PLAN DE CONTINUIDAD DE NEGOCIO			
PROCESO:	GESTIÓN TIC´S		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
7/12/2023	GTI-PLN01	5.0	**1** de **67**

PLAN DE CONTINUIDAD DE NEGOCIO DE TI

UNIDAD ADMINISTRATIVA ESPECIAL
CONTADURÍA GENERAL DE LA NACIÓN - CGN

Versión 5.0
Noviembre 2024

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM/AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Creación	5/02/2013	GIT-AI	Creación
2.0	Todas	Actualización	10/10/2018	GIT-AI	Actualización
3.0	Todas	Actualización	2/07/2019	GIT-AI	Actualización
3.1	Todas	Actualización	27/05/2020	GIT-AI	Modificación de la estructura del documento
3.2	7.1.1, 7.2.1	Actualización	24/10/2022	GIT-AI	Actualización y aprobación comité CIGD (10/11/2022)
4.0	2, 3, 6.3, 7.1	Actualización	7/12/2023	GIT-AI	• Actualización de formato del documento • Numeral 2. Revisión y ajuste de la política de continuidad de negocio • Numeral 3. Actualización tabla de cantidad de procedimientos • Numeral 6.3 Actualización misión, visión, objetivos estratégicos • Numeral 7.1 Ajuste Tablas 1,4,8,9,14,17,18,19,20,21 2
5.0	1,	Actualización	XX/11/2024	GIT-AI	• Actualización de formato del documento • Actualización de información • Ajuste a la introducción • Ajuste de tablas • Se incluye el numeral del Plan de recuperación de desastres - DRP • Revisión equipo de apoyo al oficial de seguridad - XX de noviembre de 2024

TABLA DE CONTENIDO

Pág. No.

INDICE DE TABLAS

INDICE DE FIGURAS

1. INTRODUCCIÓN

La UAE Contaduría General de la Nación, en adelante CGN, consciente de la existencia de amenazas externas e internas significativas que potencializan la ocurrencia de incidentes disruptivos con capacidad de afectar la continuidad de los productos y servicios críticos, establece el Plan de Continuidad de Negocio como una herramienta para responder de manera organizada y oportuna a eventos que podrían interrumpir la operación normal de los procesos y que puedan generar impactos negativos en el logro de los objetivos y la misión de la entidad.

En particular, el presente plan se focaliza en los procesos misionales de normalización y culturización contable, centralización de la información y consolidación de la Información y en el proceso de apoyo gestión TICs considerados como críticos en el mapa institucional de procesos. Es de anotar que este plan de continuidad se aborda desde un punto de vista tecnológico, en razón a que cada uno de los procesos de la entidad requiere soporte de componentes de tecnología para su correcto funcionamiento.

Este plan es una herramienta que permite prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los servidores públicos que prestan sus servicios para la entidad, afectar el debido desarrollo de las actividades propias de la función pública de la entidad, impedir la prestación y continuidad del servicio a los grupos de valor o el cumplimiento de los compromisos establecidos en la planeación estratégica. En este artefacto la CGN ha consolidado una serie de acciones a emprender, que ejecutadas de forma planificada permitirán responder de manera eficiente ante una eventualidad y restablecer en el menor tiempo la prestación de los servicios, mitigando el impacto negativo de la pérdida de recursos.

Adicionalmente, cabe destacar que el Plan de Recuperación por Desastre, en adelante DRP, es una parte importante de la Continuidad del Negocio. El DRP definitivo no solo proporciona un procedimiento para recuperar datos y sistemas en caso de pérdida parcial de la infraestructura de tecnológica, sino que también incluye los objetivos de continuidad del negocio, enumera las herramientas y los planes que se han hecho para que la empresa funcione lo antes posible en caso de emergencia de TI y asegurando un traspaso eficiente de información.

Un documento DRP permite unir los objetivos de la empresa con las herramientas, servicios y procedimientos de TI. Este documento configura un DRP en 4 pasos:

1. Establecer objetivos

2. Definir prioridades
3. Especificar la estrategia de respaldo y recuperación ante desastres
4. Organizar la emergencia.

Para la implementación de la gestión de continuidad del negocio se requiere poner a disposición los recursos humano, financiero, físico y tecnológico identificados en este documento, para activar la continuidad del negocio.

2. POLÍTICA DE CONTINUIDAD DEL NEGOCIO

"La UAE Contaduría General de la Nación como entidad rectora responsable de regular la contabilidad general de la nación que uniforma, centraliza y consolida la contabilidad pública, hará todo lo que esté a su alcance para asegurar la continuidad de las operaciones y los servicios que presta a las entidades y partes interesadas ante una interrupción imprevista de la plataforma tecnológica o un evento catastrófico, de tal forma que se restablezcan en el menor tiempo posible los servicios que soportan los procesos críticos de la entidad, siempre estableciendo como prioridad la preservación de la vida e integridad de sus funcionarios, contratistas y demás partes interesadas".

La revisión o actualización de esta política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la continuidad de la operación de la CGN, todos los cambios que surtan en la política deben ser aprobados y divulgados al interior de la entidad.

3. ALCANCE

La realización de las tareas que conducen al logro de objetivos misionales de la Contaduría General de la Nación se encuentra en el marco del siguiente mapa de procesos:

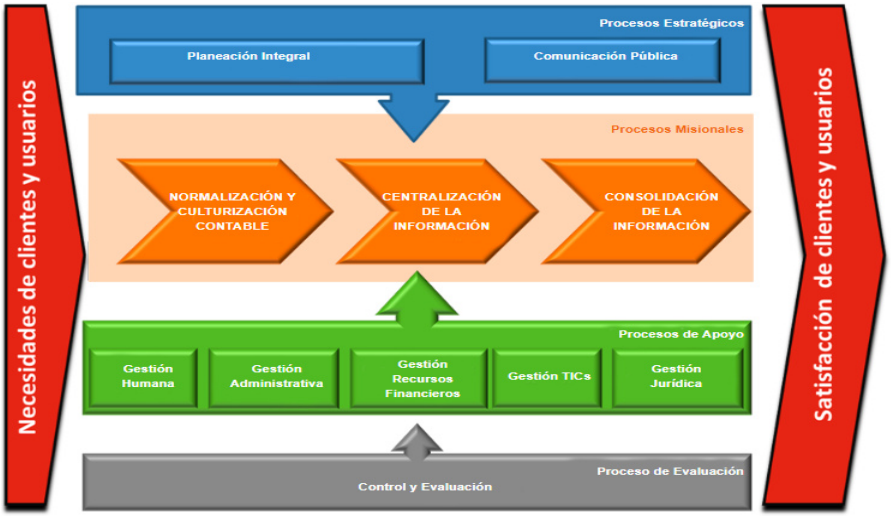


*Figura 1**: Mapa de procesos CGN***
***Fuente:** www.contaduria.gov.co*

En términos generales, cada proceso está conformado por un conjunto de procedimientos que identifica y describe el detalle de los pasos que se requieren para completar las tareas; en resumen, se tienen los siguientes procesos:

Tipo proceso	Proceso	Cantidad Procedimientos
Estratégico	Planeación Integral	16
	Comunicación Publica	2
Misional	Normatividad y Culturización	5
	Centralización de la Información	14
	Consolidación de la Información	8
Apoyo	Gestión Humana	17
	Gestión Administrativa	9
	Gestión Recursos Financieros	6
	Gestión Tics	11
	Gestión Jurídica	6
Evaluación	Control y Evaluación	1

*Tabla 3: **Alcance del PCN en los procesos de la CGN***
Fuente: propia con datos de CGN

En este plan de continuidad del negocio se cubren tres procesos misionales y un proceso de apoyo, incluyendo los procedimientos que involucran las actividades relevantes para

la producción y prestación de los principales productos y servicios de la CGN, la selección de dichos procedimientos se encuentra descrita en el numeral 6 en el ítem de "**Análisis y valoración de procesos organizacionales".**

De esta manera, se abordan 4 procesos, 9 procedimientos y se identifican 12 servicios de tecnología que apoyan el negocio de la entidad, con fundamento en su misión y sus objetivos estratégicos.

Este alcance se enfoca en los servicios tecnológicos que prestan apoyo a la misión de la entidad para facilitar sus funciones principales, esto debido a que la CGN no cuenta con los recursos presupuestales suficientes para adquirir un centro alterno que cubra todos los servicios en contingencia o de una sede alterna que cuente con las condiciones para iniciar en paralelo la operación, por lo tanto con los recursos actuales se ha identificado la capacidad de habilitar los servicios asociados a los componentes tecnológicos que la entidad puede activar como contingencia, principalmente en los casos de caídas totales o parciales de esos servicios.

Procesos	Procedimientos		
Normalización y Culturización Contable (5)	NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05		
Centralización de la Información (14)	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA	CEN-PRC16 GESTIÓN A LA INFORMACIÓN	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORÍA
Consolidación de la Información (8)	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE	CON-PRC12 CONSOLIDACIÓN CONTABLE	
Gestión TICs (9)	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA	GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO	

*Tabla 4**: Alcance general del PCN***
Fuente: Propia con datos de CGN

4. MARCO LEGAL

El desarrollo del plan de continuidad de negocio de la CGN se fundamenta en la necesidad de preservar la disponibilidad y continuidad de los productos y servicios que presta la entidad dentro del marco de implementación de la Política de Gobierno Digital, la Política de Seguridad Digital y demás disposiciones generales relacionados con los servicios digitales ciudadanos.

De igual forma, la estrategia de continuidad de negocio institucional se articula con el Modelo Integrado de Planeación y Gestión – MIPG en su tercera (3ª) dimensión: "*Gestión con valores para resultados*" en lo que respecta a los aspectos relevantes para una adecuada operación de la organización "de la ventanilla hacia adentro" y la segunda, referente a la relación Estado Ciudadano "de la ventanilla hacia afuera". En tal sentido, la implementación del plan de continuidad del negocio se constituye como un instrumento de resiliencia, recuperación y respuesta con el que se propone garantizar la preservación de la seguridad y la vida de los grupos de valor de la entidad. La adopción se enmarca bajo el Modelo de Gestión de Riesgos de Seguridad Digital dispuesto por MinTIC.

Decreto 767 de 2022 por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de TIC

Resolución 746 de 2022, por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021

Decreto 338 de 2022, por el cual se adiciona el Título 21 a la Parte 2 del Libro del Decreto Único 1078 de 2015. Establece lineamientos generales para fortalecer la gobernanza de Seguridad Digital y se dictan otras disposiciones.

Directiva Presidencia No.02 de 2022, dirigida a entidades públicas de la rama ejecutiva del orden nacional, tiene como objetivo la reiteración de la política pública en materia de seguridad digital para garantizar la implementación segura de la Política de Gobierno Digital

Directiva Presidencial No.03 de 2021, dirigida a entidades públicas de la rama ejecutiva del Orden Nacional – Lineamientos (…) Seguridad Digital

Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

Anexo 1. Modelo de Seguridad y Privacidad de la Información – MSPI – febrero 2021, por el que se definen los lineamientos para la implementación de la estrategia de seguridad digital

Resolución 1519 de 2020, por la cual se definen los estándares y directrices para publicar información señalada en la Ley 1712 de 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos

Guía Técnica Colombiana GTC-ISO 22313 Seguridad y resiliencia. Sistemas de gestión de continuidad de negocio. Orientación sobre el uso de la NTC-ISO 22301. 2020-12-16

Ley 1955 de 2018, por el cual se expide el Plan Nacional de Desarrollo 2019-2022. "Pacto por Colombia, Pacto por la Equidad".

Decreto 1499 de 2017, por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Modelo Integrado de planeación y gestión - MIPG, 3ª. Dimensión: "Gestión con valores para resultados".

Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1072 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo
Guía Técnica Colombiana GTC-ISO/IEC 27031 Tecnología de la Información. Técnicas de Seguridad. Directrices para la preparación de la Tecnología de la Información y las Comunicaciones para la Continuidad de Negocio. 2016-12-07

Norma Técnica NTC-ISO/IEC Colombiana 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. 2013-12-11

Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres
De igual forma, en el marco regulatorio sobre Política de Gobierno Digital y lo concerniente a la Gestión de la Continuidad de Negocio, se adoptan las demás disposiciones que sobre la materia son consideradas para su cumplimiento.

5. TERMINOLOGIA

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. Se debe incluir la definición de todos los tipos de activos, Informático y RH

Análisis de Impacto al Negocio (Business Impact Analysis (BIA), por su sigla en inglés): Técnicas y metodologías que pueden ser usadas para identificar, cuantificar y cualificar los impactos de negocio y sus efectos en una organización en caso de pérdida o interrupción de las actividades de misión crítica.

Emergencia: Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere de una acción inmediata.

Gestión de continuidad de negocio (Business Continuity Management (BCM), por su sigla en inglés): Proceso general que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación del negocio en caso de materializarse, y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos de información.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Modo de falla: Manera por la cual una falla es observada. Nota: Esta generalmente describe la manera en que la falla ocurre y su impacto para la operación del sistema.

MTD (Maximun Tolerable Downtime/Outage (MTD), por su sigla en inglés): Es el tiempo máximo de inactividad que la organización puede tolerar la ausencia o no disponibilidad de una función o proceso, se obtiene de la suma de RTO y WRT.

Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Partes interesadas: Es cualquier organización, grupo o individuo que pueda afectar o ser afectado por las actividades de una empresa u organización de referencia. Así cada organización dispone de sus partes interesadas, también denominadas grupos de interés, públicos de interés, corresponsables u otros.

