PLAN DE CONTINGENCIA TECNOLÓGICA

CONTADURÍA GENERAL DE LA NACIÓN

GIT DE APOYO INFORMÁTICO

Noviembre 2024

CONTADURÍA GENERAL DE LA NACIÓN	**PLAN DE CONTINGENCIA TECNOLÓGICA**		
	PROCESO	**GESTIÓN TICS**	
	FECHA DE APROBACIÓN:	**CÓDIGO:** **GTI-PLN02**	**VERSIÓN:** **4.4**

CONTROL DE VERSIONES					
Ver.	**Sección**	**Tipo**	**Fecha (DD/MM/AA)**	**Autor(es)**	**Obs.**
1.0	Todas	Creación	13 / 12 / 2012	José Leonardo Buitrago	5 guías, 3 diagramas
2.0	Todas	Actualización	22 / 12 / 2014	José Leonardo Buitrago	6 guías, 3 diagramas
3.0	Todas	Actualización	01 / 10 / 2018	Jaime García Gonzáles	34 guías, datos de contacto, directorio
4.0	Todas	Actualización	28/07/2019	GIT Apoyo Informático	
4.1	Todas	Actualización	19/12/2019	GIT Apoyo Informático	15 guías, escenarios, roles y responsabilidades, ANS, riesgos, interrupciones, pruebas
4.2	ANS, Roles y responsabilidades, tiempos de recuperación, secuencia y servicios	Actualización	15/07/2020	GIT Apoyo Informático	Ajuste ANS incluye tiempos de recuperación, cantidad de servicios Roles y responsabilidades Tiempos de recuperación, Secuencia y servicios
4.3	Todas	Actualización	27/05/2022	GIT Apoyo Informático	10 guías, escenarios, riesgos, interrupciones, pruebas, roles y responsabilidades
4.4	Todas	Actualización	XX/11/2024	GIT Apoyo Informático	Riesgos, interrupciones, pruebas Actualización de información Ajuste de tablas e ilustraciones Revisión equipo de apoyo al oficial de seguridad - XX de noviembre de 2024

TABLA DE CONTENIDO

Pág. No

INDICE DE TABLAS

Pág. No

INDICE DE ILUSTRACIONES

Pág. No

1. INTRODUCCIÓN

El presente Plan de Contingencia hace parte de manera integral del Plan de Continuidad del Negocio de la entidad, siendo así un instrumento que permita dar respuesta oportuna, adecuada y coordinada a situaciones de emergencia causadas por fenómenos destructivos de origen natural o humano, contribuyendo así a las acciones operativas requeridas para dar continuidad al negocio y retornar a su estado funcional normal de la plataforma de TI de la Contaduría General de la Nación - CGN para aquellos componentes tecnológicos identificados en el PCN.

Este plan de contingencia implementa las acciones necesarias para controlar las situaciones de emergencia identificadas en el PCN versión 5 y orienta a los administradores de TI en la recuperación de servicios en modo y tiempo de las circunstancias señaladas con el fin de dar respuesta y cumplimiento de las funciones asignadas a la Entidad.

2. GLOSARIO

BIA (Business Impact Analysis (BIA), por sus siglas en inglés) o Análisis del impacto al negocio: Proceso del análisis de actividades de las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.

MTD (Maximun Tolerable Downtime (MTD), por sus siglas en inglés) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la entidad empiece a tener pérdidas y colapse.

SITIO ALTERNO: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción

PCN (Plan de Continuidad del Negocio (PCN), por sus siglas): Es la definición de acciones a realizar, recursos a utilizar y personal a emplear (quién, qué, cómo, cuándo y dónde) en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos o servicios informáticos de la organización para responder, recuperar, reanudar y restaurar la operación a un nivel preestablecido.

RTO (Recovery Time Objective (RTO), por sus siglas en inglés): Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

RPO (Recovery Point Objective (RPO), por sus siglas en inglés): Es el período máximo tolerable de pérdida de datos de un Servicio de TI 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 (WRT), por sus siglas en inglés): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

3. GENERALIDADES

El 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 la Contaduría General de la Nación - CGN, para esto implementan procedimientos alternativos que permiten recuperar el funcionamiento normal de la operación en el menor tiempo posible en diferentes escenarios de desastre.

Una contingencia es una situación de pérdida de la capacidad de procesamiento parcial o total, debida a un incidente que causa que los procesos esenciales de la CGN se detengan por un periodo de tiempo prolongado.

El plan de contingencia se pone en marcha cuando:

1. Sea necesario activar el Plan de Continuidad del Negocio.
2. Se presente pérdida significativa de la capacidad de proceso y degradación considerable del nivel del servicio al cliente.
3. Se manifieste incapacidad de la CGN de cumplir compromisos importantes con las partes interesadas o de proteger sus propios intereses o los de sus funcionarios.

El presente plan de contingencia funciona bajo los siguientes supuestos:

1. La entidad cuenta con el personal mínimo establecido en el PCN.
2. Las ubicaciones de los medios de recuperación se encuentran identificadas, documentadas y disponibles.
3. Todos los proveedores críticos relacionados estarán disponibles y proporcionarán apoyo de manera razonable en las tareas asignadas.
4. Las guías de contingencias han sido mantenidas, están actualizadas y se pueden ejecutar.

4. POLÍTICA DE CONTINGENCIA DE LOS SERVICIOS TECNOLÓGICOS DE LA CGN

El GIT de Apoyo Informático de la CGN, de manera permanente, identificará y anticipará la pérdida de las capacidades de procesamiento de información que impacten los procesos críticos del negocio, para lo cual actualizará las guías de recuperación de los componentes de la plataforma tecnológica.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

El objetivo general de este plan es orientar a los administradores de TI y al personal del grupo PCN[1] de la CGN en la ejecución de procedimientos y actividades que permitan dar continuidad a la prestación de los servicios tecnológicos que soportan los procesos críticos de la entidad.

5.2. OBJETIVOS ESPECÍFICOS

1. Ejecutar tareas de recuperación de componentes tecnológicos teniendo en cuenta un marco de referencia que proporcione las características y condiciones ideales para el restablecimiento del servicio en cuestión.

2. Facilitar a los administradores de TI de la CGN la correcta y ordenada ejecución de las actividades previamente establecidas para la atención de incidentes con el ánimo de minimizar tiempos de respuesta y garantizar la eficacia y eficiencia de la solución.

3. Establecer una estructura organizada que incluya personal, actividades, tiempos y recursos, la cual permita optimizar la atención de una incidencia, esto es, desde la detección y reporte del problema hasta la solución definitiva.

4. Involucrar a los administradores de TI de la CGN en las labores previas, de respuesta y posteriores a un incidente; con el objetivo de detectar vulnerabilidades y desarrollar actividades preventivas, minimizar los tiempos de respuesta y garantizar el monitoreo de la solución.

6. ALCANCE

Este plan hace parte del plan de Continuidad del Negocio versión 5 – 2024 y su alcance se encuentra limitado a los escenarios de desastres identificados en él; también se enmarca en el proceso de gestión de tecnologías de información y en la infraestructura de TI de la CGN en sus componentes funcionales de hardware y software.

