

 <b>Supersolidaria</b> 	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

<b>FECHA DE EMISIÓN DEL INFORME</b>	<b>Día:</b> 15	<b>Mes:</b> 12	<b>Año:</b> 2025
-------------------------------------	----------------	----------------	------------------

<b>Dependencia y/o /Proceso</b>	AUDITORÍA AL PLAN DE CONTINUIDAD DEL NEGOCIO – SES 2025 Asesor del Despacho de la Superintendente. Oficina Asesora de Planeación y Sistemas – OAPS
<b>Nombre(s) y cargo:</b>	FREDY ALBERTO MARTÍNEZ SILVA - Asesor del Despacho ANGELICA MARÍA ZAMORA ACOSTA – Jefe de la Oficina Asesora de Planeación y Sistemas – OAPS
<b>Tipo de Auditoria:</b>	1. Cumplimiento; 2. Evaluación y 3. Seguimiento.
<b>Objetivo(s) de la Auditoria:</b>	Verificar y evaluar el nivel de avance y progreso real en la definición, elaboración, documentación e implementación del Plan de Continuidad del Negocio (PCN) de la Superintendencia de la Economía Solidaria, conforme a las disposiciones establecidas en el Documento Técnico del Plan de Continuidad del Negocio del Departamento Administrativo de la Función Pública - DAFP, las Guías 10 y 11 de preparación de las TIC'S para la continuidad del Negocio y Análisis de Impacto de Negocios - BIA del Ministerio de las TIC's y los marcos de referencia internacionales establecidos por la serie ISO 22301 de 2019 e ISO 27001 de 2022.
<b>Alcance de la Auditoría:</b>	<ol style="list-style-type: none"> <li>1. Verificar el estado actual del Plan de Continuidad del Negocio de la Supersolidaria, comprobando su fase actual (Elaboración, Operacionalización, Implementación) con el progreso real del Documento, el plan de trabajo y el avance en el cumplimiento de la acción de mejora asociada al hallazgo de la Contraloría General de la República (código 22 02 002), relacionado con la ausencia de un Plan de Continuidad del Negocio formalizado, cuya implementación ha sido pospuesta desde 2014 y que de acuerdo al compromiso de la Oficina Asesora de Planeación y Sistemas (OAPS) estaría aprobado y formalizado en los primeros meses de la vigencia 2025.</li> <li>2. Revisar y evaluar la documentación fundamental y análisis del impacto que sustentan el Plan de Continuidad del Negocio (PCN), a través de la verificación de que el BIA se haya realizado correctamente, identificando tiempos máximos de interrupción (MTPD) y objetivos de tiempo de recuperación (RTO/RPO) para los procesos identificados como críticos en la entidad.</li> <li>3. Verificar que los roles para la gestión del plan de continuidad del negocio de la SES (Documentación, Aprobación, Activación y Restablecimiento) estén formalmente asignados. Adicionalmente, constatar que el "Comité de Crisis" esté</li> </ol>

<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

	<p>formalmente constituido y que sus miembros conozcan sus responsabilidades de activación.</p> <p><b>4.</b> Verificar si los manuales existentes en materia de gestión de riesgos, emergencias y recuperación tecnológica de la SES, se encuentran formalizados, actualizados y abordan los elementos del Plan de Continuidad del Negocio, con el fin de determinar si estos contribuyen de manera efectiva a una estrategia integral de continuidad ante eventos de emergencia, desastre o contingencia de tipo social, natural, tecnológico, financiero o sanitario.</p>
<b>Criterios de la Auditoría:</b>	<ul style="list-style-type: none"> <li>• Norma ISO 22301:2019</li> <li>• Norma ISO 27001:2022</li> <li>• Est.1.4 SGCN Pro.1 Procedimiento Continuidad: Min Hacienda</li> <li>• Documento Técnico del Plan de Continuidad del Negocio: Función Pública</li> <li>• Guía 10 Min tic: Para la preparación de las Tic para la continuidad del Negocio</li> <li>• Guía 11 Min Tic: Análisis del Impacto</li> <li>• Manual de Prevención, Preparación y Respuesta ante Emergencias de la SES (MA-PLES-004)</li> <li>• Manual para la Gestión de Riesgos de la SES (MA-PLES-008)</li> <li>• Manual de Seguridad y Salud en el Trabajo de la SES (MA-PLES003)</li> <li>• Plan de Recuperación Ante Desastres Tecnológicos DRP-TIC (PLGETI- 002)</li> </ul>

<b>Jefe oficina de Control Interno</b>	<b>Auditor(es)</b>
<b>JORGE HERNANDO PEDRAZA VARGAS</b>	<b>JOHN LEONARDO MARTIN BETANCOURT</b>

## I. COMPROMISO ETICO EN EL EJERCICIO DE LA AUDITORIA INTERNA

- i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de esté.
- ii. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

## II. COMPROMISO DEL AUDITADO

No fue enviada la carta de representación firmada por la jefe o líder del proceso de la unidad auditada, por lo tanto no se declaró la responsabilidad en la oportuna preparación, presentación integral y consistencia de la información que fue entregada en el marco de la auditoría a la unidad de control interno.

