluada, a través de solicitudes y consultas realizadas por la Asesoría de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.

RESULTADOS DEL SEGUIMIENTO

1.1. GESTIÓN DE RIESGO DE LIQUIDEZ

Dentro de la evaluación que se efectuó a este apartado, que en adelante será referido como Sistema de Administración del Riesgo de Liquidez – SARL, se abordaron los siguientes aspectos:

a) Eventos de riesgo de liquidez y gestiones derivadas.
b) Gobierno del riesgo de liquidez – reuniones de comités y análisis de informes.
c) Niveles de validación de inputs, seguridad y aprobación de hojas de cálculo de ejecución de la metodología.
d) Cálculo y reporte de indicadores de alerta temprana.
e) Desarrollo de herramientas de pronóstico y previsión de liquidez
f) Revisión de metodología y resultados de las pruebas de Backtesting y Stress-testing.

A continuación, se describe su desarrollo.

a) EVENTOS DE RIESGO DE LIQUIDEZ Y GESTIONES DERIVADAS

Dentro de los procedimientos planeados de esta Asesoría de Control Interno se encuentra el indagar por la existencia de eventos de riesgos (para este particular, los asociados a liquidez) y observar cómo Enterritorio S.A. gestionó el eventual plan de respuesta sobre el suceso y la referencia a las afectaciones padecidas.

Así las cosas, de acuerdo con la respuesta entregada en memorando 202617010002503 del 2 de septiembre de 2026, el grupo de riesgos manifestó que: *"(…) para el periodo evaluado no se presentaron (sic) materialización de riesgos de liquidez"*.

De manera alterna para corroborar esta afirmación, se verificó el archivo "Informe ERO Enero-Julio 2026" (respuesta a numeral 40 de Riesgo Operacional) para ver si existió para el periodo objeto de análisis algún evento de riesgo asociado a Liquidez, donde no se detectó ninguna coincidencia, y confirmando la afirmación del grupo de riesgos.

b) GOBIERNO DEL RIESGO DE LIQUIDEZ – REUNIONES DE COMITÉS Y ANÁLISIS DE INFORMES

Para validar las instancias de gobierno y monitoreo del SARL, se buscó obtener un entendimiento de los órganos corporativos creados por Enterritorio S.A, respecto de sus integrantes, periodicidad de sus reuniones y tipos de informes que deben ser puestos bajo su consideración. De esta manera, se pudo identificar la existencia del Comité de Riesgos y el Comité Interno de Riesgos.

El Comité de Riesgos de Enterritorio S.A. es uno de los Comités de Junta Directiva normado bajo el Acuerdo No. 348 del 29 de julio de 2025, cuyas instrucciones de funcionamiento se hallan en el capítulo VII, artículos 30 al 35. Está compuesto por 3 miembros de Junta Directiva, uno de los cuales debe tener la calidad de independiente. Se reunirá ordinariamente de forma trimestral, sin perjuicio de reunirse extraordinariamente de ser necesario. El parágrafo del artículo 32 señala que la primera reunión ordinaria de cada año se realizará en febrero, de acuerdo con el plan anual de trabajo previamente apruebe la Junta Directiva.

De otra parte, el Comité Interno de Riesgos (CIR) fue creado mediante Resolución No.303 del 10 de diciembre de 2024, se reunirá por lo menos una vez al mes y extraordinariamente cuando sea necesario. Sus miembros con voz y voto son:

* Presidente de Enterritorio S.A.
* Subgerente de Estructuración de Proyectos
* Subgerente de Desarrollo de Proyectos
* Subgerente Financiero
* Subgerente Administrativo
* Subgerente de Operaciones
* Jefe Oficina Asesora Jurídica
* Gerente Grupo de Gestión de Riesgos y
* Gerente Grupo de Planeación y Desarrollo Organizacional.

Serán invitados con voz, pero sin voto el Asesor de Control Interno y el Oficial de Cumplimiento SARLAFT y Antisoborno, además de otros invitados que se requiera según los temas a tratar. La única excepción a voto será del Subgerente Financiero en aquellos casos en los que se analicen proyectos de documentos de políticas de límites de riesgo de liquidez y mercado, cupos de emisor y contraparte y modificaciones o suspensiones de ellos.

Se pudo comprobar en la sección de quorum de cada una de las actas que se enuncia a continuación (salvo la de julio que no fue suministrada por estar en proceso de firmas) la asistencia de todos los miembros precitados, con las observaciones a que hubo lugar en algunos casos.

El resumen de las sesiones efectuadas de ambos órganos se muestra en la tabla 1, con el fin de validar que, para el periodo comprendido entre enero y julio de 2026, se cumplió con lo establecido en los respectivos reglamentos. Se evidencia que el Comité de Riesgos inicial se dio en febrero, y la otra sesión trimestral se dio en mayo; el CIR sesionó mensualmente:

Tabla No1. Sesiones mensuales de Comités de Riesgo y Comités Internos de Riesgo periodo enero a julio 2026

Mes	Fechas Comité Interno de Riesgos (CIR)	Fechas Comité de Riesgos (apoyo a JD)
Enero	29-ene-2026 / 12-feb-2026	24-feb-26
Febrero	19-feb-2026 / 25-feb-2026	
Marzo	26-mar-26	28-may-26
Abril	28-abr-26	
Mayo	20-may-26	
Junio	23-jun-26	Efectuado en agosto 2026
Julio	27-jul-26	

Fuente: Elaboración ACI a partir de revisión documental sesiones Comités.

c) NIVELES DE VALIDACIÓN DE INPUTS, SEGURIDAD Y APROBACIÓN DE HOJAS DE CÁLCULO DE EJECUCIÓN DE LA METODOLOGÍA.

<u>Observación No.1:</u> Falta de esquemas de validación o trazabilidad de calidad e integridad de los inputs del modelo de riesgo de liquidez y necesidad de implementación de alertas automáticas.

<u>Criterio</u>: Con el fin de establecer la fiabilidad y calidad del modelo de gestión del riesgo de liquidez, el manual de gestión de riesgos financieros señala en el numeral 4.2.2.1 *Fuentes de información para la medición del riesgo de liquidez* que: *"Para efecto de la estimación de la estructura probabilística de los pagos e identificar el máximo pago esperado, aplicable para cada uno de los componentes, misional y funcionamiento, se utilizarán las bases de datos presupuestales. Para esto, con una periodicidad semanal los Grupos de Contabilidad y Presupuesto generarán, consultas que contengan las series históricas diarias de datos de*:

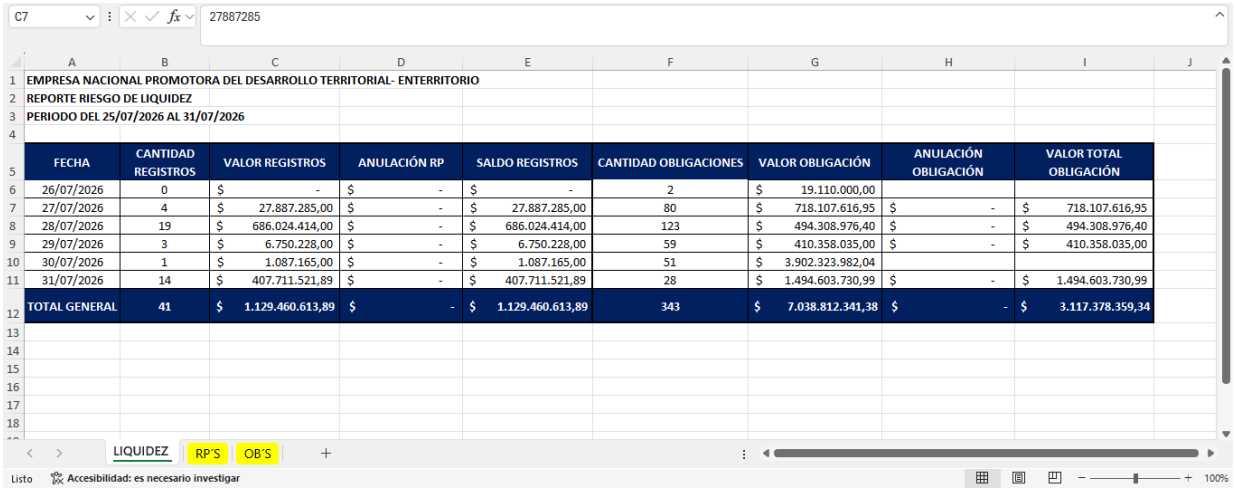
** Registros presupuestales expedidos (RPc).*
** Pagos registrados (Pc).*

Así mismo, estos grupos realizarán en forma previa a su remisión al Grupo de Gestión de Riesgos, <u>las validaciones correspondientes sobre esta información</u>, a fin de garantizar la calidad e integridad de la misma. [Énfasis añadido con subrayado].

<u>Situación observada</u>: Esta Asesoría de Control Interno realizó la siguiente indagación al grupo de riesgos: *"¿De qué manera y qué evidencia se deja de las validaciones efectuadas sobre la información consultada para garantizar la calidad y consistencia del informe consolidado de registros presupuestales y órdenes de pago de la última semana? (...)"* frente a la cual emitieron mediante memorando 202617010002503 del 2 de septiembre de 2026 la siguiente respuesta: *"de manera semanal, el Grupo de presupuesto remite el informe consolidado de registros presupuestales y órdenes de pago dirigidos al Grupo de Gestión de Riesgos el cual es el insumo principal para la generación del Informe de Medición Seguimiento y Control al Riesgo de Liquidez el cual es informado a las instancias correspondientes"*

Si bien se conoce que el aplicativo Dynamics 365 es la fuente de consulta de estas bases de datos, la contestación no enfatiza sobre cuáles son los mecanismos de validación de la extracción de la data que asegure su fiabilidad y el tipo de procesamiento que se hizo sobre ella previo a su reporte al grupo de riesgos. En particular, al revisar los archivos Excel tanto para funcionamiento como para convenios no se detectaron checks más allá de los totales de las bases de datos. Hubo conteos de RP repetidos, distorsionando la cantidad reportada (41 cuando deberían ser 39), aunque este dato en sí mismo no incide en el modelo sino en la exactitud de lo que se revela en el informe o la base de datos. La pestaña "Liquidez" presenta una tabla resumen de las hojas de RP's y Obligaciones, pero no fue posible evidenciar fórmulas o algoritmos de verificación, como se aprecia en la tabla 2, donde el dato de la celda C7 (y las demás, solo se ejemplifica para la demostración) no tiene ninguna fórmula vinculada:

Imagen No1. Data resumen de RP's y Obligaciones de la semana del 25 al 31 de julio sin formulaciones



C7 | 27887285

EMPRESA NACIONAL PROMOTORA DEL DESARROLLO TERRITORIAL- ENTERRITORIO
REPORTE RIESGO DE LIQUIDEZ
PERIODO DEL 25/07/2026 AL 31/07/2026

FECHA	CANTIDAD REGISTROS	VALOR REGISTROS	ANULACIÓN RP	SALDO REGISTROS	CANTIDAD OBLIGACIONES	VALOR OBLIGACIÓN	ANULACIÓN OBLIGACIÓN	VALOR TOTAL OBLIGACIÓN
26/07/2026	0	$ -	$ -	$ -	2	$ 19.110.000,00		
27/07/2026	4	$ 27.887.285,00	$ -	$ 27.887.285,00	80	$ 718.107.616,95	$ -	$ 718.107.616,95
28/07/2026	19	$ 686.024.414,00	$ -	$ 686.024.414,00	123	$ 494.308.976,40	$ -	$ 494.308.976,40
29/07/2026	3	$ 6.750.228,00	$ -	$ 6.750.228,00	59	$ 410.358.035,00	$ -	$ 410.358.035,00
30/07/2026	1	$ 1.087.165,00	$ -	$ 1.087.165,00	51	$ 3.902.323.982,04		
31/07/2026	14	$ 407.711.521,89	$ -	$ 407.711.521,89	28	$ 1.494.603.730,99	$ -	$ 1.494.603.730,99
TOTAL GENERAL	41	$ 1.129.460.613,89	$ -	$ 1.129.460.613,89	343	$ 7.038.812.341,38	$ -	$ 3.117.378.359,34

LIQUIDEZ | RP´S | OB´S | Listo | Accesibilidad: es necesario investigar | 100%

Fuente: Pantalla archivo "REPORTE DE LIQUIDEZ 25 JUL AL 31 JUL 2026 – FUNCIONAMIENTO"

De otra parte, llamó la atención que, por ejemplo, en correo electrónico del 15 de enero de 2026 enviado por el grupo de riesgos a las áreas indicadas en el manual con el informe, con asunto *"RE: Informe de Medición Seguimiento y Control al Riesgo de Liquidez: 09 de enero del 2026"*, se indicara en la cuarta viñeta del contenido la siguiente nota en fuente roja: *"(…) Les recordamos la importancia de informarnos si en el trascurso de la semana se radica un total pagos que superen dichos montos a fin de monitorear los límites de exposición al riesgo de liquidez".* Esto denota que no existen controles o señales de alerta diseñadas o parametrizadas para que ese requerimiento no dependa de la voluntad de las áreas productoras de la información, constituyéndose un riesgo potencial de falta de reporte, lo que tendría incidencia en el monitoreo de la exposición al riesgo de liquidez.

Recomendación: Para evitar ver la actividad expuesta como de "extracción y mensajería", se recomienda que en el correo enviado al grupo de riesgos se incluya una captura de Dynamics 365 de la barra de totales en pantalla (cantidad de registros y suma total) previo a exportar la data en los módulos de RP y Obligaciones. Posteriormente, incluir en el archivo en la pestaña "Liquidez" una construcción a partir de tablas dinámicas o fórmulas con condicionales (sumar.si, contar.si) de los datos requeridos. Esto permitirá al grupo de riesgos o cualquier órgano de control ver la tabla origen de los datos exportados y concluir sobre las revisiones previas aplicadas.

Observación No.2: Hojas de Cálculo de ejecución de la metodología de medición de Máximo Pago Estimado (MPE) con vulnerabilidades de seguridad y validación de información, y falta de revisión de resultados obtenidos.

Criterios:

a) En el manual de gestión de riesgos financieros, el numeral 4.2.2.2. – Plataforma tecnológica para la medición de riesgo de liquidez plantea: *"En razón a que para la medición del riesgo de liquidez de ENTerritorio S.A. se aplicará un modelo interno, cuyas especificaciones responden a las particularidades de la Sociedad, no será necesario aplicar un sistema de información específico; de esta manera los cálculos se realizarán en MS Excel; apoyándose en los casos en que se requiera de otras herramientas de simulación"*. [Énfasis añadido con subrayado]

b) La Circular Externa 018 de 2021 de la Superintendencia Financiera de Colombia – Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR), en el numeral 4 – Infraestructura tecnológica y sistemas de información señala que: "La entidad debe contar con los sistemas, el soporte tecnológico y la arquitectura de datos que permitan una visión comprensiva de los riesgos, el funcionamiento del SIAR, la presentación de informes, la toma de decisiones, así como el cumplimiento de los requerimientos normativos. Esta infraestructura debe contar como mínimo con: (…) b. Procedimientos para el manejo y almacenamiento de la información que permitan garantizar su confidencialidad, seguridad, calidad, disponibilidad, integridad, consistencia y consolidación [Énfasis añadido con subrayado]

c) La Circular Externa 018 de 2021 de la Superintendencia Financiera de Colombia – Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR) en el numeral 2.2. - Etapas del SIAR, señala frente al *"Monitoreo"* que: *"Consiste en realizar un seguimiento permanente y efectivo a las fuentes de riesgo, al perfil de riesgo, a las desviaciones frente a los límites y/o umbrales, a la efectividad de los controles implementados y al posible impacto de la materialización de los riesgos. Adicionalmente, debe facilitar la rápida detección y corrección de las deficiencias en el SIAR. El monitoreo debe ser intensivo en relación con las deficiencias identificadas en la gestión de los riesgos y en los correctivos y acciones de mejora"* [Énfasis añadido con subrayado]

Situación observada: Se pudo identificar concordancia entre la metodología expuesta en el Manual de Gestión de Riesgos Financieros y las hojas de cálculo en Excel donde ésta es implementada. En particular, el grupo de riesgos aportó los archivos, tanto para funcionamiento como para convenios de Máximo Pago Estimado (MPE), así como los cálculos de IRL y saldos de cuentas y recursos propios.

Sin perjuicio de lo anterior, se identifican oportunidades de mejoramiento respecto a los niveles de seguridad de los archivos Excel. Por ejemplo, para el de máximo pago estimado, se tiene:

I. No se cuenta con controles de ingreso de la información (validación de datos): no se detectaron reglas de validación de datos en ninguna de las hojas del archivo. Existe por tanto la posibilidad de que se corrompa el modelo semanal por ingresar erróneamente información (parámetros estadísticos, inclusión de cifras sin origen etc.)

II. Alta dependencia de rutas externas (posibilidad de links rotos): la hoja "Resumen día" ejecuta variados cruces mediante referencias a un archivo externo denominado [...]Consolidado. Cualquier cambio de ubicación de ese archivo base, renombramiento o falta de aplicación de actualizaciones pendientes pueden dar lugar a pérdida de conectividad o reproducción de errores de referencia o no disponibilidad de la data.

III. De otra parte, no se identificó el nivel de aprobación dentro del grupo de riesgos de los resultados del modelo (no se pudo evidenciar un documento firmado por el Gerente del grupo de riesgos o quien haga sus veces que permita determinar que estuvo al tanto de lo que ejecutaron los profesionales del área y los resultados a revelar). Esto permite establecer razonablemente la necesidad de robustecer las actividades de control y monitoreo.

Recomendaciones: hacer un protocolo en el archivo con el paso a paso de alimentación de la data, cerciorándose previamente de incluir validaciones de datos y restricciones de inclusión de información y bloqueos de campos, de tal suerte que no sean sujetos a edición.

Así mismo, se insta a diseñar esquemas de revisión de alto nivel al interior del grupo de riesgos, o actas de reuniones internas de validación de los modelos, que permita verificar la trazabilidad de los análisis y conclusiones a las revisiones realizadas por la Administración de Enterritorio S.A., con lo cual se asegura razonablemente que los resultados a escalar a las diferentes instancias corporativas surtieron las validaciones de rigor.

D) CÁLCULO Y REPORTE DE INDICADORES DE ALERTA TEMPRANA.

Observación No.3: Falta de evidencia del cálculo o comprobaciones de resultado de los Indicadores de Alertas Tempranas de Liquidez.

Criterio: El Anexo 3 del Manual de Gestión de Riesgos Financieros trae los indicadores de alerta temprana de riesgo de liquidez. En total son dos, a saber:

Tabla No.2 Indicadores de Alerta temprana

Id	Indicador	Objetivo
1	Proyección de Gastos de los Activos Líquidos = Gastos Proyectados Mes / Activos Líquidos	Generar alertas tempranas con el fin de establecer la cobertura de activos líquidos sobre los gastos proyectados mensuales para cada componente. (Misional y Funcionamiento).
2	Solidez de las contrapartes donde se tienen colocados recursos de la Entidad = Rentabilidad promedio móvil de las últimas 120 observaciones. Lo anterior equivale al 99% de confianza.	Analizar el comportamiento de las variaciones del precio de la acción de las contrapartes. El indicador alcanza un nivel Crítico cuando la rentabilidad al corte evaluado excede en 2.33 desviaciones.

Fuente: Anexo 3 Manual de Gestión de Riesgos Financieros

Situación observada: Se obtuvo el archivo "Alertas_Tempranas" del indicador 2 anterior. No se detectaron formulaciones que permitan validar el nivel crítico (rentabilidad al corte evaluado exceda 2,33 desviaciones), pues solo se observaron los rendimientos diarios de las acciones (igualmente sin formulaciones para ver lo adecuado de su cálculo). Tampoco se identificó el cálculo de indicador 1.

Recomendación: Al igual que se propuso en la observación previa, se recomienda establecer plantillas o formatos de validación con los criterios que se desea demostrar en la ejecución de las actividades, de tal manera que no solo para el ejecutor del control, sino para cualquier tercero, sea re-ejecutable y trazable las validaciones aplicadas, con su correspondiente nivel de revisión de alto nivel aplicable.

Observación No.4: Indicadores de Alerta Temprana de riesgo de liquidez no escalados a Comité Interno de Riesgos.

Criterio: El numeral 4.2.2.3 del manual de gestión de riesgos financieros sobre *"Reportes y Soportes de la medición del riesgo de liquidez"* menciona: *"con una periodicidad mensual el Grupo de Gestión de Riesgos le presentará al Comité Interno de Riesgos y de manera trimestral al Comité de Riesgos, un informe sobre los resultados de las estimaciones de requerimientos de liquidez, la evolución de los activos líquidos, el comportamiento del Indicador de Riesgo de Liquidez y de los Indicadores de Alerta Temprana"*. [Énfasis añadido con subrayado.]

Situación observada: Frente a la presentación de estos indicadores de alerta temprana ante el Comité de Riesgos e Interno de Riesgos, se inspeccionaron las siguientes actas:

- **CIR 72 del 29-ene y 12-feb**: se menciona que para el segundo semestre de 2025 se presenta incumplimiento del límite fijado para el componente de funcionamiento. No se hizo mención al indicador de solidez de las contrapartes. Se indicó que se encontraba pendiente de calcular el indicador de diciembre 2025 y que el de noviembre estaba excedido.

- **CIR 74 del 25-feb**: se menciona incumplimiento en todas las mediciones para el componente de funcionamiento en la vigencia 2025 (se refieren al indicador 1 según la gráfica observada en el acta, denominada "Revisión Indicador Alertas Tempranas", *"lo que genera la necesidad de evaluar las variables tenidas en cuenta para este indicador con el objetivo de establecer alertas tempranas que reflejen las necesidades de recursos a largo plazo mediante el monitoreo y reporte del indicador de solvencia que calcula y reporta la sociedad al grupo bicentenario para ser incluido en el sistema integral de administración de riesgos SIAR"*. No se mencionó esto último en la información aportada y no se detectó sugerencia en este Comité y los posteriores de la propuesta de indicador. En el mismo sentido, no se hizo referencia al indicador 2 de solidez de las contrapartes.

- **CIR 75 del 26 de marzo, CIR 76 del 28 de abril, CIR 77 del 20 de mayo, CIR 78 del 23 de junio:** no se citaron ni analizaron los indicadores de alertas tempranas del anexo 3.

- El acta del CIR 79 está en gestión de firmas, por lo que esta Asesoría de Control Interno inspeccionó el material complementario anexado de esa sesión, en donde tampoco se hizo mención al indicador de alerta temprana.

- Finalmente, para el caso de las certificaciones del Comité de Riesgos Trimestral, no se observó el detalle de los temas tratados, con el fin de evidenciar la consideración de los indicadores de alertas tempranas de liquidez.

Las conclusiones anteriores se refuerzan con la lectura del informe de Backtesting al 26 de junio de 2026, donde se menciona frente a las alertas tempranas que: *"Con relación al indicador de alertas tempranas vigente, al cierre de este ejercicio el indicador no cuenta con mediciones u observaciones para la vigencia 2026 lo que dificulta la realización de las pruebas de desempeño"* [Énfasis añadido con subrayado].

Respecto al indicador de solidez de contrapartes, concluyeron que: *"el seguimiento efectuado a las contrapartes donde la entidad concentra la mayor cantidad de recursos no generó mayores alertas"*, pero no se da ninguna información numérica que concrete la conclusión (es decir, no es claro a qué se refieren con "mayores alertas"). Este apartado debe ser leído en conjunto con la observación 3, donde el archivo de solidez de contrapartes solo presenta rendimientos de las acciones, pero no se halló ninguna validación de exceso sobre las 2,33 desviaciones estándar.

Recomendación: En virtud de lo anterior, se sugiere que el grupo de riesgos proponga los indicadores funcionales y ajustados a la realidad de Enterritorio S.A. y los someta a consideración de los Comités Internos de Riesgos y Comités de Riesgos, con lo cual estas instancias cumplirán igualmente con las funciones de monitoreo y seguimiento que les confieren sus reglamentos de funcionamiento. Así mismo, deberían considerarse los puntos expuestos como brechas y compromisos derivados de las sesiones de los comités como el pilar de partida para el fortalecimiento de los esquemas de medición, seguimiento y monitoreo a presentar en las reuniones subsiguientes. A su vez, esto servirá de insumo para evaluar la declaración de eventos de riesgo.

E) DESARROLLO DE HERRAMIENTAS DE PRONÓSTICO Y PREVISIÓN DE LIQUIDEZ

En este apartado se buscó validar las políticas sobre estimación de requerimientos de liquidez y medición a la exposición al riesgo de liquidez.

La viñeta 7 del numeral 4.2.4 del manual de gestión de riesgos financieros señala que: *"Compete al Grupo de Gestión de Pagaduría definir e implementar mecanismos de planeación o previsión sobre los requerimientos reales de liquidez".* Frente a esto, respecto de la respectiva indagación efectuada por esta Asesoría de Control Interno, el grupo de riesgos informó que la Sociedad cuenta con los procedimientos P-FI-29 Financiamiento ante contingencia de liquidez y el P-FI-30 Flujo de Caja. Por las limitaciones de tiempo y alcance propuesto de este ejercicio evaluador, no se llevó a cabo una verificación del funcionamiento de estas herramientas, por lo que serán objeto de revisión en la próxima revisión.

De otra parte, sí se detectó que la responsabilidad a cargo de la Subgerencia Financiera no fue acreditada, según la exposición de la siguiente observación:

Observación No.5: **Herramientas no identificadas para proyectar o pronosticar los flujos pasivos a diferentes plazos y mecanismos de planeación y previsión sobre requerimientos reales de liquidez**

Criterio: El manual de gestión de riesgos financieros señala en su numeral 4.2.4 *Políticas sobre estimación de requerimientos de liquidez y medición de la exposición al riesgo de liquidez* en la viñeta 6 que: *"Es necesario que, en la Sociedad, además de las metodologías que proponga y gestione el Grupo de Gestión de Riesgos, se implementen nuevas herramientas o se mejoren las ya existentes a través de las cuales se proyecten o pronostiquen los flujos pasivos a diferentes plazos. Para esto se establece la responsabilidad a la Subgerencia Financiera, de diseñar e implantar estos mecanismos, en coordinación con los grupos que considere pertinente para el éxito de esta actividad"*

Situación observada: En la respuesta entregada por el grupo de presupuesto en el memorando 202617010002503 del 2 de septiembre de 2026 a la indagación *"Indicar qué nueva(s) herramienta(s) implementó y/o mejoró la Subgerencia Financiera a través de las cuales se proyectan o pronostican los flujos pasivos a diferentes plazos. Suministrar evidencia de ella(s), con breve explicación de su funcionamiento"*, se mencionó que: *"(...) para el periodo evaluado no se implementaron nuevas herramientas por parte de la Subgerencia Financiera a través de las cuales se proyectan o pronostican los flujos pasivos a diferentes plazos"*. Esta respuesta no deja claridad sobre la existencia previa de una herramienta implementada para dichos efectos, lo cual contraviene el criterio precitado.

Recomendación: Para efectos de subsanar esta situación, se sugiere verificar con la Subgerencia Financiera si existe tal mecanismo y aportar un detalle de su funcionamiento. Si eventualmente no se cuenta con la herramienta, es necesario diseñarla, considerando la operación de Enterritorio SA a nivel de funcionamiento y de sus convenios. Tal mecanismo debería apalancar las mejoras o robustecimiento de la metodología de riesgo de liquidez de la Sociedad.