Plan de Continuidad de Negocio (PCN): Conjunto de procedimientos e información documentados que se desarrolla, compila y mantiene preparado para responder, recuperar, reanudar y restaurar la operación en caso de producirse un incidente, para permitir a la organización continuar desempeñando sus actividades críticas a un nivel aceptable predefinido.

Plan de Contingencia: Es una estructura estratégica y operativa, que ayuda a controlar situaciones de emergencia y a minimizar los impactos negativos que esta pueda generar sobre una organización, para esto implementa una serie de procedimientos alternativos que permitan recuperar el funcionamiento normal de la operación en el menor tiempo posible.

RPO (Recovery Point Objective, por su sigla en inglés): Es el período máximo tolerable de pérdida de datos antes de ser restablecido como consecuencia de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

RTO (Recovery Time Objective, por su sigla en inglés): Es el tiempo y nivel de servicio en el que debe ser restaurado un proceso del negocio después de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

Resiliencia: Habilidad para una organización para resistir al ser afectada por una interrupción.

Sitio alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no puedan llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

Tecnología de la Información (TI): Es el estudio, diseño, desarrollo, implementación, soporte y administración de los sistemas de información basados en computadoras, particularmente aplicaciones de software y hardware de computadoras".

Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

WRT (Work Recovery Time): Tiempo de trabajo en recuperación.

6. OBJETIVOS

6.1. Objetivo General

Definir las actividades necesarias para responder, recuperar, reanudar y restaurar adecuadamente las operaciones de negocio ante la materialización de eventualidades tecnológicas, en escenarios de catástrofe que puedan comprometer la seguridad del personal, la continuidad de las operaciones o la prestación de los servicios críticos para las partes interesadas de la CGN.

6.2. Objetivos específicos

- Asegurar la protección de los funcionarios, contratistas y demás partes interesadas que se encuentren dentro de las instalaciones de la CGN, en caso de que se materialice una situación que sea calificada como emergencia y que pueda comprometer su seguridad.
- Incrementar el nivel de confianza en la relación Ciudadano-Estado, mediante la generación de valor público a través de las capacidades institucionales de recuperación.
- Identificar la infraestructura física, tecnológica y recurso humano para los procesos, procedimientos y servicios de tecnología críticos que apoyan el negocio de la entidad, los cuales son necesarios para asegurar su continuidad.
- Reducir el impacto para el cumplimiento de las funciones misionales de la entidad, en caso de presentarse un incidente, emergencia o desastre que afecte el curso normal de las operaciones.
- Establecer lineamientos para la respuesta y tiempos mínimos de recuperación, ante incidentes o desastres que lleven a la activación del plan de continuidad de negocio.

6.3 Contexto de la CGN

6.3.1. Entorno Estratégico y Funcional

La CGN es la entidad rectora responsable de regular la contabilidad general de la nación, actualmente cuenta con aproximadamente 270 funcionarios y presta servicios a más de 4.000 entidades; en su diario quehacer se presentan múltiples interacciones que definen un marco funcional y operativo propio y característico de su propósito misional, es por esto por lo que se determina el contexto externo e interno pertinentes para el propósito del presente plan y que afectan el cumplimiento de los objetivos del PCN.

Contexto interno.

El direccionamiento estratégico institucional de la Contaduría General de la Nación se orienta hacia los tres pilares fundamentales de: generación de valor público, gestión financiera pública transparente e innovadora, y enfoque hacia la sustentabilidad, mediante la continua y eficaz prestación de sus servicios.

De esta manera se destacan los siguientes elementos:

Misión: Somos el órgano rector de la contabilidad pública en Colombia, con autoridad doctrinaria en la materia, que normaliza, centraliza y consolida la contabilidad del sector público, para elaborar el Balance General de la Nación y de la Hacienda Pública, así como otros informes contables, útiles para la toma de decisiones, la rendición de cuentas y el control de las entidades públicas, los ciudadanos y demás grupos de valor.

Visión: Seremos reconocidos como una entidad pilar del Sistema de Gestión Financiera Pública, que innova en la provisión de la información contable pública relevante y confiable para la transparencia, eficiencia y sustentabilidad social y ambiental del sector público colombiano, orientada a la creación de valor público para la sociedad.

Objetivos estratégicos: De los objetivos estratégicos institucionales de la CGN que aplican al plan de continuidad de negocio son:

Número 5. Mantener y fortalecer la calidad de la regulación contable pública, atendiendo a estándares internacionales y al contexto colombiano.

Número 7. Fortalecer el proceso de consolidación de la información contable pública, para conseguir información consolidada de calidad.

Número 9. Optimizar el desempeño de la CGN en todos sus procesos a través del mantenimiento y mejora de los sistemas del Sistema Integrado de Gestión Institucional (En el SGSI).

Número 11. Fortalecer las herramientas tecnológicas para la armonización integración de Contabilidad Pública con los demás subsistemas de la Gestión Financiera Pública.

7. GESTION DE CONTINUIDAD DE NEGOCIO

Para atender la continuidad de seguridad de la información, se incluyen en la gestión de continuidad del negocio los aspectos metodológicos del modelo de operación de seguridad y privacidad de la información relacionados con las siguientes cuatro fases: planificación, implementación (operación), revisión (gestión) y mantenimiento continuo (mejora continua) del plan, para proteger, reducir la ocurrencia, prepararse, responder y recuperarse de incidentes que interrumpan la operación de los procesos, cuando éstos ocurren, como se presenta a continuación:

*Figura 2**: Modelo de operación de seguridad y Privacidad de la Información***
Fuente: Guía 10 Continuidad de Negocio MINTIC

Los procesos misionales relacionados en el alcance del PCN son responsables de sus activos de información y de participar activamente en las actividades de reporte y restauración del PCN de acuerdo con las pautas establecidas en este plan de continuidad de negocio.

El GIT de apoyo informático de la CGN, es el responsable de levantar el inventario de activos críticos frente a la disponibilidad de la plataforma, análisis de impacto de la interrupción, comunicación detallada del diagnóstico, identificación y asignación de responsables para gestionar el riesgo y definición alternativas de la estrategia de recuperación.

Así como es el responsable de gestionar, plantear y exponer los escenarios técnicos y sus alcances de las posibles alternativas como medidas preventivas y/o actividades de recuperación, todas encaminadas evitar la interrupción de los servicios en la plataforma tecnológica.

El GIT de apoyo informático tiene la responsabilidad de custodiar, administrar las bases de datos y todo el recurso tecnológico que apoya los procesos de información misionales y salvaguardar los datos que se procesan en la entidad; así como implementar toda la tecnología a nivel de hardware (servidores, sistemas de cableado estructurado, virtualización de máquinas, aprovisionamiento de servicios de internet y correo electrónico, entre otros).

La entidad debe establecer controles con:

a. Verificación y actualización del inventario de activos de información
b. Valoración de los activos frente a la disponibilidad e integridad de la plataforma de TI
c. Valoración de los costos de alternativas de continuidad

Se cuenta con un Comité Institucional de Gestión y Desempeño donde se revisa el manejo de la gestión de incidentes críticos de seguridad en busca de una mejora continua.

7.1 Planificación

7.1.1 Análisis del Impacto del Negocio (BIA)

El análisis del impacto del negocio nos permite identificar los procesos misionales de la CGN y analizar el nivel de impacto con relación a la gestión del negocio.

En esta fase se identifican las áreas críticas del negocio para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción se deben considerar los siguientes requerimientos:

- **Identificar las funciones y procesos importantes** para la subsistencia de la entidad al momento de la interrupción, se requiere identificar cuales procesos son claves para entrar en operación prioritariamente.
- **Revisar las consecuencias tanto operacionales como financieras**, que una interrupción tendrá en los procesos considerados de alta prioridad.
- **Estimar los tiempos de recuperación**, Ante las posibles alteraciones de los procesos de alta prioridad se evalúan los tiempos para poner en funcionamiento la infraestructura de TI.

Análisis y valoración de procesos organizacionales

Los procesos y procedimientos de la organización son valorados con criterios funcionales y tecnológicos en relación con el nivel de riesgo, el impacto operacional y la complejidad de su recuperación, alineados con los objetivos estratégicos y la misión de la entidad, para identificar solo aquellos que son de carácter crítico y los cuales bajo un escenario de catástrofe o interrupción del servicio puedan afectar el funcionamiento de la entidad e impedir el logro de la misión.

Se incluye cuadro consolidado con la justificación de selección de procesos críticos de la entidad para el alcance de este PCN. Ver Anexo 2. **Justificación de selección de procesos críticos**

Según la Guía 10, MinTic: "Guía para la preparación de las TIC para la continuidad del negocio" la metodología del análisis de impacto del negocio define una serie de pasos para identificar los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre o caída del servicio, como se muestran en la siguiente figura:

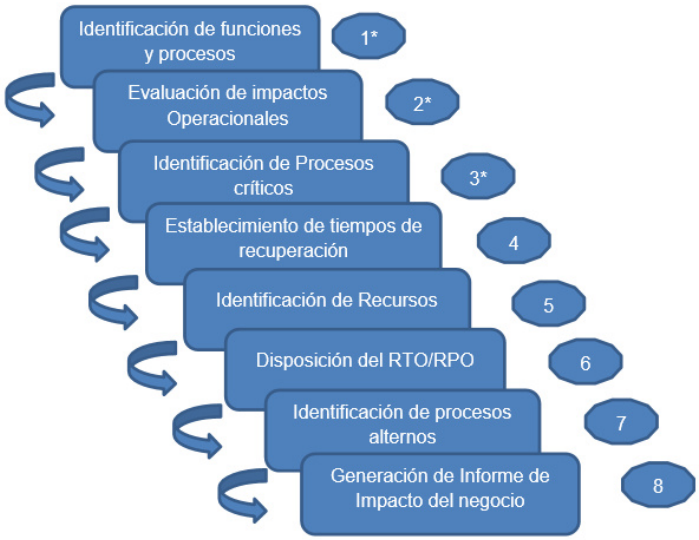


*Figura 3. **Metodología del Análisis de Impacto del Negocio***
Fuente: Guía 10 Continuidad de Negocio MINTIC

Identificación y evaluación de procesos críticos e impactos operacionales

Se identificaron y valoraron los procesos y procedimientos, aplicando los criterios para la valoración de los procesos y sus impactos operacionales como se observa en el Anexo 1. **Identificación y evaluación de procesos críticos e impactos operacionales,** dando como resultado que los siguientes procesos y procedimientos se encuentran valorados como *críticos*:

Procesos	Procedimientos
Normalización y Culturización Contable (5)	NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05
Centralización de la Información (14)	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA
	CEN-PRC16 GESTIÓN A LA INFORMACIÓN
	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORIA
Consolidación de la Información (8)	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE
	CON-PRC12 CONSOLIDACIÓN CONTABLE
Gestión TICs (11)	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA
	GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO

Gestión de recursos financieros (6)	GFI-PRC03 PLAN ANUAL MENSUALIZADO DE CAJA Y SUS MODIFICACIONES, CONTRIBUCIONES DE CUENTAS POR PAGAR Y REINTEGRO DGCPTN
	GFI-PRC04 PROCEDIMIENTO GENERAL DE PRESUPUESTO
Gestión humana (17)	GTH-PRC08 PREPARACION Y RESPUESTAS ANTE EMERGENCIAS

*Tabla 5**: Resumen resultados valoración de procesos***
Fuente: propia

Debido a que este documento tiene un enfoque totalmente tecnológico, se hace énfasis en los cuatro primeros procesos porque destacan los objetivos misionales considerados críticos dentro del alcance del presente PCN; dejando de lado los procesos de "gestión recursos financieros" y "gestión humana".

Normalización y Culturización Contable: Asegurar que las actividades de investigación contable, normalización y estrategias de capacitación permitan la generación de información contable pública uniforme, garantizando su rigor técnico.

Centralización de la Información: Garantizar que las actividades de asesoría, asistencias técnicas, complementación de normas y parametrizaciones contables en los sistemas, facilite centralizar la información reportada por las entidades contables públicas a través de las categorías definidas en los sistemas integrados de información nacional (CHIP, SIIN y SPGR), asegurando que cumplan con parámetros de consistencia, oportunidad y calidad.

Consolidación de la Información: Suministrar la información financiera consolidada y/o agregada de base contable de conformidad con el mandato constitucional y legal de manera que atienda los requerimientos de los diferentes usuarios.

Gestión TICs: Apoyar a través de la Tecnología Informática y el recurso técnico las actividades de gestión y misión institucionales.