<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

### III. METODOLOGÍA

Teniendo en cuenta el objetivo(s) y alcance de la auditoria(s), mencionados anteriormente, se desarrollaron de manera previa y posterior, respectivamente, las siguientes actividades:

- a) Conocimiento del proceso o dependencia.
- b) Diseño del plan de auditoría: Se estableció la programación del plan de trabajo para el desarrollo de la auditoría, de modo que permitiera lograr el objetivo propuesto.
- c) Reunión de apertura: la apertura de la auditoría se realizó a través del aviso de auditoría del 13 de noviembre de 2025, mediante correo electrónico se notificó la apertura de la auditoria y fecha de instalación, adjuntando el formato de Plan de Auditoria de la Unidad Auditable (planificación de la respectiva auditoria), para conocimiento previo.
- d) Obtención y análisis de la información: Fue solicitada la información pertinente a través del Memorando No. 20251300022563 del 18 de noviembre de 2025, relacionada con el objetivo (s) y alcance(s), que fuese relevante, útil, basada en hechos y confiable. Soportada en los respectivos papeles de trabajo.
- e) Análisis y evaluación de la información. La revisión fue basada en factores críticos de éxito, en estrategias y objetivos del aspecto evaluable, en los riesgos altos y extremos, metas y objetivos del proceso, con enfoque hacia la consecución de los alcances de la auditoria.
- f) Informe preliminar e informe definitivo: Socialización del informe preliminar, recepción de comentarios sobre hallazgos y observaciones, previo a la emisión, notificación y publicación del informe definitivo.
- g) Definición y suscripción del plan de mejoramiento. A partir de la notificación del presente informe y con base en los hallazgos de la auditoria, en caso de haberlos, se definirá conjuntamente con la unidad auditada, la definición y suscripción del respectivo plan de mejoramiento.

### IV. DESARROLLO DE AUDITORIA

A continuación, se detalla el resultado de la evaluación realizada por la Oficina de Control Interno, atendiendo al cumplimiento de los criterios de auditoría y en especial las normas señaladas en el Documento Técnico del Plan de Continuidad del Negocio del Departamento Administrativo de la Función Pública - DAFP, las Guías 10 y 11 de preparación de las TIC'S para la continuidad del Negocio y Análisis de Impacto de Negocios - BIA del Ministerio de las TIC's y los marcos de referencia internacionales establecidos por la serie ISO 22301 de 2019 e ISO 27001 de 2022. y demás normativa aplicable.

#### 1. ALCANCE #1.

**Verificar el estado actual del Plan de Continuidad del Negocio de la Supersolidaria, comprobando su fase actual (Elaboración, Operacionalización, Implementación) con el progreso real del Documento, el plan de trabajo y el avance en el cumplimiento de la acción de mejora asociada al hallazgo de la Contraloría General de la República (código 22 02 002).**

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

### 1.1. CONDICIÓN.


Realizada la verificación de las evidencias aportadas por el área auditada para el desarrollo de este alcance (Documento PL\_GETI\_004\_PLAN\_DE\_CONTINUIDAD\_DEL\_NEGOCIO\_V0 de Noviembre de 2025, Archivo Cronograma BCP y Memorando de respuesta 20251200023213) Se evidencia la existencia del documento PL-GETI-004 "Plan de Continuidad del Negocio" Versión 00, elaborado en noviembre de 2025. Este documento establece el marco general, objetivos y alcance.

Sin embargo, al revisar el Cronograma BCP, se reporta un avance del proyecto del 60%. El responsable indica explícitamente en las observaciones del cronograma: "El avance del proyecto de actualización BCP tiene un 60%, solo sujeto a la incorporación de los resultados del BIA y la gestión de riesgos sobre procesos críticos que también estaría en avance al 50%".

Frente a los puntos clave del alcance evaluado, la oficina de control interno encuentra que:

- Estado del Documento:** El documento maestro del PCN se encuentra en **Versión 00 (Borrador)** publicado en la Plataforma de Articulación y Balance de la Operación "PABLO" con fecha de noviembre de 2025. La OAPS confirma que esta versión corresponde a un ejercicio de alineación conceptual y no ha sido sometida a proceso de aprobación por el despacho de la Superintendente ni por Comité Institucional de Gestión y Desempeño, de conformidad con lo establecido en el Documento Técnico del Plan de Continuidad del Negocio del Departamento Administrativo de la Función Pública – DAFP.

