CONTROL DE CAMBIOS		
VERSION[1]	**FECHA**	**DESCRIPCION DE LA MODIFICACION**
1	31 de Diciembre de 2015	Primera Versión del Documento
01	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.

[1] Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en la intranet de la Secretaría Distrital de Gobierno

INTRODUCCION

La protección de la información vital de una entidad ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático.

Cualquier Sistema de Redes de Computadoras (computadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informáticos, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

Para realizar el Plan de contingencia informático de la Secretaria Distrital de Gobierno, se tiene en cuenta la información como uno de los activos más importantes de la Organización, y la infraestructura informática que está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Entidad. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es importante resaltar que para que la Secretaria Distrital de Gobierno logre sus objetivos, es indispensable el manejo de información, por lo tanto necesita garantizar tiempos de indisponibilidad mínimos para no originar distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación, ya que de continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la entidad. De acuerdo a lo anterior es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

OBJETIVOS

I. Definir las actividades de planeamiento, preparación y ejecución 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.

II. Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información, y/o en su defecto, reducir el tiempo de reacción ante la emergencia.

III. Dimensionar el riesgo potencial y tomar decisiones rápidas ante anormalidades o fallas.

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

V. Cumplir con la normatividad legal vigente.

VI. Generar cultura de Seguridad en la Entidad.

IDENTIFICACION DE PROCESOS Y SERVICIOS

Principales Procesos de Software Identificados

- SIACTUA
- SISIPEC
- CEASC
- NUSE
- Orfeo
- SICAPITAL
- SIPSE
- SIG
- SIAP

Principales servicios que deberán ser restablecidos Y/O recuperados

- Portal Web Secretaria de Gobierno
- Correo Electrónico.
- Canales de Internet.
- Mesa de Servicios

Software Base

- Base de Datos Oracle.
- Backups de la Información en Producción.

- Ejecutables de las aplicaciones.

Respaldo de la Información

- Backup de la Base de Datos.
- Backup de la Plataforma de Aplicaciones (Sistemas de Información).
- Backup del Portal Web de la Secretaria.
- Backup del Servidor de archivos.

ANALISIS DE EVALUACION DE RIESGOS Y ESTRATEGIAS

Metodología aplicada:

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

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

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

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

Aspectos de procedimiento y consideración:

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:

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

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

a) Riesgos Naturales: tales como mal tiempo, terremotos, etc.
b) Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
c) 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:

Activos susceptibles de daño:

- Personal

- Hardware
- Software y utilitarios
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

Posibles Daños

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- 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.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante robo o infidencia.

Fuentes de daño

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistemas de cómputo.
- 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).

Clases de Riesgos

- Incendio o Fuego.
- Robo común de equipos y archivos.
- Falla en los equipos.
- Equivocaciones.
- Acción virus informático.
- Fenómenos naturales.
- Accesos no autorizados.
- Ausencia del personal de sistemas.

MINIMIZACION DEL 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. Es de tener en cuenta que en lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de

poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

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, se disponen de extintores especializados, ubicados estratégicamente para cualquier eventualidad. De igual forma cada piso cuenta con un extintor debidamente cargado.	Se cumple.
No se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios nuevos, lo que no es eficaz para enfrentar un incendio y sus efectos	Realizar capacitación para el manejo de extintores y primeros auxilios.
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, para lo cual se cuenta con un acuerdo de voluntades entre la Secretaria Distrital de Gobierno y la Secretaria General para el almacenamiento seguro de estas cintas en el Archivo Distrital. De otra parte se cuenta con un convenio interadministrativo entre la Secretaria Distrital de Ambiente y la Secretaria Distrital de Gobierno el cual contempla dentro de sus obligaciones entre otras la de almacenar las copias de respaldo en áreas seguras.

Comentarios al respecto

Analizando el riesgo de incendio, permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DVD's, cartuchos, cintas y Discos duros. Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, y preferiblemente, fuera de la Secretaria Distrital de Gobierno.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos en las posibles áreas de riesgo que se debe proteger.

Robo Común de Equipos y Archivos

- Grado de Adversidad: Grave

- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Moderado

Situación Presentada	Acción Definida
Debido a que a la hora de salida de las personas particulares que ingresan a la entidad, no son registradas pues no se cuenta con vigilante. Cabe anotar que contamos con sistema de seguridad.	Se requiere que cada funcionario en el momento de retirarse de la oficina por un tiempo considerable, opte por guardar su equipo dentro de algún cajón bajo llave. Adicionalmente se requiere de la implementación de una solución de seguridad física, administrada y controlada directamente por la Entidad, que involucre un sistema de CCTV, sistema de control de activos, sistema de apoyo a requisas y sistema de control de visitantes, entre otros, que permita hacer monitoreo de todas las áreas de las oficinas y no solo de las áreas comunes como se cuenta hoy en día en el sistema administrado por la Secretaria General.
Autorización escrita firmada por el Jefe o Director de área, Personal asignado de Sistemas y funcionario responsable, para la salida de equipos de la Entidad.	Se cumple por medio del formato establecido para salida de equipos.
Por la ubicación de la Secretaría Distrital, existe riesgo para el personal de la Entidad, de ser víctima de hurto o atraco.	Solicitar la colaboración de la Policía Nacional para que realice rondas periódicas por el sector donde se encuentra ubicadas las instalaciones de la Secretaria.

Comentarios al respecto
No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe de Cada Área y del Grupo de Sistemas, esto demuestra que los equipos son vigilados por cada funcionario asignado al mencionado elemento.

Según antecedentes de otras entidades, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en complicidad con el personal de vigilancia, es relativamente fácil remover un disco duro del CPU, una unidad lectora de CD/DVD, etc. y no darse cuenta del faltante hasta días después. Estas situaciones no se han presentado en la Entidad, pero se recomienda siempre estar alerta.

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 cumple. El Centro de Datos se encuentra protegido en un lugar de acceso restringido y son manipulados solo por Grupo de Infraestructura Tecnológica. Adicionalmente, se cuenta con un sistema de UPS's que soportan el servicio eléctrico en caso de emergencia.
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 recomienda que cada funcionario mantenga su equipo conectado a las tomas naranja (UPS). En ningún caso se debe superar la capacidad instalada en cada sede, pues las UPS están dimensionadas con las cargas máximas a soportar de acuerdo con la distribución de puestos de trabajo, y dando cumplimiento a las normas de salud ocupacional.

Comentarios al respecto

Teniendo en cuenta la importancia del fluido eléctrico para el funcionamiento de la entidad, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos. El equipo de aire acondicionado y ambiente adecuado en el Centro de Datos, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales de escritorio, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico.

Por lo anterior se debe tener en cuenta lo siguiente:

Tomas a Tierra o Puestas a Tierra:

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial. La Toma a Tierra tiene las siguientes funciones principales:

a) Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.
b) Protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.
c) Facilita el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Fusibles:

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo, a continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible., una vez arreglado el problema se puede volver a conectar el equipo. Al sustituir un fusible, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el mismo. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado, asegurarse que el fusible de recambio es de la misma capacidad que el fundido. No aprobar las reparaciones de los fusibles, usando hilos de cobre o similares.

Extensiones eléctricas y capacidades:

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado. No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

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 instrucción inicial en el ambiente de trabajo presentando las políticas informáticas establecidas para manejo de sistemas.
Algunas veces el usuario que tiene conocimiento en	El técnico de sistemas debe asignar permisos y

informática intenta navegar por sistemas que no están dentro de su función diaria.	privilegios a cada usuario de acuerdo a sus funciones.
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 recomienda que cada funcionario mantenga su equipo conectado a las tomas naranja (UPS).
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.

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), pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.
Únicamente la Mesa de Servicios es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple. En las alcaldías locales se cuenta con el apoyo de los Administradores de red local, quienes son la extensión de la Mesa de Servicios en las sedes que dependen de cada alcaldía local.
Se tiene acceso restringido a los servicios que se prestan por medio de los servidores, únicamente es el administrador de servidores del Grupo de Infraestructura el encargado de cambiar configuraciones y anexar nuevos equipos virtuales.	Se Cumple.

Comentarios al respecto

Los Virus informáticos han evolucionado de tal manera que hoy en día todos conocemos la importancia de tener un programa Antivirus en el computador y aun más importante es su actualización. Si tenemos un antivirus instalado pero no lo hemos actualizado, seguramente será capaz de encontrar los virus que intenten entrar en nuestros sistemas pero no será capaz de hacer nada con ellos, dado que esta información está contenida en las definiciones de virus. La actualización del Patrón de Definiciones de virus es vital y debe de hacerse como mínimo una vez a la semana. Otra de las piezas esenciales del Antivirus, el motor, también debe de actualizarse regularmente dado que los nuevos virus requieren en muchos casos nuevos motores de escaneo para poder detectarlos, por lo que la actualización del motor también es tarea obligada.

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.

Comentarios al respecto

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos necesarios en Centro de Datos, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

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 (1D-GAR-I39 y 1D-GAR-I046) y se solicita de forma física, por medio del formato 1D-GAR-F175 o formato virtual desde la mesa de servicios.	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 administrativa 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.
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.

Comentarios al respecto

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de ocho (8) caracteres alfanuméricos, y. No se permiten claves en blanco. Además están registrados en el dominio activo, a través del cual se otorgan los permisos de acuerdo a sus responsabilidades. Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o en su defecto, el sistema se bloquea después de 10 minutos de inactividad.

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, existe un único funcionario con autorización para administrar por componente TI (Uno para Base de datos, uno para Sistemas de Información, uno para Servidores, etc.)	Es importante autorizar un administrador del sistema alterno para cada componente, con la suficiente capacitación y los permisos requeridos, en caso de que falte el funcionario del Grupo de Infraestructura o de Sistemas de Información, para evitar que los procesos de la entidad se vean paralizados.
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.	El funcionario administrador principal impartirá las debidas instrucciones al administrador alterno.
El administrador alterno necesitara conocer el inventario actualizado de los elementos con que se cuenta en la Entidad, en caso de una contingencia.	Realizar depuración al inventario de sistemas, manteniéndolo al día periódicamente. Hacer llegar la información depurada a los funcionarios asignados.
Aunque se ha diagramado un esquema general de la Red	Realizar el diagrama lógico de la red y revisar la

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.	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.

EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

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

RIESGO	EVENTO
• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht. • Fallas Punto Patch Panel. • Fallas Punto de Red.	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR
• Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco • Computador de Escritorio funciona como Servidor	FALLAS EN UN SERVIDOR
• Incapacidad • Accidente • Renuncia Intempestiva	AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE TECNOLOGÍA DE LA INFORMACIÓN.
• Corte General del Fluido eléctrico	INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
• Falla de equipos de comunicación: SWITCH, Antenas, • Fibra Óptica. • Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet.	PERDIDA DE SERVICIO DE INTERNET Y/O CONECTIVIDAD GENERAL.
• Incendio • Sabotaje	INDISPONIBILIDAD DEL CENTRO DE DATOS (DESTRUCCIÓN DE LA SALA DE SERVIDORES)

• Corto Circuito • Terremoto	

NO HAY COMUNICACIÓN ENTRE CLIENTE – SERVIDOR EN LA SECRETARIA DISTRITAL DE GOBIERNO

- ✓ Requerimiento del usuario, que no cuenta con acceso a la red.
- ✓ El personal de Mesa de Servicios procederá a identificar el problema.
- ✓ Si se constata problema con el Patch Panel, realizar cambio del mismo.
- ✓ Si no se resuelve el problema proceder a constatar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma.
- ✓ Si persiste el problema revisar los puntos de red, utilizando el diagrama lógico.
- ✓ Probar el cable UTP. Si existe daño, realizar el cambio del cable.
- ✓ Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones
- ✓ Recuperación del sistema de red para el usuario.

Recursos de Contingencia

- ✓ - Componentes de Remplazo:
- ✓ - Diagrama Lógico de la red

FALLAS DE UN SERVIDOR

Se puede producir pérdida de hardware y software, perdida del proceso automático de Backup y restore e Interrupción de las operaciones. A continuación se describen algunas causas del fallo en un Servidor:

Error Físico de Disco de un Servidor

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- ✓ Ubicar el disco malogrado.
- ✓ Avisar a los usuarios que deben salir del sistema, utilizar correo grupal y aviso telefónico a jefes de área y personal relacionado.
- ✓ Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- ✓ Bajar el sistema y apagar el equipo.
- ✓ Retirar el disco con deficiencias y reponerlo con otro del mismo tipo, formatearlo y configurar su particionamiento.
- ✓ Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- ✓ Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
- ✓ Habilitar las entradas al sistema para los usuarios.

Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
- En caso de daño físico, reconocer la tarjeta física malograda y reemplazarla con una de iguales características

Error de Tarjeta(s) Controladora(s) de Disco

Para los errores de cambio de Memoria RAM o Tarjeta Controladora de disco se deben tomar las siguientes acciones:

- Avisar a los usuarios que deben salir del sistema, utilizar correo grupal y aviso telefónico a jefes de área y personal relacionado.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar la posición de la pieza a cambiar.
- Retirar la pieza con sospecha de deterioro y tener a la mano otra igual o similar.
- Retirar la conexión de red del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

Nota: Todo cambio interno a realizarse en los equipos servidores será fuera de horario de trabajo fijado por la entidad, a menos que la dificultad apremie, cambiarlo inmediatamente.

Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna falla en los servidores de los sistemas de información de la Secretaría Distrital de Gobierno; se debe tener en cuenta:

- Verificar el suministro de energía eléctrica.
- Deshabilitar el ingreso de usuarios al sistema.
- Realizar backup de archivos contenidos en el servidor, a excepción de la carpeta raíz.
- Contar con un equipo de respaldo que permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.
- Al término de la operación de reparación se procederá a revisar que las bases de datos e índices estén correctas, para ello se deben ejecutar los sistemas de información y así poder determinar si el usuario puede hacer uso de ellos inmediatamente. Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

Recursos de Contingencia

- - Componente de Remplazo (Memoria, Disco Duro, etc.).
- - Backup diario de información del servidor

AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN.

- Directriz del Director de Planeación (escrita o vía Email) para que el Administrador alterno se encargue del centro de cómputo de la Secretaria especificando el periodo de asignación.
- Obtener la relación de los Sistemas de Información con los que cuenta la Secretaria Distrital de Gobierno, detallando usuarios, en que equipos se encuentran instalados y su utilidad.
- Conocer la ubicación de los backups de información.
- Contar con el diagrama lógico de red actualizado.

Recursos de Contingencia

- Manual de funciones actualizado del Grupo de Infraestructura de la Secretaria Distrital de Gobierno.
- Relación de los sistemas de información de la Secretaria.
- Diagrama lógico de la Red de Datos de la Secretaria Distrital de Gobierno actualizado.

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.

- Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
- Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones, para que no corten bruscamente el proceso que tienen en el momento del apagón.

- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de UPS a corriente normal (Corriente brindad por la empresa eléctrica).

Recursos de contingencia
Asegurar que el estado de las baterías del UPS, se encuentren siempre cargadas.

PERDIDA DE SERVICIO INTERNET Y/O CONECTIVIDAD GENERAL

- Realizar pruebas para identificar posible problema dentro de la entidad
- Si se evidencia problema en el hardware, se procederá a cambiar el componente
- Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor
- Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
- Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
- Realizar pruebas de operatividad del servicio.
- Servicio de Internet activo.

Recursos de Contingencia

Hardware:

- - Router
- - Software
- - Herramientas de Internet.

DESTRUCCION DEL CENTRO DE CÓMPUTO

- Contar con el inventario total de sistemas actualizado.
- Identificar recursos de hardware y software que se puedan rescatar.
- Salvaguardar los backups de información realizados.
- Identificar un nuevo espacio para restaurar el Centro de Cómputo.
- Presupuestar la adquisición de software, hardware, materiales, personal y transporte.
- Adquisición de recursos de software, hardware, materiales y contratación de personal.
- Iniciar con la instalación y configuración del nuevo centro de cómputo.
- Restablecer los backups realizados a los sistemas.

PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

El costo de la recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los

equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 7 escala Richter o un incendio de magnitud controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

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 Planeamiento y Sistemas de Información: Verificara la labor realizada por el (los) Administrador(es) de Infraestructura.

Un Plan de Recuperación de Desastres se clasifica en tres etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

Actividades previas al desastre

Se considera las actividades de actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. 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 deberá tener una relación de los Sistemas de Información con los que cuenta, 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.

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).

- 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. 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).

Actividades durante el Desastre (Plan de Emergencias)

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

Plan de Emergencias

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 la acción del siniestro causen más daños o destrucciones.

- Se debe tener en toda Oficina 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.

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 Contabilidad, Tesorería, Presupuesto y demás Sistemas de Información 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 iniciaran 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 Contingencias y Seguridad de Información, 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.

CONCLUSIONES

El presente Plan de contingencias y Seguridad en Información 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 el Área de Sistemas.

El Plan de Contingencia, es un conjunto de procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir su funcionamiento continuo, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo. Que una Entidad prepare su Plan de Contingencia, supone un avance a la hora de contrarrestar cualquier eventualidad, que puedan acarrear importantes pérdidas y llegado el caso no solo materiales sino personales y de 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.

RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, 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.

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.

DOCUMENTOS RELACIONADOS

Documentos internos

CÓDIGO SIG	NOMBRE DOCUMENTO
GDI-TIC-P001	Procedimiento para la gestión de servicios y tecnologías de la información y las comunicaciones

Normatividad vigente

NORMA	AÑO	EPÍGRAFE	ARTÍCULO(S)
N/A	N/A	N/A	N/A

Documentos externos

NOMBRE	FECHA DE PUBLICACIÓN O VERSIÓN	ENTIDAD QUE LO EMITE	MEDIO DE CONSULTA
N/A	N/A	N/A	N/A