Estructura organizacional: La estructura organizacional de la CGN es de tipo funcional, por lo que se denota alto nivel de especialidad en cada una de las subcontadurías, secretaría general y grupos internos de trabajo. Como lo representa su organigrama

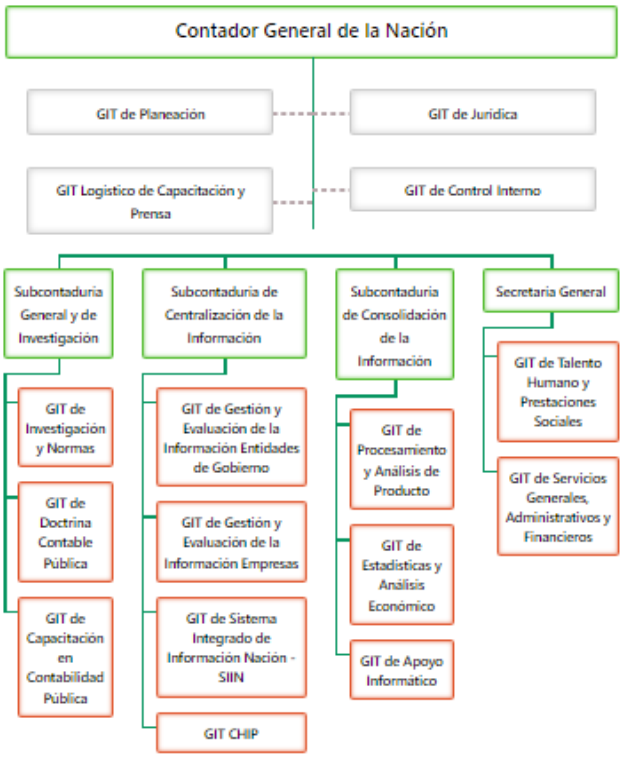


*Figura 4**: Organigrama CGN***
Fuente: www.contaduria.gov.co

El personal actual asociado a los principales cargos en el organigrama es el siguiente:

DEPENDENCIA ORGANIZACIONAL	***NOMBRE***
CONTADOR GENERAL DE LA NACIÓN	*MAURICIO GÓMEZ VILLEGAS*
COODINADORA GIT DE PLANEACIÓN	*VILMA YOLANDA NARVÁEZ*
COODINADOR GIT DE JURIDICA	*EDGAR ARTURO DIAZ VINASCO*
COODINADORA GIT LOGÍSTICO DE CAPACITACIÓN Y PRENSA	*ALLISON CRISTINA MARIN FLOREZ*
COODINADORA GIT DE CONTROL INTERNO	*KATHERINE FORERO MENDEZ*
SUBCONTADORA GENERAL Y DE INVESTIGACIÓN	*ROCIO PEREZ SOTELO*
COODINADORA GIT DE INVESTIGACIÓN Y NORMAS (E)	*CARLOS ANDRES RODRIGUEZ RAMIREZ*
GRUPO INTERNO DE TRABAJO DE CAPACITACIÓN EN CONTABILIDAD PÚBLICA (E)	*DIANA CAROLINA MONROY*

COODINADOR GIT DE DOCTRINA Y CAPACITACIÓN (E)	*SANDRA YAMILE ENDO BARRERA*
SUBCONTADORA GENERAL DE CENTRALIZACIÓN DE LA INFORMACIÓN	*JUAN CAMILO SANTAMARÍA*
COODINADORA GIT DE GESTIÓN Y EVALUACIÓN DE LA INFORMACIÓN - ENTIDADES DE GOBIERNO	*BLANCA OFELIA MARTINEZ MARTINEZ*
COODINADORA GIT GESTIÓN Y EVALUACIÓN DE LA INFORMACIÓN -EMPRESAS	*JULIÁN NOGUERA*
COODINADORA GIT SISTEMA INTEGRADO DE INFORMACIÓN NACIÓN - SIIN	*YIMMY ALEXANDER BUENO*
COODINADOR GIT CHIP	*PEDRO FLAMINIO MARTIN DIAZ*
SUBCONTADOR GENERAL DE CONSOLIDACIÓN DE LA INFORMACIÓN	*ELIZABETH SOLER CASTILLO*
COODINADOR GIT DE PROCESAMIENTO Y ANÁLISIS DE PRODUCTO (E)	*JAIME VALENCIA CUBILLOS*
COODINADOR GIT DE ESTADÍSTICA Y ANÁLISIS ECONÓMICO	*OMAR EDUARDO MANCIPE SAAVEDRA*
COODINADOR GIT DE APOYO INFORMÁTICO	*JAMIR MOSQUERA RUBIO*
SECRETARIO GENERAL	*FREDDY ARMANDO CASTAÑO*
COODINADOR GIT DE TALENTO HUMANO	*ALEXANDRA QUEMBA GOMEZ*
COODINADOR GIT DE SERVICIOS GENERALES ADMINISTRATIVOS Y FINANCIEROS	*DENIS ELIANA HERNÁNDEZ*

*Tabla 6**: Directivos y líderes de áreas organizacionales***
Fuente: www.contaduria.gov.co

Contexto externo.

La CGN hace parte de las entidades del sector hacienda, el cual está conformado así:

- Unidad Administrativa Especial Contaduría General de La Nación
- Ministerio de Hacienda y Crédito Público
- Fondo de Garantías de Instituciones Financieras - FOGAFIN
- Sociedad De Activos Especiales - SAE S.A.S
- Unidad Administrativa Especial de Gestión de Pensiones Públicas y Parafiscales – UGPP
- Financiera de Desarrollo Territorial S.A. – FINDETER
- Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales – DIAN
- Fondo de Garantías de Entidades Cooperativas – FOGACOOP

- Financiera de Desarrollo Nacional S.A. – FDN
- Fiduciaria La Previsora S.A.
- Central de Inversiones S.A.
- Superintendencia Financiera de Colombia
- Positiva Compañía de Seguros S.A.
- Coljuegos
- La Previsora S.A. Compañía de Seguros
- Superintendencia de La Economía Solidaria
- Fondo Adaptación
- Unidad Administrativa Especial de Información y Análisis Financiero - UIAF
- Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales – ITRC
- Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF

En su dinámica funcional externa, la CGN interactúa con todas las entidades públicas en materia contable, por cuanto estas son la fuente primaria de la contabilidad pública y generan el insumo básico para la elaboración de los productos y servicios que presta la entidad. Del mismo modo, interactúa con grupos de interés especializados como la CGR, Ministerio de Hacienda y Crédito Público, DANE, DNP, Banco de la República, Fondo Monetario Internacional - FMI, Banco Mundial, organismos de cooperación internacional, la academia y la ciudadanía en general.

La CGN, al igual que todas las entidades del gobierno nacional, debe ceñirse a las políticas de gobierno enmarcadas en el plan nacional de desarrollo vigente y en los planes sectoriales derivados de este; así las cosas, todo su contexto interno debe reflejar sincronía y alineación con el contexto externo en relación con los objetivos de gobierno.

En el contexto general de la CGN se identifican los siguientes elementos DOFA relacionados con el presente PCN:

CONTEXTO ORGANIZACIONAL CGN PARA PCN			
CONTEXTO INTERNO		**CONTEXTO EXTERNO**	
DEBILIDADES	**FORTALEZAS**	**AMENAZAS**	**OPORTUNIDADES**
Escenarios no contemplados en el análisis BIA	Personal idóneo para activar los planes de contingencia de los procesos críticos	Desastres naturales	Mejora continua del PCN

CONTEXTO ORGANIZACIONAL CGN PARA PCN			
CONTEXTO INTERNO		**CONTEXTO EXTERNO**	
DEBILIDADES	**FORTALEZAS**	**AMENAZAS**	**OPORTUNIDADES**
Listas de contactos desactualizadas	Centro alterno de datos para procesos críticos misional	Asignación insuficiente de recursos que respalden la continuidad de la plataforma tecnológica	Fortalecimiento de la plataforma tecnológica que respalde la continuidad de la entidad
Dificultad para la priorización de recursos y cambios frecuentes en el plan de adquisición	Alineación del Plan estratégico de Tecnologías de la Información con los objetivos de la entidad	Manifestaciones y protestas frecuentes en la ciudad, ocasionando daños intencionados a la infraestructura de la Entidad.	Existencia de nuevas tecnologías informáticas.
Demora en la apropiación de recursos	El Datacenter se encuentra en un área segura y cumple con la normatividad de cableado estructurando y con las características de un data center alterno.	Deficiencia en la interoperabilidad de los sistemas en la plataforma tecnológica y/o ataques externos a la información y las herramientas tecnológicas.	Programas de capacitación, comunicación, transferencias y fortalecimiento del conocimiento para mejorar la continuidad de las operaciones.
Planta de personal insuficiente, alta rotación y tiempo insuficiente para el desarrollo de habilidades	Implementación de la norma del sistema de gestión de seguridad de la información ISO27001:2013	Funcionarios que utilicen la información para fines no laborales.	
Desconocimiento de las características de los procesos, desconocimiento del nivel de responsabilidad y autoridad de los procesos	La CGN cuenta con el Comité Institucional de Gestión y Desempeño que da apoyo a los temas pertinentes a la continuidad del negocio		

CONTEXTO ORGANIZACIONAL CGN PARA PCN			
CONTEXTO INTERNO		**CONTEXTO EXTERNO**	
DEBILIDADES	**FORTALEZAS**	**AMENAZAS**	**OPORTUNIDADES**
Fallas en el sistema de seguridad de la información, desconocimiento de los niveles de responsabilidad y autoridad frente a los sistemas	La entidad cuenta con herramientas o plataforma tecnológicas que garantizan la seguridad y la integridad de los datos		

*Tabla 7: **DOFA de contexto organizacional relacionados PCN***
Fuente: propia

Partes Interesadas

Las partes interesadas requieren que la entidad sea proactiva para afrontar los incidentes e interrupciones del negocio, con el objeto de evitar la paralización de servicios críticos y que, en el caso de que se produzcan, existan mecanismos internos para restaurar las operaciones y procesos a la mayor rapidez en función de la necesidad de dichos servicios.

	PARTE INTERESADA
1	Ciudadanía
2	Servidores públicos
3	Proveedores y contratistas
4	Entes de control
5	Entes de regulación
6	Entes de certificación
7	Organismos multilaterales
8	Academia

*Tabla 8: **Partes interesadas***
Fuente: tomada de www.contaduria.gov.co

Entorno Tecnológico

Inventario de aplicativos informáticos del alcance del PCN

El GIT de Apoyo Informático en cumplimiento de su objetivo de "*Apoyar a través de la tecnología informática y el recurso técnico las actividades de gestión y misión institucionales" y* dar soporte tecnológico a los procedimientos del negocio definidos en el alcance del presente PCN, se requiere mantener una infraestructura de hardware y

aplicaciones de software que garanticen la continuidad de los servicios de tecnología referenciados en la tabla 7.

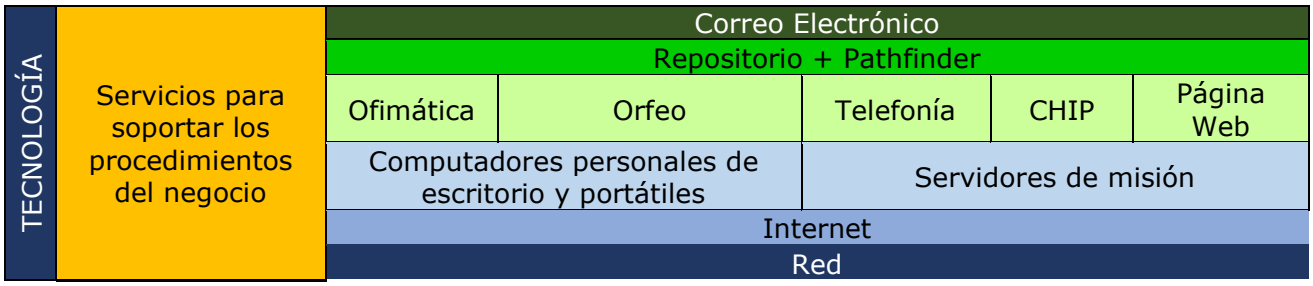


*Tabla 9**: Servicios de tecnología para soporte de procesos del alcance del PCN***
Fuente: Propia

En esencia, la CGN con el apoyo del GIT de Apoyo Informático, debe garantizar el correcto funcionamiento de los siguientes aplicativos de software: Ofimática, Orfeo, Telefonía, CHIP, página web y correo electrónico, además, la infraestructura que los soporta.

Para lo cual se realiza la identificación de los procesos de la entidad y su clasificación de criticidad para la recuperación se realiza clasificando cada procedimiento o actividad acorde con la siguiente definición de nivel:

- **Nivel A:** El procedimiento o actividad es crítica para la entidad. Una operación es crítica cuando al no contar con ésta, la misión de la entidad no puede realizarse.
- **Nivel B:** El procedimiento o actividad es una parte integral de la entidad, sin ésta la entidad no podría operar normalmente, pero la función no es crítica.
- **Nivel C:** El procedimiento o actividad no es una parte integral de la entidad. La entidad podría operar sin ella por un tiempo.