El enfoque de este documento se aplicará en 12 servicios de TI que el GIT de Apoyo Informático presta para soportar los procesos de negocio definidos en el PCN versión 5 en función de mantener la continuidad del negocio y en beneficio de los usuarios internos y externos de la Contaduría General de la Nación.

La elaboración, puesta en marcha y posible ejecución de las actividades de este plan dependen de los recursos disponibles. El factor humano, la disponibilidad de los servicios y la existencia en stock de piezas o partes contratadas con terceros, el presupuesto, entre otros, son aspectos determinantes para la correcta, oportuna y eficaz atención de un evento inesperado que pueda afectar la continuidad del negocio.

Este plan no incluye análisis, recursos, tiempos ni actividades para el restablecimiento de servicios o productos propios de otras dependencias que no hayan sido previamente incorporados en el PCN, más que las necesarias para brindar una plataforma tecnológica que permita desempeñar a cada funcionario de la CGN las labores propias de su cargo.

Teniendo en cuenta que el plan de contingencia hace parte del plan de continuidad del negocio y depende de las características propias de la entidad, se ha tenido en cuenta el documento *"buenas prácticas y recomendaciones para la gestión de la continuidad del negocio"* comprendido en la norma BS 25999-2[2] (ISO 22301:2012) con el fin de establecer patrones de análisis acordes con el objetivo de este plan.

7. ROLES Y RESPONSABILIDADES

El compromiso de la alta dirección, el o la coordinador (a) del GIT de Apoyo Informático y su equipo de trabajo, son de gran importancia, debido a que son los que tienen la responsabilidad de atender adecuadamente un incidente inesperado en la operación de la entidad, desde el instante en que se declare la interrupción hasta su restablecimiento al estado normal, reduciendo al máximo el impacto sobre la prestación de los servicios tecnológicos.

La Contaduría define tres niveles de gestión: estratégico, táctico y operativo con sus responsabilidades en el momento de suceder un incidente que genere la activación del plan de contingencia tecnológica. En cada nivel se deberá establecer un sucesor para tomar decisiones en caso de no estar presente el encargado principal.

Nivel Estratégico: Nivel que define el objetivo del plan de contingencia tecnológica, toma decisiones sobre las políticas, directrices y recursos para lograr la efectividad en caso de presentarse una interrupción del servicio tecnológico de la CGN.

Nivel Táctico: Coordina las actividades del plan de contingencia tecnológico, controla y realiza seguimiento de la situación de interrupción con las respectivas directrices para su

[2] ***BS 25999*** *– (British Standard en inglés) primera norma británica para la gestión de continuidad de negocio. Desarrollada por un amplio grupo de expertos representativos de sectores de la industria y la administración. Proporciona la base para comprender, desarrollar e implantar la continuidad de negocio en una organización.*

operación, así como escalar al nivel estratégico las necesidades de operación y del estado de su aplicación.

Nivel Operativo: Realiza la asignación de las tareas específicas en el momento de presentarse el incidente o evento inesperado que activa el plan de contingencia tecnológico, por instrucción de los niveles estratégico y táctico.

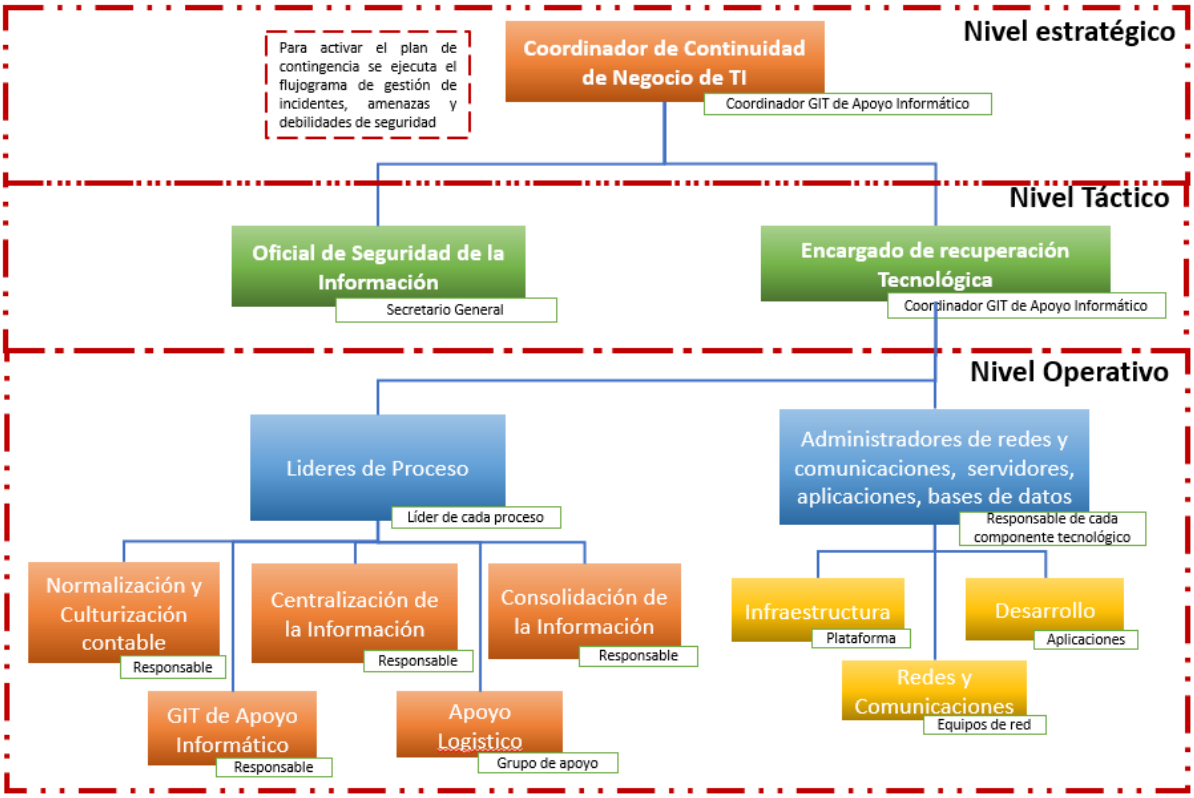

Ilustración 1 Niveles de Gestión del plan de contingencia de Tecnología de la Contaduría
Fuente: Elaborado en la CGN

En la siguiente tabla se detallan las responsabilidades de cada uno de los roles de acuerdo con el nivel de gestión de este plan de contingencia tecnológica:

Roles	Antes de interrupción	Durante la interrupción	Despues de la interrupción
Coordinador de continuidad o quien haga sus veces	Aprueba el plan de contingencia tecnológica	Esta atento al desarrollo del plan de contingencia tecnológica	Realiza analisis de la interrupción y toma decisiones de acuerdo a la criticidad
Coordinador de Informática	Lidera la elaboración y actualización del plan de contingencia tecnológica y el manejo de las situaciones críticas. Asegurar que las guías que se definan para el manejo de las situaciones de contingencia estén enmarcadas en la normatividad interna de la CGN. Socializar y promover el compromiso del área en la elaboración del plan, así como durante la ocurrencia de una contingencia. Tomar decisiones con base en los resultados de las pruebas o incidentes reales para optimizar tiempos, costos y recursos.	Monitorea y asegura el cumplimiento del plan de contingencia tecnológica	Informa de los resultados de ejecución del plan a la Alta Dirección o quien haga sus veces Actualiza el plan de congencia tecnologica Cita a reuniones de revisión del plan de contingencia tecnológica
Oficial de seguridad de la información o encargado	Analiza los incidentes o eventos de seguridad registrados según el flujograma "Gestión de incidentes, amenazas y debilidades de seguridad" del procedimiento GTI-PRC10 - Seguridad de la Información y participa con los demás miembros del nivel táctico, en la toma de decisión de activar o no el Plan de Contingencias tecnologica Identificar los riesgos de interrupción de los servicios tecnológicos y emite concepto para la toma de	Permanece en comunicación activa con el grupo de gestión del plan de contingencia tecnologica Participa activamente en la ejecución del plan.	Analizar las causas de la interrupción y los resultados de la ejecución del plan e informar el análisis realizado a los niveles estratégico y táctico.
Encargado de recuperación tecnológica	•Apoyar al nivel táctico y estratégico en la toma de decisiones de la activación del plan de contingencia tecnológica •Elaborar y actualizar periódicamente las guías de respuesta ante incidencias o eventos que pongan en riesgo la prestación de los servicios que le competan, asegurando la eficacia y eficiencia de las soluciones consignadas. •Realizar según las prioridades del análisis de riesgos e impacto correspondiente a la plataforma, equipos o servicios que administre. •Programar, coordinar y evaluar las pruebas del plan de contingencia analizando posibles acciones preventivas, de mejoramiento o complementarias las cuales optimicen la calidad de la solución. •Proponer acciones preventivas que reduzcan la probabilidad de ocurrencia de un riesgo o minimicen el impacto sobre el elemento en cuestión, en caso de materializarse. •Asegurar que la información y medios relacionados con la recuperación sean correctamente identificados y accesibles. •Identificar y gestionar los recursos requeridos para la operación del plan de contingencia tecnológica	•Gestionar las actividades del plan de contingencia tecnológica, asignando los funcionarios responsables de cada componente TI •Mantener comunicación constante con los integrantes de los niveles estratégico y táctico sobre las actividades realizadas durante la interrupción. •Realizar seguimiento a la situación durante la activación del Plan de contingencia tecnológica •Proveer soporte a los líderes y equipos de recuperación. •Planificar y gestionar el retorno a la normalidad.	•Asegurar que se documentan las lecciones aprendidas, después del retorno a la normalidad. •Programar y coordinar las pruebas del retorno a la normalidad luego que ha terminado la contingencia tecnológica. •Informar al Coordinador de informática sobre las actividades realizadas durante y después de la interrupción y los resultados obtenidos.
Lider de proceso	El lider de proceso afectado apoyara todos los niveles funcionalmente en la toma de decisiones de la activación del plan de contingencia tecnológica	Participa en la ejecución funcional del plan de contingencia tecnológica	Apoya funcionalmente el retorno a la normalidad después de terminada la contingencia tecnológica

Roles	Antes de interrupción	Durante la interrupción	Despues de la interrupción
Responsables de atención de contingencia Administradores de Infraestructura, desarrollo (aplicaciones), redes y comunicaciones, copias de respaldo	•Identificar y conocer el plan de contingencia tecnológica, así como participar, cuando haya lugar, en las actividades establecidas en el mismo o en las relacionadas con su elaboración y prueba. •Realizar de forma periódica las actividades de instalación y arranque de la infraestructura de TI y la infraestructura de recuperación. •Aplicar los procedimientos del proceso de Gestión TICs •Mantener iguales las configuraciones de los equipos de producción y de respaldo, así como de los sistemas de información y bases de datos de producción y de respaldo. •Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos. •Ejecutar las pruebas del Plan de Contingencia tecnológica •Identificar riesgos de interrupción de los servicios de TI y emitir concepto para toma de decisiones. •Participar en las actividades de continuidad (Capacitaciones, divulgación, pruebas y ejecución).	•Ejecutar las actividades registradas en el Plan de Contingencias tecnológica y las que considere necesarias para la recuperación de la infraestructura, servicio y/o aplicación afectado. •Proveer soporte técnico según requerimientos del incidente. •Ejecutar las actividades registradas en el Plan de contingencia tecnológica y las que considere necesarias para la recuperación de la plataforma o del activo de información afectado. •Asegurar la prestación del servicio en el menor tiempo posible, luego de la activación del Plan de contingencia tecnológica.	•Restaurar a la normalidad la infraestructura, servicio y/o aplicación afectado para su puesta en producción nuevamente. •Documentar las lecciones aprendidas del evento de interrupción. •Restaurar a la normalidad la plataforma o el activo de información afectado para usarlo nuevamente. •Tomar medidas correctivas frente a lo ocurrido en la activación del Plan de contingencia tecnológica para la recuperación de las actividades durante el incidente o evento. •Revisar los informes de incidencias, consecuencias y causas y elaborar el plan de remediación de acuerdo con el procedimiento GTI02-FOR04 Administración de cambios a TI. •Reportar los inconvenientes y oportunidades de mejora del del Plan de Contingencia tecnológica.
Apoyo Logistico Profesionales de las diferentes áreas que se requieran para la ejecución del plan de contingencia tecnológica	Conocer el Plan de Contingencia tecnológica	•Ejecutar actividades de logística para el desarrollo de las actividades de recuperación tales como traslados de los líderes y equipos de recuperación. •Realizar actividades relacionadas con compras necesarias de recursos durante la recuperación	Reportar los inconvenientes y oportunidades de mejora del del Plan de Contingencia tecnológica.

Tabla 1 Roles y Responsabilidades del plan de contingencia tecnológica
Fuente: Elaborado en la CGN

8. ESTRATEGIA

El GIT de Apoyo Informático conoce la importancia de contar con un plan de contingencia tecnológica completo, actualizado, revisado, probado y divulgado; en este sentido, establece el trabajo en pares para cada servicio y elemento que compone la plataforma de TI de la Contaduría General de la Nación.

Existirá un principal y un suplente, incluidos los terceros proveedores, sobre la administración y soporte de cada servicio, de esta manera, ante la ausencia del administrador principal existirá otra persona que estará en capacidades de ejecutar las tareas del servicio o dispositivo en cuestión de tal manera que se garantice la disponibilidad de este.

El plan de contingencia se encuentra disponible en el drive del correo seguridadinformática@contaduría.gov.co por lo tanto se podrá acceder externamente a este y a las guías.

9. ESCENARIOS

De acuerdo con lo establecido en el PCN versión 5 se identifican las siguientes causas de interrupción del servicio y posibles escenarios de ocurrencia.

