PLAN DE CONTINGENCIAS TECNOLOGIA DE LA INFORMACION PARA LA VIGENCIA 2025

CONTRALORÍA MUNICIPAL
BARRANCABERMEJA

DANNY MARCELA GOMEZ PUERTA
Contralora Municipal de Barrancabermeja

Barrancabermeja, Enero 2025

Tabla de Contenido

1. INTRODUCCION

Las Entidades del Estado, para asegurar el cumplimiento su misionalidad, se apoyan en los procesos de tecnología con el fin que los servicios brindados tanto a sus clientes internos como externos y demás partes interesadas, se den con la eficiencia que se requiere; así mismo, para que los productos que generan, con la oportunidad y calidad planificadas.

En tal sentido, uno de los aspectos de mayor importancia, es la salvaguarda de la información que se procesa y administra, por ello, se deben evitar riesgos de pérdida de información o riesgos de suspensión de servicios por fallas de cualquier índole. Es así como, el Plan de Contingencias de TI, se convierte en un mecanismo sustantivo para mantener en operación el conjunto de procesos, procedimientos, asegurar los recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro de TI; un plan de contingencia de TI, es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las Comunicaciones que tiene como fin, garantizar la continuidad de los servicios de TI.

El presente documento, establece roles y responsabilidades para la operación del Plan de contingencias de TI, muestra la identificación de los riesgos y los responsables de su administración, relaciona el inventario de activos de TI, sobre los cuales se deben realizar las actividades prioritarias en caso de presentarse un evento que pongan en riesgo la continuidad de la operación y de la prestación de los servicios de TI.

El plan aplica las actividades necesarias para mantener en operatividad los sistemas de información de la Contraloría Municipal de Barrancabermeja., para lo cual, establece los aspectos técnicos, humanos y de logística, que permitan afrontar cualquier contingencia.

De igual forma, el Plan de Contingencias de TI define un plan de pruebas a realizar con el objetivo de reducir la probabilidad de riesgos frente a un siniestro a un nivel aceptable, tanto para el hardware como del software y la adecuada recuperación de la información.

2. OBJETIVOS

Definir el conjunto de actividades, roles y responsabilidades que permitan el restablecimiento de la operación normal de la plataforma tecnológica de la entidad, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI, que pueda alterar el normal funcionamiento de los sistemas de información críticos y los servicios tecnológicos de la entidad.

Restablecer con la mayor brevedad posible el funcionamiento de la infraestructura tecnológica por ocurrencia de un evento, en aras de minimizar el impacto y garantizar la correcta recuperación de los sistemas y procesos de la entidad que involucren la Infraestructura de TI que se encuentren identificadas en el Análisis de impacto del negocio.

Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de TI, de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes, durante y después de la emergencia.

Definir actividades y procedimientos a ejecutar en caso de una interrupción de las operaciones de los sistemas y/o procesos que involucren la infraestructura de TI de la Contraloría Municipal de Barrancabermeja., a fin de garantizar la continuidad en la ejecución de las funciones y objetivos estratégicos de la entidad en el menor tiempo posible.

3. ALCANCE

El Plan de Contingencia de TI de la Contraloría Municipal de Barrancabermeja., descrito en este documento busca definir roles y responsabilidades, así como actividades para tomar control frente a situaciones que puedan afectar la continuidad de las operaciones que involucren infraestructura tecnológica identificada en el Análisis de Impacto, delimitado en la protección y funcionalidad mínima de los sistemas de información y servicios tecnológicos que soportan los procesos críticos de la entidad.

4. NORMATIVIDAD

A continuación, se relacionan las normas que regulan las actividades del plan de contingencias de TI de la Contraloría Municipal de Barrancabermeja.

- Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 de2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública

- Ley 594 de 2000, Ley General de Archivos

- Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

- Decreto 767de 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 2157 de 2017: Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012.

- Decreto 728 de 2017: Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

- Decreto 415 de 2016: Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

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

- Resolución 500 de 2001: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital

- CONPES 3854 – 2016: Política Nacional de Seguridad Digital.

- CONPES 3701-2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa Estrategia Nacional de Ciberseguridad y Ciberdefensa.

5. APROBACION Y ACTUALIZACION

El Plan de Contingencias de TI deberá ser aprobado en sesión de Comité de Gestión y Desempeño de la Contraloría Municipal de Barrancabermeja o quien haga sus veces y las actualizaciones a que haya lugar, serán aprobadas por las mismas instancias y se realizarán con una periodicidad de un año o cuando se requiera de acuerdo con las siguientes situaciones:

- ✓ Cambios en la infraestructura o aplicativos y/sistemas de TI.
- ✓ Resultados de análisis de riesgos que cambien los escenarios descritos para las contingencias de TI.
- ✓ Evaluación de los resultados de las pruebas al Plan de Contingencias de TI.
- ✓ Recomendaciones y/u oportunidades de mejora identificadas en auditorías u otro proceso de revisión y mejora.

6. COMUNICACIÓN Y DISTRIBUCION DEL PLAN

A continuación, se presentan algunas pautas para la comunicación y distribución del plan y sus componentes.

- ➢ Boletines internos de comunicación a fin de establecer conciencia sobre la importancia del tema.

- Charlas y talleres. Incluir el tema del manejo de contingencias de TI dentro de la estrategia de sensibilización del Plan de Seguridad y Privacidad de la Información.
- Comunicación de la Alta Dirección. Como líderes de la entidad y del proceso de Contingencia de TI, la alta dirección debe, al menos una vez al año, comunicar a los funcionarios su compromiso de salvaguardar la información y el plan de contingencias de la entidad, para lo cual utilizará cualquier medio de los mencionados anteriormente.
- Publicación de información de manera continua y accesible. En la Pagina Web de la Contraloría Municipal de Barrancabermeja

Es importante, contar con el plan de contingencias de TI y los procedimientos que hacen parte de este, disponibles en un lugar seguro fuera de las instalaciones de la sede principal, con el objeto de que en una interrupción total garantizar el acceso a estos documentos y su distribución efectiva a los diferentes equipos que participan en la recuperación de los servicios de TI.

