CONTRALORÍA
DE BOGOTÁ, D.C.

PLAN DE CONTINGENCIAS

SISTEMAS DE INFORMACIÓN

DICIEMBRE 2009

CONTRALORÍA
DE BOGOTÁ, D.C.

TABLA DE CONTENIDO

CONTRALORÍA
DE BOGOTÁ, D.C.

INTRODUCCIÓN

La Contraloría de Bogotá D.C. considera que la información es el patrimonio principal de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

El Plan de Contingencias Informático que se encuentra en el presente documento , fue adoptado mediante la Resolución Reglamentaria No. 059 de diciembre 30 de 2003 "Por la cual se adopta el Plan de Contingencias para los Sistemas de Información de la Contraloria de Bogotá, D.C. y se dictan otras disposiciones" , es un conjunto de procesos, procedimientos y recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro, teniendo como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto en la organización y en el ejercicio del Control Fiscal.

El literal "a" del Artículo 2º. de la Ley 87 de Noviembre 29 de 1993 indica que uno de los objetivos fundamentales del Sistema de Control Interno, consiste en proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten. Así mismo señala en su literal "e", la adopción de normas para la protección y utilización racional de los recursos. Como complemento, asesorar a la dirección en la continuidad del proceso administrativo como parte de su gestión y haciendo adherencia a la definición indicada en el artículo 9º. de la misma ley.

Esta exigencia legal sugiere que las dependencias de Informática y/o telemática de las entidades del orden Distrital (para nuestro caso), definan y documenten planes, normas y procedimientos que permitan la adecuada continuidad de las operaciones en caso de presentarse contingencias o situaciones de emergencia en los sistemas informáticos de las entidades gubernamentales.

El Plan está basado en un proceso dinámico y continúo que incluye no sólo las actividades a realizarse en el evento de una interrupción de la capacidad de procesamiento de datos; sino además, en las actividades realizadas anticipando dicho evento.

Una actividad principal del plan, es evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un "desastre" ocurra.

Otra actividad es facilitar la recuperación en el evento de un desastre. Para lo cual, la fase de recuperación provee tres propósitos:

1. Los roles individuales (de ejecución, coordinación y toma de decisiones) deben ser entendidos y atendidos en el contexto de todo el plan.
2. Existe la necesidad de establecer y mantener las descripciones de los procedimientos a ser realizados en el evento inesperado.
3. El plan permite un repaso administrativo, al evaluar la perfección y exactitud de cada proceso y repasa los procedimientos de recuperación sobre la marcha.

En ese sentido, El PLAN DE CONTINGENCIAS INFORMATICO se convertirá en la carta de navegación, contemplando:

- La estructura de una organización jerárquica paralela para administrar las emergencias, con mecanismos de notificación claramente definidos.
- Definición de escenarios.
- Diseños de programas de almacenamiento y estrategias.
- Detalle de la administración general del Plan.
- Establecimiento de procedimientos contingentes, organización de grupos de trabajo, funciones y responsabilidades, involucrando usuarios y administradores.

1. OBJETIVOS

Plantear y dotar a la Contraloría de Bogotá, D.C. de los procedimientos y elementos mínimos requeridos para afrontar la contingencia relacionada con el eventual cese de actividades, inoperatividad de equipos causada por razones de fuerza mayor.

Proveer una solución para mantener operativos los sistemas de información y electrónicos fundamentales de la institución, que permitan reducir el impacto en las operaciones normales cuando son interrumpidos o paralizados por contingencias que afectan parcial o totalmente las instalaciones donde se procesan aplicaciones automatizadas y los servicios de procesamiento de datos de la entidad.

Cuantificar la exposición a pérdidas asociadas a cada sistema de información automatizado y/o recursos informáticos con que cuenta la entidad, permitiendo un análisis de riesgos comprensible de los sistemas, que sirva como guía durante la ejecución del plan.

Minimizar la posible pérdida financiera y operativa en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes. Así mismo, reducir las consecuencias de la posible pérdida de información relacionada con el evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.

Mantener la prestación del servicio a los usuarios, en el nivel aceptable.

Restablecer las operaciones del Centro de Cómputo en menos de 5 días hábiles, seguidos de cese, dependiendo de la anomalía que se presente.

Asegurar la concordancia con otras regulaciones locales, distritales y estatales.

2. VENTAJAS POTENCIALES

El hecho de tener estructurado el plan de contingencias para el área de informática y los sistemas de información de la CONTRALORIA DE BOGOTA D.C., tiene algunas ventajas potenciales que ayudan a prevenir o a disminuir el impacto de los siniestros. Algunas de estas ventajas permiten:

- Determinar acciones preventivas que reduzcan el grado de vulnerabilidad; por el conocimiento que se tiene de los sistemas automatizados de información.
- Cuantificar los riesgos potenciales a que están expuestos los sistemas de información.
- Facilitar la oportuna toma de decisiones ante anomalías o fallas.
- Contribuir a generar una cultura de seguridad y control en las áreas de sistemas e institucionalmente, haciendo énfasis en el manejo de la información.
- Asegurar la estabilidad operativa y de la organización, frente a la evidencia de un siniestro.
- Medir el grado de seguridad en los sistemas de información institucionales.

3. ALCANCE

La necesidad de desarrollar un plan de contingencias, está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios electrónicos y procesamiento de la información, sobre el normal desarrollo de las actividades de la CONTRALORIA DE BOGOTA; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

Lo que supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, Software y Equipos electrónicos involucrados en los procesos críticos definidos en el Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del Centro de Cómputo principal de la entidad.

Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los grupos contingentes establecidos para la ejecución del Plan, y dependen de la diligencia y colaboración de las dependencias usuarias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

El desarrollo de las actividades y proyectos, está condicionado a la aprobación de los mismos por parte del Comité de Informática a través del Director de Informática.

4. METODOLOGÍA

Si las operaciones y procesos más importantes se encuentran automatizados en la CONTRALORIA DE BOGOTA D.C., significa que el área de informática es de gran relevancia para el funcionamiento de la misma, lo cual obliga a la consideración de los siguientes aspectos:

El tiempo durante el cual la entidad puede funcionar sin sus recursos computacionales en operación.

La identificación de las amenazas potenciales sobre la capacidad de procesamiento automatizado de la información en la entidad.

La identificación de las aplicaciones críticas que deben ser procesadas mientras se restablecen las operaciones normales en la entidad.

Identificación de las consecuencias operativas, estratégicas, legales o de servicio, por la carencia del servicio automatizado.

El valor de la inversión en el desarrollo del plan de contingencias que asegure su continuidad y normal funcionamiento.

El Plan se ha estructurado en tres grandes Fases, a saber:

1) **Fase de Mitigación:** La Contraloría, asegura la conservación de su información vital y determina donde procesar sus trabajos críticos de procesamiento de datos, sistemas o aplicaciones automáticas críticas, en caso de falla de sus equipos o de los mismos aplicativos.
2) **Fase de Emergencia:** Contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia.
3) **Fase de Recuperación:** Permite restablecer las condiciones originales y operación normal de los sistemas de información en su conjunto.

Los cuales implican el desarrollo de las siguientes Etapas:

1) Revisión: comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones de la misma.

2) Valuación del impacto por interrupción del servicio: comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones. Esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla el análisis de riesgos.

3) Implementación: se realizan actividades específicas para la reducción y eliminación de riesgos que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.

a) **Cronograma:** El diseño de un cronograma de trabajo provee la oportunidad de registrar los logros de cada tarea, verificar si las actividades han sido cumplidas o no en el tiempo previsto, y analizar cuáles han sido los principales inconvenientes que se han presentado si se detectan desviaciones importantes en el cronograma inicial, antes de la ejecución de las pruebas.

b) **Documentación:** Se prepararán y archivarán todos los documentos donde se registren las actividades, logros e inconvenientes, programas, objetivos, cronograma, procedimientos, planillas y todo aspecto fundamental referente a las acciones generadas durante el desarrollo del Plan de Contingencias, creando un historial de referencia.

4) **Simulación o simulacro:** se define el cronograma de simulacros, así como se designa a los responsables de dar inicio a las pruebas, ambientar el personal y los recursos, controlar los eventos, documentar las acciones y evaluar el resultado en su conjunto.

5) **Ejecución:** se sigue el desarrollo de:
   a) Medidas de protección planificadas por cada segmento afectado.
   b) Iniciación de las acciones destinadas, por prioridad, a controlar la situación durante los primeros instantes de la emergencia.
   c) Consideración de las responsabilidades extraordinarias que el comité directivo del plan tendría que asumir a fin de ofrecer protección y seguridad a los elementos materiales y humanos del área.
   d) Evaluación del estado del área de informática, poniendo en operación los procedimientos planificados para la recuperación total del servicio.

5. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

5.1 DEFINICIÓN

RIESGO es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad, azar o exposición.

5.2 DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos implica la valuación del impacto por interrupción del servicio, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones; esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal de los sistemas de información con que cuenta la Entidad, son entre otros:

5.2.1 Riesgos con Incidencia Externa

5.2.1.1 Políticos

Modificaciones a la constitución política ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

5.2.2 Riesgos con Incidencia Interna

5.2.2.1 Posible incumplimiento de los contratistas

Este riesgo puede ocurrir a causa del posible atraso en la ejecución o trasgresión del clausulado de los contratos de actualización, modificación, mantenimiento, que se asumieron durante la vigencia del 2002; para la aplicación de Nómina, el Sistema de Información Financiera MOISÉS.

5.2.2.2 Posibles retrasos en Procesos Administrativos

La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos con exigencia en el cumplimiento de requisitos, ampliando el tiempo de ejecución de las actividades del Plan Emergente, de manera imprevista.

5.2.2.3 Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles

Se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas, y con el probable desconocimiento de las características y especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas, de manera compatible.

5.2.2.4 Posible pérdida de información

Este riesgo tiene baja probabilidad de ocurrencia, si se tiene en cuenta que el Plan de Contingencias incluye un proceso de respaldo, que permite la mitigación del riesgo, efectuando copias de seguridad (backups), tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros) como a los archivos de bases de datos y resultados de las aplicaciones específicas en producción para cada una de las dependencias de la Entidad.

5.2.2.5 Posible falla de equipos electrónicos y Hardware fuera de inventario

Este riesgo se presenta por la Falta de Previsión, con la no inclusión de soluciones para aspectos de baja prioridad o al excluir elementos de los inventarios, por desconocimiento o por no haber sido reportados a tiempo a la Dirección de Informática.

5.2.2.6 Posibles Fallas en el Flujo de Energía Eléctrica

Este riesgo está relacionado con amenazas externas al control de la Entidad. Sin embargo, se han implementado equipos para la mitigación del riesgo de corte temporal de energía eléctrica, dado que la Contraloría de Bogotá está provista de UPS (Unidad de Poder In-interrumpido) en cada una de las redes de área local, para tener la posibilidad de salvaguardar la información durante aproximadamente una (1) hora. Si el corte es más prolongado, se debe acudir a los procedimientos de procesamiento en el centro alterno externo y en segunda instancia los procesos manuales establecidos como contingencia, hasta tanto no se solucione la falla.