La siguiente tabla presenta un compendio del software de base y operacional que avalan la prestación de los servicios tecnológicos del GIT AI y soportan los procesos y procedimientos organizacionales de la entidad:

Aplicación/ Software	Descripción	Responsable Administración	Servicio	Dato Contacto
IBM Cognos	Reportes	Orlando Chaves Beltrán	Sistema CHIP	3105569961
IBM Informix	Motor de base de datos	Orlando Chaves Beltrán	Sistema CHIP	3105569961

Aplicación/ Software	Descripción	Responsable Administración	Servicio	Dato Contacto
IBM Portal (IBM DB2)	Portal web	Ana María Gómez	Página Web, Intranet	3108613110
ORFEO	Gestión documental	Cristian Sánchez	ORFEO	3124809185
Issabel	Configuración telefonía IP	Lucero Pachón	Telefonía	3142884426
Suite Microsoft Office	Ofimática	Raúl Andrés Garay Torres	Ofimática	3177718308
IHS	Servidor web	Ana María Gómez	Sistema CHIP	3108613110
WAS	Servidor de aplicaciones	Ana María Gómez	Sistema CHIP	3108613110
AdmServices	Servidor de servicios Chip	Ana María Gómez	Sistema CHIP	3108613110
Validadores	Validador de categorías Chip	Ana María Gómez	Sistema CHIP	3108613110
Storage Navigator	Almacenamiento	Ana María Gómez	Sistema CHIP / Medio Magnético	3108613110
Pathfinder	Repositorio	Raúl Andrés Garay Torres	Repositorio	3177718308
GMail	Correo Electrónico	Raúl Andrés Garay Torres	Correo Electrónico	3177718308

*Tabla 10**: Software del alcance del PCN***
Fuente: Propia, con datos del GIT AI

Inventario de hardware del alcance del PCN

El software de base y las aplicaciones necesarias que habilitan los servicios de tecnología para soportar los procesos de negocio de la CGN, se encuentran configurados sobre la siguiente plataforma de hardware:

Componente hardware	Responsable Administración	Servicio	Dato Contacto
Servidor Pandorax	Pedro Martin Grismaldo Moreno	Repositorio fuentes-CHIP-Linux	3203925568
Servidor Pathfinder	Raul Andrés Garay Torres	Servidor de archivos	3177718308
Servidor Galatea1	Orlando Chaves Beltrán	Nueva Ver Tortoise-Win	3105569961

Componente hardware	Responsable Administración	Servicio	Dato Contacto
Servidor Setebos	Lucero Pachón	TSM7.1-Tivoli Storage Manager	3142884426
Librería Cintas	Lucero Pachón	Copias Misionales	3142884426
SAN HITACHI VSP G200	Ana María Gómez	Almacenamiento Misional	3108613110
NAS	Raul Andrés Garay Torres	Backup	3177718308
Switch_Servidores_U	Fabio Hernández Ruiz	Red	3145301170
Servidor Bestla	Raul Andrés Garay Torres	Red (DNS Primario-Win)	3177718308
Servidor Galileo	Raul Andrés Garay Torres	Red	3177718308
Switch _Servicios	Fabio Hernández Ruiz	Red	3145301170
Switches_Usuarios	Fabio Hernández Ruiz	Red	3145301170
Switch-Medellín	Fabio Hernández Ruiz	Red	3145301170
1 Firewall-Medellín	Fabio Hernández Ruiz	Red	3145301170
Servidor Helena	Cristian Sánchez	Linux-Orfeo 5.5	3124809185
Servidor Francisco	Raúl Andrés Garay Torres	Linux-Orfeo 5.5	3177718308
Servidor Europa	Cristian Sánchez	Producción-ORFEO 3.8	3124809185
Servidor Triton	Lucero Pachón	ISSABEL (Telefonía)	3142884426
Servidor Pluton (FTP)	Ana María Gómez	Sistema CHIP (FTP)	3108613110
Servidor Skylab (AIX 7.1)	Ana María Gómez	Sistema CHIP (Validador 4)	3108613110

Componente hardware	Responsable Administración	Servicio	Dato Contacto
Servidor Pheobe	Ana María Gómez	Sistema CHIP	3108613110
Servidor Argos	Ana María Gómez	Sistema CHIP (BD Informix)	3108613110
Servidor Soyuz	Ana María Gómez	Sistema CHIP (WebSphere 8,AdmService RT)	3108613110
Servidor Lapetus	Ana María Gómez	Página web CGN,Intranet	3108613110
Servidor Proteo1	Ana María Gómez	Sistema CHIP (Reporte COGNOS)	3108613110
Switch FC1	Ana María Gómez	Brocade 300 SAN Misional	3108613110
Switch FC2	Ana María Gómez	IBM 298-24 SAN Misional	3108613110
Controladora O SAN HITACHI VSP G200	Ana María Gómez	SAN Misional	3108613110
Controladora 1 SAN HITACHI VSP G200	Ana María Gómez	Misional	3108613110
Controladora 2 SAN HITACHI VSP G200	Ana María Gómez	Misional	3108613110
Router	TIGO - UNE - Tercero	Internet	
Fortinet	Fabio Hernández Ruiz	Internet	3145301170
Controladora O SAN HITACHI VSP G350	Ana María Gómez	SAN Misional Réplica Medellín	3108613110
Controladora 1 SAN HITACHI VSP G350	Ana María Gómez	SAN Misional Réplica Medellín	3108613110
Switch Brocade 300	Raul Andrés Garay Torres	SAN Gestión	3177718308
Switch Brocade 300	Raul Andrés Garay Torres	SAN Gestión	3177718308
Fortianalyzer	Fabio Hernández Ruiz	Plataforma de Reportes	3145301170

Componente hardware	Responsable Administración	Servicio	Dato Contacto
Forti AP	Fabio Hernández Ruiz	Access Point	3145301170
HMC1	Ana María Gómez	Consola de Administración Misional	3108613110
HMC2	Ana María Gómez	Consola de Administración Misional - Medellín	3108613110

*Tabla 11: **Hardware del alcance del PCN***
Fuente: Propia, con datos del GIT AI

Establecimiento de Tiempos de recuperación

Una vez identificados los procesos críticos del negocio de acuerdo con la clasificación del impacto operacional, se procede a establecer los tiempos de recuperación ante catástrofes o caídas de servicios, los cuales se describen a continuación:

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Período Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

*Tabla 12: **Descripción de tiempos de recuperación***
Fuente: Guía 11 – Análisis de Impacto de Negocios

Los tiempos de recuperación en el BIA (Business Impact Analysis) es un proceso sistemático para determinar y evaluar los efectos de cualquier imprevisto que pueda afectar a la continuidad del negocio, orientado a conocer **qué** servicio podría verse afectado y las **consecuencias** sobre los procesos de negocio.

Mediante mesas de trabajo, se estimó el tiempo de recuperación objetivo - RTO, el punto de recuperación objetivo - RPO y el tiempo máximo tolerable – MTD, fuera de servicio para cada proceso crítico en cada componente, estimando así los tiempos de recuperación con

el fin de regresarlos a su operación normal después que ha ocurrido un desastre o caída del servicio y los tiempos de almacenamiento requeridos para disminuir la pérdida de datos.

Para el desarrollo del BIA, como se mencionó anteriormente, es muy importante, además de entender los productos y servicios críticos de la organización, analizar que procesos soportan la entrega de estos servicios.

A continuación, se presentan las actividades realizadas para calcular el BIA:

A. Planeación del BIA
B. Levantamiento de la información
C. Análisis de la información
D. Presentación de resultados

A. *Planeación del BIA:* En esta etapa se planea el desarrollo de las actividades para obtener la información, analizar y aplicar los criterios de determinación del BIA así:
    - Entender previamente los procesos del negocio sobre los que se realizará el BIA.
    - Definir qué procesos del negocio se desea cubrir con el servicio que se suministrará
    - Identificar el personal responsable del servicio
    - Definir el método a utilizar para recolectar la información
    - Unificar criterios y términos utilizados.
    - Definir las fechas en que se realizará el levantamiento de información.
B. *Levantamiento de información*: Se realiza la recolección de la información necesaria para ser luego analizada con los responsables de cada componente tecnológico de acuerdo con el servicio. Ver en ayuda de memoria de trabajo evidencia BIA – PCN archivo adjunto Ayuda Memoria Trabajo BIA-PCN.pdf
C. *Análisis de la información*: Se procede a organizar, tabular y analizar la información recolectada, generando cuadros que permitan comprender de manera más sencilla los diferentes aspectos evaluados.
D. *Presentación de Resultados*: Una vez recolectada y analizada la información se presentan los resultados que arroja el análisis de la información BIA.

Componente tecnológico	RPO	RTO	WRT	MTD	Procesos	Normalización y Culturización Contable (5)	Centralización de la Información (14)			Consolidación de la Información (8)		Gestión TICs (10)		
	(Horas)				Procedimientos	NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA	CEN-PRC16 GESTIÓN A LA INFORMACIÓN	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORÍA	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE	CON-PRC12 CONSOLIDACIÓN CONTABLE	GTI-PRC01 SOPORTE A USUARIOS (MESA DE SERVICIO)	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA	GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO
Correo Electrónico	1	1	1	2		X	X	X			X	X		
PathFinder	4	1	4	5				X	X		X		X	
Aula virtual	4	1	4	5				X					X	
Siscon	4	1	4	5				X					X	
GLPI	4	1	4	5				X				X		
Ofimática*	1	1	1	2		X	X	X	X	X	X			
Orfeo	8	2	1	3			X	X		X				
Telefonía	24	3	2	5								X		
CHIP	5	4	4	8			X		X	X				
Página Web	24	4	1	5					X			X		
Intranet	24	4	1	5								X		
Computadores Personales de escritorio y portátile	8	5	2	7		X	X	X	X	X	X	X	X	X
Servidores de misión	8	24	2	26			X		X	X	X			
Internet	8	1	1	2		X	X	X	X			X	X	X
Red	8	2	1	3		X	X	X	X	X	X	X	X	X

*Tabla 13: **Tiempo de respuesta servicios tecnológicos en el alcance del PCN***
Fuente: Propia, con datos del GIT-AI

MTD (Maximun tolerable Downtime/Outage): es el tiempo máximo de inactividad que la organización puede tolerar la ausencia o no disponibilidad de una función o proceso, se obtiene de la suma de RTO y WRT.

RTO (Recovery Time Objective): Es el tiempo y nivel de servicio en el que debe ser restaurado un proceso de negocio después de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

RPO (Recovery Point Objective): Es el período máximo tolerable de pérdida de datos antes de ser restablecido como consecuencia de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.
WRT (Work Recovery Time): Tiempo de trabajo en recuperación

7.1.1.1 Definición de Los procesos críticos

Procesos de negocio

De acuerdo con lo descrito en la tabla 2; los procesos críticos de negocio que son objeto del presente PCN son: "Normalización y Culturización Contable"; "Centralización de la Información"; "Consolidación de la Información" y "Gestión Tics".

Tecnología requerida

Para soportar los procesos de negocio, el GIT AI requiere mantener en operación los siguientes servicios tecnológicos: Red, Internet, PCs, Servidores, Ofimática, Orfeo, Telefonía, CHIP, Página Web y repositorios. Esto se evidencia en los requisitos de operación

que se describen en cada uno de los procedimientos organizacionales.

La siguiente tabla muestra la relación negocio-tecnología mediante la identificación de las necesidades tecnológicas de los procedimientos de negocio.

AE										
NEGOCIO	Procesos	Normalización y Culturización Contable (5)	Centralización de la Información (14)			Consolidación de la Información (8)		Gestión TICs (10)		
	Procedimientos	NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA	CEN-PRC16 GESTIÓN A LA INFORMACIÓN	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORÍA	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE	CON-PRC12 CONSOLIDACIÓN CONTABLE	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA	GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO	
NECESIDAD	Apoyo tecnológico requerido por el procedimiento	PCs, Red, Ofimática, Repositorio, Correo Electrónico, Internet	PCs, Red, Ofimática, Orfeo. Correo Electrónico, Internet, Sistema CHIP	PCs, Red, Ofimática, Correo Electrónico, Internet, Orfeo, Repositorio, Página Web, Sistema CHIP	PCs, Red, Ofimática, Repositorio, Página Web, Sistema CHIP	PCs, Red, Ofimática, Orfeo, Sistema CHIP	PCs, Red, Ofimática, Correo Electrónico, Internet, Repositorio Pathfinder, Sistema CHIP	PCs, Red, Ofimática, Correo Electrónico, Página Web, Correo Electrónico, Internet	PCs, Red y Repositorio	PCs, Red, Internet
TECONOLOGÍA	Servicios para soportar los procedimientos del negocio	Correo Electrónioco								
		Repositorio + Pathfinder								
		soo			Orfeo		Telefonía	CHIP	Página Web	
		Computadores	Personales de escritorio y portátiles				Servidores de misión			
		Internet								
		Red								

Tabla 14: ***Relación negocio-tecnología en alcance del PCN***
Fuente: Propia, con datos de las tablas 2, 6 y 7

Periodos Críticos

A pesar de que un desastre tecnológico o natural se puede presentar en cualquier momento, se identifican como más relevantes los periodos de corte para los envíos de información de cada categoría y el período para la construcción del balance general de la nación.

Así los periodos identificados son:
Febrero 1 – marzo 15
Abril 1 – mayo 15
Junio 30 – Julio 31
Septiembre 30 – diciembre 15

Recursos mínimos para operar en Contingencia

Se requiere contar con una contingencia para operar los servicios tecnológicos descritos en la tabla 8 compuesta por:

- Red de datos.
- Servidor AIX con unidad propia de almacenamiento.
- Servidor Windows con unidad propia de almacenamiento.
- Guías de contingencia por componente, manuales y documentos de operación.
- Telefonía celular o fija o cualquier medio que facilite la comunicación.

Recursos Financieros

Se requiere tener en cuenta los recursos de inversión necesarios para soportar la contingencia como se menciona en la guía 11 de MINTIC - Análisis de impacto al negocio BIA " es necesario tener en cuenta que los responsables del negocio deben conocer la importancia de tener una inversión de TI planeada que permita innovar tecnológicamente y que responda adecuadamente a los problemas generados por la interrupción de los servicios y permita que las empresas puedan aplicar exitosamente los criterios de recuperación y reanudación de las operaciones del negocio."

Así como tener presentes los costos asociados a la reposición de los activos que tendrán que ser adquiridos como consecuencia de un posible desastre.

Personal mínimo requerido

Aunque ya han sido identificadas algunas personas necesarias para la operación tecnológica del hardware y el software (Tablas 8 y 9), en capítulos posteriores se completará con las personas de la operación estratégica y de negocio.

Tiempos de respuestas

Para asegurar la rápida reacción de los servicios tecnológicos que facilitan la continuidad de las actividades de negocio de la CGN se establecen los tiempos (en horas), que determinaran sus acuerdos de niveles de servicio (ANS).

7.1.2 Gestión del Riesgo

En esta etapa se identifican las amenazas o riesgos específicos que enfrenta la CGN en sus procesos y servicios críticos del negocio, identificados como resultado del Análisis de Impacto al Negocio (BIA), con el objetivo de determinar cómo algunos riesgos serán

controlados y mitigados a un nivel aceptable según criterios definidos de acuerdo con la metodología.

Estos riesgos se analizarán desde la perspectiva de la continuidad del negocio considerando escenarios y tecnología relacionados con los procesos determinados como críticos.

Las vulnerabilidades y amenazas a que se ven expuestos los activos de información serán las relacionadas con la indisponibilidad del servicio, de igual manera se debe realizar una efectiva gestión de riesgo y así evitar la materialización de estos.

7.1.2.1 Clasificación de Escenarios de Riesgo

A continuación, se identifican los posibles escenarios de riesgos potenciales y causas de interrupción tecnológica de acuerdo con el nivel de impacto en los procesos críticos del negocio:

	Escenario	Causa de Interrupción	Descripción
DESASTRES NATURALES			
22	Terremoto, Incendio, Colapso edificio Presencia de gases tóxicos o inflamables Inundación Ataques Terroristas	No disponibilidad de componentes de infraestructura tecnologica	Se presenta cuando uno o algunos de los componentes de la infrestructura tecnologica de la entidad se encuentra fuera de servicio por falla(s) o por la interrupción prolongada
3		No contar con los Proveedores Externos Claves	Ocurre cuando una o varias actividades del proceso crítico son realizadas por un(os) proveedor(es) y cualquier falla de éste (estos), generaría la no realización o interrupción de las actividades del proceso
9		Acceso a la edificación	Relaciona los controles, los procedimientos y las buenas prácticas que permiten mitigar el riesgo de que personal no autorizado ingrese a las instalaciones y pueda generar daños a los activos ()tecnológicos) de la CGN.
23		Administración y entorno tecnológico	Hace referencia a los hábitos y las buenas prácticas que permiten administrar, asegurar, disponer y controlar los sistemas tecnológicos, de tal forma que estén alineados con los estándares internacionales y regulaciones acionales en temas de seguridad de la información.
18		Protección anti-incendios	Relaciona la capacitación del personal, los equipos de extinción y los sistemas de control que permitan responder rápida y eficientemente a un incendio en el edificio y/o en el centro de cómputo.
11		Riesgos potencia eléctrica	Se refiere a las políticas, los controles y los procedimientos que permitan asegurar el suministro de energía eléctrica al edificio y equipos críticos.
18		Riesgos telecomunicaciones	Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.
4		Centro de datos	Hace referencia a los controles, infraestructura y procedimientos definidos para los centros de datos (principal y contingencia)
DAÑOS ACCIDENTALES O FORTUITOS			
21	Caidas totales o parciales de los servicios	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Se presenta cuando uno o varios de los servicios de la plataforma tecnologica de la entidad se encuentra fuera de servicio por falla(s) o por la interrupción prolongada

*Tabla 15**: Escenarios de riesgos potenciales y sus causas***
Fuente: propia con datos CGN

7.1.2.2 Metodología del Riesgo

La metodología de riesgos utilizada para el plan de continuidad de negocio es la aprobada por la CGN contemplada en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas", expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Función Pública que incluye:

A. Estimación del riesgo
B. Evaluación del riesgo
C. Tratamiento del riesgo
D. Plan de tratamiento del riesgo
E. Monitoreo y revisión

Como resultado de la valoración de procesos consultar Anexo 3 resultados valoración de procesos y a continuación se muestra el resumen de la valoración de los procedimientos críticos:

Abreviaturas empleadas en la tabla 14:

- CR-Complejidad Recuperación
- CRI-Criticidad
- IMP-Impacto
- PR-Probabilidad
- RS-Riesgo
- ZR-Zona Riesgo
- PON-Ponderación
- Rea-Realizable
- Est-Estándar
- Fac-Fácil
- Dif-Difícil
- Pro-Probable
- Pos-Posible
- Imp-Improbable
- Mod-Moderado
- May-Mayor
- Men-Menor
- Ext-Extrema
- Med-Media

1. IDENTIFICACIÓN DE LOS PROCESOS			Impacto operacional	2. ANÁLISIS DE RIESGO DE LOS PROCEDIMIENTOS DEL PROCESO							
Proceso	**Descripción de Proceso**	**Procedimientos**	**Nivel**	**CR**	**CRF**	**IMP**	**PR**	**RS**	**ZR**	**PON**	**REQUIERE PLAN DE CONTIN. DE NEGOCIO**
Gestión TICs (11)	Apoyar a través de la Tecnología Informática y el recurso técnico las actividades de gestión y misión institucionales.	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA	A	Rea	Ext	May	Pro	16	Alta	64	**SI**
		GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO	A	Rea	Med	Mod	Pos	16	Alta	64	**SI**
Normalización y Culturización Contable (5)	Asegurar que las actividades de investigación contable, normalización y estrategias de capacitación permitan la generación de información contable pública uniforme, garantizando su rigor técnico	NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05	A	Fac	Alta	Men	Pro	12	Alta	36	SI
Centralización de la Información (14)	Garantizar que las actividades de asesoría, asistencias técnicas, implementación de normas y parametrizaciones contables en los sistemas, facilite centralizar la información	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA	A	Est	Med	Mod	Pro	12	Alta	36	SI
		CEN-PRC16 GESTIÓN A LA INFORMACIÓN	A	Rea	Med	Mod	Pos	16	Alta	48	SI

1. IDENTIFICACIÓN DE LOS PROCESOS			Impacto operacional	2. ANÁLISIS DE RIESGO DE LOS PROCEDIMIENTOS DEL PROCESO							
Proceso	**Descripción de Proceso**	**Procedimientos**	**Nivel**	**CR**	**CRF**	**IMP**	**PR**	**RS**	**ZR**	**PON**	**REQUIERE PLAN DE CONTIN. DE NEGOCIO**
	reportada por las entidades contables públicas a través de las categorías definidas en los sistemas integrados de información nacional (CHIP, SIIF y SPGR), asegurando que cumplan con parámetros de consistencia, oportunidad y calidad.	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORÍA	A	Est	Ext	May	Pro	16	Alta	32	SI
Consolidación de la Información (8)	Suministrar información financiera consolidada y/o agregada de base contable de conformidad con el mandato constitucional y legal, de manera que atienda los requerimientos de los diferentes usuarios.	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE	A	Est	Med	Mod	Pos	16	Alta	64	SI
		CON-PRC12 CONSOLIDACIÓN CONTABLE	A	Rea	Med	May	Imp	16	Alta	64	SI

*Tabla 16: **Resumen de valoración procedimientos críticos***
Fuente: adaptado de la Guía 10 MinTic - "Guía para la preparación de las TIC para la continuidad del negocio", con datos de la CGN

7.1.2.3 Identificación de Amenazas

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de la información, que podría tener un potencial efecto negativo sobre algún componente de la plataforma tecnológica y permitir la afectación de los activos de información. Se cuenta con los siguientes ejemplos:

Naturales	Instalaciones	Humanos	Tecnológicas	Operacionales
Inundaciones	Fuego	Pérdida o Ausencia de Personal Clave	Sabotaje Informático, Ciberamenazas	Crisis Financiera
Incendios	Explosión	Problemas de Transporte	Fallas en el Centro de Datos	Perdida de Proveedores críticos
Sismos	Caída de Energía	Fallas Proveedores de Servicios	Perdida de Datos Sensibles	Fallas en Equipos
Tormentas Eléctricas	Daño por Agua	Huelgas, Marchas o Protestas	Fallas de Hardware Crítico	Aspectos Regulatorios
Tormentas	Pérdida de Acceso	Epidemias - Pandemia	Fallas de Software Crítico	Mala Publicidad
Huracanes	Falla Mecánica	Motines	Fallas en la Red de Comunicaciones	
Tornados	Deterioro - Daño	Actos Hostiles	Fallas en las Líneas Telefónicas	
		Manipulación de Materiales Peligrosos	Problemas Técnicos	
			Fallas en los Proveedores de TI	

Las amenazas pueden ser catalogadas dentro de los siguientes tipos para la CGN:

Riesgo	Amenaza en matriz de riesgos seguridad	Descripción del riesgo
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Integridad	9	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Perdida de Integridad	5	Riesgos de navegación de usuarios, privilegios de descarga e instalación y uso de software en los sistemas operativos de los equipos de cómputo y servidores
Pérdida de Disponibilidad	19	Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad (procesamiento, almacenamiento, memorIa)
Pérdida de Disponibilidad	18	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia
Pérdida de Disponibilidad	19	Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad (procesamiento, almacenamiento, memorIa)
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	10	Indisponibilidad del canal de comunicación (internet, intranet)
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	4	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnologica.
Pérdida de Disponibilidad	18	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia

*Tabla 17**: Amenazas***
Fuente: propia

Debido al carácter tecnológico de este PCN y con el propósito de garantizar el mínimo funcional de la entidad en caso de una situación de emergencia; se hace énfasis en los

riesgos asociados a los escenarios identificados en la tabla 13 y en esa medida se establecen los riesgos tecnológicos del negocio.

	Escenario	Riesgo	#Amenaza	Descripción riesgo	Servicio TI
1	Indisponibilidad de componentes TIC	Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Orfeo, Chip, Página Web, correo-e, telefonía, PCs, servidores, Internet, repositorios de datos
		Pérdida de integridad	9	Ataques informáticos internos/ externos a la infraestructura TIC (páginas Web, sw misional, hw, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	Página Web, servidores misionales, PCs, Intranet, ofimática, Chip, telefonía, Orfeo, repositorios de datos, correo-e
2	No contar con los proveedores externos clave	Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Internet, servidores
3	Acceso a la edificación	Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Página Web, servidores misionales, PCs, Intranet, ofimática, Chip, telefonía, Orfeo, repositorios de datos, correo-e
4	Administración y entorno TIC	Pérdida de integridad	5	Riesgos de navegación de usuarios, privilegios de descargas e instalación y uso de sw en los sistemas operativos de la plataforma TIC	PCs, Internet, servidores, Red, repositorios, bases de datos, página Web, Orfeo, correo-e
		Pérdida de disponibilidad	19	Indisponibilidad de los recursos TIC ocasionada por una inadecuada gestión de la capacidad (procesamiento, almacenamiento, memoria)	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
		Pérdida de disponibilidad	18	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Página Web, servidores misionales, PCs, Intranet, ofimática, Chip, telefonía, Orfeo, repositorios de datos, correo-e, Internet
5	Protección anti-incendios	Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
6	Riesgos de potencia eléctrica	Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
7	Riesgos de telecomunicaciones	Pérdida de disponibilidad	10	Indisponibilidad del canal de comunicación (Internet, Intranet)	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
8		Pérdida de disponibilidad	4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
			4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e

	Escenario	Riesgo	#Amenaza	Descripción riesgo	Servicio TI
			4	Daño de información y/o físico en centro de datos o interrupción de operaciones de la plataforma TIC	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e
9		Pérdida de disponibilidad	18	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Servidores misionales, PCs, Chip, telefonía, Orfeo, repositorios de datos, Internet, correo-e

*Tabla 18**: Riesgos y amenazas***
Fuente: propia

Los anteriores riesgos y amenazas afectan los siguientes procesos y procedimientos:

Normalización y Culturización Contable (5)	Centralización de la Información (14)			Consolidación de la Información (8)		Gestión TICs (11)	
NOR-PRC05 PROCEDIMIENTO PRODUCCIÓN DE NORMAS VERSION 05	CEN-PRC12 CIERRE Y APERTURA DE PERIODO DE UNA CATEGORIA	CEN-PRC16 GESTIÓN A LA INFORMACIÓN	CEN-PRC21 PARAMETRIZACIÓN Y MANTENIMIENTO DE UNA CATEGORÍA	CON-PRC01 MANTENIMIENTO DE PARAMETROS DE CONSOLIDACIÓN CONTABLE	CON-PRC12 CONSOLIDACIÓN CONTABLE	GTI-PRC02 ADMINISTRACIÓN DE LA PLATAFORMA TECNOLOGICA	GTI-PRC03 OPERACIÓN CENTRO DE COMPUTO

7.1.2.4 IDENTIFICACIÓN DE VULNERABILIDADES

Una vulnerabilidad es una debilidad o fallo de seguridad de la información asociada a los activos de información, que puede comprometer la integridad, disponibilidad o confidencialidad de esta y se hace efectiva cuando una amenaza la materializa. Se cuente con los siguientes ejemplos de vulnerabilidades:

Personas	Infraestructura_tecnológica	Infraestructura_física	Procesos
Falta de administración del conocimiento	Carencia o deficiencia en procesos de administración de servicios de TI y Seguridad Informática	Carencia de planes de emergencia y administración de crisis	Falta de controles medioambientales
Carencia de capacitación y entrenamiento	Falla o falta de monitoreo oportuno sobre las herramientas de Seguridad Informática	Exposición evidente a incendios e inundaciones	Falta de procedimientos alternos
Insuficiencia capacidad de personas	Inadecuadas estrategias de recuperación	Fallas de potencia eléctrica y en control de picos	Limitaciones de capacidad
Inadecuada preparación ante desastres	Falta de acuerdos de servicio con proveedores o de su seguimiento.	Ubicación o construcción inadecuada de edificios y centros de cómputo.	Falta de definición y seguimiento de acuerdos de nivel de servicio con proveedores críticos
Falta de seguridad laboral y salud ocupacional	Puntos únicos de falla en la infraestructura de TI	Falta de controles medio ambientales	Dependencia y falta de control de proveedores
Falta de pertenencia a la empresa y cultura en continuidad	Alta dependencia de proveedores de TI	Fallas en construcción de edificaciones bajo normas de sismo resistencia.	Falla en la asignación de roles y responsabilidades
Falta de segregación de funciones	Inadecuado gestión y mantenimiento de la infraestructura de TI	Carencia de control de accesos en áreas críticas restringidas.	Falta o fallas en la medición de tiempos y cantidad de recursos críticos
Falla en la administración de proveedores de servicios profesionales	Falta o inadecuados procesos de administración de incidentes, control de cambios y gestión de acceso.	Carencia de definición de planes de atención y evacuación en situaciones de emergencia	Falta de ejecución de jornadas de evacuación del edificio
Falta de políticas de comunicación formal	Falta o inadecuados procesos de administración de capacidad y desempeño.	Fallas relacionadas con aire acondicionado, suministro de energía y potencia eléctrica.	Falta o desactualizados procesos documentados de instalación y desinstalación de software crítico
Falta de políticas de retención de personal	Falla en el Inventario de componentes o partes críticas.	Fallas en el suministro de servicios públicos como el agua y la energía.	
	Ausencia de sitios alternos de procesamiento.	Fallas en los elementos físicos de protección del edificio	
	Inadecuada o deficiente configuración de seguridad		
	Falta de pruebas de recuperación y retorno, restauración de información.		
	Falta o fallas de copias de respaldos de información y configuraciones		
	Falta o falla de centros de custodias (distancia, frecuencia de recolección, convenios).		
	Malas prácticas de desarrollo de software		

Como resultado de la identificación de vulnerabilidades consultar Anexo 4 Resultados identificación de vulnerabilidades y causas por los activos de Información críticos:

7.2 IMPLEMENTACION

7.2.1 Conformación de equipos

Se conforma el "**Equipo de trabajo de PCN**" con los roles requeridos para las funciones del PCN así:

ROL	RESPONSABLE
Encargado de autorizar la continuidad de Negocio de TI	Mauricio Gómez Villegas
Encargado de coordinar la continuidad de Negocio de TI	Jamir Mosquera Rubio
Oficial de Seguridad en la información o quien haga sus veces	Freddy Armando Castaño
Encargado responsable de recuperación tecnológica	Jamir Mosquera Rubio
Líder del proceso Centralización de la Información.	Juan Camilo Santamaría
Líder del proceso Normalización y culturización contable	Rocío Pérez Sotelo

Líder del proceso Consolidación de la información	Elizabeth Soler Castillo
Líder del Proceso Gestión TICs	Jamir Mosquera Rubio

*Tabla 19**: Personal asignado por rol (Grupo PCN)***
Fuente: Propia con datos de la CGN

En función de la gestión de los procedimientos asociados a los procesos de negocio:

Procesos	Procedimiento	Responsable
Normalización y Culturización Contable (5)	NOR-PRCO5 Procedimiento Producción de Normas Versión 06	Rocío Pérez Sotelo
Centralización de la información (14)	CEN- PRC12 Cierre y Apertura de Período de una Categoría	Juan Camilo Santamaría
	CEN –PRC16 Gestión a la Información	Julián Noguera
	CEN- PRC21 Parametrización y Mantenimiento de una Categoría	Pedro Flaminio Martin Díaz
Consolidación de la información (8)	CON-PRC01 Mantenimiento de Parámetros de Consolidación Contable	Jaime Valencia Cubillos
	CON PRC12 Consolidación Contable	Jaime Valencia Cubillos
Gestión TICs (11)	GTI-PRC02 Administración de la Plataforma Tecnológica	Lucero Pachón Ana María Gómez Raúl Andrés Garay
	GTI-PRC03 Operación Centro de Cómputo	Lucero Pachón Fabio Hernández Ruiz

*Tabla 20**: Personal asignado por procedimiento de negocio del alcance del PCN***
Fuente: Propia con datos de la CGN

En función de la gestión del software:

Aplicación /Software	Responsable administrativo
IBM Cognos	Orlando Chaves Beltrán
IBM Informix	Orlando Chaves Beltrán
IBM Portal (IBM DB2)	Ana María Gómez
ORFEO	Cristian Sanchez
Issabel	Lucero Pachón

Suite Microsoft Office	Raúl Andrés Garay Torres
IHS	Ana María Gómez
WAS	Ana María Gómez
AdmServices	Ana María Gómez
Validadores	Ana María Gómez
Storage Navigator	Ana María Gómez
Pathfinder	Raúl Andrés Garay Torres
GMAIL	Luz Andrea Ochoa Leal

*Tabla 21**: Personal asignado por software del alcance del PCN***
Fuente: Propia con datos de la CGN

En función de la gestión del hardware:

Componente hardware	Responsable Administración
Servidor Pandorax	Pedro Martin Grimaldo Moreno
Servidor Pathfinder	Raúl Andrés Garay Torres
Servidor Galatea1	Orlando Chaves Beltrán
Servidor Setebos	Lucero Pachon
Librería Cintas	Lucero Pachon
SAN HITACHI VSP G200	Ana María Gómez
NAS	Raúl Andrés Garay Torres
Switch_Servidores_U	Fabio Hernández Ruiz
Servidor Bestla	Raúl Andrés Garay Torres
Servidor Galileo	Raúl Andrés Garay Torres
Switch _Servicios	Fabio Hernández Ruiz
Switches_Usuarios	Fabio Hernández Ruiz
Switch-Medellín	Fabio Hernández Ruiz
1 Firewall-Medellín	Fabio Hernández Ruiz
Servidor Helena	Cristian Sánchez
Servidor Francisco	Raúl Andrés Garay Torres
Servidor Europa	Cristian Sánchez
Servidor Skathi	Cristian Sánchez
Servidor Skathi 2	Cristian Sánchez
Servidor Triton	Lucero Pachón
Servidor Pluton (FTP)	Ana María Gómez

Servidor Skylab (AIX 7.1)	Ana María Gómez
Servidor Pheobe	Ana María Gómez
Servidor Argos	Ana María Gómez
Servidor Soyuz	Ana María Gómez
Servidor Lapetus	Ana María Gómez
Servidor Proteo1	Ana María Gómez
Switch FC1	Ana María Gómez
Switch FC2	Ana María Gómez
Controladora O SAN HITACHI VSP G200	Ana María Gómez
Controladora 1 SAN HITACHI VSP G200	Ana María Gómez
Controladora 2 SAN HITACHI VSP G200	Ana María Gómez
Router	TIGO - UNE - Tercero
Fortinet	Fabio Hernández Ruiz
Controladora O SAN HITACHI VSP G350	Ana María Gómez
Controladora 1 SAN HITACHI VSP G350	Ana María Gómez
Switch Brocade 300	Raúl Andrés Garay Torres
Switch Brocade 300	Raúl Andrés Garay Torres
Fortianalyzer	Fabio Hernández Ruiz
Forti AP	Fabio Hernández Ruiz
HMC1	Ana María Gómez
HMC2	Ana María Gómez

*Tabla 22**: Personal asignado por hardware del alcance del PCN***
Fuente: Propia con datos de la CGN. Componente Virtualizado

7.2.1.1 Equipo de trabajo de PCN

La estructura del Equipo de trabajo de PCN conformado por los siguientes integrantes: 1) Encargado de coordinar la continuidad de negocio de TI (Coordinador GIT de Apoyo Informático); 2) Oficial de seguridad de la información; 3) Encargado responsable de recuperación tecnológica y 4) Líderes de proceso.

Director de continuidad de Negocio de TI (Contador General de la Nación)			
Coordinador de continuidad de Negocio de TI (Coordinador GIT Apoyo Informático)			
Oficial de seguridad de la información o quien haga sus veces (secretario general)		Líder de recuperación tecnología (coordinador GIT Apoyo Informático) (Administradores de redes y comunicaciones, servidores, aplicaciones, bases de datos)	
Líderes de procesos			
Normalización y Culturización contable	Centralización de la Información	Consolidación de la Información	Gestión TICs

*Tabla 23**: Roles del PCN***
Fuente: propia con datos de la CGN

RESPONSABILIDADES

Director de continuidad de Negocio de TI: Este rol será realizado por el Contador general de la Nación, quien está encargado de autorizar la activación y ejecución del plan de continuidad del negocio, debe reconocer que este PCN permite a la entidad proteger la operación de sus funciones críticas ante un evento de desastre o una interrupción mayor. Es responsable de autorizar la activación de la contingencia en la situación que amerite la activación inmediata.

Director de coordinar la continuidad de Negocio de TI debe: 1) Decidir y autorizar la activación del PCN; 2) Aprobar el presupuesto para la activación del PCN de TI en la Entidad 3) Comunicar la decisión de activación del PCN.

Encargado de coordinar la continuidad de Negocio de TI: Este rol será realizado por el Coordinador del GIT de Apoyo Informático, quien está comprometido en dirigir y liderar todas las actividades del plan de continuidad del negocio, debe reconocer que este PCN permite a la entidad proteger la operación de sus funciones críticas ante un evento de desastre o una interrupción mayor. Para ello aplica mejores prácticas de continuidad del negocio y gestión de recursos que permitan la implementación, ejecución de pruebas y mejora continua del PCN de la CGN. Es responsable de declarar la contingencia en la situación donde se amerite su activación inmediata.

Encargado de coordinar la continuidad de Negocio de TI debe: 1) Decidir la activación del PCN; 2) Solicitar el presupuesto para la implementación, mantenimiento y mejora del PCN de TI en la Entidad; 3) Gestionar el nivel de riesgo tecnológico aceptable; 4) Revisar y gestionar el plan de pruebas del PCN; 5) Velar por el funcionamiento de los

componentes tecnológicos de contingencia durante el evento y 6) Suministrar la información del evento al oficial de seguridad.

Oficial de seguridad de la información o quien haga sus veces: Antes de un evento debe: 1) Asesorar metodológicamente a los líderes de proceso, y al líder de gestión de Información y comunicaciones sobre los esquemas de recuperación de la Entidad; 2)Documentar y actualizar la documentación y procedimientos asociados al PCN; 3) Actualizar la documentación con una periodicidad anual o cada vez que se presenten modificaciones importantes; 4) Proponer la creación, ajuste o eliminación de Políticas de Continuidad; 5) Verificar mediante ejercicios que el esquema contingente, así como los procesos relacionados efectivamente funcionan los ejercicios o pruebas; y 6) Diseñar, proponer y acompañar a los líderes de proceso y encargado responsable de recuperación tecnológica en la realización de ejercicios de continuidad a fin que se obtenga la madurez necesaria que le permita a la entidad estar preparada para asumir con suficiencia cualquier evento de interrupción.

Oficial de seguridad de la información o quien haga sus veces debe: 1) Consolidar los diferentes reportes efectuados por líderes de proceso y encargado responsable de recuperación tecnológica a fin de preparar reporte único dirigido a la Alta Dirección; y 2) Con base en las situaciones presentadas, proponer esquemas de mejora.

Encargado responsable de recuperación tecnológica: Tiene a su cargo la coordinación del equipo de tecnología, tanto interno de la Entidad, como aquel que desarrolla funciones en tecnología que pertenezca a un contratista. Esto con el fin de brindar a la CGN la continuidad de la operación en caso de emergencias, así como la gestión necesaria para recuperar el ambiente de producción a su estado normal; por lo cual debe: Antes de un evento: 1) Canalizar ante la Alta Dirección los proyectos y gastos asociados a mantenimiento y expansión de la plataforma contingente asociada a los procesos críticos de la Entidad; 2) Activar la operación tecnológica en modo contingente; y 3) Atender la petición de los líderes de procesos a fin de realizar las pruebas de contingencia de TI y actualizar el soporte de sus procesos.

Durante un evento: 1) Coordinar las actividades a fin de ofrecer el mejor servicio a los servidores públicos y partes interesadas de la Entidad; 2) Documentar las principales novedades o circunstancias anómalas que se presenten durante la contingencia; 3) En caso de circunstancias que se salgan de curso, para las que no se estaba preparado o para aquellas en las que se exponga fuertemente la información crítica, la vida o integridad de las personas deberá informar sin duda alguna a los miembros de la alta dirección.
Después de un evento: 1) Los administradores de TI presentarán al encargado de coordinador la continuidad de Negocio de TI el reporte sobre la recuperación de las

operaciones; y 2) Verificar que el ambiente de contingencia continúa operando según lo establecido y que la protección permanece.

Líderes de procesos:
Antes de un evento debe: 1) Establecer el grado de criticidad de sus procesos; 2) Realizar análisis de riesgo a los procesos; 3) Estimar los tiempos de recuperación de los sistemas de información que soportan proceso crítico; 4) Determinar en qué punto del tiempo se deben retomar los datos de las aplicaciones (Es decir, qué tanta información se puede perder sin afectar significativamente la actividad de la Entidad); 5) Gestionar los ejercicios que se deben efectuar a los planes de recuperación a fin de garantizar su completitud, efectividad y eficiencia, esto en coordinación con el proceso gestión de Información y comunicaciones y otras áreas con las que se requiera combinar esfuerzos; 6) Presentar los informes de los resultados de las pruebas; y 7) Designar las funciones que los colaboradores de sus grupos deban desarrollar antes, durante y después de un desastre.
Durante un evento: 1) Verificar que el personal mínimo de su grupo esté disponible para asumir las operaciones en modo contingente; 2) Coordinar con el encargado de coordinar la continuidad de Negocio de TI las actividades de recuperación y contingencia; 3) Documentar las principales novedades o circunstancias anómalas que se presenten durante la prueba o contingencia real; 4) Informar cualquier situación que se salga de curso dentro del esquema contingente.
Después de un evento: 1) Coordinar el retorno a la normalidad; 2) Verificar la adecuada condición de la plataforma de producción; y 3) Elaborar reporte sobre la operación en contingencia.

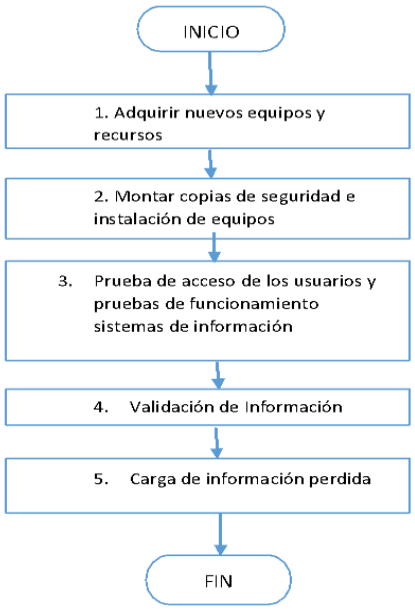
7.2.1.2 Equipo de Recuperación

Las actividades de retorno a la operación normal de la entidad están relacionadas con la estructura física de las instalaciones y la recuperación de los servicios tecnológicos.

Recuperación de las instalaciones:

Las siguientes actividades aplican en caso de que la sede principal de la entidad haya sufrido averías por ocurrencia de los escenarios; terremoto, incendio o colapso de la edificación o caída del servicio:

No.	Descripción de la Actividad	Detalle	Tiempo Estimado
1	Evaluación de daños. Responsable: Coordinador del GIT delegado por la Alta Dirección y/o Junta Directiva	Determinar la gravedad de los daños presentados en las instalaciones físicas de la GCN. La alta dirección y la Junta Directiva deben definir las acciones a realizar para la recuperación de las oficinas de la CGN	1 día
2	¿Se pueden recuperar las instalaciones?	Si, ir a la actividad 3 No, ir a la actividad 4	
3	Realizar arreglos. Responsable: Esto es responsabilidad de GIT de Servicios Generales Administrativos y Financieros	Iniciar las actividades para lograr la recuperación de las instalaciones físicas de la Entidad.	30 días
4	Búsqueda de sede alterna. Responsable: Coordinador del GIT delegado por la Alta Dirección y/o Junta Directiva	Iniciar la búsqueda de sede para alquilar en caso de no poder recuperar las instalaciones principales o durante la recuperación de la instalación principal.	7 días
5	Contratación de oficinas. Responsable: Esto es responsabilidad de GIT de Servicios Generales Administrativos y Financieros	Realizar la contratación de la sede seleccionada para las labores de la Entidad. Se debe firmar el contrato de arrendamiento para iniciar la adecuación y traslado de activos de información.	5 días

6	Adecuación de sede alterna. Responsable: Esto es responsabilidad de los Coordinadores de GIT delegados	Adecuar la nueva sede de operación de la Entidad. Se debe adquirir los equipos de oficina y los elementos necesarios para la adecuación de la nueva sede, tiempo estimado 2 días. Ejecución del proyecto, tiempo 8 días. 	10 días
7	Traslado de sede Responsable: Esto es responsabilidad de los Coordinadores de GIT delegados	Realizar el traslado de funcionarios, documentación y equipos de cómputo a la nueva sede de la Entidad.	1 día
8	Ubicación de los funcionarios. Responsable: Esto es responsabilidad de los Coordinadores de GIT delegados	Realizar la ubicación del personal en la nueva sede alterna de la Entidad. La ubicación de los puestos de trabajo de los funcionarios de la Entidad, se realizarán de acuerdo con el proceso al que pertenece, garantizando la confidencialidad de la información que se maneja.	4 horas

9	Inicio de trabajo en GIT Informática. Responsable: Coordinador del GIT Apoyo Informático	Iniciar las actividades del proceso de Gestión de Tecnología.	2 horas
10	Inicio de trabajo de los procesos de la CGN. Responsable: Líder Procesos y Coordinadores GIT delegados	Iniciar actividades en los demás procesos de la CGN de manera gradual.	2 días

*Tabla 24**: Actividades de recuperación de las instalaciones***
Fuente: Propia

Recuperación de los servicios tecnológicos

Al momento de ejecutar el plan de contingencia se debe tener en cuenta la siguiente secuencia para proceder a la recuperación de los servicios tecnológicos.

Secuencia de recuperación de servicios tecnológicos		
Secuencia	**Servicio**	
	Hardware	**Software**
1	Red	
2	Internet	
3		Correo Electrónico
4	Servidores de misión	
5	Medios magnéticos	
6		Chip
7		Página Web
8		Intranet
9	Servidores de gestión	
10		Telefonía
11		PathFinder
12		Siscon
13		Aula Virtual
14		GLPI
15		Orfeo
16		SIGI
17		Repositorios
18	PCs	
19		Ofimática

*Tabla 25**: Secuencia de recuperación de los servicios del alcance del PCN***
Fuente: Propia con datos de la CGN

Una vez finalizada y revisada la secuencia de recuperación de los servicios tecnológicos el encargado responsable de recuperación tecnológica informará el estado a todos los líderes de procesos de la CGN, que los servicios han sido recuperados a su funcionamiento normal, con el fin de continuar la operación y alerten sobre cualquier anormalidad en la operación.

Estabilización de los servicios tecnológicos

Pasadas **4 horas** de funcionamiento normal continuo, el encargado responsable de recuperación tecnológica realiza un chequeo de los servicios de la tabla 7. De no presentarse novedades, informará al "PCN" y a través de este a toda la entidad; para

luego proceder a documentar el incidente.

Verificación de los servicios tecnológicos

Se requiere continuar con la verificación y el monitoreo de los servicios de la tabla 7 al menos durante las siguientes **8 horas** después de alcanzar su estabilización. Durante este tiempo se debe finalizar la documentación y realizar una retroalimentación en el seno del grupo PCN, además se deberá actualizar este plan y/o el plan de contingencia y/o las guías de contingencias de ser necesarias.

Verificación de la continuidad de la seguridad de la información

La verificación de la continuidad de la seguridad de la información implica mantener las actividades de los procesos garantizando la confidencialidad, disponibilidad e integridad de los activos de información involucrados en el PCN. Este capítulo comprende la continuidad de la seguridad de la información desde la perspectiva tecnológica, cuyas actividades y contenidos deberán ser tenidos en cuenta durante la ejecución del PCN; en particular, de cada actividad de recuperación.

Continuidad de La Seguridad de la Información			
Actividades	**Descripción**	**Responsable**	**Registro**
Requisitos de la Seguridad de la Información en el PCN	Los requisitos de la Seguridad de la Información corresponden a: • Mantener la disponibilidad de las aplicaciones y servidores críticos. • Diseño de controles para establecer las comunicaciones seguras. • Mantener las políticas de seguridad en los equipos perimetrales de seguridad. • Validar y/o configurar las VLANS del personal requerido. • Aplicar las políticas de contraseñas seguras en caso de ser necesario un reinicio. Esta actividad propende por verificar y garantizar la aplicación de los requisitos antes descritos	Líder del Recuperación Tecnológica. Oficial de Seguridad de la Información.	Políticas de Seguridad de la Información y digital
Implementación de la continuidad de la Seguridad de la Información en el PCN	Durante esta actividad, se realiza los diferentes controles que permitan la continuidad de la Seguridad de la Información en caso de materializarse un escenario de los descritos en el documento PCN de la Entidad. Los controles implementados son: • Manual de políticas de Seguridad de la Información y digital. • Contingencia de las aplicaciones del alcance • Contingencia de suministro eléctrico. • Separación de las redes de forma virtual. • Políticas en los equipos de seguridad perimetral. • Definición de personal para la respuesta ante un escenario, actividades y tiempos de recuperación.	Líder del Recuperación Tecnológica Oficial de Seguridad de la Información	Políticas de Seguridad de la Información y digital

Continuidad de La Seguridad de la Información			
Actividades	**Descripción**	**Responsable**	**Registro**
Verificación y evaluación de la continuidad de la Seguridad de la Información	De acuerdo con el plan de pruebas definido en el PCN, y los resultados obtenidos en la primera prueba del PCN en la Entidad, se han definido nuevos tiempos de recuperación.	Encargado de coordinar la continuidad de Negocio de TI Líder del Recuperación Tecnológica	Plan de pruebas
Mejoramiento en la continuidad de la Seguridad de la Información	Durante esta actividad se realiza las mejoras evidenciadas, de acuerdo con la documentación del incidente ocurrido y a la continuidad de la Seguridad de la Información.	Encargado de coordinar la continuidad de Negocio de TI Oficial de Seguridad de la Información	Acciones correctivas y de mejora

*Tabla 26**: Continuidad de la seguridad de la información***
Fuente: Propia con datos de la CGN

Los controles que se requieren para la continuidad de la seguridad de la información del PCN de la entidad son:

a) Disponibilidad de los aplicativos: Pagina Web, CHIP, Servidores de Aplicaciones, Servidores Web, Servidores de bases de datos.
b) Disponibilidad del suministro eléctrico de la entidad.
c) Mantener el nivel de cifrado de las comunicaciones de servicio de correo electrónico.
d) Mantener la recepción de los oficios para los actos administrativos.
e) Establecer la comunicación por VPN entre la sede alterna y/o sede proveedor con los servidores ubicados en la oficina principal de la entidad.

En caso de bloqueo de acceso a las cuentas de correo del personal crítico, restablecer contraseñas seguras de acorde a las políticas de Seguridad de la Información definidas.

7.2.1.3 Logística

Proporcionará todos los recursos físicos, tecnológicos, de transporte, soporte técnico y demás necesarios para llevar a cabo las actividades de recuperación.

Está conformado por el encargado de coordinar la continuidad de Negocio de TI Coordinador GIT de Apoyo Informático y el secretario general.

Su función consiste en proporcionar la logística necesaria para disponer del transporte de equipos tecnológicos y personas o cualquier elemento físico que se requiera, así como suministrar los medios de comunicaciones, adquisición, alquiler o compra de recurso tecnológico.

Cuando suceda un evento o incidente que provoque la materialización de un riesgo identificado en este Plan, el servidor público afectado deberá realizar el respectivo reporte de inmediato a través de la mesa de servicios a la ext. 633 o al correo electrónico mesadeservicio@contaduria.gov.co. Una vez reportada la contingencia se activará por parte del encargado de coordinar la continuidad de Negocio de TI el respectivo procedimiento para el manejo de la interrupción.

De manera periódica y preventiva se debe:

- Verificar el directorio telefónico de contacto de los servidores públicos responsables y mantenerlo actualizado.
- Verificar los procedimientos de copia y restauración de seguridad de la información.
- Realizar jornadas de capacitación sobre el plan, a servidores públicos de la CGN sobre las actividades a seguir.
- Habilitar el servicio de conectividad con los proveedores y correo electrónico que se tiene definido para garantizar el servicio.
- Mantener habilitado el servicio de centro de datos alterno.
- Realizar las pruebas establecidas en el presente plan en los tiempos definidos.

7.2.1.4 Equipo de Pruebas

El plan de continuidad de negocio de la CGN debe ser probado al menos una vez al año.

Es responsabilidad de los líderes de procesos gestionar la realización de una prueba anual en la que se verifique la operación de los procesos y componentes tecnológicos de contingencia.

Las pruebas se deben programar al menos con un 1 mes de antelación.

Los tipos de pruebas que se deben realizar son:
Pruebas Unitarias: Se prueba cada elemento que compone la solución de respaldo en forma independiente. No se afectan los servicios de producción ni demás.

Pruebas integradas: Se prueban en forma integrada dos o más componentes de la solución de respaldo sin afectar los servicios de producción.
Pruebas totales: Verifican el funcionamiento de todos los elementos descritos en el plan de contingencias y secuencia de recuperación en todos los escenarios identificados.

INFORME DE PRUEBAS

Realizar un documento para evidenciar el resultado de las pruebas al PCN, que contenga al menos lo siguiente: fecha, tipo de prueba, objetivo de la prueba, escenario probado, componente tecnológico, descripción detallada de la prueba, responsable de las pruebas y personas que intervinieron; además un aparte que evidencie un análisis general de la prueba identificando las fallas y las oportunidades de mejora.

7.2.1.5 Plan de Pruebas

El plan requiere ser probado periódicamente al menos una vez al año, a fin de comprobar el funcionamiento de las actividades establecidas para atender la interrupción de un servicio tecnológico teniendo en cuenta lo siguiente:

- Establecer programación periódica de pruebas de cada componente de los servicios tecnológicos determinados en este plan, como control de calidad.
- Realizar pruebas al efectuar cambios representativos en la plataforma.
- Realizar pruebas al proveer que existe un riesgo de que suceda un incidente o evento que afecte un servicio de TI
- Realizar ejercicios de entrenamiento
- Realizar las pruebas basándose en las guías de cada componente seleccionado en este plan
- El registro de la prueba se debe realizar en el formato Anexo 5. pruebas del plan de contingencia tecnológica de este documento

Una vez ejecutadas las pruebas, es necesario efectuar una evaluación o revisión de su desarrollo para detectar las fallas y fortalezas para así realizar las actualizaciones pertinentes, si procede, con las experiencias obtenidas de los mismos.

Pruebas unitarias:

Tipo de prueba	Objetivo	Escenario /Interrupción	Componente	Descripción Prueba	Responsable	Fecha
Unitarias			Red			

	Probar cada componente de la solución de respaldo en forma independiente. No afectan servicios en producción.	Terremoto/ No disponibilidad componentes de infraestructura Inundación Presencia de gases tóxicos o inflamables/ Acceso a la edificación Colapso edificio/ Riesgo en telecomunicaciones	Internet	Probar la guía de contingencia de cada componente. Donde aplique, utilizar un ambiente de prueba o de contingencia	Encargado responsable de recuperación tecnológica	Según Cronograma
			Correo electrónico			
			Servidores de misión			
			Sistema Chip			
			Página web			
			Intranet			
			Telefonía			
			Orfeo			
			Siscon			
			Aula Virtual			
			GLPI			
			Repositorios			
			PCs			
			Ofimática			

Pruebas integradas:

Tipo de prueba	Objetivo	Escenario /Interrupción	Componente	Descripción Prueba	Responsable	Fecha
Integradas	Probar dos o más componentes de la solución de respaldo. No afectan servicios en producción	Terremoto/ No disponibilidad componentes de infraestructura Inundación Presencia de gases tóxicos o inflamables/ Acceso a la edificación Colapso edificio/ Riesgo en telecomunicaciones	Sistema Chip	Probar el plan de continuidad y el plan de contingencia con apoyo de las guías de contingencias para los componentes seleccionados	Encargado responsable de recuperación tecnológica	Según Cronograma
			Página web			
			Intranet			
			Correo electrónico			
			Siscon			
			Aula Virtual			
			GLPI			
			Orfeo			
			Telefonía			
			Ofimática			
			PCs			

Pruebas totales:

Tipo de prueba	Objetivo	Escenario /Interrupción	Componente	Descripción Prueba	Responsable	Fecha
Totales	Probar el protocolo establecido en el plan de continuidad; probar el plan de contingencias para todos los componentes identificados. Afecta a los servicios en producción	Seleccionar	Red Internet Correo electrónico Servidores de misión Sistema Chip Página web Intranet Telefonía Siscon Aula Virtual GLPI Orfeo Repositorios PCs Ofimática	Seleccionar un (1) escenario y simular la situación de recuperación de desastre de un (1) proceso, apoyados en los recursos de tiempo (tabla 11), personal (tablas 19-20) y secuencia de recuperación de servicios (tabla 23)	Encargado de coordinar la continuidad de Negocio de TI, encargado responsable de recuperación tecnológica, Líderes de procesos	Según Cronograma

7.3 PLAN DE RECUPERACIÓN DE DESASTRES - DRP

El Plan de Recuperación de Desastres Informáticos - DRP de la Contaduría, es parte integral del Plan de Continuidad del Negocio de TI – PCN y tiene como objetivo principal la continuidad de la operación de las áreas críticas del negocio ante alguna interrupción.

El DRP se centra en la recuperación de los recursos tecnológicos y datos requeridos para operar en caso de una interrupción de los procesos determinados como críticos en el BIA.

Este documento describe las estrategias del GIT de Apoyo Informático para la recuperación de los sistemas de información, aplicaciones, herramientas y servicios de TI requeridos por el BIA. Además, incluye guías detalladas de recuperación paso a paso para la activación de los servicios principales y la replicación del sistema CHIP que es el más crítico para la Contaduría.

El **RPO (Recovery Point Objective)** define el tiempo máximo tolerable de pérdida de datos antes de ser restaurados tras un desastre o interrupción, con el objetivo de evitar consecuencias inaceptables para la continuidad del negocio. Este tiempo debe ser reevaluado de forma periódica para reducir la brecha de datos entre el centro de datos principal y el alterno, buscando mantenerlo lo más cercano posible al tiempo real.

Este período de recuperación se mide desde el momento en que se notifica el incidente hasta que los usuarios funcionales tienen acceso a los aplicativos críticos, con la expectativa de que se logre en el menor tiempo posible.

Por su parte, el **DRP (Disaster Recovery Plan)** se ajusta a los planes de contingencia de la CGN, conforme a sus guías y procedimientos de TI. Estos procedimientos incluyen la replicación de datos en el centro de datos alterno, así como la verificación de versiones, parches y actualizaciones en comparación con el centro de datos principal. Este proceso tiene como objetivo asegurar que el centro de datos alterno esté alineado con el principal, de modo que, ante un evento contingente que requiera su activación o durante las pruebas y simulacros, se garantice la capacidad de operar los procesos críticos de la entidad

7.4 GESTION

7.4.1 Respuesta a eventos

Durante el evento de fenómenos naturales como terremoto, Incendio, colapso edificio, presencia de gases tóxicos o inflamables, Inundación, ataques terroristas y/o caídas totales o parciales de los servicios cuando el personal esté presente debe:

Tipo de evento: terremoto, Incendio, colapso edificio, presencia de gases tóxicos o inflamables, Inundación, ataques terroristas			
Qué hacer	**Como hacerlo**	**Quien lo hace**	**Cuando lo hace**
Control de las acciones	Conservar la calma	Todo el personal	En el momento del evento
Salvaguardar los equipos	Apagar y desconectar los equipos de cómputo, servidores, salir de la red	Todo el personal	Inmediatamente se tenga conocimiento del evento
Tomar acciones dependiendo del evento	Utilizar las herramientas para la mitigación del evento	Brigadistas, personal con conocimiento en el manejo de emergencias	Inmediatamente se tenga conocimiento del evento

Tipo de evento: caídas totales o parciales de los servicios			
Qué hacer	**Como hacerlo**	**Quien lo hace**	**Cuando lo hace**
Identificación de falla en el servicio	Percepción de la caída del servicio y reporte del evento	Todo el personal	En el momento del evento
Control de las acciones	Identificación del componente de TI afectado	Administrador del componente	En el momento del evento
Verificación del estado del componente	Análisis y diagnóstico del componente	Administrador del componente	Inmediatamente se tenga conocimiento del estado del componente
Tomar acciones dependiendo del estado del componente de TI	Utilizar los procedimientos y herramientas para la mitigación del evento	Administrador del componente	Inmediatamente se tenga conocimiento del estado del componente

7.4.2 Después del Evento

Las actividades que se mencionan a continuación corresponden a las acciones que deben realizar los usuarios de acuerdo con los escenarios catalogados como catástrofes naturales y otros, es decir, terremoto, incendio, colapso edificio, presencia de gases tóxicos o inflamables, Inundación, ataques terroristas o en caso de caídas totales o parciales de los servicios.

FASE I			
Qué hacer	**Cómo hacerlo**	**Quien lo hace**	**Cuando lo hace**
Abandonar las instalaciones y ubicarse en un área externa segura	Rápidamente sin correr, conservando la calma, usando las rutas de evacuación previamente establecidas y siguiendo las instrucciones de los brigadistas. Si hay humo utilizar un pañuelo o prenda húmeda para cubrirse la boca y la nariz Si se encuentra en pisos superiores abrir las ventanas para que el humo salga	Todo el personal	Durante el evento

FASE I			
Qué hacer	**Cómo hacerlo**	**Quien lo hace**	**Cuando lo hace**
	Si es un terremoto desalojar las instalaciones solo cuando el terremoto acabe. Alejarse de objetos que puedan caer.		
Declarar urgencia manifiesta	Mediante acto administrativo	Contador General de la Nación	Durante las dos horas siguiente a la ocurrencia del siniestro
Suplir de energía eléctrica piso 15 de la entidad	1. Reunión del comité de emergencias y desastres de la entidad con la persona encargada de la administración del edificio. 2. Diagnóstico del estado de las instalaciones de la entidad 3. De acuerdo con los procedimientos implementados por el edificio tomar decisiones para suplir la energía eléctrica en el edificio y para superar los demás daños 4. Contratar o adquirir UPS si es necesario	Comité de Emergencias y Desastres y Coordinador del GIT servicios generales, administrativos y financieros	Durante las doce horas siguientes a la ocurrencia del siniestro
Verificar estado operacional del centro de datos	1. Identificar funcionalidad y operabilidad de cada uno de los componentes de TI alojados en el centro de datos 2. Dependiendo de los daños y el estado de las instalaciones estudiar la posibilidad de habilitar espacios de trabajos. 3. Dependiendo del estado de la infraestructura tecnológica validar la posibilidad de adquirir o alquilar equipos de cómputo, servidores, equipo de ventilación, y demás que permitan restablecer los servicios prestados por la CGN	Coordinador del GIT de apoyo informático, Coordinador del GIT servicios generales, administrativos y financieros	Inmediatamente se declare la urgencia manifiesta y durante las 24 horas siguientes a la ocurrencia del siniestro

FASE I			
Qué hacer	**Cómo hacerlo**	**Quien lo hace**	**Cuando lo hace**
Reposición de equipos	Tramitar la garantía de la póliza contra todo riesgo para reponer los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones.	Coordinador del GIT servicios generales, administrativos y financieros Coordinador del GIT de apoyo informático	Durante las 48 horas siguientes al reporte del estado de los equipos presentado por el Coordinador del GIT de apoyo informático
Cerrar el proceso	Presentar un informe del incidente, de las acciones de respuesta aplicadas o acciones correctivas, proponer las acciones preventivas y de mejorar para evitar reincidencias	Oficial de seguridad con el apoyo del grupo de seguridad del proceso de Gestión Tics	Posterior a las pruebas a satisfacción

FASE II			
Qué hacer	**Cómo hacerlo**	**Quien lo hace**	**Cuando lo hace**
Recuperar la información	1. Solicitar las copias de seguridad externas. 2. Asignar el personal de recuperación de información, horarios y tareas 3.Realizar las actividades descritas en el plan de continuidad para el restablecimiento de la operación de acuerdo a los componentes y servicios que fueron catalogados como prioritarios	Coordinador del GIT de apoyo informático Equipo operativo de recuperación de acuerdo a las tareas asignadas y roles	Durante las 24 horas siguientes a la ocurrencia del siniestro Una vez esté disponible el Datacenter provisional e iniciar antes de las 48 horas de la ocurrencia del siniestro
Restaurar servicio de internet	1. llamar al soporte técnico del proveedor de internet 2. Realizar las gestiones pertinentes para restaurar el servicio	Administrador de red	Durante las 24 horas siguientes a la ocurrencia del siniestro

Diagnóstico estado recursos tecnológicos	1. Verificar el estado de los equipos de cómputo y establecer la necesidad de compra o alquiler 2. Efectuar mantenimiento al recurso tecnológico susceptible de recuperación	Coordinador del GIT de apoyo informático y sus Grupos de Infraestructura y soporte	Durante las 24 horas siguientes a la ocurrencia del siniestro
Efectuar pruebas de la operación del sistema	1. Realizar pruebas de la funcionalidad de los sistemas de información y de la integridad de las Bases de Datos 2. Aplicar las políticas de seguridad de acceso lógico al sistema	Coordinador del GIT de apoyo informático y sus Grupos de Infraestructura	Durante las 72 horas siguientes a la ocurrencia del siniestro.
Asegurar la información	Solicitar al proveedor del servicio de copias de respaldo la entrega de los medios magnéticos	Coordinador del GIT de apoyo informático	Durante las 48 horas siguientes a la ocurrencia del siniestro
Comunicar la operación del sistema	Comunicar a la alta Dirección el resultado de las acciones y el restablecimiento de los sistemas de información	Coordinador del GIT de apoyo informático	Inmediatamente se culmine las pruebas al sistema

En la etapa de recuperación se tendrán en cuenta la secuencia de la Tabla 23: secuencia de recuperación de los servicios del alcance del PCN y sus prioridades.

7.5 MEJORA CONTINUA

Se identifican oportunidades de mejora del plan de continuidad del negocio, con el registro de las lecciones aprendidas, identificación de puntos de falla, optimización de pruebas, guías, procedimientos y formatos, realizando evaluación de proceso y con los resultados de los ejercicios de prueba realizados.

La mejora continua del plan de continuidad del negocio de la entidad depende de la asignación de recursos, por cuanto permiten ampliar la capacidad de respuesta ante un incidente, lo cual conlleva a modificar la estrategia generando nuevas guías y procedimientos.

8. BIBLIOGRAFIA

Norma Técnica Colombiana NTC 5722:2012, Continuidad de Negocio, Sistemas de Gestión de Continuidad de Negocio. Requisitos, 2012-10-31, ICONTEC Internacional

Guía para la preparación de las TIC para la continuidad del negocio, Guía 10 de MINTIC

Guía de análisis de Impacto al Negocio, Guía 11 de MINTIC

Norma técnica de sistemas de gestión de seguridad de la información, NTC-ISO-IEC 27001:2013.

Norma internacional para el sistema de gestión y continuidad del negocio, NTC/ISO 22301:2019