Control de cambios

Versión	Fecha	Descripción de la modificación
01	31 de diciembre de 2015	Primera versión del documento
1	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigencia de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento corresponden íntegramente a los aprobados en la versión 1 de fecha 31 de diciembre de 2015, la cual fue aprobada por Juan Carlos Garzón Barreto, Sub Secretario de Planeación y Gestión (E), como líder del proceso Gestión y Adquisición de Recursos, vigente en ese momento.
2	23 de agosto de 2018	Se elabora el documento en el nuevo formato para manual, propuesto y actualizado por OAP, se modifica el Nombre del documento como "Manual Plan de Contingencia Informático", se agregan los numerales Tabla de contenido, alcance, se modifica Introducción, objetivos, definición y descripción del plan de contingencia informático y documentos relacionados. Lo anterior de acuerdo a los lineamientos establecidos.

Método de Elaboración	Revisa	Aprueba
El documento se elabora con base en la normatividad que regula la materia, los profesionales de DTI realizan los ajustes correspondientes, y se entregó el documento para revisión de normalización por parte de la Oficina Asesora de Planeación	**Cesar Augusto Intriago Bogotá** Director DTI **Liliana Patricia Casas Betancourt** Profesional OAP	**Lúbar Andrés Chaparro** Subsecretaria Institucional Líder de macroproceso Documento revisado y aprobado mediante registro aplicativo Hola No. **22665**

TABLA DE CONTENIDO

1 INTRODUCCIÓN

La información considerada como uno de los bienes más importantes para las Entidades, e integrada con los avances tecnológicos basados en la normatividad vigente han permitido facilitar y beneficiar a la ciudadanía mediante la prestación de sus trámites y servicios en línea, los cuales son publicados y mejorados continuamente en sus portales web. Por lo anterior y para no interrumpir el eficiente desarrollo de sus procesos misionales es muy importante contar con un plan de contingencia informático que identifique los posibles riesgos, los mitigue, sea capaz de enfrentar las emergencias presentadas y recupere en el menor tiempo posible los flujos de operación contra caídas o daños que afecten la disponibilidad del servicio.

La finalidad del Plan de Contingencia Informático, como parte de la política de seguridad, es proteger los recursos tecnológicos y las operaciones de la entidad, para garantizar la continuidad de los procesos que permiten cumplir con la misionalidad de la Secretaría Distrital de Gobierno. Con su implementación se busca establecer un adecuado sistema de seguridad física y lógica para salvaguardar los activos informáticos y recursos tecnológicos de la entidad contra posibles desastres, a través del conjunto de herramientas, mecanismos y estrategias planteadas en los sub-planes preventivo o de respaldo, de emergencia y de restauración o recuperación de los servicios de la entidad.

El plan de contingencia informático inicia con el diagnóstico para determinar los procesos y servicios internos y externos prestados por la entidad, continua con la identificación, análisis y evaluación de los riesgos o amenazas que puedan afectar las operaciones tecnológicas normales de funcionamiento y finaliza con las estrategias propuestas para proteger los activos y recursos de la entidad garantizando la continuidad del negocio en caso de afectación. La metodología propuesta se base en el ciclo de vida iterativo PDCA (plan-do-check-act, / planificar-hacer-comprobar-actuar).

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Crear mecanismos de control y estrategias de restablecimiento de los elementos de configuración, mitigando los riesgos presentados, con el fin de proteger sus activos de información y garantizar la continuidad del servicio en los procesos misionales de la entidad.

2.2 OBJETIVOS ESPECÍFICOS

a. Definir las actividades de planeación, elaboración ejecución y verificación de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos, reduciendo el grado de vulnerabilidad y exposición al riesgo.

b. Garantizar la continuidad de las operaciones de los principales elementos de configuración que componen los sistemas de información y la infraestructura tecnológica, minimizando el tiempo de reacción ante la emergencia y recuperación del servicio.

c. Identificar los principales riegos que puedan afectar los servicios de la entidad facilitando tomar decisiones rápidas ante anormalidades o fallas.

d. Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

e. Cumplir con la normatividad legal vigente.

f. Generar cultura de Seguridad en la Entidad.