La UPS actual funciona y cumple con su objetivo y tiene contrato de mantenimiento

5.2.2.7 Posible Calentamiento de la Sala de Cómputo

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la Contraloría ha implementado procedimientos para su mitigación, tales como: La implementación en el centro de cómputo principal (piso 7º) de un Sistema de Temperatura autorregulada "LIEBERT Challenger 3.000", provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura, humedad, flujos de corriente, filtros de aire, alarmas local y silenciosa. Este sistema se encuentra conectado con la cámara principal a través de conductos que están debajo del piso falso para el control de los flujos de corriente y aire, y en el techo está provisto de detectores de humo y fuego que accionan un sistema de alarmas y descarga automática de gases que apagan llamas originadas en el salón de la UPS y cuarto de computadores.

5.2.2.8 Posible Falla del Servicio Telefónico

Este riesgo está relacionado con amenazas externas al control de la Entidad, la Contraloría no puede efectuar mitigación de este riesgo. Sin embargo, se puede planear las posibles alternativas a implementar ante las posibles fallas del servicio

telefónico. La probabilidad de ocurrencia sólo es manejable por la entidad proveedora del servicio.

El impacto sobre las operaciones de la Contraloría de Bogotá es de nivel bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales implementada sobre cableado estructurado.

De otro lado, en lo que respecta al Centro de Cómputo principal de la Contraloría de Bogotá, se desarrolló un análisis del medio y los procedimientos de seguridad y control existentes.

El análisis indicó que la Entidad está en una posición favorable por lo siguiente:

1 El edificio no se encuentra en una zona que pueda presentar inundación.
2 El centro de cómputo está ubicado estratégicamente en el piso 7 del edificio sede.
3 Posee detectores de humo y fuego que accionan un sistema de alarmas y de descarga automática de gases que apagan las llamas originadas en el salón de la UPS y cuarto de computadores.
4 El acceso al software es restringido y se encuentra almacenado en un lugar seguro y adecuado.
5 El cielo raso y pisos del centro de cómputo son de material no combustibles.
6 El centro de cómputo está provisto de una Temperatura autoregulada y UPS.

6. IDENTIFICACION DE PROCESOS CRITICOS

6.1 CRITERIOS PARA IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Los planes de contingencia se consideran "requeridos" para todos los sistemas de prioridad 1, "recomendables" para todos los sistemas de prioridad 2 y "sugeridos" para todos los sistemas de prioridad 3.

6.1.1 Prioridad 1

- Todos los sistemas vitales de la organización

6.1.2 Prioridad 2

- Sistemas con múltiples interfaces.
- Sistemas o dispositivos que no pueden ser sometidos a pruebas.
- Sistemas que alimentan datos a los sistemas vitales.

6.1.3 Prioridad 3

- Sistemas cuya falla causa molestias menores

6.2 FACTORES CRÍTICOS A CONSIDERAR

6.2.1 Aplicaciones en Producción

1 Nivel de importancia de la aplicación en la entidad
2 Impacto operativo, financiero o contable
3 Oportunidad de procesamiento
4 Programas críticos
5 Comunicaciones: entrada y salida de datos
6 Implicaciones para el usuario en caso de ausencia del recurso aplicativo.
7 Documentación del sistema: manuales de usuario y procedimientos de operación.
8 Procedimientos de respaldo y recuperación a nivel aplicativo.

6.2.2 Personal

1 Funcionarios de posición clave y personal de dirección
2 Personal con alta dependencia en los sistemas automatizados
3 Personal de respaldo
4 Entrenamiento

6.2.3 Parque computacional y aplicaciones en uso

1 Servidores, computadores personales, impresoras, periféricos, etc.
2 Líneas de comunicación y equipos relacionados.
3 Sistemas operativos y programas producto.
4 Suministros: papel, formas continuas, medios magnéticos y formas especiales.

5 Archivos maestros y de movimiento considerados críticos de respaldo de los mismos.

6.3 NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

Teniendo en cuenta los criterios y factores enunciados anteriormente, se han definido los siguientes niveles de prioridad y criticidad de los recursos informáticos con que cuenta la Contraloría de Bogotá:

6.3.1 Prioridad Alta

Corresponde a todas aquellas herramientas de la Contraloría, que en el caso de no ser adaptadas oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar la actividad del Control Fiscal.

6.3.2 Prioridad Media

Se le asigna a todas aquellas herramientas de la Contraloría, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de control, cuentan con procedimientos alternativos preestablecidos.

6.3.3 Prioridad Baja

Se le asigna a todas aquellas herramientas de la Contraloría, cuya falta de adaptación no representa graves traumatismos y sus modificaciones pueden aplazarse para la última parte del proyecto.

6.3.4 Criticidad A: (Máxima)

No puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas

6.3.5 Criticidad B: (Intermedia)

No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles. Puede sustituirse parcialmente por un período, por un proceso manual.

6.3.6 Criticidad C: (Mínima)

Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles. Puede sustituirse temporalmente por un proceso manual.

6.4 PROCESOS CRÍTICOS

Con base en lo anterior, se establecieron los Procesos Críticos de la Contraloría de

Bogotá, descritos en la siguiente relación de recursos informáticos señalando la prioridad y las acciones a seguir para cada problemática en particular.

6.4.1 SOFTWARE

6.4.1.1 Software Aplicativo

6.4.1.1.1 Aplicaciones de Desarrollo Externo

Se determinó que las aplicaciones en producción que presentan un alto riesgo de pérdida de información y que pueden provocar parálisis en los procedimientos administrativos (en caso de no ser debidamente adecuadas), son aquellas elaboradas e implementadas a través de procesos contractuales; por lo tanto, serán objeto de inmediata solución.

6.4.1.1.2 Aplicaciones de Desarrollo Interno

La Dirección de Informática ha desarrollado aplicaciones que actualmente operan en la entidad, para las cuales se ha iniciado procesos de adecuación y prueba bajo la responsabilidad de ingenieros asignados a esta Dirección.

El diagnóstico del software aplicativo y procesos críticos se muestran en el Anexo 1.

6.4.2 HARDWARE

6.4.2.1 Microcomputadores

La Contraloría cuenta en la actualidad con 831 Computadores personales: 685 y computadores portátiles 146; 262 impresoras y 20 scaners, distribuidos como se presenta en el siguiente cuadro:

Cuadro 1
DISTRIBUCIÓN DE EQUIPOS DE CÓMPUTO POR MARCA

EQUIPOS ACTIVOS CONTRALORIA DE BOGOTA

MARCA	TIPO	MODELO	PROCESADOR	MEMORIA RAM	CANTIDAD
IBM	ESCRITORIO	THINK CERTRE A50	PENTIUM IV DE 2,8	1GB	140
IBM	ESCRITORIO	THINK CERTRE A50	PENTIUM IV DE 2,8	1 GB	158
DELL	PORTATIL	LATITUD 505	PENTIUM IV DE 1,6	256 MB	15
DELL	PORTATIL	LATITUD 610	PENTIUM M DE 2,1	512 MB	65
DELL	ESCRITORIO	GX520	PENTIUM IV DE 3,2	512 MB	210
HP	PORTATIL	NC6230	PENTIUM M DE 2,0	1 GB	53
TOSHIBA	PORTATIL	L300	COR DUO 1.8	1GB	8
TOSHIBA	PORTATIL	A210	COR DUO 1.8	1 GB	2
HP	PORTATIL	PAVILION	COR DUO 1.8	1 GB	3
HP	ESCRITORIO	DX2000	PENTIUM 4 DE 3,2	1 GB	177
				TOTAL	**831**

.:

IMPRESORAS ACTIVAS CONTRALORIA DE BOGOTA

MARCA	MODELO	CANTIDAD	OBSERVACIONES
LEXMARK	T630	18	
LEXMARK	T760	1	
LEXMARK	T420	44	
HP	5500	1	
HP	4600	1	
HP	2200	20	LOCALIDADES
HP	8150	1	
EPSON	2190	10	
DELL	3000CN	40	
DELL	5200DTN	30	
HP	2430	33	
HP	1320	45	
HP	1100	1	JURIDICA
HP	1500	1	GUIOMAR
PINTRONICS	5210	1	INFORMATICA
HP	880C	1	PISO 14
HP	840C	1	PISO 13
HP	720C	1	AUDITORIA

CANON	*1310*	*1*	DESPACHO
CANON	*BJ10X*	*1*	INFRAESTRUCTURA
HP	*2100*	*2*	TALENTO HUMANO Y SERVICIOS PUBLICOS
HP	*6MP*	*3*	
HP	*1200*	*1*	
HP	*8100*	*4*	
	TOTAL	**262**	

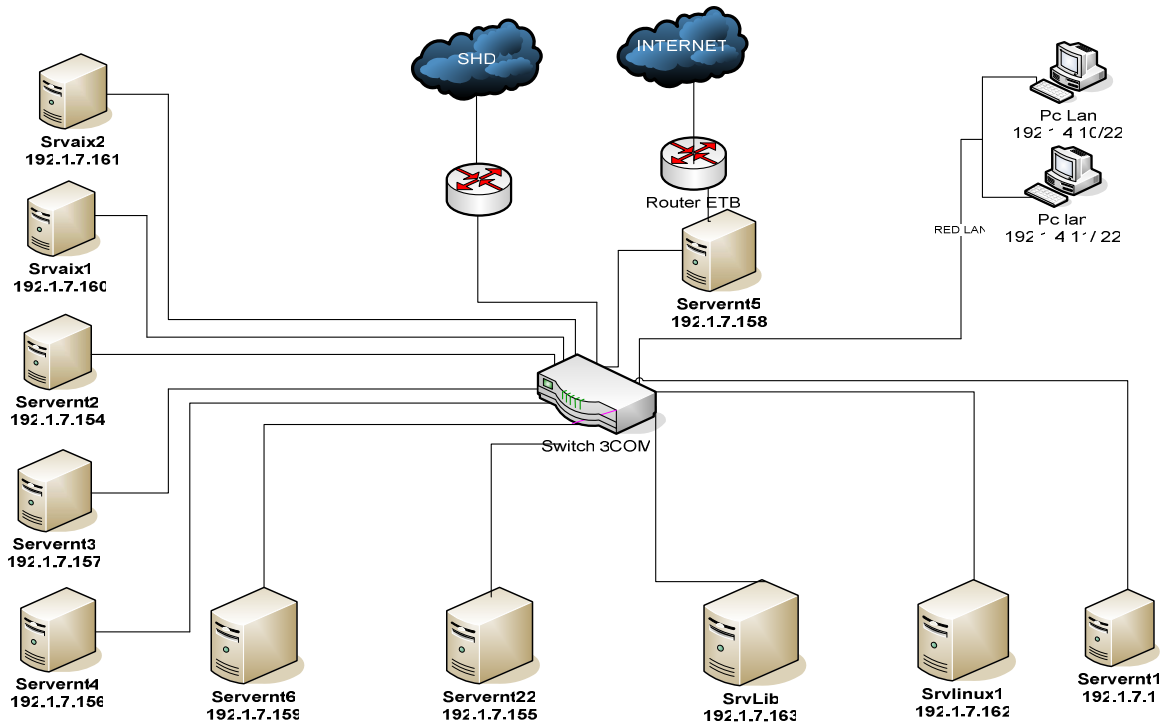
SCANER ACTIVAS CONTRALORIA DE BOGOTA

MARCA	***MODELO***	***CANTIDAD***	***OBSERVACIONES***
KODAK	*I65*	*2*	
KODAK	*I40*	*14*	
EPSON		*3*	
HP	*8250*	*1*	

Fuente: Dirección de Informática

6.4.2.2 Equipos Servidores

DIAGRAMA DE RED CONTRALORIA DE BOGOTA



A continuación se muestra la actualización de infraestructura tecnológica de servidores que hacen parte de la red de la Contraloría.

