AUDITORÍA INTERNA DE GESTIÓN
PROCESO GESTIÓN TIC’s

Mayo 30 de 2017

Apreciado Ingeniero

Mauricio Velásquez Mesa, Coordinador GIT de Apoyo Informático

El Grupo Interno de Trabajo (GIT) de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones, los Decretos 1537 de 2001, 019, 2482 y 2641 de 2012 y 943 del 21 de mayo de 2014; así como los lineamientos establecidos en la nueva Guía de Auditoria para Entidades Públicas del DAFP, y las Resoluciones CGN 328 de 2005 y 203 de 2015, tiene como función realizar la evaluación independiente al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar el cumplimiento y la efectividad de la gestión institucional y de los objetivos de la entidad, produciendo recomendaciones para asesorar al representante legal en busca del mejoramiento continuo.

En cumplimiento al Programa General de Auditorías aprobado para la vigencia 2017, por el Comité de Coordinación del Sistema de Control Interno, este GIT adelantó la Evaluación al Proceso Gestión TIC's, a fin de conocer el grado de cumplimiento de las actividades establecidas para su desarrollo y elevar las recomendaciones que sean necesarias en ejercicio del mejoramiento continuo, lo cual redundará en el cumplimiento de los Objetivos Estratégicos de la Entidad.

Los procedimientos de auditoría se realizaron sobre la base de pruebas selectivas; un procedimiento de esta naturaleza, no puede identificar todas las desviaciones de control, sino solamente aquellas que estén presentes dentro de la muestra evaluada.

Este informe fue presentado en mesa de trabajo del 2 de junio de 2017 para la suscripción del respectivo plan de mejoramiento; por tanto es importante que se termine de diligenciar el formato "CYE05-FOR02 Plan de Mejoramiento", el cual debe ser remitido por correo electrónico a más tardar el 9 de junio de 2017.

Cordialmente,

MARITZA VELANDIA CARDOZO
Coordinador GIT de Control Interno

C. C.: Dr. Pedro Bohórquez Ramírez - Contador General de la Nación

Proyectó: José Leonardo Buitrago
Revisó: Maritza Velandia Cardozo

Tabla de Contenido

OBJETIVO

Evaluar la ejecución estratégica a través de los programas, planes, proyectos y procedimientos que el proceso Gestión TIC's de la CGN desarrolla en cumplimiento de sus funciones; así como, la observancia de las políticas, la administración del riesgo y la efectividad de los controles e indicadores; con el fin de identificar vulnerabilidades, oportunidades y aspectos susceptibles de mejora.

ALCANCE

El marco de este trabajo de aseguramiento se enmarcará en el universo de auditoría inherente al proceso Gestión TIC's de la CGN, sobre unidades como: la plataforma tecnológica, la ingeniería de software, la seguridad informática, la planeación estratégica, y los planes, programas y proyectos ejecutados durante la vigencia 2016 y lo corrido de 2017.

EVALUACION DE CONTROLES

De conformidad con los resultados obtenidos, en el siguiente cuadro se presenta la metodología de evaluación con sus respectivos comentarios para la adecuada comprensión y correcta implementación del plan de mejoramiento, de acuerdo con la clasificación:

	**INADECUADO** En los procedimientos y pruebas de auditoría, se evidencia que existe un bajo grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero son muy vulnerables y deben ser objeto de intervención o ajustes que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.
	**ADECUADO CON OPORTUNIDAD DE MEJORA** En los procedimientos y pruebas de auditoría, se evidencia que existe un grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero presentan oportunidades de mejora que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.
	**SATISFACTORIO** En los procedimientos y pruebas de auditoría, se evidencia que existe un alto grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando.

1. Indicadores

Actividades de Control	Evaluación del Control	Observaciones
Implementación, seguimiento y análisis.		- Algunos indicadores carecen de las características recomendadas por el DAFP para cumplir con las funciones y beneficios propios de toda herramienta de medición.

2. Normatividad vigente aplicable

Actividades de Control	Evaluación del Control	Observaciones
Aplicabilidad de la normatividad y directrices vigentes.		- Existen actividades suscritas en planes de mejoramiento de años anteriores que propenden por el cumplimiento cabal de la Política de Soporte a Usuarios y la Política de Administración de usuarios y/o contraseñas pero que a la fecha no se han ejecutado.

3. Universo de auditoría - Unidades auditables

Subproceso y/o Actividad	Actividades de Control	Evaluación del Control	Observaciones
Soporte a Usuarios	Satisfacción de usuarios		- Las interfaces web para que los usuarios externos puedan registrar directamente sus propios requerimientos, obtener un número de ticket, hacerle seguimiento y evaluar la satisfacción del servicio prestado, aún no se han implementado.

MATRIZ DE EVALUACION DE CONTROLES			
AUDITORIA AL PROCESO			
Subproceso y/o Actividad	**Actividades de Control**	**Evaluación del Control**	**Observaciones**
Administración Plataforma TI	Plataforma misional - CHIP		- El ambiente CHIP que está en producción presenta debilidades en su componente llamado “Adm-Services”, puesto que se ha evidenciado que es a causa de éste que se generan caídas en el servicio y por consiguiente reprocesos de envíos, especialmente en días de corte donde se genera la mayor demanda.
Administración Plataforma TI	Redes y comunicaciones		- Los equipos activos de la red de datos de la entidad se encuentran desactualizados, toda vez que ya no cuentan con la garantía del fabricante ni con servicio de soporte o mantenimiento de terceros. - El switch de conexión de servidores misionales y de gestión se encuentra aproximadamente al 90 % de su capacidad y tampoco cuenta con garantía ni soporte. - Para la vigencia 2017, no se observó la inclusión del fortalecimiento de la infraestructura de la red de datos de la entidad en el Proyecto de Inversión.
Correo electrónico	Filtro anti spam y amenazas		
Proyecto de Inversión	Actualización		- Se observó, que además del fortalecimiento de los sistemas de información de la plataforma tecnológica, el proyecto de inversión incluye aspectos misionales que generan la necesidad de contar con servicios especializados que soporten la operación de la entidad, situación que requiere la revisión de los componentes del proyecto.
Administración Plataforma TI	Portal y ambientes WEB		- La versión de IBM Portal que la entidad tiene instalado en producción es la versión 7, la cual dejó de ser soportada por su fabricante desde el 31/12/2016. - La falta de un ambiente de pruebas y las limitaciones de la versión actual impiden el avance de proyectos como: la implementación de los ambientes web de CHIP en IBM Portal y la aplicación de herramientas que faciliten la consulta de estos contenidos a la población con discapacidad.
Proyecto Dispositivos Móviles	App Android y iOS		
Proyecto Georreferenciación	Geoportal SIGCGN		

Subproceso y/o Actividad	Actividades de Control	Evaluación del Control	Observaciones
Operación Centro de Cómputo	Sistema eléctrico		
Seguridad de la Información	Componente GEL - MSPI		- La aplicabilidad de los lineamientos MSPI en la entidad, presenta un porcentaje de cumplimiento inferior al 40%, debiendo ser éste a la fecha como mínimo 60%.
Administración Plataforma TI	Plataforma de gestión		- Algunas aplicaciones críticas como: servidor de archivos (Pathfinder), el antivirus y el repositorio, ejecutan sistemas operativos obsoletos que ya nos son soportados por el fabricante.
Controlador de dominio	Perfiles de usuario y seguridad		
Copias de seguridad	Custodia externa de medios		- A la fecha han pasado cinco (5) meses sin contar con el servicio de custodia externa, aunque este proceso no demanda mayor presupuesto ni complejidad en las especificaciones técnicas, aún se encuentra en la etapa de estudios previos, afectando así las estrategias de continuidad y contingencia de la entidad.
PETI	Actualización		- Con base en la Guía Técnica emitida por MinTIC's el 30 de marzo de 2016, en dónde se brindan lineamientos para estructurar un PETI, se observó que en lo que corresponde a la entidad, algunos contenidos no están incluidos o desarrollados con el grado de profundidad que ameritan. - No obstante los aspectos que el PETI incluye actualmente, no se observó contenido relacionado con gobierno de TI, análisis financiero, indicadores, riesgos, seguridad, etc., los cuales son de gran relevancia en un documento de este tipo.
Plan de Adquisiciones	Actualización		
Plan de Contingencia	Actualización		- El Plan de Contingencia de la entidad se encuentra desactualizado, toda vez que el documento principal y las guías de implementación tienen fecha de diciembre de 2014.