3 ALCANCE

El plan de contingencia informático será implementado en la Secretaría Distrital de Gobierno, a nivel central y localidades, con el fin de salvaguardar los activos de información de la entidad. Se incluyen los elementos de configuración de los sistemas de información, infraestructura y servicios tecnológicos con el fin evitar o minimizar la materialización de riesgos y garantizar el normal funcionamiento de los servicios prestados por la entidad.

4 DEFINICIONES

4.1 GLOSARIO

- **Acceso:** Es la recuperación o grabación de datos que han sido almacenados en un sistema de cómputo. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del equipo.

- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

- **Amenaza:** Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

- **Base de Datos:** Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que, además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

- **Datos:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

- **Incidente o Evento:** Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

- **Integridad:** Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan

valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

- **Privacidad:** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

- **Seguridad:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

- **Switches:** Dispositivo de interconexiones de redes informáticas

- **Cableado de la Red:** Elemento físico que permite conectar entre si a diferentes aparatos informáticos

- **Router:** Dispositivo de hardware que permite la interconexión de ordenadores en red.

- **FireWall:** Cortafuegos, es una parte de un sistema o una red que está diseña para bloquear el acceso no autorizado.

- **Backup:** Copia de seguridad o respaldo.

- **Elementos de configuración:** Es un elemento controlado por la gestión de la configuración

4.2 SIGLAS

- **DTI:** Dirección de Tecnologías e Información
- **DBMS:** Sistema Manejador de Base de datos
- **CDS:** Discos óptimos para almacenar datos
- **DVD:** Dispositivo Digital Versátil para almacenamiento de datos
- **RAM:** Memoria Principal donde se almacenan programas y datos, Memoria de acceso aleatorio.

5 DESCRIPCIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO

5.1 DIAGNOSTICO DE PROCESOS Y SERVICIOS

5.1.1 Principales Procesos de Software:

Aplicativos misionales y de apoyo definidos en la intranet de la Entidad.

5.1.2 Principales servicios que deberán ser restablecidos Y/O recuperados

- Canales de conectividad
- Bases de Datos
- Aplicativos
- Portal Web Secretaria de Gobierno

5.2 IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

5.2.1 Metodología aplicada:

Para la clasificación de los activos de las Tecnologías de Información de la Secretaria Distrital de Gobierno, se han considerado tres criterios:

a) Grado de adversidad: Un evento se define con grado de adversidad (Leve, moderada, grave y muy severo).

b) Frecuencia del Evento: Nunca, aleatoria, periódico y continuo.

c) Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

5.2.2 Aspectos de procedimiento y consideración:

a) **Plan de Contingencia:** Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- Leves (Caídas de energía de corta duración, fallas en disco duro, etc.)
- Severas (Destrucción de equipos, incendios, etc.)

b) **Riesgo**: Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgo:

- Riesgos Naturales: tales como mal tiempo, terremotos, etc.
- Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía, ataques informáticos.
- Riesgos Sociales: como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad:

c) Activos susceptibles de daño:

- Personal
- Servidores
- Software
- Información
- Energía eléctrica
- Equipos de Seguridad Perimetral
- Equipos activos
- Ups
- Aires Acondicionados

d) Posibles Daños

- No se cuenta con acceso físico a las instalaciones debido a protestas, desastres naturales, fallas sistema control de acceso.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

e) **Fuentes de daño**

- Acceso físico no autorizado
- Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario.
- Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).
- Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red, Switches, cableado de la Red, Router, FireWall).

- Ataques Informáticos

f) **Clases de Riesgos**

- Incendio o Fuego.
- Falla en los equipos.
- Equivocaciones.
- Acción virus informático.
- Fenómenos naturales.
- Accesos no autorizados.
- Ausencia del personal de sistemas.
- Ataques Informáticos

5.3 PLAN DE RESPALDO - ANTES

Describe las contramedidas preventivas que se deben realizar para evitar la materialización de la amenaza, de acuerdo a la identificación de los tipos de riesgos y análisis de afectación al buen funcionamiento de las operaciones de la entidad, resultado obtenido en el numeral 5.2 "Identificación, análisis y evaluación del riesgo".