F) REVISIÓN DE METODOLOGÍA Y RESULTADOS DE LAS PRUEBAS DE BACKTESTING Y STRESS-TESTING.

- **Pruebas de desempeño (Backtesting)**

Mediante este tipo de pruebas se pretende evaluar la exactitud y capacidad predictiva de los modelos de estimación de riesgo (para este particular, liquidez). Igualmente sirven para verificar el nivel de significancia y de ajuste de los datos estimados y se identifica la mejor distribución de probabilidades.

Enterritorio S.A. ha dispuesto para estos efectos 2 métodos, a saber: el gráfico y la prueba de proporción de fallas de Kupiec.

El numeral 4.2.5.2 del manual de gestión de riesgos financieros *"Procedimiento para la realización de pruebas de desempeño a los Modelos de Estimación de Máximo Pago"* señala que: *"De forma anual, el Profesional del Grupo de Gestión de Riesgos incluirá los resultados de las pruebas de desempeño realizadas mediante el método gráfico y aplicará el Test de Kupiec mediante el cálculo del ratio de probabilidad LR el cual contrasta con la probabilidad de falla teórica en el informe de riesgos y lo presentará al Comité Interno de Riesgos y al Comité de Riesgos"*. En este orden de ideas, fue aportado por parte del grupo de riesgos el informe de backtesting con corte al 26 de junio 2026. Se menciona en el alcance que las pruebas se efectuaron a un nivel de confianza del 95% con información disponible desde el 25 de junio de 2021 y una periodicidad semanal, por lo que se evaluaron 262 observaciones.

Como resultado se observó en el numeral 1.4.1.1. del informe precitado las conclusiones sobre el método gráfico, el cual consiste en representar gráficamente los pagos observados o reales para las fechas objeto de análisis y comparándolos con los pagos estimados del modelo dentro del horizonte de tiempo definido. Como conclusión de este método, determinaron de forma preliminar: a) subestimación del volumen de pagos (desembolsos observados exceden los niveles estimados), lo que podría generar incumplimiento en límites establecidos, y b) sobreestimación del volumen de pagos: en un número pequeño de observaciones los pagos realizados exceden el valor estimado, dando lugar a stocks de liquidez innecesarios.

Para el otro método, se obtuvo análisis del resultado comentado en la siguiente:

<u>Observación No.6:</u> Conclusión errónea del test de Kupiec en informe de Backtesting de funcionamiento y falta de revisión de las conclusiones del informe.

<u>Criterios</u>: a) el numeral 4.2.5.1 *Metodología para la realización de pruebas de desempeño a los modelos de Estimación de Máximo Pago* del manual de gestión de riesgos financieros señala en la segunda viñeta:

*"**La Prueba de Proporción de Fallas de Kupiec (1995), POF:** la cual se basa en la perspectiva de que las excepciones o violaciones pueden ser modeladas a partir de una distribución binomial, bajo el supuesto de que el modelo es preciso. El POF se apoya en un ratio de probabilidad o LR calculado como se muestra a continuación, a partir del número de violaciones observadas y el número de violaciones esperadas con base en un nivel de confianza dado:*

$$LR_{POF} = -2\ln\left(\frac{p^x(1-p)^{n-x}}{\hat{p}^x(1-\hat{p})^{n-x}}\right)$$

Donde:

- ***x** = Número de fallas o excepciones.*
- ***n** = Número de observaciones.*
- ***P~** = Probabilidad empírica, calculada como x/n.*
- ***P** = Probabilidad de falla teórica bajo el nivel de confianza fijado (α).*

De esta manera, bajo este método, se prueba la hipótesis nula de que la probabilidad empírica es similar o se ajusta a la probabilidad de falla teórica (1-α). Si el valor del estadístico excede el valor crítico (p-value) se rechaza o declina la hipótesis nula, de otra manera se acepta".

b) La Circular Externa 018 de 2021 de la Superintendencia Financiera de Colombia – Capítulo XXXI Sistema Integral de Administración de Riesgos (SIAR) en el numeral 2.2. - Etapas del SIAR, señala frente al *"Monitoreo"* que: *"Consiste en realizar un seguimiento permanente y efectivo a las fuentes de riesgo, al perfil de riesgo, a las desviaciones frente a los límites y/o umbrales, a la efectividad de los controles implementados y al posible impacto de la materialización de los riesgos. Adicionalmente, debe facilitar la rápida detección y corrección de las deficiencias en el SIAR. El monitoreo debe ser intensivo en relación con las deficiencias identificadas en la gestión de los riesgos y en los correctivos y acciones de mejora"* [Énfasis añadido con subrayado]

Situación observada: Para el caso del test de Kupiec aplicado al componente misional, se menciona que: *"se obtuvo un estadístico LR del 15,17 superior del valor crítico de 3,84 establecido en el modelo, llevando a concluir que la estimación del Máximo Pago Esperado para el componente Misional no es adecuada bajo este método. (...) al trabajar a un nivel de confianza del 95%, la prueba o test de Kupiec concluye la falta de precisión al modelo, explicado por la sobrestimación del máximo pago esperado como resultado de la disminución en los desembolsos o pagos presentados y el incremento en los registros presupuestales expedidos"*.

Para el test de Kupiec del componente de funcionamiento, se detectó un error en el informe, puesto que se indicó que la hipótesis nula no se rechaza y el modelo es adecuado, cuando al aplicar la fórmula con 0 excepciones se obtiene 26,87 como LR, superior al valor crítico (p-value) de 3,84, por lo que el modelo sería inadecuado, dando lugar al rechazo de la hipótesis nula. Se nota entonces que el modelo inmovilizaría capital que no requiere, siendo esto ineficiente:

Imagen No.2 Resultados Test de Kupiec para funcionamiento

Resultados Test de Proporción de Fallas – Kupiec –

	95%
Total Excepciones o Fallas (x)	0
Total de Observaciones (n)	262
Porcentaje de Fallas p^= (x / n)	0.00%
Eficacia del Modelo 1- (x / n)	100.00%
Nivel de Confianza (1-p)	95%
Probabilidad de Falla del Modelo (p teórico)	5%
Excepciones o Fallas Esperadas	13.1
Consistencia del modelo según el Método Gráfico	Consistente
Prueba de Proporción de Fallas de Kupiec	
$p^x(1-p)^{n-x}$	1.45742E-06
$p\hat{}^x(1-p\hat{})^{n-x}$	#¡NUM!
Prueba de Razón de Verosimilitud LR_{POF}	#¡NUM!
P-Value Chi cuadrado (1 grado libertad)	3.84
Interpretación	No se Rechaza Ho.El modelo es adecuado

Fuente: Informe "Pruebas de Backtesting al Modelo Interno Medición del Riesgo de Liquidez", página 13

Fórmula aplicada para 0 excepciones y demás datos de la tabla anterior:

$$Ln\left[\frac{\left((0{,}05^{0})\right)\times\left(0{,}95^{(262-0)}\right)}{0^{0}\times((1-0)^{262})}\right]\times(-2)=26{,}877$$

Puesto que 26,877 > 3,84, la hipótesis nula debe rechazarse.

En este orden de ideas, se puede concluir razonablemente que el informe de Backtesting no fue revisado al interior del grupo de riesgos antes de su escalamiento al Comité Interno de Riesgos. Incluso el informe no tiene evidencias de firmas de alguna instancia en señal de revisión o aprobación. En las actas del CIR inspeccionadas no hubo pronunciamiento de este órgano sobre los resultados del Backtesting, considerando los resultados expuestos a nivel de proyectos, donde se indicó que el modelo no es adecuado y carece de precisión. Se acaba de demostrar que lo mismo aplica para el componente de funcionamiento.

Recomendación: En virtud de los detalles expuestos, se recomienda que el grupo de riesgos verifique el modelo de backtesting y lo recalibre, con el fin de que pueda ser puesto a consideración de los Comités pertinentes (Interno de Riesgos y de Riesgos), previa adopción de los esquemas de revisión y documentación que se vienen comentando en observaciones anteriores aplicados por el Gerente del área o quien haga sus veces. Para evitar el riesgo de comunicación de conclusiones erróneas que induzcan a error en las reuniones de alto nivel, es necesario que, con antelación al envío del material, los jefes de las áreas revisen las conclusiones, cálculos y modelos ejecutados antes de su escalamiento. Esto permitirá que se puedan tomar decisiones razonables sobre el riesgo de liquidez de Enterritorio S.A, considerando igualmente la siguiente observación 7.

Observación No.7: Debilidades analíticas del modelo para calcular el Máximo Pago Esperado (MPE)

Criterio: el manual de gestión de riesgos financieros señala en el numeral 4.2.2.1 *Fuentes de información para la medición del riesgo de liquidez* que: *"Para efecto de la estimación de la estructura probabilística de los pagos e identificar el máximo pago esperado, aplicable para cada uno de los componentes, misional y funcionamiento, se utilizarán las bases de datos presupuestales. Para esto, con una periodicidad semanal los Grupos de Contabilidad y Presupuesto generarán, consultas que contengan las series históricas diarias de datos de*:

** Registros presupuestales expedidos (RPc).*
** Pagos registrados (Pc).* [Énfasis añadido con subrayado.]

Situación observada: desde un punto de vista analítico, la metodología empleada para el cálculo del Máximo Pago Esperado presenta las siguientes debilidades:

I. El modelo usa el saldo de los registros presupuestales (ERC) como variable base para calcular el Máximo Pago Esperado (MPE). Recuérdese que el RP funciona como mecanismo que garantiza la disponibilidad de recursos para un contrato, pero no representa el momento exacto en que el dinero saldrá del banco. Así las cosas, si el modelo acude al RP como insumo directo para calcular la caja que se necesitará en los próximos siete días, distorsiona la realidad financiera de la Sociedad.

II. El modelo actual toma el saldo total del RP (la exigibilidad sobre los recursos comprometidos) y calcula un percentil estadístico para computar el máximo pago esperado (MPE) de la siguiente semana. Al hacerlo, el modelo asume automáticamente que una porción de la totalidad del contrato podría cobrarse

en los próximos siete días, lo cual dispara un requerimiento de liquidez artificial y gigante de un momento a otro, solo porque se ingresó un nuevo contrato al sistema.

III. Como consecuencia de lo anterior, (Un MPE alto y sin congruencia con la realidad), el Back Office se ve obligado a mantener grandes cantidades de dinero "ocioso" en cuentas a la vista o inversiones de corto plazo para cubrir ese indicador de riesgo, lo que da lugar a "castigar" la Sociedad porque el exceso de liquidez inmovilizada deja de generar mayores rendimientos financieros que se obtendrían si el dinero se invirtiera en posiciones a largo plazo, alineados con el cronograma real de los proyectos.

IV. Se advierte un sesgo normativo hacia la sobreestimación pues, al definir el método gráfico (numeral 4.2.5.1 del manual) se estipula que una excepción ocurre exclusivamente "cuando a nivel gráfico se evidencie que el pago observado superó al estimado". De allí el por qué se asume en el informe de backtesting que el modelo es adecuado, pues hay una asimetría en el manual que penaliza la subestimación de liquidez (quedarse sin caja) pero ignora por completo la sobreestimación masiva (caja inmovilizada innecesariamente). Como el modelo toma los voluminosos RP y exige guardar un enorme colchón, el pago observado nunca supera al estimado, dando lugar al registro de cero excepciones.

V. El método de Simulación Histórica (LaR) asume que el futuro se comportará como el pasado. En un modelo misional como el de Enterritorio S.A. basado en estructuración de convenios, los desembolsos son eventos discretos, atípicos y sujetos a hitos de proyectos, por tanto, no son variables continuas con una distribución normal o histórica estable.

Recomendación: Por lo expuesto, se sugiere prescindir de la simulación histórica sobre saldos de RP y transitar hacia un modelo determinístico basado en los cronogramas reales de desembolsos y cuentas por pagar de los proyectos, esto es, el flujo de caja. Procediendo así se abandona la metodología actual que es un modelo estadístico sobre presupuesto. A raíz de esto, se aconseja promover una modificación al manual para incluir variables transaccionales de caja (curvas de ejecución, curvas S, programación de giros etc) y no solo bases de datos presupuestales. Un modelo que pudiera adoptarse podría corresponden al de Flujos de Caja en Riesgo – CfaR.

- **Pruebas de Esfuerzo (Stress Testing)**

Este tipo de pruebas tiene el propósito de evaluar la capacidad de Enterritorio S.A. para cubrir sus compromisos de pago, con sus activos líquidos; y de evaluar el impacto que tienen condiciones adversas y/o extremas en el Indicador de Riesgo de liquidez de la Sociedad.

Derivado de las conclusiones analíticas precitadas en la observación anterior, se puede extender su alcance a las pruebas de estrés, según la siguiente descripción:

Observación No.8: Debilidades analíticas del modelo de Stress Test

Criterio: en el manual de gestión de riesgos financieros, en el numeral 4.2.6.1 *"Metodología para la realización de pruebas de esfuerzo a los modelos de riesgo de liquidez"*, se indica: *"(…) en los escenarios de estrés es recomendable incorporar el supuesto restrictivo de no acceso a fuentes adicionales de liquidez diferentes de las que están en el balance en el momento de la estimación, lo cual equivale a suponer que no se cuenta con nuevos aportes o convenios, o ingresos a la Sociedad que puedan aumentar el disponible, o los portafolios, como tampoco con nuevos activos en los portafolios que puedan ser liquidados".*

Situación Observada: el grupo de riesgos suministró el archivo ""Resultados pruebas stress RL", en donde se asumieron pagos sucesivos sostenidos (en la página 7 del informe se manifiesta: *"Finalmente se consideró la realización de un pago extraordinario, no contemplado dentro de la serie histórica de datos (Escenario 4), donde se asumió un pago semanal de $150.000 millones relacionado con obligaciones contractuales de convenios inesperadas; en este caso la liquidez disponible cubriría pagos semanales por un total de 3 semanas"*). Esto se esquematiza en la tabla 5, extraída del numeral 4.2.1 del componente misional del informe, donde, en el escenario 4, se asumen pagos de 150.000 millones semanales y concluye que el portafolio de 414.958 millones alcanzaría para 3 semanas:

Imagen No.3. Resultados de escenarios del componente misional en prueba de stress

Escenarios Componente Misional

	Escenarios	Máximo Pago Observado / Esperado	Activos Líquidos Ajustados	Medida	IRL	Stock de Liquidez en Semanas
	Escenario Inicial / Base	**3,940,535,101**	**414,958,692,212**	**($MP_{Observado}$ /ALM)**	**0.95%**	**105**
1	MPE a un nivel de confianza del 95%.	122,960,306,724	414,958,692,212	(MPE 95% /ALM)	29.63%	3
2	Máximo Pago Histórico Observado en el último año (21-Nov-25)	11,942,799,597	414,958,692,212	($MP_{Observado}$ /ALM)	2.88%	35
3	MPE a un nivel de confianza del 99%.	188,099,545,822	414,958,692,212	(MPE 99% /ALM)	45.33%	2
4	Pago Extraordinario por $150.000 Millones para cumplir con obligaciones contractuales	151,473,671,341	414,958,692,212	(MPE 95% /ALM)	36.50%	3

Fuente: Informe "Pruebas de Stress Testing Modelo Interno de Riesgo de Liquidez", página 6

Lo mencionado se refuerza con el párrafo subsiguiente de la página 7, donde se expresa que: *"Es importante mencionar que en todos los casos se evaluaron pagos sucesivos por el mismo valor, lo cual además de extremo tiene una baja probabilidad de ocurrencia"*.

Es operativamente contradictorio simular una ejecución acelerada de proyectos (salidas extremas de caja) bajo el supuesto que el financiador no está girando los recursos de dichos convenios.

Por otra parte, el indicador IRL que arrojó en el escenario objeto de análisis un valor de 36,50% equivale en semanas a aproximadamente 3 (obtenidas como 1 / IRL, es decir, 1/0,365 = 2,73 ≈ 3). Esta formulación matemática asume que el Máximo Pago Esperado (el flujo estresado) es una constante repetitiva que consumirá el 36,5% de los activos líquidos cada siete días, hasta llegar a 0.

A la final, lo que se está concluyendo es que, matemáticamente, el modelo aplicado distorsiona la naturaleza de la variable estresada. Para ser específicos, un pago extraordinario en la gerencia de proyectos (ej: un anticipo considerable, la pérdida de un proceso legal etc.) es, por definición, un evento discreto de única ocurrencia. Al tener activos líquidos ajustados por 414.958 millones en caja y padecer eventualmente un choque de 150.000 millones, la evaluación correcta debería ser que la operación deja un margen de 264.958 millones para continuar la operación normal de los proyectos. A esto se suma el hecho de que tener la fórmula del stock de semanas como la inversa del IRL (1/IRL) supone que la Sociedad estuviera obligada a pagar una obligación extraordinaria de 150.000 millones todos los viernes hasta quedar sin saldo (lo cual es más propio de entidades financieras que de entidades dedicadas a la administración de proyectos y fiducias).

Para finiquitar la observación, la simulación Montecarlo de 10.000 iteraciones citada en el informe, al ejecutarse sobre una variable inflada como los saldos de RP's según se expuso en la observación

anterior, que no miden la verdadera maduración de cartera u obligaciones exigibles semanales, da como resultado la carencia de valor predictivo. De esta manera, Risk Simulator entrega resultados precisos, pero erróneos.

Recomendación: Como producto del análisis descrito, se sugiere que el grupo de riesgos eleve al Comité Interno de Riesgos las siguientes temáticas:

- Sustituir el stress test estadístico por análisis de escenarios determinísticos, dado que el riesgo de liquidez de Enterritorio S.A. no debería medirse mediante percentiles estadísticos de presupuesto, sino sobre hitos críticos de los convenios y proyectos. Ej: simular el impacto en la caja de un convenio si su aportante retrasa el otorgamiento de recursos en 60 días, mientras Enterritorio S.A. debe continuar con el pago de contratistas y nóminas.

- Rediseñar el límite de alertas: como consecuencia de lo anterior, el límite de 8,66% propuesto en el informe de stress test debería ser descartado y, en su lugar, atarlo al índice de cobertura de liquidez de funcionamiento, midiendo cuantos meses de gastos fijos puede soportar la Sociedad sin nuevos negocios o convenios, y no acudiendo al cálculo global que implica el ratio MPE/AL.

- Ajustar el manual de gestión de riesgos financieros en el numeral 4.2.6.1, dado que el modelo expuesto puede ser compatible con establecimientos de crédito, más no con la misionalidad de Enterritorio S.A. Así las cosas, debería considerarse el modelo CFaR (Cash Flow at Risk).

1.2. GESTIÓN DE RIESGO DE MERCADO

Para la evaluación de este sistema de administración de riesgos (en adelante, referido como SARM), el alcance de las pruebas se enfocó en los siguientes aspectos:

a) Gobierno del riesgo de mercado – reuniones de comités y análisis de informes.
b) Mapeo y documentación de condiciones faciales de nuevas inversiones.
c) Límite de inversiones admisibles
d) Oportunidad y calidad en la transmisión del Valor en Riesgo (VaR) regulatorio.
e) Cálculo del VaR interno
f) Validación de pruebas de funcionalidad de aplicativo de administración de inversiones y su reporte.
g) Arqueos de Custodios (DECEVAL – DCV)
h) Validación del Monitoreo a la Valoración de Portafolios de Inversión
i) Validación del Monitoreo a la preparación del formato 351.

Los resultados obtenidos se exponen a continuación:

a) GOBIERNO DEL RIESGO DE MERCADO – REUNIONES DE COMITÉS Y ANÁLISIS DE INFORMES.

Al igual que con el riesgo de liquidez, en este apartado se buscó verificar que los informes que deben presentarse ante el Comité Interno de Riesgos y Comité de Riesgos en materia de riesgo de mercado hayan sido puestos a su consideración, de acuerdo con las directrices del manual de gestión de riesgos financieros.

Uno de los requisitos se cita en el numeral 5.2.4.2 Plataforma Tecnológica para la Medición del Riesgo de Mercado, como sigue: *"(…) La responsabilidad en la administración de estos sistemas de información es del Grupo de Gestión de Riesgos, quien efectuará la parametrización y configuración de los mismos, acorde con los lineamientos y metodologías aprobadas por el Comité Interno de Riesgos, el Comité de Riesgos y la Junta Directiva. Así mismo, en razón a la importancia de asegurar la precisión de los cálculos y la aplicación de los parámetros definidos en los modelos es necesario que realice la validación de la funcionalidad de los aplicativos por lo menos con una periodicidad anual. Los resultados de estas validaciones; así como las propuestas de ajustes a parámetros deben ser presentados al Comité Interno de Riesgos".*

Frente a esto, En el Acta No. 70 del Comité Interno de Riesgos realizada el 27 de noviembre de 2025, en el literal f) *"Informe de Validación - Cálculo exposición riesgo de mercado (método interno). Corte 31 de octubre del 2025"* el Grupo de Gestión de Riesgos presentó el informe de validación precitado cuyo objetivo es realizar validaciones a los procedimientos y cálculos de valoración de inversiones y exposición al riesgo de mercado efectuado por el aplicativo MarkRisk, con el fin de comprobar la veracidad y confiabilidad de éstos.

Desde la perspectiva de gestión de riesgos, si bien el grupo de riesgos cumple con lo solicitado en el manual (validación por lo menos anual), la frecuencia anual es un horizonte demasiado amplio dadas las volatilidades del mercado. Así las cosas, se presenta oportunidad de mejoramiento, en el sentido de que se sugiere migrar de una validación "temporal" (en este caso, anual), a una validación por eventos. En otras palabras, mantener la que se está ejecutando, pero complementar con validaciones extraordinarias cuando haya alta volatilidad del mercado, actualizaciones del software o cambios en la metodología de cálculo.

Sin perjuicio de lo anterior, y según el contenido del acta expuesta, se presenta la siguiente observación (continúa la numeración consecutiva desde la sección anterior, para efectos de facilidad en la identificación en el contenido del informe y evitar duplicidades ante una eventual búsqueda):

Observación No.9: Falta de umbrales de tolerancia cuantitativos y su tratamiento

Criterio: Circular Externa 018 de 2021 – Capítulo XXXI de la Circular Básica Contable y Financiera 100 de 1995 de la Superintendencia Financiera de Colombia, numeral 2.2. Etapas del SIAR, que manifiesta: *"La entidad debe atender las siguientes etapas del SIAR, las cuales deben estar en línea con el MAR. (…) Control: Consiste en establecer los mecanismos tendientes a mitigar y/o minimizar la posibilidad de ocurrencia e impacto de la materialización de los riesgos inherentes a las actividades que desarrolla la entidad. Los controles deben permitirle a la entidad conocer el grado de cumplimiento de sus políticas, estrategias, procedimientos, metodologías, controles, umbrales y/o límites y marco regulatorio, así como contar con información actualizada, confiable, oportuna y completa.* [Énfasis añadido con subrayado].

Situación observada: En el Acta No. 70 del Comité Interno de Riesgos realizada el 27 de noviembre de 2025 (en donde se validó el cálculo anual de la exposición al riesgo de mercado por el método interno) se observó que se justificaron las diferencias encontradas en valoración ($30.332.090, es decir, un 0.00946%) en los procesos de interpolación que efectúa el sistema para estimar la tasa de descuento. Para las diferencias en el VaR (posición propia de $242.226 - 1.1% y proyectos $153.117 - 0.6%), se indica que es por decimales de los títulos y simulación de escenarios aleatorios. Lo que esta Asesoría de Control Interno identifica es que no se cuenta con un umbral de tolerancia cuantitativo (ej: desviaciones > 1% o X millones de pesos), máxime considerando que estas exposiciones ocurren diariamente y que cualquier error o desviación se puede acumular de manera considerable.

Recomendación: Dado lo anterior, se recomienda un protocolo de escalamiento en casos de que dichos umbrales sean superados con la acción a ejecutar, por ejemplo: suspensión de operatividad, reporte al Comité de Riesgos, Ticket con el proveedor Tecnológico, entre otras opciones que se consideren pertinentes. Calcular la diferencia absoluta y relativa de una o varias diferencias sin reglas de decisión claras (comparación frente a umbrales de tolerancia individuales y acumulados) debilitan el control porque lo supeditan al análisis del Valorador.

**

Otro de los numerales del manual de gestión de riesgos financieros sujetos a validación es el 5.2.5.1 *"Políticas y Lineamientos sobre Pruebas de Desempeño del Modelo Interno de Riesgo de Mercado"* que señala: *"La periodicidad en la ejecución de las pruebas limpias es de manera diaria y los resultados de estas pruebas deben ser consolidados y presentados al Comité Interno de Riesgos mensualmente, y al Comité de Riesgos trimestralmente, para efectos de evaluar y determinar la necesidad de ajustes a los modelos de riesgo.* [Énfasis añadido con subrayado].

Se inspeccionaron las actas del CIR desde la 72 hasta la 78, notando que la temática fue sometida a su consideración. Las pruebas diarias (limpias) se presentaron en el CIR 72 del 29 de enero 2026 y 12 de febrero 2026 con corte a diciembre de 2025, mientras que la aplicación de pruebas sucias fue presentada en el CIR 76 del 28 de abril de 2026 con la aplicación del VaR anual.

No se identificó acta trimestral del Comité de Riesgos donde se presentaron estos resultados (La certificación 079 del secretario técnico de Junta Directiva del 26-feb-2026 informa la presentación de puntos informativos de gestión de riesgos al corte de julio, agosto y septiembre 2025 sin dar detalle de dichos puntos).