SERVIDOR NOMINA (192.1.7.1)

- **Características**

  - Dell Power edge 6850
  - Procesador 3.66 Ghz(1MB Cache, Xeon Dual Processor
  - 4 Gb RAM
  - (2) de 146GB, U320, SCSI, 1IN 10KI,PE68X0
  - SO: Windows 2003

- **Servicios**

  - Servidor de Nomina

SERVIDOR SERVERNT2 (192.1.7.154)

- **Características**
    - DELL PowerEdge SC430
    - Procesador Pentium IV 2.8 Mhz
    - SO: Windows 2003 Server
    - 512 Mb RAM
    - 74.5 GB HD
- **Servicios**
    - Microsoft SQL Server 2000
    - Servidor de aplicaciones ASP y ASP.NET
    - Cliente TIVOILI
    - Servidor Intranet

SERVIDOR Servernt22 (192.1.7.155)

- **Características**
    - IBM MT-M 8149
    - Procesador Pentium IV 2.8 GHz
    - 760 GB RAM
    - 80 GB HD
    - SO: Windows 2003 Server
- **Servicios**
    - Servidor BMC Patrol

VULNERABILIDADES

SERVIDOR SERVERNT4 (192.1.7.156)

- **Características**

    - Compaq Proliant DL580
    - Procesador Pentium III Xeon 700 MHz (2)
    - 2 GB RAM
    - 80 GB HD
    - SO: Windows 2000 Server

- **Servicios**

    - Servidor de Dominio Principal (Contraloría.gov.co)
    - Servidor de Correo (Exchange 2000 Server)

SERVIDOR SERVERNT3 (192.1.7.157)

- **Características**

    - Compaq Proliant DL580
    - Procesador Pentium III Xeon 700 MHz (2)
    - 2 GB RAM
    - 80 GB HD
    - SO: Windows 2000 Server

- **Servicios**

    - Servidor de Aplicaciones
    - Consola de Administración de Mcafee

SERVIDOR SERVERNT5 (192.1.7.158/192.1.7.168)

- **Características**

    - Compaq Proliant ML370
    - Procesador Pentium III Xeon 1.4 GHz (2)
    - 2 GB RAM
    - 36 GB HD
    - SO: Windows 2000 Server

- **Servicios**

    - Servidor de Internet
    - Servidor Proxy Cache
    - Servidor Websense

SERVIDOR Servernt6 (192.1.7.159/192.1.7.164)

- **Características**

    - IBM Xseries 336
    - Procesador Pentium IV Xeon 3.6 GHz
    - 3.25 GB RAM
    - 146.8 GB HD
    - SO: Windows 2003 Server

- **Servicios**

    - Servidor Oracle OAS
    - Servidor ERP_SHD

SERVIDOR Srvaix1 (192.1.7.160/192.1.7.165)

- **Características**

    - IBM PSeries 510
    - Procesador 1.65 GHz (2)
    - 8 GB RAM
    - 146.8 GB HD
    - SO: AIX basado en UNIX

- **Servicios**

    - DB2
    - DB_STORM
    - DB_GDOCS

SERVIDOR Srvaix2 (192.1.7.161/192.1.7.166)

- **Características**

    - IBM PSeries 510
    - Procesador 1.65 GHz (2)
    - 8 GB RAM
    - 146.8 GB HD
    - SO: AIX basado en UNIX

- **Servicios**

    - Servidor de Websphere Aplication Server ver 6.0

SRVLINUX1 (192.1.7.162/192.1.7.167)

- **Características**

    - IBM Xseries 336
    - Procesador Pentium IV Xeon 3.6 GHz
    - 3.25 GB RAM
    - 146.8 GB HD
    - SO: Linux Redhat ES 4

- **Servicios**

    - Servidor Sivicof

SERVIDOR Srvlib (192.1.7.163)

- **Características**

    - IBM Xseries 306
    - Procesador Pentium IV 3.2 GHz (2)
    - 2 GB RAM
    - 160 GB HD
    - SO: Windows 2003 Server

- **Servicios**

- Servidor de Librerías (TSM)
- Servidor TIVOLI

6.4.3 EQUIPOS ELECTRÓNICOS

Los equipos electrónicos no-informáticos con que cuenta el centro de cómputo que requieren ser ajustados o reemplazados, son:

- UPS: La Entidad cuenta con UPS marca IPM y APEL.
  La Contraloría no cuenta en la actualidad con contrato de mantenimiento preventivo ni correctivos para estos elementos. Las UPS IMP presentan problemas en cuanto a su autonomía de funcionamiento debido a que la vida útil de sus baterías se ha cumplido, lo que significa, que en eventual momento de corte del fluido eléctrico no se puede mantener los sistemas en funcionamiento.

- Sistemas de Alarmas
  El sistema de alarma contra incendios requiere ajustes en cuanto a su distribución debido a la remodelación a que fue sometido el Centro de Cómputo. No se tiene contrato de mantenimiento para este dispositivo.

6.4.4 EQUIPOS DE COMUNICACIONES

6.4.4.1 Infraestructura de Redes

La Entidad cuenta con 2 enlaces de radiofrecuencia para interconectar las sedes ubicadas en el Edificio Lotería de Bogotá, y Dirección de Generación de Tecnología. Al interior de la red se cuenta con una topología en estrella cuyo nodo principal esta ubicado en el piso 7, Centro de Computo del Edificio Lotería de Bogotá.

La estructura de la red maneja cableado UTP nivel 5 y 6 para su segmento horizontal con switchs en sus bordes y un Backbone de fibra óptica para su

segmento vertical que convergen en switch principal.

La Contraloría cuenta con una conexión a la red de la Secretaría de Hacienda la cual permite acceder a aplicaciones como PREDIS, PAC y SEGPLAN. Además se cuenta con acceso remoto al Sistema Integrado de Información Catastral-SIIC.

6.4.4.1.1 Sede Edificio Lotería de Bogotá

Ubicado en la Carrera 32 # 26a - 10. Pisos 1, 2 y 6 al 17. En los pisos hay cableado estructurado UTP, categoria 5 y 5E, para la red de voz y datos, cada piso cuenta con equipos activos (switches) y sus respectivos Patch Panel de tendido horizontal tanto como para voz como para datos, y cada piso cuenta con un Backbone de fibra óptica la cual se encuentra centralizada en el piso 7 donde funciona el centro de cableado principal.

6.4.4.1.2 Sede Bodega San Cayetano

Ubicada en la Calle 50 # 79-54. Cuenta con cableado estructurado UTP,categoria 5 y 5E, para la red de voz y datos, cuenta con equipos activos (switches) y sus respectivos Patch Panel de tendido horizontal tanto como para voz como para datos para los pisos 1, 2 y 3. La conexión con la sede principal se realiza a través de un canal corporativo de 512 KBPS, suministrado por la ETB.

6.4.4.1.3 Sede Dirección de Participación Ciudadana

Ubicada en la calle 27ª # 35-45. Cuenta con cableado estructurado UTP nivel 5 para los pisos 2 y 3. La conexión con la sede principal se realiza a través de un enlace de radiofrecuencia.

6.4.4.1.4 Sede Oficinas Asesoras de Asuntos Disciplinarios y Control Interno

Ubicada en la calle 24 # 35-17. En los pisos hay cableado estructurado UTP, categoria 6, para la red de voz y datos, (se aclara que hay elementos de conectividad como jacks, patch cords en categoría 5 y 5E) cuenta con equipos activos (switches) y sus respectivos Patch Panel de tendido horizontal tanto como para voz como para datos La interconexión de esta sede con el Edificio Lotería de Bogotá se realiza a través de un canal corporativo de 512 KBPS, suministrado por la ETB.

6.4.4.2 Hardware de Comunicaciones

En el siguiente cuadro se muestra el Consolidado de Recursos por Sede, relacionando los puntos de red, enlaces de radiofrecuencia y switches de cada uno de los edificios:

Cuadro 2
DISTRIBUCIÓN DE DISPOSITIVOS DE COMUNICACIONES

SEDE	PUNTOS DE RED	ANTENAS RADIOFRECUENCIA	SWITCHES
Lotería de Bogotá	922	1	- 1 Switch de Backbone 3COM 4007 Layer 2 - 30 switchs de borde 3COM SuperStack 3
Participación Ciudadana	39	1	1 Concentrador 3COM SuperStack 3
Control Interno y Asuntos Disciplinarios	54	Canal corporativo de 512 KBPS suministrado por la ETB	1 Concentrador 3COM SuperStack 3
Bodega San Cayetano	33	Canal corporativo de 512 KBPS suministrado por la ETB 1	1 Concentrador 3COM SuperStack 3

Fuente: Centro de Computo- Dirección de Informática

7. DEFINICION Y CONFORMACION DEL GRUPO DE TRABAJO

Para dar cumplimiento al desarrollo del plan de contingencias en las áreas de sistemas de la entidad, es necesario tratarlo como un proyecto. Por esta razón, se conformarán el comité directivo y el grupo de desarrollo, ambos responsables del plan. Se sugiere la estructuración del grupo encargado del desarrollo, implantación y mantenimiento del plan de contingencias.

7.1 COMITÉ DIRECTIVO

Conformado por funcionarios de nivel directivo de la Contraloría de Bogotá, quienes participan en el Comité de Informática:

- Contralor de Bogotá
- Contralor Auxiliar
- Director de Apoyo al Despacho
- Director de Planeación

- Director de Generación de Tecnología, Cooperación Técnica y Capacitación
- Director de Informática
- Director Administrativo y Financiero
- Director de Control Interno
- Representante de las Direcciones Sectoriales.

7.1.1 Responsabilidades

- Definir los lineamientos del plan de contingencias para las áreas de informática de la Contraloría de Bogotá.
- Orientar y evaluar el desarrollo e implantación del plan.
- Ejercer un control documentado y un seguimiento formal al proyecto.
- Estudiar, evaluar y decidir sobre los requerimientos que se presenten en el desarrollo e implantación del plan.
- Recomendar acerca de la adquisición o el mantenimiento de equipos, programas e instalaciones.
- Coordinar el desarrollo, implantación y mantenimiento del plan de contingencias.
- Supervisar el cumplimiento de las labores asignadas al grupo de desarrollo del plan.

- Estudiar, evaluar y decidir sobre los requerimientos o recomendaciones planteadas por el grupo de desarrollo.
- Efectuar seguimiento y controlar los costos que se incurren en el desarrollo, implantación y mantenimiento del plan.
- Aprobar el establecimiento de convenios, contratos o adquisición de recursos para el plan.
- Organizar y disponer los recursos para el grupo de desarrollo del plan.

7.2 COORDINADOR DEL PLAN DE CONTINGENCIAS

El Coordinador del Plan es el Canal de Comunicación entre el Grupo de Desarrollo del plan y el Comité Directivo, a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan de Contingencias, los niveles de ejecución del Plan y el estado de los Recursos Informáticos que cubre el Plan.

Así mismo, debe encargarse de monitorear y asegurar el cumplimiento estricto del

Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo. Proveer los recursos necesarios y notificar las decisiones a los funcionarios delegados.

El Coordinador del Plan de Contingencias es el Director de Informática de la Contraloría de Bogotá y en su ausencia el Ingeniero que delegue, integrante de la Dirección de Informática y perteneciente al Grupo de Centro de Computo, dado el tipo de labores especificas a desarrollar dentro del plan (realización de copias de seguridad y restauración de las mismas) labores que son compatibles con las tareas cotidianas que desarrolla este grupo.

7.3 GRUPO DE DESARROLLO DEL PLAN

Está conformado por funcionarios de nivel medio, responsables de la ejecución de las áreas definidas dentro del plan. El grupo estará conformado por personal de las áreas administrativas y operativas de sistemas automatizados (funcionarios usuarios finales encargados del manejo de aplicaciones y equipos de computo), el grupo de centro de cómputo, grupo de soporte técnico y grupo de análisis y desarrollo de la Dirección de Informática y el apoyo del grupo de Salud Ocupacional de la Contraloría de Bogotá. Ellos han sido delegados y encargados por los niveles directivos de cada una de las áreas usuarias. Grupo de Desarrollo del Plan, en ella se define la asignación específica de cada funcionario en el subgrupo que le corresponda.

Funciones

- Ejecutar, en tiempo y forma, cada una de las actividades planeadas.
- Documentar y formalizar el plan de contingencias.
- Ordenar la documentación inherente y los papeles de trabajo del proyecto.
- Diseñar planes de entrenamiento para los funcionarios de la entidad, a todo nivel, para que se involucren en las tareas del plan.
- Diseñar cronogramas y apoyar logísticamente las pruebas de cada segmento del plan.
- Mantener operativo y debidamente actualizado el plan de contingencias.

El Coordinador del Plan y los funcionarios de la Dirección de Informática, elaborarán el plan de trabajo para el desarrollo e implantación del proyecto.
Así mismo, se conformarán los siguientes subgrupos de trabajo para la ejecución

del Plan.

7.3.1 Subgrupo de Atención de Emergencias

Conformado por un representante del Grupo de Salud Ocupacional, el jefe de piso del área afectada o su suplente y el responsable (o su suplente) del procedimiento a seguir según el aspecto afectado; estas personas son las designadas por el Contralor Auxiliar en el Programa de Salud Ocupacional. Este grupo se encargará de activar las medidas necesarias para salvaguardar los recursos humanos y materiales en caso de emergencias.

7.3.2 Subgrupo de supervisión

Conformado como mínimo, por personal del área afectada encargados de la operación de sistemas automatizados, el cual prestará apoyo e información al grupo de atención de emergencias, si así lo amerita. Encargándose, así mismo, de supervisar la situación del segmento no afectado por el siniestro en el momento de la contingencia y de informar al ingeniero de la Dirección de Informática coordinador de los sistemas afectados, para que apoye las labores de supervisión, dirija, participe en la ejecución del plan y la soporte técnicamente.

7.3.3 Subgrupo de evaluación de daños

Conformado por los mismos funcionarios del subgrupo de supervisión con el apoyo de los ingenieros del grupo de soporte de la Dirección de Informática, quienes se encargarán de la revisión de la planta física, identificando los daños físicos y lógicos (Hardware y Software) originados durante la contingencia, para luego, informar los resultados al grupo de desarrollo.

7.3.4 Subgrupo de Reorganización

Conformado por los funcionarios del área; que forman parte del grupo de desarrollo, el cual se encargará de la evaluación de los daños y de la toma de decisiones pertinentes encaminadas al rescate progresivo de las funciones del área afectada.

7.3.5 Grupo de Seguimiento y Control

Conformado por los funcionarios representantes de la Oficina Asesora de Control

Interno, apoyados por el ingeniero coordinador de las labores del área afectada y que hace parte del grupo de desarrollo; quienes se encargaran de hacer seguimiento y control a las labores que se ejecuten, velando por el respeto del plan y la seguridad en su efectiva aplicación, así como la coherencia y consistencia en la aplicación de los procedimientos establecidos.

8. PLAN DE MITIGACION

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Los cuales se resumen a continuación:

8.1 PROCESO DE RESPALDO

El Proceso de Respaldo establecido como procedimiento de Mitigación, a través del cual la Contraloría asegura la conservación de su información vital y determina donde realizar sus trabajos críticos de procesamiento de datos en caso de falta o falla de sus equipos.

El diseño del proceso de respaldo incluye los cinco (5) principales componentes de un sistema de información, a saber:

- Los datos
- La documentación
- Los programas (software)
- Los procedimientos
- Los equipos (hardware)

8.1.1 Proceso de Respaldo Externo

Como sitio de respaldo externo se entiende una instalación diferente a la sede principal de la entidad donde se almacena una copia de los archivos de backups de la entidad, para que ante cualquier eventualidad que se presente en la sede principal se pueda reiniciar labores con los archivos almacenados en el sitio de respaldo externo.

En la entidad la instalación física que cumple con los requisitos de almacenamiento requeridos se encuentra ubicada en la Bodega de San Cayetano.

8.1.2 Plan de Backups y Equipos de Respaldo

Un backup es una copia de seguridad de la información en un segundo medio (cinta - cartridge) que nos garantiza recuperar la información contenida en nuestras maquinas en caso de que se presente alguna falla en el disco duro, un borrado accidental o un accidente imprevisto.

Estos backup deben ser ejecutados por:

1 El administrador del centro de computo
2 Usuarios con privilegios para realizar copias de seguridad.

La Contraloría de Bogotá adquirió una Solución de backup automatizado (EBS) y un Sistema de Almacenamiento en Discos (SAN), para realizar las copias de seguridad de la Entidad.

8.1.2.1 Definición de Niveles de Backup

Los niveles de backup que se han establecido como política en la dirección de Informática son los siguientes:

ANUAL: Debe realizarse al final de cada año (último día del año), es un backup total en cintas que se guardan indefinidamente.

SEMESTRAL: Debe realizarse al final de cada semestre un backup total (último día de cada semestre exceptuando el último día del año). Estas cintas se pueden denominar semestre1, semestre2 y se reutilizan anualmente.

MENSUAL: Debe realizarse al final de cada mes un backup total (último día de cada mes exceptuando el último día del año). Estas cintas se pueden denominar mes1, mes2, mes3,…. mes12 y se reutilizan anualmente.

SEMANAL: Se debe realizar al final de la semana (último día de la semana), es un backup total en cintas. Estas cintas se pueden denominar semana1,….semana4 y se reutilizan mensualmente.

DIARIO: Se debe realizar al final del día, es un backup total de la información diaria en cintas independientes. Estas cintas se pueden denominar Lunes, Martes, Miércoles y Jueves y se reutilizan semanalmente.

EN LINEA: Este backup se hace siempre y cuando se posea la infraestructura para copiar los archivos o directorios considerados como información vital al disco duro de un servidor remoto.

8.1.3 Procedimiento para Efectuar Backup's o Copias de Respaldo a la Información de las Dependencias

Este procedimiento se realiza acorde con la resolución reglamentaria 042 de 2005 del Sistema de Gestión de la Calidad (procedimiento para el manejo y control de registros magnéticos (backups) numeral 7.0, 7.1, 7.2, 7.3.

7. MATRIZ PARA LA DESCRIPCION DEL PROCEDIMIENTO:

7.1 Backups Bases de Datos en Servidores

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
1	Profesional Centro de Cómputo	Determina de acuerdo a la periodicidad establecida si el backup a realizar es diario, semanal, mensual o semestral.		Existe un grupo de cintas para backups diarios, otro para semanales, mensuales y semestrales
		Verifica en la Planilla de Control de Backups el número de la cinta correspondiente y registra la fecha de ejecución.	Planilla de Control de Backups	
		Selecciona en la Cintoteca la cinta correspondiente y prepara en el servidor (el) (los) archivo(s) a respaldar.	Cinta o Datacartridge	
		Ejecuta la acción adecuada para respaldar (el)(los) archivo(s).		
		Finalizada la copia de (el)(los) archivo(s) se regresa la cinta a su lugar de origen.		

7.2 Backup Semestral de Información Institucional

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
2	Director de Informática	Envía memorando al Contralor, Contralor Auxiliar, Directores Técnicos , Jefes de Oficinas Asesoras y Grupo de Actuaciones Especiales informando acerca del backup semestral de información institucional, indicando que se debe recopilar en un equipo con suficiente espacio en disco duro dentro de un directorio conformado por las iniciales DT seguido del código de la dependencia (DT#####) y que se encuentre conectado a la red.	Memorando	
3	Contralor, Contralor Auxiliar, Directores Técnicos, Jefes de Oficinas Asesoras y Grupo de Actuaciones Especiales	Solicita a todos sus funcionarios que seleccionen los archivos que ameriten ser conservados en copia de seguridad, en su última versión y preferiblemente establecer nombres cortos, combinado con fechas para definir los nombres de estos.		
		Asigna un funcionario para que realice la compilación de los archivos en el equipo seleccionado.		
4	Profesional y/o técnico de la Dependencia	Diseña en el computador seleccionado y dentro del directorio DT##### la estructura con los subdirectorios contenidos y copia en ella los archivos relevantes de la dependencia.		
5	Contralor, Contralor Auxiliar, Directores Técnicos, Jefes de Oficinas Asesoras y Grupo de Actuaciones especiales	Envía a la Dirección de Informática memorando informando que el directorio asignado para incluir los archivos que ameriten mantenerse en backup se encuentra conformado donde se indique: - Nombre y código de la Dependencia - Nombre del responsable del backup en la Dependencia - Ubicación e identificación en la red del computador que contiene la información - Nombre del directorio principal - Estructura gráfica del directorio principal completa.	Memorando	
6	Profesional Centro de Cómputo	Ubica a través de la red el directorio principal de cada una de las dependencias y procede a copiar la información en un servidor del Centro de Cómputo asignado para tal fin. Registra la acción realizada en un planilla de control de backup institucional	Planilla de control de Backup Institucional	

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
		Una vez centralizada toda la información en el servidor procede a copiar todos los datos en dos cintas (datacartridge) debidamente identificadas con el contenido de su información, la primera de ellas con destino a la cintoteca del Centro de Cómputo y la otra para el centro alterno.	Cinta (datacartridge)	

7.3 Recuperación de Información Institucional

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
7	Contralor, Contralor Auxiliar, Directores Técnicos, Jefes de Oficinas Asesoras y Grupo de Actuaciones Especiales	Envía memorando a la Dirección de Informática solicitando la recuperación de un backup o parte de este, indicando la fecha y ubicación de la información en la estructura de directorios de la respectiva dependencia.	Memorando	
8	Director de Informática.	Asigna profesional del Centro de Cómputo para realizar la tarea correspondiente		
9	Profesional Centro de Cómputo	Ubica la cinta correspondiente y restaura la información en el disco duro del servidor para luego enviarla vía red a la dependencia solicitante.		
		Proyecta respuesta para la firma del Director de Informática, informando fecha y ubicación donde fueron restaurados los datos solicitados.		

8.1.4 Centro de Cómputo Alterno

.

CENTRO ALTERNO DE RESPALDO

La entidad no cuenta con un centro alterno, pero con motivo de la reubicación de la sede de la Contraloria de Bogotá. ., se ve en la imperiosa necesidad de trasladar su centro de cómputo del Edificio Lotería de Bogotá a un espacio adecuado con las características físicas de seguridad, humedad, aireación propias para el correcto desempeño de los servidores y elementos activos de red.

Adicionalmente, el centro de procesamiento de datos o centro de cómputo, con su sigla en inglés Data Center, es la ubicación física donde se concentran todos los

recursos de cómputo y comunicaciones, necesarios y esenciales para el procesamiento de la información de la entidad.

Dichos recursos consisten principalmente de equipos servidores de aplicaciones, servidores de bases de datos, servidores de correo electrónico, servidores de autenticación, servidores de Internet, servidores de seguridad (Firewall, Proxy, antivirus), sistemas de almacenamiento centralizado de datos (SAN – Storage Area Network), servidores de respaldo/ recuperación y sistemas de comunicaciones (red de datos, switches, routers), entre otros.

El centro de cómputo o Data Center se constituye en un elemento esencial y estratégico para la Contraloría de Bogotá D.C., teniendo en cuenta que los componentes allí contenidos, han requerido un alto nivel de inversión y concentran la información crítica para el funcionamiento de la entidad, razón por la cual, requiere ser protegidos en ambientes físicos y lógicos adecuados de disponibilidad, confidencialidad e integridad, que garanticen el uso por parte de los funcionarios y la ciudadanía en general.

Teniendo en cuenta que el centro de cómputo (Data Center) requieren condiciones ambientales adecuadas, suministro de potencia, comunicación y acceso permanentes, seguridad física y lógica de los elementos y sistemas de información, monitoreo las 24 horas al día, con elementos y personal especializado, y actualmente ninguna de las sedes temporales de la Contraloría de Bogotá D.C. provee este tipo de condiciones, las cuales requieren para su adecuación la inversión de recursos económicos y técnicos importantes, en un edificio que no de propiedad de la Entidad, por lo tanto, es necesario contratar con una empresa especializada los servicios de arrendamiento de un sitio para hospedar o alojar el Centro de cómputo (Data Center) de la Entidad, en las condiciones ambientales, físicas y lógicas, que mitiguen los riesgos de daños a la infraestructura de equipos de cómputo y comunicaciones, y garanticen la disponibilidad, integridad y confidencialidad del la información de la Contraloría de Bogotá D.C.

Actualmente, se encuentra en trámite un convenio para contratar con la Empresa de Teléfonos de Bogotá, el centro alterno para el funcionamiento del centro de computo, debido a entre otras situaciones el reforzamiento de la estructura del edificio de la Contraloría de Bogota, piso 7 donde funciona actualmente el centro de computo.

9. FASE DE EMERGENCIA

Presenta las acciones detalladas que deben ser llevadas a cabo durante la emergencia. Provee una serie de instrucciones a las áreas Operativas y Administrativas, en caso de materializarse el riesgo.

Las soluciones que deben ser implementadas para mantener la continuidad de los procesos críticos en el momento de la materialización de los riesgos son las siguientes, para cada proceso crítico asociado a un riesgo, se define una acción o procedimiento a seguir.

9.1 SOFTWARE

9.1.1 Aplicaciones Críticas en Producción

9.1.1.1 De Desarrollo Externo

Con la entrada en desarrollo el convenio firmado entre la Contraloria de Bogota y la Secretaria de Hacienda el 30 de diciembre de 2008, entra en implementacion SI CAPITAL, que comprende los módulos de:

-

9.1.1.1.1 Software Financiero

Aplicación: MOISÉS (Tesorería, Contabilidad y Presupuesto)

Estado Actual: Se contrató con el proveedor la actualización, mantenimiento y soporte técnico del sistema financiero MOISÈS software integrado por los módulos de Presupuesto, Tesorería y Contabilidad así:

- Software Sistema Financiero Moisés versión Clipper 5.2 compuesto por los módulos de Presupuesto, Contabilidad y Tesorería.

- El soporte técnico por un año, se tendrá asistencia técnica, telefónica permanente y en caso necesario asistencia personalizada que realizará máximo en 48 después del reporte de analizar el problema.

- Mantenimiento de la aplicación se harán dos mantenimientos preventivos cada seis meses.

Proveedores: MOISES HARDWARE Ltda.

Usuario: Subdirección Financiera - Dirección Administrativa y Financiera.

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes aplicaciones o soluciones:

1) Para el manejo del Presupuesto, se tiene implementada la aplicación PREDIS, desarrollada por la Secretaría de Hacienda del Distrito Capital, La cual fue cedida por dicha entidad a través de un Convenio Interinstitucional.

   El PREDIS apoya las actividades relacionadas con la preparación del presupuesto, desde el anteproyecto hasta el decreto de liquidación e incluye interfaces automáticas con el sistema SIDIF de la Tesorería Distrital, lo cual permitirá en cualquier momento conocer el estado de ejecución presupuestal por las distintas entidades.

2) Para el manejo de la Contabilidad, Tesorería, Activos Fijos e Inventarios, se plantea la implementación de Hojas de Cálculo Excel, para la información crítica y de producción diaria. Actualmente, algunos de estos procesos se basan en la implementación de este tipo de herramientas.

   Así mismo, ante la posible falla o incompatibilidad de la aplicación PREDIS, se plantea la utilización de Hojas de Cálculo Excel, para el registro de la información crítica en esta área. Se utiliza la Aplicación PCT desarrollada en Clipper 5.2, para manejar el presupuesto paralelamente con el Sistema Financiero Moisés, recurso que se utiliza por la Subdirección como herramienta de verificación y análisis de la información presupuestal.

9.1.1.1.2 Software Recurso Humano

Aplicación: Sistema de Información para la Administración del Personal SIAP.

Estado Actual: En la actualidad, la Nómina desarrollada por el SISE se procesa en un Servidor de la Contraloría de Bogotá, ubicado en el piso 7, Dirección Técnica de Informática. Se configuraron tres (3) clientes en los equipos de la Dirección de Talento Humano que son los responsables del Manejo de la Aplicación. A la fecha se cuenta con un contrato de mantenimiento con el proveedor Syscom_Sistemas Ltda, el cual realiza los cambios en el sistema solicitados por el usuario.

Proveedor: SISE

Usuario: Dirección de Talento Humano

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes aplicaciones o soluciones:

1) Seguir con la ejecución del contrato de mantenimiento con Syscom_Sistemas Ltda.
2) Asignar un ingeniero de la Dirección de Informática que se encargue de realizar las modificaciones al SIAP, para realizar estas labores es primordial:
   - Contratar el mantenimiento de los productos Oracle, para el adecuado funcionamiento del SIAP.
   - Capacitar al funcionario en la herramienta en la cual fue desarrollada la aplicación.
   - Adquirir amplios conocimientos en el área normativa y en el área de liquidación.
   - Adquirir amplios conocimientos en el funcionamiento de la aplicación SIAP.
3) Desarrollo e Implementación de una Base de Datos de bajo nivel (sencilla) en Access, por parte de la Dirección de Informática, con la colaboración de

los usuarios de la Dirección del Talento Humano, la cual procesará la información crítica, durante el tiempo que dure la contingencia.

4) Elaboración y estructuración de una Hoja de Cálculo Excel, por parte de la Dirección de Informática, con la colaboración de los usuarios de la Dirección del Talento Humano, para el procesamiento de la información crítica.
5) De otro lado, ante la posible falla de la aplicación anterior se plantea la implementación de la aplicación PERNO, desarrollada por la Secretaría de Hacienda del Distrito Capital, aprovechando la homogeneidad de su estructura con la de la entidad. Esta sería cedida por dicha entidad a través de un Convenio Interinstitucional, el cual no implica inversión financiera. Actualmente, esta aplicación ya ha sido probada por la Secretaría y se encuentra en producción en Entidades del Distrito, que se acogieron a los convenios.

9.1.1.1.3 Software Liquidación de Aportes

Aplicación: DATÁISS (Autoliquidador de Aportes)

Estado Actual: El programa DATAISS es el software con que actualmente se reporta la Liquidación de Aportes de Seguridad Social en medio magnético al ISS y a todas las administradoras que conforman el Sistema de Seguridad Social (Fondos de Pensiones, EPS, ARP). Se tiene contratado el mantenimiento por un año con el proveedor.

Proveedor: ANUISS

Usuario: Dirección de Talento Humano

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes aplicaciones o soluciones:

Se plantea la implementación de un aplicativo de nivel bajo (sencillo), en hoja electrónica o base de datos, para garantizar la continuidad de los procesos críticos de presentación de información a las entidades externas; aprovechando que la información histórica se encuentra en formato DBF de fácil migración a

herramientas como ACCESS o EXCEL.

9.1.1.1.4.PREFIS (Sistema para el manejo y control del Procesos de Responsabilidad Fiscal)

Estado Actual: En vista de que con el cambio de la ley 42 del 93 y el nacimiento se la ley 610 de 2000, el aplicativo para el manejo del proceso de responsabilidad Fiscal queda obsoleto, se llevo a cabo la realización de un sistema multiusuario, en el servidor de base de datos SQL SERVER 2000 con una interfaz en Visual Basic 6.0 Service Pack 6, que permite un manejo similar al que se llevaba con el REFIS pero mejorando, en aspectos tales como la duplicidad de datos, obligatoriedad de llaves de registro, consultas e informes, ampliando su cobertura para que cada abogado lleve los procesos, con la coordinación de las secretarias comunes de cada dependencia. Aparte de ello una interfaz más amigable, de fácil interacción y visualización, de los expedientes. Y un manejo de los hallazgos Fiscales en firme y las Indagaciones Preliminares que aperturan. Además de contar con un árbol dinámico que maneja las etapas del Proceso de Responsabilidad, permitiendo así la modificación de los pasos del proceso si se requiere o si la ley cambia esto Solucionando el problema presentado con las Hojas Electrónicas. Donde se llevaba la información.

Usuarios: Dirección de Responsabilidad Fiscal, Subdirección de Responsabilidad Fiscal, Direcciones Sectoriales y GUIFO.

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, o caída del servidor.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se tiene la posibilidad de poner en producción un aplicativo de nivel bajo (sencillo), en hoja electrónica o base de datos, para garantizar la continuidad del proceso. Se tiene una hoja electrónica llamada SIRESCO en donde se va guardando la información básica de los etapas de los procesos.

Desarrollado por: Los pasantes de la Universidad Distrital Nidia Torres y Luis Ernesto Bocanegra en el 2005 y mantenimiento en el 2006.

9.1.1.1.5 Sistema de Información de Almacén e Inventarios

Aplicación: ALMACEN E INVENTARIOS

Estado Actual: Software desarrollado en CLIPPER 5.1, que permite registrar las transacciones del almacén de la entidad (las entradas, las salidas, los reintegros, las bajas, cierre diario, cierre mensual, catalogo) además nos permite registrar el manejo de los inventarios de la misma (altas, bajas, elementos depreciables, elementos no depreciables, sobrantes, faltantes, inventario físico por centro de costo, kardex de inventario).

Proveedor: LUIS ORLANDO OSPINA

Usuario: Subdirección Financiera - Dirección Administrativa y Financiera.

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se tiene la posibilidad de poner en producción un aplicativo de nivel bajo (sencillo), en hoja electrónica o base de datos, para garantizar la continuidad del proceso.

9.1.1.2 De Desarrollo Interno, bajo la responsabilidad directa de la Dirección de Informática

9.1.1.2.1 Software Administrativo

Aplicación: ATENCION A USUARIOS

Estado Actual: Software desarrollado en ACCESS 97, que permite controlar los servicios prestados de mantenimiento correctivo y preventivo sobre los computadores e impresoras de la Entidad. Mantiene una base de datos con la información de configuración de los equipos (hoja de vida) y su ubicación dentro de la Entidad.

Ing. Desarrollador: LUIS ARMANDO SANCHEZ OLIVEROS

Usuario: Dirección de Informática.