#### Versión 00 (Borrador) PCN publicado en PABLO

CÓDIGO	NOMBRE	VERSION	PROCESO	TIPO DE DOCUMENTO	CONSULTA PUBLICA	COPIA CONTROLADA	FLUJO DE REVISIÓN	FLUJO DE APROBACIÓN	REGISTRADO POR	CONSULTAR
PL-GETI-004	PLAN DE CONTINUIDAD DEL NEGOCIO	0	GETI - GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	PL PLANES	Publico	SI	ANGELICA MARIA ZAMORA ACOSTA	ANGELICA MARIA ZAMORA ACOSTA	SANDRA MILENA ANDRADE MURILLO	

- Porcentaje de Avance:** Según el cronograma, el proyecto de actualización BCP tiene un avance del **60%**, sujeto a la incorporación total de los resultados del BIA y la gestión de riesgos.
- Formalización:** No existe acto administrativo de formalización vigente para el PCN 2025. La OAPS reconoce que para futuras actualizaciones será necesario gestionar la aprobación ante el Comité de Gestión y Desempeño.
- Hallazgo Contraloría General de la República:** El compromiso relacionado con el hallazgo de la Contraloría (código 22 02 002) se encuentra en **proceso (abierto)**. Aunque existe el documento base PL\_GETI\_004, al no estar aprobado formalmente ni implementado al 100%, el riesgo de "ausencia de un PCN formalizado" persiste materialmente.

<b>ELABORADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>REVISADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>APROBADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno
---	--	--

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

## 1.2. ESTADO DE AVANCE DEL PCN.

Se comparó el compromiso adquirido ante la Contraloría General de la República (CGR) frente a la realidad operativa a noviembre de 2025, encontrando lo siguiente:

### *ESTADO DE MADUREZ DEL PCN VS. COMPROMISOS*

Componente del PCN	Estado Actual	% Avance Real	Evidencia / Observación
<b>Documento Maestro</b>	En Borrador (V0)	90% (Redacción)	El documento existe como PL_GETI_004, versión 00, fecha Noviembre 2025. Falta documentar el análisis completo de impacto del negocio BIA.
<b>Incorporación BIA</b>	Parcial	50% - 90%	Dependiendo del proceso, la incorporación de resultados varía. Globalmente se estima en un 50%. La herramienta no ha cubierto el 100% del universo de procesos de la entidad.
<b>Aprobación Formal</b>	Pendiente	0%	No cuenta con firma de aprobación ni acto administrativo. Se requiere someter al Comité Institucional de Gestión y Desempeño.
<b>Implementación</b>	En Proceso	60% Global	El cronograma indica un avance general del proyecto del 60%, sujeto al cierre del BIA.

Teniendo en cuenta lo anterior, se evidencia que la entidad ha superado la fase de "Inexistencia del PCN" (que originó el hallazgo de la Contraloría 22 02 002) pero se encuentra aún en la fase de "Diseño/Elaboración".

El hallazgo de la Contraloría General de la República frente al PCN, muestra avances documentales, pero no puede cerrarse definitivamente hasta que el ciclo del BIA concluya y se realicen las pruebas que validen la operatividad del plan descrito en el documento PL-GETI-004.

## 1.3. HALLAZGO.

El documento "PL\_GETI\_004\_PLAN\_DE\_CONTINUIDAD\_DEL\_NEGOCIO\_V0" de Noviembre de 2025 es un borrador (V0) sin aprobación de Comité ni acto administrativo. Avance del proyecto al 60%, por lo cual el **Plan de Continuidad del Negocio (PCN)** se encuentra técnicamente en una fase de construcción, que, a la fecha está en el (60%).

La condición de "borrador no aprobado" impide la ejecución legal de los protocolos de recuperación, la realización de pruebas de efectividad y la capacitación del personal, dejando a la organización vulnerable ante cualquier incidente y en incumplimiento de la normativa vigente.

De acuerdo a la evidencia revisada y basada en los hechos expuestos por esta oficina en el desarrollo de este primer alcance, a pesar de contar con la estructura documental (Versión 0), el PCN se encuentra en fase de cierre de "Elaboración". La falta de completitud en la incorporación del BIA (50% de avance en procesos restantes) impide que el plan sea funcionalmente operativo.

<b>ELABORADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>REVISADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>APROBADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno
---	--	--

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

La OCI considera pertinente indicar que, el hallazgo fue generado con base en la evidencia recolectada durante el proceso de auditoría y refleja una situación o "desviación" existente en el momento de la elaboración del presente informe.

### 1.3.1 CRITERIO:

Lineamientos, estándares y acciones definidos en el Documento Técnico del Plan de Continuidad del Negocio del Departamento Administrativo de la Función Pública – DAFP Versión 5, las Guías 10 y 11 de preparación de las TIC’S para la continuidad del Negocio y Análisis de Impacto de Negocios - BIA del Ministerio de las TIC’s y los marcos de referencia internacionales establecidos por la serie ISO 22301 de 2019 e ISO 27001 de 2022.