Para el caso de lo solicitado en el numeral 5.3.1 – *Seguimiento al Valor en Riesgo de Mercado* que manifiesta que: *"Con el objetivo de realizar un adecuado seguimiento a los valores en riesgo que registran los portafolios de inversiones que posee la Sociedad, el profesional del Grupo de Gestión de Riesgos debe (...). Así mismo, debe remitir un informe periódico al Comité Interno de Riesgos, al Comité de Riesgos y a la Junta Directiva que presenten de manera clara y comprensible:*

** Las exposiciones por instrumento financiero, portafolio y tipo de riesgo*
** Los límites vigentes, su cumplimiento y nivel de utilización*
** El efecto de las exposiciones sobre el patrimonio, portafolio y utilidades"* [Énfasis añadido con subrayado]

Se observó en el acta 76 del CIR (28 de abril de 2026) en el literal g) Pruebas de desempeño (backtesting). Modelo Interno de Riesgos de Mercado que se presentaron los resultados de la aplicación de la metodología al portafolio total, a cada portafolio (Enterritorio S.A. y Proyectos), por clase de activo y por especie. También se presentó los límites por tipo de activo, límite por operador y límite por duración total. No se identificó el efecto de las exposiciones sobre el patrimonio, portafolio y utilidades.

b) MAPEO Y DOCUMENTACIÓN DE CONDICIONES FACIALES DE NUEVAS INVERSIONES

Mediante memorando de solicitud de información 202617010002503 del 2 de septiembre de 2026, esta Asesoría de Control Interno solicitó: *"Indicar si en el periodo evaluado (enero – julio de 2026) se tuvieron nuevas inversiones. En caso afirmativo, suministrar el Anexo 4 pertinente de todas ellas"*, frente a lo cual

el grupo de riesgos contestó que: *"Durante el periodo de enero a julio de 2026 no se tuvieron nuevas inversiones".*

c) LÍMITE DE INVERSIONES ADMISIBLES

Observación No.10: **Sobrepaso de límite de inversiones admisibles en portafolios de Enterritorio S.A. y Proyectos**

Criterio: Manual de gestión de riesgos financieros, numeral 5.3.3 Límites por tipo de activo, señala que: *"De acuerdo con el numeral 11. Marco de Negociación establecido en el Manual de Operaciones de Tesorería de ENTerritorio S.A. se podrán invertir en los activos que se señalan allí. Teniendo en cuenta la posibilidad de invertir en estos activos, se definen los siguientes límites como una proporción del valor nominal del portafolio para cada día, es decir, se ajustan al valor del portafolio al corte de evaluación de los límites:*

• Operaciones de reporto activas. = (5%)
• Títulos derivados de procesos de titularización emitidos en desarrollo de procesos de titularización autorizados por la Superintendencia Financiera. = (5%)
• Operaciones con contratos forward, contratos de futuros, opciones y swaps únicamente con el fin de protegerse frente a las fluctuaciones de tasas de interés o cambio de moneda. = (5%)
• Transacciones con títulos valores en pesos o en cualquier otra denominación, excepto las emisiones propias, en caso de que ENTerritorio S.A. decida emitir títulos valores = (5%)
• Títulos de renta fija emitidos, avalados, aceptados o garantizados por instituciones vigiladas por la Superintendencia Financiera = (10%)
Títulos emitidos, avalados o garantizados por el Fondo de Garantías de Instituciones Financieras (FOGAFIN). = (10%)
• Títulos de renta fija emitidos por entidades no vigiladas por la Superintendencia Financiera. Estos títulos deberán contar con calificaciones de riesgos = (10%)
• Títulos de deuda pública interna y externa, emitidos o garantizados por la Nación = (20%)
• Títulos emitidos por el Banco de la República = (20%)
• Bonos y títulos hipotecarios y otros títulos de contenido crediticio derivados de procesos de titularización de cartera hipotecaria avalados por el Gobierno Nacional = (20%)
• Depósitos a la vista en establecimientos de crédito = (20%)
• ENTerritorio S.A. invertirá en inversiones de carácter forzoso que determine el Gobierno Nacional = (30%)

Situación observada: esta Asesoría de Control Interno tomó el formato 351 del 5 de junio de 2026, con el cual construyó una tabla dinámica discriminada por: portafolio, emisor, especie y total nominal. Dado que los títulos de todos los portafolios (posición propia y proyectos) son CDT's emitidos por entidades vigiladas por la Superintendencia Financiera de Colombia, opera el siguiente límite: "Títulos de renta fija emitidos, avalados, aceptados o garantizados por instituciones vigiladas por la Superintendencia Financiera = (10%)". Se pudo apreciar que el 100% de la concentración de los títulos sobrepasan el 10% de límite:

Tabla No.3 Concentración de emisores y títulos a valor nominal portafolio al 5 de junio de 2026

Suma de VALOR NOMINAL			
PORTAFOLIO	**EMISOR**	**ESPECIE**	**Total**
C194048-	**BANCO DE OCCIDENTE**	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	1.500.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	3.500.000.000
Total C194048-			**5.000.000.000**
C194126-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	1.400.000.000
Total C194126-			**1.400.000.000**
C211041-	**BANCO DE OCCIDENTE**	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	1.000.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	5.000.000.000
	TUYA S.A.	CDT TASA FIJA TUYA S.A. BASE 360	1.000.000.000
Total C211041-			**7.000.000.000**
C211045-	**BANCO DE BOGOTA**	CDT TASA FIJA BANCO DE BOGOTA BASE 365	4.600.000.000
	BANCO DE OCCIDENTE	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	6.500.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	5.500.000.000
Total C211045-			**16.600.000.000**
C212015-	**TUYA S.A.**	CDT TASA FIJA TUYA S.A. BASE 360	500.000.000
Total C212015-			**500.000.000**
C212017-	**BANCO GNB SUDAMERIS S.A.**	CDT TASA FIJA BANCO SUDAMERIS BASE 360	3.000.000.000
Total C212017-			**3.000.000.000**
C212045-	**BANCO DE OCCIDENTE**	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	1.000.000.000
Total C212045-			**1.000.000.000**
C212046-	**BANCO GNB SUDAMERIS S.A.**	CDT TASA FIJA BANCO SUDAMERIS BASE 360	2.000.000.000
Total C212046-			**2.000.000.000**
C212071-	**BANCO DE OCCIDENTE**	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	1.000.000.000
Total C212071-			**1.000.000.000**
C212080-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	400.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 360	3.500.000.000
		CDT TASA VARIABLE BANCO DE BOGOTA IPC BASE 360	6.000.000.000
	BANCO ITAU CORPBANCA COLOMBIA S.A.	CDT TASA FIJA BANCO ITAU CORPBANCA BASE 360	500.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	7.300.000.000
	BANCOLOMBIA S.A.	CDT TASA FIJA BANCOLOMBIA BASE 360	3.000.000.000
	BBVA S.A.	CDT TASA FIJA BANCO BBVA BASE 360	1.000.000.000
Total C212080-			**21.700.000.000**
C212081-	**BANCO DE OCCIDENTE**	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	9.400.000.000
Total C212081-			**9.400.000.000**

Suma de VALOR NOMINAL			
PORTAFOLIO	**EMISOR**	**ESPECIE**	**Total**
C213004-	**BANCO DE BOGOTA**	CDT TASA FIJA BANCO DE BOGOTA BASE 365	1.000.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	1.000.000.000
Total C213004-			**2.000.000.000**
C216144-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	500.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 365	500.000.000
Total C216144-			**1.000.000.000**
C216220-	**TUYA S.A.**	CDT TASA FIJA TUYA S.A. BASE 360	500.000.000
Total C216220-			**500.000.000**
C217045-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	1.300.000.000
Total C217045-			**1.300.000.000**
C221004-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	1.500.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 365	3.600.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	2.000.000.000
	TUYA S.A.	CDT TASA FIJA TUYA S.A. BASE 360	1.000.000.000
Total C221004-			**8.100.000.000**
C221017-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	2.500.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 365	4.500.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	1.500.000.000
	MIBANCO S.A.	CDT TASA FIJA MIBANCO BASE 360	2.000.000.000
Total C221017-			**10.500.000.000**
C223004-	**BANCO DE BOGOTA**	CDT TASA FIJA BANCO DE BOGOTA BASE 365	7.500.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	7.000.000.000
	BANCOLOMBIA S.A.	CDT TASA FIJA BANCOLOMBIA BASE 360	1.000.000.000
Total C223004-			**15.500.000.000**
C223006-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	500.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 365	3.500.000.000
	MIBANCO S.A.	CDT TASA FIJA MIBANCO BASE 360	800.000.000
Total C223006-			**4.800.000.000**
C223007-	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	7.800.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 360	12.500.000.000
		CDT TASA VARIABLE BANCO DE BOGOTA IPC BASE 360	7.500.000.000
	BANCO DE OCCIDENTE	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	1.600.000.000
		CDT TASA VARIABLE BANCO DE OCCIDENTE IPC BASE 360	5.000.000.000

Suma de VALOR NOMINAL			
PORTAFOLIO	**EMISOR**	**ESPECIE**	**Total**
	BANCO ITAU CORPBANCA COLOMBIA S.A.	CDT TASA FIJA BANCO ITAU CORPBANCA BASE 360	500.000.000
	BANCOLOMBIA S.A.	CDT TASA FIJA BANCOLOMBIA BASE 360	1.000.000.000
Total C223007-			**35.900.000.000**
C224010-	**BANCO DE BOGOTA**	CDT TASA FIJA BANCO DE BOGOTA BASE 365	7.300.000.000
	BANCO DE OCCIDENTE	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	4.000.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	1.000.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	5.500.000.000
Total C224010-			**17.800.000.000**
C224014-	**BANCO DE BOGOTA**	CDT TASA FIJA BANCO DE BOGOTA BASE 365	11.000.000.000
	BANCO DE OCCIDENTE	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	7.500.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA FIJA BANCO SUDAMERIS BASE 360	1.500.000.000
	BANCO ITAU CORPBANCA COLOMBIA S.A.	CDT TASA FIJA BANCO ITAU CORPBANCA BASE 360	2.300.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	7.000.000.000
	MIBANCO S.A.	CDT TASA FIJA MIBANCO BASE 360	2.000.000.000
	TUYA S.A.	CDT TASA FIJA TUYA S.A. BASE 360	2.000.000.000
Total C224014-			**33.300.000.000**
ENTERRITO	**AV VILLAS**	CDT TASA FIJA BANCO AV VILLAS BASE 360	2.000.000.000
	BANCO DE BOGOTA	CDT TASA FIJA BANCO DE BOGOTA BASE 360	1.500.000.000
	BANCO DE OCCIDENTE	CDT TASA FIJA BANCO DE OCCIDENTE BASE 360	5.200.000.000
	BANCO FINANDINA	CDT TASA VARIABLE BANCO FINANDINA IBR BASE 360	5.000.000.000
	BANCO GNB SUDAMERIS S.A.	CDT TASA VARIABLE BANCO GNB SUDAMERIS IBR BASE 360	5.500.000.000
	BANCO POPULAR S.A.	CDT TASA FIJA BANCO POPULAR BASE 360	10.000.000.000
	BANCOLOMBIA S.A.	CDT TASA FIJA BANCOLOMBIA BASE 360	3.000.000.000
	BBVA S.A.	CDT TASA FIJA BANCO BBVA BASE 360	1.000.000.000
	DAVIVIENDA	CDT TASA FIJA BANCO DAVIVIENDA BASE 360	1.500.000.000
		CDT TASA VARIABLE BANCO DAVIVIENDA IPC BASE 365	2.000.000.000
	FINDETER	CDT TASA FIJA FINDETER BASE 360	2.000.000.000
	GMAC FINANCIERA DE COLOMBIA	CDT TASA FIJA GMAC FINANCIERA DE COLOMBIA BASE 365	3.100.000.000
	RCI COLOMBIA S.A.	CDT TASA FIJA RCI COLOMBIA S.A. BASE 360	5.000.000.000
	TUYA S.A.	CDT TASA FIJA TUYA S.A. BASE 360	5.200.000.000
Total ENTERRITO			**52.000.000.000**
Total general			**251.300.000.000**

Fuente: Elaboración propia a partir del formato 351 del 5 de junio de 2026

Recomendación: A raíz de lo expuesto en la tabla que antecede, se sugiere parametrizar alertas en los aplicativos de administración de inversiones que permitan anticipar cualquier sobrepaso a los límites establecidos en la conformación de los portafolios de posición propia o de proyectos. De ser pertinente, y según las inversiones que le son permitidas hacer a Enterritorio S.A., se insta a analizar la pertinencia de ajustar los límites del manual, considerando que los niveles de concentración en un mismo tipo de especie (para el particular, CDT's) pueden llegar a ser sobrepasados por estrategias de inversión que requieren ser previamente validadas por el grupo de tesorería.

d) OPORTUNIDAD Y CALIDAD EN LA TRANSMISIÓN DEL VALOR EN RIESGO (VAR) REGULATORIO.

Observación No.11: Desvíos en remisión de información de riesgos de mercado – Valor en riesgo por módulos.

Criterios:

- De acuerdo con el documento de la Superintendencia Financiera de Colombia "Anexo I - Remisión de Información Parte I - Proformas F.0000" en lo concerniente al tema de Riesgos de Mercado, Proforma "Valor en riesgo por módulos", proforma F.0000-129 Formato 386, la periodicidad de transmisión de este formato es, para el caso de Enterritorio como IOE (Institución Oficial Especial), Diaria. La fecha de corte de la información es el mismo día y la fecha de reporte es antes de las 9:00 a.m. del día hábil siguiente. El tipo y número de reporte es el 55 - Valor en Riesgo.

- Procedimiento P-RI-05 Medición y Transmisión diaria de riesgo de mercado por el método estándar, numeral 5 "Condiciones Generales", que señala: *"El Grupo de Gestión de Riesgos transmite en los medios establecidos los archivos firmados entre 8:20 am y 9:00 a.m." y "El Grupo de Gestión de Riesgos debe mantener un control sobre el cumplimiento de las trasmisiones de medición de riesgo de mercado, en el cual se registra los tiempos en que se cumplieron las actividades de cierre del portafolio de inversiones, generación de informe, firma y trasmisión de archivos. De manera periódica estos resultados se presentan al Comité Interno de Riesgos y al Comité de Auditoría y Riesgos a fin de que se determinen las posibles acciones cuando reiteradamente las actividades se ejecuten por fuera de los horarios de referencia".*

Situación observada: Esta Asesoría de Control Interno solicitó al grupo de riesgos *"(…) el CIDT de transmisión del VaR estándar (Formato 386) a la Superintendencia Financiera de Colombia (SFC), adjuntando los formatos correspondientes y soporte en Excel de los cálculos que se están reportando (junto con las fuentes de información aplicables", para la siguiente muestra de días y semanas:*

Tabla No.4. Muestra de días solicitada para validación de transmisión VaR regulatorio

Mes	Días
Enero	13, 16, 22
Febrero	11, 17, 20
Marzo	6, 9, 25
Abril	3, 6, 27
Mayo	8, 12, 14
Junio	10, 19, 29
Julio	15, 28, 31

Fuente: elaboración propia Asesoría de Control Interno

El grupo de gestión de riesgos contestó al requerimiento mediante el memorando 202617010002503 del 2 de septiembre de 2026, en donde se validó en una tabla los 21 elementos de la muestra precitada, donde se identificaron 3 desviaciones que se catalogan como no recurrentes, y que se muestran enseguida:

Tabla No.5 Desviaciones en horario de transmisión VaR Regulatorio

Mes	Fecha corte	Fecha límite hábil	Fecha observada envío	Hora observada de envío	CIDT
Febrero	20-feb-2026	23-feb-2026	23-feb-2026	12:43 p.m.	2026037952-00
Marzo	9-mar-2026	10-mar-2026	10-mar-2026	9:10 a.m.	2026048639-00
Julio	31-jul-2026	3-ago-2026	3-ago-2026	9:57 a.m.	2026154072-00

Fuente: Elaboración propia Asesoría de Control Interno

Se identifica entonces que, de los 21 días seleccionados aleatoriamente para validar la oportunidad en la transmisión, 3 se hicieron en horarios que superan las 9:00 am (14%), lo cual genera brecha por lo indicado en los criterios mencionados previamente.

Recomendación: Por tratarse de desviaciones no sistemáticas, se atribuye la ocurrencia a hechos aislados, por lo que se sugiere fortalecer el control mediante programación con antelación de las transmisiones. Para lograrlo, los cálculos y factores a transmitir deberían obtenerse preferiblemente desde finales del día anterior, con el fin de evitar errores del validador de la Superintendencia Financiera de Colombia. Si eventualmente la extemporaneidad horaria obedeció a fallas de la plataforma del Regulador, Enterritorio S.A. debería procurar guardar pantallazos de los errores y constancia de las mesas de ayuda que genere, con el fin de documentar la trazabilidad y diligencia en el reporte oportuno de las transmisiones.

e) CÁLCULO DEL VAR INTERNO

Observación No.12: Falta de evidencia de ejecución del VaR interno para un día específico por las tres metodologías

Criterio: manual de gestión de riesgos financieros, numeral 5.2.2 – *Procedimiento para la medición de riesgos de mercado* que manifiesta: *"(…) "Obtener el valor en riesgo de la siguiente manera, acorde con la metodología aplicada:*

** **Simulación histórica**: ordenar los retornos absolutos de menor a mayor y buscar en la distribución el valor en riesgo equivalente al nivel de confianza definido.*

** **Paramétrico**: Ajustar los retornos a una distribución normal, calcular la media y desviación estándar de los retornos y con base en estos parámetros y el nivel de confianza definido obtener el valor en riesgo aplicando la fórmula de distribución normal inversa.*

** **Montecarlo**: Generar una serie aleatoria de retornos con el número de simulaciones definidas en los parámetros, la cual debe tener la misma media y desviación estándar que sustenta la serie histórica de los retornos. Posteriormente, conformar una distribución y hallar el valor en riesgo acorde con el percentil definido.*

Situación observada: Aunque esta Asesoría de Control Interno seleccionó aleatoriamente el día 23 de julio de 2026 para verificar el cálculo de VaR efectuado por el Grupo de Riesgos, en la respuesta entregada por memorando 202617010002503 del 2 de septiembre de 2026, en el numeral 5, indicaron: *"Se remite el informe de validación del cálculo de exposición al riesgo de mercado por el método interno el cual se efectúa de manera anual y cuyos resultados son socializados en el Comité interno de riesgos. Así mismo, se remite el acta y la presentación del ejercicio en el mes de noviembre del 2025 ante dicho comité"*

Se revisó el numeral 5.2.2. - *Procedimiento para la Medición de Riesgos de Mercado*, y no se identificó que se mencionara que bajo el método interno la medición fuera anual (lo propio se hizo con el procedimiento P-RI-04 *"Medición y Seguimiento del Riesgo de Mercado por el Método Interno y Verificación del Cumplimiento de Límites de Riesgo de Mercado* V8 del 28 de junio de 2024). De hecho, se buscaba validar el cumplimiento del manual en el numeral 5.2.2. precitado.

A raíz de lo anterior, no se pudo corroborar la aplicación de la metodología por los 3 métodos enunciados.

Recomendación: En caso de que eventualmente el grupo de riesgos cuente con el cálculo interno del VaR diario, se insta a enviar los resultados obtenidos a esta Asesoría de Control Interno para su análisis en lo que respecta al día solicitado. Sin perjuicio de esto, el error u omisión ocurrida (si existiere) pudo haberse determinado por inexactitud o malinterpretación del requerimiento de información por parte de los grupos evaluados (en este particular, el grupo de riesgos) y su respuesta.

f) VALIDACIÓN DE PRUEBAS DE FUNCIONALIDAD DE APLICATIVO DE ADMINISTRACIÓN DE INVERSIONES Y SU REPORTE

Observación No.13: Aplicativos de administración de inversiones sin parametrizaciones de criterios aprobados por Comité de Riesgos, Comité Interno de Riesgos y Junta Directiva.

Criterio: manual de gestión de riesgos financieros, numeral 5.2.4.2 Plataforma Tecnológica para la medición del riesgo de mercado: *"(…) La responsabilidad en la administración de estos sistemas de información es del Grupo de Gestión de Riesgos, quien efectuará la parametrización y configuración de los mismos, acorde con los lineamientos y metodologías aprobadas por el Comité Interno de Riesgos, el Comité de Riesgos y la Junta Directiva. Así mismo, en razón a la importancia de asegurar la precisión de los cálculos y la aplicación de los parámetros definidos en los modelos es necesario que realice la validación de la funcionalidad de los aplicativos por lo menos con una periodicidad anual. Los resultados de estas validaciones; así como las propuestas de ajustes a parámetros deben ser presentados al Comité Interno de Riesgos"*. [Énfasis añadido con subrayado].

Situación observada: en la solicitud de información de esta Asesoría de Control Interno se requirió al grupo de riesgos: *"Indicar si el aplicativo donde se hace el cierre de las operaciones de inversión tiene parametrizados los límites de que trata el numeral 5.3.4 del Manual de Gestión de Riesgos Financieros. En caso afirmativo, enviar pantallazo de dichas parametrizaciones, así como de las señales de alerta que genere al momento en que se sobrepasen dichos límites. (…)"*

La respuesta obtenida mediante memorando 202617010002503 del 2 de septiembre de 2026 fue la siguiente**:** *"Se menciona que el aplicativo donde se efectúa el cierre de las operaciones de inversión no tiene parametrizados los límites de que trata el numeral 5.3.4 del Manual de Gestión de Riesgos Financieros. Sin embargo, desde el grupo de Gestión de Riesgos se efectúa el monitoreo de manera diaria a estos límites mediante los informes diarios de utilización de cupos de inversión y contraparte y*

del mismo modo son informados de manera mensual en el Comité Interno de Riesgos. (…). Así mismo, es importante mencionar que los límites que se mencionan en el numeral 5.3.4 empezaron a regir a partir del 30 de mayo del 2026 (…)".

Al contrastar esta respuesta frente a lo indicado en el numeral 5.2.4.2 *"Plataforma Tecnológica para la medición del riesgo de mercado"*, se detecta una brecha en la optimización del control, puesto que señala: *"La medición del riesgo de mercado se debe apoyar en herramientas tecnológicas que garanticen la confiabilidad de las mediciones y la exactitud de los informes y/o archivos de salida. Se debe procurar la integración de este sistema con el sistema transaccional de inversiones de tal forma que mediante interfaces o funcionalidades se generen en forma automática los archivos de parámetros, condiciones o flujos de las inversiones, facilitando la medición y evitando riesgos operativos relacionados con la manipulación y/o modificación de los datos"* [énfasis añadido con subrayado]

Se adiciona a esto el hecho de que el mismo numeral precitado señala que: *"Para garantizar la adecuada funcionalidad de estos sistemas se debe contar con contratos de mantenimiento y/o soporte interno que cubran la actualización por cambios de normativa y/o ajustes de metodologías y el soporte para la corrección de fallas. Lo anterior con el apoyo del Grupo de Tecnología de la Información"*.

Finalmente, se refuerza la observación con el siguiente planteamiento que se encuentra en el citado numeral: *"La responsabilidad en la administración de estos sistemas de información es del Grupo de Gestión de Riesgos, quien efectuará la parametrización y configuración de los mismos, acorde con los lineamientos y metodologías aprobadas por el Comité Interno de Riesgos, el Comité de Riesgos y la Junta Directiva"* [énfasis añadido con subrayado].

En conclusión, la Sociedad está aplicando un control compensatorio detectivo en lugar del control preventivo automatizado, lo que da lugar a un riesgo operativo latente que se admite en el texto del manual que debe ser evitado.

Recomendación: que el grupo de riesgos procure diseñar y presentar un cronograma (plan de acción) para la implementación técnica de los límites en el(los) aplicativo(s) en el corto plazo, con las correspondientes pruebas de funcionamiento. El Gerente del área o quien haga sus veces debería hacer seguimiento a los hitos de dicho cronograma y asegurar que las mejoras potenciales no sean impedimento para continuar con la operación en tesorería de Enterritorio S.A.

g) ARQUEOS DE CUSTODIOS (DECEVAL – DCV)

Respecto a este punto, Se identifica oportunidad de mejoramiento en materia documental, dado que el procedimiento EI-PR-RI-09 “Monitoreo a las Inversiones en Custodia” no indica periodicidad en la que se efectúan arqueos de custodios de inversiones. Pese a esto, en el memorando de respuesta indicaron que se hace semanalmente.

El grupo de riesgos entregó entonces un total de 30 archivos (total de semanas en el periodo evaluado 1 de enero al 31 de julio de 2026). Se inspeccionaron aleatoriamente 5 carpetas: a) 20260122, b) 20260219, c) 20260326, d) 20260409 y e) 20260611. Se pudo constatar que cada una de ellas contiene 2 archivos: "EspecieValorizadas_Fecha" (extracto del custodio) y "Monitoreo Custodia_Fecha". Al analizarlos, se pudo detectar que:

I. El extracto del custodio (DECEVAL en este caso, dado que no se tienen especies en DCV) está en archivo .txt, editable, y no tiene un encabezado que permita validar la fecha de generación/impresión del

archivo y la fecha de los saldos de cierre del custodio. Si bien los batch de cierre de los custodios ocurre al final del día, eso explica por qué el nombre del archivo del extracto está nombrado con el día siguiente al de la validación. Sin embargo, para un tercero que requiera re-ejecutar el procedimiento, no se tiene evidencia de la oportunidad de la descarga. Se aconseja dejar pantallazos de evidencia de esto último y validar que el Back Office (grupo de Pagaduría) tenga imposibilidad de editar los archivos txt (lo cual debe ser extensible al Middle Office - Grupo de Riesgos).

II. El archivo Excel "Informe de Monitoreo a las Inversiones en Custodia" tiene en el campo "Fecha de Monitoreo" la fórmula "hoy()", la cual se actualiza con la apertura de los archivos Excel, dañando la trazabilidad de la oportunidad de ejecución de la prueba, por lo que se recomienda dejar la versión PDF impresa digital, o eliminar la fórmula.

III. Para el grupo de riesgos, el cruce asegura que los títulos negociados realmente estén depositados a nombre de la Entidad en el custodio. En consecuencia, mitiga el riesgo de fraude externo o error del intermediario, pero asume “ciegamente” que el reporte del portafolio ya refleja la realidad contable. Al no hacer el cruce contra registros contables, Enterritorio S.A. se expone a riesgos de integridad y exactitud, dado que pueden existir operaciones cerradas y custodiadas que aún no han sido registradas contablemente, o viceversa (por fechas de corte o fallas de interfaz); o el portafolio operativo puede tener el título, pero la contabilidad podría estar calculando mal los rendimientos, amortizaciones o valoraciones a precios de mercado. En este orden de ideas, se recomienda fortalecer el control con una "conciliación a tres bandas" (Custodio - Sistema de Portafolio - Contabilidad). Puesto que el control interno no opera bajo esquema de silos, no debería ser oponible que dicha revisión corresponda a otra área.

En el acta 76 del CIR se indica que para febrero y marzo no hubo diferencias en la validación de custodios; lo propio en el acta 77 sobre el mes de abril y acta 78 sobre el mes de mayo. Para el acta 79, se informó que se encontraba en proceso de firmas, no obstante, en su anexo se indica que se comunicó que no hubo diferencias a nivel de monitoreo de custodios. Finalmente, los informes se encuentran sin firmar, es decir, no hay evidencia de revisión.

h) VALIDACIÓN DEL MONITOREO A LA VALORACIÓN DE PORTAFOLIOS DE INVERSIÓN

El grupo de riesgos indicó en el memorando de respuesta que adjuntaba la evidencia del monitoreo a la valoración de inversiones de posición propia y de proyectos realizados en febrero y junio de 2026 con los soportes aplicables. Así las cosas, entregó las siguientes 6 carpetas: 694_13feb26, 695_24feb26, 696_28feb26, 706_05jun26, 707_23Jun26 y 708_30Jun26. Cada una de ellas contiene el archivo Excel denominado "Hoja_valoración_fecha", el archivo txt con los precios PIP y el correo electrónico de notificación.

Se analizó el contenido de los archivos Excel, encontrando las siguientes situaciones:

- En la columna AX de la hoja "Valoración Total" denominada "Validación del Spread", en la primera línea de datos (fila 2) la fórmula evalúa el tipo de título en lugar del margen, y difiere del resto de fórmulas de las filas subsiguientes. La columna se encontraba oculta y se ven resultados "Verdadero" y "Falso" sin explicación de la incidencia en los resultados de la valoración.

- Es probable que se pueda presentar desalineación a nivel de redondeos en la columna AO (precio PIP), dado que la fórmula empleada fuerza un redondeo a 3 decimales, la cual es comparada en la

columna subsiguiente frente a los datos del sistema origen de la información que, comúnmente, arroja los precios con mayor precisión, dando lugar eventualmente a "falsos negativos" sistemáticos.

- Para la convención de días al vencimiento se asumen 90 días para los CDT tasa variable asumiendo erróneamente que el corte de valoración siempre coincide con la fecha exacta de causación del cupón.

- Se detecta un riesgo de valoración en títulos UVR (columna AS - Valor presente PIP), pues la condición para TES UVR multiplica el precio de mercado por la variable K2 (precio de compra inicial). Financieramente la valoración debe proyectarse sobre el valor nominal que figura en la columna L. Esto podría generar una distorsión en la valoración del portafolio (no ocurrió porque en esta ocasión los valores de sendas columnas son iguales).