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se implementará la elaboración de planillas y registro de los servicios prestados a los diferentes equipos de la Entidad en una hoja de cálculo de EXCEL.

Aplicación: SICRE (COAREAS)

Estado Actual: Software desarrollado en PowerBuilder 4.0 y manejador de base de datos Watcom. La aplicación para el control del flujo de correspondencia entre áreas fue rediseñada para ajustar su funcionamiento a las necesidades actuales de la entidad del manejo de la documentación del Sistema de Gestión de la Calidad NTC ISO 9001:2000. Permite el control de la correspondencia que se origina y recibe en cada una de las dependencias de la Contraloría en especial la que se origina y recibe internamente, a su vez permite controlar la correspondencia recibida y enviada externamente.

Ing. Desarrollador: CARLOS GUSTAVO DUEÑAS

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se implementará la elaboración de planillas y registro de la correspondencia en hoja electrónica usando tablas dinámicas y macros e impresión de rótulos mediante combinación de correspondencia en procesador de palabra WORD.

Aplicación: RADICADO

Estado Actual: Software desarrollado en PowerBuilder 4.0 y manejador de base de datos Watcom. La aplicación de Radicación y correspondencia fue rediseñada y nuevamente implementada para ajustar su funcionamiento a la necesidades actuales de la entidad. Permite el control de la correspondencia externa que se recibe y se produce en cada una de las dependencias.

Ing. Desarrollador: CARLOS GUSTAVO DUEÑAS

Usuario: Dirección Administrativa y Financiera, áreas de radicación de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se implementará la elaboración de planillas y registro de la correspondencia en hoja electrónica usando tablas dinámicas y macros e impresión de rótulos mediante combinación de correspondencia en procesador de palabra WORD.

Aplicación: SISTEMA DE INFORMACIÓN PARA EL CONTROL Y SEGUIMIENTO DE MULTAS

Estado Actual: Software desarrollado en PowerBuilder 4.0 y manejador de base de datos Watcom. La aplicación se encuentra en producción, es utilizada para actualizar la centralización de todas las multas impuestas mediante el proceso coactivo y a su vez permite las consultas por entidades afectadas y funcionarios involucrados.

Ing. Desarrollador: CARLOS GUSTAVO DUEÑAS

Usuario: Oficina Asesora Jurídica

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información.

Soluciones en contingencia: Aunque el proceso no ha sido considerado como crítico, ante la posible materialización de los riesgos o falla de la aplicación actual,

se tiene la posibilidad de poner en producción un aplicativo de nivel bajo (sencillo), en hoja electrónica o base de datos, para garantizar la continuidad del proceso. Sin embargo, en el momento se están desarrollando ajustes y actualizaciones de la misma.

Aplicación: SISTEMA DISTRITAL DE INFORMACION DISCIPLINARIA

Estado Actual: Software desarrollado en ambiente WEB, por la Secretaria General de la Alcaldía Mayor de Bogotá, para ser utilizado por las entidades del Distrito a través de su página.

La Contraloría tiene conexión a través de Internet, la información reposa en los servidores de la Secretaria General de la Alcaldía Mayor de Bogotá, y la Administración la efectúa la misma Secretaria.

Este servicio no tiene ningún costo, solamente el uso de Internet.

Desarrollado por: SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA

Usuario: Únicamente la Oficina de Asuntos Disciplinarios

Riesgos Asociados: Caída de la RED, daño del servidor de la Secretaria General, Posible pérdida de información.

Soluciones en contingencia: Aunque el proceso no ha sido considerado como crítico, ante la posible materialización de los riesgos o falla de la aplicación actual, la Secretaria General realiza back ups de la información, de acuerdo con base en las políticas establecidas para este procedimiento.

Este sistema empezó a ser utilizado por la Contraloría a partir de junio 12 de 2006.

Aplicación: SISTEMA DE INFORMACION PARA LA GESTION Y CONTROL DE QUEJAS Y RECLAMOS PARA LA CONTRALORIA DE BOGOTA.-PQR

Estado Actual: Software desarrollado en VISUAL BASIC 6.0 y conectado a una base de datos SQL Server 2000, con un modulo WEB diseñado en ASP que le permite al ciudadano acceder a la página de la Entidad para colocar su queja.

El sistema esta diseñado para gestionar los derechos de petición interpuestos ante la Entidad por los ciudadanos . Permite generar reportes y estadísticas de los mismos.

Este sistema fue puesto en marcha el 3 de noviembre de 2004.

Ing. Desarrollador: Pasantes de la Universidad Distrital: Edwin Alfonso y Gabriel Quintero.

Usuario: Sistema en tiempo real, en donde todas las dependencias de la Entidad, acceden a la información que se encuentra en este sistema.

Riesgos Asociados: El no ingreso oportuno de la información al sistema, y falla del Servidor, en donde está instalada, Posible pérdida de información.

Soluciones en contingencia: El no ingreso oportuno de la información se mitiga llevando en un libro radicador cada derecho que va llegando a la Entidad y una carpeta para cada derecho de petición en donde se encuentra el documento fisico por cada uno de los tramites que se han realizado.

En caso de caída del sistema o daño del servidor, se tiene como alternativa la información física de cada una de los derechos de petición, los cuales son distribuidos a cada dependencia que le corresponde resolver cada caso, pero finalmente quien centraliza los derechos de petición es la Oficina de Quejas y Reclamos.

Aplicación: ISONET : SOFTWARE DE APOYO A LA PLANIFICACION, IMPLEMENTACION Y MANTENIMIENTO DEL SISTEMA DE GESTION DE CALIDAD SGC NORMA ISO 9001-2000 DE LA CONTRALORIA DE BOGOTA

Estado actual: Esta aplicación se encuentra desarrollada en Visual Basic .NET y manejador de base de datos SQL Server 2000, este software de apoyo al sistema de gestión de calidad SGC, se encuentra en producción desde el 2006. Contribuye al control, distribución, administración y consulta de los documentos y registros, racionalizando los costos en el uso del papel, insumos de impresión y multicopiado y además permite la programación, registro y seguimiento de tareas claves como auditorias internas de calidad, reporte y control de indicadores de gestión, consulta y control de normatividad y reporte y control de acciones correctivas, preventivas y de mejora.

Con su implementación se logra que todos los procesos y dependencias proporcionen información veraz, actualizada, organizada, completa y oportuna relacionada con cada uno de los módulos que lo integran:

Documentos: A través de este módulo se realiza la consulta y actualización de los documentos y planes adoptados en la entidad que son exigidos por la norma ISO 9001:2000, permite realizar desde la solicitud de elaboración o modificación de los documentos hasta la aprobación por parte del Contralor.

Normatividad: Permite el registro, actualización y control de las normas externas, así como la generación del listado de documentos externos.

Auditorias de calidad: A través de este módulo se permite a la oficina asesora se control interno y usuarios autorizados la consulta, modificación, aprobación de documentos y programación, registro y seguimiento de auditorias y no conformidades.

Reporte de acciones: Facilita el registro de las acciones correctivas, preventivas y de mejora así como el reporte de su seguimiento tal como lo establece la norma de calidad y el procedimiento adoptado en la entidad.

Plan de actividades: En este módulo se realiza la consulta, modificación y actualización de actividades e indicadores formulados para una vigencia en desarrollo del Plan Estratégico. Los usuarios de acuerdo con su perfil podrán

reportar datos de las variables responsabilidad de las dependencias y consultar los consolidados por proceso.

Desarrollador: Contrato celebrado con Edward Humberto Sandoval Gómez.

Usuario: Todas las dependencias.

Riesgos Asociados: Pérdida de información por mal funcionamiento de la aplicación o de los equipos donde están instaladas.

Soluciones en contingencia: Esta aplicación se encuentra instalada en un servidor ubicado en el centro de cómputo de la Dirección de Informática, el cual esta incluido en el procedimiento de copias de respaldo (backups) vigente. Ante una posible materialización de los riesgos, se dispondría de la copia de respaldo del día anterior y sería viable su instalación en un servidor de respaldo.

Aplicación: SIVICOF : SISTEMA DE VIGILANCIA Y CONTROL FISCAL – APLICATIVO PARA EL DISEÑO, RECEPCION Y CONSULTA DE LA CUENTA

Estado actual: El Sistema de Vigilancia y Control Fiscal de la Contraloría de Bogotá es la plataforma informática que se orienta a servir de respaldo tecnológico al proceso de Rendición de la Cuenta, como el mecanismo por el cual los sujetos de control reportarán de manera electrónica la información y documentos que reflejen el desarrollo de su gestión durante la vigencia fiscal.

ARQUITECTURA DEL SISTEMA	
Sistemas Operacionales (SO) de servidores	Windows 2000/2003 Server®, Linux® y Unix® en general.
Sistemas Operacionales (SO) de usuarios finales	Windows 98/2000/XP® Linux®
Metodología de diseño	Orientado a Objetos (OO).
Bases de datos	DB2®.
Herramienta de desarrollo	Orientado a Objetos (OO), basado en tecnología JAVA®.
Diseño y desarrollo multicapa	Tres (3) capas independientes: datos, aplicaciones y clientes.

SIVICOF entró en producción oficialmente el 12 de octubre de 2006, con la primera rendición mensual por parte de los sujetos de control adscritos a ésta Contraloría, formalizada por la resolución 020 de septiembre de 2006, en donde se adopta como mecanismo para la rendición de cuentas.

El SIVICOF se caracteriza por una arquitectura multinivel, en donde se distinguen cuatro módulos: Dos módulos locales y dos Web.

El módulo de administración local StormAdmin, es donde se gestiona el manejo de los formatos, las reglas de validación, las alertas y los parámetros que definen los formatos electrónicos y sus características.

El módulo de usuario StormUser, es de uso de los sujetos de control para la elaboración de los formatos electrónicos que componen las diversas cuenta, fue distribuido mediante CD'S instaladores a cada sujeto de control, además esta disponible para descarga desde el módulo Web del SIVICOF.

Ésta módulo permite a los sujetos de control diligenciar los formularios requeridos por el ente controlador para la rendición de cuentas. Evita los múltiples desplazamientos hacia el mismo, típicos de cada rendición, y reduce el nivel de rechazo, pues permite validar la información en un 90% al momento de generar los archivos antes de ser presentados.

El módulo StormWeb maneja dos tipos de usuario el administrador y el sujeto de control.

El Administrador parametriza y define por este módulo, las características de rendición por sujeto de control, como las periodicidades, los términos, los informes, los usuarios, los perfiles y los roles.

El módulo StormReport, es el mecanismo dispuesto para que los funcionarios de la Contraloría de Bogotá, accedan a la información reportada por los sujetos de control, tan pronto y como esta sea recibida por el sistema.

Por la condición de ser Módulos Web, estos dos últimos no requieren de una instalación.

Con la implementación del SIVICOF, se ha logrado estandarizar la información que es requerida a los Sujetos de Control, reducir la cantidad de solicitudes de información idéntica en diferentes momentos, facilitar el procesamiento de la información requerida en la cuenta unificando su forma de diligenciamiento, presentación y consulta, validar y verificar la integridad y consistencia de la información en las oficinas del Sujeto de Control, reducir el nivel desplazamientos y tiempos de entrega para los sujetos de control, reducir el tiempo y los esfuerzos del personal de la contraloría respecto al recibimiento de la cuenta de los más de 500 sujetos de control, y optimizar el uso de los recursos informáticos existentes, permitiendo a los sujetos de control enviar la cuenta desde sus oficinas a través de la WEB.