7. ROLES Y RESPONSAILIDADES DENTRO DEL PLAN DE CONTINGENCIAS DE TI

Para el manejo de la activación del Plan de Contingencia de TI en alguno de sus escenarios, es importante destacar que los procesos de Talento Humano y Gestión financiera son quienes en primera instancia deberán establecer los protocolos de comunicación primarios con la empresa de Seguridad y Vigilancia a fin de establecer los canales de comunicación al interior de la entidad en caso de presentarse alguna contingencia como la caída del fluido eléctrico, inundación, sismo, o en el evento de la programación o ejecución de actividades de mantenimiento que afecten el fluido eléctrico de la entidad, en días laborales y no laborales y/o cuando se encuentren o no servidores en las sedes de la entidad.

Seguidamente y dependiendo la criticidad de la situación de contingencia, el proceso de Planeación Estratégica por medio de la Oficina de Talento Humano, serán los encargados de difundir las comunicaciones oficiales tanto internas o externas (si los servicios afectados involucran servicios a la ciudadanía o los sujetos de control), donde se indiquen las acciones y/o noticias frente a los temas que están afectando el servicio o el restablecimiento de los mismos.

De igual manera, se deberá priorizar la comunicación entre los procesos de Gestión Financiera y Talento Humano en cuanto la organización y requerimientos de logística.

Por su parte el encargado de las Tecnologías de la Información y las Comunicaciones procederá a poner en marcha los protocolos de atención a la contingencia de acuerdo al escenario materializado.

De otra parte, es fundamental el compromiso de los servidores públicos de la entidad, especialmente de la alta Dirección, Talento Humano y Tecnologías de la Información y las Comunicaciones, debido a que son ellos quienes tienen la responsabilidad de comunicar y gestionar de forma adecuada el incidente tecnológico (prevención, mitigación, preparación, alertas, respuestas, rehabilitación y/o reconstrucción), que afecte la operación normal de la entidad, desde el momento que se declare la interrupción hasta la vuelta a la normalidad, buscando siempre reducir al mínimo el impacto sobre la prestación del servicio.

A continuación, se definen tres niveles de gestión (estratégico, táctico y operativo) y sus responsabilidades durante una situación de contingencia de TI, organización que permite segregar funciones y roles para que las tareas y procesos responsables no presenten conflicto alguno; en cada nivel se debe establecer un plan de sucesión para que en caso de no estar disponible el servidor público principal, pueda su reemplazo actuar con la misma autoridad y responsabilidad.

Nivel Estratégico: A este nivel corresponde la planeación del logro de los objetivos del Plan de Contingencias de TI, se basa en decidir y asignar las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción tecnológica no planeada en la entidad.

Nivel Táctico: Llevará a cabo la coordinación de las actividades que se deriven del Plan de Contingencias de TI, así como la evaluación de las situaciones de interrupción y dará lineamientos para la operación de mismos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación de TI y brindará los insumos para la evaluación.

Nivel Operativo: Este nivel realiza las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el Plan de Contingencias de TI de la entidad. Se ejecuta a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

8. MODELO DE GESTION DE TI

A continuación, se describe el modelo de gestión de TI de la Contraloría Municipal de Barrancabermeja desde la perspectiva de la Arquitectura empresarial.

8.1. Sistemas de Información

Actualmente, los procesos se apoyan en sistemas de información adquiridos a terceros por compra, diseñados a la medida, como de otras entidades estatales los cuales la Contraloría Municipal de Barrancabermeja los usa de acuerdo a su dinámica funcional.

Así mismo, la entidad cuenta con contratos de soporte y mantenimiento especialmente para los sistemas misionales y para los demás el soporte es brindado directamente con funcionarios del área TI.

A continuación, se presenta la descripción de cada uno de los sistemas de información con que cuenta la entidad.

Tabla 1. Sistemas de Información de la Contraloría Municipal de Barrancabermeja

ID	Proceso	Categoría	Sistema de Información	Fortalezas	Oportunidades de Mejora
01	Participación Ciudadana	Estratégico	Sistema de Información de Atención al Ciudadano - SIAC	➢ Interacción con la ciudadanía. ➢ Radicación de PQRSD y certificaciones en línea. ➢ Seguimiento a la solicitud en línea. ➢ Respuesta en línea y Digital	Divulgación y campañas de capacitación sobre el uso y manejo de la interfaz por parte de la ciudadanía
02	Gestión Financiera	Apoyo	Sistema de Información	➢ Almacenamiento en la Nube.	

			Financiera – Delfín (Contabilidad, Presupuesto, Nomina e Inventarios)	➢ Backup y Soporte por parte del Desarrollador y contratista. ➢ Ambiente Web	
03	Talento Humano	Estratégico	Servidor DNS y Directorio Activo – ThinkServer Lenovo TS150	➢ Almacenamiento local y Facilidad de Amplitud. ➢ Carpetas por Proceso con niveles de seguridad de acceso y carpetas compartidas	Conexión Física para todas las terminales (Cable e Red Par Trenzado UTP, Categoría 6)

Fuente: Elaboración Propia

8.2 Servicios Tecnológicos

Los servicios tecnológicos que brinda la Dirección de TIC, están diseñados para mantener un correcto funcionamiento de la plataforma tecnológica de la entidad. Así mismo, al no depender del contexto en el cual se estén usando, se garantiza que se pueden usar por varios procesos de operación y otros servicios o incluso otros usuarios, tanto internos como externos, lo que permite brindar una respuesta oportuna a las diferentes eventualidades que en materia de tecnologías de la información puedan afectar el funcionamiento apropiado de la red de datos, equipos tecnológicos, red comunicaciones, entre otros servicios asociados.

A continuación, se describen los principales servicios que brinda el proceso de Gestión de Gestión de Tecnologías de la Información y las Comunicaciones.