- Se detecta una “caducidad” en la serie de datos, dado que el vector de búsqueda de la columna AS cruza la fecha de valoración (junio de 2026) con la pestaña "Datos" para indexar el valor de la UVR. No obstante, la serie histórica de dicha matriz finaliza en mayo de 2013, lo que obligará a la fórmula a retornar un error irrecuperable con repercusiones en el algoritmo de cálculo.

- Hay un error conceptual en los días al vencimiento, dado que la columna AQ calcula los días utilizando la sintaxis "Días360(H2, J2), es decir, desde la fecha de compra hasta el vencimiento. Para un recálculo a precios de mercado, el plazo remanente debe medirse desde la fecha de valoración (Columna AA).

- En el ejercicio no se identifica que se haya hecho la conciliación frente a registro contables.

- Eliminar del campo "Fecha de Valoración" la fórmula Hoy (), para evitar distorsionar la trazabilidad del ejercicio de valoración.

Recomendación: establecer niveles de seguridad en la hoja de cálculo y aplicar segregación de funciones, lo cual es un estándar para herramientas ofimáticas (End-user Computing - EUC). Adicionalmente, dejar pantallazos de las extracciones y consultas que hace el Middle Office, con lo cual garantizaría la trazabilidad y re-ejecución de la rutina de valoración desde sus fuentes de origen, pues no se pudo constatar en los resultados que esos insumos fueron provistos por el profesional del grupo de riesgos.

i) VALIDACIÓN DEL MONITOREO A LA PREPARACIÓN DEL FORMATO 351.

El grupo de gestión de riesgos remitió el "Informe de Validación Formato 351 - Proforma F.000-110 Composición del Portafolio de Inversiones" el cual se efectúa una vez en el semestre. Para estos efectos, se entregó la información con corte al 30 de abril de 2026. Como resultado, se identificó inconsistencia de la columna 9 - Clase de Inversión en virtud de que 2 CDT de Banco de Bogotá identificados con los números de documento 17103 y 17273 se encuentran registrados como CDAT. No fue posible ver el archivo Excel con todas las validaciones aplicadas por el grupo de riesgos.

Como conclusión, el grupo de riesgo indicó que la desviación precitada se presentó en 2 de 125 títulos, se solicitó generar el respectivo evento de riesgo operativo por las inconsistencias generadas en la revisión y se solicitaron las respectivas aclaraciones. Se identificó el archivo "Respuesta Monitoreo", en donde efectivamente se corrobora la existencia del error de clasificación advertido en la operación

realizada el 26 de septiembre de 2025, y subsanando en el aplicativo como corresponde. No se detalla quién dio la respuesta por parte del Back Office y los efectos materializados en un evento de riesgo operativo.

La situación anterior fue informada en el acta 77 del CIR del 20 de mayo de 2026.

Desde el punto de vista de diseño del control, se está aplicando un control detectivo periódico a un riesgo de materialización continua (hay un desfase entre la periodicidad semestral de validación y la diaria de transmisión del formato).

Recomendación: migrar a un control preventivo automatizado mediante la parametrización de reglas de validación (validación de campos obligatorios, topes lógicos, clasificaciones, etc) que bloqueen la generación del archivo si existen inconsistencias previas a la transmisión, y que genere un informe de errores y excepciones para su identificación y subsanación. En lo posible, es ideal contar con el log de auditoría de los cambios implicados.

Aunque el control semestral podría conservarse, en vez de validarse la confección del archivo, debería enfocarse en verificar la robustez y la efectividad de las alertas automáticas y los bloqueos del sistema (entre otros asuntos).

1.3. GESTIÓN DE RIESGO OPERACIONAL

Para la evaluación de este sistema de administración de riesgos (en adelante, referido como SARM), el alcance de las pruebas se enfocó en los siguientes aspectos:

a) Perfil de riesgo – actualización
b) Indicadores de Riesgo Operacional 2026 y su comportamiento
c) Normativa SARO y cambios para considerar en el SIAR.
d) Registro de eventos de riesgo operacional-ERO, y monitoreo.
e) Planes de tratamiento ERO
f) Medición y control Riesgos Operacionales
g) Monitoreo a la Gestión del Riesgo Operacional

Los resultados obtenidos se exponen a continuación:

a) PERFIL DE RIESGO - ACTUALIZACIÓN

Se realizó verificación documental a la actualización del Perfil de Riesgos Operacional, en cumplimiento de lo registrado en los numerales 7.2.1 IDENTIFICACIÓN del Manual Del Sistema Integral de Administración de Riesgos-SIAR (M-RI-08) versión 04 del 2025 y 7.3.1 IDENTIFICACIÓN del Manual de Gestión de Riesgos Operacionales (M-RI-03) versión 14 del 2025; identificando las siguientes actividades ejecutadas en el mes de junio:

- Comunicación de la actualización del Perfil de Riesgo SIAR 2026 - Operacional, Soborno, Fraude y Corrupción (18° versión) a todos los responsables y/o gerentes de grupo o área, mediante radicado interno No.202617010000893 del 28 de junio; con plazo máximo de remitir observaciones frente a los ajustes propuestos al 30 de junio.

- Correo electrónico de recordatorio para actualización del perfil de riesgo y asistencia a la socialización de la nueva metodología programada para el 04 de junio.
- Consolidación de matrices de riesgos de los 17 procesos de la Sociedad, identificando los cambios y/o ajustes relevantes para la vigencia 2026.
- Informe de actualización de perfiles de riesgo para los 17 procesos de la Sociedad.
- Análisis de los ajustes realizados a los perfiles de riesgo por parte de los 17 procesos de la Sociedad; los cuales fueron comunicados mediante correos electrónicos de solicitudes y respuestas en las siguientes fechas. No obstante, para el 76% (13) de los procesos, no se identificó aprobación directa de los cambios efectuados a las matrices.

Tabla No.6 Sesiones de actualización perfil de riesgos

Proceso	Fecha de comunicación Grupo Gestión de Riesgo	Fecha de respuesta proceso	Fecha límite respuesta procesos
Gestión de Riesgo	02/06/2026	No se identificó	30/06/2026
Gestión Integral de Procesos	02/06/2026 y 03/07/2026	02/06/2026	30/06/2026
Gestión de las Comunicaciones	09/06/2026	No se identificó	30/06/2026
Direccionamiento estratégico	02/06/2026 y 01/07/2026	30/06/2026	30/06/2026
Auditoría Interna	09/06/2026 y 02/07/2026	26/06/2026	30/06/2026
Estructuración de Proyectos	02/06/2026	No se identificó	30/06/2026
Gestión de Talento Humano	02/06/2026, 30/06/2026 y 01/07/2026	16/06/2026, 30/06/2026	30/06/2026
Evaluación de Proyectos	No se identificó	No se identificó	30/06/2026
Gerencia y Gestión de Proyectos	02/06/2026	No se identificó	30/06/2026
Gestión de Tecnologías de la Información	No se identificó	No se identificó	30/06/2026
Gestión Administrativa	09/06/2026	No se identificó	30/06/2026
Gestión Comercial	09/06/2026	No se identificó	30/06/2026
Relacionamiento Ciudadano	09/06/2026 y 01/07/2026	No se identificó	30/06/2026
Gestión de Proveedores	09/06/2026	No se identificó	30/06/2026
Gestión Financiera	02/06/2026	No se identificó	30/06/2026
Gestión Documental	No se identificó	No se identificó	30/06/2026
Gestión Jurídica	16/06/2026	No se identificó	30/06/2026

Fuente: Elaborado ACI a partir de soportes de actualización perfiles de riesgos 2026.

Si bien, se identificó que la actualización abarco el 100% (17) de los procesos de la Sociedad, efectuando una reevaluación de los riesgos y controles institucionales; el perfil de riesgos se mantuvo en “Moderado” a corte julio del 2026.

Imagen No.4 – Perfil de Riesgo Operacional al 30 de junio del 2026



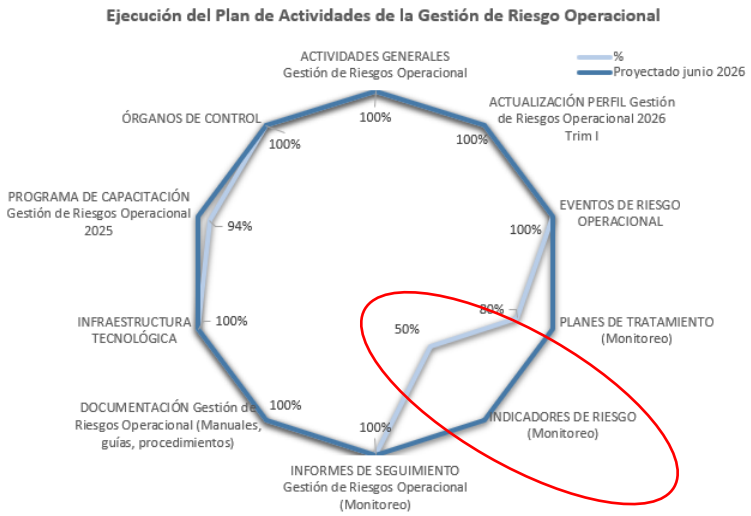
Fuente: Matriz de Riesgo del Sistema Integral de Administración de Riesgo - SIAR

El detalle de los ajustes se amplía en el apartado *Medición y control* del presente numeral.

b) INDICADORES DE RIESGO OPERACIONAL 2026 Y SU COMPORTAMIENTO

Se inspeccionó el documento entregado por el grupo de riesgos denominado "Aspectos Relevantes del Sistema Integral de Administración del Riesgo SIAR II Trimestre 2026" en donde, respecto de los indicadores de riesgo operacional, se manifestó el siguiente estado del plan de actividades de Gestión de Riesgo Operacional:

Imagen No.5 – Grado de ejecución del plan de actividades del SARO



Fuente: Informe “"Aspectos Relevantes del Sistema Integral de Administración del Riesgo SIAR II Trimestre 2026"

Se aprecia que la etapa de monitoreo, correspondiente a Indicadores de Riesgo, se tasó una ejecución del plan en un 50%. Al ver el análisis del hito, se indicó lo siguiente: *"Se evidencian debilidades en la medición de los indicadores y hojas de vida. Adicional, al cargue de información por parte de los*

responsables en el aplicativo GRC. Para el tercer trimestre ya se cuenta con un proyecto de actualización de indicadores claves de riesgo con los gestores de riesgo, líderes de proceso y Grupo de desarrollo organizacional".

No es claro cómo se midió el avance de 50%, si se tiene en cuenta que se mencionan las debilidades de medición y hojas de vida de indicadores y que, además, se encuentra en implementación el Capítulo VIII de la Guía Metodológica de Riesgos V7 del DAFP que requiere de surtir 3 hitos, donde el primero es *"Reportar los indicadores claves para cada uno de los 17 procesos (máx 3 por proceso)"* y que *"Para el tercer trimestre de la presente vigencia ya se estima reportar con un proyecto de actualización de indicadores claves de riesgo con los gestores de riesgo, líderes de proceso y Grupo de Desarrollo Organizacional para ser asociados con los procesos de la Sociedad"*.

Sin perjuicio de lo anterior, el grupo de riesgos aportó el memorando de respuesta 202616010001183 del 29 de julio de 2026 mediante el cual el Gerente del Grupo de Planeación y Desarrollo Organizacional respondió a la solicitud del 23 de julio de 2026 efectuada por correo por el Gerente del Grupo de Gestión de Riesgos, donde adjuntó el archivo "Batería de indicadores", el cual consta de 2 pestañas: la primera, los indicadores de gestión por proceso; y la segunda, los indicadores estratégicos por cada programa estratégico que hace parte integral del plan institucional 2026. En dicho comunicado, se manifiesta que: *"Con estos insumos, el grupo de gestión de riesgos puede definir junto con los líderes de proceso cuáles son los indicadores clave que deben quedar definidos".*

Al analizar el archivo precitado, en la pestaña "Batería Indicadores SIG 2026", se filtró por el proceso de "Gestión de Riesgo", en donde, para efectos de esta evaluación, se identificó el indicador "SIG-RI-211 - Actualización perfiles de riesgos operacional - fraude Enterritorio", con una periodicidad semestral y una meta de 100. Seguidamente, se validó el archivo de la hoja de vida de este indicador, cuya fecha de creación fue el 12 de junio de 2025 y última modificación el 3 de enero de 2026. Llama la atención que la fecha fin sea el 31-dic-2046 (posiblemente, un error tipográfico, pudiendo ser 2026).

Al analizar el resto del contenido, se enuncia que la fórmula es: # de perfiles actualizados en el periodo (X) / # de perfiles planeados en el periodo (Y) * 100. Se advierte error en la explicación de las variables, pues X e Y tienen la misma información en ella.

Se manifiesta que en los 2 semestres de 2025 hubo avance del 100%, y en el primer semestre de 2026 también avance del 100%, sin embargo, no se observó el cronograma base que permitiera llegar a esas conclusiones; adicionalmente, no se logra vincular el objetivo del indicador con su formulación.

En virtud de lo señalado en los párrafos anteriores, y la falta de disponibilidad de información, no fue posible validar el comportamiento en el tiempo, y según la periodicidad, del indicador propuesto. Adicionalmente, el ejercicio se efectuará en el tercer trimestre de 2026.

Recomendación: Enterritorio S.A. debería buscar mecanismos de seguimiento a los hitos del cronograma de actividades propuesto dentro de las actividades de Riesgo Operacional, vinculando el alto nivel directivo en las áreas para validar su avance y su pertinencia. Así mismo, procurar obtener un mecanismo que ayude a medir los grados de avance de las tareas y validación frente a soportes debidamente respaldados dentro de las hojas de vida de los indicadores. Dado que se viene comentando sobre fallas en el diseño de estas hojas de vida y su cargue en el aplicativo GRC, se insta a buscar espacios de capacitación (dirigidos a los grupos, o generales) que otorguen protocolos de creación, diseño y seguimiento.

c) NORMATIVA SARO Y CAMBIOS PARA CONSIDERAR EN EL SIAR.

Se inspeccionó el informe de aspectos relevantes SIAR II trimestre 2026 respecto del Riesgo Operacional, y no se identificó nueva normativa sobre este sistema de administración de riesgos. Los cambios que se han presentado es a nivel del SIAR por la agregación de nuevos pilares al sistema (por ejemplo, gestión de riesgos estratégicos (SARE), la gestión de riesgos ambientales y sociales (SARAS), Gestión de Grandes Exposiciones y Concentración de Riesgos y Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

El esquema entonces es el siguiente:

Imagen No.6 – Esquema SIAR 2026



Fuente: Informe "Aspectos Relevantes del Sistema Integral de Administración del Riesgo SIAR II Trimestre 2026"

d) REGISTRO DE EVENTOS DE RIESGO OPERACIONAL-ERO

De lo reportado por el Grupo Gestión de riesgos se identificó que a corte julio del 2026 se registraron 350 ERO; para los cuales el análisis se presenta a continuación:

Identificación eventos ERO:

Tras la revisión detallada de la base de datos suministrada por el Grupo de Gestión de Riesgos, se evidenció que aun cuando se reportan 350 ERO en el periodo de enero a julio de 2026, la cifra real asciende a 365 materializaciones de riesgo. Esta diferencia obedece a que en un mismo registro o reporte individual se evidenció la ocurrencia simultánea de varios riesgos asociados; tal y como se evidencia en los siguientes 8 reportes en que se materializaron 23 riesgos:

Tabla No.7 Reporte ERO múltiple a julio del 2026

Referencia	Fecha Registro	Fecha Inicio (Fecha materialización)	Fecha Descubrimiento	Fecha Finalización (Fecha acciones correctivas)	Proceso Afectado	Proceso Reportante	Riesgo Identificado
202600043	5/03/2026	5/03/2026	5/03/2026	5/03/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-7, ROPEGG-17
202600044	13/03/2026	3/03/2026	3/03/2026	16/03/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-7, ROPEGG-17
202600092	31/03/2026	10/03/2026	10/03/2026	31/03/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-6, ROPEGG-7
202600093	31/03/2026	1/03/2026	1/03/2026	31/03/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-6, ROPEGG-7, ROPEGG-50
202600116	16/04/2026	15/04/2026	15/04/2026	16/04/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-12, ROPEGG-17
202600118	23/04/2026	20/02/2026	20/04/2026	28/04/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-7, ROPEGG-12, ROPEGG-17
202600228	26/06/2026	1/03/2026	22/06/2026	22/06/2026	Gestión Del Riesgo – Sarlaft	Gestión Del Riesgo - Sarlaft	ROPERI-2, ROPERI-1, ROPERI-8, ROPERI-10, ROPERI-24, ROPERI-26
202600344	27/07/2026	23/07/2026	23/07/2026	28/07/2026	Gerencia y Gestión De Proyectos	Gerencia y Gestión De Proyectos	ROPEGG-7, ROPEGG-12, ROPEGG-17

Fuente: Elaboración ACI, a partir del reporte ERO a julio del 2026

De igual forma, se identificó que los ERO realmente cuantificados en la vigencia 2026 son 325; ya que, 38 se materializaron en el 2025 (37 para el riesgo ROPERC-4 y 1 para el ROPEEV-20), 1 en el 2024 (ROPEGG-7) y 1 en el 2021 (ROPEGG-49), pero se reportaron por los procesos responsables en enero, abril y julio del 2026.

Finalmente, de los 365 eventos se identificaron 3 clasificados en categoría Tipo A (Generan pérdidas y afectan el estado de resultados de la Entidad), evidenciando que los controles existentes presentan fallas y/o debilidades metodológicas al no prevenir la materialización de eventos con impacto económico directo, lo que expone a la Sociedad a un posible detrimento patrimonial:

202600039: Se registró una provisión contable por **$283.100.000** en el marco del Contrato Interadministrativo No. 223006 de 2023 con Fondo Paz, fundamentada en los memorandos técnicos y jurídicos No. 202622010000893 y No. 202670010000163 de enero de 2026. La medida atiende el riesgo de indisponibilidad oportuna de recursos para la contratación de personal en territorio, lo que compromete la gestión de alertas tempranas y la verificación de los Incentivos para la Paz, exponiendo a la Sociedad a impactos reputacionales e incumplimientos de los productos pactados.

202600095: Materialización de pérdida económica por fallo adverso del Juzgado 26 Civil del Circuito de Bogotá (Rad. 11001310302620210017700), el cual ordenó el pago a favor del Consorcio Proyectar Colombia mediante transacción aprobada por **$3.635.564.506** (incluye actas de servicio, daño emergente, indexación y costos, con un descuento aplicado de $308.502.511). El desembolso se ejecutó

el 29 de abril de 2026 (Obligación OBLI2026-003225), representando un consumo del 5,67% de la liquidez del componente de funcionamiento y manteniendo el Indicador de Riesgo de Liquidez (IRL) agregado en 1,67% al cierre del 1 de mayo de 2026.

202600120: Materialización de riesgo jurídico por sentencia laboral adversa proferida por el Juzgado 01 Laboral, la cual declaró la existencia de contrato de trabajo a favor del demandante. La decisión judicial condenó a la Entidad al pago de **$1.127.896.708** por concepto de salarios, prestaciones sociales, indemnizaciones y aportes al Sistema General de Seguridad Social (especialmente en el subsistema de pensiones).

Tabla No.8 ERO tipo A del 2026

Fecha Inicio (Fecha mate-rialización)	Riesgo Identifi-cado	Con-trato	Convenio	Cuantía – Pérdida Estimada	Pérdida Real Total - Cuantía bruta	Cuantía de otras recupe-raciones	Pérdida Total	Fecha de Registro Contable
29/01/2026	ROPEGG-7	223006	223006	$ 0,00	$ 283.100.000,00	$ 0,00	$ 283.100.000,00	30/01/2026
1/04/2026	ROPEJU-4	2131909	No aplica	$ 3.635.564.506,00	$ 3.635.564.506,00	$ 0,00	$ 3.635.564.506,00	30/04/2026
21/04/2026	ROPEJU-4	No aplica	No aplica	$ 1.400.000.000,00	$ 1.127.896.708,00	$ 272.103.292,00	$ 1.127.896.708,00	7/05/2026
Total				$ 5.035.564.506,00	$ 5.046.561.214,00	$ 272.103.292,00	$ 5.046.561.214,00	

Fuente: Elaboración ACI, a partir del reporte ERO a julio del 2026

Observación No.14 Oportunidad en el Reporte ERO:

Criterio: De acuerdo con lo señalado en:

a. El Manual del Sistema Integral de Administración de Riesgos- SIAR (M-RI-08) versión 04 del 2025, 6.2.10 Gestores De Riesgo, numeral 6. "*Reportar de manera inmediata, una vez identificado los eventos o situaciones que afecten los objetivos de la Sociedad*"

b. La Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03) versión 8 del 2023, numeral 2. Responsabilidades Generales, titulo Responsabilidades de los Gestores de riesgo, punto No.1 "*Reportar de manera inmediata, una vez identificado los eventos de riesgos operacional que le informan los colaboradores de su proceso.*"

Situación observada: Una vez cuantificados los ERO reportados a corte julio del 2026, se procedió a verificar si el reporte por parte de los procesos responsables en el aplicativo CGR fue oportuno. Para lo cual, se contrastó la fecha del registro en el aplicativo contra la fecha del descubrimiento del evento; en donde:

Tabla No.9 Criterios Valoración Oportunidad reportes ERO

Fecha registro = Fecha descubrimiento o máximo 24 horas después del evento	OPORTUNO
Fecha registro > Fecha descubrimiento	INOPORTUNO

Fuente: elaboración ACI.

- El 1% (5) de los reportes de eventos ocurridos entre los meses de enero, febrero, marzo y junio fueron realizados **oportunamente**; es decir, el mismo día o entre las 24 horas siguientes del descubrimiento de la materialización de los 6 riesgos:

    - ROPEGG-50, 2 veces (16/01/2026 y 25/06/2026)
    - ROPEGG-7, 3 veces (29/01/2026, 27/02/2026 y 5/03/2026)
    - ROPEGG-17, 1 vez (5/03/2026)

- El 99% (345) de los reportes de eventos fueron realizados de manera **inoportuna**; lo anterior, debido a que:

    - 305 reportes de eventos que ocurrieron a julio del 2026 fueron reportados entre 1 o 2 meses después de la fecha del descubrimiento.
    - 38 reportes de eventos que ocurrieron en mayo y diciembre del 2025 (37 para el riesgo ROPERC-4 y 1 para el ROPEEV-20), fueron reportados en enero, abril y julio del 2026.
    - El reporte del riesgo que ocurrió en mayo del 2024 (ROPEGG-7), fue reportado en enero del 2026.
    - El reporte del riesgo que ocurrió en noviembre del 2021 (ROPEGG-49), fue reportado en enero del 2026.

- El riesgo con mayor concentración de ERO en el periodo de seguimiento fue el ROPERC-4 *("Inoportunidad en el cumplimiento de los términos de Ley para atender las PQRDSF"),* registrando 313 materializaciones que equivalen al 85,75 % del total de eventos reportados; lo que representa una debilidad crítica en la Sociedad, donde las medidas adoptadas no han logrado subsanar la causa raíz de las extemporaneidades, supeditando la gestión a acciones reactivas frente al trámite de solicitudes ciudadanas.

Recomendación: se recomienda al Grupo de Gestión de Riesgos analizar la viabilidad de adoptar como parámetro de cumplimiento, el umbral de reporte dentro de las 24 horas siguientes al descubrimiento del evento e incluirlo como lineamiento interno en la Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03); para posterior divulgar y capacitar a los colabores de la Sociedad, principalmente a los Gestores de Riesgos sobre la importancia estratégica del reporte oportuno en el marco de la gestión de riesgos operacionales.

Acciones implementadas ERO

El análisis cualitativo de las respuestas operativas frente a los ERO reportados a 2026 revela un sistema con alta capacidad de reacción y contención posterior, pero con debilidades estructurales en la prevención y en la automatización de procesos clave; a continuación, el detalle de lo evidenciado:

Tabla No.10 Diagnóstico acciones implementadas ante ERO 2026

Categoría de Riesgo	Evaluación de las Acciones	Diagnóstico Principal
Relacionamiento con el Ciudadano (ROPERC)	Parcialmente Adecuadas	Las medidas de control (semáforos y reportes periódicos) logran encausar la gestión administrativa, pero no resuelven la causa raíz: la falta de respuesta oportuna dentro de los términos legales iniciales por parte de los procesos ejecutores.
Riesgos Jurídicos (ROPEJU)	Adecuadas	Frente de mayor efectividad en la mitigación del impacto financiero. Las acciones se enfocaron en la negociación y suscripción de acuerdos transaccionales que generaron eficiencias y contención de pérdidas probables en litigios.
Eventos de Fraude (ROPEEV)	Adecuadas (Reactivas)	Rigor en las acciones penales y técnicas posteriores a la detección de la irregularidad (como en el caso de Vivienda Rural). Sin embargo, la acción es netamente reactiva, reflejando vacíos en los controles preventivos de validación en campo o de supervisión previa.
Gestión Contractual (ROPEGG)	Parcialmente Adecuadas	La respuesta institucional ha dependido del uso recurrente de prórrogas y suspensiones. Si bien estos mecanismos resuelven la coyuntura contractual inmediata, no solucionan las deficiencias de planeación o de ejecución del contratista/interventor desde el origen.
Tecnológicos / Reportes (ROPERI)	Inadecuadas / Básicas	La atención de incidentes (como las fallas en la transmisión del VaR a la SFC y los registros de Moodle) se apoya en reprocesos manuales y gestión por demanda, sin contar con protocolos de contingencia automáticos ni parametrizaciones sólidas.

Fuente: Elaboración ACI, a partir del reporte ERO a julio del 2026

Recomendación: Es importante que los procesos junto con su equipo de trabajo alineen la ejecución de sus actividades hacia controles de mayor efectividad y de carácter preventivo; ya que, es necesario trascender el uso de mecanismos de contingencia o de mero seguimiento formal (como prórrogas, reportes de semáforos o reprocesos manuales) e implementar acciones orientadas a resolver las causas raíz que originan los eventos de riesgo. Para ello, cada proceso debe evaluar periódicamente el diseño de sus controles en acompañamiento del Grupo Gestión de Riesgos, priorizando la automatización de actividades, la optimización de los tiempos de respuesta y la verificación previa en la operación diaria, garantizando así una gestión del riesgo oportuna, sostenible y alineada con los objetivos del SIAR y SARO.

e) PLANES DE TRATAMIENTO ERO

En este apartado se buscó identificar los planes de tratamiento de riesgos vigentes a corte julio del 2026, formulados e implementados por los procesos responsables en cumplimiento de los numerales 6.2.8 Gestores de Riesgo: *"Apoyar la definición de planes de contingencia y la formulación de planes de tratamiento para mitigar los riesgos, acorde con las políticas definidas en la actividad, la ejecución de las respectivas acciones y el seguimiento y reporte frente a avances y cumplimiento."*, 7.3.2.4 Evaluación y tratamiento de riesgos: *"La decisión de asumir riesgos es exclusivamente potestad de la Presidencia o del Comité Interno de Riesgos. En ningún caso el responsable de proceso podrá asumir riesgos que se encuentren ubicados en la zona de severidad "Significativo" y "Considerable", para los cuales deberá formular e implementar planes de tratamiento para mitigarlos."* y 7.8 Registro de Eventos: *"Como resultado del análisis y seguimiento de los eventos de riesgo operacional con alto impacto o probabilidad se deben definir planes de tratamiento para mitigar o prevenir la ocurrencia de nuevos eventos de riesgo, cuya responsabilidad está a cargo de los responsables de proceso."*

Frente a esto, revisados los informes de Aspectos relevantes del SIAR I y II trimestre del 2026, se identificaron los siguientes planes de tratamiento ERO vigentes en la Sociedad:

Tabla No.11 Planes de tratamiento ERO vigentes

PROCESO	CÓDIGO RIESGO	PLAN DE TRATAMIENTO	AVANCE %	Estado al II trimestre 2026
Gestión Comercial	ROPEGCO-3	TRATCM2401	90%	En ejecución de actividades (mesa de trabajo)
Gestión de Riesgos	ROPERI-2	TRATRI2504	95%	En ejecución de actividades (delegación nuevo responsable para atender actividades del plan por parte del grupo de operaciones)
Gerencia y Gestión de Proyectos	ROPEGG-7	TRATGG26010	50%	Sin reporte de avances en la ejecución de actividades; se mantienen las realizadas en el I trimestre (actas de comité, reporte de indicadores)
Evaluación de Proyectos	ROPEEV-9	TRATEV2404	100%	Se cumple el plan de tratamiento.
Evaluación de Proyectos	ROPEEV-11	TRATEV2405	100%	Se cumple el plan de tratamiento.
Estructuración de Proyectos	ROPEEP-7	TRATES2505	40%	En ejecución de actividades (mesa de trabajo)
Estructuración de Proyectos	ROPEEP-15	TRATES2506	5%	En ejecución de actividades (mesa de trabajo)

Fuente: Elaboración ACI a partir de informes de Aspectos relevantes SIAR I y II trimestre 2026.