Y contramedidas correctivas en los casos de revisión periódica acordada o después de presentada la incidencia, con el fin de evaluar si las acciones propuestas para mitigar el riesgo fueron eficaces, ineficaces o no estaban prevista, lo cual obliga a realizar un nuevo análisis de riesgo para mejor el plan de contingencia propuesto.

5.3.1 Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad, de acuerdo a los lineamientos contemplados en los documentos "GDI-TIC-M005 Manual de soporte físico y lógico de la infraestructura tecnológica de la secretaría distrital de gobierno" y "GDI-TIC-IN015 Instrucciones para la realización de copias de seguridad, pruebas de restauración y restauración de información". Se establece los procedimientos relativos a:

- Sistemas e Información
- Equipos de Cómputo
- Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a. Sistemas de Información

La Entidad cuenta con un catálogo de Sistemas de Información, tanto los de desarrollo propio, como los desarrollados por empresas externas.

b. Equipos de Cómputo

Se debe tener en cuenta el registro de Hardware, impresoras, scanner, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional). Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución, de acuerdo a los lineamientos impartidos en el documento GDI-TIC-IN015 Instrucciones para la realización de copias de seguridad, pruebas de restauración y restauración de información. Las copias de seguridad son las siguientes:

- Backup del Sistema Operativo: Todas las versiones de sistema operativo instalados en la Red. (Periodicidad – Semestral).
- Backups de los datos (Base de datos, passsword y todo archivo necesario para la correcta ejecución del software aplicativos de la institución). (Periodicidad – Mensual).

5.3.2 Medición y prevención de las clases de riesgo

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo, .

Incendio o Fuego

- Grado de Adversidad: Muy Severo
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Alto

Situación Presentada	Acción Definida
En el Centro de Cómputo donde están ubicados los servidores, equipos de comunicación y conectividad, está dotado de un sistema contra incendios y se cuenta con extintores ubicados estratégicamente para cualquier eventualidad.	Se cumple.
A los servidores se les realizan backups de la información generada periódicamente, pero no existe ninguna otra copia de respaldo exterior.	Después de realizar backups de los servidores de forma mensual, se debe almacenar en cintas magnéticas y buscar la manera de vincular este proceso con la extracción segura de la Entidad con algún servicio de Bodegaje y/o almacenamiento seguro.
Se adquieren servicios en las nubes de Oracle y Azure, lo que permite tener un sitio alterno donde se publicaran aplicativos de la Entidad permitiendo así tener redundancia en los diferentes servicios que están ubicados en el Centro de Datos.	Se cumple

Falla en los Equipos

- Grado de Adversidad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave

Situación Presentada	Acción Definida
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de equipos en desuso o que sean declarados para dar de baja.
Cada área funcional se une a la Red de datos a través del cableado estructurado que se centraliza en el Centro de Datos principal, la falta de energía en el Centro de Datos, originaria la ausencia de uso de los servicios de red.	Se cuenta con un sistema de UPS's que soportan el servicio eléctrico en caso de falla eléctrica.
Falla switch de core	Contar con redundancia o sistema de alta disponibilidad, que cumpla con las funciones del

	equipo principal en caso de falla. Contar con la garantía y el soporte especializado sobre el equipo.
Falla Firewall	Contar con redundancia o sistema de alta disponibilidad, que cumpla con las funciones del equipo principal en caso de falla. Contar con la garantía y el soporte especializado sobre el equipo.
Fallas Servidores de aplicaciones	Se debe contar con herramientas de respaldo que nos permitan recuperar el servidor afectado.
Fallas Servidores de Bases de Datos	Se debe contar con mecanismos de respaldo que nos permitan recuperar la información y la configuración de estas máquinas en caso de presentarse fallas.

Equivocaciones en el manejo del sistema

- Grado de Adversidad: Moderado
- Frecuencia de Evento: Periódico
- Grado de Impacto: Moderado

Situación Presentada	Acción Definida
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Realizar capacitación al ingreso sobre el manejo de los sistemas a cargo y generar documentación, manuales e instructivos.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple.
Se presentan equivocaciones en el manejo de información debido a que, al momento de iniciar actividades en el cargo asignado, no se suministran manuales, o se hace entrega puntual de instrucciones o políticas de manejo y/o operación de las distintas plataformas, Sistemas Operativos y demás elementos de TI.	Definir políticas de informática claras y precisas, las cuales se deben comunicar a los funcionarios al ingresar a ocupar sus respectivos cargos o al cumplir con sus obligaciones contractuales, al igual que cualquier modificación a las mismas. Generar manuales y documentación de los diferentes sistemas.