Desarrollador: Macroproyectos LTDA.

Usuarios: Entidades sujeto de control, Direcciones Sectoriales, Dirección de Economía y Finanzas Distritales, Grupo Especial de Investigaciones Forenses, Dirección de Informática y Dirección de Planeación.

Riesgos Asociados: Pérdida de información por mal funcionamiento de la aplicación o de los equipos donde están instaladas.

Caída en el servidor de procesamiento de información con el cual se valida la información enviada por los sujetos de control.

Soluciones en contingencia: Esta aplicación se encuentra instalada en un servidor ubicado en el centro de cómputo de la Dirección de Informática, el cual esta incluido en el procedimiento de copias de respaldo (backups) vigente. Ante una posible materialización de los riesgos, se dispondría de la copia de respaldo del día anterior y sería viable su instalación en un servidor de respaldo.

Se cuenta con servidores instalados en maquinas separadas, que respaldan la atención y procesamiento de información continua de los archivos recibidos.

También se puede dar la ampliación de los plazos de entrega de la información de los sujetos de control

Actualizaciones:

En el mes de Junio de 2009 se realizaron actualizaciones a la versión 2 de cada uno de los módulos implementando nuevas funcionalidades tales como:

- **StormAdmin**: Entorno gráfico tipo Windows, entorno de formulación mucho mas fácil e intuitivo, asociación y excepción de formularios y formulas de manera individual o grupal, generación de reportes de administración.

- **StormUser**: Entorno gráfico tipo Windows, actualización automática a través de Internet, compatibilidad para carga de archivos de la versión 1, almacenamiento automático de archivos, filtros sobre la información diligenciada, temas de visualización, desplegar u ocultar columnas

- **StormWeb**: Autenticación con firma digital, acceso a información actualizada respecto al sistema y la cuenta, envío de archivos str y documentos electrónicos firmados digitalmente, descarga de archivos enviados

- **StormReport**: Mayor rapidez en la generación de consultas mediante la actualización del WAS, creación de nuevos reportes disponibles para los auditores tales como GeneraXls Rendición, entidades que rindieron determinado formato, entidades con y sin certificados.

Aplicación: SIGESPRO . SISTEMA DE INFORMACION DE GESTION DE PROCESOS Y DOCUMENTOS

Estado actual: SIGESPRO está desarrollado en J2EE con Base de Datos DB2 y servidor de aplicaciones WEBSPHERE APLICATION SERVER (WAS). Este sistema cubre los Procesos de: Gestión Documental, Micro, Macro, Responsabilidad Fiscal y de la Oficina Jurídica.

El Proceso de Gestión Documental permite el Recibo y Envío de Correspondencia Externa agilizando así el control, distribución, administración, seguimiento y consulta de los documentos digitalizados y clasificados por dependencia, por tercero, por clase documental, por tipo documental y por trámite aminorando los costos en el uso del papel e insumos de impresión.

Maneja un único consecutivo para toda la entidad minimizando el riesgo de duplicidad en el consecutivo en la entidad.

El Recibo y Envío Interno de correspondencia actualmente, se encuentra en proceso de implementación.

El Proceso Micro, con base en la Resolución Reglamentaría No.026 del 28 de Diciembre de 2007 permite el registro de cada una de sus actividades, clasificando cada proceso según el tipo de auditoria, dejando registro de los documentos soporte de cada actividad y el grupo de auditores que participó en cada proceso e igualmente dejando registro del cronograma de actividades

El Proceso Macro está en producción pero no se está utilizando.

El Proceso de Responsabilidad Fiscal está en producción pero no se está utilizando.

El Proceso de la Oficina Jurídica está en producción pero no se está utilizando.

SIGESPRO permite consultar la correspondencia tanto enviada como recibida en forma digital en tiempo real, la consulta de los documentos y planes adoptados por la entidad y que son exigidos por la norma ISO 9001:2000.

Desarrollador: Contrato celebrado con Macroproyectos S.A.

Usuario: Todas las dependencias.

Riesgos Asociados: Pérdida de información en el servidor donde se almacena la Base de Datos.

Soluciones en contingencia: Este sistema se encuentra instalada en un servidor ubicado en el centro de cómputo de la Dirección de Informática, el cual esta incluido en el procedimiento de copias de respaldo (backups) vigente. Ante una posible materialización de los riesgos, se dispondría de la copia de respaldo del día anterior y sería viable su instalación en un servidor de respaldo.

Aplicación: SIMUC, SISTEMA DE MULTAS

Aplicativo creado para el control de multas, costas y agencias en derecho, reintegros, responsabilidad fiscal y sanciones disciplinarias, su función esta

enfocada en la liquidación de los intereses y el control del dinero que van pagando los ejecutados,

Entró en producción para la Dirección de Responsabilidad Fiscal y Jurisdicción Coactiva, el 21 de enero de 2009, en versión 1.0, a la fecha se han realizado diferentes ajustes solicitados por la dependencia

Desarrollado en Visual Basic 6.0, la base datos Sql Server 2000 y tiene una conexión autónoma a exel (para los cálculos).

Desarrollador: LUIS ERNESTO BOCANEGRA RAIRAN.

Usuarios: Dirección de Subdirección Coactiva

Riesgos Asociados: Caída del servidor

Soluciones en Contingencia: Backup de los servidores y los funcionarias harían las liquidaciones manualmente en Excel.

En el momento en que se presente la emergencia, para cualquiera de las aplicaciones críticas citadas anteriormente, los grupos de trabajo deben iniciar y seguir los siguientes pasos:

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
1	Reporte de la falla al funcionario encargado de los sistemas, que pertenece a la dependencia y que hace parte del grupo de desarrollo.	Teléfono. Reporte de Errores	Inmediato	Usuario
2	Inhabilitar el uso del equipo o equipos que utilizan dicha aplicación y advertencia a los usuarios para no desarrollar ninguna actividad relacionada.	Listado de usuarios, medio de comunicación.	Inmediato, Máximo 15 minutos	Funcionario Encargado de la Dependencia
3	Reporte de la falla a la	Teléfono. Reporte	Inmediato,	Funcionario Encargado

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
	Línea de Atención a Usuarios	de Errores	Máximo 30 minutos	de la Dependencia
4	Dirigirse a la dependencia en donde se ha presentado la falla	Medio de transporte, reporte de errores, orden de servicio	Máximo 30 minutos, dependiendo del lugar donde se halla presentado la falla	Ingeniero del Grupo de Desarrollo y Técnico de Soporte encargados de la vigilancia y soporte de la aplicación reportada en emergencia.
5	Identificación, Diagnóstico y Análisis de las fallas y su alcance.	Fuentes, documentación soporte de la aplicación, equipo de soporte y pruebas (herramientas y medios magnéticos)	Dependiendo del nivel de criticidad de la falla (alta, media, baja), pero no mayor de 1 hora.	Ingeniero del Grupo de Desarrollo, Funcionario delegado en la dependencia y Técnico de Soporte encargados de la vigilancia y soporte de la aplicación reportada en emergencia
6	Reporte al Coordinador del Plan de Contingencias	Teléfono y documento de diagnóstico de la falla	Inmediatamente se haya terminado el diagnóstico respectivo, máximo 15 minutos después.	Ingeniero del Grupo de Desarrollo
7	Notificación al Comité Directivo de la Situación, para que ellos tomen la decisión de liberar y poner en ejecución el Plan de Contingencias, si así lo amerita.	Teléfono, Plan de Contingencias y documento de diagnóstico de la falla.	Inmediato, máximo 15 minutos.	Coordinador del Plan de Contingencias.
8	Si se pone en marcha el Plan de Contingencias, el coordinador debe identificar el área o áreas afectadas con el fin de notificar al personal encargado de las mismas, para llevar a cabo las actividades del Plan.	Teléfono, Plan de Contingencias y documento de diagnóstico de la falla.	Entre 15 y 30 minutos.	Coordinador del Plan de Contingencias.
9	Localizar los recursos necesarios para dar inicio al Plan relacionado con el área afectada	Inventarios, Plan de Contingencias, documento de diagnóstico de la	El mínimo dependiendo de la ubicación de los recursos	Coordinador Centro de Computo, Coordinador Grupo Línea de atención a

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
		falla, último backup, manuales de usuario y técnico de la aplicación afectada. Medios magnéticos necesarios.	necesarios. Máximo 1 hora.	usuarios, Ingeniero del Grupo de Desarrollo y Técnico de Soporte encargados de la vigilancia y soporte de la aplicación reportada en emergencia
10	Implementar la solución y ejecutar las actividades establecidas en el Plan para mantener la continuidad del proceso afectado.	Recursos necesarios localizados en la actividad 9.	El mínimo dependiendo de la complejidad de la solución. No debe ser mayor a 5 horas.	Ingeniero del Grupo de Desarrollo, Funcionario delegado en la dependencia y Técnico de Soporte encargados de la vigilancia y soporte de la aplicación reportada en emergencia
11	Reportar al Coordinador del Plan de Contingencias, la conclusión de las actividades previstas y la puesta en marcha de la solución.	Reporte de las actividades realizadas, debidamente firmada por el usuario, como recibo a satisfacción.	Entre 15 y 30 minutos.	Ingeniero del Grupo de Desarrollo encargado de la vigilancia y soporte de la aplicación reportada en emergencia
12	Monitorear el correcto funcionamiento de la solución implementada, con el fin de avisar cualquier anomalía a la Dirección de Informática.	Documentación del proceso afectado.	Observación permanente, mientras dure la contingencia	Funcionario delegado en la dependencia encargado de la vigilancia y soporte de la aplicación reportada en emergencia
13	Iniciar las acciones pertinentes para el restablecimiento del proceso normal (ubicar al proveedor, hacer efectivas pólizas, hacer soporte correctivo, contratar nuevas soluciones, etc., según convenga o este planeado).	Plan de Contingencias. Documentación soporte del proceso.	No mayor a un (1) mes dependiendo del nivel de criticidad del proceso afectado.	Ingeniero del Grupo de Desarrollo, Funcionario delegado en la dependencia, encargados de la vigilancia y soporte de la aplicación reportada en emergencia y Director de Informática

9.1.2 Software Ofimático

Estado Actual: La entidad en la actualidad cuenta a nivel de software con:

Software Ofimático: Microsoft Office 4.2, Microsoft Office 97, Microsoft Office 2000 y Microsoft Office XP, Microsoft Office 2003.

Software Operativo: Windows 95, Windows 98, Windows NT Workstation y Windows XP.

Proveedor: Entre otros AJC IT SOLUCIONES INFORMATICAS, SISA, PNUD, SOFTWARE Y ALGORITMOS S.A. y distribuidores autorizados MICROSOFT.

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Ante la posible materialización de los riesgos se plantea la utilización de los medios originales del software existente para realizar las respectivas reinstalaciones.

En el momento en que se presente la emergencia, el usuario debe seguir el procedimiento Atención a Usuarios establecido en la Resolución Reglamentaria 046 del SGC del 2005:

CUADRO 3
PROCEDIMIENTO DE ATENCIÓN A USUARIOS

7.4 ATENCIÓN A USUARIOS

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
1	Contralor Auxiliar Jefes de Oficinas Asesoras Directores Subdirectores Coordinadores	Informan a la línea de atención a usuarios los problemas detectados en Hardware y Software.		El reporte puede ser telefónicamente, personalmente o con memorando.