De lo informado por el Grupo Gestión de Riesgos en sus informes, se registra el cierre de 2 de los 7 planes de tratamiento vigentes (asociados a los riesgos ROPEEV-9 y ROPEEV-11), ya que se cumplió el 100% de las actividades. Por las limitaciones de tiempo y alcance propuesto de este seguimiento, no se llevó a cabo la verificación de la ejecución y/o cumplimiento de las actividades formuladas en cada uno de los 7 planes; por lo que serán objeto de verificación en el próximo seguimiento.

f) MEDICIÓN Y CONTROL DE RIESGOS OPERACIONALES

En cumplimiento del numeral 7.3.2 Análisis y Valoración de los Riesgos del M-RI-03, se verificó la matriz de riesgos consolidada para la vigencia 2026; identificando para el I trimestre no hubo cambios respecto de las zonas de riesgo inherente y residual, perfil de riesgo (Moderado) y cantidad de riesgos y controles; por lo tanto, se corroboró que se registran los 264 riesgos y 424 controles identificados en la vigencia 2025 para los 17 procesos de la entidad.

Así mismo, se identificó que el 69% (294) de los controles son de tipología Preventiva, el 9% (37) son Correctivos y el 22% (93) son Detectivos.

De otra parte, verificada la matriz propuesta derivada de la actualización del perfil de riesgos realizada en el mes de junio, se identificaron los siguientes cambios:

- Variación de la cantidad de riesgos, disminuyendo de 264 a 126 (47,7%); obedeciendo no a una supresión de controles, sino a una estrategia de unificación de causas y mitigación de duplicidades, ya que, la mayoría de las causas e impactos de los riesgos derogados fueron consolidados o reasignados a riesgos vigentes. Por ejemplo, los riesgos ROPEAU-5, ROPEAU-

7, ROPEAD-1, ROPEAD-4 tuvieron sus causas asociadas y trasladadas a los riesgos ROPEAU-2 y ROPEAD-2.

No obstante, se identificaron las siguientes debilidades:

Gerencia y Gestión de Proyectos: teniendo en cuenta que en el informe de actualización del perfil de riesgos del proceso, no se detalló las justificaciones de eliminación de los riesgos ROPEGG-2, ROPEGG-4, ROPEGG-6, ROPEGG-8, ROPEGG-9, ROPEGG-10, ROPEGG-11, ROPEGG-18, ROPEGG-19, ROPEGG-21, ROPEGG-23, ROPEGG-25, ROPEGG-26, ROPEGG-29, ROPEGG-30, ROPEGG-31, ROPEGG-32, ROPEGG-33, ROPEGG-34, ROPEGG-35, ROPEGG-36, ROPEGG-38, ROPEGG-42, ROPEGG-43, ROPEGG-44, ROPEGG-45, ROPEGG-46, ROPEGG-51, ROPEGG-53, ROPEGG-54 y ROPEGG-55; no se pudo identificar las justificaciones de la eliminación o derogación, ni la certeza de que su cubrimiento fuera reasignado en los riesgos vigentes.

Evaluación de Proyectos: teniendo en cuenta que no se aportó el informe que detalla la actualización del perfil de riesgos del proceso, no se pudo identificar las justificaciones de la eliminación o derogación de los riesgos ROPEEV-5, ROPEEV-9, ROPEEV-11, ROPEEV-12, ROPEEV-13, ROPEEV-17, ROPEEV-21, ROPEEV-23, ROPEEV-25, ROPEEV-29, ROPEEV-30, ROPEEV-32 y ROPEEV-33, y los ajustes a los riesgos que se mantienen en la matriz.

Así entonces, riesgos críticos sobre fraude documental (ROPEEV-23), contratación fraudulenta (ROPEEV-25), soborno en aprobaciones/pagos (ROPEEV-29, 30, 32) y seguridad de datos (ROPEEV-33) quedaron formalmente derogados sin certeza de que su cubrimiento fuera reasignado en los demás riesgos vigentes.

Gestión de las Tecnologías de la Información: la eliminación de 8 riesgos especializados (ROPETI-2, 5, 7, 8, 9, 10, 11 y 13) para unificarlos exclusivamente en el riesgo *ROPETI-1 Falta de integridad, confidencialidad y disponibilidad de los aplicativos, portales, sistemas de información, Core del negocio, plataforma tecnológica o servicios en la nube*; debilita la especificidad de los monitoreos realizados a la subutilización de software, fallas de hardware, licencias no autorizadas, hurto de equipos, operaciones no autorizadas y fugas de información por soborno.

Gestión de Riesgos: se eliminaron 5 riesgos independientes sobre Protección de Datos Personales (ROPERI-21, 23, 25, 27 y 28) y se reasignaron de forma agrupada en los riesgos ROPERI-20 (*Limitación de los derechos o uso ilegítimo que tienen los titulares con respecto a sus datos personales*) y ROPERI-22 (*Incumplimiento en la obligación de registrar las bases de datos y suscripción de contratos con terceros sin cláusulas de responsabilidad sobre el manejo de la información, datos personales, lineamientos de Gestión de Riesgos y recursos tecnológicos*). Así mismo, se suprimieron los riesgos ROPERI-7 (*consulta en listas vinculantes*) y ROPERI-9 (*gestión de operaciones inusuales y sospechosas*), pasando sus causas al riesgo ROPERI-8 (*Omisión, inoportunidad o inconsistencias de la base de Eventos de Riesgo Operacional (ERO), operaciones inusuales o sospechosas e incidentes de seguridad de la información y datos personales*); de lo anterior, se identifica:

Incumplimiento de la Ley 1581 de 2012 / SIC), ya que, el marco normativo expedido por la Superintendencia de Industria y Comercio (SIC) exige que la Entidad realice el correcto tratamiento de datos sensibles y de Niños, Niñas y Adolescentes - NNA (Anterior ROPERI-25);

ya que, requieren autorización previa y explícita, y su fusión en ROPERI-20 visibiliza un tratamiento ordinario a un dato con protección. Adicional, se menciona que con las causas se complementa la numero 10 del ROPERI-20, la cual no se identifica (se registran únicamente 9 causas)

Afectación al Monitoreo Específico del SARLAFT (Circular Externa 018 de 2021 - SFC): El Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) exige el seguimiento riguroso y diferenciado de la detección y reporte de Operaciones Inusuales y Sospechosas - ROS (Anterior ROPERI-9) y la consulta en listas vinculantes e inhibitorias (Anterior ROPERI-7). Al fusionar el riesgo de reporte de ROS con el registro de la base general de ERO de la Entidad en el riesgo ROPERI-8, se desdibuja la prioridad técnica y la confidencialidad que exige la normativa de la Superintendencia Financiera de Colombia para las alertas de SARLAFT, exponiendo a la Sociedad a investigaciones y sanciones administrativas o de supervisión.

Tabla No.12 Riesgos Operacionales eliminados a julio del 2026

Proceso	Riesgos eliminados
Auditoría Interna	ROPEAU-5, ROPEAU-7
Gestión Administrativa	ROPEAD-1, ROPEAD-4, ROPEAD-6, ROPEAD-9, ROPEAD-10, ROPEAD-11, ROPEAD-12, ROPEAD-13
Gestión de las Comunicaciones	ROPECO-1
Relacionamiento con el Ciudadano	ROPERC-1, ROPERC-3, ROPERC-6
Direccionamiento Estratégico	ROPEDE-2, ROPEDE-4, ROPEDE-5
Gestión Integral de Procesos	ROPESI-2, ROPESI-5
Gestión de Riesgos	ROPERI-3, ROPERI-4, ROPERI-7, ROPERI-9, ROPERI-13, ROPERI-21, ROPERI-23, ROPERI-25, ROPERI-27, ROPERI-28, ROPERI-31
Gestión de Proveedores	ROPEPR-12, ROPEPR-13, ROPEPR-14
Gestión del Talento Humano	ROPETH-4, ROPETH-6, ROPETH-7, ROPETH-11, ROPETH-13, ROPETH-14, ROPETH-18, ROPETH-21, ROPETH-22, ROPETH-26, ROPETH-27, ROPETH-28, ROPETH-29, ROPETH-31, ROPETH-33
Gerencia y Gestión de Proyectos	ROPEGG-2, ROPEGG-4, ROPEGG-6, ROPEGG-8, ROPEGG-9, ROPEGG-10, ROPEGG-11, ROPEGG-18, ROPEGG-19, ROPEGG-21, ROPEGG-23, ROPEGG-25, ROPEGG-26, ROPEGG-29, ROPEGG-30, ROPEGG-31, ROPEGG-32, ROPEGG-33, ROPEGG-34, ROPEGG-35, ROPEGG-36, ROPEGG-38, ROPEGG-42, ROPEGG-43, ROPEGG-44, ROPEGG-45, ROPEGG-46, ROPEGG-51, ROPEGG-53, ROPEGG-54, ROPEGG-55
Evaluación de Proyectos	ROPEEV-5, ROPEEV-9, ROPEEV-11, ROPEEV-12, ROPEEV-13, ROPEEV-17, ROPEEV-21, ROPEEV-23, ROPEEV-25, ROPEEV-29, ROPEEV-30, ROPEEV-32, ROPEEV-33
Estructuración de proyectos	ROPEEP-5, ROPEEP-6, ROPEEP-13, ROPEEP-14, ROPEEP-18, ROPEEP-20, ROPEES-23, ROPEES-24, ROPEES-25, ROPEES-26, ROPEES-27, ROPEES-28, ROPEES-29 y ROPEES-30

Proceso	Riesgos eliminados
Gestión Financiera	ROPEFI-2, ROPEFI-9, ROPEFI-11, ROPEFI-12, ROPEFI-13, ROPEFI-14, ROPEFI-19, ROPEFI-21, ROPEFI-24, ROPEFI-26, ROPEFI-27, ROPEFI-28, ROPEFI-29, ROPEFI-31, ROPEFI-34, ROPEFI-37, ROPEFI-38, ROPEFI-39
Gestión Jurídica	ROPEJU-4, ROPEJU-7, ROPEJU-9, ROPEJU-10
Gestión de las Tecnologías de la Información	ROPETI-2, ROPETI-5, ROPETI-7, ROPETI-8, ROPETI-9, ROPETI-10, ROPETI-11, ROPETI-13
Gestión Documental	ROPEDO-5, ROPEDO-9

Fuente: Elaborado ACI a partir de soportes de actualización perfiles de riesgos 2026.

- Para 7 riesgos no se identificó cambios en el marco de la actualización del perfil de riesgos: Gerencia y Gestión de Proyectos (ROPEGG-17 y ROPEGG-50), Estructuración de proyectos (ROPEEP-7, ROPEEP-10, ROPEEP-15 y ROPEEP-16), y Gestión Financiera (ROPEFI-8)

- En materia de controles, se identificó variación pasando de 424 a 431; donde el 70% (300) son de tipología Preventiva, el 9% (38) son Correctivos y el 22% (93) son Detectivos.

Recomendación:

Se recomienda a los líderes de proceso que, en articulación con el Grupo de Gestión de Riesgos, revisen la actualización del perfil de riesgos efectuada en junio de 2026, con el fin de verificar que las consolidaciones de riesgos realizadas se encuentren debidamente alineadas con las operaciones reales de la Sociedad y la normatividad vigente aplicable. En dicho ejercicio, es importante garantizar entre otros que, los eventos de interrupción de infraestructura y tecnología mantengan fichas independientes de las conductas éticas o de soborno, desglosar las categorías tecnológicas en dominios operativos claros y restablecer el seguimiento específico sobre las obligaciones legales y regulatorias asegurando una evaluación objetiva de la mitigación del riesgo institucional.

Adicional, monitorear de forma continua el impacto de la consolidación de riesgos efectuada en junio de 2026, dado que un número reducido de riesgos concentra ahora múltiples causas transversales. Así mismo, evaluar la efectividad de los controles clave asociados, toda vez que la falla de un control podría elevar de manera simultánea la zona de riesgo residual en varios procesos institucionales.

g) MONITOREO A LA GESTIÓN DEL RIESGO OPERACIONAL

En el marco de la verificación del cumplimiento de los lineamientos señalados en el numeral 7.3.3 Monitoreo del M-RI-03; se solicitó al Grupo Gestión de Riesgos el soporte de los informes de monitoreo y socialización ante las instancias correspondientes; corroborando que el monitoreo se consolida en el marco del informe trimestral sobre aspectos relevantes del SIAR (numeral *Gestión del Riesgo Operacional del SIAR)* que ahora se presenta de manera trimestral:

Tabla No.13 Instancias de monitoreo SARO

Documento	Instancia socialización	No. Sesión	Fecha sesión	Soportes
Informe Aspectos relevantes SIAR I trimestre 2026	Comité Interno de Riesgos (CIR)	76	28/04/2026	Acta y Presentación Power Point
Informe Aspectos relevantes SIAR II trimestre 2026	Comité Interno de Riesgos (CIR)	79	27/07/2026	Acta y Presentación Power Point

Fuente: Elaboración ACI a partir de información reportada por el Grupo Gestión de Riesgos.

No obstante, se recomienda al Grupo Gestión de Riesgos ajustar el M-RI-03 actualizando la periodicidad del monitoreo (ahora trimestral). Así mismo, solicitar la publicación del informe del II trimestre, ya que, al 11 de septiembre no se encuentra en el Catálogo de Gestión Documental/Intranet de la Sociedad.

1.4 PLAN DE CONTINUIDAD DEL NEGOCIO (PCN)

Dentro de la evaluación que se efectuó a este apartado, se abordaron los siguientes aspectos:

a. Manual Plan de Continuidad del Negocio
b. Actividades del Plan de Continuidad
c. Plan de Prevención y Atención de Emergencias
d. Plan de Financiamiento ante Contingencia de Liquidez
e. Medición y control de Riesgos PCN
f. Gestión de eventos de riesgo materializados PCN

A continuación, se describe su desarrollo:

a. MANUAL PLAN DE CONTINUIDAD DE NEGOCIO:

En el numeral 8.4 PLAN DE CONTINUIDAD DEL NEGOCIO – PCN del Manual del Sistema Integral de Administración De Riesgos (SIAR) versión 04 del 2025 de la Sociedad, se registra la declaración general de la gestión de riesgos de continuidad y la implementación de esta mediante el Manual de Continuidad del Negocio (M-RI-05) versión del 2025.

Así entonces, revisado el documento M-RI-05 el cual registra la metodología para la gestión de esta tipología de riesgo; inicialmente se identifica que en su marco normativo aún se mantiene la Norma AS/NZS 4360:2004 que fue sustituida por la ISO 31000:2009 y posterior revisión ISO 31000:2018, lo cual representa un desfase normativo importante en el entendido que el Capítulo XXXI de la Circular Básica Contable y Financiera de la SFC exige que los sistemas de administración de riesgos (SIAR) adopten metodologías técnicas estandarizadas, actualizadas y con criterios internacionales vigentes.

Situación que fue identificada en el seguimiento Parte No.1 emitido durante el I semestre de la vigencia en curso por esta Oficina. Si bien, se remitió un borrador de la versión n°7 del Manual que se encuentra en etapa de gestión de aprobación por la Junta Directiva (previamente revisada por el Comité Interno de Riesgos en sesión No.79 del 27 de julio del 2026), aún persiste la norma citada registrada en el documento. Por tanto, se recomienda ajustar el documento eliminando la norma citada que se encuentra actualmente derogada.

b. ACTIVIDADES DEL PLAN DE CONTINUIDAD DEL NEGOCIO (CICLO PHVA):

Etapa Planear:

- **Perfil de Riesgos de Continuidad de Negocio (10.1.2):**

Conforme a la periodicidad anual requerida en el numeral 10.1.2 Actualización del Perfil de Riesgos de Continuidad, se identificó cumplimiento con la formalización de la actualización del Perfil de Riesgos SIAR 2026 (versión 18° - Operacional, Soborno, Fraude y Corrupción) y la consolidación de la matriz con corte a junio de 2026. Como resultado de este ejercicio, los riesgos asociados a la Continuidad del Negocio (PCN) disminuyeron, pasando de 15 a 8 riesgos de continuidad.

- **Actividades del PCN (10.1.3):**

En cumplimiento de lo descrito en el numeral 10.1.3 Planificación de las Actividades del Año del Manual M-RI-05 y las 3 actividades contenidas en el numeral 6.1 Elaboración y Aprobación del Programa Anual de Pruebas del procedimiento P-RI-17 Pruebas al Plan de Continuidad del Negocio, se identificó cumplimiento con la aprobación del Cronograma del PCN por el Comité Institucional de Gestión y Desempeño – Sesión Ordinaria No. 01 del 22 de enero del 2026, previa revisión técnica de la Coordinación de Gestión de riesgos el 15 de enero.

Teniendo en cuenta que en el informe de seguimiento Parte 1 emitido por esta Oficina, se identificó que el cronograma no contemplaba la inclusión de la actividad de *"Verificación de los requerimientos y ANS de los componentes de la estrategia de continuidad"*, señalada en el manual de continuidad del negocio M-RI-05 numeral 10.1.3 Planificación de las Actividades del Año; el Grupo Gestión de Riesgos en su informe de Aspectos relevantes del SIAR I trimestre 2026 señaló:

> *"Medida parcial adoptada: Se realizará mesa de trabajo para analizar la recomendación y aplicabilidad con el proceso de gestión de proveedores y gestión de TI."*

No obstante, en la información suministrada para la consolidación de este informe no se evidenciaron soportes que acrediten la realización de la mesa de trabajo destinada a analizar la inclusión de la actividad citada. Así mismo, y dado que la exigencia corresponde a una disposición de carácter interno, los procesos responsables deben asegurar su implementación e inclusión durante la vigencia en curso.

Por otra parte, y de acuerdo con lo informado para la vigencia 2026 se identificaron variaciones, modificaciones y/o rediseños en las actividades formuladas para 3 de sus 4 componentes respecto de la vigencia 2025 derivado del Análisis de Impacto de Negocio-BIA de la vigencia 2025. No obstante, no se aportó evidencia documental para contrastar los siguientes cambios mencionados en el cronograma frente a la vigencia anterior:

- **Pruebas de Continuidad de aplicativos:** ajuste frecuencia de simulacros a los aplicativos críticos de 4 a 6 jornadas anuales.
- **Capacitación de personal mínimo vital:** Inclusión de módulos de "Gestión del Cambio" ante actualizaciones o reestructuraciones de los roles críticos de la entidad.
- **Simulacro de sede alterna:** implementación del modelo hibrido para conectividad del personal crítico hacia el entorno Cloud.

Etapa hacer:

- **Ejecución del PCN (10.2.1):**

Teniendo en cuenta que el Cronograma del PCN 2026 incluye las pruebas, simulacros y validaciones, junto con sus responsables, periodicidad y ventanas de ejecución; en los informes trimestrales presentados en el marco de las sesiones del Comité Interno de Riesgos del 28 de abril y 27 de julio (No.76 y No.79), las actividades se distribuyeron de la siguiente manera:

Tabla No.14 Distribución Actividades PNC por trimestre

Actividad Principal	Primer Trimestre	Segundo Trimestre
A. Ejecución Del Plan De Continuidad Del Negocio	6	6
B. Mantenimiento Y Fortalecimiento De La Estrategia De Continuidad	0	1
C. Monitoreo Al Plan De Continuidad Del Negocio	2	4
D. Plan De Sensibilización Y Capacitación	1	3
E. Plan De Pruebas, Simulacros Y Validaciones	3	5
Total general	**12**	**19**

Fuente: Elaborado ACI a partir Informes de Aspectos relevantes del SIAR I y II trimestre 2026

De igual forma, se informó que para julio se contaban con 14 actividades programadas, de las cuales 2 presentaron desviaciones; pero para las cuales no se logró verificar su ejecución debido a la falta de soportes suministrados por parte del Grupo Gestión de Riesgos:

- Actividad Retraso en el Simulacro Técnico de Aplicativos Críticos (Sesión 3), debido a ventana de mantenimiento imprevisto por parte del proveedor de la infraestructura de nube.

  Plan de Acción: Reprogramación prioritaria para la primera semana de agosto, coordinando el despliegue fuera de horario laboral para no impactar la operación diaria.

- Actividad Actualización rezagada del Directorio de Personal Mínimo Vital, debido a novedades de personal y desvinculaciones reportadas de forma tardía por el área de Talento Humano.

  Plan de Acción: Automatización del cruce de bases de datos mediante un script mensual entre TI y Riesgos, logrando la subsanación total de la información.

  El seguimiento a las desviaciones citadas fue presentado ante el Comité Interno de Riesgos, sesión ordinaria del 19 de agosto del 2026.

Observación No.15 Resultados ejecución del cronograma PCN

Criterio: lo señalado en el Manual de Continuidad del Negocio (M-RI-05) versión 6 del 2025:

> *"Una vez aprobado el cronograma de actividades, esta se debe realizar en el tiempo establecido, además deben cumplir con los requerimientos de calidad, completitud, eficiencia y participación necesarios para darse como finalizada la actividad.*

Como prueba de la realización de las actividades, se deben guardar las evidencias correspondientes, teniendo siempre como base los formatos establecidos en el Sistema de Gestión de Calidad para el Plan de Continuidad del Negocio. Estas evidencias se deben entregar al Oficial de Continuidad del Negocio en formato Digital, quien será el encargado de realizar el monitoreo a la ejecución de las actividades y presentará al Comité Institucional de Gestión y Desempeño – CIGD los resultados.

Si previo a la finalización del plazo de ejecución de una actividad no ha podido ser ejecutada, se debe presentar el requerimiento de aplazamiento en la siguiente sesión del Comité Institucional de Gestión y Desempeño - CIGD, explicando los motivos por los cuales se ha retrasado la ejecución de la actividad y proponiendo una nueva fecha de ejecución. Una vez aprobada la modificación por el CIGD, se deben realizar los cambios en el cronograma de actividades del PCN y se debe dar a conocer a todos los participantes del PCN."

Situación evidenciada: Si bien, el Grupo Gestión de riesgos reportó que el cronograma del PCN cuenta con porcentaje de cumplimiento a julio del 85.7%; no se logró corroborar el porcentaje señalado, debido a que: 1) no se remitió el cronograma formulado para el 2026; 2) para el 68% (21) de actividades no se aportaron soportes; 3) para el 22% (7) de las actividades los soportes presentados se encuentran incompletos y; 4) solo el 10% (3) de las actividades cuentan con soportes completos que soportan la ejecución de las actividades programadas.

Por consiguiente, lo anterior incumple los criterios del M-RI-05 señalados anteriormente en materia de consolidación documental de las evidencias que soportan el cumplimiento de las actividades registradas en el cronograma.

A continuación, se presenta el comportamiento general de las actividades por cada categoría del cronograma (A, B, C, D y E), consolidando lo reportado en los informes trimestrales a julio del 2026 y los soportes aportados:

A. Ejecución Del Plan De Continuidad Del Negocio

A corte 31 de julio, para esta categoría se registró la ejecución de las 12 actividades programadas asociadas a la inscripción de brigadistas, actualización de los listados de colaboradores por piso, revisión equipos de prevención y atención de emergencias, y las rutas de evacuación, verificación y modelo diligenciado del formato de Evaluación de daños a la infraestructura física y tecnológica, actualización del Árbol de llamadas, consolidación del Inventario y Verificación de Aplicaciones y Servicios de TI Críticos Instaladas en el Centro de Cómputo Alterno.

