ALCALDIA DE LEBRIJA-SANTANDER

ESTRATEGIAS DE PRUEBAS DEL PLAN DE CONTINUIDAD DE TIC 2025

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.

2. OBJETIVO GENERAL

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.

2.1 OBJETIVOS ESPECIFICOS

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 de Bogotá D.C., a fin de garantizar la continuidad en la ejecución de las funciones y objetivos estratégicos de la entidad en el menor tiempo posible.

3. MARCO NORMATIVO

TIPO DE NORMA	DESCRIPCIÓN
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de 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	Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de

TIPO DE NORMA	DESCRIPCIÓN
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de 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	Por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de

4. APROBACIÓN Y ACTUALIZACIÓN

El Plan de Contingencias de TI deberá ser aprobado en sesión de Comité de Política de Gobierno Digital de la Alcaldia de Lebrija 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.

5. COMUNICACIÓN Y DISTRIBUCIÓN DEL PLAN

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

* Publicación de información de manera continua y accesible. En la Intranet de la Contraloría de Alcaldia de Lebrija, este medio se debe utilizar para difundir el plan de contingencias de TI.
*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 SGSI.
*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.

6. ROLES Y RESPONSABILIDADES

Para el manejo de la activación del Plan de Contingencia de TI en alguno de sus escenarios, es importante destacar que el proceso de Gestión Administrativa y Financiera es quien en primera instancia deberá 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 Direccionamiento Estratégico por medio de la Oficina Asesora de Comunicaciones, serán los encargados de difundir las comunicaciones oficiales tanto internas o externas (si los servicios afectados involucran servicios a la ciudadanía o los sujetos e 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 Administrativa y Financiera y Gestión de Tecnologías de la Información y las Comunicaciones, en cuanto la organización y requerimientos de logística.

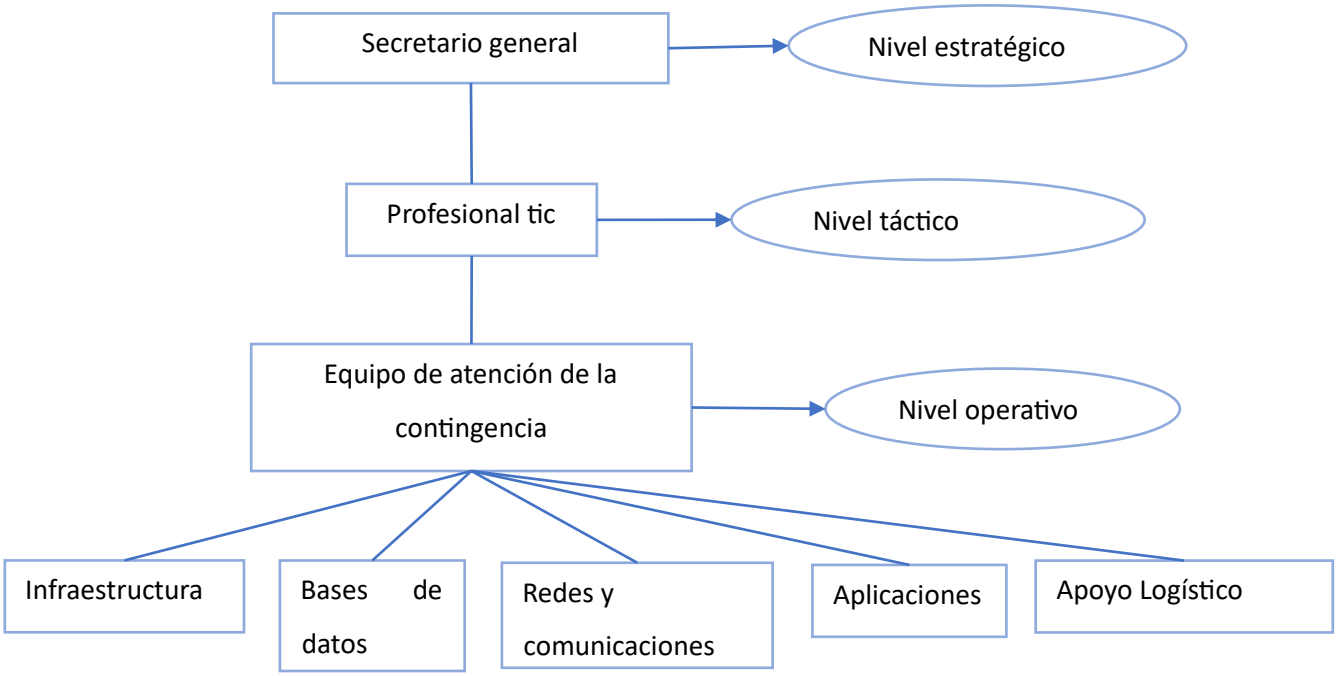
Por su parte el proceso de Gestión de Tecnologías procederá a poner en marcha los protocolos de atención de la contingencia de acuerdo con el escenario materializado.

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.



7. 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.

7.1. 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.

7.1. 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 de la Dirección de TIC responsables del proceso o sistema 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.

7.2. 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.

Tipo y frecuencia de pruebas técnicas de TI.