Subproceso y/o Actividad	Actividades de Control	Evaluación del Control	Observaciones
Plan de Continuidad del Negocio	Actualización		- Las estrategias propuestas en 2014 para la implementación y fortalecimiento del PCN aún no han sido implementadas: 1. Definir un plan de contingencia, completo, actualizado... 2. Establecer el trabajo en pares para cada servicio... 3. Contar con un servicio de custodia externa para medios magnéticos… 4. Contar con soporte especializado para las aplicaciones... 5. Definir, establecer y divulgar un flujograma de comunicaciones…
Seguridad de la Información	Incidentes de Seguridad		
Administración Plataforma TI	Sistemas de almacenamiento		
Seguridad perimetral	UTM - Firewall		
Contingencia y continuidad	Centro alterno de datos		- Según la auditoría CGR vigencia 2015 y OCI vigencia 2016 – 2017, aún existen componentes del sistema CHIP instalados en máquinas recibidas en comodato pertenecientes al Municipio de Medellín, dichos servidores podrían ser requeridos por su dueño en cualquier momento y la CGN no tendría capacidad de reemplazarlos inmediatamente.
Contingencia y continuidad	Data Center		
Proyecto Atención al Ciudadano	Adecuación tecnológica		

CONCLUSIÓN

El GIT de Apoyo Informático ha adelantado labores que han fortalecido la infraestructura tecnológica de la entidad, lo cual se evidenció a través de la adquisición de procesamiento y almacenamiento para la plataforma de gestión, la actualización del sistema de copias de respaldo y la ampliación de cobertura de aires acondicionados en el centro de datos; así mismo, el proceso Gestión TIC's ha desarrollado actividades que propenden por mejorar el servicio al ciudadano, como son: aplicación de coordenadas en el Geoportal para brindar mayor precisión en las consultas, mejoras visuales en la app para dispositivos móviles, generación de los certificados en línea para cada una de las categorías que las entidades reportan, nueva funcionalidad para el manejo del código CUIN y la gestión para los usuarios de Investigación y Estadística de la Contaduría, notificación de estados de envío por medio de correo electrónico, desarrollo del aplicativo MEFP-2014 (Manual de Estadísticas de Finanzas Públicas) (MEFP-2014) y entrega del reporte anual al Fondo Monetario Internacional, entre otros.

Sin embargo, existen algunos elementos, planes y servicios del proceso de Gestión TIC's en estado de vulnerabilidad y que por su relevancia deberían ser objeto de intervención inmediata, específicamente en lo que tiene que ver con la infraestructura de red, la custodia externa de información sensible, el Plan de Contingencia, el Plan de Continuidad del Negocio y la normatividad aplicable. De igual manera, existen aspectos susceptibles de mejora, que también deben ser ajustados de acuerdo con las observaciones y recomendaciones establecidas en el presente informe.

Dada la importancia que tienen los indicadores como mecanismos de medición y control en la gestión del proceso, se les debe dar un tratamiento prioritario, ser evaluados y ajustados para su fortalecimiento y así cumplir con los objetivos institucionales de la CGN.

Así mismo, es importante anotar la cordialidad y disponibilidad para atender esta auditoría durante su etapa de ejecución, evidenciándose el compromiso con el Programa General de Auditorías vigencia 2017, aprobado por la alta dirección.

1. Indicadores

Una vez detectadas las falencias técnicas en la aplicación SIGI, las cuales impiden el acceso amplio y suficiente a toda la información actualizada y relacionada con los indicadores, el GIT de Control Interno se abstiene de consultar dicha fuente como referente para realizar cualquier tipo de comparación o análisis.

El proceso Gestión TIC's consta de ocho (8) indicadores, los cuales son evaluados trimestralmente como se observa en el Cuadro de Mando Integral publicado en la página web de la entidad; en cuanto a las características básicas, claves de formulación y criterios para la selección de los mismos establecidos por el Departamento Administrativo de la Función Pública (DAFP), se presentan los siguientes resultados:

Indicador / Características	Pertinencia	Independencia	Costo	Confiabilidad	Simplicidad	Oportunidad	No Redundancia	Focalizado en áreas controlables	Participación	Disponibilidad	Sensibilidad	Funcionalidad	Utilidad
Disponibilidad plataforma de gestión	I	C	C	C	C	C	C	C	C	C	C	C	C
Disponibilidad de plataforma misional	C	C	C	C	C	C	C	C	C	C	C	C	C
Efectividad, desarrollo y soporte	C	C	C	C	C	C	C	C	C	C	C	C	C
Satisfacción a usuarios de mesa de servicios	C	C	C	I	C	C	C	C	P	I	I	I	P
Disponibilidad de LAN	I	C	C	C	C	C	C	C	P	C	C	C	C
Disponibilidad de internet	I	I	C	C	C	C	C	P	P	C	C	C	C
Disponibilidad de los sistemas de información	I	C	C	C	I	C	P	P	C	C	C	P	P
Pérdida de disponibilidad y confidencialidad de la información	I	C	C	P	I	C	C	P	C	P	P	C	C

Cumple: C - Incumple: I - Cumple parcialmente: P

Los indicadores que se refieren a la plataforma misional y a la efectividad de las labores de desarrollo, se ajustan a las características básicas definidas por el DAFP que permiten establecer el grado de avance de los resultados esperados, aumentan el grado de satisfacción de los usuarios, fortalecen la imagen institucional y garantizan el proceso de mejora continua de la entidad.

OBSERVACIÓN

Disponibilidad plataforma de gestión: La pertinencia hace referencia a los productos esenciales de cada institución, si bien la plataforma de gestión apoya actividades que pueden ser misionales, no representa en si misma alguno de los productos o servicios de la entidad.

Satisfacción a usuarios de mesa de servicios: Los resultados de la calificación de este indicador están motivados principalmente por la ausencia de la evaluación de satisfacción del usuario externo, más aún cuando éste representa aproximadamente el 90% de los requerimientos que se abren en la Mesa de Servicios; afectando así características como: confiabilidad, participación, disponibilidad, sensibilidad, funcionalidad y utilidad.

Disponibilidad de LAN: La pertinencia hace referencia a los productos esenciales de cada institución, si bien la disponibilidad de LAN apoya actividades que pueden ser misionales, no representa en si misma alguno de los productos o servicios de la entidad.

Disponibilidad de Internet: La pertinencia hace referencia a los productos esenciales de cada institución, si bien la red Internet apoya actividades que pueden ser misionales, no representa en si misma alguno de los productos o servicios de la entidad. Este servicio es prestado por un tercero, por tanto el factor de independencia tampoco se puede alcanzar.

Disponibilidad de los sistemas de información: Los resultados de la calificación de este indicador están motivados principalmente por lo amplio del término “sistemas de información”, toda vez que por su definición bien podría referirse al sistema CHIP, al sistema de registro de ingreso de personal o a alguna de las plataformas que existen en la entidad.

Pérdida de disponibilidad y confidencialidad de la información: Los resultados de la calificación de este indicador están motivados principalmente por dos aspectos; el primero relacionado con la palabra “pérdida” la cual puede generar dificultades de interpretación y el segundo con la forma en cómo se evalúa, dado que dos (2) de los veintitrés (23) numerales de la política no se cumplen, el promedio de los últimos siete trimestres es de 91.31%.

Los indicadores anteriormente mencionados carecen de las características recomendadas por el DAFP para cumplir con las funciones y beneficios propios de toda herramienta de medición como son: establecer el grado de avance o logro de los objetivos trazados y de los resultados esperados del proceso, con el fin de facilitar el proceso de toma de decisiones.