Así entonces:

- 8 de las actividades se realizaron dentro de las fechas programadas:

-. A.1.1 Inscripción de Brigadistas (Edificio ENTerritorio S.A y otras sedes) – **Correo electrónico del 07/04/2026 de convocatoria a ser parte de la brigada de emergencia y documento Excel "LISTADO BRIGADISTAS 2026"**
-. A.1.2 Actualizar el listado de colaboradores por piso (Edificio ENTerritorio y otras sedes) – **Documento Excel "Listado colaboradores planta Enterritorio 2026"; no obstante, no se identifica si este es el documento actualizado.**

-. A.1.3 Revisión equipos de prevención y atención de emergencias (Edificio ENTerritorio S.A y otras sedes) marzo y mayo– **sin soporte de ejecución.**
-. A.1.9 Actualizar Árbol de Llamadas (marzo y junio) – **sin soporte de ejecución.**
-. A.2.1 Inventario y Verificación de Aplicaciones y Servicios de TI Críticos Instaladas en el Centro de Cómputo Alterno (2 veces-trimestral) – **sin soporte de ejecución.**

- 2 actividades presentaron retraso debido que al primer trimestre no presentó ejecución (A.1.4 Revisión rutas de evacuación, marzo y mayo); ya que, el Plan de Emergencias y los Planes Operativos Normalizados PON se encontraba en actualización por parte de la ARL Positiva – **Documento rotulado "Informe Seguridad y Salud en el Trabajo" con el cual se informó el retraso en la ejecución de la actividad; sin fecha de emisión)**
- Para 1 actividad no se pudo verificar su ejecución, teniendo en cuenta que no fue incluida en el informe del I trimestre (A.1.7 Verificación y modelo diligenciado del formato de Evaluación de daños a la infraestructura física) – **sin soporte de ejecución.**
- 1 actividad fue ejecutada posterior a la fecha programada en el cronograma; teniendo en cuenta que debía ejecutarse al 31 de marzo y se realizó el 07 de abril (A.1.8 Verificación y modelo diligenciado formato de Evaluación de daños a la infraestructura tecnológica) – **sin soporte de ejecución.**

B. Mantenimiento Y Fortalecimiento De La Estrategia De Continuidad

Se registró que durante el II trimestre se realizó mesa de trabajo con el equipo de Tecnologías de la Información y el Operador Tecnológico (22/04/2026), con el fin de consolidar el Análisis Punto Únicos de Falla; el cual incluye toda la infraestructura tecnológica de la Sociedad (Sistemas de información, aplicativos, herramientas online, etc.); **para la cual no se aportó soporte de ejecución.**

C. Monitoreo Al Plan De Continuidad Del Negocio

Para el monitoreo al PCN se observa que se programaron 6 actividades a corte julio del 2026; de las cuales 5 se realizaron dentro de las fechas programadas. Respecto de la actividad relacionada con el seguimiento a los planes de acción cuya periodicidad se estableció de manera trimestral, solo se identificó reporte y avance para el II trimestre:

- C.1.1 Monitoreo al PCN – **sin soporte de ejecución**
- C.1.2 Seguimiento Planes de Acción – **sin soporte de ejecución**
- C.2.1 Seguimiento al cronograma de mantenimiento del edificio ENTerritorio S.A. (Depende del plan anual de mantenimiento del Edificio - PLANTAS ELECTRICAS, BOMBAS Y EYECTOR, SUBESTACIONES ELECTRICAS, ALARMAS Y CITOFONOS, ASCENSORES Y EXTINTORES) – **sin soporte de ejecución**
- C.2.2 Mantenimiento al sistema eléctrico pisos de ENTerritorio S.A. – **sin soporte de ejecución.**
- C.2.4 Mantenimiento infraestructura física interna de los pisos de ENTerritorio S.A (2 veces-trimestral) – **sin soporte de ejecución.**

D. PLAN DE CAPACITACIÓN (Sensibilización y formación)

Se identificó la programación de 4 actividades de capacitación y/o sensibilizaciones enfocadas en atención a emergencias por parte del equipo de emergencias y los colaboradores y capacitación en pista de entrenamiento para la brigada; las cuales fueron realizadas en mayo y junio de la vigencia en curso. Respecto de la capacitación a la brigada en normatividad y responsabilidades vigentes, a julio no se

identificó su ejecución. Aunque al I trimestre se reportó que se debió al cambio de la ARL, no se evidencian soportes de reprogramación de la actividad:

- D.1.2 Charla PCN y Atención a Emergencias - Brigadistas y Equipo de Atención a Emergencias – **sin soporte de ejecución.**
- D.1.3 Sensibilización PCN y Atención a Emergencias - Colaboradores – **sin soporte de ejecución.**
- D.2.5 Capacitación a Brigadas - Normatividad y Responsabilidades – **Documento rotulado "Informe Seguridad y Salud en el Trabajo" con el cual se informó el retraso en la ejecución de la actividad; sin fecha de emisión)**
- D.2.6 Capacitación a Brigadas - Pista de Entrenamiento – **sin soporte de ejecución.**

E. PLAN DE PRUEBAS (Validación y simulacros)

En los informes de seguimiento, se identificó que las 8 actividades programadas estuvieron enfocadas en la realización de pruebas a accesos remotos (CCA), restauración de bases de datos y aplicativos, comparación de versiones entre el CCP y el CCA, pruebas de recorridos en aplicativos y el simulacro de activación PCN (Prueba de escritorio con el ECMC). Así entonces, para cada una de las pruebas se identificó:

- En la prueba anual de Accesos Remotos en Operación Normal (E.1.1) realizada el 25 de marzo, se validó el funcionamiento de las conexiones remotas en operación normal de la VPN y los aplicativos GRC, ServiPro 4, Métrica 5 y nómina que maneja la empresa; sin identificación de hallazgos por lo que se identificó 100% de efectividad – **soportes captura de pantalla de reunión, grabación de las pruebas e informes de resultados.**
- En la prueba de recorrido (E.1.2) realizada el 15 de junio a los aplicativos lira, nómina y tiquetes se identificaron inconsistencias con estos 2 últimos, por lo cual el 26 de junio se realizaron nuevamente validaciones para identificar que los errores identificados fueran subsanados efectivamente y no afectaran la continuidad de las actividades. Respecto del aplicativa lira, su validación se programó para el mes de julio – **Documento "F-RI-13_PRUEBA DE RECORRIDO" diligenciado con las pruebas realizadas al 05/06/2026 y Grabación reunión preparación prueba de recorrido.**
- Para la prueba y validación de conexiones mediante Accesos Remotos – CCA (E.1.4) realizada el 15 de junio, se tuvo en cuenta los aplicativos ServiPro, Métrica pro 5, GRC, lira, nómina y tiquetes; sin identificación de inconsistencias o novedades – **Grabación de la sesión.**
- (E.2.3) El simulacro de activación PCN (Prueba de escritorio con el ECMC) se realizó el 21 de mayo, enfocada a permitir la apertura en el Centro de Computo Alterno - CCA para realizar las verificaciones de ingreso y operación en caso de una contingencia materializada; sin novedades durante la ejecución, lo cual evidencia la implementación de estrategias preventivas frente a la mitigación de riesgos ante una emergencia – **traza correos del 21/05/2026 con la ejecución del simulacro, soporte captura de pantalla de la sesión del simulacro e informe de resultados del simulacro.**
- En la validación y comparación de versiones CCP Vs CCA (E.3.1- 2 veces-trimestral) los cuales incluyen todos los componentes del sistema, incluyendo front-end, repositorios y bases de datos no se identificaron diferencias entre ambas infraestructuras, lo que confirma la capacidad para garantizar la continuidad operativa y la integridad de los datos replicados – **Traza correos electrónicos del 21/05/2026 con el cual se informa inicio de la prueba "Santo y seña".**

- Se han realizado 8 pruebas en el marco de la validación de restauración bases de datos y aplicativos (E.3.2- 2 veces-trimestral), en las cuales no se reportaron novedades que pudieran afectar el acceso a la información – **sin soporte de ejecución.**

  De acuerdo con lo anterior, se reitera que las pruebas de continuidad se limitaron exclusivamente a los aplicativos críticos identificados (GRC, ERP, Nómina, SevimPro4, IGMétrica 5, LIRA y Tiquetes). En consecuencia, aplicaciones como Catálogo Documental, Discoverer, FVS, GEOTEC y ORFEO quedaron sin cobertura, lo que incrementa la exposición a fallas o indisponibilidad ante eventuales escenarios de contingencia.

Finalmente, y teniendo en cuenta que posteriormente los resultados obtenidos del seguimiento fueron documentados en el Informe de aspectos relevantes del Sistema Integral de Administración de Riesgos (SIAR) I y II trimestre de 2026, y socializados en el marco de las sesiones del Comité Interno de Riesgos No.76 y No.79 (28 de abril y 27 de julio; respectivamente); la ausencia de sustento documental les resta objetividad, veracidad e integridad a los resultados presentados ante esta instancia.

Recomendación: Se recomienda al Oficial de Continuidad del Negocio implementar estrategias y/o un mecanismo riguroso de archivo y trazabilidad que garantice el soporte documental completo de cada actividad ejecutada por parte de los procesos responsables.

- **Plan de pruebas (10.2.2):**

En cumplimiento de lo descrito en el numeral 10.1.3 Planificación de las Actividades del Año y el numeral 10.2.2 del Manual M-RI-05 y a partir de la revisión documental, el plan fue aprobado por el Comité Institucional de Gestión y Desempeño – Sesión Ordinaria No. 01 del 22 de enero del 2026 (Acta CIGD-01-2026); y posterior socializado a las partes interesadas de los procesos críticos y al personal mínimo vital mediante sesiones virtual (Plataforma TEAMS) del 12 de febrero.

Observación No.16 Resultados Ejecución del Plan de pruebas

Criterio: lo señalado en:

a. El procedimiento Pruebas al Plan de Continuidad del Negocio P-RI-17 versión 05 del 2024, contenido integral.

b. Los numerales 15.2.2.1 Preparación de las Pruebas, 15.2.2.2 Ejecución de las Pruebas y 15.2.2.3 Cierre de las Pruebas, del Manual de Continuidad del Negocio (M-RI-05) versión 6 del 2025:

   "15.2.2.1 Preparación de las Pruebas
   La fase de preparación tiene como objetivo definir la estrategia anual de pruebas relacionada con el Plan de Continuidad del Negocio que aplicará la Sociedad. Adicionalmente, dentro de la fase de preparación, para cada prueba se define el tipo de pruebas a ejecutar, los recursos requeridos para ejecutar las pruebas, el diseño de las actividades que se probarán y la fecha de ejecución de estas. (…)

   15.2.2.2 Ejecución de las Pruebas
   Durante esta fase se deben realizar las siguientes actividades:

• Asegurar el diligenciamiento de los formatos diseñados para documentar la prueba, registrando el desarrollo de todas las actividades ejecutadas (tanto las que se consideraron en el diseño de la prueba como las que no).
• Asegurar la documentación de las tareas ejecutadas por parte de los participantes encargados de las actividades.
• Registrar las observaciones y situaciones anormales que se presenten durante la ejecución de las pruebas.
• Gestionar las firmas requeridas en los formatos de pruebas y las listas de chequeo.

15.2.2.3 Cierre de las Pruebas
Durante esta fase se deben realizar las siguientes actividades:
• Consolidar la información generada durante el proceso de pruebas por parte de los participantes.
• Finalizar y formalizar los formatos de documentación de las pruebas.
• Ejecutar una reunión con los participantes en las pruebas, posterior a la
(…)"

Situación evidenciada: Según lo reportado por el Grupo Gestión de riesgos, de acuerdo con el cronograma y la planeación anual, el estado general del plan de pruebas presenta un 80% de cumplimiento de las actividades. No obstante, y teniendo en cuenta lo registrado en la Observación No.15 Resultados ejecución del cronograma PCN, numeral E. PLAN DE PRUEBAS (Validación y simulacros), se identificaron debilidades con la documentación de los soportes de ejecución para el 100% de las actividades, en especial las ejecutadas con periodicidad mensual o trimestral lo que no permite una trazabilidad continua de su desarrollo.

Así mismo, se evidencia una debilidad estratégica en la cobertura del plan, toda vez que las pruebas operativas y de contingencia se limitaron a un grupo reducido de aplicativos, excluyendo sistemas esenciales para la operación como Catálogo Documental, Discoverer, FVS, GEOTEC y ORFEO; lo cual incrementa el riesgo de indisponibilidad operativa ante la materialización de un evento de interrupción.

Recomendación: se recomienda al Oficial de Continuidad del Negocio implementar estrategias para garantizar el soporte documental completo de cada actividad ejecutada por parte de los procesos responsables. Así mismo, coordinar con el proceso responsable la viabilidad de revisar y ampliar el alcance del Plan de Pruebas de Continuidad para incluir la totalidad de los sistemas e infraestructura crítica de la entidad (Catálogo Documental, Discoverer, FVS, GEOTEC y ORFEO), garantizando así una evaluación integral de la resiliencia operativa y una oportuna rendición de cuentas ante el Comité Interno de Riesgos.

- **Análisis de Impacto Al Negocio – BIA (Business Impact Analysis) – (10.2.4)**

El Manual M-RI-05 establece que el BIA es el insumo principal para la consolidación del PCN y su actualización debe surtirse una vez al año; así entonces, y con el fin de identificar el cumplimiento de lo señalado; se solicitó al Grupo Gestión de Riesgos el soporte documental de la actividad citada. No obstante, reportaron que la actualización se encuentra en proceso de planeación y estructuración (socialización metodología para diligenciamiento del formato F-RI-09 Actualización del BIA)

Así entonces, la verificación de la actividad citada se realizará en la próxima evaluación.

Etapa Verificar:

- **Monitoreo al Plan de Continuidad del Negocio (10.3.2)**

En cumplimiento de lo señalado en el numeral 10.3.2 del M-RI-05, el 7.2.4 Monitoreo del M-RI-08 y 4.3.1.4 del P-RI-13, el Grupo Gestión de Riesgos aporto soporte documental de la socialización de los resultados del monitoreo realizado al PCN durante las siguientes sesiones del Comité de Riesgos:

- Sesión No.76 del 28 de abril, donde se socializó el Informe de aspectos relevantes del Sistema Integral de Administración de Riesgos (SIAR) I trimestre de 2026; indicando el estado del cronograma del PCN (83%) y del Plan de pruebas del PCN (100%)
- Sesión No.79 del 27 de julio, socializando resultados del Informe de Aspectos Relevantes del Sistema Integral de Administración de Riesgos SIAR. II Trimestre 2026; indicando que el cronograma del PCN para el II trimestre se cumplió en un 100%.

No obstante, y teniendo en cuenta las observaciones No. 15 y 16 la ausencia de sustento documental les resta objetividad, veracidad e integridad a los resultados presentados ante esta instancia.

Observación No17. Monitoreo al Plan de Continuidad de Negocio – Indicador

Criterio: lo señalado en el numeral 8.1.1 Políticas Generales del Manual de Continuidad del Negocio (M-RI-05) versión 06 del 2025: "*Se debe realizar la valoración de la eficacia del Plan de Continuidad del Negocio de acuerdo con el indicador "Gestión del Plan de Continuidad del Negocio" del Sistema de Gestión de Calidad*"

Situación observada: teniendo en cuenta que la Sociedad dispone del indicador *"Gestión del Plan de Continuidad del Negocio"*; se solicitó al Grupo Gestión de Riesgos el seguimiento realizado al indicador a corte julio del 2026 con sus soportes correspondientes. En la respuesta cargada en la Carpeta OneDrive compartida *"SIAR Parte 2"* se informó *"Al cierre del mes de julio, el indicador consolidado presenta un desempeño del 85.7%, ubicándose dentro del Rango Aceptable (Zona Amarilla) de la entidad, afectado principalmente por las dos desviaciones operativas previamente reportadas en el cronograma físico: (…)"*

No obstante, y teniendo en cuenta que no se aportó el informe de seguimiento ni los soportes correspondientes, no se logró verificar el cálculo del resultado del indicador y el análisis correspondiente al mismo. Esta situación se articula con lo evidenciado en la *Observación No.15 (Resultados ejecución del cronograma PCN)*, donde la omisión en la remisión del cronograma base y la incompleta sustentación probatoria de las actividades ejecutadas impiden corroborar la veracidad del avance físico reportado. En consecuencia, la falta de soportes de las variables del indicador contraviene lo dispuesto en el numeral 8.1.1 del *Manual de Continuidad del Negocio (M-RI-05)* respecto a la evaluación objetiva de la eficacia del PCN, restándole integridad a la información sobre la gestión de la Sociedad.

Recomendación: se recomienda al Grupo Gestión de Riesgos implementar controles de archivo y trazabilidad que garanticen que las evaluaciones de eficacia del PCN presentadas ante el Comité Interno de Riesgos se encuentren sustentadas en evidencias objetivas y verificables, dando estricto cumplimiento al numeral 8.1.1 del *Manual M-RI-05*.

c. PLAN DE PREVENCIÓN Y ATENCIÓN DE EMERGENCIAS

Con el fin de corroborar el cumplimiento de las actividades formuladas para el Plan de la vigencia 2026 (aprobado en el Comité Institucional de Gestión y Desempeño-Sesión Ordinaria No. 01 del 22 de enero del 2026), se solicitó al Grupo Gestión de Riesgos el plan con los soportes de ejecución. No obstante, se registra la siguiente situación:

Observación No.18 Resultado Ejecución del Plan de Prevención y Atención de Emergencias

Criterio: lo señalado en el numeral 10. Planes de Acción Ante Emergencias del Plan de Prevención y Atención de Emergencias L-TH-01 versión 06 del 2024: *"Los planes de acción relacionan las actividades principales que se deben desarrollar en caso de emergencia, estos se componen de Objetivos, Responsables, Actividades a desarrollar antes, durante y después del evento."*

Situación evidenciada: Según lo informado por el Grupo de Gestión de Riesgos, el Plan de Emergencias registra un avance general del 92 % con corte a julio; no obstante, no se logró corroborar el porcentaje señalado, debido a que no se remitió el plan con las actividades formuladas para el 2026 ni los soportes que documentan la ejecución de las siguientes actividades reportadas y la socialización ante el Comité Interno de Riesgos sesión de agosto:

- **Inspección de equipos de emergencia (Finalizado):** Ejecución mensual de revisiones al 100 % de los extintores, botiquines y sistemas de alarma en todas las sedes de la entidad.
- **Conformación y dotación de la brigada (Finalizado):** Actualización del listado de miembros activos de la brigada y entrega formal de la dotación técnica de protección.
- **Simulacro de evacuación parcial (Finalizado):** Realización satisfactoria del ejercicio de escritorio y de la evacuación en nodos críticos durante mayo de 2026.
- **Simulacro Distrital / Nacional de Evacuación (Planificado):** Programado para el 5 de octubre (segundo semestre de 2026), encontrándose actualmente en fase de coordinación logística externa.

Así entonces, ante la ausencia del plan de actividades formulado para la presente vigencia y la falta de evidencias o soportes documentales que acrediten la ejecución de actividades clave, generan incertidumbre sobre la ejecución real de las actividades del plan; encaminadas a preparar las respuestas de la Sociedad frente a eventuales emergencias.

Recomendación: Se recomienda la consolidación de un repositorio de evidencias y soportes documentales completos que respalden el cumplimiento de cada acción (actas de inspección de equipos, registros de entrega de dotación a brigadistas y memorias informativas de los simulacros). Así mismo, se debe asegurar que los reportes de avance presentados periódicamente ante el Comité Interno de Riesgos cuenten con el debido sustento probatorio que garantice la idoneidad y veracidad de la información reflejada.

d. PLAN DE FINANCIAMIENTO ANTE CONTINGENCIA DE LIQUIDEZ

De acuerdo con lo corroborado, el cronograma de actividades del plan para la vigencia 2026 (aprobado en el Comité Institucional de Gestión y Desempeño-Sesión Ordinaria No. 01 del 22 de enero del 2026) asociadas a la mitigación del riesgo de liquidez registra un avance del 100 % frente a las metas planificadas a la fecha de corte, sin que se hayan identificado desviaciones operativas:

- **Pruebas de estrés de flujo de caja (*Stress Testing*) (Finalizado):** Concluidas de manera satisfactoria en junio de 2026, y las cuales permitieron proyectar escenarios críticos de indisponibilidad operativa de ingresos, confirmando que no se compromete el capital de trabajo mínimo requerido.
- **Monitoreo de indicadores de alerta temprana (*EWIs*) (En ejecución / Al día):** Realizado con periodicidad mensual hasta julio de 2026, manteniendo la totalidad de las variables financieras en rangos de normalidad (Zona Verde).
- **Validación de cupos y líneas de crédito contingentes (Finalizado):** Ejecutada en mayo de 2026 mediante la verificación y actualización formal de vigencias ante las entidades financieras.

  Los resultados fueron presentados en el marco del Comité Interno de Riesgos, sesión del 19 de agosto del 2026.

  De acuerdo con lo anterior, se concluye que la gestión del Plan evidencia un nivel de cumplimiento satisfactorio. Dicha gestión demuestra la efectividad de las medidas preventivas adoptadas por la Sociedad para garantizar la solidez financiera y la resiliencia liquida en el marco del SIAR.

e. MEDICIÓN Y CONTROL DE RIESGOS PCN

Revisada la matriz de riesgos aprobada para la vigencia 2026 que se encuentra publicada en el Sistema Integrado de Gestión-Intranet de la Sociedad, se corroboró que al I trimestre, en materia del PCN se mantuvieron los 15 riesgos y 93 controles (en total 182 asociados teniendo en cuenta que varios le aplican a más de un riesgo), reportados para la vigencia anterior.

Así mismo, para optimizar la carga operativa del Plan de Continuidad se identifica que el diseño del control es de manera transversal, es decir, el 44% (41 de 93 controles) cuenta con una cobertura múltiple que mitiga aproximadamente dos riesgos simultáneamente; lo cual genera una alta eficiencia en la mitigación sin duplicar esfuerzos. En donde el 72% son de tipología preventiva, evidenciando que la estrategia de control se concentra en el origen de las amenazas. Al actuar directamente sobre las causas, el sistema opera bajo un enfoque de prevención temprana, garantizando un Plan de Continuidad que minimiza la exposición antes de que se afecte la operación; consolidando la primera barrera de seguridad que se establece para reducir el riesgo.

De otra parte, al corte julio del 2026 se evidenció ajuste a la matriz de riesgos identificando que para el Plan de Continuidad de Negocio disminuyeron de 15 a 8, así:

Tabla No.15 Actualización de Riesgos Plan de Continuidad del Negocio al II trimestre

PROCESO	RIESGO POR PILAR	CÓDIGO RIESGO	NOMBRE RIESGO	ZONA DE RIESGO INHERENTE	No Controles	ZONA DE RIESGO RESIDUAL	ESTADO
Gestión Administrativa	Gestión Riesgo Operacional - PCN - Gestión Riesgo Liquidez	ROPEAD-1	Daño parcial o total de los bienes muebles e inmuebles de la Sociedad	CONSIDERABLE	9	BAJO	**SE ELIMINA**

PROCESO	RIESGO POR PILAR	CÓDIGO RIESGO	NOMBRE RIESGO	ZONA DE RIESGO INHERENTE	No Controles	ZONA DE RIESGO RESIDUAL	ESTADO
		ROPEAD-6	Ocurrencia de eventos de origen ambiental	MODERADO	7	BAJO	**SE ELIMINA**
Gestión Integral de Procesos	Gestión Riesgo Operacional - Seguridad de la información - PCN	ROPESI-1	Incumplimiento de los requisitos y resultados del Sistema Integrado de Gestión (SIG)	MODERADO	25	MODERADO	SE MANTIENE Se ajusta nombre del riesgo Los controles varían de 10 a 25
	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Antisoborno - Gestión de Riesgo de Integridad Pública	ROPESI-3	Aceptar o solicitar sobornos, comisiones o dadivas para la manipulación de la información del Sistema Integrado de Gestión	CONSIDERABLE	14	MODERADO	SE MANTIENE Se ajusta riesgo por pilar Se ajusta nombre del riesgo Los controles varían de 14 a 13
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez - Gestión Riesgo Mercado	ROPERI-2	Omisión, inoportunidad o inconsistencias en la generación o transmisión de los reportes obligatorios de Gestión de Riesgos o respuestas a solicitudes de información	CONSIDERABLE	22	CONSIDERABLE	SE MANTIENE Se ajusta nombre del riesgo Los controles varían de 19 a 22
	Gestión Riesgo Operacional - Gestión Riesgo Mercado - PCN	ROPERI-3	Generación de informes inexactos de medición y seguimiento de utilización y disponibilidad de cupos	CONSIDERABLE	10	BAJO	**SE ELIMINA**
	Gestión Riesgo Operacional - Seguridad de la información - PCN	ROPERI-24	Pérdida de integridad, confidencialidad y disponibilidad de la información la plataforma tecnológica	MODERADO	25	MODERADO	SE MANTIENE

PROCESO	RIESGO POR PILAR	CÓDIGO RIESGO	NOMBRE RIESGO	ZONA DE RIESGO INHERENTE	No Controles	ZONA DE RIESGO RESIDUAL	ESTADO
Gestión del Talento Humano	Gestión Riesgo Operacional - Gestión Riesgo Liquidez - PCN - Gestión de Riesgo de Integridad Pública	ROPETH-1	Demoras, inconsistencias, incumplimientos u omisiones en las directrices y normativas aplicables al pago de nómina de la sociedad.	MODERADO	18	BAJO	SE MANTIENE Se ajusta Riesgo por pilar Se ajusta nombre del riesgo Los controles varían de 3 a 18
	Gestión Riesgo Operacional - PCN - Gestión Riesgo Liquidez - Gestión Riesgos Ambientales y Sociales	ROPETH-12	Lesiones, muerte o afectaciones de salud de colaboradores o visitantes dentro de las instalaciones de la Empresa	CONSIDERABLE	11	MODERADO	SE MANTIENE Se ajusta Riesgo por pilar Se ajusta nombre del riesgo Los controles varían de 6 a 11
	Gestión Riesgo Operacional - PCN - Gestión Riesgo Liquidez	ROPETH-13	Posibles afectaciones de salud	MODERADO	7	BAJO	**SE ELIMINA**
	Gestión Riesgo Operacional - PCN - Gestión Riesgo Liquidez	ROPETH-19	Incumplimiento en la cuota de vinculación de aprendices SENA, indisponibilidad y alta rotación del recurso humano	MODERADO	8	MODERADO	SE MANTIENE Se ajusta Riesgo por pilar Se ajusta nombre del riesgo Los controles varían de 4 a 8
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez	ROPETI-1	Falta de integridad, confidencialidad y disponibilidad de los aplicativos, portales, sistemas de información, Core del negocio, plataforma tecnológica o servicios en la nube	CONSIDERABLE	43	BAJO	SE MANTIENE Se ajusta nombre del riesgo Los controles varían de 26 a 43

PROCESO	RIESGO POR PILAR	CÓDIGO RIESGO	NOMBRE RIESGO	ZONA DE RIESGO INHERENTE	No Controles	ZONA DE RIESGO RESIDUAL	ESTADO
		ROPETI-5	Indisponibilidad total o parcial de la plataforma tecnológica de la Sociedad	CONSIDERABLE	26	MODERADO	**SE ELIMINA**
		ROPETI-9	Daño o malfuncionamiento del hardware o software	CONSIDERABLE	9	MODERADO	**SE ELIMINA**
	Gestión Riesgo Operacional - PCN	ROPETI-7	Indisponibilidad o deficiencias en las funcionalidades de los aplicativos	MODERADO	7	MODERADO	**SE ELIMINA**

Fuente: elaboración ACI a partir de la matriz de riesgos SIAR vigencia 2026 (Riesgo por Pilar que contiene PCN)

Donde, de los soportes entregados por el Grupo de Gestión de Riesgos, las modificaciones se realizaron en el marco de la actualización del perfil de riesgo para la vigencia 2026, con el fin de contar con una matriz que refleje la realidad de los procesos que integran el PCN. No obstante, se identificaron las siguientes debilidades en los cambios realizados:

Gestión Administrativa: el riesgo ROPEAD-1 contemplaba eventos catástrofe como daños por alteración del fluido eléctrico, falta de mantenimiento de planta física, desastres naturales, orden público, terrorismo e incumplimientos de seguridad física. Al trasvasarlo a ROPEAD-2 (*"Ofrecer, prometer, entregar, aceptar o solicitar dadivas para permitir o facilitar la pérdida, sustracción, daño o destrucción de bienes o activos sin cumplir con las condiciones contractuales pactadas"*). Esta unificación resulta técnicamente incorrecta e inviable, ya que, un desastre natural (terremoto, inundación) o un fallo en el fluido eléctrico no tienen ninguna relación causal con estipulaciones contractuales ni con el ofrecimiento o aceptación de sobornos; y pretender mitigar eventos naturales o fallas de infraestructura física bajo un riesgo de soborno/corrupción debilita la gestión de riesgos de continuidad.

Gestión de las Tecnologías de la Información: la eliminación de 3 riesgos especializados (ROPETI-5, 7 y 9) para unificarlos exclusivamente en el riesgo *ROPETI-1 Falta de integridad, confidencialidad y disponibilidad de los aplicativos, portales, sistemas de información, Core del negocio, plataforma tecnológica o servicios en la nube*; debilita la especificidad de los monitoreos realizados a la subutilización de software, fallas de hardware, licencias no autorizadas, hurto de equipos, operaciones no autorizadas y fugas de información por soborno.

De otra parte, si bien se logró mitigar o consolidar los riesgos del Plan de Continuidad de 15 a 8 (una reducción del 46%), el inventario de controles aumentó de 93 a 105. Esto demuestra que los 8 riesgos remanentes son de naturaleza más compleja o crítica, exigiendo un marco de control más robusto, especializado y diversificado para garantizar la continuidad de la Sociedad; donde el 77% son controles preventivos y el 22,9% se complementan con Detectivos y correctivos (13 y 11; respectivamente)

f. GESTIÓN DE EVENTOS DE RIESGO MATERIALIZADOS PCN

Con el fin de verificar si dentro del periodo de seguimiento se reportaron eventos de riesgo materializados relacionado con el Plan de Continuidad del Negocio, se solicitó al Grupo de Gestión de Riesgos la base consolidada; identificando lo siguiente:

- 8 reportes de evento materializados para los riesgos identificados ROPERI-2 y ROPERI-24 asociados a los Pilares de “Gestión Riesgo Operacional - Seguridad de la información -PCN - Gestión Riesgo Liquidez - Gestión Riesgo Mercado” y “Gestión Riesgo Operacional - Seguridad de la información -PCN”.