Así mismo, la exigencia del Plan de Continuidad del Negocio (PCN) para el sector público se fundamenta principalmente en el marco de la Gestión del Riesgo de Desastres (Ley 1523 de 2012) y la Gestión de la Seguridad de la Información (Política de Gobierno Digital), siendo la Función Pública la entidad que emite lineamientos y documentos técnicos, como el Documento Técnico del Plan de Continuidad del Negocio, que referencia la NTC 5722 y exige la planificación para la continuidad de funciones misionales ante incidentes, integrándose con el Sistema de Gestión de Calidad y Control Interno (Decreto 1072 de 2015).

El Documento Técnico del Plan de Continuidad del Negocio (Función Pública), proporciona los requisitos y la metodología para entidades públicas, basándose en estándares internacionales como la norma NTC 5722 (continuidad del negocio) y la ISO 31000 (gestión de riesgos).

### 1.3.2. CAUSAS:

- Posible Cronograma de proyecto no realista: Se subestimó el tiempo necesario para realizar el BIA (Análisis de Impacto al Negocio) y el RA (Análisis de Riesgos), lo que retrasó la fase de documentación.
- Posible Insuficiencia de recursos asignados: Falta de personal dedicado o presupuesto para contratar consultoría especializada que finalice el 40% restante (pruebas, capacitación, divulgación).
- Posible flujo de aprobación de (actos administrativos) lento o complejo, reteniendo el documento en una fase de "revisión".

### 1.3.3. CONSECUENCIAS:

- Incapacidad de respuesta ante desastres: Al no estar operativo ni probado, ante una interrupción (ciberataque, falla eléctrica, desastre natural), la entidad no sabrá cómo reaccionar, elevando el tiempo de caída de los servicios.
- Sanciones regulatorias CGR: La falta de un PCN aprobado puede acarrear sanciones o multas por parte de los entes de control ( Hallazgo Contraloría General de la República).

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

- Pérdida de datos o activos: Sin estrategias de respaldo y recuperación formalizadas, existe un riesgo alto de pérdida irrecuperable de información.

#### 1.4. RECOMENDACIONES. (Para el Plan De Mejoramiento)

A partir del hallazgo identificado, se formulan las siguientes recomendaciones para ser incluidas y atendidas por la OAPS y el Asesor del Despacho en el plan de mejoramiento correspondiente:

1. **Priorización de la Finalización del BIA:** Se recomienda declarar como "prioridad crítica" la culminación del Análisis de Impacto al Negocio (BIA) para el 50% de los procesos restantes. Sin el BIA completo, cualquier estrategia de recuperación plasmada en el documento PL\_GETI\_004 carece de sustento técnico real.
2. **Cronograma de Cierre del PCN Reajustado:** Establecer una fecha definitiva dentro del primer trimestre de 2026 para completar el 40% restante del proyecto del PCN en su versión final, incluyendo el cierre completo del BIA.
3. **Compleitud Documento Maestro del PCN de la SES:** cerrar la brecha del 40% faltante en la construcción del PCN antes del cierre del primer trimestre de la próxima vigencia.
4. **Aprobación y Formalización por Comité:** Presentar la versión final del PCN ante el Comité Institucional de Gestión y Desempeño, para su validación y aprobación técnica y estratégica. Quedará como soporte el Acta de reunión del Comité con la decisión de aprobación.
5. **Divulgación y Capacitación:** Ejecutar una jornada de socialización del PCN aprobado a los líderes de proceso y personal crítico (con roles de recuperación).

## 2. ALCANCE #2.

**Revisar y evaluar la documentación fundamental y análisis del impacto que sustentan el Plan de Continuidad del Negocio (PCN), a través de la verificación de que el BIA se haya realizado correctamente, identificando tiempos máximos de interrupción (MTPD) y objetivos de tiempo de recuperación (RTO/RPO) para los procesos identificados como críticos en la entidad.**

### 2.1. CONDICIÓN.

Realizada la verificación de las evidencias aportadas por el área auditada para el desarrollo de este alcance (Matriz BIA Consolidada Supersolidaria con actividades críticas; Secciones del BIA en Cronograma BCP), la Oficina de Control Interno evidencia la aplicación de la metodología identificando lo siguiente:

- **Procesos Críticos:** Se han priorizado actividades en procesos como Gestión Financiera (Cierre contable, Recaudo), Gestión Jurídica (Tutelas) y TI.

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

- **Métricas:** La matriz cumple e incluye columnas para MTPD (Periodo Máximo de Inactividad), RTO (Tiempo Objetivo de Recuperación) y RPO (Punto Objetivo de Recuperación).
- **Criticidad:** Se observa la categorización de actividades (Ej. "Actividad de criticidad Moderada", "Alta").

El reporte de avance (Cronograma) indica que, al mes de noviembre de 2025, se han realizado sesiones con procesos clave (PLESI, CODI, GEJU, GREF, etc..) alcanzando un ajuste del 90% en estos, pero restan sesiones con otros procesos, situando el avance global de la aplicación del BIA en un 50%.