Acción de Virus Informático

- Grado de Adversidad: Muy Severo
- Frecuencia de Evento: Continuo
- Grado de Impacto: Grave

Situación Presentada	Acción Definida
Se cuenta con un software antivirus para la entidad (Trend Micro).	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad a la finalización del contrato.
Se cuenta con privilegios de acceso a los servidores y segmentos de red diferentes para evitar la propagación de virus.	Se cumple.

Fenómenos Naturales

- Grado de Adversidad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave

Situación Actual	Acción Correctiva
En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención.
Aunque existen épocas de lluvia fuertes, las instalaciones de la secretaria están debidamente protegidas.	Tomar medidas de prevención.
Los servidores principales se encuentran en un ambiente libre de filtraciones.	Ante la mínima filtración se debe informar de inmediato a la Dirección, para realizar el respectivo mantenimiento correctivo y preventivo.

Accesos No Autorizados

- Grado de Adversidad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave

Situación Presentada	Acción Definida
Se controla el acceso al sistema de red mediante Directorio Activo, en donde se permite el uso de servicios de red con un usuario y con su respectiva clave.	Se cumple.
La asignación de usuario se realiza de acuerdo a los parámetros y políticas establecidas por la Dirección y se solicita en forma virtual a través de los medios designados de acuerdo al documento "GDI-TIC-P001 Procedimiento para la gestión de servicios de tecnologías de la información y las comunicaciones".	Se debe solicitar por escrito (E-mail) a la Mesa de Servicios la creación de usuarios y los permisos que se requiere sean asignados, o cualquier cambio referente a los mismos.
La oficina Gestión del talento humano no comunica con celeridad a la Mesa de Servicios, cuando un funcionario sale a vacaciones o se retira de la entidad a fin de desactivar ese usuario.	Se debe informar a la Mesa de Servicios, que funcionario sale a vacaciones para así bloquear el respectivo usuario por el tiempo de ausencia, igualmente en caso de retiro definitivo.
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software. Se debe habilitar en todos los sistemas de información utilizados en la Entidad, la funcionalidad de solicitar de manera obligatoria el cambio de contraseña en los periodos de tiempo que indique el manual de políticas de uso y seguridad de la información, con el fin de fortalecer la cultura de manejo de contraseñas de manera responsable.
Se cuenta con perfiles de navegación para restringir y proteger a la Entidad de páginas maliciosas y optimizar los recursos de red.	Se cumple
No se cancelan los usuarios del personal que se retira de la entidad de forma inmediata, recurriendo en algunos casos a utilizar la contraseña del funcionario ausente.	Tan pronto se informe que un funcionario se retira definitivamente se debe cancelar este usuario.

Ausencia del personal a cargo de las labores administrativas de TI

- Grado de Adversidad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave

Situación Presentada	Acción Definida
En la secretaria, la planta de personal del área de tecnología es reducido, se cuenta con un funcionario por componente TI (Uno para Base de datos, uno para Sistemas de Información, uno para Servidores, uno para redes, etc.)	Es importante reforzar el personal del área de sistemas con personal capacitado que tenga el conocimiento y la experiencia como backup de las personas que tienen a cargo al acceso y manejo de los diferentes sistemas, Bases de Datos, Directorio Activo, Redes, Servidores, Equipos activos y de seguridad perimetral.
El funcionario de Grupo de Infraestructura o de Sistemas de Información, es la única persona con claves de acceso al sistema, conocedor del manejo de la red y los sistemas de información.	Se debe generar políticas de manejo de contraseñas y copias de respaldo de las contraseñas utilizadas para los sistemas más importantes del área.
Aunque se ha diagramado un esquema general de la Red de Datos de la Entidad, en caso de fallas en la red y ausencia del funcionario del Grupo de Infraestructura encargado, no existe un diagrama lógico completo en el cual se definan las conexiones de red existentes, de forma que agilice la labor de recuperación del sistema.	Realizar el diagrama lógico de la red y revisar la demarcación de cada uno de los puntos de red físicos para que en caso de falla se agilice el trabajo de inspección y por ende la recuperación del sistema, para el centro de datos.