Responsable	Tipo de prueba	Frecuencia
Oficina TIC.	Desempeño de Sistemas de Información.	Semestral en infraestructura de respaldo.
Oficina TIC.	Pruebas de alta disponibilidad del servicio internet.	Mensual
Oficina TIC.	Prueba de alta disponibilidad de infraestructura de seguridad perimetral	Mensual
Oficina TIC.	Pruebas de restauración de copias de respaldo.	Mensual
Oficina TIC.	Prueba de potencia de la UPS Sistemas de alimentación ininterrumpida.	Mensual

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; estas pruebas pueden ser complementarias con las pruebas de restauración de información.

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 Alcaldia de Lebrija. 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.

7.3. 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	DESCRIPCIÓN
Planeamiento de la prueba	Definir los equipos participantes, los objetivos específicos de la prueba y confirmar con la localidad alterna 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 alternos para la prueba.	Incluye contar con todos los elementos necesarios para iniciar el proceso de prueba.
Puesta en producción de los equipos de cómputo o sistemas de información en la sede alterna 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 la localidad alterna 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.

7.4. 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.

8. ANEXO

Formato de documentación de pruebas del plan de continuidad de TI

RIESGO PARA EVALUAR	*<Nombre del riesgo a evaluar de acuerdo con lo descrito en la sección "Identificación de Riesgos" del Plan de Contingencia de TI >*		
TIPO DE INTERRUPCION	*<Identificar el tipo de interrupción a trabajar de acuerdo con lo descrito en la sección "Clasificación de interrupciones y nivel de afectación a los servicios de TI" del Plan de Contingencia de TI>*		
ESCENARIO DE PRUEBA	*<Referir el escenario de prueba que se va a simular de acuerdo con lo descrito en el documento "Guía acciones por contingencias".*		
OBJETIVO DE LA PRUEBA	*<Describir la finalidad de la prueba a realizar>*		
RECURSO PARA PROBAR	*<Nombre del sistema de información, aplicativo y/o infraestructura tecnológica y/o servicio de TI que se va a probar de acuerdo con lo descrito en la sección "Inventario de servicios e infraestructura de TI" del Plan de Contingencia de TI*		
FECHA	**DURACIÓN**	**RESPONSABLE**	**DESCRIPCION**
<dd/mm/aaaa del diligenciamiento del formato>	**<Tiempo estimado de la duración de la prueba>**	**<responsable de la ejecución de la prueba>**	**<Descripción resumida de la prueba a realizar>**

ALCANCE: <Describir el alcance del plan de pruebas, identificando el lugar de la prueba, los recursos, servicio, aplicativos y/o servicios que serán sometidos a pruebas y los tipos de prueba que se realizarán, de acuerdo con lo descrito en la sección "Tipos y frecuencia de pruebas" de este documento.>

REQUISITOS PARA LA PRUEBA

* Recurso Humano: <Especificar el recurso humano necesario para la ejecución del plan de pruebas, incluyendo los descritos en la sección "Roles y responsabilidades" dentro del Plan de Contingencias de TI", así como los proveedores involucrados>
* Requerimientos Hardware: <Especificar los requerimientos de hardware (sistema operativo, memoria, servidor de aplicaciones, red, etc.) para la ejecución del plan de pruebas>
* Requerimientos Software: <Especificar los requerimientos de software y copias de respaldo para la ejecución del plan de pruebas>
* Requerimientos de Logística: <Especificar los requerimientos logísticos que se requieran (ejemplo: transporte, autorizaciones, entre otros) para la ejecución del plan de pruebas>

PLAN DE PRUEBAS

<Por cada tipo de prueba diligencie un cuadro> **Tipo de prueba:**	*<Tipo de prueba, citar el tipo de prueba a realizar de acuerde a lo descrito en la sección "Tipo y frecuencia de las pruebas" de este documento>*
Identificador:	*<Identificador único de la prueba, puede estar compuesta por la fecha y un número consecutivo>*
Líder de la prueba:	*<Nombre de la persona líder de la prueba>*
Objetivo:	*<Objetivo de la ejecución del tipo de prueba>*

Técnica:	*<Técnica empleada para ejecutar la prueba. Secuencia de pasos y condiciones que debe seguir el equipo de pruebas para ejecutarla >*
Precondiciones:	*<Condiciones previas para la ejecución de la prueba>*
Criterios de éxito:	*<Criterios para considerar que la ejecución de la prueba generó resultados satisfactorios>*
Precondiciones:	*<Conjunto de condiciones que deben ser ciertas o que se deben cumplir antes de iniciar la prueba>*
Resultado esperado:	*<Resultado que se espera obtener con la ejecución de la prueba, se debe establecer antes de ejecutar la prueba>*
Secuencia de pasos para la ejecución de la prueba:	*<Descripción de cada uno de los pasos que se requieren para Ejecutar la prueba, teniendo como referencia lo descrito en el numeral "Etapas de la prueba" del presente documento>*
Resultado obtenido:	*<Resultado obtenido después de ejecutar la prueba. En caso de que el resultado obtenido sea diferente al resultado esperado se deben describir dichas diferencias y las posibles causas que las generaron>*
Fecha ejecución:	*<Fecha en la cual se ejecuta la prueba – formato dd/mm/aaaa>*
Anexos:	*<Relación de los anexos que complementan la ejecución de la prueba>*
Observaciones:	*<Observaciones adicionales de la prueba>*