De igual manera, se evidencia una matriz BIA consolidada que evalúa impactos operacionales, financieros, reputacionales y legales. Frente a la Identificación de Métricas encontramos que la matriz define claramente lo siguiente:

- **MTPD (Periodo Máximo Tolerable de Inactividad):** Definido en días/horas (Ej: "Menor a 8 horas" para procesos críticos).
- **RTO (Objetivo de Tiempo de Recuperación):** Asignado por prioridad (Ej: Prioridad 1 para procesos críticos como acciones de tutela o fallos de primera instancia).
- **RPO (Objetivo de Punto de Recuperación):** Definido en términos de pérdida de datos tolerable.

Análisis de Criticidad: Se realizó un muestreo de la Matriz BIA Consolidada para verificar si se está identificando correctamente los tiempos críticos (RTO/RPO) según la norma ISO 22301, así:

#### *Muestreo de Criticidad de Procesos*

Proceso / Área	Actividad Crítica Identificada	MTPD (Tiempo Máximo Tolerable)	RTO (Tiempo Objetivo Recuperación)	RPO (Pérdida de Datos Tolerable)	Nivel de Criticidad
<b>Defensa Jurídica</b>	Fallos de primera instancia / Tutelas	Menor a 1 día	<b>Prioridad 1</b> (0-8 horas)	0-8 horas	<b>Alta/Crítica</b>
<b>Gestión Financiera</b>	Cierre Contable / Declaración Impuestos	4 días	<b>Prioridad 2</b> (8-24 horas)	8-24 horas	<b>Alta</b>
<b>Planeación (PLES)</b>	Formulación de Proyectos	Superior a 5 días	<b>Prioridad 5</b> (>72 horas)	> 72 horas	<b>Leve</b>
<b>Tecnología (GETI)</b>	Soporte a PABLO / Secop	3 días	<b>Prioridad 2</b> (8-24 horas)	Variable	<b>Moderada</b>

<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

La metodología BIA es correcta y se alinea con la Guía 11 del MinTIC. No obstante, la herramienta no ha cubierto el 100% del universo de procesos de la entidad, lo que deja brechas en la identificación de tiempos de recuperación para la totalidad de la operación.

- Procesos Avanzados: PLESI, CODI, COIN, EVGS, GEJU, GREF, GEDO, GITH y GECO13.
- Procesos Pendientes: Resto de la entidad (sesiones programadas hasta el 9 de diciembre de 2025).

La metodología BIA es adecuada y se alinea con ISO 22301, pero su ejecución es parcial (50% - 90%), lo que impide tener un mapa completo de criticidad de la entidad a la fecha del corte del presente informe.

## 2.2. HALLAZGO.

No se generan hallazgos para este alcance, debido a que no se evidencia un incumplimiento normativo y procedimental respecto a la metodología y estructuración del análisis del impacto al negocio BIA. Sin embargo se generan las siguientes recomendaciones.

## 2.3. RECOMENDACIONES QUE NO IMPLICAN PLAN DE MEJORAMIENTO.

- Acelerar las sesiones de trabajo con los procesos restantes y reportadas en el cronograma para completar el 100% del Análisis de Impacto al Negocio BIA, antes del cierre de la vigencia 2025.
- Diseñar un cronograma de pruebas para el primer trimestre de 2026 que permita validar los RTOs definidos en la matriz BIA y la efectividad del DRP tecnológico (PL-GETI-002).

## 3. ALCANCE #3

**Verificar que los roles para la gestión del plan de continuidad del negocio de la SES (Documentación, Aprobación, Activación y Restablecimiento) estén formalmente asignados. Adicionalmente, constatar que el "Comité de Crisis" esté formalmente constituido y que sus miembros conozcan sus responsabilidades de activación.**

### 3.1. CONDICIÓN:

Realizada la verificación de las evidencias aportadas por el área auditada para el desarrollo de este alcance (PL\_GETI\_004 "Sección 7: Roles" y Memorando de respuesta de la OAPS No. 20251200023213), la Oficina de Control Interno evidencia que el documento PL\_GETI\_004 define teóricamente los roles (Líder de Continuidad, Comité de Crisis, Equipos de Recuperación).

Sin embargo, en la respuesta al memorando de auditoría, la OAPS declara que no existe un "Comité de Crisis" formalmente constituido como ente independiente. La OAPS argumenta que, dado el nivel de madurez, las funciones del Comité de Crisis han sido asignadas de manera transitoria al Comité de Seguridad y Privacidad de la Información.

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

Teniendo en cuenta lo anterior y frente a los puntos clave del alcance evaluado, la oficina de control interno evidencia lo siguiente:

- **Inexistencia del Comité de Crisis:** La OAPS informa explícitamente que "no ha constituido formalmente un Comité de Crisis" debido a que no ha alcanzado el nivel de madurez requerido en el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Roles Transitorios:** Las funciones de gobernanza y toma de decisiones ante incidentes han sido asumidas transitoriamente por el Comité de Seguridad y Privacidad de la Información (Comité SPI).
- **Documentación de Roles:** El borrador del PCN en su Sección 7 define teóricamente los roles (Líder de Continuidad, Comité de Crisis, Equipos de Recuperación), pero estos nombramientos no están operativa ni administrativamente formalizados en la práctica más allá del papel.

Frente a la obligatoriedad normativa para la conformación y creación del comité de crisis, a través del memorando No. 20251200023213, la OAPS expone lo siguiente: *"Es importante precisar que ni el Decreto 338 de 2022 ni la Resolución 500 de 2021 exigen explícitamente la creación de un "Comité de Crisis" bajo esa denominación específica. No obstante, ambas normas sí establecen la obligatoriedad de definir roles, responsabilidades y una instancia institucional capaz de coordinar la gestión y respuesta a incidentes de seguridad digital, articulando funciones de análisis, reporte, toma de decisiones y comunicación con autoridades externas como CSIRT-Gob./COLCERT.*

*En consecuencia, aunque el término "Comité de Crisis" corresponde a una práctica de implementación y madurez organizacional, la existencia de una instancia que cumpla esas funciones se hace necesaria, por lo que la Entidad ha mitigado esta exigencia mediante la asignación transitoria de dichas responsabilidades al Comité de Seguridad y Privacidad de la Información".*

Teniendo en cuenta lo anterior, la Oficina de Control Interno evaluó la estructura de mando propuesta en el borrador del PCN frente a la realidad reportada en el memorando, así:

**Estructura de Respuesta: Ideal (PCN) vs. Real**

Rol en el Plan (PCN)	Responsabilidad Teórica	Situación Real Reportada	Nivel de Riesgo
<b>Comité de Crisis</b>	Activación del plan y toma de decisiones estratégicas.	<b>No constituido.</b> Funciones asumidas transitoriamente por el Comité de Seguridad (Comité SPI).	<b>Alto.</b> El Comité SPI tiene un enfoque técnico/preventivo, no necesariamente de respuesta a desastres organizacionales.
<b>Líder de Continuidad</b>	Jefe OAPS / Planeación.	Asignado en borrador. Ejerce funciones de coordinación.	<b>Medio.</b> El rol existe, pero carece de acto administrativo que le dé potestad de mando en crisis.
<b>Equipos de Respuesta</b>	Ejecución de procedimientos de recuperación.	Definidos en papel (Borrador PCN), sin evidencia de capacitación o simulacros específicos.	<b>Alto.</b> En una crisis real, el personal podría desconocer sus funciones.

<b>ELABORADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>REVISADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>APROBADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno
---	--	--

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

La OAPS explica la ausencia del Comité de Crisis por falta de "madurez del MSPI". Sin embargo, la Oficina de Control Interno considera que la gestión de crisis no debe depender exclusivamente de la madurez tecnológica, sino de la capacidad administrativa.

Si bien existe una medida de mitigación (asignación de funciones al Comité de Seguridad), la norma ISO 22301 sugiere una estructura de gobierno clara para la continuidad del negocio. La falta de un comité de crisis dedicado o la falta de formalización explícita de estas funciones dentro del reglamento del Comité de Seguridad y Privacidad de la Información podría ralentizar la toma de decisiones en un evento real de desastre mayor.

### 3.2. HALLAZGO.

Durante la evaluación del presente alcance, orientado a verificar la asignación formal de roles para la gestión del Plan de Continuidad del Negocio (PCN) y la constitución del Comité de Crisis, la Oficina de Control Interno evidenció y expuso las debilidades actuales en la formalización de la estructura de gobernanza para la Continuidad del Negocio e inexistencia de un Comité de Crisis independiente.

**Inexistencia formal del Comité de Crisis:** La OAPS confirmó mediante el Memorando No. 20251200023213 que no se ha constituido formalmente un "Comité de Crisis". Las funciones de gobernanza, toma de decisiones y respuesta ante desastres han sido asumidas de manera transitoria por el Comité de Seguridad y Privacidad de la Información (Comité SPI).

**Falta de formalización administrativa de roles:** Si bien el documento PL\_GETI\_004 (Sección 7) define teóricamente los roles (Líder de Continuidad, Comité de Crisis, Equipos de Recuperación), estos nombramientos carecen de actos administrativos que les otorguen potestad de mando real.

**Ausencia de capacitación y pruebas:** No se evidenció capacitación específica ni realización de simulacros para los "Equipos de Respuesta", lo que implica que la definición de estos roles se limita a lo documental (borrador del PCN) sin trascender a la práctica operativa.

#### 3.2.1 CRITERIO:

La situación descrita contraviene o presenta brechas frente a los siguientes marcos de referencia:

ISO 22301 (Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio): *Cláusula 5.3 (Roles, responsabilidades y autoridades):* La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización. *Cláusula 7.5 (Información documentada) y 8.4 (Estructura de respuesta a incidentes):* Exige una estructura formalizada para la respuesta ante incidentes que tenga la capacidad de activar el plan.