RECOMENDACIÓN

Se deben generar mecanismos que aseguren el estudio y aplicabilidad de las mejores prácticas en la construcción de indicadores, teniendo en cuenta aspectos como la tipología, medidas de desempeño claves, así como referentes comparativos y principales características; lo anterior con el objetivo de contar con herramientas que faciliten la medición y control de las actividades críticas del proceso.

2. Normatividad vigente aplicable

Tomando el numeral 5° de este documento como referente base y teniendo en cuenta el análisis realizado en auditorías recientemente ejecutadas, a continuación se realiza un consolidado del estado actual del cumplimiento normativo aplicable al proceso Gestión TIC's:

Base Normativa	Estado Actual
Política de Soporte a Usuarios	En la auditoría realizada durante el mes de septiembre de 2016 al procedimiento GTI-PRC01 se observó lo siguiente: *"Los Acuerdos de Niveles de Servicio (ANS's) estipulados en la Política de Soporte a Usuarios para la atención de solicitudes e incidentes, tiene un grado de incumplimiento superior al 10%, porcentaje que afecta negativamente el nivel de satisfacción de los usuarios y aumenta la probabilidad de materialización de los riesgos inherentes al proceso involucrado; más aún, teniendo en cuenta que en aquellos casos donde la prioridad es "crítica" y el impacto es "alto" solo el 75% de éstos se soluciona oportunamente".* Posteriormente se suscribió el respectivo plan de mejoramiento que relacionaba el 23 de enero de 2017, como fecha de implementación de la acción a realizar, pero hasta el momento no se ha hecho efectiva.

Base Normativa	Estado Actual
Política de Administración de usuarios y/o contraseñas	En la auditoría realizada durante el mes de noviembre de 2015 al procedimiento GTI-PRC02 se observó lo siguiente: *"Evaluada la Política de Administración de Usuarios y Contraseñas, se evidenció que no se están ejecutando con la frecuencia establecida los cambios de contraseña para los usuarios administradores de servidores y equipos activos de red, los cuales fueron observados en los registros allegados por el usuario que evidencian cambios de contraseñas para los meses de enero, febrero, marzo, abril y mayo de 2014, así como de enero y junio para la vigencia 2015, debiendo ser esta una tarea a ejecutar los primeros 5 días de cada mes. Incumpliendo el numeral 6.4 de la Política de Administración de Usuarios y Contraseñas".* Posteriormente se suscribió el plan de mejoramiento que relacionaba el 20 de mayo de 2016 como fecha de aplicación de la acción a realizar; hasta el momento no se ha hecho efectiva.
Política de Seguridad Informática y Política de Copias de Respaldo	Una de las actividades del Plan de Mejoramiento correspondiente a la auditoría realizada durante el mes de diciembre de 2016 al procedimiento GTI-PRC010 menciona: *"Realizar una revisión y posterior actualización de la Política de Seguridad de la Información; estableciendo las actividades que se pueden y deben realizar de acuerdo a plataforma tecnológica con la que se cuenta en la CGN".* Esta actividad tiene fecha de finalización el 29 de junio de 2017.
Política de Desarrollo y Mantenimiento de Software	En la auditoría realizada durante el mes de diciembre de 2015 al procedimiento GTI-PRC07 se observó lo siguiente: *"Evaluada la Política de Desarrollo y Mantenimiento de Software, y la Resolución 151 del 10 de junio de 2010, se evidenció que para las vigencias 2014 y 2015 existen diez (10) Órdenes de Cambio de las cuales solo tres (3) fueron aprobadas en Comité ETT. Adicionalmente, el auditado informó que no se han generado actas de Comité CARCC. Incumpliendo de esta manera el numeral 10 de las "Políticas Generales" correspondientes al título 2.1 de la Política de Desarrollo y Mantenimiento de Software, y la Resolución 151 del 10 de junio de 2010 en lo que disponen los literales a y b del artículo 2°, y los literales b y c del artículo 5°. 6.".* Posteriormente se suscribió el respectivo plan de mejoramiento que se cerró en el mes de septiembre de 2016 después de verificar la ejecución de la acción a realizar.
Decreto 2693 del 21 de diciembre de 2012. Estrategia de Gobierno en Línea (GEL).	Una de las actividades del Plan de Mejoramiento correspondiente a la auditoría realizada durante el mes de diciembre de 2016 al procedimiento GTI-PRC010 menciona: *"Dar cumplimiento a la creación e implementación del Modelo de Seguridad y Privacidad de la Información; con el fin de superar los rezagos que se han generado y alcanzar las metas definidas para las vigencias futuras.".* Esta actividad tiene fecha de finalización el 29 de junio de 2017.

Base Normativa	Estado Actual
Leyes del Derechos de Autor	En la auditoría realizada durante el mes de agosto de 2016 al procedimiento GTI-PRC05 se recomendó lo siguiente: *"De igual manera se debe reconocer y dar el respectivo tratamiento, al potencial riesgo de "violación del derecho de autor", causado por aplicaciones que requieren el pago del debido licenciamiento y que hoy día son posibles de instalar en algunos equipos de la entidad sin autorización ni control por parte del GIT de Apoyo Informático.".* Posteriormente en mesa de trabajo se acordó la inclusión de este riesgo en el contexto de la seguridad de la información.
Decreto 2844 del 05 de agosto de 2010. Sistema de Seguimiento a Proyectos de inversión.	• El Proyecto de Inversión del GIT de Apoyo Informático tiene como nombre: Fortalecimiento de los Sistemas de Información y Consolidación Contable Nacional, tenía una vigencia inicial de cuatro (4) años (2014 – 2017) pero fue ampliada hasta 2019 por el DNP. • Se observó que el grupo de Proyección Tecnológica realiza actualizaciones mensuales al Proyecto de Inversión según el avance en la ejecución, las liberaciones de saldos o aplazamientos del presupuesto. • Se consultó el sistema SPI (Seguimiento a Proyectos de Inversión) y se observó que es consecuente en contenido y actualización con la documentación que se maneja al interior del GIT de Apoyo Informático.

OBSERVACIÓN

Existen actividades suscritas en planes de mejoramiento de años anteriores que propenden por el cumplimiento cabal de la Política de Soporte a Usuarios y la Política de Administración de usuarios y/o contraseñas pero que a la fecha no se han ejecutado, poniendo en un potencial riesgo la seguridad de la información de la entidad y afectando negativamente los niveles de satisfacción de los usuarios internos y externos de la CGN.

RECOMENDACIÓN

Generar estrategias que propendan por la toma de conciencia sobre la importancia de implementar oportunamente las actividades propuestas en los planes de mejoramiento, toda vez que éstas tienen por objeto corregir, fortalecer y asegurar la mejora continua del proceso, más aún cuando se trata de la aplicabilidad y cumplimiento de políticas que hacen parte del sistema de gestión de la entidad que protegen a los usuarios en el uso de herramientas tecnológicas y garantizan su satisfacción al utilizar los servicios que la CGN presta.