- Si bien se registraron 8 reportes, en el mes de junio la situación presentada con la herramienta Moodle de la Sociedad repercutió en la materialización de 6 riesgos: ROPERI-2, ROPERI-1, ROPERI-8, ROPERI-10, ROPERI-24, ROPERI-26; para un total de 13 riesgos materializados.

  -. Riesgos del PCN: 2

  - ROPERI-2: 8 veces
  - ROPERI-24: 1 vez

  -. Riesgos asociados a otros pilares: 4

  - ROPERI-1: 1 vez
  - ROPERI-8: 1 vez
  - ROPERI-10: 1 vez
  - ROPERI-26: 1 vez

- 7 de los 9 eventos fueron identificados en el proceso de Pagaduría y los 2 restantes por el Oficial de Cumplimiento de la Sociedad.

- 7 de los 9 eventos, fueron reportados por el proceso Gestión del Riesgo y 2 en conjunto con el proceso de SARLAFT.

- Para los 9 eventos registrados, se implementó plan de acción oportuno por el proceso responsable con el fin de contrarrestar el impacto en la continuidad del negocio.

- Teniendo en cuenta que los 9 eventos registrados fueron clasificados en la categoría B de Tipo de perdida (No generan pérdidas y por lo tanto no afectan el estado de resultados de la Entidad), no resultó en un impacto económico y/o financiero que generen pérdidas para la Sociedad.

- 7 de los 9 eventos registrados se relacionan con inconsistencias durante la transmisión del Informe 55 (Reporte Diario de Riesgo Operacional) a la Superfinanciera debido a información pendiente y/o errores en la plataforma de cargue del ente de control; mientras que los 2 restantes se relacionan con fallas en la herramienta Moodle para cruce de información de acceso a los cursos de SARLAFT y Antisoborno de la Sociedad.

Observación No.19 Oportunidad en el Reporte de riesgos PCN:

Criterio: De acuerdo con lo señalado en:

El Manual del Sistema Integral de Administración de Riesgos- SIAR (M-RI-08) versión 04 del 2025, 6.2.10 Gestores De Riesgo, numeral 6. "*Reportar de manera inmediata, una vez identificado los eventos o situaciones que afecten los objetivos de la Sociedad"*

La Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03) versión 8 del 2023, numeral 2. Responsabilidades Generales, titulo Responsabilidades de los Gestores de riesgo, punto No.1 "*Reportar de manera inmediata, una vez identificado los eventos de riesgos operacional que le informan los colaboradores de su proceso."*

Situación observada: Una vez cuantificados los riesgos materializados reportados a corte julio del 2026, se procedió a verificar si el reporte por parte de los procesos responsables en el aplicativo CGR fue oportuno. Para lo cual, se contrastó la fecha del registro en el aplicativo contra la fecha del descubrimiento del evento; en donde:

Tabla No.16 Criterios Valoración Oportunidad reportes PCN

Fecha registro = Fecha descubrimiento o máximo 24 horas después del evento	OPORTUNO
Fecha registro > Fecha descubrimiento	INOPORTUNO

Fuente: elaboración ACI.

El 100% (8) de los reportes de eventos ocurridos entre febrero y julio fueron realizados de manera **inoportuna**; es decir, entre 7 días o 1 mes después del descubrimiento de la materialización de los 2 riesgos (ROPERI-2 y ROPERI-24).

La socialización del resultado del seguimiento a la materialización de riesgos se realizó en el marco de la presentación de los informes sobre Aspectos Relevantes del Sistema Integral de Administración de Riesgos SIAR del I y II trimestre (sesiones del Comité Interno de Riesgos No.76 y No.79 del 28 de abril y 27 de julio; respectivamente).

De otra parte, la atención de incidentes (como las fallas en la transmisión del VaR a la SFC y los registros de Moodle) se apoya en reprocesos manuales y gestión por demanda, sin contar con protocolos de contingencia automáticos ni parametrizaciones sólidas.

Recomendación: se recomienda al Grupo de Gestión de Riesgos analizar la viabilidad de adoptar como parámetro de cumplimiento, el umbral de reporte dentro de las 24 horas siguientes al descubrimiento del evento e incluirlo como lineamiento interno en la Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03); para posterior divulgar y capacitar a los colabores de la Sociedad, principalmente a los Gestores de Riesgos sobre la importancia estratégica del reporte oportuno para favorecer una toma de decisiones más efectiva, la retroalimentación continua del SIAR/PCN y el fortalecimiento del sistema de control interno.

1.5 SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para la evaluación de este sistema de administración de riesgos (en adelante, referido como SARM), el alcance de las pruebas se enfocó en los siguientes aspectos:

a) Medición y control Riesgos de Seguridad de la Información-SI
b) Monitoreo a la Gestión de Riesgos de Seguridad de la Información
c) Activos de Información- actualización
d) Logs de Auditoría
e) Gestión de eventos de riesgo materializados en Seguridad de la Información
f) Monitoreo al Plan de tratamiento de riesgos SI
g) Gestión de eventos de seguridad de la información

Los resultados obtenidos se exponen a continuación:

a) MEDICIÓN Y CONTROL DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN-SI

Con el fin de identificar si la matriz de riesgos para la vigencia 2026 sufrió cambios respecto de la identificación de riesgos de seguridad de la información, se verificó la matriz de riesgos a corte I trimestre y la propuesta con ajuste en el mes de junio (en función de la actualización del perfil de riesgos); identificando los siguiente:

Al I trimestre, se corroboró el no registro de cambios en los riesgos respecto de la vigencia anterior; registrando 53 riesgos que incluyen el pilar de seguridad de la información para 13 procesos y con 412 controles formulados, así:

Tabla No.17 Distribución Riesgos de Seguridad de la Información por proceso

Proceso	Riesgo por pilar	Código riesgo	Confidencialidad (C)- Integridad (I) - Disponibilidad (D)	Zona de Riesgo Inherente	No Controles	Zona de Riesgo Residual
Auditoría Interna	Gestión Riesgo Operacional - Seguridad de la información	ROPEAU-5	I	MODERADO	7	MODERADO
Auditoría Interna	Gestión Riesgo Operacional - Seguridad de la información	ROPEAU-7	I	MODERADO	7	BAJO
Auditoría Interna	Gestión Riesgo Operacional - Seguridad de la información	ROPEAU-10	I	MODERADO	4	BAJO
Gestión de las Comunicaciones	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPECO-3	C	MODERADO	3	BAJO
Relacionamiento con el Ciudadano	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPERC-3	C	MODERADO	6	BAJO
Relacionamiento con el Ciudadano	Gestión Riesgo Operacional - Seguridad de la información	ROPERC-5	I	CONSIDERABLE	10	MODERADO
Relacionamiento con el Ciudadano	Gestión Riesgo Operacional - Seguridad de la información	ROPERC-6	I	CONSIDERABLE	7	BAJO
Gestión Integral de Procesos	Gestión Riesgo Operacional - Seguridad de la información - PCN	ROPESI-1	ID	MODERADO	10	MODERADO

Proceso	Riesgo por pilar	Código riesgo	Confidencialidad (C)- Integridad (I) - Disponibilidad (D)	Zona de Riesgo Inherente	No Controles	Zona de Riesgo Residual
Gestión Integral de Procesos	Gestión Riesgo Operacional - Seguridad de la información - PCN	ROPESI-3	ID	CONSIDERABLE	14	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información -PCN - Gestión Riesgo Liquidez - Gestión Riesgo Mercado	ROPERI-2	ID	CONSIDERABLE	19	CONSIDERABLE
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información Gestión Riesgo Liquidez - Gestión Riesgo Mercado	ROPERI-11	CID	CONSIDERABLE	8	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información Gestión Riesgo Liquidez - Gestión Riesgo Mercado	ROPERI-16	CID	MODERADO	4	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-18	CID	MODERADO	14	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-19	CI	MODERADO	4	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-20	CI	MODERADO	5	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPERI-21	CID	MODERADO	4	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPERI-22	CID	MODERADO	5	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-23	CID	BAJO	3	BAJO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información -PCN	ROPERI-24	CID	MODERADO	25	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-25	CID	MODERADO	3	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPERI-26	CID	MODERADO	3	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-27	CID	MODERADO	3	MODERADO
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-28	CID	MODERADO	4	BAJO

Proceso	Riesgo por pilar	Código riesgo	Confidencialidad (C)- Integridad (I) - Disponibilidad (D)	Zona de Riesgo Inherente	No Controles	Zona de Riesgo Residual
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez - Gestión Riesgo Mercado	ROPERI-29	CI	CONSIDERABLE	7	BAJO
Gestión de Proveedores	Gestión Riesgo Operacional - Seguridad de la información	ROPEPR-13	I	MODERADO	4	MODERADO
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información	ROPETH-6	ID	MODERADO	9	BAJO
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETH-24	C	MODERADO	4	BAJO
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETH-28	ID	CONSIDERABLE	7	MODERADO
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información	ROPETH-31	CD	MODERADO	3	BAJO
Gerencia y Gestión de Proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEGG-20	CID	MODERADO	7	MODERADO
Gerencia y Gestión de Proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEGG-38	CID	MODERADO	5	MODERADO
Evaluación de Proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEEV-4	CID	MODERADO	6	MODERADO
Evaluación de Proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEEV-22	CID	MODERADO	4	MODERADO
Evaluación de Proyectos	Gestión Riesgo Operacional - Seguridad de la Información	ROPEEV-33	CID	MODERADO	3	MODERADO
Estructuración de proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEEP-12	CID	MODERADO	5	BAJO
Estructuración de proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEEP-16	No aplica	MODERADO	2	MODERADO
Estructuración de proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEES-26	I	MODERADO	7	BAJO
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPEFI-30	CID	CONSIDERABLE	4	MODERADO
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-34	CID	CONSIDERABLE	4	MODERADO

Proceso	Riesgo por pilar	Código riesgo	Confidencialidad (C)- Integridad (I) - Disponibilidad (D)	Zona de Riesgo Inherente	No Controles	Zona de Riesgo Residual
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-39	I	CONSIDERABLE	5	MODERADO
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-40	I	MODERADO	2	MODERADO
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-41	No aplica	MODERADO	1	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -PCN - Gestión Riesgo Liquidez	ROPETI-1	I	CONSIDERABLE	26	BAJO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPETI-2	I	CONSIDERABLE	8	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPETI-3	D	CONSIDERABLE	13	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez	ROPETI-5	CID	CONSIDERABLE	26	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-8	CI	MODERADO	4	BAJO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez	ROPETI-9	CID	CONSIDERABLE	9	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-10	CID	CONSIDERABLE	7	MODERADO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-11	CID	MODERADO	8	BAJO
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPETI-13	CID	CONSIDERABLE	29	MODERADO
Gestión Documental	Gestión Riesgo Operacional - Seguridad de la Información -Gestión Riesgo Liquidez	ROPEDO-5	C	MODERADO	10	MODERADO
Gestión Documental	Gestión Riesgo Operacional - Seguridad de la Información	ROPEDO-8	I	CONSIDERABLE	11	BAJO

Fuente: Elaborado ACI a partir de Matriz Riesgo SIAR (Riesgo por Pilar que contiene SGSI)

De los 412 controles registrados, se identificó que el 84% (345 controles) cuenta con una cobertura que mitiga dos o más riesgos simultáneamente sin duplicar esfuerzos; y, por consiguiente, son 137 en total; de los cuales el 73% son de tipología preventiva. Lo anterior evidencia que se mantiene en tendencia el enfoque de prevención temprana, enfocada en evitar incidentes de seguridad desde su origen y reducir costos que impliquen su mitigación; evidenciando la gestión proactiva del riesgo en el marco del SIAR. No obstante, es importante validar que este porcentaje de controles no genere rigidez operativa ni descuide la capacidad de detección y respuesta ante eventos no previstos.

Finalmente, y respecto de la verificación a que los controles se encuentren alineados con la declaración de aplicabilidad, según anexo A de la ISO 27001:2022; se identificó que el 59% (82 controles) la mantiene.

Recomendación: revisar y ajustar el catálogo de controles de seguridad de la información con el objetivo de elevar la alineación actual (59 %) con la declaración de Aplicabilidad del Anexo A de la ISO 27001:2022, asegurando que los 156 controles consolidados cuenten con un mapeo directo frente a los estándares internacionales de seguridad.

**

Respecto de la matriz propuesta para el II trimestre del 2026 derivada de la actualización del perfil de riesgos, se identificó:

-. Eliminación de 26 riesgos, para los cuales se identificaron las siguientes debilidades:

- Fusionar la protección de datos sensibles o simplemente derogar el riesgo contractual (ROPEGG-38) expone a la Entidad a investigaciones de la Superintendencia de Industria y Comercio (SIC). La Ley 1581 del 2012 exige que el cumplimiento de deberes de terceros tenga controles e indicadores de seguimiento independientes por parte de las entidaes.
- La eliminación de 7 riesgos especializados (ROPETI-2, 5, 8, 9, 10, 11 y 13) para unificarlos exclusivamente en el riesgo *ROPETI-1 Falta de integridad, confidencialidad y disponibilidad de los aplicativos, portales, sistemas de información, Core del negocio, plataforma tecnológica o servicios en la nube*; debilita la especificidad de los monitoreos realizados a la subutilización de software, fallas de hardware, licencias no autorizadas, hurto de equipos, operaciones no autorizadas y fugas de información por soborno.
- La eliminación de los riesgos ROPEFI-34 (*"Información financiera adulterada"*) y el ROPEFI-39 (*"Ofrecer, prometer, entregar, aceptar o solicitar dádivas para presentar o transmitir informes/reportes con información inconsistente, inválida o inoportuna"*) para trasladar sus causas a ROPEFI-30 (*Ofrecer, prometer, entregar, aceptar o solicitar dadivas para facilitar, manipular o cometer hurto, robo, malversación o apropiación en la gestión financiera)*; no es viable, en el entendido de que fusionar eventos intencionados de alteración maliciosa de cifras y delitos de soborno/corrupción (dolo), se confunden con las fallas humanas o del sistema contable. Esto impide que el Oficial de Cumplimiento o el área de Gestión del Riesgo midan de manera independiente el riesgo de Fraude en Informes Financieros, contraviniendo las directrices de la SFC sobre transparencia contable.
- La eliminación del riesgo ROPETH-31 (*"Pérdida de expedientes disciplinarios"*) y asociación de sus causas al riesgo ROPETH-24 (*"Filtración, pérdida o inconsistencias de la información personal de las hojas de vida de los funcionarios, historias laborales y expedientes*

disciplinarios"); contraviene la normatividad vigente en materia de reserva legal (Código Disciplinario Único - Ley 1952 de 2019) y su pérdida o extravío acarrea consecuencias de responsabilidad penal, disciplinaria e invalidez de actuaciones procesales de la Sociedad. Encasillar el extravío de un expediente disciplinario reservado como una simple inconsistencia de información administrativa de personal resta la gravedad jurídica al evento e invisibiliza las medidas de control físico y de custodia que exige la Ley para los procesos disciplinarios en el sector público.

Tabla No.18 Riesgos Seguridad de la información eliminados al II trimestre

Proceso	Riesgo por pilar	Código riesgo
Auditoría Interna	Gestión Riesgo Operacional - Seguridad de la información	ROPEAU-5 y ROPEAU-7
Relacionamiento con el Ciudadano	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPERC-3
Relacionamiento con el Ciudadano	Gestión Riesgo Operacional - Seguridad de la información	ROPERC-6
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPERI-21
Gestión de Riesgos	Gestión Riesgo Operacional - Seguridad de la información	ROPERI-23, ROPERI-25, ROPERI-27 y ROPERI-28
Gestión de Proveedores	Gestión Riesgo Operacional - Seguridad de la información	ROPEPR-13
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información	ROPETH-6 y ROPETH-31
Gestión del Talento Humano	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETH-28
Gerencia y Gestión de Proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEGG-38
Evaluación de Proyectos	Gestión Riesgo Operacional - Seguridad de la Información	ROPEEV-33
Estructuración de proyectos	Gestión Riesgo Operacional - Seguridad de la información	ROPEES-26
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-34
Gestión Financiera	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPEFI-39
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPETI-2
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez	ROPETI-5
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-8
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - PCN - Gestión Riesgo Liquidez	ROPETI-9
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-10
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información - Gestión Riesgo Liquidez	ROPETI-11
Gestión de las Tecnologías de la Información	Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez	ROPETI-13
Gestión Documental	Gestión Riesgo Operacional - Seguridad de la Información -Gestión Riesgo Liquidez	ROPEDO-5

Fuente: Elaborado ACI a partir de Matriz Riesgo SIAR (Riesgo por Pilar que contiene SGSI)

-. Para el II trimestre, se identificó que el perfil de controles de Seguridad de la Información disminuyó de 412 a 405, donde el 78,3% del total de controles (317 de 405) opera de manera transversal mitigando aproximadamente dos riesgos simultáneamente (y, por ende, son 156 en total). Así mismo, la arquitectura de control presenta una madurez orientada a la prevención (72%), complementada con un 28% de controles de detección y corrección (25 y 19; respectivamente), lo cual garantiza una estrategia defensiva en profundidad adecuada para la protección de los activos de información de la Sociedad.

b) MONITOREO A LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN-SI

En el marco de la verificación del cumplimiento de los lineamientos señalados en el numeral 7.2.4 del M-RI-08; se solicitó al Grupo Gestión de Riesgos el soporte de los informes de monitoreo y socialización ante las instancias correspondientes; identificando cumplimiento, toda vez que el monitoreo se consolida en el marco del informe trimestral sobre aspectos relevantes del SIAR (numeral *Seguimiento al Sistema de Gestión de Seguridad de la Información)* que ahora se presenta de manera trimestral:

Tabla No.19 Instancias de monitoreo SI

Documento	Instancia socialización	No. Sesión	Fecha sesión	Soportes
Informe Aspectos relevantes SIAR I trimestre 2026	Comité Interno de Riesgos (CIR)	76	28/04/2026	Acta y Presentación Power Point
Informe Aspectos relevantes SIAR II trimestre 2026	Comité Interno de Riesgos (CIR)	79	27/07/2026	Acta y Presentación Power Point

Fuente: Elaboración ACI a partir de información reportada por el Grupo Gestión de Riesgos.

No obstante, se recomienda al Grupo Gestión de Riesgos la publicación del informe de seguimiento del II trimestre en el repositorio del Catálogo de Gestión Documental/Intranet; ya que al 11 de septiembre no se identifica su publicación.

c) ACTIVOS DE INFORMACIÓN - ACTUALIZACIÓN

-. De conformidad con lo reportado por el Grupo Gestión de Riesgos, la actualización de la matriz de riesgos de información se realizará durante el II semestre en coordinación los 17 procesos de la sociedad; no obstante, a corte julio del 2026 se remitieron mediante correos electrónicos del 14 de mayo, 12 de junio y 10 de julio piezas infográficas relacionadas con el concepto de activos de información, metodología para su identificación, roles y responsabilidades, entre otros aspectos relevantes para su gestión dentro de la sociedad.

Por tanto, la verificación de la actualización de los activos de información se verificará en el marco de la próxima evaluación.

d) LOGS DE AUDITORÍA

Observación No.20 Aplicación Logs de Auditoría

Criterio: lo señalado en los siguientes numerales del Manual de Políticas de Seguridad de la Información (M-RI-06) versión 07 del 2026:

7.13 Control de Acceso, numeral h. *"El Grupo de Gestión de las Tecnologías de la Información debe habilitar el almacenamiento y garantizar los respaldos (Logs) de la información relacionada con usuarios y privilegios (…)"*

7.31 Protección de registros: *El Grupo de Gestión de las Tecnologías de la Información es responsable de garantizar el respaldo de la información de registros contables, registros de base de datos, registros de transacciones (logs), registros de auditoría (audit logs) y procedimientos operacionales y demás registros de control que existan en cada sistema de información, detallando los tiempos de retención, el tipo de medio de almacenamiento, la forma de conservación y el responsable.*

10.14 Registro de eventos
10.15 Actividades de registro
(…)
•Activar los logs de auditoría en los sistemas operativos, aplicativos, bases de datos, equipos activos de red, dispositivos de seguridad y servidores, con el fin de registrar las actividades de los usuarios de estos recursos y la infraestructura tecnológica de la Empresa.
• Los logs de eventos deben registrar también las fallas e indisponibilidades de la infraestructura tecnológica y/o sistemas de información.
• El Grupo de Gestión de las Tecnologías de la Información debe implementar un estándar de creación y gestión de logs de eventos en el que se especifique para los diferentes recursos de la plataforma tecnológica como mínimo: el tipo de eventos y usuarios a auditar, periodicidad del registro, tiempos de retención de los logs y usuarios habilitados para realizar auditoría.
(…)
Los administradores de las aplicaciones que operan en la Empresa deben habilitar y generar logs de auditoría en la periodicidad establecida."

Situación observada: de los soportes remitidos por el Grupo Gestión de Riesgos y consolidados por el Grupo de Gestión de Tecnologías y de la Información, se describe controles de acceso centralizados (AD) y custodia restringida del repositorio, pero no se aportó evidencia técnica específica de los mecanismos anti-alteración de los logs ya almacenados (inmutabilidad, integridad/hashing) ni el listado de perfiles de AD con acceso al repositorio NFS; por lo cual la verificación se basó principalmente en la declaración del responsable del proceso y en capturas de pantalla generales del SIEM, sin soporte documental adicional (política o matriz de roles de acceso) que permita una verificación plenamente independiente.

Así mismo, se reporta que la periodicidad de ejecución de logs de auditoría a las bases de datos es de manera quincenal, sin remitir documento formal que documente explícitamente la periodicidad citada; lo mismo que la política/procedimiento de retención de logs (independiente de la configuración técnica del SIEM) que sustente y formalice el periodo de conservación de 6 meses reportado.

Sin perjuicio de lo anterior, se evidenció que el operador tecnológico ejecuta y documenta monitoreo quincenal efectivo sobre las 6 bases de datos (SIIF -ORFEO -IGCART -METAREP -SDGEA y ENTBDAPP): en los 14 cortes quincenales del periodo se identificaron, analizaron y gestionaron oportunamente eventos relevantes a partir de la revisión de los logs, entre ellos fallas de Dataguard en sitio alterno en SIIF_RAC, ORFEO_RAC e IGCART_RAC (enero y febrero), error de archivelog en SDGEA (enero-febrero), parchados de servidor (feb, may, jun-jul) y el bloqueo de la aplicación SEVINPRO en IGCART el 12 de junio (con reinicio de base de datos y depuración de la secuencia bloqueada).

Cada observación derivó en una acción correctiva documentada en el mismo informe, no obstante, no se recibió evidencia de un mecanismo formal (tickets, alertas o actas) adicional al propio informe narrativo del operador tecnológico que permita trazar de manera independiente la revisión de logs como una actividad de seguridad diferenciada del monitoreo general de desempeño/disponibilidad de las bases de datos.

La respuesta de TI remite además al repositorio compartido "SGSI 2026" como fuente de los informes de revisión y monitoreo.

Recomendación: se recomienda al Grupo de Gestión de las Tecnologías de la Información formalizar y documentar el procedimiento estandarizado para la gestión y retención de logs de auditoría en concordancia con los numerales 7.13, 7.31, 10.14 y 10.15 del *Manual M-RI-06*, oficializando mediante acto o documento normativo la periodicidad quincenal de revisión y la política de conservación de seis meses. Así mismo, se deben implementar y aportar evidencias técnicas que garanticen la inmutabilidad e integridad de los registros almacenados (mecanismos de *hashing* y matriz de roles de Active Directory para el acceso al repositorio NFS), e instrumentar un mecanismo formal de trazabilidad independiente (como registros tickets, alertas automáticas o actas técnicas) que permita auditar la revisión periódica de logs de manera diferenciada de la gestión rutinaria de disponibilidad de la infraestructura.

e) GESTIÓN DE EVENTOS DE RIESGO MATERIALIZADOS EN SEGURIDAD DE LA INFORMACIÓN

Con el fin de verificar si dentro del periodo de seguimiento se reportaron eventos de riesgo materializados en Seguridad de la Información, se solicitó al Grupo de Gestión de Riesgos la base consolidada; identificando lo siguiente:

- 3 de los 6 riesgos materializados que fueron registrados en 8 reportes por parte del proceso de Gestión de Riesgos, se asoció con la seguridad de la información (ROPERI-26, Pilar Gestión Riesgo Operacional - Seguridad de la información -Gestión Riesgo Liquidez)

- Se implementó plan de acción oportuno por el proceso responsable con el fin de contrarrestar el impacto de las inconsistencias presentadas con la base de datos que integra la herramienta Moodle de la Sociedad y el reporte ante la Superfinanciera.

- Teniendo en cuenta que los eventos registrados fueron clasificados en la categoría B de Tipo de perdida (No generan pérdidas y por lo tanto no afectan el estado de resultados de la Entidad), no resultó en un impacto económico y/o financiero que generen pérdidas para la Sociedad.

Observación No.21 Oportunidad en el Reporte de riesgos SI:

Criterio: De acuerdo con lo señalado en:

El Manual del Sistema Integral de Administración de Riesgos- SIAR (M-RI-08) versión 04 del 2025, 6.2.10 Gestores De Riesgo, numeral 6. "*Reportar de manera inmediata, una vez identificado los eventos o situaciones que afecten los objetivos de la Sociedad"*

La Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03) versión 8 del 2023, numeral 2. Responsabilidades Generales, titulo Responsabilidades de los Gestores de riesgo,

punto No.1 "*Reportar de manera inmediata, una vez identificado los eventos de riesgos operacional que le informan los colaboradores de su proceso.*"

Situación observada: Una vez identificado el riesgo en materia de seguridad de la información materializado a corte julio del 2026, se procedió a verificar si el reporte por parte del proceso responsable en el aplicativo CGR fue oportuno. Para lo cual, se contrastó la fecha del registro en el aplicativo contra la fecha del descubrimiento del evento; en donde:

Tabla No.20 Criterios Valoración Oportunidad reportes SI

Fecha registro = Fecha descubrimiento o máximo 24 horas después del evento	OPORTUNO
Fecha registro > Fecha descubrimiento	INOPORTUNO

Fuente: elaboración ACI.

El 100% (8) de los reportes de eventos ocurridos entre febrero y julio fueron realizados de manera **inoportuna**; es decir, entre 7 días o 1 mes después del descubrimiento de la materialización de los 3 riesgos (ROPERI-2, ROPERI-24 y ROPERI-26).

La socialización del resultado del seguimiento a la materialización de riesgos se realizó en el marco de la presentación de los informes sobre Aspectos Relevantes del Sistema Integral de Administración de Riesgos SIAR del I y II trimestre (sesiones del Comité Interno de Riesgos No.76 y No.79 del 28 de abril y 27 de julio; respectivamente).

De otra parte, la atención de incidentes (como las fallas en la transmisión del VaR a la SFC y los registros de Moodle) se apoya en reprocesos manuales y gestión por demanda, sin contar con protocolos de contingencia automáticos ni parametrizaciones sólidas.

Recomendación: se recomienda al Grupo de Gestión de Riesgos analizar la viabilidad de adoptar como parámetro de cumplimiento, el umbral de reporte dentro de las 24 horas siguientes al descubrimiento del evento e incluirlo como lineamiento interno en la Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03); para posterior divulgar y capacitar a los colabores de la Sociedad, principalmente a los Gestores de Riesgos sobre la importancia estratégica del reporte oportuno para favorecer una toma de decisiones más efectiva, la retroalimentación continua del SIAR/SGSI y el fortalecimiento del sistema de control interno.

f) MONITOREO AL PLAN DE TRATAMIENTO DE RIESGOS SI

Observación No.22 Monitoreo al Plan de tratamiento de riesgos SI:

Criterio: De acuerdo con lo señalado en:

El numeral 10.8 Gestión de vulnerabilidades técnicas del Manual de Políticas de Seguridad de la Información (M-RI-06) versión 7 del 2026, punto *d) El Grupo de Gestión de las Tecnologías de la Información debe participar en la definición de los planes de tratamiento para mitigar los riesgos y realizar la remediación de las vulnerabilidades en seguridad informática, identificadas en la infraestructura tecnológica. Así mismo, incluirá la revisión del avance de los mencionados planes dentro de sus actividades de monitoreo al cumplimiento de lineamientos de seguridad de la información"*

El Manual del Sistema Integral de Administración de Riesgos- SIAR (M-RI-08) versión 04 del 2025, numerales 6.2.4 Comité Interno de Riesgos, 6.2.9 Responsables de proceso y sus equipos de trabajo, 7.2.4 Monitoreo:

"*6.2.4 comité Interno de Riesgos*
Revisar, modificar y hacer seguimiento a los planes de acción, manejo o tratamiento de riesgos que se propongan y/o evaluar la eficacia de los controles y de los planes de tratamiento con base en los informes proferidos por el Grupo de Gestión de Riesgos y la Asesoría de Control Interno.

6.2.9 Responsables de proceso y sus equipos de trabajo
7. *Proponer e implementar planes de tratamiento para prevenir o reducir la ocurrencia o consecuencias de los riesgos, gestionar la ejecución de las actividades y realizar seguimiento al cumplimiento de estos (…)*

7.2.4 Monitoreo
(…) Cuando se materialicen desviaciones significativas en la operación se deberá formular e implementar planes de tratamiento para mitigarlos."

Situación observada: con el fin de verificar la gestión de los planes de tratamiento de riesgos en materia de Seguridad de la Información vigentes, se solicitó al Grupo Gestión de Riesgos el plan con las evidencias que soportan el avance o ejecución a julio del 2026; identificando que se encuentra vigente el TRATRI2504 asociado al riesgo *"ROPERI-2: Omisión, inoportunidad y/o inconsistencias en la generación y/o transmisión de los reportes obligatorios de riesgos o de respuestas a solicitudes de información";* debido a materialidades en la integridad de la información asociadas a los contratos en la vigencia 2025.

No obstante, a julio del 2026 el plan presenta un nivel de avance crítico; ya que, de las 9 actividades programadas, únicamente 1 registra estado "Cumplida" (11.1%), mientras que las ocho (8) restantes figuran en estado "Abierta" (88.9%). Dado que las fechas de terminación pactadas vencieron entre junio y octubre de 2025, el plan se encuentra en extemporaneidad vencida, lo que afecta el fortalecimiento de los controles sobre el ERP y el módulo SARLAFT.

Así mismo, para verificar el cumplimiento del plan, no se adjuntaron los soportes documentales exigidos en la columna "Soportes para verificación de cumplimiento" (tales como las actas de mesa de trabajo con el proveedor, los correos de aprobación de desarrollos o las certificaciones del despliegue en el ERP). Si bien en el Informe de Aspectos relevantes del SIAR del I trimestre del 2026 se registra que el plan tiene un porcentaje de cumplimiento del 95%, la falta de estos soportes impide verificar la ejecución real o el avance físico de las 9 actividades.

La única evidencia remitida corresponde a la traza de correos del periodo mayo–julio de 2026 sobre la "Validación de integridad ERP-SARLAFT". Lejos de certificar el avance de las actividades del plan, esta traza confirma un retraso operativo y falta de participación por parte de las áreas involucradas:

- Falta de asistencia y comunicación: Con corte al 02/07/2026 y 04/06/2026, se evidencia que la Subgerencia de Operaciones no asistió a las sesiones programadas, no se contactó con el Grupo de TI ni envió la lista de temas para las capacitaciones acordadas.

- Incumplimiento reiterado de compromisos: En los registros del 28/05/2026, 26/05/2026 y 19/05/2026, se reiteran solicitudes y compromisos no atendidos oportunamente por parte de la Subgerencia de Operaciones para la entrega de insumos de capacitación.

Recomendación: es importante que el Grupo de Gestión de Riesgos, en articulación con la Subgerencia de Operaciones y la Gestión de Tecnologías de la Información (TI), den atención prioritaria a este plan estableciendo una mesa de trabajo extraordinaria para identificar el estado real de las 8 actividades abiertas que se encuentran en extemporaneidad vencida desde la vigencia 2025.

g) GESTIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Observación No.23 Gestión de eventos de seguridad de la información

Criterio: lo señalado en el numeral 7.23 Evaluación de eventos de seguridad de la información y decisiones sobre ellos del Manual de Políticas de Seguridad de la Información (M-RI-06) Versión 07 del 2026 *"Con base en el reporte de eventos de seguridad de la información, el Grupo de Gestión de las Tecnologías de la información en conjunto con el Oficial de Seguridad de la Información, monitorea el tipo, volumen e impacto y define si corresponde a un incidente de seguridad de la información. Una vez definido como incidente debe generar un informe con la identificación, evaluación, investigación y plan de tratamiento para la contención del incidente. Los incidentes de seguridad de la información deben ser reportados como eventos de riesgo operativo al grupo de Gestión de Riesgos mediante el diligenciamiento del formato F-RI-06 Registro de eventos de riesgo operativo."*

Situación observada: teniendo en cuenta que en los informes mensuales de gestión (informe SOC), a corte julio del 2026 se registraron 232 eventos de seguridad de la información, los cuales fueron escalados al grupo perimetral para su contención y solución; se desconoce el estado de los 11 tíquets y/o registros que quedaron pendientes de gestión:

Tabla No.21 Detalle gestión eventos de seguridad de la información a julio del 2026

No. Informe	Periodo	Eventos Detectados	Escalados a Perímetro	Estado Final (Cerrados)	Pendientes / En Gestión	Detalle	Incidentes Materializados
1	27/12/2025 - 26/01/2026	69	69	59	**10**	**TK ID: 46312, 46314, 46315, 46317, 46449, 46450, 46507, 46519, 46546, 46562**	No
2	27/01/2026 - 26/02/2026	56	56	56	0		No
3	27/02/2026 - 26/03/2026	28	28	28	0		No
4	27/03/2026 - 26/04/2026	25	25	24	**1**	**TK-1408**	No
5	27/04/2026 - 26/05/2026	27	27	27	0		No
6	27/05/2026 - 26/06/2026	15	15	15	0		No
7	27/06/2026 - 26/07/2026	12	12	12	0		No
	TOTAL	**232**	**232**	**221**	**11**		

Fuente: Elaboración ACI, a partir de los informes de gestión SOC enero a julio del 2026.

De acuerdo con lo anterior, se identificó una inconsistencia de trazabilidad entre informes consecutivos: en el informe de enero (periodo 1) 10 eventos quedaron en estado "Escalado" al cierre del corte, sin que el informe de febrero (periodo 2) retome su seguimiento o confirme el cierre definitivo; situación similar se presentó con el caso TK-1408 del informe de abril (periodo 4), que no se evidencia formalmente cerrado en el informe de mayo.

Así entonces, no se identificó un mecanismo documental de continuidad de casos pendientes entre periodos mensuales, lo que puede afectar la trazabilidad y rendición de cuentas del riesgo en el marco del SIAR/SGSI.

De otra parte, en los informes de enero a marzo de 2026 no incluyen la sección de *"Gestión de Incidentes"* (con indicadores alineados a ISO/IEC 27001:2022) que sí se implementó de manera consistente a partir de abril de 2026. Esta falta de uniformidad en la estructura documental del primer trimestre limita la trazabilidad y comparabilidad del criterio *"cero incidentes materializados"* para todo el periodo evaluado; a pesar de lo reportado por el Grupo TI mediante memorando 202615010002183 del 9/09/2026: *"Frente a la solicitud de "2 informes de análisis forense con cadena de custodia documentada --- conforme a ISO/IEC 27032: 2012", nos permitimos certificar que durante el periodo objeto de evaluación (julio 2025 a julio 2026) no se presentó ni materializó ningún incidente de seguridad de la información de criticidad Moderada, mayor o catastrófica en la plataforma tecnológica de la entidad. El Anexo Técnico No. 2 estipula que este servicio se activará bajo demanda "para los casos en que sea necesario investigar incidentes informáticos". En consecuencia, al registrarse un total de cero (0) eventos críticos, los informes forenses y los registros de cadena de custodia asociados no fueron requeridos ni generados en la operación real. Exigir estos documentos como un entregable obligatorio e histórico resulta improcedente ante la ausencia de eventos que justificaran su ejecución."*; lo anterior, en el marco del seguimiento al cumplimiento contractual Anexo Técnico No. 2 / INA-007-2024 (Contrato No. 2024612) que actualmente adelante la ACI.

Recomendación: se recomienda al proceso de Gestión de Tecnologías de la Información en articulación con el Oficial de Seguridad de la Información, formalizar e implementar la trazabilidad continua y cierre de los eventos de seguridad que al periodo de corte evaluado se registren como “Escalados”; lo mismo que, solicitar al proveedor la homologación retroactiva o la confirmación expresa de dicho indicador de gestión de incidentes para los meses de enero, febrero y marzo de 2026.

CONCLUSIONES

- **Gestión de Riesgo de Liquidez:**

Con base a los resultados analizados del Backtest y Stresstest, se recomienda replantear la metodología que está basada en el componente presupuestal (RP y obligaciones) transicionando hacia componentes de proyectos y su ejecución (hitos / entregables), procurando acompasar la misionalidad de Enterritorio S.A. (Estructuración y Desarrollo de Proyectos) con los movimientos de caja semanales que se pretenden modelar. No se observó la revisión de estos reportes al interior del grupo de riesgos, puesto que el Stresstest tuvo un error que no fue advertido (cálculo de fallas del test de Kupiec)

Así mismo, se detectó que, si bien los modelos se ejecutan en hojas de cálculo de Excel, éstas no cuentan con validaciones, restricciones y bloqueos que impidan la ocurrencia de un riesgo operativo de pérdida o ingreso erróneo de información. Se debe procurar dejar evidencia de las extracciones (oportunidad y

completitud) y verificaciones que aplican otras áreas. Idealmente, tener un protocolo paso a paso permitirá también mitigar el riesgo de concentración de la actividad en un solo contratista, con lo cual, cualquiera podría re-ejecutar las rutinas de los modelos, sin temor a perder su historicidad y trazabilidad.

Se pudo corroborar que el grupo de riesgos aplica la metodología escrita en el manual de gestión de riesgos financieros frente al riesgo de liquidez.

Los órganos competentes para la gestión del riesgo de liquidez sesionaron durante el periodo objeto de análisis con el quorum requerido y haciendo análisis sobre los informes que, por disposición del manual, deben observar.

- **Gestión de Riesgo de Mercado:**

Al igual que con el riesgo de liquidez, en el riesgo de mercado se usan hojas de cálculo para las validaciones de las valoraciones de portafolios de posición propia y de proyectos (adicional a los aplicativos dispuestos para esos efectos), así como del cálculo del Valor en Riesgo. En consecuencia, se recomienda aplicar los mismos controles de acceso, edición e ingreso de data para evitar daños en los modelos. Especial atención merece la vinculación de hojas de cálculo de diferente origen, que pueden llegar a comprometer la funcionalidad, resultados y trazabilidad de los resultados obtenidos.

Por otra parte, Enterritorio S.A. debería procurar parametrizar los límites, alertas y umbrales aprobados por los órganos competentes en los sistemas de información, lo cual otorga mayor confiabilidad que los reportes detectivos diseñados manualmente, dado que se privilegiarían los controles automáticos y se mitigan los riesgos operacionales por el factor humano.

Para las conciliaciones de portafolios de inversión y custodios no se está efectuando el cruce a nivel de registros contables, el cual se aconseja aplicar y asegurar así su razonabilidad y la de la administración de las inversiones. Así mismo, se detectaron 2 especies con inadecuada clasificación, lo cual puede comprometer la exactitud de las valoraciones de las inversiones. No se identificó su reporte como evento de riesgo.

La mayor parte de las transmisiones de VaR regulatorio fueron oportunas, salvo por 3 situaciones (14% de la muestra de 21 ítems seleccionados aleatoriamente), las cuales no se consideran reiterativas, pero que ameritan un control de programación que evite la extemporaneidad en hora de remisión (antes de las 9:00 a.m.).

- **Gestión de Riesgo Operacional:**

No fue posible establecer en qué se basa el avance del 50% en el plan de trabajo de riesgo operacional respecto al componente de indicadores, puesto que durante el ejercicio no se obtuvo fuente de datos que permitiera llegar a dicha conclusión y porque, además, se menciona que en el tercer trimestre de 2026 se adelantarán las pruebas piloto correspondientes.

El riesgo operacional derivado de la inadecuada clasificación e inversiones que se detectó en riesgo de mercado no fue identificado, junto con sus consecuencias (a nivel de registro de valoración).

Durante el periodo evaluado (enero a julio de 2026), la Sociedad evidenció una evolución madura en la gestión del riesgo operacional al actualizar el Perfil de Riesgos para la totalidad de los 17 procesos. Este ejercicio permitió racionalizar la matriz mediante la reducción del 47,7 % de los riesgos (pasando de 264 a 126). Se verificó que dicha disminución no obedeció a una supresión imprevista de controles, sino a la unificación estratégica de causas e impactos transversales y a la mitigación de duplicidades, incrementando la densidad de cobertura por riesgo y conservando una postura de control predominantemente preventiva (70%).

No obstante, dicha reorganización generó vacíos en la cobertura, la trazabilidad documental y el cumplimiento normativo. En la verificación se identificó la eliminación de riesgos misionales sin el adecuado respaldo probatorio, la unificación inadecuada de fallas operativas o de infraestructura física dentro de fichas de soborno y corrupción, y la concentración excesiva de causas en riesgos tecnológicos. Adicionalmente, se debilitó el seguimiento específico a exigencias legales sobre tratamiento de datos personales, prevención del lavado de activos y custodia de expedientes bajo reserva legal, lo que incrementa la vulnerabilidad y exposición regulatoria de la Sociedad ante los entes de vigilancia y control.

Se identificó la materialización de 3 Eventos de Riesgo Operacional (ERO) Tipo A que generaron pérdidas reales y provisiones contables por una cuantía bruta total de $5.046.561.214. Destaca entre estos la materialización de un riesgo jurídico por fallo judicial adverso que requirió un desembolso por $3.635.564.506 (afectando en un 5,67% la liquidez del componente de funcionamiento), lo que evidencia la necesidad de fortalecer los controles preventivos y la valoración de contingencias en los procesos misionales y jurídicos.

Del consolidado de 350 reportes de ERO analizados (correspondientes a 365 materializaciones de riesgo), el 99 % (345 reportes) se efectuó de manera inoportuna en la herramienta GRC, es decir, entre uno y dos meses después de su descubrimiento, e integrando incluso eventos extemporáneos ocurridos en las vigencias 2021, 2024 y 2025. Esta falencia limita la capacidad de respuesta temprana y desvirtúa la oportunidad del monitoreo institucional.

- **Plan de Continuidad del Negocio (PCN)**

El Manual de Continuidad del Negocio (M-RI-05 versión 6) mantiene en su marco normativo la norma AS/NZS 4360:2004 (sustituida por la ISO 31000), lo cual representa una inconsistencia técnica frente a los requerimientos del Capítulo XXXI de la Circular Básica Contable y Financiera de la Superintendencia Financiera de Colombia (SFC), que exige la adopción de metodologías e instrumentos internacionales vigentes.

A pesar de que el Grupo de Gestión de Riesgos reportó un avance del 85,7 % en el cronograma del PCN y del 92 % en el Plan de Emergencias al corte de julio de 2026, no fue posible corroborar la ejecución real de las actividades; dado que no se aportaron los cronogramas oficiales formulados para la vigencia 2026 y a que los soportes de ejecución de actividades (tales como revisiones de equipos de emergencia, mantenimientos físicos/tecnológicos, capacitaciones y árboles de llamadas) se identificaron incompletos o inexistentes.

Las pruebas operativas y los simulacros ejecutados se concentraron de manera restrictiva en 8 aplicativos definidos como críticos (GRC, ERP, Nómina, ServiPro4, IGMétrica 5, LIRA y Tiquetes). Se concluye que sistemas de información para la gestión institucional como Catálogo Documental, Discoverer, FVS, GEOTEC y ORFEO carecieron de cobertura en las validaciones de resiliencia, incrementando la exposición ante eventuales escenarios de contingencia o indisponibilidad tecnológica.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**

El marco de control de Seguridad de la Información fue optimizado mediante la reducción de 53 a 27 riesgos en el perfil institucional y el ajuste del catálogo a 405 controles (156 controles únicos consolidados). La arquitectura refleja un perfil maduro con un 78,3% de controles de aplicación transversal (que mitigan dos o más riesgos en paralelo) y una inclinación proactiva enfocada en la prevención (72%), complementada adecuadamente con controles detectivos (16%) y correctivos (12%).

Si bien se constató que el operador tecnológico ejecuta un monitoreo quincenal efectivo sobre las seis bases de datos institucionales (SIIF, ORFEO, IGCART, METAREP, SDGEA y ENTBDAPP) a través de 14 cortes evaluados (solucionando oportunamente fallas de DataGuard, errores de *archivelog* y eventos de indisponibilidad), la gestión de logs de auditoría presenta debilidades formales e independientes de control. Lo anterior obedece a que la evaluación dependió de reportes narrativos y capturas generales del SIEM, al no aportarse evidencias sobre mecanismos técnicos de inmutabilidad e integridad (*hashing*), el listado de perfiles AD con acceso al repositorio NFS, ni la formalización documental de la periodicidad quincenal y del periodo de retención de seis meses exigidos en los numerales 7.13, 7.31, 10.14 y 10.15 del *Manual M-RI-06*.

Respecto de los 8 eventos de riesgo materializado asociados con la seguridad de la información, se evidenció que su registro en la plataforma GRC fue inoportuno al realizarse entre 7 días o un mes después de su ocurrencia. Adicionalmente, la contención del incidente y las fallas en reportes ante el ente de control continuaron apoyándose en reprocesos manuales y atención por demanda, evidenciando la falta de protocolos de contingencia automatizados en la infraestructura de TI.

RECOMENDACIONES

- Con base a los resultados analizados del Backtest y Stresstest, se insta al grupo de riesgos y posteriormente al Comité Interno de Riesgos y Comité de Riesgos a analizar, fortalecer y aprobar la metodología para la estimación del Máximo Pago Estimado (MPE), en el sentido de transitar hacia un modelo de flujos de caja en riesgo (CFaR), dado que introducir el componente presupuestal como rector del modelo puede generar fuertes distorsiones sobre las conclusiones y pruebas de desempeño y esfuerzo, que pudieran conducir a decisiones erróneas o a inadecuado aseguramiento del riesgo de liquidez.

- En el mismo sentido, se sugiere adoptar esquemas de revisión al interior del grupo de riesgos sobre los resultados de la ejecución de los modelos, para evitar conclusiones erróneas como las del stress test en materia de prueba de fallos de Kupiec para el componente misional, e incluso, la concordancia entre lo indicado en el manual sobre las restricciones de caja y los supuestos utilizados para los escenarios de la modelación.

- Todas las hojas de cálculo que soportan los modelos de riesgos de mercado, liquidez y otros cuantitativo deberían contar con protocolos de manejo, restricciones de acceso, ingreso de información y alertas, de tal suerte que el riesgo de manipulación involuntaria o intencional de la data no se materialice. Así las cosas, se recomienda trabajar junto al grupo de Tecnologías de la Información en el diseño de plantillas y modelos. Así mismo, diseñar acuerdos de niveles de servicio con las áreas en donde hagan las validaciones y suministren la evidencia de ellas, para asegurar razonablemente el uso de bases de datos confiables para correr los modelos.

- Por las funciones que les confiere sus reglamentos de funcionamiento, es ideal que los órganos competentes realicen pronunciamientos sobre lo adecuado de las metodologías empleadas y los modelos, dado que en las actas no se detectaron los análisis correspondientes. Con esto, se logra el cumplimiento de sus funciones según los documentos precitados.

- Se recomienda parametrizar los umbrales y límites aprobados por los órganos competentes para que operen controles automáticos de alertas y restricciones sobre los controles manuales detectivos de corridas de los modelos. Para el efecto, se puede acudir a los recursos que otorgan los contratos de mantenimiento de las plataformas. Posteriormente, se debería procurar aplicar las verificaciones de funcionamiento en ambiente de pruebas pertinentes antes de su entrada a producción.

- Procurar que cualquier desviación o anomalía detectada en la ejecución de los modelos invite a declarar el eventual evento de riesgo, de tal suerte que el asunto no quede de forma absoluta en manos de la potestad del profesional que ejecuta las pruebas.

- Fortalecer la capacitación en materia de diseño de indicadores de gestión de riesgo operacional, y llevar a cabo las mesas de trabajo con el grupo de riesgos que permitan contar con la batería de indicadores que ayuden al monitoreo del desempeño del SARO de la Sociedad. Deberían también validarse los efectos de la entrada en vigor desde junio 2026 de la Circular Externa 004 de 2026 que reemplaza la Circular Externa 100 de 1995.

- Se recomienda a los líderes de proceso que, en articulación con el Grupo de Gestión de Riesgos, revisen la actualización del perfil de riesgos efectuada en junio de 2026, con el fin de verificar que las consolidaciones de riesgos realizadas se encuentren debidamente alineadas con las operaciones reales de la Sociedad y la normatividad vigente aplicable. En dicho ejercicio, se deberá garantizar entre otros que, los eventos de interrupción de infraestructura y tecnología mantengan fichas independientes de las conductas éticas o de soborno, desglosar las categorías tecnológicas en dominios operativos claros y restablecer el seguimiento específico sobre las obligaciones legales y regulatorias asegurando una evaluación objetiva de la mitigación del riesgo institucional.

- Se recomienda al Grupo Gestión de Riesgos la actualización de la *Guía para el diligenciamiento del registro de Eventos de Riesgo Operacional (G-RI-03)*, formalizando como estándar de cumplimiento el reporte en la plataforma GRC dentro de las 24 horas siguientes al descubrimiento del evento. Paralelamente, adelantar jornadas de sensibilización y capacitación dirigidas a los Gestores de Riesgos de cada proceso sobre la relevancia estratégica del reporte oportuno para la toma de decisiones.

- Se insta a los procesos que en acompañamiento técnico del Grupo Gestión de Riesgos, analice la viabilidad de superar la dependencia de controles reactivos o meramente formales ante eventos materializados (tales como prórrogas contractuales, reportes de seguimiento o revalidaciones manuales). Se debe priorizar el rediseño de controles enfocado en la solución de las causas raíz, incorporando la automatización de validaciones operativas previas para evitar la recurrencia de eventos ERO Tipo A.

- Se recomienda monitorear de forma continua el impacto de la consolidación de riesgos efectuada en junio de 2026, dado que un número reducido de riesgos concentra ahora múltiples causas transversales. Así mismo, evaluar la efectividad de los controles clave asociados, toda vez que la falla de un control podría elevar de manera simultánea la zona de riesgo residual en varios procesos institucionales.

- Agilizar la gestión de aprobación ante la Junta Directiva de la versión 07 del Manual, asegurando la eliminación explícita de referencias a normas derogadas (AS/NZS 4360:2004) y garantizando su estricta alineación con los estándares internacionales vigentes (ISO 31000) y las exigencias de la Circular Básica Contable y Financiera (Capítulo XXXI) de la SFC.

- Se recomienda al Oficial de Continuidad del Negocio revisar el repositorio de evidencias de ejecución del cronograma del PCN, con el fin de solicitar a los procesos responsables los soportes faltantes para completitud del 100% de la carpeta digital; la cual asegura el sustento de los porcentajes de avance reportados al Comité Interno de Riesgos.

- Coordinar entre la Oficina de Gestión de Riesgos y el área de Tecnologías de la Información la ampliación del alcance del Plan para la vigencia en curso y futuras; ya que, es indispensable incluir en los ejercicios de simulación y restauración a las aplicaciones Catálogo Documental, Discoverer, FVS, GEOTEC y ORFEO, asegurando la verificación integral de la resiliencia operativa frente a desastres.

- Revisar y ajustar el catálogo de controles de seguridad de la información con el objetivo de elevar la alineación actual (59 %) con la declaración de Aplicabilidad del Anexo A de la ISO 27001:2022, asegurando que los 156 controles consolidados cuenten con un mapeo directo frente a los estándares internacionales de seguridad.

- Cumplir estrictamente con el cronograma del segundo semestre de 2026 para la actualización de la matriz de activos de información en los 17 procesos de la Sociedad, reforzando las campañas de divulgación infográfica con sesiones de trabajo técnico que garanticen la correcta identificación de propietarios, custodia y clasificación de la información confidencial de la Sociedad.

- Documentar e integrar las evidencias de cumplimiento exigidas para las 9 acciones formuladas en el Plan de Tratamiento TRATRI2504 (actas de mesas de trabajo con el proveedor, correos de aprobación de desarrollos y certificaciones de despliegue en el ERP). Lo anterior, a través de los procesos responsables (Subgerencia de Operaciones y Gestión TIC), con el fin de subsanar la condición de extemporaneidad vencida y garantizar el efectivo fortalecimiento de los controles sobre el ERP y el módulo SARLAFT.

- Se recomienda al Grupo de Gestión de las Tecnologías de la Información formalizar y documentar el procedimiento estandarizado para la gestión y retención de logs de auditoría conforme a los lineamientos del Manual M-RI-06, oficializando de forma escrita la periodicidad de ejecución quincenal y la política de conservación de seis meses (cumplimiento documental al control A.5.33 de la Norma ISO/IEC 27001:2022). Así mismo, se deben implementar y evidenciar controles técnicos que garanticen la inmutabilidad e integridad de los logs almacenados (mediante algoritmos de *hashing* y matrices de roles AD para el acceso al repositorio NFS) y establecer un mecanismo formal e independiente de trazabilidad (como registros en sistema de *ticketing* o alertas de seguridad) que permita auditar la revisión de logs de manera diferenciada respecto a la operación de infraestructura.
- Incluir en los informes de gestión del SOC un capítulo o matriz de seguimiento a los tíquets pendientes de periodos anteriores, garantizando la confirmación documental de su estado final (cerrado/abierto) en el reporte del periodo subsecuente. Lo anterior, con el fin de subsanar las rupturas en la secuencia de monitoreo, asegurar el cumplimiento del numeral 7.23 del Manual M-RI-06 y dar estricta aplicación al principio de monitoreo continuo del Sistema Integral de Administración de Riesgos (SIAR).

Atentamente,

ORLANDO CORREA NUÑEZ
Asesor con Funciones de Control Interno

Elaboró:
Manuela Hernández Jaramillo. Contrato No. 20261144 – Auditor ACI
Carlos Eduardo Buitrago Cano, Contrato No. 20261190 – Auditor ACI