5.4 PLAN DE EMERGENCIA - DURANTE

Considera las contramedidas que se deben aplicar durante la materialización de la amenaza, para mitigar las consecuencias generadas por el siniestro.

Cuando se materializa un riesgo, este puede producir un Evento, por tanto, a continuación, se describen los eventos a considerar dentro del Plan de Contingencia.

RIESGO	EVENTO	MEDIDA APLICADA	RECURSO DE CONTINGENCIA
FALLAS DE RED GENERAL	No hay comunicación con aplicaciones y servicios de red	-Requerimiento del usuario reportando la falla. - Validación de primer nivel equipos de comunicaciones (ping). - Validación física de los lets (indicadores) alarmados. - Reportar al proveedor la falla presentada.	- Soporte especializado proveedor de conectividad -Diagrama Lógico de la red -Cables de fibra -Cables Utp
FALLA DE RED USUARIO	No hay comunicación entre el usuario y los diferentes servicios de red.	-Requerimiento del usuario reportando la falla. -Validación de primer nivel por parte del grupo de soporte de mesa de servicios. - Validar si tarjeta de red linkea - Si no está linkenado solicitar validar estado del punto de red en el centro de datos. - Si el punto de red está funcionando correctamente validar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma -Validar estado patch cord. Si persiste la falla Validar por parte del segundo nivel -Que el punto de red	Cables Utp Tarjetas de Red Equipo Activo Contrato soporte equipos activos

		del usuario esté conectado en el centro de datos. -Validar estado del punto de red en el equipo activo. -Probar el cable UTP. Si existe daño, realizar el cambio del cable -Validar cable de red desde patch panel a equipo activo. -Revisar estado de la interfaz equipo activo.	
FALLAS SERVIDOR	No hay acceso a aplicativos o Información	-Validación de segundo nivel de la falla presentada -Validar fallas en componentes de harware, disco duro, memorias, fuentes, ventilador, procesador	Stock repuestos servidor Backup periódico de la información. Contrato mantenimiento preventivo servidores. Backup máquinas virtuales para restauración de los servicios.
FALLAS UPS	Daño de equipos, perdida de información	-Validación estado de los ups. - Validación estado de las baterías. -Mantenimientos preventivos.	Contrato de mantenimiento preventivo Ups.
VIRUS	Perdida de información	-Validación de primer nivel en sitio. -Validar que tenga cliente de antivirus instalado. -Validar que el cliente de antivirus este	Contrato de mantenimiento software antivirus.

		activo. -Correr el cliente de antivirus para escanear el equipo en busca del virus. Validación de segundo nivel -Revisar consola de antivirus para generar reportes de virus. -Actualizar desde la consola las listas de virus reportados. Mandar actualizaciones a los clientes.	
CORTE GENERAL DE FLUIDO ELECTRICO	No hay acceso a aplicativos o Información	- Revisar funcionamiento de las UPS mientras entra en servicio la planta eléctrica de respaldo. -Activar planta eléctrica para mantener el servicio.	UPS, Planta Eléctrica, contrato mantenimiento Ups
FALTA DE PERSONAL	Demoras en respuesta a solicitudes y nuevos proyectos	-Diagrama de servicios administrador por funcionario. -Definir funcionario de respaldo para los procesos críticos de infraestructura. -Implementar metodología para el manejo de contraseñas de acceso a los diferentes recursos de T.I	-Contratos de soporte para los procesos críticos de la Entidad (Bases de Datos, Equipos activos, Servidores) -Soporte especializado en el grupo de mesa de servicios. -Manual de funciones del área