3. Universo de auditoría - Unidades auditables

A continuación se presentan los resultados obtenidos después de aplicar las pruebas propuestas en el numeral 8.3 de este documento:

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
1	Riesgo de insatisfacción de los usuarios.	Comprobar que la satisfacción de los usuarios internos y externos de la CGN esté siendo medida y gestionada conforme al principio de mejora continua.	• Para la vigencia 2017, como se observó en los estudios previos, se tiene proyectado suscribir un contrato que garantice la implementación de las siguientes funcionalidades relacionadas con el gestor de requerimientos Service Desk: - Renovación de licenciamiento. - Actualización de versiones. - Habilitación de interfaces web para que los usuarios externos puedan registrar directamente sus propios requerimientos, obtener un número de ticket, *hacerle seguimiento y evaluar la satisfacción del servicio prestado.*
2	Riesgo de fallo o no disponibilidad de la plataforma misional.	Revisar que la arquitectura y configuración de los elementos de hardware y software en los ambientes de producción, desarrollo, pruebas, contingencia, etc., estén alineados con las mejores prácticas de administración.	• Existen seis (6) ambientes CHIP: producción, pre-producción, pruebas, capacitación, desarrollo y contingencia; instalados sobre cinco (5) servidores físicos IBM Power 740 y uno (1) Power 720 sobre los cuales se practicó mantenimiento preventivo el pasado 4 de marzo de 2017 y cuya garantía está vigente hasta junio del mismo año. • El ambiente de producción tiene implementado un sistema de replicación en alta disponibilidad para la base de datos CHIP, la cual reposa en la misma unidad física de almacenamiento (SAN) pero en diferente ubicación lógica (LUN). • La base de datos del Boletín de Deudores Morosos del Estado (BDME) también tiene implementado un sistema de replicación en alta disponibilidad. • Los componentes, aplicaciones y servicios de los diferentes ambientes, se encuentran distribuidos entre los seis (6) servidores físicos mencionados anteriormente con el objetivo de cubrir y balancear la demanda de recursos. • *Algunos de los ambientes tienen usos diferentes a los originalmente destinados según su nombramiento, es decir; se encontró que el ambiente de pre-producción es utilizado para que los usuarios estratégicos hagan parametrizaciones, en el ambiente de capacitación se adelantan pruebas del proyecto "miles a pesos".* • *El ambiente CHIP que está en producción presenta debilidades en su componente llamado "Adm-Services", puesto que se ha evidenciado que es a causa de éste que se generan caídas en el servicio y por consiguiente reprocesos de envíos, especialmente en días de corte donde se genera la mayor demanda.*

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
3	Riesgo de fallo o no disponibilidad de la red de datos interna e Internet.	Comprobar que la arquitectura y configuración de la red de datos propende por la seguridad, el alto desempeño y la versatilidad en la administración.	• La entidad cuenta con dos (2) enlaces (activo-activo) de conexión a internet, de 24 Mbps cada uno, escalable a 48 Mbps en fechas de corte. • *Los equipos activos de la red de datos de la entidad se encuentran desactualizados, toda vez que ya no cuentan con la garantía del fabricante ni con servicio de soporte o mantenimiento de terceros.* • *Para la vigencia 2017, no se observó la inclusión del fortalecimiento de la infraestructura de la red de datos de la entidad en el Proyecto de Inversión.* • *Aunque los principales equipos de la red (backbone) están configurados en forma redundante para brindar la mayor disponibilidad posible, ya no cuentan con garantía ni soporte en caso de fallo.* • *El switch de conexión de servidores misionales y de gestión se encuentra aproximadamente al 90 % de su capacidad y tampoco cuenta con garantía ni soporte.* • *El firewall está configurado de forma redundante para brindar la mayor protección contra amenazas, pero solo será soportado por el fabricante hasta diciembre de 2017 tiempo después del cual no se contará con los servicios unificados contra amenazas (UTM).* • *Algunos equipos de red ubicados en los pisos superiores de la entidad (switches de borde), cuentan con velocidades obsoletas (10/100) que merman el desempeño de la red para los usuarios conectados a los mismos.* • *Lo equipos de conexión inalámbrica de la entidad no cuentan con la capacidad para atender la demanda de servicio que se genera en cada piso.* • *La falta de soporte y garantía generalizada de los equipos activos de red, limitan los avances en la adopción de buenas prácticas como: redes virtuales (vlans) e IPv6.* • *El último mantenimiento de los equipos activos de la red se efectuó en el año 2015.* • *Los enlaces redundantes de conexión a internet pertenecen al mismo proveedor.*
4	Riesgo de ataques cibernéticos por deficiencias en el filtrado de correo electrónico.	Comprobar que el filtrador se encuentre configurado y afinado para impedir el paso de correo no deseado y amenazas como spyware, phishing, etc.	• El servicio de filtrado de correo no está configurado en una aplicación independiente, sino que hace parte de las opciones de administración de la plataforma de correo electrónico de la entidad. • La actualización y fortalecimiento del servicio de filtrado de correo se basa en un sistema inteligente que aprende de las experiencias e instrucciones de los mismos usuarios. • El nivel de especificidad en la configuración y creación de políticas es alto, toda vez que la solución permite filtrar contenidos o tipos de archivos específicos incluso por usuario, ya sea para mensajes entrantes o salientes.

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
5	Riesgo de adoptar un enfoque tecnológico incompatible con las necesidades y misión de la entidad.	Verificar que las actividades del Proyecto de Inversión se ajusten a las necesidades de la entidad, así como su avance y cumplimiento en la ejecución.	• El Proyecto de Inversión del GIT de Apoyo Informático tiene como nombre: Fortalecimiento de los Sistemas de Información y Consolidación Contable Nacional, tenía una vigencia inicial de cuatro (4) años (2014 – 2017) pero fue ampliada hasta 2019 por el Departamento Nacional de Planeación (DNP). • Los objetivos específicos ajustados a la cadena de valor son los siguientes: - Fortalecer la disponibilidad de los sistemas de información contable. - Fortalecer la plataforma de tecnologías de información y comunicaciones de la CGN. - Adoptar e implementar en el sector público normas internacionales en materia contable. - Fortalecer la estrategia de seguridad de la información. • Se observó que el grupo de Proyección Tecnológica realiza actualizaciones mensuales al Proyecto de Inversión según el avance en la ejecución, las liberaciones de saldos o aplazamientos del presupuesto. • Se consultó el sistema SPI (Seguimiento a Proyectos de Inversión) y se observó que es consecuente en contenido y actualización con la documentación que se maneja al interior del GIT de Apoyo Informático. • *Se observó, que además del fortalecimiento de los sistemas de información de la plataforma tecnológica, el proyecto de inversión incluye aspectos misionales que generan la necesidad de contar con servicios especializados que soporten la operación de la entidad, situación que requiere la revisión de los componentes del proyecto.*
6	Riesgo de fallo o no disponibilidad de los ambientes web de la entidad.	Asegurar que la arquitectura y los ambientes que implementan los ambientes web de la entidad, se encuentren alineados a las mejores prácticas en desempeño y seguridad.	• La asignación de recursos de hardware para IBM Portal en cuanto a procesamiento, memoria y almacenamiento cumple con los requerimientos sugeridos por el fabricante. • El servidor Lapetus en donde se encuentran alojadas la intranet y la web de la entidad permite la gestión de contenidos de forma remota, así mismo se respalda a diario. • La página web de la entidad ha implementado mecanismos de lectura y audición que facilita la consulta de los contenidos a la población discapacitada. (COVERTIC) • *La versión de IBM Portal que la entidad tiene instalado en producción es la versión 7, la cual dejó de ser soportada por su fabricante desde el 31 de diciembre del año 2016.* • *No existe un ambiente de IBM Portal para el desarrollo de pruebas que permitan la posterior aplicación de actualizaciones o nuevas funcionalidades en producción.* • *Las limitaciones de la versión 7 de IBM Portal generan restricciones funcionales y de cumplimiento, por ejemplo: no es posible adjuntar archivos para los servicios en línea que lo requieren, la versión 6 del SDK ya no es compatible con la mayoría de navegadores, no es posible autenticar el acceso a intranet con el LDAP de la entidad, el módulo de seguridad no cumple al 100% con los lineamientos del Manual 4 de Gobierno en Línea.* • *La falta de un ambiente de pruebas y las limitaciones de la versión actual impiden el avance de proyectos como: la implementación de los ambientes web de CHIP en IBM Portal y la aplicación de herramientas que faciliten la consulta de estos contenidos a la población con discapacidad.*

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
7	Riesgo de fallo o no disponibilidad de la aplicación de la CGN para celulares.	Revisar que la arquitectura y la infraestructura implementada en este proyecto, garantice la disponibilidad y estabilidad de acceso permanente para todos sus potenciales usuarios.	• La App Contaduría está en su versión 1.1.0 disponible en la tienda Play Store de Google para dispositivos con sistemas operativos Android, la última actualización se realizó el 14 de julio de 2016. • La aplicación se desarrolla principalmente en lenguaje java y se ejecuta sobre tecnología Power y sistemas operativos AIX. • Esta App se produce a través de los procedimientos relacionados con el desarrollo de software de la entidad como son las pruebas, el mezclado, la generación de versión y el despliegue. • Las fuentes y documentación del proyecto están ubicadas en el repositorio de datos de informática instalado en el servidor Pandora. • La consulta al BDME se encuentra en desarrollo, así como la disponibilidad de esta App para sistemas operativos iOS de Apple. • *La aplicación ha sido descargada 1659 veces, sin embargo solo 284 usuarios la mantienen en sus dispositivos móviles.* • *Algunos contenidos como el organigrama, la atención de PQRD's y la política de privacidad se encuentran desactualizados.*
8	Riesgo de fallo o no disponibilidad del sistema de georreferenciación publicado en la web de la entidad.	Comprobar que la arquitectura y la infraestructura implementada en este proyecto, garantice la disponibilidad y estabilidad de acceso permanente para todos sus potenciales usuarios.	• La aplicación de georreferenciación está en su versión 3.1 disponible en la página web de la entidad y del sistema CHIP, la última actualización se realizó el 4 de abril de 2016. • La aplicación se desarrolla principalmente en lenguaje java y se ejecuta sobre tecnología Power y sistemas operativos AIX. • Esta aplicación se produce a través de los procedimientos relacionados con el desarrollo de software de la entidad como son las pruebas, el mezclado, la generación de versión y el despliegue. • Las fuentes y documentación del proyecto están ubicadas en el repositorio de datos de informática instalado en el servidor Pandora. • Está en desarrollo la consulta al BDME a través de tecnologías de georreferenciación.

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
9	Riesgo de no disponibilidad de los sistemas de información de la entidad por fallos o insuficiencia eléctrica.	Comprobar la existencia de los planos eléctricos, el correcto funcionamiento de la planta eléctrica y la adecuada configuración de las UPS's.	• La CGN cuenta con capacidad eléctrica de 72 KVA fijada por el proveedor del servicio. • La planta eléctrica con la que cuenta el edificio tiene una capacidad de 120 KVA con autonomía de 18 horas y tiempo de respuesta de cinco (5) segundos. • La entidad cuenta con dos UPS's marca APC, serie Symetra, una con capacidad de 40 KVA y la otra de 80 KVA. La garantía está vigente hasta octubre de 2017 y el último mantenimiento se realizó en diciembre de 2016. • En el centro de cómputo de la entidad existen tres (3) tableros eléctricos; el primero con los breakers independientes por piso y los otros dos corresponden a las conexiones de las UPS's con los servidores. • Se accedió a la interface web de administración y se observó que el estado del banco de baterías es óptimo, brindando en promedio una hora y media de respaldo con una carga eléctrica del 25%. • *Se observó un mapa de distribución de puestos de trabajo que relaciona el número de los puntos de corriente, pero no contiene conexiones ni capacidades de los elementos de la red eléctrica.*
10	Riesgo de incumplimiento de las metas GEL establecidas por Min TIC's y afectación del Índice de Transparencia Nacional (ITN).	Verificar que los tres logros GEL, hayan sido aplicados en la entidad según los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).	• Se está gestionando la inclusión del esquema de Gobierno de TI dentro del alcance del Comité SIGI de la entidad, para garantizar la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión. (Lineamiento LI.GO.01) • En cuanto a la implementación de un repositorio de datos para uso de toda la entidad, se aclaró que: Secretaría General, como administradora de la gestión documental y con el apoyo de informática, debe generar estrategias para la adquisición de una solución propietaria que cuente con soporte y garantía. (Lineamiento LI.INF.15) • Se observó que en marzo de 2017, el Comité SIGI de la entidad aprobó la Política de Seguridad y Privacidad de la Información propuesta por el GIT de Apoyo Informático, con el propósito de avanzar y fortalecer ese aspecto. (Lineamiento LI.SIS.22) • El GIT de Apoyo Informático participa activamente en el Comité Sectorial de Tecnología liderado por el Ministerio de Hacienda, para obtener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI. (Lineamiento LI.ES.13) • En lo relacionado con la identificación de las áreas con oportunidad de mejora, se aclaró que inicialmente se adoptó un enfoque interno, el cual se está fortaleciendo a través del monitoreo constante de los elementos de TI y el análisis de nuevas tecnologías por parte del grupo de proyección tecnológica. (Lineamiento LI.GO.13) • *Con base en el informe de auditoría realizada al procedimiento PRC010 "Seguridad de la Información" el pasado 21 de diciembre de 2016 y no obstante las aclaraciones anteriores, las cuales propenden por el avance y aplicabilidad de los lineamientos MSPI en la entidad, aún se cuenta con un porcentaje de cumplimiento inferior al 40%, debiendo ser éste a la fecha como mínimo 60%.*

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
11	Riesgo de fallo o no disponibilidad de la plataforma de gestión.	Revisar que la arquitectura y configuración de los elementos de hardware y software en los diferentes ambientes, estén alineados con las mejores prácticas de administración.	• En el año 2016 el GIT de Apoyo Informático fortaleció la infraestructura de gestión con la adquisición de un (1) enclosure PowerEdge FX2, tres (3) servidores Dell PowerEdge FC630 y dos (2) switches de conectividad SAN sobre los cuales se practicó mantenimiento preventivo el pasado enero de 2017 y cuya garantía está vigente hasta el año 2021. • Junto con el hardware se adquirió el software de virtualización VMWare 6.0 para toda la plataforma. • Los servicios de dominio, copias de respaldo (TSM), SIGI y Cognos aún se ejecutan en máquinas físicas independientes. • *En cuanto a las copias de seguridad de la plataforma, en 2016 se adquirió una solución que permite crear copias de respaldo de equipos virtualizados que aún se encuentra en implementación.* • *De forma complementaria se realizan clones semanales de cada máquina virtual los fines de semana en horas de la noche, pero no se encontraron evidencias de pruebas de restauración que aseguren la funcionalidad y completitud de los mismos.* • *Algunas aplicaciones críticas como: servidor de archivos (Pathfinder), el antivirus y el repositorio, ejecutan sistemas operativos obsoletos que ya nos son soportados por el fabricante.*
12	Riesgo de accesos restringidos o indebidos a servicios o aplicaciones por fallo o no disponibilidad del Controlador de Dominio.	Revisar la configuración de los roles, las políticas, la replicación, la resolución de nombres y la seguridad en la administración de usuarios.	• El servicio de Controlador de Dominio (DC) esta implementado en dos (2) máquinas físicas HP ProLiant DL380 independientes, a las cuales se les realizó mantenimiento preventivo en el mes de diciembre de 2016. • El servicio de DC se ejecuta sobre sistema operativo Windows Server 2012 desde septiembre de 2015 momento en que también se realizó la actualización de dominio CONTADURIA a CGN. • La configuración del DC consta de un servidor principal y uno secundario, los cuales trabajan de forma simultánea y desarrollan los servicios DHCP (Protocolo de Configuración Dinámica de Host) y DNS (Domain Name System). • La prueba de replicación entre el controlador de dominio primario y secundario fue exitosa. • La configuración de red de los servidores de dominio permite que las solicitudes de los usuarios internos vayan directamente a los servidores de la entidad, sin pasar obligatoriamente por el firewall (cortafuegos), esto reduce la carga sobre el mismo y mejora los tiempos de respuesta. • El servicio DHCP está configurado para asignar direcciones IP dinámicas con renovación cada 60 días, excepto para aquellos usuarios que requieren IP's fijas como los que usan VPN's para conexiones remotas. • *Aunque los servidores HP ProLiant DL380 cuentan con contrato vigente de mantenimiento preventivo, ya no cuentan con la garantía de fábrica puesto que fueron adquiridos en el año 2012.*

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
13	Riesgo de imposibilidad de recuperación ante pérdida de información misional sensible.	Comprobar que los medios magnéticos de las copias de seguridad de la información sensible, se encuentren almacenados externamente en instalaciones adecuadas para tal fin.	• En la vigencia 2016, la CGN contó con el servicio de custodia externa de elementos de TI prestado por la empresa THOMAS MTI desde el 02 de mayo hasta el 31 de diciembre, para un máximo de 150 medios. • *Una vez revisada la bitácora se observó que la frecuencia de envíos de cintas a custodia externa fue superior a ocho (8) días, en algunos casos pasaron 20 días entre un envío y otro.* • *En lo que tiene que ver con la vigencia 2017, se observó que a la fecha (27 de abril) el proceso de adquisición de este servicio aún se encuentra en estudios previos.*
14	Riesgo de incumplimiento o incompatibilidad de la visión tecnológica de la entidad respecto al direccionamiento estratégico de la misma.	Verificar que las acciones propuestas en el Plan Estratégico de Tecnologías de la Información, se ajusten al marco estratégico de referencia, así como comprobar el grado de avance y el alcance de los objetivos propuestos.	• Existe un Plan Estratégico de TI publicado en la intranet con vigencia 2014 – 2017 que incluye, entre otros, el marco estratégico de referencia, la situación actual de TIC's de la entidad, la situación deseada a largo plazo, análisis de continuidad y riesgos. • *Con base en la Guía Técnica emitida por MinTIC's el 30 de marzo de 2016, en dónde se brindan lineamientos para estructurar un PETI, se observó que en lo que corresponde a la entidad, algunos contenidos no están incluidos o desarrollados con el grado de profundidad que ameritan.* • *No obstante los aspectos que el PETI incluye actualmente, no se observó contenido relacionado con gobierno de TI, análisis financiero, indicadores, riesgos, seguridad, etc., los cuales son de gran relevancia en un documento de este tipo.* • *No se observó evidencia de socialización de este documento con las demás áreas involucradas en el desarrollo y cumplimiento del mismo.*
15	Riesgo de adquirir servicios o productos innecesarios descuidando las prioridades misionales de la entidad.	Verificar que las actividades propuestas en el Plan de Adquisiciones, se ajusten a las necesidades de la entidad, así como su avance y cumplimiento en la ejecución.	• En el mes de enero se elabora un Plan de Adquisiciones inicial con base en el Proyecto de Inversión y las necesidades de los grupos internos del GIT de Informática, mensualmente se realizan actualizaciones según el avance en la ejecución, las liberaciones de saldos o aplazamientos del presupuesto. • Se observó seguimiento actualizado al proceso de adquisición de cada elemento adquirido, desde la elaboración de estudios previos hasta el control de pagos según las condiciones del contrato.
16	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios e infraestructura que informática soporta, por ausencia o desactualización del Plan de Contingencia.	Verificar que el Plan de Contingencia se encuentre actualizado e incluya guías de implementación para todas las líneas internas de trabajo que conforman el GIT de Apoyo Informático.	• *La última actualización del Plan de Contingencia del GIT de Apoyo Informático, así como de las guías de implementación, se realizó en diciembre de 2014.*

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
17	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios que la CGN presta, por ausencia o desactualización del Plan de Continuidad del Negocio.	Comprobar que en el GIT de Apoyo Informático están dadas las condiciones técnicas, para cumplir con lo que el Plan de Continuidad del Negocio (PCN) demanda, en lo que tiene que ver con infraestructura y administración de TI.	• En el mes de noviembre de 2014, el GIT de Apoyo Informático se comprometió a desarrollar cinco (5) estrategias para fortalecer el PCN, como son: *1. Definir un plan de contingencia completo, actualizado, revisado, probado y divulgado al interior del área. (Los resultados del numeral 16 de esta tabla confirman que esta estrategia no se cumple actualmente)* *2. Establecer el trabajo en pares para cada servicio y elemento que compone la plataforma de TI de la Contaduría General de la Nación. (Los resultados del numeral 16 de esta tabla confirman que esta estrategia no se cumple actualmente)* *3. Contar con un servicio de custodia externa para medios magnéticos, en los cuales estén almacenadas las copias de respaldo de la información de los equipos AIX, Windows y repositorio de datos. (Los resultados del numeral 13 de esta tabla confirman que esta estrategia no se cumple actualmente)* *4. Contar con soporte especializado para las aplicaciones proveídas por terceros, garantía extendida en hardware para los equipos de la plataforma y la proyección para la adquisición del servicio de centro de datos alterno son aspectos complementarios que apoyan la eficacia y eficiencia de este plan. (Los resultados del numeral 3 de esta tabla confirman que esta estrategia no se cumple actualmente)* *5. Definir, establecer y divulgar un flujograma de comunicaciones y directorio de responsables. (Los resultados del numeral 16 de esta tabla confirman que esta estrategia no se cumple actualmente)*
18	Riesgo de ataques cibernéticos por deficiencias en la detección y gestión de incidentes de seguridad.	Evidenciar que cada incidente de seguridad haya sido atendido, solucionado y documentado según el plan de acción mencionado en el procedimiento correspondiente.	• El 27 de febrero de 2017 se presentó un ataque en la modalidad de suplantación de identidad, el cual fue avisado, gestionado y documentado por el administrador del servicio. • Existe un grupo de seguridad al interior del GIT de Apoyo Informático que propende por el fortalecimiento de la cultura de la gestión de incidentes, para esto se han trabajado aspectos como: reporte de eventos veraces, documentación y seguimiento a través de Service Desk, creación de un diagrama de flujo detallado para la atención de incidentes y actualización del procedimiento de seguridad de la información. • Se adoptó la recomendación del Comité Sectorial de Tecnología liderado por el Ministerio de Hacienda, que sugiere reportar las incidencias de seguridad a los grupos de respuesta a emergencias con el fin de recibir ayuda y soporte según sea necesario. A continuación se citan algunos de ellos: - **ColCert** (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) - **CCP** (Centro Cibernético Policial) - **CSIRT** (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad).

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
19	Riesgo de no disponibilidad de los sistemas de información de la entidad por fallos o insuficiencia en los sistemas de almacenamiento.	Revisar que la arquitectura y configuración de los elementos de hardware y software en los diferentes ambientes, estén alineados con las mejores prácticas de administración.	• La plataforma misional cuenta con una SAN Hitachi AMS 2100 que tiene una capacidad efectiva de 19 TB, 4 TB disponibles y último mantenimiento preventivo en febrero de 2017. • Adicionalmente, la plataforma misional cuenta con una SAN Hitachi VSP G200, adquirida en 2016 con capacidad efectiva de 30 TB, la cual aún se encuentra en proceso de afinamiento y migración. • La plataforma de gestión implementa una SAN DELL SCV 2000 adquirida en 2016 con capacidad efectiva de almacenamiento DE 52 TB, 37 TB disponibles y último mantenimiento preventivo en enero de 2017. • Todos los sistemas de almacenamiento cuentan con sistemas RAID (Conjunto Redundante de Discos Independientes) que aumentan la disponibilidad y respaldo de la información que allí se almacena. • Se consultaron las interfaces de administración de las soluciones de almacenamiento sin encontrar errores o problemas que pusieran en riesgo el funcionamiento o disponibilidad de las mismas.
20	Riesgo de ataques cibernéticos por deficiencias en la gestión del UTM de la entidad.	Comprobar que el sistema de seguridad perimetral se encuentre actualizado y configurado para brindar la mayor protección contra amenazas posible. Revisar que las conexiones VPN no ponen en riesgo la seguridad de la información de la entidad.	• El firewall de la entidad es un FortiGate 310B configurado en alta disponibilidad (activo - activo) cuyo último mantenimiento se efectuó el 25 de julio de 2016. • El firewall cuenta con elementos UTM como son: antivirus, control de aplicaciones, IPS y filtrado web, los cuales fortalecen la seguridad perimetral de la red de la entidad. • El firewall cuenta con funciones como: administración de VPN's, administración de grupos de usuarios, log de eventos y notificación automática de amenazas, lo cual permite a los usuarios internos y externos, conectarse a la red de datos de forma segura. • El firewall instalado en el centro de datos de Medellín es un FortiGate 100D, éste cuenta con características UTM licenciadas hasta el 10 de octubre de 2020. • *El firewall FortiGate 310B de uso de la entidad en Bogotá, está próximo a dejar de ser respaldado por el fabricante, el 31 de diciembre de 2017, FORTINET, dejará de dar soporte y de producir actualizaciones para este equipo, lo cual genera potenciales riesgos de seguridad en la plataforma tecnológica de la entidad, en caso de no ser renovado.* • *El licenciamiento UTM del firewall, el cual brinda los servicios de antivirus, filtrado web, IPS y control de aplicaciones, caducan el próximo 9 de noviembre de 2017, lo cual genera potenciales riesgos de seguridad en la plataforma tecnológica de la entidad, en caso de no ser renovado.*
21	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten la sede de la entidad en la ciudad de Bogotá, por ausencia de un centro alterno de datos.	Comprobar la disponibilidad y seguridad del centro alterno de datos de Medellín, para el soporte de las aplicaciones misionales en sus ambientes productivos.	• El centro alterno de datos de la CGN se encuentra ubicado en el centro de datos de la alcaldía de Medellín ubicado en el edificio de la Alpujarra. • El centro de datos alterno de la CGN cuenta con un servidor físico IBM Power 740 con 160 MB de RAM, donde reposan los servicios CHIP del ambiente de producción. • Adicionalmente, consta de un firewall FortiGate 100D, dos (2) switches D-Link de 16 puertos, dos canales dedicados (MPLS - Multiprotocol Label Switching) activo-pasivo de 12 MB cada uno y una conexión a internet de 20 MB de ancho de banda. • En el mes de marzo de 2017 se realizó mantenimiento preventivo al servidor IBM Power 740 y al firewall FortiGate 100D.