Escenario		Causa de Interrupción	Descripción
DESASTRES NATURALES			
22	Terremoto, Incendio, Colapso edificio	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	Terremoto	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	Terremoto, Incendio, Colapso edificio, Presencia de gases tóxicos o inflamables	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	Terremoto, Incendio, Colapso edificio	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	Incendio	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	Terremoto, Incendio, Inundación	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	Terremoto, Incendio, Colapso edificio	Riesgos telecomunicaciones	Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.
4	Terremoto, Incendio, Colapso edificio, inundación	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 2 Escenarios y causa de interrupción tecnológicos
Fuente: Tomada de Plan de Continuidad del Negocio, versión 3.1

De igual manera se han establecido los tiempos de respuesta de los servicios tecnológicos que afectan a los procesos de negocio más relevantes de la entidad, como se muestra en la siguiente tabla:

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 3 Tiempos de respuesta servicios tecnológicos en el alcance del PCN

Fuente: Tomada de Plan de Continuidad del Negocio, versión 5

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

Así como se estableció la prioridad para la recuperación de los servicios en el siguiente orden:

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 4 secuencia de recuperación de los servicios del alcance del PCN
Fuente: Tomada de Plan de Continuidad del Negocio, versión 5

10. PLAN DE ACCIÓN

En consecuencia, con lo descrito en el numeral 9, las acciones del plan de contingencia se enmarcan en la gestión de los escenarios y la ocurrencia de las situaciones que puedan interrumpir los servicios por tiempo prolongado, para lo cual la Contaduría General de la Nación cuenta con una infraestructura tecnológica que soporta la permanente ejecución de los procesos misional y de apoyo; en razón a que el foco del plan de acción son los procesos misionales, se entiende por ***plataforma misional****: todos los componentes informáticos de hardware, software y procedimientos relacionados directamente con actividades de los procesos de normalización y culturalización contable, la centralización y la consolidación de la información; en otras palabras, son los componentes tecnológicos que ayudan a la Contaduría a realizar su misión*.

Para la ejecución de las actividades de este plan de acción se debe tener en cuenta la estructura establecida en el archivo maestro contingencia con el fin de ubicar las guías, manuales, diagramas y material relacionado.

Los servicios deben ser recuperados de acuerdo con la prioridad establecida en la tabla 4. La actividad de recuperación de un servicio no debe exceder los tiempos establecidos en la tabla 3.

En razón a que la ejecución de la acción de recuperación de un servicio depende del escenario y del servicio impactado; para la ubicación y ejecución de la respectiva guía orientarse con la siguiente tabla No 5:

Recuperación de servicios tecnológicos				
Secuencia	Servicio			
	Hardware	Software	Ejecutar guía	Ubicación
1	Red		GUÍA DE IMPLEMENTACIÓN CONTINGENCIA RED DE DATOS	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Red/TIC-SEG-PCO-GUIA-IMPLEMENTACION-ReddeDatos.docx
2	Internet		GUÍA DE IMPLEMENTACIÓN CONTINGENCIA PLATAFORMA LINUX - LIFERAY PORTAL PRODUCCIÓN	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Internet-Portal/TIC-SEG-PCO-GUIA-PCH-PORTAL-RT.docx
3		Correo Electrónico	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA CORREO ELECTRÓNICO – EMAIL	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Correo/SEG-PCO-GUI-COR-GuiaContingenciaCorreoElectr%C3%B3nico_2022.docx
4	Servidores de misión			
5	Medios magnéticos			
6		CHIP	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA PLATAFORMA AIX – CHIP | CHIP PRODUCCIÓN	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Chip/TIC-SEG-PCO-GUIA-PCH-CHIP-RT.docx
7		Pagina Web	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA PLATAFORMA LINUX - LIFERAY PORTAL PRODUCCIÓN	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Internet-Portal/TIC-SEG-PCO-GUIA-PCH-PORTAL-RT.docx
8		Intranet		
10		Telefonía	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA PLATAFORMA TELEFONÍA IP	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Telefon%C3%ADa/TIC-SEG-PCO-GUIA-REX-PlataformaTelefonia.docx
11		PathFinder	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA PATHFINDER	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG (Seguridad)/SGS (Sistema Gestion Seguridad)/PCO (Plan Contingencia)/PCO (Plan Contingencia 2024)/PRU (Pruebas)/Pathfinder
12		Siscon	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA GESTION DOCUMENTAL SISCON	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG (Seguridad)/SGS (Sistema Gestion Seguridad)/PCO (Plan Contingencia)/PCO (Plan Contingencia 2024)/PRU (Pruebas)/SISCON
13		Aula Virtual	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA AULA VIRTUAL	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG (Seguridad)/SGS (Sistema Gestion Seguridad)/PCO (Plan Contingencia)/PCO (Plan Contingencia 2024)/PRU (Pruebas)/Aula Virtual
14		GLPI	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA MESA DE SERVICIOS GLPI	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG (Seguridad)/SGS (Sistema Gestion Seguridad)/PCO (Plan Contingencia)/PCO (Plan Contingencia 2024)/PRU (Pruebas)/GLPI
15		Orfeo	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA GESTIÓN DOCUMENTAL | ORFEO 5.5	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Orfeo/TIC-SEG-PCO-GUIA-PCH-ORFEO-%20Guia%20Contingencia%20Orfeo%205.5.doc
16		SIGI		
17		Repositorios	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA GESTIÓN DOCUMENTAL PATHFINDER	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Pathfinder/TIC-SEG-PCO-GUIA-Servidor-Archivos-Pathfinder.docx
18				http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Pathfinder/TIC-SEG-PCO-GUIA-Servidor-Archivos-Pathfinder.docx
19	PCs			
20		Ofimática	GUÍA DE IMPLEMENTACIÓN CONTINGENCIA OFIMÁTICA	http://galatea.contaduria.gov.co/svn/TIC_Gestion_TICs/trunk/SEG%20(Seguridad)/PCO%20(Plan%20Contingencia)/PCO%20(Plan%20Contingencia%202022)/PRU%20(Pruebas)/Ofim%C3%A1tica/TIC-SEG-PCO-GUIA-PVR-Ofimatica.docx

Tabla 5 Recuperación de los servicios tecnológicos
Fuente: Elaborado en la CGN

Para la recuperación de algún otro servicio que no se encuentre en el alcance del presente plan de contingencia, la situación deberá ser gestionada como un incidente y la guía de contingencia debe ser consultada en el archivo “Maestro Contingencias.xls”, el instructivo de manejo puede ser consultado en el archivo Leame.docx

11. INFRAESTRUCTURA DE TI

Los servicios tecnológicos que soportan los procesos de la Contaduría General de la Nación están soportados en una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos instalados en un centro de datos propio ubicado en las instalaciones de la Contaduría.

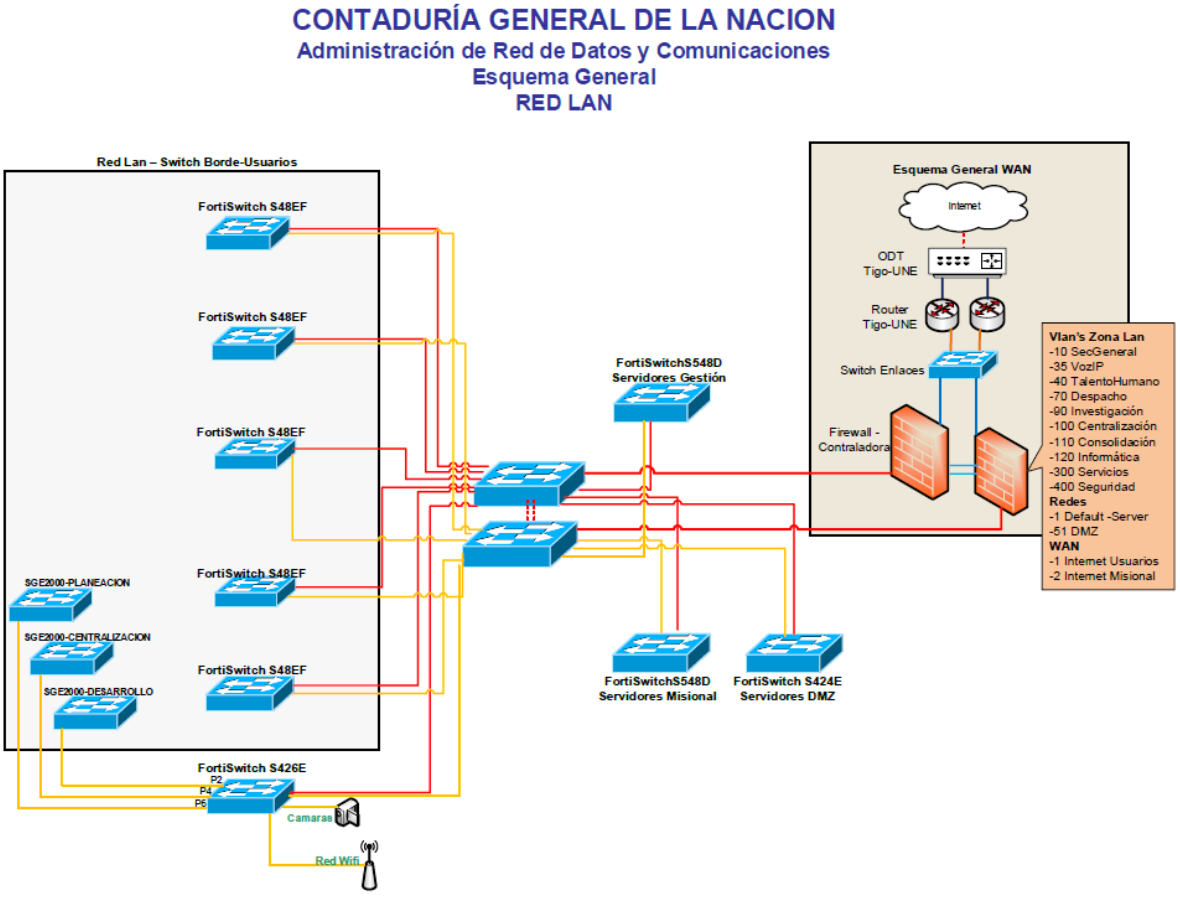

Ilustración 2 Topología de la red de datos
Fuente: Elaborado en la CGN

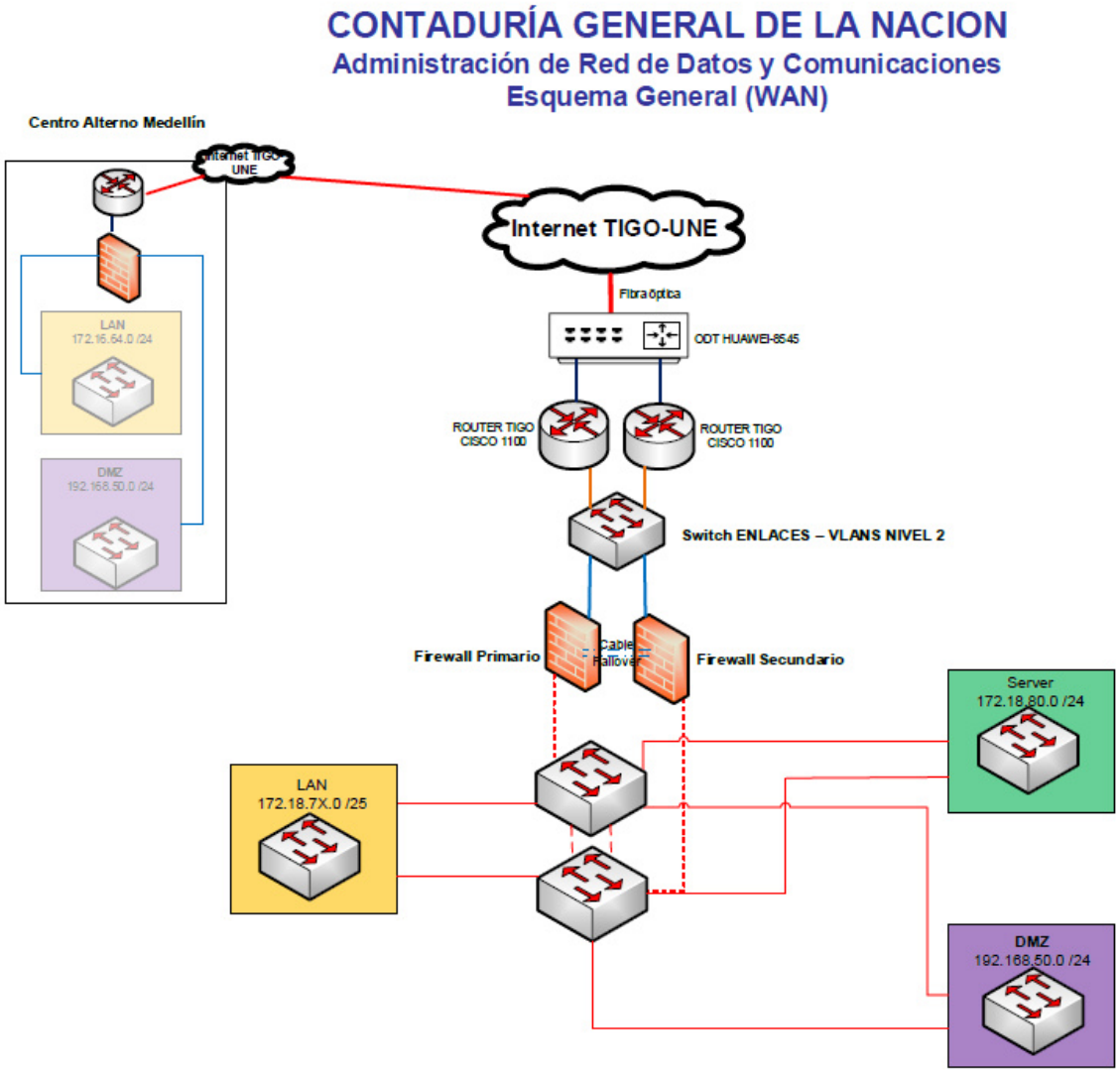

Ilustración 3 Topología de la red de comunicaciones
Fuente: Elaborado en la CGN

Infraestructura del data center de la Contaduría

Infraestructura del data center de la Contaduría	
CANTIDAD	**DESCRIPCIÓN**
2	Firewall Fortigate
1	Fortianalyzer
1	Sistema de detección y extinción de incendios
3	UPS

2	Aire Acondicionado
7	Switch de borde
3	Server HP
2	Switch de CORE
3	Switch BROCADE 300
1	Server DELL POWER EDGE FX2S (Chasis enclouser Dell FX2)
1	SAN HITACHI VSP G200
8	Access Point
3	SERVER DELL
7	Server IBM
2	HMC
1	Librería Cintas
1	NAS
43	Máquinas virtuales Vcenter
2	Máquinas Virtuales (Setebos)

Tabla 6 Infraestructura del data center de la Contaduría
Fuente: Elaborado en la CGN

12. ACUERDOS DE NIVELES DE SERVICIO DE TECNOLOGÍA

El GIT de Apoyo Informático ha establecido los Acuerdos de Niveles de Servicio (ANS), para la prestación de los servicios definidos de acuerdo con el nivel de complejidad y afectación que cause sobre la infraestructura tecnológica, incluyendo los tiempos de recuperación que deben ser tenidos en cuenta en caso de contingencia.

			HORARIOS				
No	SERVICIO	CANALES DE ACCESO	DISPONIBILIDAD	TIEMPO DE RECUPERACION	SOPORTE	USO	REQUISITOS PARA ACCEDER AL SERVICIO
1	Correo Electrónico	Los usuarios acceden al servicio por medio de la página de la Contaduría o ingresando a gmail en el explorador	7 días 24 horas los 365 días del año	Por contrato se establece tiempo de solución de incidentes reportados <= 3 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	7 días 24 horas los 365 días del año.	Tener acceso a Internet
2	PathFinder	Los usuarios acceden al servicio localmente o por medio de la VPN	5 x 8 los días hábiles del año	Alistamiento de equipo, restauración de backup y puesta en fucionamiento - Disponibilidad en 24 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener usuario valido para poder acceder a los repositorios y servidores de archivos de la CGN
3	Siscon	Los usuarios acceden al servicio localmente o por medio de la VPN	7 x 8 los días hábiles del año	Alistamiento de equipo, restauración de backup y puesta en fucionamiento - Disponibilidad en 1 hora	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener vínculo laboral (planta o Contratista) con la Contaduría Tener usuario registrado en la intranet
4	Aula Virtual	Los usuarios acceden al servicio por pagina WEB, localmente o por medio de la VPN	8 x 8 los días hábiles del año	Alistamiento de equipo, restauración de backup y puesta en fucionamiento - Disponibilidad en 2 hora	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener acceso a la aplicación y usuario registrado
5	GLPI	Los usuarios acceden al servicio por la Intranet, localmente o por medio de la VPN	9 x 8 los días hábiles del año	Alistamiento de equipo, restauración de backup y puesta en fucionamiento - Disponibilidad en 1 hora	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener vínculo laboral (planta o Contratista) con la Contaduría Tener usuario registrado en la intranet
6	Ofimática	Los usuarios acceden al servicio localmente o por medio de la VPN	5 x 8 los días hábiles del año	Alistamiento de equipo, instalación de sistema operativo y herramientas de ofimatica Disponibilidad desde el instante que se cuente con un equipo en 5 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener usuario valido para poder acceder a las herramientas y demás aplicaciones instaladas en los equipos con placa de Contaduría
7	Orfeo	Los usuarios acceden al aplicativo por medio de la Intranet de la Contaduría o en la pagina web de la CGN\servicio al ciudadano\PQRSD el formulario es enviado al aplicativo Orfeo	7 días a la semana 24 horas al día	Alistamiento de equipo, restauración de backup y puesta en fucionamiento - Disponibilidad en 24 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	Tener vínculo laboral (planta o Contratista) con la Contaduría Tener usuario registrado en el aplicativo ORFEO
8	Telefonía	Los usuarios acceden al servicio por medio de teléfono 4926400 Ext 234 o 236	5 x 8 los días hábiles del año	Disponibilidad de acuerdo a reporte de fallo	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año	Tener acceso a los telefonos
9	CHIP	Los usuarios externos (reportantes) acceden los servicios del sistema a través de la página web de la CGN\productos\Chip Los canales de atención a solicitudes se realizan por canal telefónico 4926400 ext. 234 o 236 a mesa de servicio.	7 días 24 horas los 365 días del año	Restauración de backup en caso que se requiera y puesta en funcionamiento centro alterno de Medellín-Disponibilidad en 24 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	Días hábiles de 7:30 a.m. a 4:30 p.m.	Navegador Mozilla Firefox o Google Chrome Acceso a internet Guía de Instalación y Operación del CHIP
10	Página Web	Realizar la solicitud por la Mesa de Servicios.	7 días 24 horas los 365 días del año.	Alistamiento de servidor, restauración de backup y puesta en fucionamiento Disponibilidad desde el instante que se cuente con el servidor de 72 horas	7 días 24 horas los 365 días del año.	7 días 24 horas los 365 días del año.	Realizar la solicitud por la Mesa de Servicios
11	Intranet	Los usuarios acceden al servicio únicamente por medio de la Intranet de la Contaduría	7 días 24 horas los 365 días del año.		Lunes a viernes de 7:30 a.m. a 4:30 p.m.	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	Tener vínculo laboral (planta o Contratista) con la Contaduría Tener usuario registrado en la intranet
12	Computadores Personales de escritorio y portátiles	Los usuarios acceden al servicio por medio de teléfono 4926400 - Ext. 234 o 236 realizando la solicitud	5 x 8 los días hábiles del año	Alistamiento de equipo, instalación de sistema operativo y herramientas de ofimatica y restauración de información. Disponibilidad desde el instante que se cuente con un equipo en 5 horas por equipo	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	5 x 8 los días hábiles del año.	Tener Usuario valido para poder acceder a los Equipos de Cómputo con Placa de la Contaduría
13	Servidores de misión	Estar autorizado y tener acceso al Data center	7 días 24 horas los 365 días del año.	Alistamiento de servidores, restauración de backup y puesta en fucionamiento Disponibilidad desde el instante que se cuente con los servidores de 72 horas	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	7 días 24 horas los 365 días del año.	Tener Aplicaciones Misionales en los Servidores que están en el Data center del piso 15 de la Contaduría
14	Internet	Realizar la solicitud por la Mesa de Servicios.	7 días 24 horas los 365 días del año.	Por contrato se establece una disponibilidad del 99,7%	Lunes a viernes de 7:30 a.m. a 4:30 p.m.	7 días 24 horas los 365 días del año.	Realizar la solicitud por la Mesa de Servicios.
15	Red	Realizar la solicitud por la Mesa de Servicios.	7 días 24 horas los 365 días del año	Alistamiento de equipos de red, restauración de configuraciones y puesta en fucionamiento Disponibilidad desde el instante que se cuente con los equipos de 72 horas	7 días 24 horas los 365 días del año	7 días 24 horas los 365 días del año.	Solicitar el Servicios para hacer la habilitación respectiva del dispositivo a conectar

Tabla 7 Acuerdos de nivel de servicio de la Contaduría
Fuente: Elaborado en la CGN

13. IDENTIFICACION DE RIESGOS

En este Plan de Contingencia Tecnológica de la Contaduría General de la Nación, se tienen en cuenta los riesgos tecnológicos identificados en el proceso de Gestión TICs en el mapa de riesgos institucional.

	Escenario	Riesgo	Amenaza en matriz de riesgos seguridad	Descripción riesgo	Afectación									
					Procesos / Procedimientos									Servicio Tecnológico
					Normalización y Culturización Contable (5)	Centralización de la Información (14)			Consolidación de la Información (8)		Gestión TICs (10)			
					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	
3	Indisponibilidad de componentes de infraestructura tecnologica	Pérdida de Confidencialidad	22	Pérdida de la confidencialidad ocasionada por acceso no autorizado a sistemas y servicios, o abuso de derechos de acceso a sistemas y servicios provocado por algún funcionario / contratista. - Riesgos de navegación de usuarios con privilegios avanzados	x	x	x	x	x	x	x	x	x	ORFEO, SIGI, CHIP, Página Web, correo electronico,Telefonia, Pc, Servidores, Internet, repositorio, GLPI, SISCON, Aula Virtual
		Pérdida de Integridad	10	Ataques informáticos internos/externos a la infraestructura tecnológica	x	x	x		x	x	x	x	x	Página web, Servisores de gestión, servidores misionales,PCs, Intranet, ofimática, SIGI, CHIP,Telefonia, Orfeo, Repositorios, correo electrónico, GLPI,
4	No contar con los Proveedores Externos Claves	Pérdida de Disponibilidad	3	Contratos de soporte no vigentes	x	x	x	x	x	x	x	x	x	Internet, servidores
5	Acceso a la edificación	Pérdida de Disponibilidad	9	Desastres naturales, problemas de órden público	x	x	x	x	x	x	x	x	x	Página web, Servidores de gestión, servidores misionales,PCs, Intranet, ofimática, SIGI, CHIP,Telefonia, Orfeo, Repositorios, correo electrónico,Internet, GLPI, SISCON, Aula Virtual
6	Administración y entorno tecnológico	Perdida de Integridad	5	Instalación y uso de software con vulnerabilidades conocidas en los sistemas operativos de los equipos de cómputo y servidores	x	x	x	x	x	x	x	x	x	Pc, Internet, Servidores, red, Repositorios, Bases de datos, página web, SIGI, Orfeo, correo electrónico, GLPI, SISCON, Aula Virtual
		Pérdida de Disponibilidad	23	Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad gestionada inadecuadamente	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, medios mgnéticos
		Pérdida de Disponibilidad	21	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	x	x	x	x	x	x	x	x	x	Página web, Servidores de gestión, servidores misionales,PCs, Intranet, ofimática, SIGI, CHIP,Telefonia, Orfeo, Repositorios, correo electrónico,Internet, GLPI, SISCON, Aula Virtual
		Pérdida de Disponibilidad	8	Pérdida de la información generada por las actividades propias de la gestión del proceso	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, Medios magnéticos, correo electrónico, GLPI, SISCON, Aula Virtual
7	Protección anti-incendios	Pérdida de Disponibilidad	18	Indisponiobilidad de los equipos de protección contra incendios en caso de emergencia	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, medios magnéticos, correo electrónico
9	Riesgos potencia eléctrica	Pérdida de Disponibilidad	11	Indisponibilidad del fluido eléctrico continuo en el centro de datos y estaciones de trabajo relevantes en los procesos del alcance del PCN	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, medios magnéticos, correo electrónico, GLPI, SISCON, Aula Virtual
10	Riesgos telecomunicaciones	Pérdida de Disponibilidad	18	Indisponibilidad del canal de comunicación	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, CHIP,Telefonia, Repositorios, Internet, correo electrónico, GLPI, SISCON, Aula Virtual
11	Centro de datos	Pérdida de Integridad	4	Daño de información o en las instalaciones de procesamiento de datos (Datacenter)	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, Correo electrónico, GLPI, SISCON, Aula Virtual
		Pérdida de Integridad	18	Daño en equipos informáticos	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, GLPI, SISCON, Aula Virtual
		Pérdida de Disponibilidad	22	Pérdida de la disponibilidad de las instalaciones de procesamiento de información	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, medios magnéticos, correo electrónico, GLPI, SISCON, Aula Virtual
9	Caídas totales o parciales de los servicios	Pérdida de Disponibilidad	21	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	x	x	x	x	x	x	x	x	x	Servidores de gestión, servidores misionales,PCs, SIGI, CHIP,Telefonia, Orfeo, Repositorios, Internet, medios magnéticos, correo electrónico, GLPI, SISCON, Aula Virtual

Tabla 8 Riesgos del proceso Gestión TICs
Fuente: Elaborado en la CGN

14. INTERRUPCIONES Y NIVEL DE AFECTACIÓN A SERVICIOS DE TI

La activación del plan de contingencias de TI de la Contaduría depende del resultado del procedimiento GTI-PRC010 Seguridad de la información, flujograma **gestión de incidentes**, amenazas y debilidades de seguridad y de las decisiones tomadas de acuerdo con este plan de contingencia tecnológica y el tipo de interrupción en los servicios tecnológicos.

Los incidentes que aplican a la activación de actividades de contingencia se evalúan de acuerdo con el impacto que generan en la prestación de servicios tecnológicos de la Contaduría y su nivel de materialización del riesgo, acorde a la siguiente tabla:

Tipo de interrupción	Descripción	Escenarios	Respuesta
TOTAL	Evento que afecta el funcionamiento total del centro de datos para prestar los servicios y no se puede ingresar a las instalaciones	Terremoto, incendio, colapso del edificio, falla eléctrica continua	Ejecución de guías en eL centro de datos alterno de acuerdo a La guía **Nota:** El centro alterno solamente aplica al sistema CHIP producción
PARCIAL	Evento que afecta mas de un componente tecnológico critico de manera importante, provocando la suspensión parcial del funcionamiento de servicios críticos	Caídas totales o parciales de los servicios	Activar procesos de contingencia de acuerdo al componente afectado
ESPECIFICA	Evento que afecta algún componente tecnológico especifico, afectando la prestación de servicios tecnológicos	Caídas totales o parciales de los servicios	Activar procesos de contingencia de acuerdo al componente afectado

Tabla 9 Interrupciones de servicios TICs
Fuente: Elaborado en la CGN

Se tendrán en cuenta para el restablecimiento y aplicación de la contingencia, los tiempos de respuesta de servicios tecnológicos dados en la tabla 3 de este plan.

15. LOGISTICA DE CONTINGENCIA

Cuando suceda un evento o incidente que provoque la materialización de un riesgo identificado en este Plan, el funcionario o funcionarios afectados deberán realizar el respectivo reporte de inmediato a través de la mesa de servicios a la ext. 234 o 236 o al

correo electrónico mesadeservicio@contaduria.gov.co Una vez reportada la contingencia se activará por parte del Coordinador del GIT de Apoyo Informático el respectivo procedimiento para el manejo de la interrupción.

De manera periódica y preventiva se debe:

- Verificar el directorio telefónico de contacto de los funcionarios responsables y mantenerlo actualizado.
- Verificar los procedimientos de copia y restauración de seguridad de la información.
- Realizar jornadas de capacitación sobre el plan, a funcionarios de las diferentes áreas sobre las actividades a seguir en el proceso de contingencia.
- 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.

16. PRUEBAS Y ACTUALIZACION

El plan de contingencia 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, al activar una contingencia.
- 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 1. 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.

16.1 TIPOS Y FRECUENCIA DE PRUEBAS

En cubrimiento y alcance los tipos de pruebas pueden ser:

- **Prueba general o particular**: Son pruebas donde se activa el centro de datos alterno y tiene una periodicidad de al menos un año, puede ser parcial de algún componente, por secciones o total. Se prueba el desempeño de la plataforma de contingencia y su funcionamiento. Consiste en realizar simulacros en horarios hábiles y no hábiles, en diferentes casos:
    - Prueba de continuidad de energía eléctrica con UPS en caso de corte del servicio de energía y verificación de subida de UPS
    - Prueba del canal de respaldo de internet Vs la caída del canal principal
    - Prueba de equipos de respaldo y sistemas de información
    - Recuperación de la información de las copias de respaldo de acuerdo con procedimiento de restauración

17. BIBLIOGRAFÍA

Plan de Continuidad del Negocio CGN – 2022, Contaduría General de la Nación, 2022, GIT de Apoyo Informático.

Plan de Continuidad del Negocio CGN – 2024, Contaduría General de la Nación, 2024, GIT de Apoyo Informático.

Plan de Contingencia CGN – 2014, Contaduría General de la Nación, 2014, GIT de Apoyo Informático.

Plan de Contingencia CGN – 2024, Contaduría General de la Nación, 2024, GIT de Apoyo Informático.

NTC-ISO/IEC 27001:2013, Norma Técnica Colombiana NTC-ISO/IEC 27001. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

ISO 22301:2012, 2013, Sistemas de Gestión y Continuidad del Negocio. Requisitos.

NTC 5722:2012, 2013, Norma Técnica Colombiana NTC 5722 Continuidad de Negocio. Sistemas de Gestión de Continuidad de Negocio. Requisitos

GTC-ISO/IEC 27031:2016, Guía Técnica Colombiana GTCISO/IEC 27031, Directrices para la preparación de la tecnología de Información y las comunicaciones para la continuidad del negocio.
NTC-ISO/IEC 27005:2020, Norma Técnica Colombiana NTC-ISO/IEC 27001. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.

BS 25999, Norma británica para la gestión de continuidad de negocio, Proporciona la base para comprender, desarrollar e implantar la continuidad de negocio en una organización.

18. ANEXOS

Anexo 1. FORMATO DE PRUEBAS DEL PLAN DE CONTINGENCIA TECNOLÓGICA

CONTADURÍA GENERAL DE LA NACIÓN	**FORMATO DE PRUEBAS DEL PLAN DE CONTINGENCIA TECNOLÓGICA**

En este formato se documenta la realización de la prueba a las medidas de contingencia establecidas en el proceso Gestión TICs, de manera que se asegure su pertinencia para responder ante posibles incidentes y a pérdidas que estos generan en la operación, de manera que se revisen el (los) plan(es) de continuidad del negocio para garantizar su actualización y eficacia.

OBJETIVO DE PRUEBA: *<Describir la finalidad de la prueba a realizar>*		
RECURSO POR PROBAR: *<Nombre del sistema de información, aplicativo y/o infraestructura tecnológica y/o servicio de TI que se va a probar de acuerdo con lo descrito en "servicios e infraestructura de TI" del Plan de Contingencia tecnológica>*		
PARTICIPANTES		
NOMBRE	**CARGO**	**DEPENDENCIA/GIT**

DESARROLLO

I. ESCENARIO DE LA PRUEBA:

FECHA	DURACION	LIDER DE PRUEBA	DESCRIPCION
<formato dd/mm/aaaa de la fecha de ejecución de la prueba >	*<Tiempo estimado de la duración de la prueba>*	*<responsable de la ejecución de la prueba>*	*<Descripción resumida de la prueba a realizar>*

Alcance: *<Describir el alcance del plan de pruebas, identificando el lugar de la prueba, los recursos, servicio, aplicativos y/o servicios que serán sometidos a pruebas y los tipos de prueba que se realizarán>*

Escenario de Interrupción: <*Incluir el escenario de interrupción que se simulará en la prueba>*

REQUISITOS PARA LA PRUEBA

- **Recurso Humano:** *<Especificar el recurso humano necesario para la ejecución del plan de pruebas de acuerdo con los roles y responsabilidades, así como los proveedores involucrados>*
- **Requerimientos Hardware***: <Especificar los requerimientos de hardware (sistema operativo, memoria, servidor de aplicaciones, red, etc.) para la ejecución del plan de pruebas>*
- **Requerimientos Software:** *<Especificar los requerimientos de software y copias de respaldo para la ejecución del plan de pruebas>*
- **Requerimientos de Logística:** *<Especificar los requerimientos logísticos que se requieran (ejemplo: transporte, autorizaciones, entre otros) para la ejecución del plan de pruebas>*

II. DESCRIPCIÓN:

1. **Descripción del incidente:** *<Incidente>*

2. **Descripción del riesgo:** *<Riesgo>*

3. **Causas del Incidente:** *<Descripción de posibilidad de causas>*

III. PLAN DE PRUEBAS:

<diligenciar uno por cada tipo de prueba>

Tipo de prueba:	*<Especificar el tipo de prueba a realizar de acuerdo con lo especificado en numeral de Tipo y frecuencia de pruebas del plan de contingencia tecnológica>*
Líder de prueba:	*<Nombre de la persona líder de la prueba>*
Secuencia:	*<Secuencia de pasos con su descripción y condiciones que debe seguir el equipo de pruebas para la ejecución o nombre de la guía que se debe seguir>*
Precondiciones:	*<Condiciones que se deben cumplir antes de iniciar la prueba>*
Criterios de éxito:	*<Criterios para considerar que la ejecución de la prueba generó resultados satisfactorios>*
Resultado esperado:	*<Resultado que se espera obtener con la ejecución de la prueba, se debe establecer antes de ejecutar la prueba>*

Resultado obtenido:	*<Resultado obtenido después de ejecutar la prueba. En caso de que el resultado obtenido sea diferente al resultado esperado se deben describir dichas diferencias y las posibles causas que las generaron>*
Fecha de ejecución:	*<Fecha en la cual se ejecuta la prueba – formato dd/mm/aaaa>*
Anexos:	*<Relación de los anexos que complementan la ejecución de la prueba>*
Observaciones:	*<Observaciones adicionales de la prueba>*

APROBACION DE LA SOLICITUD DE PRUEBA

SOLICITADA POR
Cargo:
Cargo:
Nombre:
Firma:
GIT:
Fecha:

APROBADA POR
Nombre:
Firma:
GIT:
Fecha:

REPORTE DE RESULTADOS DE LA PRUEBA

REALIZADA POR
Cargo:
Nombre:
Firma:
GIT:
Fecha:

ACEPTADA POR
Cargo:
Nombre:
Firma:
GIT:
Fecha:

IV. EJECUCIÓN y RETORNO: Paso a Paso de la ejecución y retorno

No.	Actividad	Responsable	Fecha – Hora Inicio *Formato: dd/mm/aaaa – hh:mm*	Fecha – Hora de Finalización *Formato:dd/mm/aaaa – hh:mm*	Tiempo (horas-minutos)
1.					
2.					
3.					
4.					
5					
6					
7					
8					
9					

OBSERVACIONES:

- ...
- ...