Tabla 2. Descripción de Servicios Tecnológicos de la Contraloría Municipal de Barrancabermeja

Servicio	Descripción	Alcance y Funcionalidad	Importancia
Impresión y Digitalización	Permitir la impresión controlada y escaneo de los documentos producidos por los funcionarios de la Contraloría Municipal de Barrancabermeja, como resultado de sus funciones, teniendo en cuenta la estrategia de "cero papel" de la Contraloría Municipal de Barrancabermeja.	Este servicio va dirigido a todos los usuarios de la Contraloría Municipal de Barrancabermeja	Por la cobertura dentro de la entidad y complejidad que maneja en las dependencias y procesos se cataloga como ALTO.
Conectividad Wi-Fi	Brindar Conectividad Inalámbrica a los grupos auditores y en general a todos los funcionarios que por su contexto laboral requieren un despliegue constante por las diferentes áreas y dependencias de la Contraloría Municipal de Barrancabermeja, facilitando el trabajo y el uso de equipos	Servicio en la Sede de la Contraloría Municipal de Barrancabermeja, para equipos de computo y otros dispositivos de los funcionarios de la entidad. Para aquellas personas que se vinculan en Prestación de Servicios y que actualmente no cuentan con equipos	El servicio de conectividad inalámbrica para la Contraloría Municipal de Barrancabermeja, ha sido una herramienta que se ha vuelto indispensable en la labor que desarrolla la mayoría de funcionarios que no permanecen dentro de la Sede Principal pero que cuentan

	portátiles y PCs asignados por el área de almacén e Inventarios y demás dispositivos tecnológicos que requieran conectividad.	de escritorio y/o ALL IN ONE como los que actualmente cuenta la Contraloría Municipal de Barrancabermeja y para los que se les suministra equipos portátiles para la realización de sus actividades.	con equipos que permiten acceder a este servicio como lo son los equipos portátiles, Celulares y Ultrabooks, para la realización de funciones de las áreas que constantemente se despliegan dentro de la Sede Principal en búsqueda de información, actualización y solución de diferentes temáticas que por su naturalidad requieren un accedo a red constante.
Equipos de Computo	Garantizar el funcionamiento de los equipos de cómputo que los funcionarios usan para el desarrollo de sus funciones. Incluye mantenimiento Preventivo y correctivo.	Este servicio de soporte va dirigido a todos los Equipos de Cómputo de la Contraloría Municipal de Barrancabermeja	Funcionalidad física y de software del Sistema Operativo y demás aplicaciones instaladas en los Equipos de cómputo de la Contraloría Municipal de Barrancabermeja
Gestión de Herramientas de Ofimática	Brindar el Soporte Técnico sobre el funcionamiento de	Este servicio de soporte va dirigido a todos los Equipos de	Funcionalidad Herramientas informáticas y

	las herramientas de ofimática para optimizar, automatizar y mejorar las actividades de oficina.	Cómputo de la Contraloría Municipal de Barrancabermeja	demás aplicaciones instaladas en los Equipos de cómputo de la Contraloría Municipal de Barrancabermeja.
Gestión de Préstamo de Equipos Portátiles y Recursos Audiovisuales	Gestión de adquisición, instalación y/o préstamos de equipos portátiles y equipos audiovisuales como apoyo a las actividades de las dependencias que requieren su uso en casos ce capacitaciones, socializaciones y de mas actividades que lo requieran.	Este servicio de soporte va dirigido a la configuración de equipos de audio y video en las actividades que así lo requieran de la Contraloría Municipal de Barrancabermeja	Funcionalidad Herramientas informáticas y demás aplicaciones instaladas en los Equipos de cómputo de la Contraloría Municipal de Barrancabermeja
Correo Electrónico	Se refiere a los servicios asociados a la cuenta de correo electrónico, tales como creación y configuración de cuentas de correo, restauración de buzones y sincronización, Programación de correos futuros, creación,	Este servicio de soporte va dirigido a la creación y configuración de usuarios que estén previamente aprobados por la dirección de Talento Humano	El Servicio de Correo electrónico se brinda para los funcionarios de Carrera, Provisionales y para algunos Contratistas que trabajan en la Contraloría Municipal de Barrancabermeja

	modificación y eliminación de listas de distribución, compartir contactos y calendario.		
Almacenamiento en la Nube	Se refiere al almacenamiento en la nube de hasta 1 TB, por cuenta de correo asociada, actualmente conocida como Google Drive	Este servicio sirve para el almacenamiento de información en la nube para funcionarios con cuenta de correo electrónico de la entidad a la cual pueden acceder desde cualquier lugar con conexión a internet	El servicio de almacenamiento en la nube se brinda a funcionarios con cuenta de correo electrónico de la entidad y es un servicio de almacenamiento alterno y moderno de gran demanda y usabilidad empresarial y comercial.
Servidores	Hace referencia a la Administración, configuración y disponibilidad de los servidores de la Contraloría Municipal de Barrancabermeja	Este servicio de soporte va dirigido los servidores que están en el Data center, el cual está ubicado en el tercer piso de la Oficina de la Contraloría Municipal de Barrancabermeja en el Estadio Daniel Villa Zapata, Tribuna Nor-Oriental y Servidor Web de la Pagina Institucional	Dirigido para la continuidad y administración de las aplicaciones que están instaladas en estos Servidores de la Contraloría Municipal de Barrancabermeja
Bases de Datos	Proporcionar a los usuarios finales la	Este servicio de soporte va dirigido a	Servicio de las Bases de Datos es

	facilidad de almacenar, organizar y consultar información organizada con características afines entre sí, para ser utilizada por una o más aplicaciones de la manera más eficiente.	las Bases de Datos de los diferentes procesos de la Contraloría Municipal de Barrancabermeja.	la que da la continuidad y el funcionamiento de las Aplicaciones Misionales que tiene la Contraloría Municipal de Barrancabermeja
Almacenamiento	Servicio que comprende la asignación de espacio de almacenamiento virtual por parte del funcionario designado por la Dirección de TIC para cada dependencia, continua con la estructuración de la información, la realización exitosa de las copias y termina con la restauración de la información que se requiera por solicitud de los usuarios.	Dirigido a las copias de respaldo que soliciten los usuarios sobre archivos o aplicaciones que se necesiten como respaldo para los diferentes procesos que manejan en las diferentes dependencias de la Contraloría Municipal de Barrancabermeja	Permite el almacenamiento de archivos o aplicaciones para tener duplicidad de la información según sea solicitada por seguridad de la información
Seguridad Perimetral	Actividades orientadas a garantizar la confidencialidad,	La seguridad Informática de la entidad se basa en el Subsistema de	Por medio de este servicio se controla y garantiza el servicio de Internet, y el

	integridad y disponibilidad de la información y la plataforma tecnológica de la Entidad y sus servicios asociados.	Gestión de Seguridad de la Información, la administración del equipo de seguridad perimetral firewall y Políticas del Directorio activo. Se complementa con protección de equipos con software antivirus y en el caso requerido la encriptación de información.	óptimo funcionamiento de las aplicaciones WEB que tiene la entidad. Se protegen los equipos de cómputo contra la presencia de software malicioso que pretenda daño o robo de información.
Portal Web	Servicios asociados con los sitios WEB desarrollados y mantenidos por la Contraloría con el propósito de divulgar información y ofrecer servicios de interés general para los colaboradores de la entidad o para los públicos externos.	Está constituido por la página Web e intranet donde se ofrecen los diferentes servicios para usuarios internos y externos de la entidad.	Por medio de este servicio se realizan publicaciones de las diferentes tareas, informes, información, cumplimiento normativo, servicios y actividades que se realizan en la Contraloría Municipal de Barrancabermeja
Internet	Brindar conectividad segura y confiable para el envío y recepción de información (voz, datos, videos e	El servicio es utilizado por la Sede Principal y Única de la Contraloría Municipal de Barrancabermeja	Este servicio es importante para la funcionalidad de las aplicaciones Web, correo electrónico y demás actividades

	imágenes entre otros).		que realiza la Contraloría con otras entidades y el funcionamiento de sus actividades en general.
Gestión de Usuarios	Servicio para la asignación o modificación de perfil, asignación de credenciales de ingreso a los diferentes servicios de red y aplicaciones para los funcionarios de la Contraloría Municipal de Barrancabermeja.	El servicio hace referencia a las solicitudes que realizan los funcionarios para la asignación de usuarios o accesos a las aplicaciones y/o equipos tecnológicos que tiene la Entidad.	Es importante para que los funcionarios puedan ingresar a las aplicaciones y realizar las diferentes actividades que se realizan en la Entidad.
Copias de Respaldo	Servicio que incluye tecnologías que permiten configurar y administrar los servidores de copia de respaldo de la información, teniendo en cuenta el Plan de Seguridad y Aseguramiento de la Información 2025.	El servicio busca respaldar la información que se considera crítica y mantener su disponibilidad en el momento requerido. Se respalda la información contenida en las carpetas de trabajo de los funcionarios y procesos de la entidad, de la pagina web institucional y las audiencias del área de Responsabilidad	Mantener respaldo de la información considerada como crítica en la entidad y que se encuentra almacenada en las bases de datos de los sistemas de información misionales y de los archivos alojadas en los servidores y equipos de computo de la Contraloría Municipal de Barrancabermeja.

		fiscal y Jurisdicción coactiva.	
Conexión VPN	Servicio de Conexión a un servicio o equipo interno de la red LAN de la entidad mediante el establecimiento de una conexión cifrada de la información a través SSL desde redes externas a la red LAN institucional	Servicio de acceso seguro mediante protocolo SSL a un equipo de la red LAN de la entidad. El servicio está disponible para funcionarios o terceros que lo requieran con el fin de realizar algún soporte a aplicativos o equipos del centro de datos.	Permitir el acceso seguro a un equipo de cómputo o servicio interno de la red LAN de la entidad desde un equipo remoto que se encuentra fuera de la red de cómputo institucional.
Video Conferencia	Servicio que consiste en facilitar y disponer al usuario una herramienta de comunicación en tiempo real (audio y video) para la realización de reuniones, comités etc. en forma virtual y remota.	El Servicio de Video conferencia abarca la disposición y asesoría en el uso de la herramienta.	Permitir a los usuarios de la Contraloría Municipal de Barrancabermeja, realizar reuniones de trabajo de manera virtual y remota mediante herramientas de video conferencia.
Chat y foro	Servicio de gestión técnica de los módulos de CHAT y FORO dispuestos en la cuenta de correo electrónico institucional, para la participación ciudadana y de	Los módulos de CHAT y FORO son de uso de las dependencias que requieran realizar actividades de participación al interior de la entidad o al exterior con la	Prestar servicio de gestión técnica a los módulos de chat y foro dispuestos en las cuentas de correo institucional

	funcionarios en actividades que programen las diferentes dependencias de la entidad, como medio de comunicación y realización de eventos.	ciudadanía en general.	
Software de Protección de Antivirus	Servicio de protección antivirus a equipos de cómputo de la entidad que detecta y elimina virus informáticos y muchos otros tipos de amenazas informáticas.	La protección antivirus se garantiza a nivel local en los equipos de cómputo y equipos servidores de la entidad.	Garantizar los pilares de la Seguridad, como son: la confidencialidad, integridad y disponibilidad de la información y de la plataforma tecnológica de la Contraloría Municipal de Barrancabermeja a los equipos de cómputo de la entidad en uso de los funcionarios.
Mesa de Trabajo o ayuda – soporte a usuarios	Servicio para el registro de incidencias, solicitudes de servicio, de soporte y gestión de incidentes y requerimientos de servicios de TI para los usuarios de la	La Mesa de Servicio es el punto único de contacto entre el proveedor de servicios y usuarios, para el registro, gestión de incidentes y requerimientos de servicio, bajo los parámetros de	Prestar servicio de gestión de procesos, solución de requerimientos de soporte, atención de incidentes de manera integral en el área de TIC, para los usuarios de la Contraloría

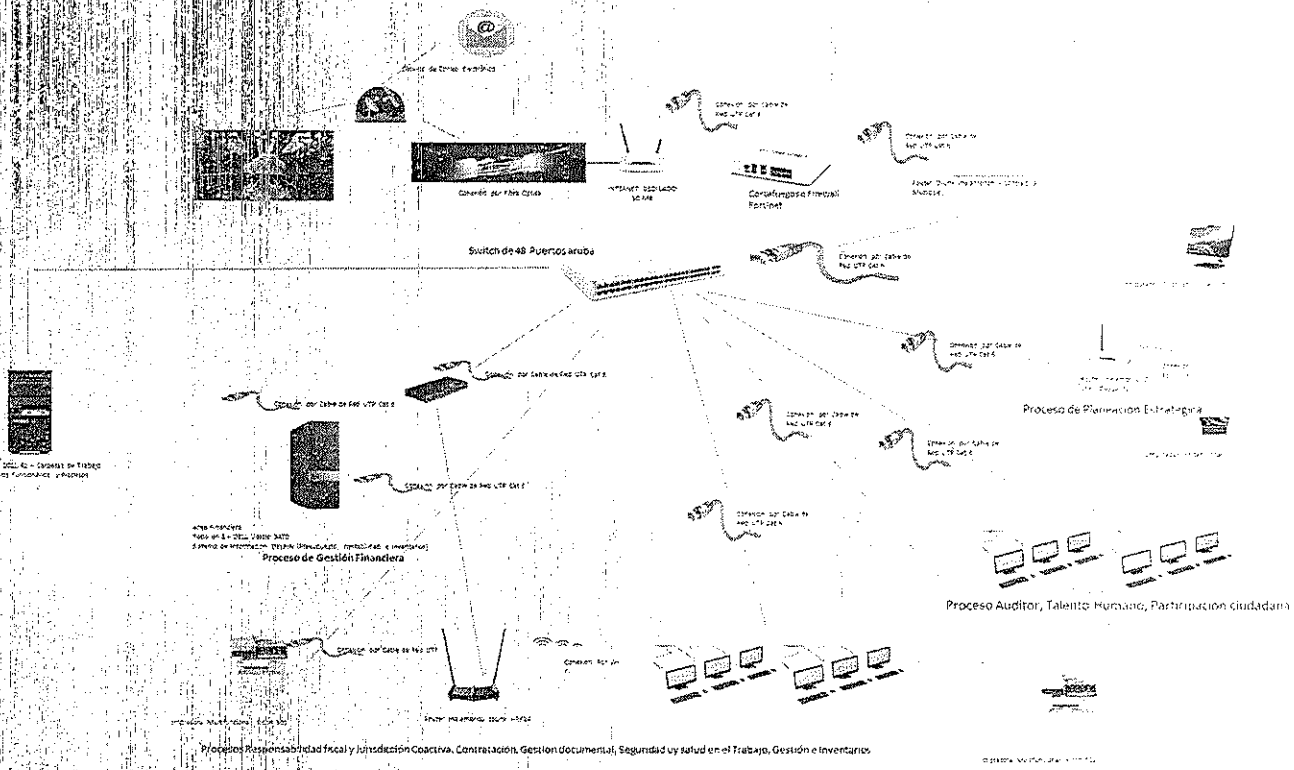
	Contraloría Municipal de Barrancabermeja.	tiempo de respuesta acordados en los niveles de servicio, con el fin de restaurar y optimizar el servicio con un mínimo de impacto en la operación de la Entidad.	Municipal de Barrancabermeja

Fuente: Elaboración Propia

8.3 Infraestructura Tecnológica

Para soportar los servicios tecnológicos que se entregan a los Procesos de la Contraloría Municipal de Barrancabermeja, se tiene establecida una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos.

Figura 2. Topología de Red de la Contraloría Municipal de Barrancabermeja 2025



Fuente: Elaboración Propia

9. Identificación de Riesgos

Para el Plan de Contingencias de TI de la Contraloría Municipal de Barrancabermeja, se tienen en cuenta los siguientes riesgos.

Tabla 3. Riesgos del Proceso de Gestión de Tecnologías de la Información

Riesgos	Causas	Controles
Posibilidad de afectación reputacional por pérdida de integridad y/o confidencialidad y/o disponibilidad de la información almacenada en las bases de datos de los sistemas de información y aplicaciones que se encuentran en producción y con acceso por direccionamiento público, debido a ataques informáticos.	Ataques informáticos	La infraestructura de seguridad compuesta por antivirus y el firewall, detectan y controlan los ataques informáticos presentados sobre los recursos de TI disponibles en la Entidad.
Posibilidad de afectación económica y reputacional por interrupciones no planificadas de la infraestructura tecnológica en la prestación de servicios de TI, debido a la ausencia de planes de continuidad.	Ausencia de planes de continuidad	Los profesionales con rol de administración de la infraestructura, verifican que se actualice y se realicen las pruebas al Plan de Contingencias.
Posibilidad que los servidores de aplicaciones y de bases de datos en producción, infraestructura virtual y conjunto de discos (SAN) no se encuentren disponibles.	Mantenimiento insuficiente	El equipo técnico de la Dirección de TIC monitorea periódicamente la infraestructura del Data Center, para determinar alertas y necesidades de recursos de TI, que garanticen la disponibilidad de los servicios.
Posibilidad de afectación reputacional por el	Falta de asignación y/o disminución de los recursos	El equipo de la Dirección de TIC verifica que las

Incumplimiento en el desarrollo de las estrategias de Tecnologías de Información y las Comunicaciones, debido a la falta de asignación y/o disminución de los recursos presupuestales, que afecte la ejecución de los proyectos de tecnología.	presupuestales asignados para la gestión de TI.	necesidades de TI a presentar, correspondan a un diagnóstico de requerimientos de bienes y servicios, para garantizar el óptimo funcionamiento de la plataforma tecnológica que apoye la misionalidad de la Entidad.
Posibilidad de extracción o alteración de información de los aplicativos DELFIN, SIAC Y Carpetas Compartidas con fines de beneficio personal o hacia un particular, debido a debilidades en la aplicación de controles a las modificaciones de información	Debilidades en la aplicación de controles a las transacciones de modificación de datos de los aplicativos DELFIN, SIAC Y Carpetas Compartidas.	Aplicación del procedimiento de control de acceso y aplicación de las políticas de seguridad de la información. Revisión periódica de la seguridad lógica de acceso a los sistemas DELFIN, SIAC Y Carpetas Compartidas.

Fuente: Elaboración Propia

10. Clasificación de Interrupciones y Nivel de Afectación a los servicios de TI.

La activación o no del plan de Contingencias de TI de la Contraloría Municipal de Barrancabermeja, dependerá del resultado de la ejecución del procedimiento de Gestión de Incidentes de Seguridad y/o las decisiones tomadas por los niveles Estratégico y Táctico descritos en este Plan, frente a la situación que genere la interrupción del servicio tecnológico.

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia de TI son evaluados de acuerdo con el impacto que tienen sobre la prestación del servicio tecnológico de la Contraloría Municipal de Barrancabermeja, de acuerdo con la siguiente clasificación:

Tabla 4. Clasificación de la Interrupción

Tipo de Interrupción	Características	Ejemplos
TOTAL	Evento que inhabilita el centro de datos para prestar sus servicios. No permite que el equipo de tecnología siga laborando en las instalaciones de la empresa.	Terremotos. Incendio general. Orden Público. Fallo eléctrico en el sector.
PARCIAL	Evento que afecta a más de un recurso informático de manera drástica ocasionando la suspensión parcial del funcionamiento del hardware o software considerados como críticos.	Fallas técnicas en equipos servidores que alojan más de un aplicativo, bases de datos.
ESPECIFICA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática.	Fallas técnicas de un equipo que aloja un sistema o servicio. Ausencia de personal clave.

La evaluación de la afectación de los servicios de TI se definió con base en el impacto que puede generar la materialización de alguno de los riesgos identificados en el proceso de Gestión de Tecnologías de la Información en el desarrollo de las actividades propias de cada proceso, de la siguiente manera:

Tabla 5. Niveles de afectación de los servicios de TI.

Recurso Afectado	Nivel de Afectación
Servidores	3
Computadores	2
Sistemas de Información y/o aplicativos	3
Servicio de Internet	3
Correo Electrónico	3
Página Web	2

Red de datos	3
Impresoras y escáneres	2
Corriente eléctrica	3

11. Aspectos Generales para la atención de una Contingencia

El Plan de Contingencias de TI, se activa frente a una situación de interrupción de un servicio y/o infraestructura de TI o de acuerdo con lo determinado por el procedimiento de Gestión de Incidentes de Seguridad y/o lo que exprese el nivel estratégico o táctico del plan de contingencias de TI.

A continuación, se presentan las actividades generales que se deben tener en cuenta por los roles definidos dentro del plan, para la atención de una situación de contingencia de TI.

Tabla 6. Actividades y responsables para el manejo de contingencias de TI en la Contraloría Municipal de Barrancabermeja

Actividad	Responsable	Acción
1	Funcionarios Públicos de la Contraloría Municipal de Barrancabermeja.	Reportar la falla en el sistema de mesa de servicios o ayuda que tenga dispuesta la entidad siguiendo el procedimiento de Atención de requerimientos de soporte a los sistemas de información y equipos informáticos.
2	Responsable del Sistema de Mesa de Servicios o ayuda del área de TI. Profesional Especializado, Profesional Universitario o Técnico	✓ Analiza la falla. En caso de corresponder a un incidente de seguridad, inicia el procedimiento de Gestión de Incidentes de seguridad. ✓ Evalúa y determina si el incidente corresponde a una contingencia. En este caso informa al responsable del Plan de contingencias de TI.

		✓ Si la situación no es un incidente de seguridad, pero afecta la operación de algún servicio de TI, inicia el procedimiento correspondiente.
3	Responsable de Tecnologías de la Información y las Comunicaciones y Administradores de Infraestructura y Aplicaciones Equipos de apoyo de acuerdo con la especialidad	✓ Autoriza la puesta en marcha del Plan de Contingencia de TI, notificando a las áreas afectadas y a los niveles estratégico y táctico del Plan de Contingencias de TI. ✓ Ejecuta las actividades de recuperación junto con el equipo de atención e informa al Gestor del Plan de Contingencias de TI (según lo descrito en el escenario de contingencia a solucionar). ✓ Realiza pruebas de recuperación del servicio y/o infraestructura afectada y reporta al Gestor del Plan de Contingencias la finalización de las actividades implementadas. ✓ Inicia las acciones pertinentes para el restablecimiento del proceso normal (según lo descrito en el escenario de contingencia a solucionar). ✓ Actualiza Hoja de vida del equipo, servidor o del sistema de información sobre la incidencia presentada. ✓ Realizar análisis de las fallas presentadas y de los indicadores del proceso. ✓ Documenta los resultados y lecciones aprendidas. ✓ Autoriza la finalización del plan.

	✓ Informa a las áreas afectadas la normalización en la prestación de los servicios de TI. ✓ Autoriza el cierre de la contingencia e informa al Comité o a la Alta Dirección, el balance de la situación de contingencia.

11.1. Sistemas de Información y aplicaciones

- Realizar inventario de los Sistemas de Información y/o Aplicativos afectados de acuerdo con las características relacionadas en el documento Plan de Contingencias de TI.
- Preparar y configurar un equipo de cómputo de acuerdo con las características y condiciones de conectividad especificadas relacionadas en el documento Plan de Contingencias de TI del Sistema de Información y/o Aplicación afectado.
- Restaurar copia de seguridad de la base de datos correspondiente, así como la copia de respaldo más reciente del código fuente o del archivo de instalación o ejecutable.
- Revisar permisos de acceso y cuentas de usuario del sistema de información afectado.
- Verificar la conexión entre la base de datos y el sistema y/o aplicativo.
- Realizar pruebas de procesamiento y transaccionalidad de datos entre los sistemas y/o aplicativos en el equipo dispuesto para la atención de la contingencia.
- Paralelo a estas actividades, en el sistema afectado, se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencias de TI.
- En caso de que la contingencia se presente en un servicio, sistema de información y/o aplicativo que cuente con un soporte técnico y/o garantía, se debe informar al contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio

establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

11.2. Recursos Tecnológicos e Infraestructura

- Realizar inventario físico de la infraestructura afectada de acuerdo con las características relacionadas en el documento Plan de Contingencias de TI.
- Determinar las características técnicas de la infraestructura física afectada.
- Con la infraestructura no afectada y dependiendo la situación presentada, realizar las actividades planteadas en los diferentes escenarios para atender la contingencia y restaurar el servicio de TI afectado.
- Verificar las conexiones entre servicios de TI y la infraestructura dispuesta para la atención de la contingencia.
- Realizar pruebas de transaccionalidad de datos y/o conexiones en el equipo dispuesto para la atención de la contingencia.
- Paralelo a estas actividades, en la infraestructura afectada se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencias de TI.
- En caso de que la contingencia se presente en infraestructura que cuente con un soporte técnico y/o garantía, se debe informar al contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

11.3. Recurso Humano

Profesional Universitario y/o especializado del área TIC, y Jefes de Proceso o funcionario encargado según el proceso o recurso afectado

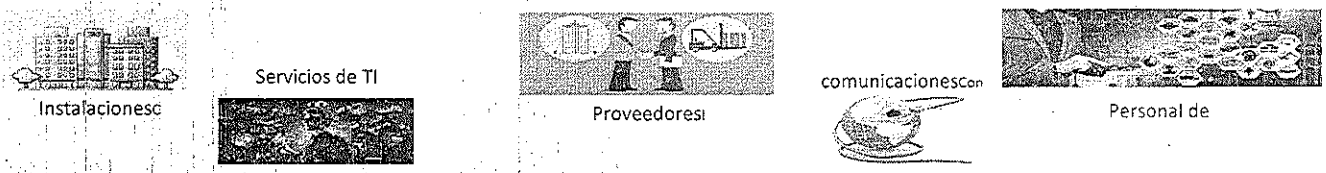
11.4. Aspectos Logísticos

Cuando ocurra una situación inesperada que conlleve a la materialización de un riesgo identificado en este Plan de Contingencia de TI, el funcionario afectado o los funcionarios afectados deberán reportarlo de inmediato a través de la mesa de servicios o ayuda que tenga dispuesta la entidad o comunicándose directamente con el área TIC o a los correos electrónicos sistemas@contraloriabarrancabermeja.gov.co y talento.humano@contraloriabarrancabermeja.gov.co. Una vez reportada la contingencia se activará por parte del área de TIC, el respectivo procedimiento para el manejo de la interrupción.

11.5. Escenarios de Contingencia

De las actividades generales a ejecutar en una contingencia, las responsabilidades y tareas de los roles que intervienen en el Plan de Contingencias de TI y los riesgos identificados para el proceso de Gestión de Tecnologías de la Información, surgen de escenarios que el área de Tecnologías de la Información y las Comunicaciones identificó para la atención y tratamiento; escenarios en los cuales los recursos tecnológicos, personas, proveedores e infraestructura se pueden ver afectados por una situación que causa interrupción total o parcial y que afectan el normal funcionamiento de los servicios de TI que soportan los procesos de la entidad.

Figura 3. Escenarios de contingencias de TI



12. Estrategias de pruebas del Plan de contingencias de TI

Las estrategias de recuperación que se describen a continuación definen los planes de la entidad para responder a un incidente y detallan cómo debe responder el proceso e

Gestión de TI. Al determinar estas estrategias de recuperación, se debe tener en cuenta que se deben considerar aspectos tales como:

- ✓ Presupuesto
- ✓ Cobertura del seguro
- ✓ Recursos — personas e instalaciones físicas
- ✓ Posición de la alta dirección sobre los riesgos
- ✓ Tecnología
- ✓ Datos
- ✓ Proveedores
- ✓ Requisitos de conformidad

En esta sección se definen los aspectos básicos que requieren ser probados periódicamente, a fin de medir el comportamiento integral e individual de los recursos asignados y/o los procedimientos definidos para la atención de una interrupción de un servicio de TI.

12.1. Tipos y frecuencia de pruebas

La programación de las pruebas obedece a varios factores entre los cuales se pueden mencionar:

- ✓ Programación periódica establecida con los equipos de administración de sistemas de información y plataforma tecnológica como mecanismo de control de calidad de la función de contingencia.
- ✓ Cuando se realicen modificaciones de hardware, software operativo, de infraestructura y/o aplicativos; o cuando existan cambios significativos en la plataforma tecnológica cubierta por el plan.

También pueden realizarse cuando se prevea el riesgo de que suceda un evento que afecte la entidad, como problemas laborales o de orden público.

12.1.1. Pruebas de escritorio

Se trata de un tipo de prueba programada y controlada que consiste en una revisión detallada del Plan de Contingencias de TI y los procedimientos implicados.
Para su ejecución se verifica la existencia del plan y sus procedimientos, y se convoca a los diferentes funcionarios responsables de los procesos o sistemas de información a participar en un taller en donde se da lectura al plan en forma ordenada, bajo la moderación del responsable del Plan de Contingencia de TI, con el fin de determinar fallas y omisiones con el criterio experto de quienes participan. Es recomendable ejecutar este tipo de prueba antes de ejecutar una prueba real y una vez sea publicada alguna actualización del presente Plan.

12.1.2. Pruebas técnicas

Este tipo de pruebas pueden ser parciales o totales, donde se prueban secciones o elementos individuales del Plan de contingencias de TI, como puede ser, un aplicativo o una plataforma o se prueban todos los componentes.

Responsable	Tipo de Prueba	Frecuencia
Profesional del Área de TIC	Desempeño de Sistemas de Información.	Conforme al cronograma establecido por el área TIC y secretaría general.
Profesional del Área de TIC, Profesional Proceso de Gestión Financiera y PQRSD	Desempeño de Sistemas de Información DELFI y SIAC	Semestral
Profesional del Área de TIC	Pruebas de alta disponibilidad del servicio internet.	3 pruebas anuales
Profesional del Área de TIC	Prueba de alta disponibilidad de infraestructura de seguridad perimetral.	3 pruebas anuales
Profesional del Área de TIC	Pruebas de restauración de	3 pruebas anuales

	copias de respaldo.	
Profesional del Área de TIC	Prueba de potencia de la UPS Sistemas de alimentación ininterrumpida.	1 prueba al año

✓ **Pruebas de desempeño a Sistemas de Información**

Estas pruebas consisten en evaluar y verificar que un Sistema de Información o aplicación de software realiza las actividades que fueron desarrolladas dentro del mismo, estas pruebas podrán incluir pruebas de seguridad y gestión de usuarios y son realizadas bajo los parámetros y cronogramas definidos por la secretaria general y el área TIC, estas pruebas pueden ser complementarias con las pruebas de restauración de información.

✓ **Pruebas de desempeño a Sistemas de Información DELFIN y SIAC**

Consiste en instalar y preparar los equipos de contingencia de los sistemas de información DELFIN y SIAC, con las características técnicas requeridas de acuerdo con los servicios de TI que se requieran con el fin de verificar el funcionamiento y puesta en producción.

✓ **Prueba de alta disponibilidad del Servicio de Internet**

Consiste en desconectar el canal activo del servicio de Internet, para que entre en servicio la redundancia de este, la prueba se realiza con servicios activos e inactivos y estos deberán continuar funcionando en tiempo real sin inconvenientes.

✓ **Prueba de alta disponibilidad de infraestructura de seguridad perimetral**

Consiste en desconectar el equipo principal activo de seguridad perimetral, para que entre en servicio la redundancia de este, la prueba se realiza con servicios activos e inactivos y estos deberán continuar funcionando en tiempo real sin inconvenientes

✓ **Prueba de Restauración de Información**

Consiste en realizar una restauración de las copias de seguridad más reciente que se tienen de los sistemas de información y/o aplicativos que se seleccionen, utilizando los procedimientos existentes de restauración y verificar la comunicación entre los aplicativos y las bases de datos.

✓ **Prueba de la UPS**

Los sistemas de alimentación ininterrumpida - UPS (por sus siglas en inglés - Uninterruptible Power Supply), son el sistema que garantiza la energía eléctrica a los equipos de cómputo de la Contraloría Municipal de Barrancabermeja, cuando haya una suspensión de este servicio.
La prueba consiste en verificar la activación automática de la puesta en marcha de la UPS cuando se suspende la energía eléctrica. Adicionalmente se puede realizar prueba de autonomía, la cual debe mantener el suministro de energía a los equipos conectados a la red eléctrica regulada.

12.2. Etapas de la Prueba

A continuación, se presentan las etapas que se deben realizar para el desarrollo de una prueba al Plan de Contingencias de TI.

ETAPA	DESCRIPCION
Planeamiento de la prueba	Definir los equipos participantes, los objetivos específicos de la prueba y confirmar con los funcionarios responsables de procesos la fecha y hora de realización.
Notificación de la prueba a los equipos de trabajo.	Notificar a los equipos participantes la realización de la prueba y verificar que todos ellos estén enterados.
Alistamiento y habilitación de los sitios	Incluye contar con todos los elementos

alternos para la prueba.	necesarios para iniciar el proceso de prueba.
Puesta en producción de los equipos de cómputo o sistemas de información en el lugar que se haya determinado para la prueba.	Actividades de los equipos de recuperación tendientes a restaurar y sincronizar los Aplicaciones.
Operación en los sitios alternos para la prueba.	Actividades de los equipos de recuperación tendientes a probar la operación en los sitios alternos para los equipos de contingencia.
Limpieza de los datos después de la prueba	Borrar todos los archivos sensibles en el lugar y equipos de contingencia.
Evaluación de la prueba	Reunirse con el personal que participó en la prueba para identificar problemas y aciertos del plan de contingencia de TI.

12.3. Evaluación de la prueba

Una vez se haya realizado la prueba y como actividad final, es necesario efectuar una evaluación o revisión de su desarrollo en la cual estén analizados los objetivos, los parámetros, los criterios establecidos, las fallas y fortalezas.

12.4. Documentación de las pruebas

Para realizar el registro de la ejecución de las pruebas al Plan de Contingencias de TI, se utilizará el formato descrito en el Anexo 1 – "Formato de Documentación de Pruebas del Plan de Contingencias de TI" de este documento.

13. Implementación del plan de contingencia de TI

En el Plan de Contingencias de TI se describen las actividades necesarias para mantener operantes y/o reestablecer los servicios de TI, sistemas de información, aplicativos y la infraestructura tecnológica que los soporta. Los instructivos y manuales técnicos son de índole confidencial, es solo para uso del personal encargado o de cada sistema o infraestructura.

14. ANEXO

Anexo 1. Formato de Documentación de pruebas del Plan de Contingencias de TI

CONTROL DE FIRMAS

Aprobado en Comité Institucional de Gestión y Desempeño – Acta No. 01 del 28 de enero de 2025.

CARLOS ARTURO VÁSQUEZ ALDANA
Secretario General

Proyecto: Héctor Fidel Castaño Sorza, Profesional Externo – Ingeniero de Sistemas