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
			• La base de datos del sistema CHIP ubicada en el centro de datos de Bogotá, replica en tiempo real la información a la base de datos contingente del centro de datos de Medellín. • *No existe un sistema automatizado de monitoreo que garantice la disponibilidad de los servicios contingentes en caso de ser requeridos.* • *Existen componentes del sistema CHIP instalados en máquinas recibidas en comodato pertenecientes al Municipio de Medellín, dichos servidores podrían ser requeridos por su dueño en cualquier momento y la CGN no tendría capacidad de reemplazo inmediato.* • *En el mes de diciembre de 2016 se activaron los servicios contingentes de la ciudad de Medellín debido al traslado de los equipos desde el centro de datos de UNE de la calle 76, hacia el centro de datos de la CGN en Bogotá; pero no existen pruebas documentadas de la activación, operación y regreso a la normalidad de dichos servicios.* • *No se observaron reportes de gestión generados por el administrador del centro de datos alterno de Medellín, en donde se puedan verificar actividades de mantenimiento o índices de disponibilidad del servicio que presta.*
22	Riesgo de incumplimiento de acuerdos de niveles de servicio por eventos o situaciones que afecten la infraestructura de la entidad y no disponer de un data center en la misma ciudad para una inmediata recuperación.	Comprobar la disponibilidad y seguridad del centro de datos de la calle 76, para el soporte de las aplicaciones y equipos que allí reposen.	• La CGN contó con servicio de collocation en el centro de datos de UNE ubicado en la carrera 9 N° 75 – 49 desde diciembre de 2013 hasta diciembre de 2016. • La conectividad del centro de datos constaba de dos (2) canales de internet (activo – activo) de 24 MB cada uno y de un canal dedicado de 20 MB que conectaba el centro de datos de la entidad en Bogotá. • Los equipos llevados en collocation fueron los servidores misionales, la SAN misional, el robot de copias de respaldo y algunos equipos activos de red, los cuales fueron distribuidos en cuatro (4) racks y contaban con servicio de manos remotas. • Durante la vigencia 2016 se observó un (1) informe técnico de falla del 28 de marzo en donde se gestionaba un problema en las comunicaciones de internet el cual fue solucionado en un tiempo aproximado de 30 minutos. • *Se observó intercambio de correos electrónicos entre la CGN y UNE que prueban la gestión del servicio de collocation, pero no se observaron reportes generados por el administrador del centro de datos de UNE, en donde se puedan verificar actividades de mantenimiento o índices de disponibilidad del servicio prestado.*
23	Riesgo de incumplir con los estándares de atención al ciudadano por no contar con la adecuación tecnológica necesaria.	Evidenciar que el GIT de Apoyo Informático cuenta con la infraestructura tecnológica, para la actualización del servicio de atención al ciudadano en lo relacionado con: recepción, atención, solución y registro de requerimientos.	• El 15 de diciembre de 2016 se publicó en SIGI la primera versión del procedimiento PI-PRC24 “Servicio al Ciudadano”, el cual fue producto de un diagnóstico general que incluyó a todos los canales y todos los procedimientos que la CGN dispone para brindar el servicio de atención al ciudadano. • Adicionalmente, durante la vigencia 2016 se renovó el licenciamiento de la herramienta para la gestión de requerimientos “Service Desk” y se optimizó la plataforma tecnológica que dicha aplicación requiere incluyendo un ambiente de pruebas. • Desde el mes de febrero de 2017, el GIT de Apoyo Informático está generando estrategias de fortalecimiento de identidad del servicio de atención al ciudadano, a través del ícono VUSON (Ventanilla única de Servicios Online) publicado en la página web de la entidad.

N°	Riesgo a nivel de proceso	Enfoque de las pruebas	Resultados de las pruebas
			• Para la vigencia 2017, como se observó en los estudios previos, se tiene proyectado suscribir un contrato que garantice la implementación de las siguientes funcionalidades relacionadas con el gestor de requerimientos Service Desk: - Renovación de licenciamiento y actualización de versiones. - Integración entre el software de gestión de requerimientos y el gestor documental. - Habilitación de interfaces web para que los usuarios externos puedan registrar directamente sus propios requerimientos, obtener un número de ticket, hacerle seguimiento y evaluar la satisfacción del servicio prestado.

OBSERVACIÓN

Una vez efectuadas las pruebas encontramos las siguientes observaciones según el factor y un potencial riesgo específico:

N°	Factor	Riesgo a nivel de proceso	Observación
1	Soporte a Usuarios	Riesgo de insatisfacción de los usuarios.	• Las interfaces web para que los usuarios externos puedan registrar directamente sus propios requerimientos, obtener un número de ticket, hacerle seguimiento y evaluar la satisfacción del servicio prestado, aún no se han implementado.
2	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la plataforma misional.	• El ambiente CHIP que está en producción presenta debilidades en su componente llamado “Adm-Services”, puesto que se ha evidenciado, que es a causa de éste que se generan caídas en el servicio y por consiguiente reprocesos de envíos, especialmente en días de corte donde se genera la mayor demanda.
3	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la red de datos interna e Internet.	• Los equipos activos de la red de datos de la entidad se encuentran desactualizados, toda vez que ya no cuentan con: la garantía del fabricante, servicio de soporte o mantenimiento de terceros. • El switch de conexión de servidores misionales y de gestión se encuentra aproximadamente al 90 % de su capacidad y tampoco cuenta con garantía ni soporte. • Para la vigencia 2017, no se observó la inclusión del fortalecimiento de la infraestructura de la red de datos de la entidad en el Proyecto de Inversión.
5	Proyecto de Inversión	Riesgo de adoptar un enfoque tecnológico incompatible con las necesidades y misión de la entidad.	• Se observó, que además del fortalecimiento de los sistemas de información de la plataforma tecnológica, el proyecto de inversión incluye aspectos misionales que generan la necesidad de contar con servicios especializados que soporten la operación de la entidad, situación que requiere la revisión de los componentes del proyecto.
6	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de los ambientes web de la entidad.	• La versión de IBM Portal que la entidad tiene instalado en producción es la versión 7, la cual dejó de ser soportada por su fabricante desde el 31/12/2016. • La falta de un ambiente de pruebas y las limitaciones de la versión actual impiden el avance de proyectos como: la implementación de los ambientes web de CHIP en IBM Portal y la aplicación de herramientas que faciliten la consulta de estos contenidos a la población con discapacidad.

N°	Factor	Riesgo a nivel de proceso	Observación
10	Seguridad de la Información	Riesgo de incumplimiento de las metas GEL establecidas por Min TIC's y afectación del Índice de Transparencia Nacional (ITN).	• La aplicabilidad de los lineamientos MSPI en la entidad, presenta un porcentaje de cumplimiento inferior al 40%, debiendo ser éste a la fecha como mínimo 60%.
11	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la plataforma de gestión.	• Algunas aplicaciones críticas como: servidor de archivos (Pathfinder) y el antivirus ejecutan sistemas operativos obsoletos que ya nos son soportados por el fabricante.
13	Copias de seguridad	Riesgo de imposibilidad de recuperación ante pérdida de información misional sensible.	• A la fecha han pasado cinco (5) meses sin contar con el servicio de custodia externa, aunque este proceso no demanda mayor presupuesto ni complejidad en las especificaciones técnicas, aún se encuentra en la etapa de estudios previos, afectando así las estrategias de continuidad y contingencia de la entidad.
14	PETI	Riesgo de incumplimiento o incompatibilidad de la visión tecnológica de la entidad respecto al direccionamiento estratégico de la misma.	• Con base en la Guía Técnica emitida por MinTIC's el 30 de marzo de 2016, en dónde se brindan lineamientos para estructurar un PETI, se observó que en lo que corresponde a la entidad, algunos contenidos no están incluidos o desarrollados con el grado de profundidad que ameritan. • No obstante los aspectos que el PETI incluye actualmente, no se observó contenido relacionado con gobierno de TI, análisis financiero, indicadores, riesgos, seguridad, etc., los cuales son de gran relevancia en un documento de este tipo.
16	Plan de Contingencia	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios e infraestructura que informática soporta, por ausencia o desactualización del Plan de Contingencia.	• El Plan de Contingencia de la entidad se encuentra desactualizado, toda vez que el documento principal y las guías de implementación tienen fecha de diciembre de 2014.
17	Plan de Continuidad del Negocio	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten los servicios que la CGN presta, por ausencia o desactualización del Plan de Continuidad del Negocio (PCN).	• Las estrategias propuestas en 2014 para la implementación y fortalecimiento del PCN aún no han sido implementadas: *1. Definir un plan de contingencia, completo, actualizado, revisado, probado y divulgado…* *2. Establecer el trabajo en pares para cada servicio y elemento que compone la plataforma de TI …* *3. Contar con un servicio de custodia externa para medios magnéticos…* *4. Contar con soporte especializado para las aplicaciones proveídas por terceros …* 5. *Definir, establecer y divulgar un flujograma de comunicaciones…*
21	Contingencia y continuidad	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten la sede de la entidad en la ciudad de Bogotá, por ausencia de un centro alterno de datos.	• Según la auditoría CGR vigencia 2015 y OCI vigencia 2016 – 2017, aún existen componentes del sistema CHIP instalados en máquinas recibidas en comodato pertenecientes al Municipio de Medellín, dichos servidores podrían ser requeridos por su dueño en cualquier momento y la CGN no tendría capacidad de reemplazarlos inmediatamente.

RECOMENDACIÓN

Una vez efectuadas las pruebas encontramos las siguientes recomendaciones según el factor y riesgo específico:

N°	Factor	Riesgo a nivel de proceso	Recomendación
2	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la plataforma misional.	• Dar uso a los ambientes según su destinación inicial, toda vez que se observó que el ambiente de pre-producción es utilizado para que los usuarios estratégicos hagan parametrizaciones y que en el ambiente de capacitación se adelantan pruebas del proyecto “miles a pesos”.
3	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la red de datos interna e Internet.	• Adelantar acciones para que los principales equipos de la red (backbone) cuenten con garantía y soporte en caso de fallo. • Actualizar los equipos de red ubicados en los pisos superiores de la entidad (switches de borde), para contar con velocidades (10/100/1000) que garanticen el alto desempeño de la red de datos. • Actualizar los equipos de conexión inalámbrica de la entidad para atender de forma óptima la demanda de servicio que se genera en cada piso. • Adquirir equipos activos de red que faciliten la adopción de buenas prácticas como: redes virtuales (vlans) e IPv6. • Gestionar enlaces redundantes de conexión a internet con diferentes proveedores.
6	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de los ambientes web de la entidad.	• Crear un ambiente de IBM Portal para la ejecución de pruebas que permitan la posterior aplicación de actualizaciones o nuevas funcionalidades en producción.
7	Proyecto Dispositivos Móviles	Riesgo de fallo o no disponibilidad de la aplicación de la CGN para celulares.	• Validar la funcionalidad y amigabilidad de la aplicación toda vez que ha sido descargada 1659 veces pero solo 284 usuarios la mantienen en sus dispositivos móviles. • Actualizar el organigrama, la atención de PQRD’s y la política de privacidad.
9	Operación Centro de Cómputo	Riesgo de no disponibilidad de los sistemas de información de la entidad por fallos o insuficiencia eléctrica.	• Solicitar a quien corresponda, levantar el mapa del centro de cómputo y de los puestos de trabajo, que relacione el número de los puntos de corriente con conexiones y capacidades de los elementos que conforman la red eléctrica de la entidad.
11	Administración Plataforma TI	Riesgo de fallo o no disponibilidad de la plataforma de gestión.	• En cuanto a las copias de seguridad de la plataforma, se recomienda dar celeridad al proceso de implementación iniciado en 2016 que permite crear copias de respaldo de equipos virtualizados. • Programar y ejecutar pruebas de restauración que aseguren la funcionalidad y completitud de las copias de seguridad de la plataforma misional.

N°	Factor	Riesgo a nivel de proceso	Recomendación
12	Controlador de dominio	Riesgo de accesos restringidos o indebidos a servicios o aplicaciones por fallo o no disponibilidad del Controlador de Dominio.	• Asegurar que los servicios que presta el Controlador de Dominio se ejecuten sobre equipos que cuenten con garantía y soporte vigente por parte del fabricante. • Estudiar la viabilidad de instalar los servicios del Controlador de Dominio sobre la plataforma de virtualización que fue adquirida y actualizada recientemente.
13	Copias de seguridad	Riesgo de imposibilidad de recuperación ante pérdida de información misional sensible.	• Asegurar que la frecuencia de envío de la información sensible a custodia externa, se ajuste a las mejores prácticas y necesidades de la entidad, toda vez que se observó que en algunos casos pasaron hasta 20 días entre un envío y otro.
14	PETI	Riesgo de incumplimiento o incompatibilidad de la visión tecnológica de la entidad respecto al direccionamiento estratégico de la misma.	• Se recomienda actualizar y socializar este plan en toda la entidad, toda vez que el alcance del mismo es transversal y la consecución de las metas allí plantadas depende también de la participación de todos los procesos que componen el sistema de gestión de la entidad.
20	Seguridad perimetral	Riesgo de ataques cibernéticos por deficiencias en la gestión del UTM de la entidad.	• Iniciar el proceso de adquisición de un nuevo firewall con servicios UTM, el cual mantenga la configuración redundante y sea soportado por el fabricante por un período mínimo de cinco (5) años.
21	Contingencia y continuidad	Riesgo de imposibilidad de recuperación ante eventos o situaciones que afecten la sede de la entidad en la ciudad de Bogotá, por ausencia de un centro alterno de datos.	• Elaborar manuales o pruebas documentadas de la activación, operación y regreso a la normalidad de los servicios contingentes de la ciudad de Medellín.
23	Proyecto Atención al Ciudadano	Riesgo de incumplir con los estándares de atención al ciudadano por no contar con la adecuación tecnológica necesaria.	• Suscribir a la mayor brevedad un contrato que garantice la implementación de las siguientes funcionalidades relacionadas con el gestor de requerimientos Service Desk: - Renovación de licenciamiento. - Actualización de versiones. - Integración entre el software de gestión de requerimientos Service Desk y el gestor documental Orfeo a través de servicios web. - Habilitación de interfaces web para que los usuarios externos puedan registrar directamente sus propios requerimientos, obtener un número de ticket, hacerle seguimiento y evaluar la satisfacción del servicio prestado.