FALLAS EQUIPOS DE COMUNICACION	No hay acceso a aplicativos, internet o Información	-Pruebas de primer nivel hacia los diferentes equipos de comunicación para detectar cual está fallando (Router, Core, switch de borde, firewall) - Si el problema está en el Router se revisa en sitio para validar alertas en los lets -Reportar al proveedor de servicios de comunicación la falla presentada. Si el problema está en el Core, se activa equipo de respaldo, y se solicita servicio a la empresa de mantenimiento pata restaurar el principal. Si el problema está en el firewall se activa equipo secundario para mantener los servicios y se solicita el soporte a la empresa para revisar la falla en el equipo principal y restaurar.	Contrato proveedor de servicios de conectividad. Implementación de servicios de redundancia en el core, firewall Contrato mantenimiento equipos activos Contrato mantenimiento equipos de seguridad perimetral
INCENDIO, TERREMOTO	INDISPONIBILIDAD DEL CENTRO DE DATOS	-Implementar sistemas de control de incendios especializado para datacenter. -Realizar inventario de los servicios implementados en el datacenter -Realizar backup de la	-Mantenimiento preventivo sistema control de incendios. -Contratar servicios de nube que permitan restablecer los servicios que se tienen implementados en el datacenter principal. -Diagrama de servicios

		información y de los servidores que se encuentran en el datacenter. -Evaluar el daño -Restablecer o instalar nuevo centro de datos de acuerdo al daño presentado -Remplazar equipos afectados -Restaurar los backups -Restaurar servicios	de la entidad que están alojados en el datacenter -Implementar servicios de almacenaje de los backups en lugar externo a la Entidad.

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

a. Buscar Ayuda de Otros Entes

Es de tener en cuenta que solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que las acciones del siniestro causen más daños o destrucciones.

- Se tiene en las dependencias correspondientes los números de teléfono y direcciones de organismos e instituciones de ayuda.

- Todo el personal debe conocer la localización de vías de Escape o Salida: Deben estar señalizadas las vías de escape o salida.

- Instruir al personal de la entidad respecto a evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local u otros entes.

- Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades.

c. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

5.5 PLAN DE RECUPERACION - DESPUES

Comprende las contramedidas que se deben ejecutar después de materializada y controlada la amenaza, para restaurar los elementos informáticos, tecnológicos, y reanudar los servicios de la entidad.

* Evaluación de daños.

* Traslado de datos desde la ubicación de emergencia a la habitual.

* Reanudación de la actividad.

* Desactivación del precontrato de alquiler.

* Reclamaciones a la compañía de seguros.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto, se definen los siguientes responsables:

Administrador(es) de Infraestructura: Sera responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.

Dirección de Tecnologías e Información: Verificara la labor realizada por el (los) Administrador(es) de Infraestructura.

5.5.1 Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de la Secretaria Distrital de Gobierno se debe atender los procesos de Financiera, Talento Humano, Tecnologías e Información y demás primordiales para el funcionamiento de la Entidad, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de actividades implica la colaboración de todos los funcionarios, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones. Los trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos de la institución, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de accesorios dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información,

debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencia, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

e. Retroalimentación de Actividades

Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

6 CONCLUSIONES

El presente Plan de contingencias de la Secretaria Distrital de Gobierno, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información. Este Plan está sujeto a la infraestructura física y las funciones que realiza la Dirección de Tecnologías e Información.

Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Minimización de riesgos, Identificación de posibles eventos para el Plan de Contingencia, Establecimiento del Plan de Recuperación y Respaldo, Plan de Emergencias y Verificación e implementación del plan.

No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Centro de Cómputo.
Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

7 RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Contingencia, con la finalidad de instruir adecuadamente al personal de la Secretaria Distrital de Gobierno.

Adicionalmente al plan de contingencias se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados. Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento. Cuando los administradores de infraestructura se encuentren ausentes, se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la Entidad no se vea interrumpida.

8 DOCUMENTOS RELACIONADOS

8.1 Documentos internos

Código	Documento
GDI-TIC-P001	Procedimiento para la gestión de servicios y tecnologías de la información y las comunicaciones.
GDI-TIC-IN015	Instrucciones para la realización de copias de seguridad, pruebas de restauración y restauración de información.
GDI-TIC-M005	Manual de soporte físico y lógico de la infraestructura tecnológica de la secretaría distrital de gobierno.

8.2 Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
NTC 5722	2012	N/A	N/A
ISO 22301	2012	N/A	N/A
ISO 27005	2018	N/A	N/A
ISO 31000	2018	N/A	N/A

8.3 Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Guía para la preparación de las TIC para la continuidad del negocio.	Versión 1 15/12/2010	MINTC	Virtual http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf