



Plan

Continuidad del negocio - PCN



URF | Unidad de Proyección Normativa
y Estudios de Regulación Financiera

Contenido

1.	Introducción	5
2.	Objetivo.....	5
3.	Objetivos específicos.....	6
4.	Alcance.....	7
5.	Marco normativo y referencial	7
6.	Productos esperados	8
7.	Términos y definiciones	9
8.	Roles y responsabilidades	11
9.	Metodología de continuidad del negocio	14
9.1.	Identificación de procesos críticos	14
9.2.	Análisis de Impacto al Negocio (BIA)	19
9.2.1.	Identificación y evaluación del impacto	19
9.2.2.	Determinación del tiempo máximo de Recuperación (RTO)	21
9.2.3.	Determinación del punto máximo de pérdida de información (RPO)	24
9.2.4.	Definición de niveles mínimos de operación (NMO).....	29
9.2.5.	Establecimiento de recursos esenciales	30
9.2.6.	Resultados institucionales de análisis de impacto – BIA	32
9.3.	Análisis de riesgos de interrupción.....	35
9.3.1.	Enfoque conceptual del análisis de riesgos de interrupción	36
9.3.2.	Estructura conceptual de los riesgos de interrupción	36
9.3.3.	Metodología para el análisis de riesgos de interrupción	38
9.3.4.	Resultados institucionales de riesgos de interrupción	52
9.4.	Estrategias de continuidad	55
9.4.1.	Enfoque metodológico de las estrategias	55
9.4.2.	Metodología para la construcción de estrategias	56
9.4.3.	Criterios para la definición de estrategias	57
9.4.4.	Tipología de estrategias de continuidad	57
9.4.5.	Estructuración de las estrategias por categorías de interrupción	58

9.4.6. Resultados institucionales de las estrategias de continuidad	59
9.5. Procedimientos de respuesta y recuperación	61
9.5.1. Activación del plan.....	62
9.5.2. Respuesta inicial y gestión del incidente	63
9.5.3. Operación en contingencia	64
9.5.4. Recuperación y retorno a la normalidad	67
9.5.5. Evaluación posterior al incidente	68
9.5.6. Roles en los procedimientos de respuesta y recuperación	69
9.5.7. Resultados institucionales de procedimientos de respuesta y recuperación para los procesos críticos.....	69
9.6. Protocolo de comunicaciones en contingencia.....	72
9.6.1. Principios de comunicación en contingencia	72
9.6.2. Matriz de comunicaciones en contingencia	72
9.6.3. Vocerías autorizadas por ámbitos de gestión.....	74
9.7. Integración con la planeación institucional	74
9.8. Mejora continua	75
10. Plan de pruebas, simulacros y validación	76
10.1. Tipos de ejercicios	76
10.2. Criterios de evaluación de simulacros	77
11. Documento referente	78
12. Datos de elaboración y control de cambios	79

Índice de tablas

Tabla 1 Matriz de criterios de evaluación.....	15
Tabla 2 Matriz de escala de impacto.....	15
Tabla 3 Matriz de análisis de procesos críticos.....	16
Tabla 4 Matriz conceptual de MTD (Tiempo Máximo Tolerable de Interrupción).....	17
Tabla 5 Matriz Tiempo Máximo Tolerable de Interrupción (MTD)	18
Tabla 6 Matriz de impacto para el BIA	21
Tabla 7 Matriz de clasificación del impacto final.....	21
Tabla 8 Matriz de preguntas orientadoras por dimensiones para establecer el RTO	22
Tabla 9 Matriz orientadora de niveles por dimensión	23
Tabla 10 Matriz de clasificación del impacto Vs intervalo de tiempo	24
Tabla 11 Matriz de preguntas orientadoras por dimensiones para establecer el RPO	25
Tabla 12 Matriz orientadora de niveles de impacto por dimensión para establecer el RPO	26
Tabla 13 Matriz de escala institucional de RPO.....	27
Tabla 14 Ejemplo de tabla de respuestas del proceso Gestión Financiera.....	27
Tabla 15 Ejemplo de rango de pérdida aceptable.....	28
Tabla 16 Ejemplo RPO final del proceso Gestión Financiera	29
Tabla 17 Componentes de los NMO (QUÉ debe mantenerse activo)	29
Tabla 18 Ejemplo de niveles mínimos de operación para un proceso crítico.....	30
Tabla 19 Categorías de Recursos Esenciales (CON QUÉ se sostiene la operación)	31
Tabla 20 Ejemplo de Recursos Esenciales (CON QUÉ se sostiene la operación).....	32
Tabla 21 Diferencia entre NMO y recursos esenciales	32
Tabla 22 Resumen matricial del BIA – Procesos críticos URF	33
Tabla 23 Evaluación de impacto por dimensión - Procesos críticos URF	33
Tabla 24 Determinación de RTO y RPO - Procesos críticos URF	33
Tabla 25 Detalle niveles mínimos de operación (NMO) - Procesos críticos URF.....	34
Tabla 26 Recursos esenciales - Procesos críticos URF.....	34
Tabla 27 Justificación técnica del nivel crítico o muy alto - Procesos críticos URF	35
Tabla 28 Clasificación de riesgos de interrupción de la URF	38
Tabla 29 Metodología para el análisis de riesgos de interrupción	40
Tabla 30 Escala metodológica para la clasificación del nivel de afectación en la continuidad	41
Tabla 31 Clasificación cuantificada del nivel de afectación.....	41
Tabla 32 Ejemplo de nivel de afectación	42

Tabla 33	Método objetivo para el análisis de causas de interrupción	43
Tabla 34	Clasificación objetiva de causas	43
Tabla 35	Escala para evaluar la incidencia de la causa	44
Tabla 36	Ejemplo de vulnerabilidad.....	45
Tabla 37	Método para la evaluación de controles existentes	46
Tabla 38	Escala de evaluación de controles frente a la continuidad.....	46
Tabla 39	Ejemplo método de evaluación de controles existentes.....	47
Tabla 40	Valoración cuantitativa del ejemplo de evaluación de controles	48
Tabla 41	Método para la definición de acciones de continuidad	49
Tabla 42	Regla de decisión para definir la acción dominante y sugerencia de la complementaria	50
Tabla 43	Tipología de acciones de continuidad	51
Tabla 44	Ejemplo de análisis de riesgos	52
Tabla 45	Resultados institucionales de riesgos de interrupción	54
Tabla 46	Metodología para la construcción de estrategias de continuidad	56
Tabla 47	Tipología de estrategias de continuidad.....	57
Tabla 48	Estrategias de continuidad por categoría de interrupción	59
Tabla 49	Resultados institucionales de las estrategias de continuidad	61
Tabla 50	Procedimiento de activación del plan	63
Tabla 51	Matriz de actividades de respuesta inicial y gestión del incidente.....	64
Tabla 52	Matriz de operación en contingencia	66
Tabla 53	Matriz de criterios para mantener la operación en contingencia.....	66
Tabla 54	Matriz de criterios para mantener la operación en contingencia.....	67
Tabla 55	Matriz de validación para retorno a la normalidad	68
Tabla 56	Matriz de actividades de evaluación posterior al incidente	69
Tabla 57	Matriz de roles y responsabilidades para los procedimientos de respuesta y recuperación.....	69
Tabla 58	Resultados institucionales de procedimientos de respuesta y recuperación para los procesos críticos	72
Tabla 59	Matriz de comunicaciones en contingencia.....	73
Tabla 60	Matriz de vocerías autorizadas por ámbito de gestión.....	74
Tabla 61	Matriz de tipos de ejercicios	77
Tabla 62	Matriz de evaluación de simulacros	78

1. Introducción

El Plan de Continuidad del Negocio (PCN) de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, establece el marco estratégico y operativo que permite mantener y restablecer los procesos críticos ante eventos que interrumpan su operación. Su propósito es asegurar que la Entidad cuente con las capacidades necesarias para anticipar, responder y recuperarse de incidentes disruptivos, mediante la identificación de riesgos, el análisis de impactos y la definición de estrategias de continuidad y recuperación que garanticen la prestación ininterrumpida de las funciones misionales.

La URF, entidad pública del orden nacional, adscrita al Ministerio de Hacienda y Crédito Público, tiene como misión la preparación normativa y la generación de conocimiento técnico en materia cambiaria, monetaria y crediticia, así como en las actividades financiera, bursátil, aseguradora y solidaria de ahorro y crédito. Su labor contribuye al fortalecimiento de la estabilidad, solidez, inclusión, innovación y desarrollo del sistema financiero colombiano, en beneficio de los consumidores y del interés público.

En este contexto, el PCN constituye un instrumento esencial para proteger la continuidad regulatoria, la integridad de la información, la seguridad de los activos institucionales y la capacidad operativa de la Entidad. Su diseño se fundamenta en la NTC/ISO 22301:2019, los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el Decreto 1658 de 2016 (artículo 8) y en las mejores prácticas de gestión de continuidad aplicadas por entidades del orden nacional.

Este documento es de obligatorio cumplimiento para todos los servidores, contratistas y partes interesadas de la URF, y se integra al Sistema de Gestión Institucional (SGI) como un componente clave de la gestión del riesgo operativo, asegurando una respuesta coordinada, oportuna y eficiente ante cualquier evento que pueda comprometer la operación institucional.

2. Objetivo

Establecer el marco estratégico y operativo que permita mantener y restablecer los procesos críticos de la Unidad ante eventos que interrumpan su operación, mediante la identificación de riesgos y análisis de impactos, la definición de estrategias y procedimientos de respuesta y recuperación, y la asignación de roles, recursos y mecanismos de coordinación, con el fin de garantizar la prestación continua de las funciones misionales, proteger la información y los activos institucionales, y asegurar un retorno ordenado, oportuno y eficiente a la

normalidad, en coherencia con el enfoque de gestión pública y los lineamientos del MIPG.

3. Objetivos específicos

- Identificar procesos críticos — Determinar y documentar los procesos, servicios y actividades esenciales de la URF, así como sus dependencias internas y externas, para priorizar la continuidad operativa en situaciones de interrupción.
- Realizar el Análisis de Impacto al Negocio (BIA) — Evaluar los impactos operativos, legales, reputacionales y financieros derivados de la interrupción de los procesos críticos, estableciendo tiempos máximos de recuperación (RTO/RPO) y niveles mínimos de operación.
- Evaluar riesgos y escenarios de interrupción — Identificar amenazas internas y externas que puedan afectar la continuidad del negocio y analizar su probabilidad y severidad para definir medidas de mitigación.
- Definir estrategias de continuidad y recuperación — Establecer alternativas operativas, tecnológicas, logísticas y de personal que permitan mantener o restablecer los procesos críticos dentro de los tiempos definidos.
- Diseñar y documentar los procedimientos de respuesta — Elaborar protocolos claros para la activación del plan, la gestión de incidentes, la comunicación interna y externa, la operación en contingencia y la recuperación gradual.
- Asignar roles y responsabilidades — Definir la estructura de gobernanza del plan, los equipos de continuidad, sus funciones, líneas de reporte y mecanismos de coordinación interdependencias.
- Establecer el plan de comunicaciones en contingencia — Diseñar los canales, mensajes, responsables y protocolos para garantizar la comunicación oportuna con servidores, directivos, entidades externas y grupos de valor durante una interrupción.
- Implementar mecanismos de soporte tecnológico y documental — Definir los recursos tecnológicos, respaldos de información, accesos alternos y repositorios que permitan operar en contingencia y recuperar la información institucional.

- Ejecutar pruebas, simulacros y ejercicios de validación — Realizar ejercicios periódicos para verificar la efectividad del plan, identificar brechas y fortalecer la capacidad de respuesta institucional.
- Establecer el proceso de mejora continua — Incorporar lecciones aprendidas, resultados de pruebas, auditorías y retroalimentación para actualizar el plan y asegurar su vigencia y pertinencia.

4. Alcance

Comprende desde la identificación y priorización de los procesos críticos, sus recursos asociados y las dependencias internas y externas que los soportan, hasta la definición, activación y ejecución de las estrategias y procedimientos necesarios para mantener o restablecer su operación durante y después de una interrupción.

Incluye el análisis de impactos, la gestión de incidentes, la operación en contingencia, la recuperación gradual y el retorno a la normalidad. Su ámbito de aplicación abarca todas las áreas, servidores públicos, sistemas de información, infraestructura, proveedores y terceros que intervienen en la prestación de los servicios misionales y de apoyo de la URF, garantizando que las medidas de continuidad se apliquen de manera integral, coordinada y conforme a los lineamientos institucionales y normativos.

5. Marco normativo y referencial

El marco normativo que sustenta el Plan de Continuidad del Negocio integra estándares internacionales y lineamientos nacionales que orientan la gestión del riesgo, la seguridad de la información y la articulación con el Sistema de Gestión Institucional - SGI. La siguiente matriz consolida los principales referentes aplicables a la URF, describiendo su alcance y la forma en que cada uno aporta criterios, obligaciones y buenas prácticas para el diseño, implementación y mejora del PCN, facilitando su trazabilidad y evaluación de cumplimiento.

Referente	Descripción y alcance	Aplicación al PCN
NTC/ISO 22301:2019	Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Continuidad del Negocio.	Define estructura del PCN, requisitos de análisis de impacto (BIA), tiempos de recuperación (RTO/RPO), pruebas, mejora continua y liderazgo.
ISO 31000:2018	Estándar internacional para la gestión del riesgo, aplicable a cualquier organización.	Alinea el análisis de riesgos del PCN con el enfoque institucional de identificación, valoración y tratamiento de riesgos.

Referente	Descripción y alcance	Aplicación al PCN
MIPG – DAFP	Modelo Integrado de Planeación y Gestión. Dimensión de Gestión con Valores para el Resultado.	Integra el PCN con la planeación institucional, el control interno y la gestión del desempeño.
Decreto 1658 de 2016, Art. 8	Establece el soporte del MHCP a la URF en servicios transversales de infraestructura y TIC.	Define responsabilidades compartidas en continuidad tecnológica, respaldos, infraestructura y recuperación.
Ley 594 de 2000	Ley General de Archivos. Regula la gestión documental y la protección de documentos vitales.	Obliga a identificar, proteger y garantizar la recuperación de documentos esenciales para la operación.
Decreto 1499 de 2017	Reglamenta el MIPG y articula el sistema de gestión con el control interno.	Vincula el PCN con el ciclo de planeación, seguimiento, evaluación y mejora institucional.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.	Alinea el PCN con lineamientos de ciberseguridad, gestión de incidentes y protección de activos de información.
BCI Good Practice Guidelines	Referente internacional de buenas prácticas en continuidad del negocio.	Complementa la ISO 22301 con metodologías, escenarios, estrategias y prácticas de pruebas y simulacros.

6. Productos esperados

- **Mapa de procesos críticos priorizados:** Documento que identifica los procesos esenciales de la URF, sus dependencias, recursos y niveles mínimos de operación.
- **Análisis de Impacto al Negocio (BIA):** Informe que determina los impactos operativos, legales, reputacionales y financieros, así como los tiempos máximos de recuperación (RTO/RPO) de cada proceso crítico.
- **Matriz de riesgos y escenarios de interrupción:** Producto que consolida amenazas, vulnerabilidades, niveles de riesgo y medidas de mitigación asociadas a la continuidad.
- **Inventario de recursos críticos y requerimientos mínimos:** Relación de infraestructura, tecnología, personal, insumos y accesos necesarios para operar durante una contingencia.
- **Estrategias institucionales de continuidad y recuperación:** Documento que define las alternativas operativas, tecnológicas y logísticas para mantener o restablecer los procesos críticos.
- **Procedimientos de activación, respuesta y recuperación:** Protocolos operativos que describen paso a paso cómo actuar ante una interrupción, cómo operar en contingencia y cómo retornar a la normalidad.

- **Plan de comunicaciones en contingencia:** Lineamientos, mensajes, responsables y canales para garantizar la comunicación interna y externa durante incidentes.
- **Plan de pruebas, simulacros y validación:** Cronograma y metodología para evaluar la efectividad del plan y medir la capacidad de respuesta institucional.
- **Informe de lecciones aprendidas y mejora continua:** Documento que consolida hallazgos, brechas y acciones de mejora derivadas de ejercicios, auditorías o incidentes reales.

7. Términos y definiciones

- **Activación del Plan:** Momento en el cual la URF pone en marcha los procedimientos de continuidad y recuperación ante la ocurrencia de un evento disruptivo.
- **Análisis de Impacto al Negocio (BIA):** Herramienta que identifica los procesos críticos, evalúa los impactos derivados de su interrupción y determina los tiempos máximos de recuperación (RTO/RPO).
- **Amenaza:** Evento, condición o agente externo o interno con potencial de causar una interrupción en la operación de la URF.
- **Capacidad de Recuperación:** Habilidad institucional para restablecer procesos, servicios y recursos dentro de los tiempos definidos.
- **Contingencia:** Situación anormal que afecta la operación normal de la URF y que requiere la aplicación de medidas temporales para mantener la continuidad.
- **Continuidad del Negocio:** Conjunto de estrategias, procedimientos y recursos que permiten asegurar la operación de los procesos críticos ante interrupciones.
- **Evento Disruptivo:** Suceso inesperado que afecta la disponibilidad de recursos, infraestructura, personal o tecnología, generando interrupciones en la operación.
- **Equipo de Continuidad:** Grupo de servidores responsables de coordinar la activación, ejecución y seguimiento del plan de continuidad.

- **Gestión de Incidentes:** Proceso para identificar, analizar, responder y documentar eventos que afectan la operación institucional.
- **Impacto:** Consecuencia operativa, legal, reputacional, financiera o tecnológica derivada de la interrupción de un proceso crítico.
- **Interrupción:** Pérdida parcial o total de la capacidad operativa de un proceso, servicio o recurso institucional.
- **Mitigación:** Acciones orientadas a reducir la probabilidad o el impacto de un evento disruptivo.
- **Normalización:** Retorno ordenado y seguro a las condiciones normales de operación después de una contingencia.
- **Plan de Continuidad del Negocio (PCN):** Documento que establece las estrategias, procedimientos y responsabilidades para mantener o restablecer los procesos críticos de la URF.
- **Proceso Crítico:** Actividad o conjunto de actividades esenciales para el cumplimiento de la misión institucional y cuya interrupción genera impactos significativos.
- **Recuperación:** Conjunto de acciones orientadas a restablecer la operación de los procesos críticos dentro de los tiempos definidos.
- **Recursos Críticos:** Elementos indispensables para la operación de los procesos críticos, tales como personal, tecnología, infraestructura, información y proveedores.
- **Riesgo de Interrupción:** Probabilidad de que un evento disruptivo afecte la continuidad de los procesos institucionales.
- **RTO – Recovery Time Objective:** Tiempo máximo permitido para restablecer un proceso crítico después de una interrupción.
- **RPO – Recovery Point Objective:** Punto máximo de pérdida de información aceptable para un proceso crítico, medido en tiempo.
- **Simulacro:** Ejercicio práctico que permite evaluar la efectividad del plan y la capacidad de respuesta institucional.

- **Tolerancia a la Interrupción:** Tiempo máximo durante el cual un proceso puede permanecer inactivo sin generar impactos inaceptables.

8. Roles y responsabilidades

Roles	Línea de defensa a la que pertenece el rol	Responsabilidades
Comité Institucional de Gestión y Desempeño	Línea estratégica	Es la instancia estratégica responsable de orientar, aprobar y supervisar el Plan de Continuidad del Negocio de la URF. Le corresponde aprobar el plan y sus actualizaciones de acuerdo con los ciclos de planeación institucional, garantizando que las acciones derivadas del PCN se articulen y se incorporen en el plan de acción anual de cada vigencia, conforme a las prioridades misionales y a los lineamientos del MIPG. Así mismo, realiza seguimiento a la implementación del plan, revisa la eficacia de los controles, valida los resultados de pruebas y simulacros, y orienta acciones de mejora continua para fortalecer la capacidad institucional de respuesta y recuperación ante interrupciones.
Subdirección Jurídica y de Gestión Institucional	Primera línea	Coordina el soporte administrativo y tecnológico prestado por el MHCP; gestiona requerimientos de infraestructura, tecnología y logística para la continuidad.
Ministerio de Hacienda y Crédito Público	Primera línea	Brinda el soporte necesario para garantizar la continuidad de los servicios institucionales, incluyendo plataformas, infraestructura, accesos, seguridad de la información y servicios transversales, conforme al artículo 8 del Decreto 1658 de 2016.
Gerentes públicos y líderes de procesos	Primera línea	• Lideran la identificación y documentación de los procesos críticos, sus riesgos, dependencias y recursos esenciales. • Definen los tiempos máximos de recuperación (RTO/RPO) y los niveles mínimos de operación. • Activan los procedimientos de continuidad y contingencia cuando se presenta un evento disruptivo. • Coordinan la ejecución de actividades operativas durante la interrupción y el retorno a la normalidad. • Garantizan la aplicación de los protocolos definidos en el plan y reportan incidentes que afecten la continuidad. • Aseguran la disponibilidad del personal y los recursos necesarios para la operación en contingencia.
Equipos de trabajo	Primera línea	Ejecutan las actividades operativas del plan, aplican los protocolos de respuesta y reportan afectaciones que comprometan la continuidad.

Roles	Línea de defensa a la que pertenece el rol	Responsabilidades
Direccionamiento y Planeación	Segunda línea	El proceso de Direccionamiento y Planeación asume la coordinación integral del Plan de Continuidad del Negocio, liderando su definición, implementación, seguimiento y mejora continua. Le corresponde coordinar la formulación y actualización del plan, articularlo con la gestión del riesgo, la planeación estratégica y los lineamientos del MIPG, y asegurar que las acciones derivadas del PCN se incorporen en el Plan de Acción Anual de cada vigencia, conforme a los ciclos de planeación institucional. Durante la activación del plan, actúa como coordinador operativo, convocando a los equipos de continuidad, consolidando información, gestionando la toma de decisiones y reportando a la alta dirección. Además, lidera el seguimiento a la ejecución de las estrategias de continuidad, coordina la realización de pruebas y simulacros, y consolida las lecciones aprendidas para la mejora continua del plan. También articula las necesidades de soporte administrativo y tecnológico con la Subdirección Jurídica y de Gestión Institucional, quien coordina el apoyo prestado por el Ministerio de Hacienda y Crédito Público, conforme al artículo 8 del Decreto 1658 de 2016.
Proceso de Gestión de Comunicaciones	Segunda línea	Diseña y ejecuta la estrategia de comunicación en contingencia; garantiza la difusión oportuna, clara y coherente de la información interna y externa durante interrupciones; apoya la activación del plan mediante mensajes oficiales, coordinación con vocerías y manejo de comunicaciones con grupos de valor; asegura la trazabilidad y registro de comunicaciones emitidas durante el evento.
Líderes de sistemas de gestión y temas transversales	Segunda línea	Aportan lineamientos técnicos en seguridad de la información, talento humano, infraestructura, comunicaciones y otros temas que soportan la continuidad.
Proceso de Gestión de la Información	Segunda línea	Responsable de recuperación tecnológica, se encarga de ejecutar procedimientos de restauración de sistemas y servicios tecnológicos, en coordinación con el MHCP.

Roles	Línea de defensa a la que pertenece el rol	Responsabilidades
Equipo de Continuidad del Negocio	Segunda línea	El equipo de continuidad estará integrado por la Subdirectora Jurídica y de Gestión Institucional; los líderes de los procesos de Direccionamiento y Planeación, Gestión de la Información y Seguridad de la Información, Gestión de Comunicaciones, Gestión de Talento Humano, Adquisición de Bienes y Servicios y Gestión Financiera; así como por los Subdirectores de Desarrollo de Mercados y de Regulación Prudencial, quienes en conjunto lideran el proceso misional de Desarrollo de Estudios y Proyección Normativa. Este equipo es el responsable de ejecutar las acciones operativas del Plan de Continuidad del Negocio de la URF durante la activación, respuesta, operación en contingencia y retorno a la normalidad. Está integrado por los actores que cumplen funciones de coordinación, gestión de incidentes, comunicaciones y recuperación operativa. Sus responsabilidades son: • Coordinación del Plan de Continuidad: Lidera la activación del plan, convoca y coordina a los integrantes del equipo de continuidad, consolida información relevante para la toma de decisiones y reporta a la alta dirección. • Gestión de Incidentes: Atiende, analiza y gestiona los incidentes que afecten la operación institucional; determina acciones inmediatas, define escalamiento y mantiene el registro de los eventos. • Comunicaciones en Contingencia: Gestiona la comunicación interna y externa durante interrupciones, en coordinación con el proceso de Gestión de Comunicaciones; asegura mensajes claros, oportunos y coherentes para servidores, directivos y grupos de valor. • Retorno a la Normalidad: Coordina la transición desde la operación en contingencia hacia la operación normal, verificando la integridad de la información, la estabilidad de los procesos y la disponibilidad de los recursos necesarios para restablecer la operación institucional.
Proceso de Control y Evaluación	Tercera línea	El Proceso de Control y Evaluación, como tercera línea de defensa, realiza la verificación independiente del Plan de Continuidad del Negocio. Evalúa su eficacia, el cumplimiento de roles y procedimientos, y la pertinencia de los controles definidos. Revisa los resultados de pruebas y simulacros, identifica brechas y riesgos emergentes, y emite recomendaciones de mejora para fortalecer la preparación, respuesta y recuperación institucional. Además, verifica que las acciones de mejora se integren en los instrumentos de planeación y hace seguimiento a su implementación, asegurando trazabilidad y retroalimentación continua para la alta dirección.

9. Metodología de continuidad del negocio

La metodología adoptada por la URF para la construcción, implementación y actualización del Plan de Continuidad del Negocio se fundamenta en un enfoque integral de gestión del riesgo, análisis del impacto, definición de estrategias y establecimiento de procedimientos operativos para garantizar la preparación, respuesta y recuperación ante eventos disruptivos. Esta metodología se desarrolla a través de cinco componentes principales:



Imagen No.1. Componentes del plan de continuidad

9.1. Identificación de procesos críticos

La identificación de procesos críticos constituye el punto de partida del plan. Para ello, cada proceso institucional evalúa su contribución al cumplimiento de la misión, los servicios esenciales que presta y las consecuencias de una interrupción. Este análisis permite determinar qué procesos requieren continuidad prioritaria y cuáles deben contar con estrategias específicas de recuperación.

La identificación de los procesos críticos de la Unidad se realizó mediante una metodología estructurada que permite determinar cuáles procesos deben mantenerse o restablecerse con mayor prioridad ante una interrupción. Este

análisis se desarrolló con base en los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, la Norma ISO 22301 y las buenas prácticas de gestión de continuidad del negocio.

El proceso inició con el levantamiento de información de todos los procesos institucionales, considerando sus productos, actividades esenciales, recursos requeridos, dependencias internas y externas, y obligaciones normativas asociadas. Esta información permitió comprender el rol de cada proceso dentro de la operación institucional y su nivel de sensibilidad ante una interrupción.

Posteriormente, cada proceso fue evaluado mediante una matriz de análisis de criticidad, construida con criterios objetivos que permiten medir el impacto potencial de su interrupción. Los criterios aplicados fueron: impacto misional, impacto legal y regulatorio, impacto financiero, impacto reputacional y de atención al ciudadano, y dependencia tecnológica y de información.

Criterio	Descripción	Peso
Impacto misional	Afectación a la función regulatoria o a la misión institucional.	25%
Impacto legal y regulatorio	Incumplimiento de leyes, sanciones, obligaciones normativas.	25%
Impacto financiero	Afectación a pagos, ingresos, presupuesto, estados financieros.	20%
Impacto reputacional y ciudadanía	Afectación a la confianza pública, transparencia, atención al ciudadano.	15%
Dependencia tecnológica/información	Necesidad de sistemas críticos, datos, SGEDA, seguridad digital.	15%

Tabla 1 Matriz de criterios de evaluación

Cada criterio se valoró en una escala de 1 a 5 y se ponderó según su relevancia para la continuidad del negocio.

Valor	Significado
1	Impacto mínimo, manejable con controles manuales.
2	Impacto bajo, afecta parcialmente el proceso.
3	Impacto moderado, afecta la operación institucional.
4	Impacto alto, compromete obligaciones o servicios.
5	Impacto crítico, afecta misión, legalidad o continuidad.

Tabla 2 Matriz de escala de impacto

El resultado de esta valoración permitió calcular un puntaje total de criticidad para cada proceso. Criticidad total = $\sum(\text{Impacto por criterio} \times \text{Peso})$

Proceso	Impacto misional (25%)	Impacto legal (25%)	Impacto financiero (20%)	Impacto reputacional (15%)	Dependencia tecnológica (15%)	Puntaje total	Nivel de criticidad
Gestión Financiera	5	5	5	4	4	4.75	Crítico
Gestión de la Información	4	5	4	4	5	4.55	Crítico
Desarrollo de Estudios y Proyección Normativa	5	4	3	4	4	4.25	Crítico
Dirección y Planeación	4	5	3	4	4	4.15	Crítico
Control y Evaluación	4	5	3	4	3	4.00	Crítico
Relación con la Ciudadanía y Grupos de Valor	3	4	2	5	3	3.55	Esencial
Gestión de Comunicaciones	3	3	2	5	3	3.30	Esencial
Adquisición de Bienes y Servicios	3	4	3	3	3	3.25	Esencial
Gestión Humana	2	3	2	3	2	2.45	Apoyo

Tabla 3 Matriz de análisis de procesos críticos

- Los procesos con puntajes ≥ 4.0 se clasifican como **críticos**, dado que su interrupción afecta la misión regulatoria, el cumplimiento legal, la operación financiera o la disponibilidad de la información institucional.
- Los procesos con puntajes entre **3.0 y 3.9** se clasifican como **esenciales**, ya que su interrupción afecta la relación con los grupos de valor, la comunicación pública o la operación contractual.
- Los procesos con puntajes ≤ 2.9 se clasifican como **de apoyo**, pues su interrupción puede gestionarse con medidas temporales sin comprometer la continuidad institucional.

De manera complementaria, se aplicó una matriz de Tiempo Máximo Tolerable de Interrupción (MTD), que permitió estimar el periodo máximo durante el cual cada

proceso puede permanecer inactivo sin generar afectaciones severas a la misión institucional, al cumplimiento normativo o a la operación financiera.

La articulación entre la matriz de criticidad y la matriz de MTD permitió clasificar los procesos en tres categorías:

- Procesos críticos, que deben mantenerse o restablecerse en un plazo no mayor a 24 horas.
- Procesos esenciales, que pueden interrumpirse hasta por 72 horas.

Procesos de apoyo, cuya interrupción puede ser mayor sin comprometer la operación institucional.

Nivel de MTD	Rango de tiempo tolerable	Descripción conceptual	Implicaciones para la continuidad
MTD 0-24 horas	Interrupción máxima permitida: hasta 24 horas	Corresponde a procesos cuya interrupción genera afectaciones inmediatas a la misión institucional, incumplimientos legales o regulatorios, riesgos financieros o indisponibilidad de información crítica.	Requieren activación inmediata de estrategias de continuidad, recursos priorizados, redundancias y procedimientos de recuperación rápida.
MTD 24-72 horas	Interrupción máxima permitida: entre 24 y 72 horas	Procesos cuya interrupción no afecta de manera inmediata la misión, pero sí compromete la operación institucional, la relación con los grupos de valor o la transparencia si no se restablecen en un corto plazo.	Requieren planes de restablecimiento acelerado, medidas temporales y coordinación con procesos críticos.
MTD 3-7 días	Interrupción máxima permitida: entre 3 y 7 días	Procesos de apoyo cuya interrupción puede gestionarse con controles compensatorios sin comprometer la continuidad de los procesos críticos o esenciales.	Requieren planes de recuperación gradual, priorización secundaria y mecanismos alternos de operación.

Tabla 4 Matriz conceptual de MTD (Tiempo Máximo Tolerable de Interrupción)

Proceso	Nivel de criticidad (según tabla 3)	MTD estimado	Justificación
Gestión Financiera	Crítico	0-24 horas	Maneja pagos, nómina, impuestos, PAC, contabilidad y obligaciones legales de cumplimiento inmediato.
Gestión de la Información	Crítico	0-24 horas	Soporta SGEDA, seguridad digital, documentos vitales, TRD/CCD/TCA y aplicativos institucionales. Su interrupción afecta toda la operación.
Desarrollo de Estudios y Proyección Normativa	Crítico	24-72 horas	Proceso misional; afecta la agenda normativa, estudios y proyectos regulatorios con impacto nacional.

Proceso	Nivel de criticidad (según tabla 3)	MTD estimado	Justificación
Dirección y Planeación	Crítico	24-72 horas	Administra SGI, riesgos, PTEP, planes estratégicos y continuidad del negocio. Afecta gobernanza institucional.
Control y Evaluación	Crítico	24-72 horas	Tercera línea de defensa; informes de ley, auditorías, plan de mejoramiento y cumplimiento MECI.
Relación con la Ciudadanía y Grupos de Valor	Esencial	48-72 horas	Afecta transparencia, atención al ciudadano, lenguaje claro y participación. Impacto reputacional.
Gestión de Comunicaciones	Esencial	48-72 horas	Manejo de crisis, comunicación pública, medios y canales institucionales.
Adquisición de Bienes y Servicios	Esencial	48-72 horas	Afecta continuidad contractual, SECOP II y abastecimiento institucional.
Gestión Humana	Apoyo	3-7 días	Procesos de bienestar, capacitación, SIGEP y disciplinarios pueden gestionarse temporalmente sin afectar la continuidad crítica.

Tabla 5 Matriz Tiempo Máximo Tolerable de Interrupción (MTD)

- Los procesos con $MTD \leq 24$ horas requieren estrategias inmediatas de continuidad y procedimientos de recuperación priorizados.
- Los procesos con MTD entre 24 y 72 horas requieren planes de restablecimiento rápido, pero permiten medidas temporales.
- Los procesos con MTD superiores a 72 horas pueden gestionarse con controles compensatorios sin comprometer la operación crítica.

Los resultados obtenidos fueron validados con los líderes de proceso y revisados por el Comité Institucional de Gestión y Desempeño, garantizando que la clasificación reflejara la realidad operativa, normativa y estratégica de la Entidad.

Como resultado del análisis, se identificaron como procesos críticos para la continuidad del negocio aquellos cuya interrupción afecta de manera directa la misión regulatoria de la URF, el cumplimiento de obligaciones legales y financieras, la disponibilidad de la información institucional o la gobernanza del Sistema de Gestión Institucional. Estos procesos son:

- Gestión Financiera
- Gestión de la Información
- Desarrollo de Estudios y Proyección Normativa
- Dirección y Planeación

- Control y Evaluación

Estos procesos requieren estrategias específicas de continuidad, recursos priorizados y procedimientos de respuesta y recuperación que aseguren su operación en escenarios de contingencia.

9.2. Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio (BIA) es el componente central del Plan de Continuidad del Negocio, ya que permite identificar, medir y priorizar los efectos que tendría la interrupción de los procesos institucionales, especialmente aquellos clasificados como críticos. Su propósito es determinar qué procesos deben restablecerse primero, en qué tiempos, y con qué recursos mínimos, para asegurar la continuidad operativa de la URF ante eventos disruptivos.

El BIA se fundamenta en dos dimensiones principales:

- El análisis conceptual del impacto, que identifica los tipos de afectación que puede generar la interrupción de un proceso.
- El análisis metodológico, que cuantifica dichos impactos y permite establecer el Tiempo Máximo Tolerable de Interrupción (MTD) y los Requerimientos Mínimos de Operación (RMO).

9.2.1. Identificación y evaluación del impacto

Cada proceso crítico es evaluado para determinar las consecuencias de su interrupción en cinco dimensiones:

- **Operativa:** Corresponde a la afectación en la capacidad de la URF para ejecutar sus actividades esenciales, generar sus productos institucionales o cumplir con su función de proyección regulatoria. Una interrupción operativa puede detener procesos misionales, retrasar entregables o impedir la prestación de servicios internos y externos.
- **Financiera:** Incluye pérdidas económicas directas o indirectas, retrasos en pagos, afectación del presupuesto, sanciones pecuniarias o costos adicionales derivados de la interrupción. En la URF, este impacto es especialmente relevante en procesos como Gestión Financiera y Adquisición de Bienes y Servicios..
- **Reputacional:** Se refiere a la afectación de la confianza pública, la percepción de transparencia, la credibilidad institucional y la relación con los

grupos de valor. Procesos como Comunicaciones y Relación con la Ciudadanía son particularmente sensibles a este tipo de impacto.

- **Legal y regulatoria:** Comprende el incumplimiento de leyes, normas, obligaciones regulatorias, auditorías, reportes obligatorios o compromisos sectoriales. Este impacto es crítico en procesos como Direccionamiento y Planeación, Control y Evaluación y Gestión Financiera.
- **Tecnológica:** Incluye la indisponibilidad de sistemas, pérdida de información, fallas de seguridad digital o interrupción de aplicativos esenciales. Este impacto afecta transversalmente a todos los procesos, pero es determinante en Gestión de la Información.

Para adelantar el ejercicio de identificación del impacto, es necesario recopilar información detallada sobre los productos del proceso, las actividades esenciales, los recursos requeridos (humanos, tecnológicos, físicos y proveedores), las dependencias internas y externas, así como la normatividad aplicable. Esta información permite comprender de manera integral el rol del proceso dentro de la operación institucional.

Nivel de Impacto	Descripción General	Impacto Operativo 25%	Impacto Financiero 20%	Impacto Reputacional 15%	Impacto Legal-Regulatorio 25%	Impacto Tecnológico 15%
1 Bajo	Afectación mínima, manejable sin medidas adicionales.	Retrasos menores sin afectar productos esenciales.	Costos marginales o inexistentes.	Sin afectación perceptible.	No compromete obligaciones.	Fallas menores sin pérdida de información.
2 Moderado	Afectación parcial, controlable sin activar continuidad.	Retrasos que requieren reprogramación.	Costos moderados o reprocesos puntuales.	Inquietudes internas o de grupos de valor.	Riesgo bajo de incumplimiento.	Indisponibilidad temporal de herramientas no críticas.
3 Alto	Afectación significativa a un proceso crítico.	Suspensión temporal de actividades esenciales.	Costos significativos o pérdida de eficiencia.	Afectación visible ante grupos de valor.	Riesgo de incumplimiento de obligaciones.	Indisponibilidad de sistemas críticos por varias horas.

Nivel de Impacto	Descripción General	Impacto Operativo 25%	Impacto Financiero 20%	Impacto Reputacional 15%	Impacto Legal-Regulatorio 25%	Impacto Tecnológico 15%
4 Muy Alto	Compromete el cumplimiento o misional.	Imposibilidad de ejecutar productos misionales.	Costos elevados o afectación presupuestal.	Pérdida de confianza o cuestionamientos públicos.	Incumplimiento de obligaciones regulatorias.	Pérdida de información o fallas críticas prolongadas.
5 Crítico	Impacto severo que requiere activar el PCN.	Paralización total del proceso crítico.	Pérdidas significativas o afectación a la sostenibilidad.	Daño reputacional grave o sostenido.	Incumplimientos con consecuencias sancionatorias.	Indisponibilidad total de sistemas esenciales o pérdida masiva de datos.

Tabla 6 Matriz de impacto para el BIA

Cada nivel asignado se multiplica por su ponderación. Ejemplo: Si un proceso obtiene 4 en impacto operativo $\rightarrow 4 \times 0.25 = 1.0$. Posteriormente, se suman los puntajes ponderados de las cinco dimensiones: Impacto Total = $\sum$ (Nivel asignado X Ponderación). El resultado final siempre estará entre 1.0 y 5.0.

Con el puntaje total se clasifica el proceso en una categoría institucional:

Rango de Puntaje	Clasificación del Impacto
1.0 – 2.4	Bajo
2.5 – 3.4	Moderado
3.5 – 4.4	Alto
4.5 – 5.0	Crítico

Tabla 7 Matriz de clasificación del impacto final

Para cada una de las cinco dimensiones evaluadas, el líder del proceso deberá asignar un nivel de impacto (1 a 5) y, de manera obligatoria, justificar de forma clara, objetiva y verificable la razón por la cual se selecciona dicho nivel, sustentando la valoración en evidencias operativas, normativas, tecnológicas o de gestión que permitan asegurar la trazabilidad y consistencia del análisis.

9.2.2. Determinación del tiempo máximo de Recuperación (RTO)

El RTO es el tiempo máximo que un proceso crítico puede permanecer interrumpido antes de que los impactos se vuelvan inaceptables para la URF. Determinarlo correctamente es clave porque define cuándo debe restablecerse el proceso y qué tan urgente es su recuperación.

Para garantizar que la determinación del RTO (Recovery Time Objective) sea objetiva, verificable y consistente entre procesos, la URF utiliza tres instrumentos metodológicos complementarios:

1. La Matriz de Preguntas Orientadoras por Dimensión, que permite identificar el nivel de afectación que genera la interrupción del proceso.
2. La Matriz Orientadora de Niveles por Dimensión, que traduce esas respuestas en un nivel de impacto: bajo, moderado, alto, muy alto o crítico.
3. La Matriz de Clasificación del Impacto vs Intervalo de Tiempo, que convierte ese nivel en un rango sugerido de RTO.

Estas tres tablas se articulan de manera secuencial para obtener un RTO objetivo, trazable y sustentado en evidencia operativa, normativa y tecnológica.

Preguntas por dimensiones	Rango sugerido de RTO
Operativas	¿En qué momento se detienen actividades esenciales? ¿Cuándo se afecta la entrega de un producto misional? ¿A partir de qué momento se acumula trabajo no recuperable?
Legales y regulatorias	¿Existe un plazo normativo o contractual que obligue a operar antes de cierto tiempo? ¿Hay reportes obligatorios con periodicidad fija que no pueden retrasarse?
Tecnológicas	¿La indisponibilidad del sistema afecta la operación inmediata? ¿Cuánto tiempo puede transcurrir antes de que la falta de acceso a la información se vuelva crítica?
Reputacionales	¿En qué momento la interrupción genera afectación visible ante grupos de valor o entidades de control?
Financieras	¿Cuándo los costos, reprocesos o pérdidas de eficiencia se vuelven significativos o insostenibles?

Tabla 8 Matriz de preguntas orientadoras por dimensiones para establecer el RTO

El análisis de estas preguntas permite identificar el momento límite en el que la interrupción deja de ser aceptable. Ese momento constituye el punto de quiebre operativo.

Una vez revisadas las preguntas orientadoras, se establece el nivel para cada dimensión, de acuerdo con la información aportada por la siguiente matriz:

Nivel	Descripción general	Operativa	Legal-Regulatoria	Tecnológica	Reputacional	Financiera
Bajo	Afectación mínima, manejable sin activar continuidad.	Retrasos menores sin afectar actividades esenciales.	No existe riesgo de incumplimiento.	Fallas menores sin afectar sistemas críticos.	Sin afectación perceptible para grupos de valor.	Costos marginales o inexistentes.

Nivel	Descripción general	Operativa	Legal-Regulatoria	Tecnológica	Reputacional	Financiera
Moderado	Afectación parcial, controlable con ajustes internos.	Retrasos que requieren reprogramación, sin pérdida de productos misionales.	Riesgo bajo de incumplimiento si la interrupción se prolonga.	Indisponibilidad temporal de herramientas no críticas.	Inquietudes internas o de algunos grupos de valor.	Reprocesos o costos moderados.
Alto	Afectación significativa a procesos críticos.	Suspensión temporal de actividades esenciales.	Riesgo real de incumplimiento normativo o contractual.	Indisponibilidad de sistemas críticos por varias horas.	Afectación visible ante grupos de valor o antes de control.	Costos significativos o pérdida de eficiencia.
Muy alto	Compromete el cumplimiento o misional en el corto plazo.	Imposibilidad de ejecutar productos misionales clave.	Alto riesgo de incumplimiento con consecuencias formales.	Fallas críticas prolongadas que comprometen la operación institucional.	Pérdida de confianza o cuestionamientos públicos.	Pérdidas elevadas o afectación presupuestal.
Crítico	Impacto severo que requiere activar el PCN.	Paralización total del proceso crítico.	Incumplimientos con consecuencias sancionatorias.	Indisponibilidad total de sistemas esenciales o pérdida masiva de datos.	Daño reputacional grave o sostenido.	Pérdidas severas que comprometen la sostenibilidad institucional.

Tabla 9 Matriz orientadora de niveles por dimensión

Cada clasificación debe incluir una justificación objetiva, basada en:

- Evidencia operativa
- Obligaciones normativas
- Dependencias tecnológicas
- Riesgos reputacionales
- Impactos financieros

Finalmente, se debe identificar el nivel predominante que corresponde al más alto entre las cinco dimensiones evaluadas.

Ejemplo:

- Operativa: Muy alta
- Legal, reputacional y financiera: Crítica
- Tecnológica: Alta

Nivel predominante: crítico; este nivel representa el riesgo máximo asociado a la interrupción.

Clasificación del impacto	Rango sugerido de RTO
Bajo	48-72 horas
Moderado	24-48 horas
Alto	8-24 horas
Muy Alto	4-8 horas
Crítico	0-4 horas

Tabla 10 Matriz de clasificación del impacto Vs intervalo de tiempo

El líder del proceso determina cuándo la interrupción deja de ser tolerable, considerando:

- Plazos normativos
- Periodicidad de actividades esenciales
- Dependencias tecnológicas críticas
- Sensibilidad de la información
- Riesgos reputacionales o financieros

El RTO final debe ubicarse dentro del rango sugerido, pero puede ajustarse hacia el límite inferior o superior según la evidencia disponible. Este valor constituye, además, un insumo esencial para la definición del RPO, los niveles mínimos de operación y las estrategias de continuidad que se desarrollan en los numerales siguientes.

9.2.3. Determinación del punto máximo de pérdida de información (RPO)

El RPO (Recovery Point Objective) corresponde a la cantidad máxima de información que la URF puede permitirse perder en caso de una interrupción, sin que ello genere afectaciones inaceptables a la operación institucional, al cumplimiento normativo o a la función misional. Mientras el RTO define cuándo debe restablecerse un proceso, el RPO define cuánta información puede perderse sin comprometer la continuidad del negocio y se relaciona directamente con:

- La frecuencia de actualización de la información.
- La criticidad de los datos que maneja el proceso.
- La dependencia tecnológica del proceso.
- La sensibilidad normativa asociada a la información.

Un RPO bajo implica que la información debe respaldarse con mayor frecuencia; un RPO alto indica que el proceso puede tolerar pérdidas mayores sin afectar su operación.

Para garantizar que la determinación del RPO (Recovery Point Objective) sea objetiva, consistente y verificable, la URF utiliza tres instrumentos complementarios para cada proceso crítico:

- La tabla de preguntas orientadoras por dimensión, que permite identificar la sensibilidad del proceso frente a la pérdida de información.
- La matriz orientadora de niveles de impacto por dimensión para establecer el RPO.
- La escala institucional de RPO, que traduce esa sensibilidad en un rango de pérdida aceptable (en horas).

Las tres tablas se articulan mediante un procedimiento secuencial que asegura que el RPO no sea una estimación subjetiva, sino un resultado derivado de un análisis técnico.

Dimensión	Preguntas clave
Operativa	¿Cada cuánto se actualiza la información esencial del proceso?
Legal-Regulatoria	¿Existe obligación normativa de conservar información en tiempo real o con periodicidad específica?
Tecnológica	¿Qué tan dependiente es el proceso de sistemas que registran datos en línea?
Financiera	¿La pérdida de datos genera reprocesos costosos o riesgos de inconsistencias?
Reputacional	¿La pérdida de información afecta la confianza pública o la transparencia?

Tabla 11 Matriz de preguntas orientadoras por dimensiones para establecer el RPO

Las preguntas orientadoras permiten evaluar qué tan grave sería la pérdida de información para el proceso en cinco dimensiones: Operativa, Legal-Regulatoria, Tecnológica, Financiera y Reputacional.

El líder del proceso debe responder cada pregunta con base en evidencia real: periodicidad de actualización, obligaciones normativas, dependencia de sistemas, criticidad de los datos, etc.

Posteriormente, de acuerdo con las respuestas de las preguntas orientadoras y mediante la matriz orientadora de niveles de impacto por dimensión para establecer el RPO, el líder del proceso clasifica de manera objetiva el nivel de sensibilidad frente a la pérdida de información, usando los niveles: baja, moderada, alta, muy alta, crítica.

Nivel	Descripción general	Operativa	Legal-Regulatoria	Tecnológica	Reputacional	Financiera
Baja	La pérdida de información es mínima y manejable sin afectar la operación.	La información perdida puede reconstruirse fácilmente sin afectar actividades esenciales.	No existe obligación normativa de conservar la información en tiempo real ni riesgo de incumplimiento.	La pérdida de datos no afecta sistemas críticos ni la continuidad de la operación.	La pérdida no es visible para los grupos de valor ni afecta la percepción de transparencia.	No genera costos relevantes, reprocesos significativos ni riesgos contables.
Moderada	La pérdida de información genera afectaciones parciales, pero controlables.	Se requiere reprocesar información, pero sin afectar productos misionales ni plazos críticos.	Existe riesgo bajo de inconsistencias, pero puede corregirse sin sanciones ni incumplimientos.	La pérdida afecta la eficiencia, pero no compromete la operación si se cuenta con respaldos periódicos.	Puede generar inquietudes internas, sin impacto externo relevante.	Genera reprocesos o costos moderados, manejables dentro del presupuesto.
Alta	La pérdida de información afecta procesos críticos y genera riesgos relevantes.	La reconstrucción de la información es compleja y puede afectar la entrega de productos esenciales.	Existe riesgo real de incumplimiento normativo o contractual si la información no se recupera.	La pérdida de datos en sistemas críticos afecta la operación durante varias horas.	La pérdida puede ser percibida por grupos de valor o entes de control y afectar la confianza.	Genera costos significativos, riesgos de errores contables o afectación a estados financieros.
Muy alta	La pérdida de información compromete la misión institucional en el corto plazo.	La información perdida es difícil o imposible de reconstruir y afecta directamente productos misionales.	Se configura un alto riesgo de incumplimiento con posibles consecuencias formales o sancionatorias.	La pérdida de datos críticos compromete la integridad de sistemas y la gestión de información institucional.	Genera cuestionamientos públicos, pérdida de confianza o afectación reputacional relevante.	Las pérdidas económicas o riesgos financieros son elevados y afectan la sostenibilidad operativa.
Crítica	La pérdida de información es severa y requiere activar el PCN.	Se pierde información esencial e irrecuperable que impide la operación del proceso crítico.	Se materializan incumplimientos con consecuencias legales, regulatorias o sancionatorias graves.	Se produce pérdida masiva de datos o indisponibilidad total de información esencial.	Genera daño reputacional grave o sostenido, con afectación a la credibilidad institucional.	Las pérdidas económicas o riesgos financieros son severos y comprometen la sostenibilidad institucional.

Tabla 12 Matriz orientadora de niveles de impacto por dimensión para establecer el RPO

Posterior a este paso, se debe identificar el nivel predominante, que corresponde siempre al nivel más alto entre las dimensiones evaluadas, dado que representa el riesgo máximo asociado a la interrupción. Una vez determinado, este nivel se relaciona con la escala institucional de RPO para obtener el rango de pérdida aceptable (por ejemplo: Crítico → 0–1 h; Alta → 4–24 h)."

Nivel	Rango de pérdida aceptable	Significado
RPO 0–1 h	Crítico	Información en tiempo real
RPO 1–4 h	Muy alto	Alta sensibilidad normativa o tecnológica
RPO 4–24 h	Alto	Actualización diaria
RPO 24–48 h	Moderado	Información no crítica
RPO > 48 h	Bajo	Procesos de apoyo

Tabla 13 Matriz de escala institucional de RPO

El resultado esperado de este paso es convertir la sensibilidad identificada en un intervalo de tiempo concreto.

Finalmente, el líder del proceso ajusta el RPO final dentro del rango sugerido, con base en evidencia verificable sobre la frecuencia de actualización, obligaciones normativas, dependencia tecnológica y riesgos financieros o reputacionales.

Ejemplo:

Dimensión	Preguntas orientadoras	Respuesta del proceso	Nivel estimado
Operativa	¿Cada cuánto se actualiza la información esencial?	La información de pagos, PAC y registros presupuestales se actualiza en tiempo real.	Crítico
Legal–Regulatoria	¿Existe obligación normativa de conservar información sin pérdida?	Sí. La pérdida de datos puede generar incumplimiento de obligaciones legales y fiscales.	Crítico
Tecnológica	¿La indisponibilidad del sistema afecta la operación inmediata?	Sí. La operación depende de SIIF, SECOP II y aplicativos financieros.	Muy alto
Financiera	¿La pérdida de datos genera reprocesos costosos o riesgos?	Sí. La pérdida de registros puede generar duplicidad de pagos, errores contables o sanciones.	Muy alto
Reputacional	¿La pérdida de información afecta la confianza institucional?	Sí. La pérdida de datos financieros afecta la credibilidad ante MinHacienda y entes de control.	Alto

Tabla 14 Ejemplo de tabla de respuestas del proceso Gestión Financiera

Los niveles asignados fueron: Crítico, Crítico, Muy alto, Muy alto y Alto

El nivel predominante es Crítico, porque:

- Es el nivel más alto asignado.
- Afecta dimensiones legales y operativas.
- Representa el mayor riesgo institucional.

Resultado del paso: Sensibilidad del proceso: Crítica

Según la escala institucional:

Nivel	Rango de pérdida aceptable
Crítico	RPO 0–1 hora

Tabla 15 Ejemplo de rango de pérdida aceptable

Esto significa que el proceso no puede perder más de 1 hora de información sin generar afectaciones inaceptables.

Resultado del paso: RPO sugerido: 0–1 hora

El líder del proceso debe revisar:

- Frecuencia real de actualización
- Obligaciones normativas
- Dependencia tecnológica
- Riesgos financieros

En Gestión Financiera:

- La información se actualiza cada 15 minutos.
- La pérdida de datos puede generar errores contables y sanciones.
- SIIF y aplicativos financieros operan en tiempo real.

Por tanto, el rango sugerido (0–1 hora) debe ajustarse hacia el límite inferior.

Resultado del paso: RPO final recomendado: 30 minutos

El RPO final debe ser:

- Justificado por el líder del proceso
- Documentado en el BIA
- Validado por el equipo de Continuidad del Negocio
- Socializado en el Comité Institucional de Gestión y Desempeño

Resultado final: RPO final del proceso Gestión Financiera: 30 minutos

Elemento	Resultado
Proceso	Gestión Financiera

Elemento	Resultado
Nivel predominante de sensibilidad	Crítico
RPO sugerido (según escala)	0-1 hora
RPO final ajustado	30 minutos
Justificación	Actualización en tiempo real, obligaciones legales, riesgo financiero y dependencia tecnológica crítica.

Tabla 16 Ejemplo RPO final del proceso Gestión Financiera

El RPO final constituye un insumo esencial para la definición de los niveles mínimos de operación y para la formulación de las estrategias de continuidad que se desarrollan en los numerales siguientes.

9.2.4. Definición de niveles mínimos de operación (NMO)

Los Niveles Mínimos de Operación definen qué debe seguir funcionando durante una interrupción para evitar impactos altos o críticos; corresponden a la operación mínima indispensable que el proceso crítico debe garantizar dentro del RTO y sin exceder el RPO.

Componente	Descripción	Ejemplo
Actividades esenciales	Actividades que no pueden detenerse sin generar impactos altos o críticos.	- Registro de pagos obligatorios - Gestión de información crítica - Atención mínima a grupos de valor
Productos mínimos	Entregables indispensables para cumplir obligaciones misionales o normativas.	- Incumplimientos normativos - Afectación misional - Pérdida de información crítica - Riesgos reputacionales o financieros
Personal mínimo	Roles indispensables para ejecutar las actividades esenciales.	- Roles críticos - Perfiles indispensables - Suplencias o reemplazos - Personal habilitado para operar en contingencia

Tabla 17 Componentes de los NMO (QUÉ debe mantenerse activo)

Los Niveles Mínimos de Operación (NMO) representan el umbral básico de funcionamiento que cada proceso crítico debe garantizar durante una interrupción, con el fin de evitar que los impactos operativos, legales, tecnológicos, reputacionales o financieros se vuelvan inaceptables para la URF.

Los NMO responden a la pregunta:

¿Qué es lo mínimo que debe seguir funcionando para que el proceso no se detenga por completo y no se materialicen impactos críticos?

A continuación se presenta un ejemplo ilustrativo de cómo se definen los Niveles Mínimos de Operación para un proceso crítico, con base en los componentes establecidos en este numeral:

Componente	Descripción del componente	Ejemplo aplicado
Actividades esenciales	Actividades que no pueden detenerse sin generar impactos altos o críticos.	• Registro de pagos obligatorios • Validación de disponibilidad presupuestal • Gestión de información financiera crítica
Productos mínimos	Entregables indispensables para cumplir obligaciones misionales o normativas.	• Reporte diario de ejecución presupuestal • Consolidado mínimo de pagos aprobados • Actualización de registros financieros esenciales
Personal mínimo	Roles indispensables para ejecutar las actividades esenciales.	• Profesional financiero responsable del registro • Analista de pagos • Suplente habilitado para operación en contingencia

Tabla 18 Ejemplo de niveles mínimos de operación para un proceso crítico

Los Niveles Mínimos de Operación permiten establecer con precisión qué debe mantenerse activo durante una interrupción para asegurar la continuidad esencial del proceso, en coherencia con el RTO y el RPO previamente determinados. El ejemplo anterior ilustra cómo estos componentes se aplican en un proceso crítico real. Estos niveles constituyen la base para identificar los recursos indispensables y las capacidades mínimas requeridas para operar en escenarios de contingencia, los cuales se desarrollan en el siguiente numeral.

9.2.5. Establecimiento de recursos esenciales

Los recursos esenciales corresponden a los elementos mínimos que cada proceso crítico requiere para operar dentro de los Niveles Mínimos de Operación (NMO) definidos en el numeral anterior; son los habilitadores que permiten ejecutar las actividades esenciales y entregar los productos mínimos.

Estos recursos permiten sostener la operación durante una interrupción, garantizando que el proceso pueda cumplir con su RTO y su RPO, evitando que los impactos operativos, normativos, tecnológicos, reputacionales o financieros se vuelvan inaceptables para la URF. Su definición constituye un insumo

indispensable para el diseño de las estrategias de continuidad y para la activación efectiva del Plan de Continuidad del Negocio.

Los recursos esenciales responden a la pregunta:

¿Qué elementos mínimos necesita el proceso para operar en contingencia?

Recurso	Descripción
Recursos humanos	Personal crítico, suplencias y competencias necesarias.
Recursos tecnológicos	Sistemas, aplicativos, plataformas y conectividad indispensable.
Información crítica	Datos, bases de datos y documentos vitales requeridos para operar dentro del RPO.
Recursos físicos/logísticos	Equipos, espacios, insumos y medios alternos de trabajo.
Recursos de comunicación	Canales, protocolos y contactos necesarios para coordinar la operación.
Soporte externo	Proveedores o entidades externas indispensables para la continuidad.

Tabla 19 Categorías de Recursos Esenciales (CON QUÉ se sostiene la operación)

El siguiente ejemplo, ilustra con qué elementos un proceso crítico puede sostener sus Niveles Mínimos de Operación durante una interrupción, garantizando el cumplimiento del RTO y del RPO.

Recurso	Descripción del recurso	Ejemplo aplicado
Recursos humanos	Personal crítico, suplencias y competencias necesarias para ejecutar las actividades esenciales.	- Profesional financiero responsable del registro de pagos - Analista de disponibilidad presupuestal - Suplente habilitado para operación en contingencia
Recursos tecnológicos	Sistemas, aplicativos, plataformas y conectividad indispensable para operar dentro del RTO.	- Acceso a SIIF Nación - SECOP II para validación contractual - Correo institucional y VPN activa - Conectividad mínima estable
Información crítica	Datos, bases de datos y documentos vitales requeridos para operar sin exceder el RPO.	- Registros presupuestales actualizados - Base de datos de pagos en tiempo real - Documentos soporte de obligaciones financieras
Recursos físicos / logísticos	Equipos, espacios, insumos y medios alternos de trabajo.	- Equipos portátiles con acceso seguro - Puestos de trabajo alternos - Suministros básicos para operación mínima

Recurso	Descripción del recurso	Ejemplo aplicado
Recursos de comunicación	Canales, protocolos y contactos necesarios para coordinar la operación en contingencia.	• Chat institucional • Teléfonos de emergencia del equipo • Protocolos de comunicación con MinHacienda
Soporte externo	Proveedores o entidades externas indispensables para la continuidad.	• Mesa de ayuda SIIF • Soporte técnico de aplicativos financieros • Entidades bancarias para validación de pagos

Tabla 20 Ejemplo de Recursos Esenciales (CON QUÉ se sostiene la operación)

La definición de los Niveles Mínimos de Operación y de los Recursos Esenciales permite establecer con claridad qué debe mantenerse activo y con qué elementos debe sostenerse la operación durante una interrupción. Dado que en algunos casos estos dos aspectos pueden percibirse como similares, a continuación se presenta una tabla comparativa que distingue de manera explícita su alcance y propósito.

Elemento	NMO (QUÉ)	Recursos Esenciales (CON QUÉ)
Propósito	Define la operación mínima que debe mantenerse.	Define los elementos necesarios para sostener esa operación.
Enfoque	Actividades, productos y personal mínimo.	Sistemas, información, equipos, insumos, comunicaciones.
Relación con RTO/RPO	Determina qué debe estar funcionando dentro del RTO.	Determina qué debe estar disponible para cumplir el RTO y el RPO.
Naturaleza	Funcional / operativa.	Habilitadora / de soporte.

Tabla 21 Diferencia entre NMO y recursos esenciales

9.2.6. Resultados institucionales de análisis de impacto – BIA

Una vez desarrollados los conceptos y metodologías anteriormente presentadas, a continuación se presentan los resultados obtenidos para la Unidad:

Proceso crítico	Nivel predominante de impacto	RTO sugerido	RTO final	RPO sugerido	RPO final	NMO definidos	Recursos esenciales
Gestión Financiera	Crítico	0-4 h	2 h	0-1 h	30 min	3 actividades esenciales	6 categorías completas
Gestión de la Información	Crítico	0-4 h	1 h	0-1 h	15 min	4 actividades esenciales	6 categorías completas
Desarrollo de Estudios y Proyección Normativa	Muy alto	24 h	24 h	4-24 h	4 h	3 actividades esenciales	5 categorías

Proceso crítico	Nivel predominante de impacto	RTO sugerido	RTO final	RPO sugerido	RPO final	NMO definidos	Recursos esenciales
Direccionamiento Planeación	Muy alto	24 h	24 h	4-24 h	6 h	3 actividades esenciales	5 categorías
Control y Evaluación	Muy alto	24 h	24 h	4-24 h	6 h	3 actividades esenciales	5 categorías

Tabla 22 Resumen matricial del BIA – Procesos críticos URF

Proceso crítico	Operativa	Legal-Regulatoria	Tecnológica	Financiera	Reputacional	Nivel predominante
Gestión Financiera	Crítico	Crítico	Muy alto	Muy alto	Alto	Crítico
Gestión de la Información	Crítico	Crítico	Crítico	Muy alto	Muy alto	Crítico
Desarrollo de Estudios y Proyección Normativa	Muy alto	Muy alto	Alto	Moderado	Muy alto	Muy alto
Direccionamiento y Planeación	Muy alto	Muy alto	Alto	Moderado	Muy alto	Muy alto
Control y Evaluación	Muy alto	Muy alto	Alto	Moderado	Muy alto	Muy alto

Tabla 23 Evaluación de impacto por dimensión - Procesos críticos URF

Proceso crítico	RTO sugerido	RTO final	RPO sugerido	RPO final
Gestión Financiera	0-4 h	2 h	0-1 h	30 min
Gestión de la Información	0-4 h	1 h	0-1 h	15 min
Desarrollo de Estudios y Proyección Normativa	24 h	24 h	4-24 h	4 h
Direccionamiento y Planeación	24 h	24 h	4-24 h	6 h
Control y Evaluación	24 h	24 h	4-24 h	6 h

Tabla 24 Determinación de RTO y RPO - Procesos críticos URF

Proceso crítico	Actividades esenciales	Productos mínimos	Personal mínimo
Gestión Financiera	Registro de pagos, validación presupuestal, emisión de reportes	PAC, nómina, obligaciones fiscales, reportes SIIF	Profesional financiero, analista, suplente
Gestión de la Información	Gestión documental mínima, acceso a SGEDA, control de versiones	Documentos vitales, TRD/CCD,	Líder documental, analista, suplente

Proceso crítico	Actividades esenciales	Productos mínimos	Personal mínimo
		comunicaciones oficiales	
Desarrollo de Estudios y Proyección Normativa	Elaboración mínima de conceptos, revisión urgente de proyectos	Conceptos regulatorios, agenda normativa	Profesional jurídico/económico, analista
Direccionamiento y Planeación	Seguimiento SGI, gestión de riesgos, coordinación del PCN	Informes SGI, matrices de riesgo, PTEP	Líder del proceso, analista
Control y Evaluación	Emisión mínima de informes de ley, seguimiento a planes	Informes de auditoría, planes de mejoramiento	Auditor líder, analista

Tabla 25 Detalle niveles mínimos de operación (NMO) - Procesos críticos URF

Proceso crítico	Humanos	Tecnológicos	Información crítica	Físicos y logísticos	Comunicación	Soporte externo
Gestión Financiera	3 roles críticos	SIIF, SECOP II, correo, VPN	Registros presupuestales, pagos, soportes	Equipos portátiles, conectividad	Chat institucional, teléfonos	SIIF, bancos
Gestión de la Información	3 roles críticos	SGEDA, SIC, TRD, CCD, TCA	Documentos vitales, bases de datos	Equipos, repositorios alternos	Protocolos de contingencia	MHCP – soporte TI
Desarrollo de Estudios y Proyección Normativa	Expertos jurídicos/económicos	Repositorios normativos, bases documentales	Agenda normativa, proyectos	Equipos, conectividad	Canales internos	Soporte jurídico externo
Direccionamiento y Planeación	Líder + analista	SMGI	Planes, informes, matrices	Equipos, conectividad	Comunicación interna	Soporte MHCP
Control y Evaluación	Auditor líder + analista	SMGI, repositorios	Informes, hallazgos, planes	Equipos, conectividad	Protocolos internos	Soporte técnico MECI

Tabla 26 Recursos esenciales - Procesos críticos URF

Proceso crítico	Justificación técnica del nivel predominante
Gestión Financiera	Maneja pagos, nómina, impuestos, PAC, contabilidad y obligaciones legales inmediatas. Su interrupción afecta la operación institucional y el cumplimiento normativo.
Gestión de la Información	Soporta SGEDA, seguridad digital, documentos vitales, TRD/CCD/TCA. Su interrupción afecta toda la operación institucional.
Desarrollo de Estudios y Proyección Normativa	Afecta la agenda normativa, estudios y proyectos regulatorios con impacto nacional.

Proceso crítico	Justificación técnica del nivel predominante
Direccionamiento y Planeación	Afecta SGI, planeación institucional, riesgos, gobernanza institucional y continuidad del negocio.
Control y Evaluación	Afecta informes de ley, auditorías, planes de mejoramiento y cumplimiento MECI.

Tabla 27 Justificación técnica del nivel crítico o muy alto - Procesos críticos URF

Los resultados del Análisis de Impacto al Negocio evidencian que los cinco procesos clasificados como críticos concentran los mayores riesgos operativos, normativos, tecnológicos, financieros y reputacionales para la URF, por lo que requieren tiempos de recuperación estrictos, niveles mínimos de operación claramente definidos y recursos esenciales priorizados.

La consolidación de estos hallazgos permite comprender con precisión la sensibilidad institucional frente a una interrupción y establece la base técnica para formular las estrategias de continuidad y recuperación que garanticen la operación ininterrumpida de las funciones misionales. Con este análisis, la URF cuenta con un insumo robusto, objetivo y verificable para orientar la toma de decisiones y asegurar la resiliencia institucional ante eventos disruptivos.

9.3. Análisis de riesgos de interrupción

El análisis de riesgos de interrupción en la Unidad se desarrolla con el propósito de identificar, analizar y gestionar los eventos que pueden afectar la continuidad de la operación institucional, particularmente en los procesos críticos previamente definidos a partir del Análisis de Impacto al Negocio (BIA).

Este análisis se fundamenta en los riesgos de gestión actualmente identificados por los procesos y gestionados en el Sistema de Monitoreo de la Gestión Institucional – SMGI, los cuales son reinterpretados desde la perspectiva de continuidad para determinar su capacidad de generar interrupciones o afectaciones significativas en la ejecución de las actividades, la disponibilidad de los recursos y la prestación de los servicios a los grupos de valor.

En este sentido, los riesgos de interrupción no constituyen una categoría independiente, sino una lectura transversal de los riesgos existentes en el SMGI que permite establecer su incidencia directa sobre los procesos críticos.

De esta manera, el análisis se articula con los resultados del BIA, estableciendo un vínculo entre los procesos priorizados por su relevancia institucional y los eventos que pueden comprometer su funcionamiento, facilitando la identificación de

vulnerabilidades y la definición de medidas orientadas a garantizar la continuidad de la operación.

9.3.1. Enfoque conceptual del análisis de riesgos de interrupción

El análisis de riesgos de interrupción se enfoca en identificar aquellos eventos cuya materialización puede:

- Interrumpir total o parcialmente la ejecución de los procesos
- Afectar la prestación del servicio
- Generar indisponibilidad de recursos críticos
- Comprometer el cumplimiento de obligaciones institucionales

Este enfoque se encuentra directamente alineado con los procesos críticos definidos en el documento, en la medida en que permite identificar qué riesgos pueden afectar su continuidad y orientar la definición de acciones de respuesta, contingencia y recuperación.

9.3.2. Estructura conceptual de los riesgos de interrupción

La identificación de los riesgos de interrupción en la URF se fundamenta en el análisis de los riesgos de gestión registrados en el Sistema de Monitoreo de la Gestión Institucional – SMGI, desde una perspectiva orientada a la continuidad de la operación. En este sentido, los riesgos no se analizan de forma individual aislada, sino que se agrupan en función de la naturaleza de las afectaciones que pueden generar sobre los procesos críticos.

Conceptualmente, los riesgos de interrupción se organizan a partir de dos criterios:

- **Origen del riesgo:** fuente principal desde la cual se puede generar la afectación (tecnológica, operativa o administrativa).
- **Tipo de impacto en la continuidad:** forma en que el evento afecta la operación (interrupción total, reducción de capacidad o generación de reprocesos).

A partir de estos criterios, es posible identificar patrones comunes en los riesgos gestionados en el SMGI, los cuales permiten estructurar categorías que reflejan las principales fuentes de interrupción en la Unidad. Esta agrupación facilita la comprensión del comportamiento de los riesgos, su análisis sistemático y su posterior tratamiento en el marco del Plan de Continuidad.

Como resultado de este ejercicio, los riesgos de interrupción se agrupan en tres categorías principales:

- Los asociados a la tecnología e información
- Los relacionados con la disponibilidad de recursos físicos y servicios
- Los derivados de fallas en los procesos administrativos.

La siguiente matriz presenta la clasificación de los riesgos de interrupción, vinculando cada categoría con los riesgos específicos identificados en el SMGI y los efectos que pueden generar sobre la operación institucional:

Categoría de interrupción	Código del riesgo	Riesgo identificado	Proceso crítico afectado	Enfoque de interrupción	Principales efectos en la continuidad
Tecnología e información	URF_36_GI	Pérdida de integridad, disponibilidad o confidencialidad de la información	Gestión de la información / Desarrollo de estudios y proyección normativa	Afectación a sistemas, datos y plataformas institucionales	Paralización de procesos; pérdida de memoria institucional; interrupción del servicio
	URF_26_GI	Desorganización de archivos físicos y electrónicos	Gestión de la Información	Fallas en la gestión documental	Dificultad operativa; retrasos en la gestión; pérdida de información
Recursos físicos y servicios	URF_28_AD	Pérdida, daño o deterioro de bienes	Dirección y Planeación / Adquisición de bienes y servicios	Indisponibilidad de recursos físicos	Retrasos en actividades; limitación de la capacidad operativa
	URF_21_AD	Incumplimiento en la ejecución contractual	Dirección y Planeación / Adquisición de bienes y servicios	Indisponibilidad de bienes o servicios contratados	Interrupción de actividades; reprocesos; afectación del cumplimiento
	URF_24_AD	Retrasos en la suscripción de contratos	Dirección y Planeación / Adquisición de bienes y servicios	Demoras en la provisión de bienes y servicios	Falta de disponibilidad oportuna de recursos; afectación operativa
Procesos administrativos	URF_06_GF	Inconsistencias en la liquidación, cargue y/o pago de la nómina	Gestión Financiera	Fallas en procesos financieros internos	Reprocesos; afectación a servidores; riesgos reputacionales
	URF_07_GF	Inoportunidad en la presentación de	Gestión Financiera	Incumplimiento de obligaciones frente a entes externos	Riesgos legales; incumplimiento normativo

Categoría de interrupción	Código del riesgo	Riesgo identificado	Proceso crítico afectado	Enfoque de interrupción	Principales efectos en la continuidad
		información financiera			
	URF_05_RV	Incumplimiento en tiempos de respuesta a PQRS	Control y Evaluación	Fallas en la atención al ciudadano	Afectación del servicio; posibles sanciones; impacto reputacional
	URF_02_GC	Divulgación de información inoportuna, confusa o poco confiable	Dirección y Planeación /Gestión de comunicaciones	Fallas en comunicación institucional	Desinformación; reprocesos; pérdida de credibilidad
	URF_25_EJ_PN	Citación inadecuada de fuentes en documentos técnicos y estudios	Desarrollo de Estudios y Proyección Normativa	Fallas en la calidad técnica de los productos	Reprocesos; pérdida de credibilidad; afectación reputacional

Tabla 28 Clasificación de riesgos de interrupción de la URF

La clasificación presentada permite estructurar de manera integral los riesgos de interrupción, facilitando la comprensión de su origen, su relación con los procesos críticos y su impacto sobre la operación institucional. Esta organización constituye el insumo base para el desarrollo metodológico del análisis, en el cual se aborda la identificación, valoración y tratamiento de dichos riesgos, así como la definición de acciones orientadas a fortalecer la continuidad del servicio.

9.3.3. Metodología para el análisis de riesgos de interrupción

La metodología para el análisis de riesgos de interrupción se estructura como un proceso secuencial que permite pasar de los riesgos de gestión registrados en el SMGI a su valoración desde la perspectiva de continuidad, articulándolos con los procesos críticos definidos en el BIA. Este enfoque permite analizar de manera sistemática los riesgos en función de su incidencia sobre los procesos críticos, facilitando su valoración, priorización y tratamiento dentro del Plan de Continuidad, a partir de la aplicación de una metodología estructurada que se desarrolla a través de las siguientes etapas.

Etapas	Descripción	Objetivo metodológico	Fuente (SMGI / BIA)	Resultado esperado
Identificación	En esta etapa se delimitan los riesgos de gestión que, por su naturaleza, pueden generar afectaciones en la continuidad de la operación. Para ello se revisan en el SMGI la descripción	Definir el universo de riesgos de interrupción	Riesgos SMGI clasificados (8.3.2)	Conjunto de riesgos con potencial de afectar

Etapa	Descripción	Objetivo metodológico	Fuente (SMGI / BIA)	Resultado esperado
	del riesgo, sus consecuencias y los recursos o servicios que pueden verse afectados. Bajo este criterio, se integran al análisis aquellos riesgos que pueden comprometer la disponibilidad de información, la oportunidad del servicio, la operación financiera, la planeación institucional o la calidad de los productos de evaluación y regulación.			procesos críticos
Asociación	Una vez identificados, los riesgos se relacionan con los procesos críticos definidos en el BIA. Esta relación permite que el análisis no se limite al riesgo como evento aislado, sino que establezca con claridad qué parte de la operación de la Unidad puede verse afectada. Así, el método asegura la articulación entre la gestión del riesgo y la continuidad del negocio, dado que el mismo riesgo puede comprometer directamente la capacidad de respuesta, recuperación o prestación del servicio de un proceso crítico.	Relacionar riesgos con procesos críticos	BIA + procesos críticos	Trazabilidad riesgo – proceso crítico
Valoración	Análisis del impacto del riesgo sobre la operación (interrupción, reducción o reproceso). En esta etapa se incorpora el componente metodológico de valoración operativa, que complementa la valoración tradicional del SMGI. Su aplicación consiste en: - Evaluar cómo el riesgo afecta la operación del proceso - Determinar si genera interrupción, reducción o reproceso - Clasificar el riesgo según el nivel de afectación.	Determinar afectación en la continuidad	SMGI análisis operativo +	Determinación del nivel de criticidad del riesgo en términos de continuidad
Análisis de causas	Esta etapa corresponde al componente metodológico de análisis de vulnerabilidad, orientado a comprender por qué puede materializarse el riesgo. Su aplicación consiste en: - Identificar causas registradas en el SMGI - Analizar patrones comunes (tecnológicos, operativos, administrativos, externos)	Identificar vulnerabilidades	Causas SMGI	Comprensión de vulnerabilidades / Factores de interrupción

Etapa	Descripción	Objetivo metodológico	Fuente (SMGI / BIA)	Resultado esperado
	-Identificar factores críticos que incrementan la probabilidad de interrupción			
Evaluación de controles	En esta etapa se desarrolla el componente metodológico de evaluación de la capacidad de respuesta actual. Su aplicación consiste en: -Revisar los controles asociados a cada riesgo en el SMGI -Evaluar su tipo (preventivo, detectivo o correctivo) -Analizar su efectividad frente a la interrupción	Medir capacidad de mitigación	Controles SMGI	Identificación de fortalezas y brechas en el control del riesgo
Definición de acciones	Esta etapa integra el componente metodológico de gestión del riesgo orientada a la continuidad. Su aplicación consiste en: -Definir acciones frente a la materialización del riesgo -Articular las acciones del SMGI con medidas de continuidad -Establecer mecanismos de respuesta operativa	Establecer respuesta ante interrupción	SMGI + continuidad	Conjunto de acciones orientadas a mantener o restablecer la operación

Tabla 29 Metodología para el análisis de riesgos de interrupción

La aplicación integrada de estas etapas permite consolidar un análisis estructurado en el cual cada riesgo es abordado de manera integral, garantizando la coherencia entre la gestión del riesgo institucional y el enfoque de continuidad del negocio. Este desarrollo metodológico no solo facilita la trazabilidad entre riesgos, procesos críticos y medidas de manejo, sino que también constituye la base para la definición de las estrategias y acciones que se desarrollan en los numerales siguientes.

En este sentido, y con el fin de asegurar la adecuada aplicación del método, es necesario profundizar en algunos aspectos específicos derivados de las particularidades identificadas en la matriz de la metodología para el análisis de riesgos de interrupción, los cuales se abordan a continuación:

Etapa de valoración desde la perspectiva de continuidad

La valoración complementa la calificación del SMGI mediante un enfoque específico de continuidad, orientado a determinar qué tanto puede afectar el riesgo la operación del proceso crítico, mediante los siguientes instrumentos:

Variable de análisis	Criterio de evaluación	Puntaje 1	Puntaje 2	Puntaje 3
Continuidad del proceso	Grado en que el riesgo afecta la ejecución del proceso crítico	No interrumpe el proceso	Reduce parcialmente la capacidad operativa	Interrumpe total o casi totalmente el proceso
Disponibilidad de recursos esenciales	Afectación a información, sistemas, personal o recursos indispensables	Los recursos permanecen disponibles	Se afecta parcialmente uno o más recursos esenciales	Se pierde o genera indisponibilidad de uno o más recursos esenciales
Impacto en el servicio	Efecto del riesgo sobre la prestación del servicio o entrega del producto	Impacto menor o interno	Impacto significativo en oportunidad o calidad	Afectación directa del servicio o imposibilidad de prestarlo
Capacidad de recuperación inmediata	Posibilidad de restablecer la operación con controles o ajustes ordinarios	Recuperación inmediata con ajustes menores	Recuperación posible con medidas de contingencia	Requiere activación de medidas extraordinarias de recuperación

Tabla 30 Escala metodológica para la clasificación del nivel de afectación en la continuidad

Para clasificar el nivel de afectación en la continuidad, se evalúa cada riesgo frente a las cuatro variables anteriores y se asigna un puntaje entre 1 y 3 por cada una.

Posteriormente, se suman los puntajes obtenidos y se clasifica el nivel de afectación conforme a la siguiente escala:

Rango de puntaje total	Nivel de afectación	Interpretación metodológica	Resultado esperado
4 a 6	Medio	El riesgo genera retrasos, reprocesos o afectaciones manejables sin detener el proceso crítico	Requiere ajustes operativos y seguimiento reforzado
7 a 9	Alto	El riesgo reduce significativamente la capacidad operativa o afecta recursos relevantes del proceso crítico	Requiere medidas de contingencia y priorización operativa
10 a 12	Crítico	El riesgo compromete la continuidad del proceso crítico, afecta recursos esenciales o impide la prestación del servicio	Requiere activación inmediata de medidas de continuidad y recuperación

Tabla 31 Clasificación cuantificada del nivel de afectación

La clasificación del nivel de afectación se realiza mediante la evaluación objetiva del comportamiento esperado del proceso crítico frente a la materialización del riesgo, considerando su impacto sobre la operación, la disponibilidad de recursos esenciales, la prestación del servicio y la capacidad de recuperación inmediata. El

puntaje total obtenido permite identificar de manera homogénea el nivel de afectación del riesgo en términos de continuidad y facilita su priorización dentro del análisis.

Ejemplo de aplicación:

Código del riesgo	Proceso crítico afectado	Categoría de interrupción	Continuidad del proceso	Recursos esenciales	Impacto en el servicio	Capacidad de recuperación	Total	Nivel
URF_36_GI_ Pérdida de integridad, disponibilidad o confidencialidad de la información	Gestión de la Información	Tecnología e información	3	3	3	3	12	Crítico
URF_28_AD_ Pérdida, daño o deterioro de bienes	Dirección y Planeación	Recursos físicos y servicios	2	2	2	2	8	Alto
URF_06_GF_ Inconsistencias en la liquidación, cargue y/o pago de la nómina	Gestión Financiera	Procesos administrativos	1	2	2	1	6	Medio

Tabla 32 Ejemplo de nivel de afectación

Etapas de análisis de causas y determinación de vulnerabilidad

El análisis de causas de interrupción tiene por objeto determinar, de manera objetiva, qué factores pueden originar la materialización de los riesgos previamente asociados a los procesos críticos. Para ello, se toman como insumo las causas registradas en el SMGI, y se evalúa su incidencia sobre los recursos, actividades y condiciones esenciales que sostienen la continuidad de cada proceso crítico.

Metodológicamente, esta etapa se desarrolla mediante un procedimiento secuencial que permite pasar de la causa registrada en el riesgo a la identificación de la vulnerabilidad de continuidad que debe ser tratada en el Plan.

Paso metodológico	Cómo se hace	Criterio objetivo de análisis	Resultado esperado
1. Identificación de causas	Se revisan en el SMGI las causas documentadas para cada riesgo priorizado	La causa debe estar expresamente registradas en el riesgo correspondiente	Listado de causas por riesgo

Paso metodológico	Cómo se hace	Criterio objetivo de análisis	Resultado esperado
2. Clasificación de la causa	Cada causa se agrupa según su naturaleza	Se clasifica como tecnológica, operativa, administrativa o externa, según el origen del factor	Tipología homogénea de causas
3. Relación con el proceso crítico	Se analiza si la causa afecta recursos, actividades o condiciones necesarias para el proceso crítico	La causa se relaciona con el proceso cuando afecta información, sistemas, recursos físicos, personal clave o prestación del servicio	Asociación causa-proceso crítico
4. Evaluación de incidencia	Se determina la magnitud de la afectación que la causa puede generar sobre la continuidad	Se evalúa si la causa puede detener el proceso, reducir significativamente su capacidad o generar reprocesos	Nivel de incidencia de la causa
5. Determinación de vulnerabilidad	Se identifica la condición específica que facilita la interrupción	La vulnerabilidad se formula como la debilidad observable derivada de la causa	Vulnerabilidad de continuidad identificada

Tabla 33 Método objetivo para el análisis de causas de interrupción

Criterio de clasificación de las causas: Para asegurar uniformidad en el análisis, las causas deben clasificarse con base en su naturaleza predominante. Esta clasificación no se realiza por intuición, sino por el tipo de condición que origina la afectación registrada en el riesgo.

Tipo de causa	Criterio de clasificación	Ejemplo de aplicación
Tecnológica	La causa está asociada a fallas en sistemas, accesos, plataformas, seguridad digital o disponibilidad de información	Debilidad en controles de acceso; fallas en aplicativos; pérdida de información
Operativa	La causa proviene de errores en la ejecución de actividades o del incumplimiento de procedimientos	Errores en registros; omisión de actividades; fallas en procesamiento
Administrativa	La causa se origina en debilidades de gestión, seguimiento, supervisión o control	Falta de seguimiento; controles insuficientes; debilidad en supervisión
Externa	La causa depende de proveedores, servicios externos, plataformas compartidas o terceras entidades	Fallas del MHCP; indisponibilidad de proveedores; servicios institucionales externos

Tabla 34 Clasificación objetiva de causas

Si una causa puede ubicarse en más de una categoría, se clasifica según el factor que tenga mayor incidencia sobre la continuidad del proceso crítico.

Criterio objetivo para evaluar la incidencia de la causa: El análisis no termina en clasificar la causa; debe determinarse qué tan directamente puede afectar la continuidad. Para ello, cada causa se evalúa frente a cuatro variables observables:

- Afectación a recursos esenciales: si compromete información, sistemas, personal, infraestructura o insumos clave.
- Afectación a actividades críticas: si impide o dificulta la ejecución de actividades esenciales del proceso.

- Impacto en el servicio o producto: si compromete la entrega del servicio o del producto esperado.
- Capacidad de compensación: si la Unidad puede continuar operando con controles o medidas ordinarias.

Variable	Puntaje 1	Puntaje 2	Puntaje 3
Recursos esenciales	No afecta recursos esenciales	Afecta parcialmente un recurso esencial	Genera indisponibilidad de un recurso esencial
Actividades críticas	No interrumpe actividades críticas	Dificulta o retrasa actividades críticas	Impide ejecutar actividades críticas
Servicio o producto	Afectación menor o interna	Afecta oportunidad o calidad	Impide prestar el servicio o entregar el producto
Capacidad de compensación	Puede manejarse con ajustes menores	Requiere contingencia operativa	Requiere medidas extraordinarias de recuperación

Tabla 35 Escala para evaluar la incidencia de la causa

Regla de decisión:

- 4 a 6 puntos - Incidencia media
- 7 a 9 puntos - Incidencia alta
- 10 a 12 puntos - Incidencia crítica

Una vez valorada la causa, se formula la vulnerabilidad de continuidad. La vulnerabilidad no es la causa en sí misma, sino la condición del proceso crítico que queda expuesta y que puede facilitar la interrupción.

Fórmula metodológica de construcción: Causa identificada + elemento afectado + efecto sobre la continuidad = vulnerabilidad

Ejemplo de formulación

Nombre del riesgo	Proceso crítico afectado	Causa identificada	Tipo de causa	Elemento o afectado	Puntaje total	Nivel de incidencia	Vulnerabilidad identificada
URF_36_GI Pérdida de integridad, disponibilidad o confidencialidad de la información	Gestión de la Información	Debilidad en controles de acceso en sistemas de información	Tecnológica	Información crítica / sistemas	12	Crítica	Exposición a pérdida o indisponibilidad de información esencial para la operación

Nombre del riesgo	Proceso crítico afectado	Causa identificada	Tipo de causa	Elemento afectado	Puntaje total	Nivel de incidencia	Vulnerabilidad identificada
URF_28_AD Pérdida, daño o deterioro de bienes	Dirección y Planeación	Uso inadecuado de bienes y debilidad en seguimiento físico	Administrativa	Recursos físicos (bienes)	8	Alta	Riesgo de indisponibilidad de recursos necesarios para soportar la operación
URF_06_GF Inconsistencias en la liquidación, cargue y/o pago de la nómina	Gestión Financiera	Errores en el procesamiento de información de nómina	Operativa	Información financiera / actividad crítica	6	Media	Generación de reprocesos que afectan la oportunidad y confiabilidad de la operación financiera

Tabla 36 Ejemplo de vulnerabilidad

Etapas de evaluación de controles

La evaluación de controles existentes tiene como propósito determinar, de manera objetiva, en qué medida los controles registrados en el Sistema de Monitoreo de la Gestión Institucional – SMGI, contribuyen a reducir la exposición de los procesos críticos frente a los riesgos de interrupción, considerando las causas y vulnerabilidades previamente identificadas.

Dado que los controles en el SMGI ya se encuentran clasificados como preventivos, detectivos o correctivos, esta etapa no contempla su reclasificación, sino su análisis funcional, orientado a evaluar si estos controles:

- Atienden efectivamente la causa del riesgo
- Protegen el elemento afectado del proceso crítico
- Contribuyen a reducir la probabilidad o el impacto de la interrupción

El análisis se desarrolla a partir de la relación estructurada construida en las etapas anteriores:

- **Riesgo → Causa → Elemento afectado → Vulnerabilidad**

Sobre esta base, se evalúan los controles existentes con criterios objetivos que permitan determinar su contribución real a la continuidad.

Paso metodológico	Cómo se hace	Criterio objetivo de análisis	Resultado esperado
1. Identificación del control	Se toman del SMGI los controles asociados a cada riesgo	El control debe estar directamente vinculado al riesgo	Listado de controles por riesgo
2. Relación con la causa	Se analiza si el control actúa sobre la causa identificada	El control es pertinente si previene o mitiga la causa	Nivel de cobertura de la causa
3. Relación con el elemento afectado	Se evalúa si el control protege el recurso o actividad crítica afectada	El control es adecuado si protege el elemento identificado (información, sistema, recurso, actividad)	Nivel de protección del elemento
4. Análisis de aplicabilidad	Se verifica si el control se ejecuta en la operación real del proceso	El control debe ser aplicable en condiciones normales y en escenarios de interrupción	Condición de aplicabilidad
5. Evaluación de efectividad	Se contrasta el control con la información de monitoreo y riesgo residual en el SMGI	El control es efectivo si reduce la exposición del riesgo o contiene su materialización	Nivel de efectividad
6. Determinación de suficiencia	Se evalúa el conjunto de controles frente a la vulnerabilidad identificada	El conjunto es suficiente si cubre causas críticas y protege el proceso	Capacidad de respuesta actual

Tabla 37 Método para la evaluación de controles existentes

Criterios objetivos para evaluar los controles: La evaluación se realiza sobre variables observables que permiten determinar el aporte real del control.

Variable	Puntaje 1	Puntaje 2	Puntaje 3
Cobertura de la causa	No actúa sobre la causa	Actúa parcialmente	Actúa directamente sobre la causa crítica
Protección del elemento afectado	No protege el elemento	Protege parcialmente	Protege directamente el elemento afectado
Aplicabilidad operativa	No es aplicable o depende de condiciones externas	Aplicación parcial o no sistemática	Aplicación recurrente y verificable
Evidencia de efectividad	No hay evidencia de reducción del riesgo	Evidencia parcial	Evidencia clara en el monitoreo del SMGI

Tabla 38 Escala de evaluación de controles frente a la continuidad

Regla de decisión

- 4 a 6 puntos - Controles débiles (alta exposición residual)
- 7 a 9 puntos - Controles parcialmente suficientes
- 10 a 12 puntos - Controles suficientes

Con el fin de ilustrar la aplicación del método de evaluación de controles existentes, a continuación se presenta una tabla de ejemplo en la que se desarrollan, para algunos riesgos de interrupción asociados a procesos críticos, los seis puntos metodológicos definidos para esta etapa.

Nombre del riesgo	Proceso crítico afectado	Paso metodológico	Aplicación al caso	Resultado
URF_36_GI _Pérdida de integridad, disponibilidad o confidencialidad de la información	Gestión de la Información	1. Identificación del control	En el SMGI se encuentran asociados, entre otros, los siguientes controles: gestión de vulnerabilidades técnicas, copias de respaldo de la información, seguimiento a la gestión de la información digital y acuerdos de confidencialidad.	Se identifican controles directamente vinculados al riesgo.
		2. Relación con la causa	Las causas del riesgo incluyen debilidad en la asignación de controles de acceso, insuficiencia de pruebas de software y contraseñas sin protección. Los controles señalados actúan directamente sobre esas causas, especialmente los relativos a vulnerabilidades técnicas, controles de acceso y respaldo.	Cobertura directa de la causa principal.
		3. Relación con el elemento afectado	El elemento afectado corresponde a la información crítica y a los sistemas que soportan la gestión documental y digital del proceso. Los controles identificados protegen directamente dichos elementos.	Protección directa del elemento afectado.
		4. Análisis de aplicabilidad	En el monitoreo del primer cuatrimestre se evidencian actividades como seguimiento general al estado de organización documental y a la implementación del RID, FUID y RAI, lo que demuestra que los controles son aplicables en la operación real del proceso.	Control aplicable de manera real y verificable.
		5. Evaluación de efectividad	El mapa de riesgos indica que, después de la aplicación de controles, el riesgo residual se ubica en zona moderada , lo que evidencia reducción de la exposición, aunque no su eliminación total.	Existe evidencia de efectividad parcial-alta.
		6. Determinación de suficiencia	Con base en la cobertura de la causa, la protección del elemento afectado, su aplicabilidad y la evidencia de mitigación residual, se concluye que los controles son relevantes y funcionales, pero la persistencia del riesgo residual en zona moderada indica que requieren complemento desde el Plan de Continuidad.	Controles parcialmente suficientes para continuidad.

Tabla 39 Ejemplo método de evaluación de controles existentes

Valoración cuantitativa del ejemplo de evaluación de controles:

Variable de evaluación	Criterio aplicado al riesgo URF_36_GI	Puntaje
Cobertura de la causa	Los controles actúan directamente sobre causas como debilidad en controles de acceso, vulnerabilidades técnicas y respaldo de información.	3
Protección del elemento afectado	Los controles protegen directamente la información crítica y los sistemas del proceso de Gestión de la Información.	3
Aplicabilidad operativa	Los controles presentan evidencia de aplicación en el monitoreo institucional del proceso.	3
Evidencia de efectividad	El riesgo residual disminuye a zona moderada, lo que evidencia mitigación, aunque no control pleno.	2
Total		11

Tabla 40 Valoración cuantitativa del ejemplo de evaluación de controles

De acuerdo con la regla metodológica definida para esta etapa, un puntaje total de 11 ubica el conjunto de controles en el nivel de suficiente; sin embargo, desde la perspectiva de continuidad, el hecho de que el riesgo residual permanezca en zona moderada indica que, aunque los controles reducen de manera importante la exposición, todavía subsisten condiciones que justifican medidas complementarias en el Plan de Continuidad, especialmente por tratarse de un riesgo que afecta un proceso crítico y recursos esenciales para la operación institucional.

Este ejemplo permite evidenciar cómo la evaluación objetiva de los controles registrados en el SMGI aporta a la determinación de su suficiencia frente a la continuidad del proceso crítico y sirve de base para definir medidas complementarias en el Plan de Continuidad.

Etapas de definición de acciones

La definición de acciones de continuidad tiene como propósito establecer, de manera estructurada y verificable, las medidas que debe adoptar la Unidad para mantener o restablecer la operación de los procesos críticos ante la materialización de los riesgos de interrupción identificados y analizados en las etapas anteriores.

Esta etapa se desarrolla tomando como base:

- El riesgo y el proceso crítico afectado
- La causa y la vulnerabilidad identificada
- Los controles existentes y su nivel de suficiencia, y
- Las acciones de manejo y contingencia ya previstas en el SMGI.

Metodológicamente, esta etapa permite pasar del análisis a la respuesta operativa. Su función no es volver a describir el riesgo, sino definir qué acción debe ejecutarse, sobre qué elemento, con qué finalidad y en qué momento, para asegurar la continuidad del proceso crítico. En este sentido, las acciones de continuidad deben ser coherentes con las estrategias generales del Plan, que incluyen operación manual o degradada, reasignación de personal, respaldo y restauración de información, uso de medios alternos y coordinación interinstitucional.

La definición de acciones de continuidad se estructura a partir de la siguiente lógica metodológica:

Riesgo → Proceso crítico → Vulnerabilidad → Suficiencia de controles → Tipo de acción requerida → Acción de continuidad

Esta secuencia permite asegurar que cada acción quede técnicamente justificada y que su formulación responda a la exposición real del proceso crítico frente al riesgo, y no a una decisión discrecional.

Paso metodológico	Cómo se hace	Criterio objetivo de análisis	Resultado esperado
1. Identificación del riesgo y proceso crítico	Se toma el riesgo previamente priorizado y el proceso crítico afectado	El riesgo debe haber sido analizado en las etapas anteriores	Riesgo priorizado con trazabilidad al proceso crítico
2. Identificación de vulnerabilidad	Se toma la vulnerabilidad determinada en el análisis de causas	La vulnerabilidad debe expresar la condición que puede facilitar la interrupción	Punto específico que debe ser intervenido
3. Revisión de controles existentes	Se verifica el nivel de suficiencia del conjunto de controles	Si los controles son insuficientes o parcialmente suficientes, se requieren acciones complementarias	Necesidad de acción de continuidad identificada
4. Selección del tipo de acción	Se define el tipo de respuesta más adecuada frente al riesgo	La acción debe responder al elemento afectado y a la vulnerabilidad identificada	Acción alineada con la necesidad del proceso
5. Definición operativa de la acción	Se establece qué se hace, sobre qué recurso, con qué propósito y en qué momento	La acción debe ser clara, ejecutable y verificable	Acción formulada para el Plan
6. Integración al Plan de Continuidad	La acción se vincula con estrategias, procedimientos y responsables institucionales	La acción debe poder integrarse en la operación de contingencia y recuperación	Acción incorporada al esquema de continuidad

Tabla 41 Método para la definición de acciones de continuidad

La definición del tipo de acción requerida se realiza de manera objetiva mediante la combinación de tres variables ya definidas en etapas anteriores:

- Nivel de afectación en la continuidad del riesgo (crítico, alto o medio).
- Suficiencia de los controles existentes (suficientes, parcialmente suficientes o débiles).
- Elemento afectado del proceso crítico (información, sistemas, recursos físicos, actividades críticas o servicio).

La decisión metodológica se expresa así:

Tipo de acción requerida = función del nivel de afectación + suficiencia de controles + naturaleza del elemento afectado

Esta regla permite que la respuesta de continuidad se derive del análisis efectuado y no de una decisión intuitiva.

Nivel de afectación	Suficiencia de controles	Elemento afectado	Acción dominante	Acción complementaria sugerida
Crítico	Débiles o parcialmente suficientes	Información / sistemas	Contención + recuperación inmediata	Verificación + mejora
Crítico	Suficientes	Información / sistemas	Contención + recuperación + verificación	Preventiva de continuidad + mejora
Alto	Débiles o parcialmente suficientes	Recursos físicos / actividades críticas	Operación en contingencia + recuperación	Normalización + mejora
Alto	Suficientes	Recursos físicos / actividades críticas	Operación en contingencia	Preventiva de continuidad + normalización
Medio	Débiles	Actividades / procesos / servicio	Ajuste operativo + contención	Normalización + mejora
Medio	Suficientes o parcialmente suficientes	Actividades / procesos / servicio	Ajuste operativo	Preventiva de continuidad o normalización

Tabla 42 Regla de decisión para definir la acción dominante y sugerencia de la complementaria

Esta tabla define la acción dominante, pero no limita la incorporación de acciones complementarias de tipo preventivo, de normalización o de mejora, cuando el riesgo, el proceso crítico o el contexto operativo así lo requieran.

Una vez determinado el tipo de acción requerida, esta se formula dentro de una tipología homogénea que facilite su incorporación al Plan:

Tipo de acción	Propósito	Ejemplos de aplicación general en continuidad
Preventiva de continuidad	Reducir la exposición del proceso crítico frente a fallas futuras o fortalecer su resiliencia	Refuerzo de validaciones, aseguramiento adicional de respaldos, preparación de recursos alternos
Contención	Limitar el impacto del evento y evitar su propagación	Suspender accesos, aislar incidentes, detener la difusión de información incorrecta
Operación en contingencia	Mantener el funcionamiento mínimo del proceso durante la afectación	Operación manual o degradada, reasignación temporal de actividades, uso de medios alternos
Recuperación	Restablecer el recurso o la actividad afectada	Activar respaldos, restaurar sistemas, corregir información, reponer bienes
Normalización	Retornar a la operación ordinaria una vez controlado el evento	Verificar integridad, actualizar registros, formalizar cierre de contingencia
Mejora	Incorporar aprendizajes o ajustes para fortalecer la continuidad	Actualizar controles, ajustar procedimientos, retroalimentar el plan

Tabla 43 Tipología de acciones de continuidad

Esta tipología recoge de manera ordenada las estrategias y procedimientos ya previstos en el Plan, tales como operación en contingencia, respaldo y restauración, coordinación institucional, comunicación y retorno a la normalidad.

Una acción de continuidad queda correctamente formulada cuando responde a las cuatro preguntas siguientes:

1. ¿Qué se hace?
2. ¿Sobre qué elemento o recurso se aplica?
3. ¿Con qué propósito de continuidad se ejecuta?
4. ¿En qué momento se activa?

Fórmula metodológica de redacción = Acción concreta + elemento afectado + propósito de continuidad + momento o condición de activación

Ejemplos de redacción:

- Habilitar la última copia de respaldo de la información crítica, para restablecer su disponibilidad, cuando se presente indisponibilidad del sistema o pérdida de acceso. Esta lógica es coherente con las acciones de contingencia documentadas en el SMGI para el riesgo URF_36_GI.

- Suspender de manera inmediata los accesos comprometidos, para contener la afectación sobre la confidencialidad de la información, cuando se detecte un incidente de seguridad. Esto también se encuentra alineado con las acciones de contingencia registradas para el riesgo URF_36_GI.

Variable metodológica	Resultado
Riesgo	URF_36_GI – Pérdida de integridad, disponibilidad o confidencialidad de la información
Proceso crítico afectado	Gestión de la Información
Vulnerabilidad	Exposición a pérdida o indisponibilidad de información esencial para la operación
Nivel de afectación	Crítico
Suficiencia de controles	Parcialmente suficientes
Elemento afectado	Información crítica / sistemas
Regla aplicada	Crítico + controles parcialmente suficientes + información/sistemas
Acción dominante	Contención + recuperación inmediata
Acción complementaria	Verificación / mejora
Acción formulada	Suspender accesos comprometidos y habilitar la última copia de respaldo cuando se detecte afectación a la disponibilidad, integridad o confidencialidad.

Tabla 44 Ejemplo de análisis de riesgos

De esta manera, la definición de acciones de continuidad se configura como una etapa metodológica orientada a traducir el análisis técnico del riesgo en medidas concretas para mantener o restablecer la operación de los procesos críticos. Su valor dentro del Plan de Continuidad radica en que permite seleccionar, con criterios objetivos, la acción dominante requerida, complementar la respuesta con medidas de prevención, normalización o mejora, y asegurar su articulación con las estrategias institucionales de contingencia, recuperación y retorno a la normalidad previstas en el Plan.

9.3.4. Resultados institucionales de riesgos de interrupción

Los resultados integran los riesgos del SMGI con su impacto en los procesos críticos, las vulnerabilidades, la suficiencia de controles y las acciones de continuidad, asegurando una respuesta coherente frente a la interrupción.



Categoría de interrupción	Código y nombre del riesgo	Proceso crítico afectado	Nivel de afectación	Vulnerabilidad identificada	Suficiencia de controles	Acción dominante	Acción complementaria	Acción de continuidad (formulada)
Tecnología e información	URF_36_GI – Pérdida de integridad, disponibilidad o confidencialidad de la información	Gestión de la Información / Desarrollo de estudios y proyección normativa	Crítico	Exposición a pérdida o indisponibilidad de información crítica	Suficientes*	Contención + recuperación + verificación	Preventiva + mejora	Suspender accesos comprometidos y habilitar la última copia de respaldo para restablecer la información; posteriormente verificar su integridad y fortalecer controles de seguridad
	URF_26_GI – Desorganización de archivos físicos y electrónicos	Gestión de la Información	Alto	Pérdida de trazabilidad y acceso a información institucional	Parcialmente suficientes	Operación en contingencia + recuperación	Normalización + mejora	Implementar repositorios alternos y reorganizar la información crítica para garantizar la continuidad del proceso
Recursos físicos y servicios	URF_28_AD – Pérdida, daño o deterioro de bienes	Dirección y Planeación / Adquisición de bienes y servicios	Alto	Indisponibilidad de recursos físicos necesarios para la operación	Parcialmente suficientes	Operación en contingencia + recuperación	Normalización + mejora	Activar recursos alternos y gestionar la reposición o recuperación del bien afectado
	URF_21_AD – Incumplimiento en la ejecución contractual	Dirección y Planeación / Adquisición de bienes y servicios	Alto	Dependencia de bienes o servicios contratados	Parcialmente suficientes	Operación en contingencia + recuperación	Preventiva + normalización	Implementar alternativas operativas temporales y gestionar proveedores alternos o ajustes contractuales
	URF_24_AD – Retrasos en la suscripción de contratos	Dirección y Planeación / Adquisición de bienes y servicios	Alto	Demora en disponibilidad de recursos contractuales	Parcialmente suficientes	Operación en contingencia	Preventiva + normalización	Reprogramar actividades críticas y activar mecanismos alternos de provisión cuando se presenten retrasos contractuales



Categoría de interrupción	Código y nombre del riesgo	Proceso crítico afectado	Nivel de afectación	Vulnerabilidad identificada	Suficiencia de controles	Acción dominante	Acción complementaria	Acción de continuidad (formulada)
Procesos administrativos	URF_06_GF – Inconsistencias en la liquidación, cargue y/o pago de la nómina	Gestión Financiera	Medio	Reprocesos que afectan la oportunidad y confiabilidad del proceso	Parcialmente suficientes	Ajuste operativo	Preventiva + normalización	Aplicar validaciones extraordinarias y realizar ajustes o reintegros frente a inconsistencias detectadas
	URF_07_GF – Inoportunidad en la presentación de información financiera	Gestión Financiera	Alto	Riesgo de incumplimiento normativo por retrasos	Parcialmente suficientes	Operación en contingencia + normalización	Mejora	Priorizar la elaboración y envío de reportes mediante mecanismos alternos cuando exista riesgo de incumplimiento
	URF_05_RV – Incumplimiento en tiempos de respuesta a PQRS	Control y Evaluación	Medio	Afectación en la atención al ciudadano	Parcialmente suficientes	Ajuste operativo	Preventiva + normalización	Priorizar y gestionar respuestas urgentes mediante canales alternos
	URF_02_GC – Divulgación de información inoportuna, confusa o poco confiable	Dirección y Planeación / Gestión de comunicaciones	Medio	Riesgo de desinformación institucional	Parcialmente suficientes	Ajuste operativo	Normalización + mejora	Corregir y comunicar información oficial ajustada cuando se identifiquen errores
	URF_25_EJ_PN – Citación inadecuada de fuentes en documentos técnicos y estudios	Desarrollo de Estudios y Proyección Normativa	Medio	Afectación a la calidad técnica de productos	Parcialmente suficientes	Ajuste operativo	Preventiva + mejora	Corregir el documento técnico y reforzar controles de revisión antes de su emisión

Tabla 45 Resultados institucionales de riesgos de interrupción

Los resultados evidencian que:

- Los riesgos críticos se concentran en información y tecnología, afectando transversalmente la operación
- Los riesgos altos están asociados a recursos físicos y servicios
- Predominan controles parcialmente suficientes, lo que implica necesidad de acciones de continuidad
- Las vulnerabilidades se relacionan principalmente con:
 - dependencia tecnológica
 - dependencia de recursos
 - debilidades operativas

El análisis de riesgos de interrupción desarrollado en este numeral integra de manera coherente los riesgos del SMGI con los procesos críticos definidos en el BIA, permitiendo identificar vulnerabilidades, evaluar la suficiencia de los controles y establecer acciones de continuidad basadas en criterios objetivos. Este enfoque garantiza la trazabilidad del análisis y la consistencia metodológica entre el diagnóstico y la respuesta operativa, constituyéndose en un insumo clave para la definición de estrategias y procedimientos del Plan de Continuidad.

9.4. Estrategias de continuidad

Las estrategias de continuidad definen el enfoque institucional de respuesta que debe adoptar la Unidad para mantener o restablecer la operación de sus procesos críticos frente a la materialización de riesgos de interrupción.

Estas se formulan en coherencia con los resultados del Análisis de Impacto al Negocio (BIA) y del análisis de riesgos desarrollado en el numeral 8.3, con el fin de garantizar la continuidad de la operación dentro de los tiempos de recuperación definidos (RTO), sin superar los niveles de pérdida de información aceptables (RPO) y asegurando el cumplimiento de los niveles mínimos de operación.

9.4.1. Enfoque metodológico de las estrategias

Desde el punto de vista metodológico, las estrategias no corresponden a actividades individuales ni a pasos operativos; las estrategias representan el enfoque de respuesta institucional frente a un tipo de interrupción, se definen a partir de la agrupación de las acciones de continuidad identificadas en el análisis de riesgos, organizándolas según el tipo de respuesta requerida.

En este sentido:

- las acciones de continuidad corresponden a la ejecución concreta frente a un riesgo específico
- las estrategias de continuidad corresponden al marco de respuesta que orienta cómo actúa la Unidad

De esta manera, una misma estrategia puede materializarse en diferentes acciones, dependiendo del proceso crítico afectado, el tipo de vulnerabilidad y el escenario de interrupción. Este enfoque garantiza la trazabilidad entre el análisis de riesgos y la respuesta institucional.

9.4.2. Metodología para la construcción de estrategias

Las estrategias de continuidad se construyen a partir de los resultados del análisis desarrollado en el numeral 8.3, mediante un proceso estructurado que permite transformar los riesgos y sus acciones asociadas en enfoques de respuesta institucional.

Paso	Elemento de entrada	Análisis requerido	Resultado	Ejemplo
1. Identificación del riesgo	Riesgos de interrupción (8.3)	Determinar qué evento afecta la continuidad del proceso crítico	Riesgo caracterizado	Pérdida de información
2. Identificación de acciones	Acciones de continuidad (acción dominante, complementaria o formulada)	Identificar qué se hace frente al riesgo	Acciones definidas	Restaurar backup, validar datos
3. Clasificación del tipo de respuesta	Acciones identificadas	Clasificar según su finalidad: prevenir, contener, contingencia, recuperar, normalizar o mejorar	Clasificación del tipo de respuesta (preventiva, contención, contingencia, recuperación, etc.)	Recuperación
4. Agrupación de acciones	Conjunto de acciones clasificadas	Agrupar acciones que responden de manera similar frente al riesgo	Grupo de acciones homogéneas	Restauración + verificación
5. Definición de la estrategia	Grupo de acciones	Formular el enfoque de respuesta en términos estratégicos (no operativos)	Estrategia formulada en términos de enfoque (no operativo)	Recuperación de información

Tabla 46 Metodología para la construcción de estrategias de continuidad

Estrategia de continuidad = agrupación de acciones de continuidad según el tipo de respuesta requerida frente a la interrupción.

La metodología anterior permite garantizar que las estrategias:

- No se definan de manera aislada
- Respondan directamente al análisis de riesgos
- Mantengan coherencia entre diagnóstico y respuesta

9.4.3. Criterios para la definición de estrategias

Los siguientes criterios orientan la selección y priorización de las estrategias definidas. La formulación de cada estrategia se realiza considerando:

- Nivel de afectación del riesgo
- Suficiencia de los controles existentes
- Tipo de elemento afectado
- Tiempo máximo tolerable de interrupción (MTD)
- RTO y RPO definidos en el BIA

Estos criterios garantizan que la estrategia esté alineada con la realidad operativa de los procesos críticos y con la capacidad institucional de respuesta.

9.4.4. Tipología de estrategias de continuidad

Las estrategias se organizan según el tipo de respuesta requerida frente a la interrupción:

Tipo de estrategia	Propósito	Momento de aplicación
Preventiva de continuidad	Reducir la exposición y fortalecer la resiliencia	Antes de la interrupción
Contención	Limitar el impacto del evento	Durante el evento
Operación en contingencia	Mantener el funcionamiento mínimo	Durante la interrupción
Recuperación	Restablecer la operación	Después del evento
Normalización	Retornar a condiciones normales	Fase de cierre
Mejora	Incorporar lecciones aprendidas	Posterior al evento

Tabla 47 Tipología de estrategias de continuidad

9.4.5. Estructuración de las estrategias por categorías de interrupción

Las estrategias de continuidad, una vez construidas a partir del análisis de riesgos conforme a la metodología definida en el numeral 8.4.2, se organizan por categoría de interrupción con el fin de facilitar su aplicación y garantizar coherencia en la respuesta institucional frente a los diferentes tipos de afectación.

Categoría de interrupción	Tipo predominante	Enfoque de la estrategia	Objetivo de continuidad	Estrategias principales	Procesos críticos asociados	Resultados esperados
Tecnología e información	Recuperación / Contención	Asegurar la disponibilidad, integridad y acceso a la información y sistemas institucionales	Garantizar que los procesos críticos continúen operando sin pérdida significativa de información ni indisponibilidad tecnológica	- Activación de copias de respaldo de información - Recuperación de sistemas críticos - Implementación de accesos alternos - Refuerzo de controles de seguridad de la información - Verificación de integridad de datos	Gestión de la Información Desarrollo de Estudios y Proyección Normativa	Restablecimiento de la operación tecnológica en tiempos definidos (RTO), sin superar niveles de pérdida aceptables (RPO), garantizando continuidad operativa
Recursos físicos y servicios	Contingencia	Garantizar la disponibilidad de infraestructura, bienes y servicios necesarios para la operación	Mantener la operación mediante el uso de recursos alternos y asegurar la reposición o disponibilidad oportuna de recursos críticos	- Activación de recursos físicos alternos - Reasignación de bienes y equipos - Gestión de proveedores alternos - Reposición o recuperación de activos - Ajustes en la provisión de servicios	Dirección y Planeación Adquisición de Bienes y Servicios	Continuidad operativa mediante recursos sustitutos, evitando la paralización de actividades críticas
Procesos administrativos	Contingencia /	Asegurar la continuidad de	Mantener la operación mediante	- Priorización de actividades	Gestión Financiera Control y	Continuidad del servicio y cumplimiento

Categoría de interrupción	Tipo predominante	Enfoque de la estrategia	Objetivo de continuidad	Estrategias principales	Procesos críticos asociados	Resultados esperados
	Normalización	actividades críticas, cumplimiento normativo y prestación del servicio	ajustes operativos y priorización de actividades clave	críticas - Reprogramación de tareas - Aplicación de validaciones extraordinarias - Uso de canales alternos de atención - Ajustes en productos o entregables	Evaluación Dirección y Planeación Gestión de Comunicaciones Desarrollo Normativo	de obligaciones institucionales, minimizando reprocesos y afectaciones reputacionales

Tabla 48 Estrategias de continuidad por categoría de interrupción

Las estrategias de continuidad establecidas permiten estructurar una respuesta institucional coherente frente a los riesgos de interrupción, asegurando la alineación entre el análisis realizado y las medidas necesarias para mantener o restablecer la operación de los procesos críticos, sirviendo como base para el desarrollo de los procedimientos operativos definidos en el siguiente numeral.

9.4.6. Resultados institucionales de las estrategias de continuidad

Los siguientes resultados institucionales corresponden a la aplicación de las estrategias de continuidad, en términos de la capacidad de la Unidad para mantener y restablecer la operación:

Componente de análisis	Resultado institucional de la estrategia	Base metodológica de referencia	Efecto esperado en la continuidad
Procesos críticos priorizados	La Unidad cuenta con estrategias orientadas a mantener o restablecer la operación de los procesos críticos identificados: Gestión Financiera, Gestión de la Información, Desarrollo de Estudios y Proyección Normativa, Dirección y Planeación, y Control y Evaluación.	Procesos críticos definidos en el BIA.	Priorización de la respuesta institucional frente a interrupciones.

Componente de análisis	Resultado institucional de la estrategia	Base metodológica de referencia	Efecto esperado en la continuidad
Tiempos de recuperación	Las estrategias se orientan a restablecer los procesos dentro de los tiempos definidos para cada proceso crítico, por ejemplo 2 horas para Gestión Financiera, 1 hora para Gestión de la Información y 24 horas para Desarrollo de Estudios y Proyección Normativa, Dirección y Planeación y Control y Evaluación.	RTO final definido en el BIA.	Recuperación oportuna de la operación institucional.
Pérdida de información aceptable	Las estrategias consideran medidas para mantener la pérdida de información dentro de los límites aceptables, por ejemplo 30 minutos para Gestión Financiera, 15 minutos para Gestión de la Información, 4 horas para Desarrollo de Estudios y Proyección Normativa y 6 horas para Dirección y Planeación y Control y Evaluación.	RPO final definido en el BIA.	Protección de la información crítica y reducción de reprocesos.
Operación mínima durante la interrupción	Las estrategias permiten sostener las actividades esenciales, productos y personal mínimos definidos para cada proceso crítico.	Niveles mínimos de operación (NMO).	Continuidad funcional de los procesos en escenarios de contingencia.
Disponibilidad de recursos esenciales	Las estrategias contemplan el uso y aseguramiento de recursos humanos, tecnológicos, de información crítica, físicos, de comunicación y soporte externo requeridos por los procesos críticos.	Recursos esenciales por proceso crítico.	Viabilidad operativa de la continuidad y recuperación.
Respuesta frente a interrupciones tecnológicas y de información	La Unidad consolida estrategias orientadas a respaldo, restauración, acceso alternativo y protección de la información para riesgos que afectan disponibilidad, integridad o confidencialidad. Esta necesidad es consistente con riesgos como URF_36_GI, que puede generar pérdida de memoria institucional, paralización de procesos e interrupción del servicio. ,	Riesgos de interrupción de tecnología e información. ,	Capacidad de recuperación tecnológica y documental.
Respuesta frente a interrupciones por recursos físicos y servicios	La Unidad consolida estrategias orientadas al uso de recursos alternos, provisión sustituta y reposición o recuperación de activos frente a riesgos asociados a bienes y servicios. Esto es consistente con riesgos como URF_28_AD y URF_21_AD, cuyos efectos incluyen retrasos, afectación operativa e indisponibilidad de bienes o servicios.	Riesgos de interrupción por recursos físicos y servicios.	Continuidad operativa mediante recursos de soporte alternativos.

Componente de análisis	Resultado institucional de la estrategia	Base metodológica de referencia	Efecto esperado en la continuidad
Respuesta frente a interrupciones en procesos administrativos	La Unidad consolida estrategias orientadas a priorización de actividades, ajustes operativos, validaciones extraordinarias y mecanismos alternos de atención, frente a riesgos que pueden generar reprocesos, incumplimientos o afectación del servicio, como URF_06_GF, URF_07_GF, URF_05_RV y URF_25_EJ_PN.	Riesgos de interrupción en procesos administrativos.	Continuidad del servicio, del cumplimiento normativo y de la calidad de los productos institucionales.
Articulación institucional de la respuesta	Las estrategias institucionales de continuidad y recuperación son un producto esperado del plan y se complementan con los procedimientos de activación, respuesta y recuperación, así como con la estructura de roles y responsabilidades y el inventario de recursos críticos.	Productos esperados del plan y estructura general del PCN.	Respuesta coordinada, trazable y verificable frente a eventos disruptivos.
Fortalecimiento de la resiliencia institucional	Las estrategias se orientan a garantizar la prestación continua de las funciones misionales, proteger la información y los activos institucionales y asegurar un retorno ordenado, oportuno y eficiente a la normalidad.	Objetivo general y alcance del plan.	Mayor capacidad institucional de prevención, respuesta y recuperación.

Tabla 49 Resultados institucionales de las estrategias de continuidad

9.5. Procedimientos de respuesta y recuperación

Los procedimientos de respuesta y recuperación constituyen el componente operativo del Plan de Continuidad del Negocio (PCN). Su propósito es establecer las acciones secuenciales, responsables, recursos y mecanismos de coordinación necesarios para activar el plan, gestionar incidentes, operar en contingencia y retornar a la normalidad, garantizando la continuidad de los procesos críticos dentro de los tiempos definidos en el BIA (RTO/RPO).

Estos procedimientos se estructuran en cuatro fases:

- Activación del plan
- Respuesta inicial y gestión del incidente
- Operación en contingencia
- Recuperación y retorno a la normalidad

Cada fase incluye actividades específicas, responsables institucionales y criterios de escalamiento.

9.5.1. Activación del plan

La activación del PCN se realiza cuando un evento disruptivo afecta o puede afectar la operación de uno o más procesos críticos. La activación puede ser:

- Automática, cuando el incidente genera indisponibilidad inmediata de recursos esenciales.
- Por decisión del Equipo de Continuidad, cuando el impacto potencial supera la capacidad operativa normal.
- Por instrucción del Comité Institucional de Gestión y Desempeño, en eventos de alto impacto institucional.

Procedimiento de activación:

Actividad	Descripción ampliada	Responsable	Tiempo de gestión	Resultado esperado
1. Detección del incidente	Identificación de cualquier evento, anomalía, falla tecnológica, indisponibilidad de infraestructura, ausencia de personal crítico o afectación operativa que pueda comprometer la continuidad de un proceso crítico. Incluye incidentes reportados por terceros o proveedores.	Cualquier servidor	Inmediato	Incidente detectado y comunicado sin retrasos.
2. Notificación inicial	Comunicación inmediata al líder del proceso afectado y al proceso de Direccionamiento y Planeación, proporcionando información básica: qué ocurrió, cuándo, qué recursos están afectados y si hay impacto visible.	Servidor que detecta el incidente	< 10 minutos	Activación del protocolo de evaluación preliminar.
3. Evaluación preliminar	Análisis rápido del incidente para determinar su severidad, alcance, procesos afectados, riesgos asociados y si compromete los tiempos definidos en el BIA. Incluye verificación con Gestión de la Información cuando hay afectación tecnológica.	Líder del proceso + Direccionamiento y Planeación	< 30 minutos	Diagnóstico inicial claro y documentado.
4. Decisión de activación	Determinación formal de activar el PCN cuando el incidente supera la capacidad operativa normal o afecta recursos esenciales. La decisión se basa en criterios	Direccionamiento y Planeación	< 15 minutos	Activación oficial del PCN.

Actividad	Descripción ampliada	Responsable	Tiempo de gestión	Resultado esperado
	definidos: impacto, severidad, riesgo de incumplimiento legal o afectación misional.			
5. Convocatoria del Equipo de Continuidad	Llamado inmediato a los integrantes del Equipo de Continuidad mediante canales oficiales (correo, Teams, teléfono), indicando tipo de incidente, nivel de activación y acciones iniciales requeridas.	Direccionamiento y Planeación	< 15 minutos	Equipo de Continuidad reunido y operativo.
6. Comunicación inicial	Emisión de mensaje oficial a servidores, directivos y partes interesadas, informando la activación del PCN, instrucciones iniciales y canales de comunicación habilitados.	Gestión de Comunicaciones	< 30 minutos	Información clara y oportuna para toda la entidad.

Tabla 50 Procedimiento de activación del plan

La activación del Plan de Continuidad del Negocio constituye el punto de partida para una respuesta organizada, oportuna y proporcional al nivel de afectación generado por el incidente. Una vez emitida la decisión de activación, el proceso de Direccionamiento y Planeación asume la coordinación integral de las acciones iniciales, garantizando la articulación entre los líderes de proceso, el Equipo de Continuidad y las áreas de soporte institucional.

Esta fase asegura que la Entidad cuente con información clara, roles definidos y mecanismos de comunicación efectivos para iniciar la gestión del incidente bajo un marco de control, trazabilidad y alineación con los tiempos establecidos en el BIA, permitiendo así una transición ordenada hacia las fases de respuesta, operación en contingencia y recuperación.

9.5.2. Respuesta inicial y gestión del incidente

Una vez activado el plan, se ejecutan las acciones inmediatas para contener el impacto y asegurar la continuidad mínima.

Actividad	Descripción	Responsable	Tiempo de gestión	Resultado esperado
Verificación de afectación	Confirmar impacto real sobre procesos críticos.	Líder del proceso	< 1 hora	Diagnóstico inicial validado.

Actividad	Descripción	Responsable	Tiempo de gestión	Resultado esperado
Activación de suplencias	Activar personal alternativo según el BIA.	Líder del proceso	< 1 hora	Continuidad operativa mínima garantizada.
Aseguramiento de recursos esenciales	Garantizar disponibilidad de tecnología, información y logística.	Gestión de la Información + Subdirección Jurídica y Gestión Institucional	< 2 horas	Recursos críticos disponibles.
Implementación de controles iniciales	Acciones para contener el impacto del incidente.	Equipo de Continuidad	< 2 horas	Riesgo inicial mitigado.
Escalamiento	Definir si el incidente requiere intervención de alta dirección.	Direccionamiento y Planeación	Según severidad	Decisiones oportunas y trazables.

Tabla 51 Matriz de actividades de respuesta inicial y gestión del incidente

La fase de respuesta inicial y gestión del incidente garantiza que la URF actúe de manera inmediata, coordinada y basada en información verificable ante cualquier afectación operativa. Durante esta etapa, los líderes de proceso y el Equipo de Continuidad ejecutan acciones orientadas a contener el impacto, estabilizar la operación y asegurar la disponibilidad de los recursos esenciales definidos en el BIA.

El proceso de Direccionamiento y Planeación mantiene la coordinación integral de las actividades, asegurando que las decisiones se adopten con criterios técnicos, trazabilidad y alineación con los tiempos máximos de recuperación establecidos.

Esta fase permite establecer las condiciones mínimas para la continuidad operativa y prepara a la Entidad para una transición ordenada hacia la operación en contingencia, evitando la ampliación del impacto y preservando la integridad de la información, los servicios y los activos institucionales.

9.5.3. Operación en contingencia

La matriz de operación en contingencia establece las actividades necesarias para garantizar los Niveles Mínimos de Operación (NMO) durante una interrupción, detallando las acciones, responsables y tiempos que permiten sostener la continuidad institucional bajo condiciones adversas.

Actividad	Descripción ampliada	Responsable	Tiempo de gestión	Resultado esperado
Activación de procedimientos alternos	Implementación inmediata de los procedimientos alternos definidos por cada proceso crítico en el BIA. Incluye operación manual, uso de plantillas, repositorios espejo, mecanismos alternos de aprobación, flujos simplificados y cualquier medida diseñada para garantizar los NMO.	Líder del proceso	Inmediato tras activación del PCN	Continuidad operativa mínima garantizada sin interrupciones críticas.
Uso de recursos alternos	Activación de recursos alternos definidos en el PCN: equipos de respaldo, VPN, accesos remotos, repositorios duplicados, infraestructura alterna, canales de comunicación alternos y redundancias tecnológicas.	Gestión de la Información	< 1 hora	Recursos esenciales disponibles y funcionales para operar en contingencia.
Implementación de estrategias de continuidad	Aplicación de las estrategias operativas, tecnológicas, logísticas y de personal definidas en el numeral 8.4, según el tipo de interrupción. Incluye activación de suplencias, redistribución de cargas, uso de infraestructura alterna y priorización de recursos.	Equipo de Continuidad + Líder del proceso	Durante toda la contingencia	Estrategias aplicadas de manera coherente con el análisis de riesgos y el BIA.
Priorización de actividades esenciales	Ejecución exclusiva de actividades esenciales definidas en el BIA, suspendiendo temporalmente actividades no críticas para evitar sobrecarga operativa y garantizar el cumplimiento de los RTO.	Líder del proceso	Durante toda la contingencia	NMO garantizados sin comprometer recursos críticos.
Comunicación permanente	Establecimiento de comunicación continua con el Equipo de Continuidad para reportar novedades, riesgos emergentes, cambios en la disponibilidad de recursos y decisiones operativas.	Líder del proceso + Equipo de Continuidad	Cada 2 horas o según necesidad	Flujo de información oportuno y trazable para la toma de decisiones.

Actividad	Descripción ampliada	Responsable	Tiempo de gestión	Resultado esperado
Registro de acciones ejecutadas	Documentación detallada de todas las acciones realizadas, decisiones adoptadas, tiempos, responsables y resultados. Este registro alimenta la trazabilidad del incidente y la evaluación posterior.	Equipo de Continuidad	Durante toda la contingencia	Registro completo y verificable del manejo del incidente.
Evaluación periódica de estabilidad	Revisión continua del estado de los recursos, la efectividad de los procedimientos alternos, la estabilidad de la operación y la necesidad de ajustar estrategias.	Direccionamiento y Planeación + Líder del proceso	Cada 4 horas o según criticidad	Confirmación de que la operación en contingencia se mantiene estable y controlada.

Tabla 52 Matriz de operación en contingencia

La permanencia de operación en contingencia depende de la evaluación continua de riesgos y condiciones técnicas que puedan comprometer la estabilidad del proceso. Por ello, los siguientes criterios para mantener la operación en contingencia definen los umbrales que determinan si la Entidad debe continuar aplicando los procedimientos alternos o si existen condiciones suficientes para iniciar el retorno a la normalidad.

Criterio	Descripción ampliada	Implicación operativa
Indisponibilidad de recursos críticos	Persistencia de fallas en infraestructura, sistemas, personal crítico, proveedores esenciales o accesos necesarios para operar normalmente.	Se mantienen procedimientos alternos y estrategias de continuidad.
Riesgo de pérdida de información superior al RPO	Existencia de riesgo de pérdida de datos que supere el punto máximo aceptable definido en el BIA.	No se puede retornar a la normalidad hasta garantizar integridad de la información.
Riesgo de incumplimiento legal o regulatorio	Persistencia de condiciones que puedan generar incumplimientos normativos, contractuales o regulatorios.	Se priorizan actividades esenciales y se mantienen controles reforzados.
Afectación a la seguridad de la información o infraestructura	Riesgos activos relacionados con ciberseguridad, accesos no autorizados, fallas de integridad, disponibilidad o confidencialidad.	Se mantiene contingencia hasta eliminar riesgos residuales.

Tabla 53 Matriz de criterios para mantener la operación en contingencia

La operación en contingencia permite a la URF mantener la continuidad de sus procesos críticos bajo condiciones adversas, asegurando los Niveles Mínimos de

Operación definidos en el BIA. En esta fase, las estrategias de continuidad, los procedimientos alternos, los recursos redundantes y la priorización de actividades esenciales se convierten en los mecanismos clave para sostener la estabilidad institucional y evitar que el incidente genere un impacto mayor.

9.5.4. Recuperación y retorno a la normalidad

La fase de recuperación inicia cuando el incidente ha sido controlado y existen condiciones seguras para restablecer la operación normal. A partir de este momento, la recuperación se desarrolla siguiendo la secuencia de actividades definida para garantizar un retorno ordenado y estable.

Actividad	Descripción	Responsable	Tiempo de gestión	Resultado esperado
Verificación de restauración	Confirmación de que los recursos tecnológicos, documentales, logísticos y de infraestructura han sido completamente restablecidos y funcionan de manera estable.	Gestión de la Información + Líder del proceso	< 4 horas	Condiciones listas para retorno.
Validación de integridad de información	Verificación de que la información recuperada no presenta pérdidas superiores al RPO y que los respaldos son íntegros y consistentes.	Gestión de la Información	< 2 horas	Información segura y validada.
Restablecimiento gradual	Retorno progresivo a los procedimientos normales, priorizando procesos críticos según su RTO y verificando estabilidad operativa en cada fase.	Líder del proceso	Según RTO	Operación normal restablecida.
Desactivación de procedimientos alternos	Cierre formal de la operación en contingencia y reactivación de los procedimientos habituales.	Líder del proceso	< 1 hora	Procedimientos normales reactivados.
Comunicación de cierre	Emisión de mensaje oficial informando el retorno a la normalidad, instrucciones finales y próximos pasos.	Gestión de Comunicaciones	< 30 minutos	Servidores informados y alineados.

Tabla 54 Matriz de criterios para mantener la operación en contingencia

La fase de recuperación y retorno a la normalidad asegura que la URF restablezca su operación habitual de manera ordenada, segura y verificable, una vez superadas las condiciones que dieron origen a la contingencia. Este cierre operativo permite confirmar la estabilidad de los procesos críticos, la integridad de

la información y la disponibilidad plena de los recursos esenciales, dejando a la Entidad en condiciones de retomar sus actividades regulares y avanzar hacia la evaluación posterior del incidente y la mejora continua del PCN.

El retorno a la normalidad solo se declara oficialmente cuando todos los criterios de la siguiente lista de verificación han sido cumplidos:

Criterio	Verificación	Responsable
Verificación de sistemas	¿Todos los sistemas críticos están operando normalmente (SIIF, SGEDA, correo, VPN)?	Gest. Información / MHCP
Integridad de información	¿Se verificó la integridad de los datos (sin pérdida, corrupción ni inconsistencias)?	Gest. Información
Nómina y pagos	¿No hay pagos pendientes ni inconsistencias en registros financieros?	Gestión Financiera
PQRSD y atención ciudadana	¿Se atendieron las solicitudes represadas durante la contingencia?	Relación con la Ciudadanía / Control y Evaluación
Comunicación de cierre	¿Se emitió comunicado de cierre a grupos de valor internos y externos?	Dir. General / Gestión de Comunicaciones
Registro del incidente	¿Se documentó el evento, las acciones y el tiempo de recuperación en el SMGI?	Coordinador PCN

Tabla 55 Matriz de validación para retorno a la normalidad

9.5.5. Evaluación posterior al incidente

Una vez finalizado el evento, se realiza una evaluación integral para identificar oportunidades de mejora.

Actividad	Descripción	Responsable	Tiempo de gestión	Resultado esperado
Análisis de causas	Identificar causas raíz del incidente.	Equipo de Continuidad	< 5 días	Causas documentadas en el SMGI de acuerdo con la metodología institucional .
Evaluación de efectividad	Analizar desempeño del PCN durante el evento.	Dirección y Planeación	< 7 días	Brechas identificadas.
Recomendaciones de mejora	Proponer ajustes al PCN.	Control y Evaluación	< 10 días	Acciones de mejora definidas y documentadas en el módulo de mejoras del SMGI, de acuerdo con los lineamientos de plan de mejoramiento.

Actividad	Descripción	Responsable	Tiempo de gestión	Resultado esperado
Actualización del PCN	Incorporar lecciones aprendidas.	Dirección y Planeación	< 15 días	PCN actualizado.

Tabla 56 Matriz de actividades de evaluación posterior al incidente

9.5.6. Roles en los procedimientos de respuesta y recuperación

El cumplimiento de los procedimientos de respuesta y recuperación requiere una definición clara de los roles institucionales y de sus responsabilidades operativas durante cada fase del incidente.

En coherencia con la estructura de gobernanza establecida en el numeral de roles y responsabilidades, este apartado presenta la matriz que asigna funciones específicas a los actores involucrados en la activación del Plan, la gestión del incidente, la operación en contingencia y el retorno a la normalidad.

Rol	Responsabilidades principales
Coordinador del PCN (Dirección y Planeación)	Activación del plan, coordinación general, toma de decisiones, reporte a la alta dirección.
Líder del proceso afectado	Evaluación del impacto, activación de suplencias, ejecución de procedimientos alternos.
Equipo de Continuidad	Gestión operativa del incidente, soporte técnico y logístico, seguimiento.
Gestión de la Información	Restauración tecnológica, respaldo y recuperación de datos.
Gestión de Comunicaciones	Mensajes oficiales, comunicación interna y externa.
Control y Evaluación	Verificación independiente posterior al incidente.

Tabla 57 Matriz de roles y responsabilidades para los procedimientos de respuesta y recuperación

9.5.7. Resultados institucionales de procedimientos de respuesta y recuperación para los procesos críticos

La gestión de un incidente exige que cada proceso crítico cuente con lineamientos claros para su respuesta, operación en contingencia y recuperación. Este numeral presenta la matriz consolidada que reúne, en un solo instrumento, las actividades esenciales que deben ejecutar los procesos críticos de la URF en cada fase del

incidente, incluyendo las acciones de respuesta inicial y de recuperación necesarias para restablecer la operación.

Proceso crítico	Actividad	Descripción	Responsable	Tiempo	Resultado esperado
Gestión Financiera	Verificación de plataformas financieras	Validar disponibilidad de SIIF, SECOP, bancos y sistemas de pago.	Líder del proceso	< 1 hora	Diagnóstico del impacto financiero.
	Activación de suplencias	Activar personal alterno para garantizar pagos y registros.	Líder del proceso	Inmediato	Continuidad mínima asegurada.
	Mecanismos manuales de operación	Uso de formatos manuales para compromisos, obligaciones y pagos.	Equipo financiero	Durante contingencia	Flujo financiero básico garantizado.
	Restablecimiento de plataformas	Reactivar sistemas financieros y accesos.	Gestión de la Información	< 4 horas	Sistemas operativos.
	Validación de integridad de registros	Verificar consistencia de datos y registros.	Gestión Financiera	< 6 horas	Información íntegra.
	Normalización de trámites	Registrar pendientes y actualizar sistemas.	Equipo financiero	Según carga	Operación normalizada.
Gestión de la Información	Diagnóstico de afectación tecnológica	Identificar sistemas, redes o accesos afectados.	Gestión de la Información	< 1 hora	Mapa de afectación.
	Activación de respaldos	Activar copias de seguridad o repositorios espejo.	Equipo TI	Inmediato	Información disponible.
	Accesos alternos	Habilitar VPN, escritorios remotos o servidores alternos.	Gestión de la Información	< 2 horas	Continuidad tecnológica mínima.
	Restauración de servicios	Reactivar servidores, redes y aplicaciones.	Gestión de la Información	< 4 horas	Servicios restablecidos.
	Validación de integridad de datos	Comparar respaldos con información operativa.	Equipo TI	< 6 horas	Datos íntegros.
	Reactivación de flujos tecnológicos	Restablecer automatizaciones e integraciones.	Gestión de la Información	Según complejidad	Operación normalizada.

Proceso crítico	Actividad	Descripción	Responsable	Tiempo	Resultado esperado
Desarrollo de Estudios y Proyección Normativa	Aseguramiento de documentos normativos	Verificar disponibilidad de borradores, insumos y análisis.	Líder del proceso	< 1 hora	Documentos protegidos.
	Repositorios alternos	Activar repositorios espejo o copias locales.	Gestión de la Información	Inmediato	Continuidad documental.
	Priorización normativa	Identificar proyectos con impacto regulatorio inmediato.	Líder del proceso	< 2 horas	Priorización definida.
	Restablecimiento de repositorios oficiales	Reactivar carpetas y bases documentales.	Gestión de la Información	< 4 horas	Repositorios normalizados.
	Consolidación de versiones trabajadas	Integrar avances manuales o remotos.	Líder del proceso	< 6 horas	Documentos actualizados.
	Reactivación del flujo normativo	Retomar revisiones y articulaciones externas.	Equipo técnico	Según cronograma	Flujo normativo restablecido.
Direccionamiento y Planeación	Coordinación de activación del PCN	Liderar activación y convocar al Equipo de Continuidad.	Direccionamiento y Planeación	Inmediato	Activación ordenada.
	Evaluación preliminar	Determinar severidad, alcance y procesos afectados.	Direccionamiento y Planeación	< 30 minutos	Diagnóstico inicial.
	Articulación con líderes	Coordinar medidas iniciales y priorización.	Direccionamiento y Planeación	Durante contingencia	Respuesta coordinada.
	Validación para retorno	Confirmar condiciones para normalizar operación.	Direccionamiento y Planeación	< 2 horas	Autorización de retorno.
	Restablecimiento gradual	Supervisar retorno por fases según RTO.	Direccionamiento y Planeación	Según proceso	Retorno ordenado.
	Cierre del incidente	Registrar cierre y activar evaluación posterior.	Direccionamiento y Planeación	< 24 horas	Incidente cerrado.
Control y Evaluación	Verificación de afectación a mecanismos de control	Identificar afectación a indicadores, reportes o seguimiento.	Control y Evaluación	< 1 hora	Diagnóstico inicial.

Proceso crítico	Actividad	Descripción	Responsable	Tiempo	Resultado esperado
	Mecanismos alternos de seguimiento	Uso de formatos manuales o repositorios espejo.	Equipo de Control	Durante contingencia	Seguimiento mínimo garantizado.
	Priorización de reportes críticos	Identificar reportes regulatorios urgentes.	Líder del proceso	< 2 horas	Priorización definida.
	Restablecimiento de herramientas	Reactivar tableros, sistemas y repositorios.	Gestión de la Información	< 4 horas	Herramientas operativas.
	Actualización de información	Integrar registros manuales o alternos.	Control y Evaluación	< 6 horas	Información consolidada.
	Reinicio del ciclo de seguimiento	Retomar monitoreo normal.	Equipo de Control	Según cronograma	Seguimiento normalizado.

Tabla 58 Resultados institucionales de procedimientos de respuesta y recuperación para los procesos críticos

9.6. Protocolo de comunicaciones en contingencia

El plan de comunicaciones define los mensajes clave, los públicos, las vocerías, los canales y los tiempos necesarios para garantizar una comunicación oportuna y coherente durante una interrupción operativa.

9.6.1. Principios de comunicación en contingencia

- **Oportunidad:** La primera comunicación interna se emite dentro de las dos primeras horas de activación.
- **Veracidad:** Solo se comunica información verificada. Ningún servidor puede dirigirse a medios sin autorización del Director General.
- **Coherencia:** Todos los mensajes externos deben ser aprobados por la Dirección General y el proceso de Gestión de Comunicaciones.
- **Trazabilidad:** Toda comunicación emitida durante el evento se registra con fecha, hora, canal y responsable.

9.6.2. Matriz de comunicaciones en contingencia

La gestión de comunicaciones durante un incidente requiere mensajes oportunos, coherentes y dirigidos a los públicos adecuados. La siguiente matriz establece los tipos de comunicación, vocerías, canales y tiempos que deben aplicarse en cada fase del evento, garantizando información clara, trazable y alineada con las directrices del PCN.

Tipo de comunicación	Público	Vocero	Canal	Tiempo	Mensaje clave
Activación del PCN (interno)	Servidores y Directivos URF	Coordinador PCN	Correo institucional / Teams / WhatsApp Equipo	Primeras 2 horas	La URF ha activado su Plan de Continuidad ante [describir evento] . Por favor, sigan las instrucciones del líder de su proceso. El Equipo de Continuidad coordinará las acciones. Mantengan sus equipos portátiles disponibles y confirmen acceso a VPN.
Notificación MHCP	Dirección de Tecnología MHCP	Subdirectora Jurídica y de Gestión Institucional	Correo oficial + teléfono	Primeras 2 horas	La URF informa la activación de su PCN ante [evento]. Se requiere soporte en: [especificar: VPN / SIIF / infraestructura]. Punto de contacto URF: [nombre y teléfono].
Comunicado a grupos de valor (externo)	Grupos de valor y partes interesadas de la URF	Dirección General / Proceso Gestión de Comunicaciones	Sitio web URF / correo oficial/Redes sociales	Primeras 4 horas (si la afectación es visible)	La Unidad de Regulación Financiera informa que está atendiendo una situación que afecta temporalmente [servicio o tema]. Las funciones misionales continúan en modalidad de contingencia. Para consultas urgentes: [canal alternativo].
Actualización de estado (interno)	Servidores y Directivos URF	Coordinador PCN	Correo / Teams	Cada 4 horas durante el evento	Actualización PCN – [hora]: Los sistemas [estado]. Procesos en operación normal: [lista]. Procesos en contingencia: [lista]. Próxima actualización: [hora]. Para soporte: [contacto].
Comunicado de cierre (interno y externo)	Todos los grupos de valor	Director General / Coordinador PCN/ Proceso Gestión de Comunicaciones	Correo / sitio web / Teams	Al retornar a la normalidad	La URF informa que sus operaciones han retornado a condiciones normales. Se agradece la comprensión durante el evento. Los trámites pendientes serán atendidos en [plazo].

Tabla 59 Matriz de comunicaciones en contingencia

9.6.3. Vocerías autorizadas por ámbitos de gestión

Las vocerías durante un incidente deben mantenerse estrictamente controladas para garantizar mensajes coherentes, oportunos y alineados con el Plan de Continuidad del Negocio. Solo las personas expresamente designadas en este apartado están autorizadas para emitir comunicaciones internas o externas, según su ámbito. Ningún otro servidor de la URF puede entregar información o declaraciones sobre la situación, salvo instrucción directa de la Dirección General.

Vocero	Ámbitos de gestión	Público autorizado
Director(a) General URF	Externo	Entidades que participan en el ciclo regulatorio
Subdirectora Jurídica y Gest. Institucional	Interno y MHCP	Dirección de Tecnología MHCP, Entidades de soporte.
Coordinador PCN (Dirección y Planeación)	Interno	Servidores URF, Equipo de Continuidad, líderes de proceso.
Proceso Gestión de Comunicaciones	Externo	Grupos de valor y partes interesadas

Tabla 60 Matriz de vocerías autorizadas por ámbito de gestión

Esta delimitación garantiza coherencia institucional, protege la integridad de la información y evita interpretaciones o declaraciones no oficiales durante la gestión del incidente.

9.7. Integración con la planeación institucional

La continuidad del negocio se articula con los instrumentos de planeación estratégica y operativa de la URF para asegurar que las acciones definidas en el PCN se ejecuten, financien y evalúen dentro de los ciclos institucionales. Esta integración garantiza que las medidas de preparación, respuesta y recuperación se mantengan como parte del Sistema de Gestión Institucional y no como un componente aislado.

El PCN se incorpora al Plan Estratégico Institucional como un elemento de gestión del riesgo estratégico y de fortalecimiento de la capacidad institucional. En el Plan de Acción Institucional se incluyen anualmente las actividades de actualización, pruebas, seguimiento y mejora del PCN, así como los recursos necesarios para su implementación. De igual forma, los requerimientos de bienes y servicios esenciales para la continuidad se integran al Plan de Adquisiciones, asegurando su disponibilidad oportuna.

Los riesgos de interrupción identificados en el BIA y en el análisis de riesgos del PCN se articulan con el Mapa de Riesgos Institucional, permitiendo su tratamiento dentro del Sistema de Control Interno. Asimismo, las medidas de protección, respaldo y recuperación tecnológica se alinean con el Plan de Seguridad y Privacidad de la Información y con las responsabilidades del proceso de Gestión de la Información.

El PCN se revisa anualmente dentro del ciclo institucional de planeación, bajo la coordinación del proceso de Direccionamiento y Planeación. Esta revisión incluye la actualización de procesos críticos, tiempos de recuperación, estrategias, recursos esenciales y resultados de pruebas o incidentes reales. Los avances y ajustes se reportan en los mecanismos institucionales de seguimiento, como el Sistema de Monitoreo de la Gestión Institucional – SMGI.

La integración del PCN con la planeación institucional asegura que la continuidad del negocio sea un componente permanente de la gestión estratégica y operativa de la URF, permitiendo asignar recursos, fortalecer capacidades y garantizar la mejora continua del sistema de continuidad.

9.8. Mejora continua

La mejora continua del Plan de Continuidad del Negocio es un proceso permanente que garantiza su vigencia, eficacia y alineación con la evolución institucional, tecnológica y normativa de la URF. Este enfoque implica revisar de manera sistemática los procedimientos, capacidades y recursos definidos en el PCN, incorporando aprendizajes derivados de pruebas, simulaciones, auditorías, incidentes reales y cambios en los procesos críticos.

El proceso de Direccionamiento y Planeación lidera la actualización del PCN dentro del ciclo anual de planeación institucional, asegurando que los ajustes necesarios se integren en el Plan de Acción Institucional, el Mapa de Riesgos Institucional y los instrumentos de seguimiento y evaluación. Asimismo, los resultados de las pruebas de continuidad, las revisiones posteriores a incidentes y las recomendaciones de auditoría se documentan y se traducen en acciones de mejora que fortalecen la capacidad de respuesta y recuperación de los procesos críticos.

La mejora continua garantiza que el PCN permanezca actualizado, operativo y alineado con las necesidades misionales de la URF, permitiendo que la Entidad mantenga su resiliencia institucional y responda de manera efectiva ante cualquier interrupción que afecte la prestación de sus servicios.

El PCN se somete a revisión y actualización obligatoria en los siguientes eventos:

- Anualmente, como parte del ciclo de planeación institucional (PTEP y Plan de Acción).
- Después de cada simulacro o ejercicio de validación, incorporando las brechas identificadas.
- Después de cada activación real del plan, con base en las lecciones aprendidas.
- Cuando se produzcan cambios significativos en la estructura institucional, los procesos críticos o el entorno tecnológico.
- Cuando nuevas disposiciones normativas (MIPG, ISO, Decretos) exijan ajustes.

El Proceso de Control y Evaluación realizará auditorías independientes al PCN de acuerdo con la programación que se defina en el Plan Anual de Auditoría, evaluando la eficacia de los controles, el cumplimiento de los procedimientos y la pertinencia de las estrategias. Los resultados se reportarán al Comité Institucional de Coordinación de Control Interno y se incorporarán en el Plan de Mejoramiento Institucional.

10. Plan de pruebas, simulacros y validación

La URF implementará un programa anual de pruebas y simulacros para verificar la efectividad del PCN, identificar brechas y fortalecer la capacidad de respuesta institucional. El programa es de obligatorio cumplimiento conforme a la NTC/ISO 22301:2019 (cláusula 8.5) y los lineamientos del MIPG.

10.1. Tipos de ejercicios

Los ejercicios de pruebas y simulacros permiten evaluar la capacidad de la URF para responder y recuperarse ante una interrupción, así como validar la efectividad de los procedimientos definidos en el PCN. Los tipos de ejercicios descritos a continuación establecen distintos niveles de alcance y profundidad, desde simulaciones de análisis en mesa hasta pruebas funcionales y verificaciones técnicas, garantizando una evaluación integral y progresiva del sistema de continuidad.

Tipo	Descripción	Frecuencia	Responsable
Ejercicio de escritorio (Tabletop)	Simulación de escenario de crisis mediante discusión en mesa. El Equipo de Continuidad analiza respuestas sin ejecutarlas.	1 vez por año (S1)	Coordinador PCN + Equipo Continuidad
Prueba funcional parcial	Activación real de un componente del plan: prueba de restauración de respaldos, activación de trabajo remoto, o ejercicio de comunicaciones.	1 vez por año (S2)	Gest. Información + Coordinador PCN
Prueba de respaldos tecnológicos	Verificación técnica de que los respaldos de información son recuperables dentro del RPO definido.	Trimestral	Proceso Gestión de la Información / MHCP
Actualización del árbol de contactos	Verificación de que todos los datos de contacto del Equipo de Continuidad están vigentes.	Semestral	Dirección y Planeación

Tabla 61 Matriz de tipos de ejercicios

10.2. Criterios de evaluación de simulacros

La evaluación de los simulacros es un componente esencial del proceso de mejora continua del PCN; permite medir el desempeño institucional frente a escenarios de interrupción y determinar si los procedimientos, tiempos y capacidades operan conforme a lo previsto.

Los criterios definidos a continuación permiten valorar de manera objetiva la activación, la recuperación, la gestión de la información, las comunicaciones y la efectividad de los controles, identificando brechas y oportunidades de mejora para fortalecer la resiliencia de la URF.

Criterio	Descripción evaluativa	Preguntas guía	Evidencias esperadas
Tiempo de activación	Verifica si el Equipo de Continuidad fue convocado y respondió dentro del tiempo objetivo.	¿La activación se realizó dentro del tiempo definido? ¿Hubo retrasos o fallas en la convocatoria?	Registro de hora de activación, confirmación de asistencia, bitácora del Coordinador PCN.
Tiempo de recuperación	Confirma si los procesos críticos se restablecieron dentro del RTO y si existieron cuellos de botella.	¿El proceso alcanzó el nivel mínimo de operación dentro del RTO? ¿Qué retrasó la recuperación?	Tiempos de restablecimiento, reportes de líderes de proceso, evidencia de operación mínima.

Criterio	Descripción evaluativa	Preguntas guía	Evidencias esperadas
Integridad y disponibilidad de la información	Evalúa si la información recuperada cumple el RPO y si los respaldos funcionaron adecuadamente.	¿La información recuperada corresponde al punto de recuperación esperado? ¿Hubo pérdida de datos?	Logs de restauración, reportes de TI, verificación de integridad de archivos.
Efectividad de las comunicaciones	Determina si los mensajes fueron emitidos a los públicos correctos, por voceros autorizados y en los tiempos definidos.	¿Los mensajes se enviaron a tiempo? ¿Se usaron los canales adecuados? ¿Hubo desviaciones de vocería?	Copias de mensajes, registros de envío, matriz de comunicaciones aplicada.
Desempeño de controles y procedimientos	Valida si los controles operativos, tecnológicos y administrativos actuaron conforme a lo previsto.	¿Los controles funcionaron como se esperaba? ¿Alguno falló o no se aplicó?	Checklists de control, reportes de TI, evidencias de aplicación de procedimientos.
Coordinación interprocesos	Analiza la articulación entre líderes de proceso, tiempos de respuesta y flujo de información.	¿Hubo coordinación fluida entre procesos? ¿Se generaron cuellos de comunicación?	Bitácoras, actas del ejercicio, reportes de interacción entre procesos.
Brechas y oportunidades de mejora	Identifica fallas, desviaciones o vacíos del plan y oportunidades para fortalecer capacidades.	¿Qué no funcionó? ¿Qué debe ajustarse? ¿Qué capacidades deben fortalecerse?	Informe post-ejercicio, listado de acciones correctivas, plan de mejora.

Tabla 62 Matriz de evaluación de simulacros

En conjunto, la aplicación de estos criterios garantiza que cada simulacro se convierta en un ejercicio real de aprendizaje organizacional, permitiendo evaluar con rigor la capacidad de respuesta de la URF y la efectividad de sus procedimientos de continuidad. Los resultados obtenidos en estas evaluaciones alimentan directamente el ciclo de mejora continua del PCN, fortalecen la resiliencia institucional y aseguran que la Unidad mantenga niveles adecuados de preparación frente a posibles interrupciones operativas.

11. Documento referente

Tipo	Nombre
Caracterización	Caracterización del proceso de Direccionamiento y Planeación

12. Datos de elaboración y control de cambios

Control de cambios			
Fecha	Versión	Cód. Solicitud	Descripción del cambio
2026-07-23	1	TS-1280	Elaboración de la primera versión del documento que desarrolla el marco metodológico, conceptual y los resultados institucionales.

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Daissy Tatiana Santos Yate
Cargo:	Asesora – Direccionamiento y Planeación
Revisión	
Nombre:	Paola Patricia Rodríguez Angulo
Cargo:	Subdirectora Jurídica y de Gestión Institucional
Aprobación	
Nombre:	Comité Institucional de Gestión y Desempeño
Cargo:	Acta No. 04 de 2026 – Sesión ordinaria