Decreto 338 de 2022 y Resolución 500 de 2021: Aunque no exigen la denominación exacta de "Comité de Crisis", sí establecen la obligatoriedad de definir roles, responsabilidades y una instancia institucional efectiva para coordinar la gestión, toma de decisiones y comunicación con autoridades

<b>ELABORADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>REVISADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>APROBADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno
---	--	--

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

externas (CSIRT/COLCERT). La asignación "transitoria" sin una formalización explícita en el reglamento del Comité SPI debilita el cumplimiento de este mandato.

### 3.2.2 CAUSAS:

- Dado el nivel de madurez, las funciones del Comité de Crisis han sido asignadas de manera transitoria al Comité de Seguridad y Privacidad de la Información, el cual tiene un enfoque técnico/preventivo, no necesariamente de respuesta a desastres organizacionales.
- La decisión administrativa de utilizar al Comité de Seguridad y Privacidad de la Información (Comité SPI) como mecanismo de mitigación transitorio para suplir las funciones de crisis.

### 3.2.3 CONSECUENCIAS:

La falta de un Comité de Crisis dedicado o formalmente empoderado, sumado a la falta de formalización de roles operativos, genera los siguientes riesgos de nivel Alto:

- Ineficacia en la toma de decisiones: Ante un evento de desastre mayor (no solo ciberseguridad, sino físico o natural), el Comité SPI podría carecer del enfoque estratégico global o de la disponibilidad inmediata requerida, ralentizando la activación del PCN.
- Confusión operativa: Al no existir actos administrativos ni capacitación práctica (simulacros), los miembros de los Equipos de Recuperación y el Líder de Continuidad podrían desconocer sus límites de autoridad y funciones específicas durante una emergencia real.
- Falta de respaldo legal: El "Líder de Continuidad" podría verse imposibilitado para ejecutar acciones críticas (gastos de emergencia, contratación, movilización de personal) si su rol no está respaldado por un acto administrativo en firme, dependiendo únicamente de un borrador o una asignación teórica.

### 3.3 RECOMENDACIONES. (Para el Plan De Mejoramiento)

1. Actualizar el Acto Administrativo o Reglamento Interno del "Comité de Seguridad y Privacidad de la Información" que incluya un capítulo o párrafo que le asigne formalmente las funciones de "Comité de Crisis de Continuidad de Negocio", otorgándole la potestad para tomar decisiones financieras, operativas y administrativas ante desastres mayores, asegurando que no se limite únicamente a incidentes de seguridad digital.
2. Formalizar la asignación de roles del Plan de Continuidad del Negocio (PCN), generando comunicaciones oficiales (memorandos internos) notificando a los funcionarios que ocupan los roles definidos en el documento PL\_GETI\_004, anexando sus funciones específicas en caso de desastre.
3. Realizar un cronograma de capacitación y al menos un simulacro de prueba de roles con los miembros del Comité SPI y los líderes de equipo designados donde deban interactuar frente

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

a un escenario hipotético, para verificar la cadena de mando. Esto con el fin de validar si la estructura transitoria actual es realmente eficaz para responder a una crisis o si se confirma la necesidad de crear el Comité de Crisis independiente.

#### 4. ALCANCE #4.

**Verificar si los manuales existentes en materia de gestión de riesgos, emergencias y recuperación tecnológica de la SES, se encuentran formalizados, actualizados y abordan los elementos del Plan de Continuidad del Negocio, con el fin de determinar si estos contribuyen de manera efectiva a una estrategia integral de continuidad ante eventos de emergencia, desastre o contingencia de tipo social, natural, tecnológico, financiero o sanitario.**

##### 4.1. CONDICIÓN.

Realizada la verificación de las evidencias aportadas por el área auditada para el desarrollo de este alcance, la Oficina de Control Interno evidencia lo siguiente:

- **DRP-TIC (PL-GETI-002):** Se encuentra actualizado a noviembre de 2025 (Versión 01). Contiene procedimientos detallados de recuperación (backup, restauración, bases de datos) y se alinea con los RTOs tecnológicos.
- **Manual de Emergencias (MA-GITH-003):** Formalizado en noviembre de 2025. Incluye análisis de vulnerabilidad, PON (Procedimientos Operativos Normalizados) y estructura de brigadas.
- **Gestión de Riesgos (MA-PLES-008):** Actualizado a enero de 2025. Establece la metodología para identificar riesgos que podrían activar el PCN.

La Oficina de Control Interno verificó que estos documentos complementarios se encuentran formalizados y disponibles en la herramienta PABLO (Módulo SIG). De igual manera, el borrador del PCN (V0) incluye una sección de evaluación de riesgos que considera amenazas físicas, naturales y tecnológicas, alineada con la metodología de la entidad.

Teniendo en cuenta lo anterior, se verificó si los documentos actuales funcionan como "islas" o como un sistema integrado y articulado con lo expuesto en el documento (borrador) PL\_GETI\_004\_PLAN\_DE\_CONTINUIDAD\_DEL\_NEGOCIO\_V0 de la entidad.

Documento Existente	Estado de Formalización	Articulación con el PCN 2025
Plan de Continuidad del Negocio (PCN)	<b>Borrador V0</b>	Es el documento integrador. Referencia a los demás planes.
Modelo de Seguridad y Privacidad de la Información (MSPI)	<b>Aprobado y Formalizado</b>	El PCN depende de este modelo para definir el Comité de Crisis.
Plan de Recuperación de Desastres (DRP)	<b>Formalizado</b>	El PCN delega la recuperación tecnológica explícitamente al DRP.
Manual de Emergencias (MA-PLES-004)	<b>Formalizado</b>	El PCN delega la evacuación y seguridad física a este manual.

<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>APROBADO POR</b>
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

 <b>Supersolidaria</b>	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
--	--	---

Dado lo anterior, esta oficina evidencia que el punto débil es el documento superior (Plan de Continuidad del Negocio) que une a los otros planes operativos (DRP y Emergencias), ya que es el único que permanece en estado de (borrador) no aprobado ni formalizado.

De otra parte, se resalta que la integración de estos planes complementarios es correcta, toda vez que el borrador del PCN redirecciona de manera clara al momento de existir amenazas, así:

- *Amenaza Tecnológica:* Activa DRP.
- *Amenaza Física/Natural:* Activa Manual de Emergencias

En general, la entidad cuenta con un sistema documental robusto y actualizado en los componentes complementarios del PCN (Tecnología, Emergencias Físicas y Riesgos).

## 5. RESUMEN RESULTADO GENERAL DE LOS ALCANCES DE AUDITORÍA.

Aspecto Evaluado	Estado	Observación Principal
<b>Formalización del PCN</b>	Incompleto	El documento es un borrador (V0) sin aprobación de Comité Institucional de Gestión y Desempeño, ni acto administrativo. Avance del proyecto al 60%.
<b>Ejecución del BIA</b>	En Proceso (Retrasado)	Metodología correcta y métricas (RTO/RPO) definidas. Cobertura parcial de procesos (aprox. 50% - 90% según el área).
<b>Comité de Crisis</b>	No Existe	No se ha constituido. Funciones asumidas temporalmente por el Comité SPI.
<b>Manuales de Apoyo</b>	Cumple	Planes de Emergencia y DRP formalizados en PABLO e integrados conceptualmente al PCN.

## 6. CONCLUSIÓN GENERAL

La Oficina de Control Interno evidencia progreso en la estructuración de la estrategia de continuidad del negocio en la entidad, mediante la elaboración del documento base PL\_GETI\_004 y la ejecución técnica del BIA. Sin embargo, a la fecha de la auditoría, la entidad NO cuenta con un Plan de Continuidad del Negocio formalizado, aprobado y plenamente implementado.

El estado actual del PCN es de "Elaboración". La falta de formalización del documento maestro y la ausencia de un Comité de Crisis específico representan brechas significativas frente a los estándares ISO 22301 y los requisitos para el cierre efectivo del hallazgo de la Contraloría General de la República, incrementando la alta vulnerabilidad de la continuidad del negocio.

Las recomendaciones que no requieren plan de mejoramiento se generan estrictamente en el marco de la función evaluativa independiente de la Oficina de Control Interno (OCI) y buscan orientar la mejora continua de los procesos, la prevención de riesgos y el cumplimiento de las metas institucionales, sin implicar una desviación o incumplimiento normativo relevante.

ELABORADO POR	REVISADO POR	APROBADO POR
<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno

	<b>INFORME DEFINITIVO DE AUDITORIA</b>	<b>Código:</b> FT-COIN-007 Marzo-2025 <b>Versión:</b> 02
---	--	---

**V. SUSCRIPCION DE PLAN DE MEJORAMIENTO**

Se requiere DEL PROCESO AUDITADO O UNIDAD AUDITADA, la definición y suscripción del respectivo plan de mejoramiento. La etapa inicial de FORMULACION, será diligenciada por la oficina de control interno, quien, como valor agregado, incluirá recomendaciones para el hallazgo; sin embargo, las propias que proponga el auditado junto con las recomendadas, deben ser consensuadas, durante la etapa siguiente de DEFINICION Y SUSCRIPCION de dicha actividad.

Atentamente,



**JORGE HERNANDO PEDRAZA VARGAS**  
Jefe Oficina de Control Interno

Elaboró: John Leonardo Martin Betancourt - Auditor Contratista OCI  
Revisó: Jorge Hernando Pedraza Vargas – Jefe de la Oficina de Control Interno

<b>ELABORADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>REVISADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno	<b>APROBADO POR</b> <b>Nombre:</b> Jorge Hernando Pedraza Vargas <b>Cargo:</b> Jefe Oficina de Control Interno
---	--	--