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
	con funciones directivas Profesionales Técnicos			
2	Profesional Universitario y/o Técnico Dirección de Informática.	Recibe la solicitud del servicio (Hardware ó Software). Ingresa en la Aplicación "Atención a Usuarios" los datos del funcionario y falla presentada. Analiza reporte y asigna funcionario del grupo SOS que atenderá el servicio reportado. Imprime orden de servicio y registra en la "Planilla de Reparto" Firma la planilla de reparto y entrega la orden de servicio generada al Técnico y/o funcionario del grupo SOS.	Planilla de Reparto Orden de Servicio	Los registros deben contener como mínimo la siguiente información: ORDEN DE SERVICIO: fecha de solicitud, problema detectado, nombre funcionario que solicita, teléfono, nombre funcionario grupo SOS, descripción detallada del problema. PLANILLA DE REPARTO: fecha de entrega, nombre funcionario asignado, firma de quien entrega y recibe la orden de servicio y descripción.
3	Profesional Universitario y/o Técnico Dirección de Informática.	Recibe orden de servicio y firma planilla de reparto. Verifica falla y/o requerimiento del funcionario en la dependencia y elabora diagnóstico, registrando todos los campos en la orden de servicio y determina qué tipo de intervención se requiere. Si se requiere compra de repuesto se ejecuta procedimiento 7.5		

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
		"Instalación de elementos de Computo y/o Repuestos para Estaciones de Trabajo e impresoras"		
4	Profesional universitario y/o Técnico Dirección de Informática.	Si no se requiere la compra de repuestos: Subsana la falla, hace firmar al usuario la satisfacción del servicio en la Orden de Servicio. Registra en la planilla de reparto el servicio atendido, la fecha de devolución de la orden de servicio y firma.	Orden de Servicio	
5	Profesional universitario y/o técnico Dirección Técnica de Informática.	Actualiza en la Aplicación "Atención a Usuarios" el cierre de la solicitud atendida. Registra en la planilla de reparto la fecha de atención de la solicitud.	Planilla de Reparto	Se verifica la firma del usuario en la Orden de Servicio

9.2 HARDWARE

9.2.1 Microcomputadores

Estado Actual: se encuentran en funcionamiento 927 equipos de cómputo, que se encuentran distribuidos en las diferentes dependencias de la entidad.

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Ante la posible materialización de los riesgos, se plantea el uso del hardware existente, desarrollando un proceso de redistribución de equipos para cubrir de manera óptima las necesidades reales y críticas de las dependencias y por ende de toda la Entidad.

En el momento en que se presente la emergencia, los usuarios deben iniciar y seguir los mismos pasos del cuadro anterior (ver cuadro 3) procedimiento Atención a Usuarios Resolución Reglamentaria 046 de 2005

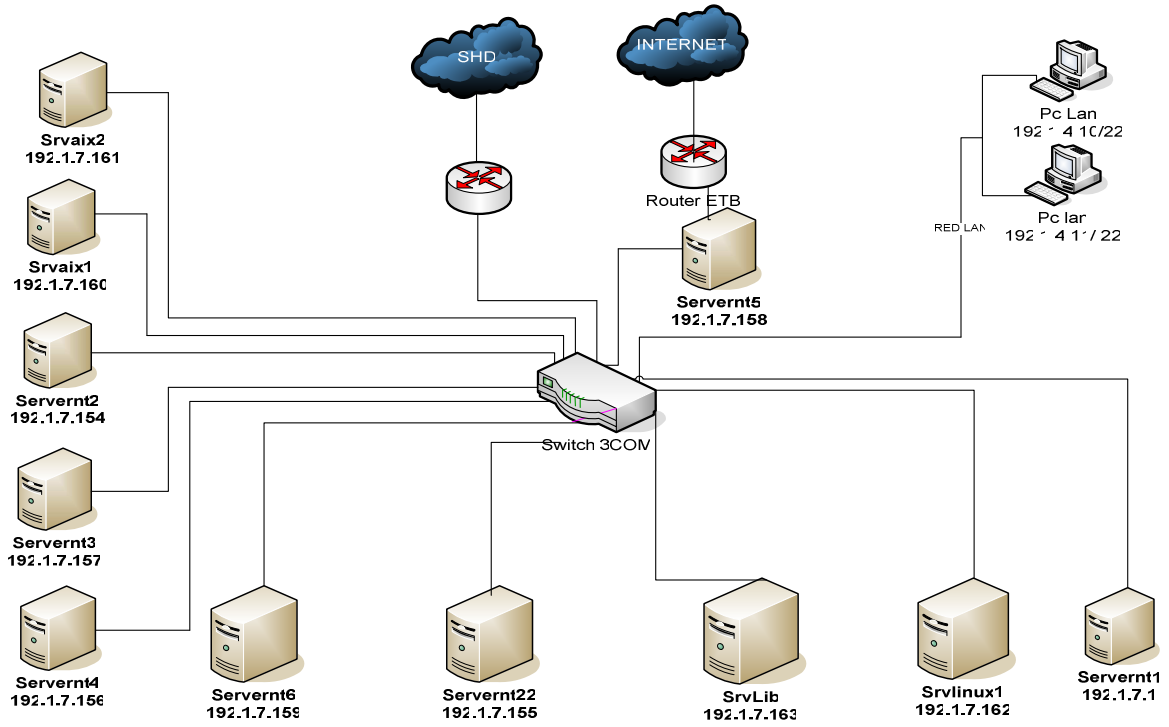
El 13 de diciembre de 2004,se empezó el reemplazo de los computadores existentes por computadores IBM, Pentium 4, 256 MB, disco duro de 80 MB, (299 computadores), windows XP, Office 2003.

Con este reemplazo tecnológico, se minimizó el riesgo asociado al mal funcionamiento de las aplicaciones criticas, la posible perdida de información y las fallas en los equipos de computo..

Equipos Servidores

Estado Actual: A continuación se muestra la estructura actual de la red de la Contraloria de Bogotá actualizada con la ultima plataforma tecnológica adquirida,

la cual se encuentra descrita en el item 6.4.2.2, con sus respectivos nombres de maquina y IP, descripción de su contenido.



Usuario: Centro de Computo y Usuarios de Aplicaciones implementadas en los servidores activos.

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Posible incumplimiento de los contratistas, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles.

Soluciones en Contingencia: Se debe garantizar el mantenimiento preventivo/correctivo 7*24.

En el momento en que se presente la emergencia, los usuarios deben iniciar y seguir los mismos pasos del cuadro anterior (ver cuadro 3) procedimiento 7.4 Atención a usuarios Resolución Reglamentaria 046 del SGC de Diciembre 22/05.

9.3 EQUIPOS ELECTRÓNICOS

Estado Actual: Actualmente se cuenta con 13 UPSs de las cuales una de ellas está fuera de servicio y en espera de soporte.

Proveedor: Varios (Ver Capítulo 6)

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Posibles retrasos en procesos administrativos, demoras en la efectividad de algunas comunicaciones, problemas en el control de asistencia del personal, Posible daño de equipos o pérdida de protección ante ausencia de fuente regulada y soporte en corte de energía eléctrica.

Soluciones en contingencia: se realizó un estudio de conveniencia y oportunidad dirigido a la Dirección Administrativa y Financiera para que se adelante la contratación del mantenimiento correctivo y/o preventivo, que incluye el reemplazo de los bancos de baterías existentes de las UPS.

En el caso de no contar con fluido eléctrico regulado los equipos deben estar protegidos con reguladores de voltaje.

10. FASE DE RECUPERACION

Permite restablecer las condiciones originales y operación normal del sistema. El cual contempla:

- Definición de las políticas (parámetros, límites, horas de recuperación)
- Definición de los objetivos y requerimientos de la continuidad
- Definiciones, términos y suposiciones

Durante los primeros 5 días de interrupción prolongada del procesamiento de datos o desastre, si la interrupción del servicio va a ser por largo tiempo luego del desastre, se debe poner en ejecución la fase de recuperación del siniestro en el Centro de Cómputo alterno externo.

La estimación del tiempo en que va a durar la interrupción del servicio, se obtiene una vez se ejecute la Fase de Emergencia y una vez se halla evaluado el alcance de las fallas que se presentaron. Dicha estimación la debe obtener el Coordinador del Plan de Contingencias, apoyado en el trabajo y resultados presentados por el grupo de desarrollo del Plan.

El Plan presupone que debe utilizarse un Centro de Cómputo alterno externo al edificio sede de la CONTRALORÍA DE BOGOTÁ D.C., si la emergencia afecta en forma general (en un 60% o más) las instalaciones físicas y técnicas con que se cuenta.

Entonces, durante los 5 días siguientes al desastre, deberán prepararse las copias de respaldo de aplicaciones y procedimientos automatizados utilizados por las diferentes oficinas usuarias afectadas. El plan busca que las capacidades del servicio inicial del procesamiento de datos sean restauradas en el sitio alternativo en el 5º día siguiente al desastre. La reestructuración total de las capacidades del procesamiento para la red en línea están contempladas en fases durante 5 días a 28 días hábiles.

10.1 PREPARACIÓN REQUERIDA PARA RECUPERACIÓN DE DESASTRES

Los grupos de recuperación de desastre, deben estar organizados a lo largo de las líneas funcionales con la Dirección de Informática de la CONTRALORÍA DE BOGOTÁ D.C. y la representación de las Direcciones usuarias, en la misma forma en que está organizado el grupo de desarrollo. Cada grupo es responsable del restablecimiento y mantenimiento de los procedimientos de recuperación antes del desastre. Los esfuerzos de planeación son para moderar el esfuerzo de la recuperación y maximizar el éxito de los procedimientos implementados en el evento de un desastre.

10.1.1 Grupo de Centro de Cómputo

10.1.1.1 Responsabilidades

- Mantener las especificaciones para las configuraciones de hardware que deben ser instaladas en los diferentes equipos del centro de cómputo alterno.
- Mantener y mejorar los procedimientos de recuperación de desastres del grupo de operaciones del computador.
- Evaluar la instalación del software del sistema (al momento de la recuperación) y de los datos con la asistencia del grupo de soporte técnico y de las aplicaciones en producción, en la forma usual.
- Implementar los procedimientos dados por otros grupos de recuperación para generar y/o almacenar materiales que deben estar fuera del edificio y son necesarios para la recuperación.
- Mantener la configuración de la red para todos los sistemas de comunicación de datos.
- Mantener un plano de la configuración de la red a ser implementada en el evento de un desastre.
- Evaluar los procedimientos de backup's para establecer los servicios de comunicación de datos en el evento de un desastre.

10.1.1.2 Coordinador del Grupo

El Coordinador del Centro de Cómputo de la Contraloría, quien administra las operaciones de los sistemas.

10.1.1.3 Miembros del Grupo

- Grupo Centro de Computo
- Grupo de Atención a Usuarios.

10.1.2 Grupo de Atención a Usuarios

10.1.2.1 Responsabilidades Predesastres

- Proveer procedimientos para crear copias legibles por los equipos, de todos los componentes del software del Sistema, librerías de software de aplicaciones, drivers y controladores de dispositivos, Software de instalación, actualización, utilitarios y antivirus.
- Ejecutar los procedimientos para mantener copias de respaldo en el centro de almacenamiento alterno con la información de las aplicaciones críticas, de los directorios de trabajo de cada una de las dependencias de la Contraloría de Bogotá y el recurso de software necesario para las mismas.
- Evaluar y Verificar el software de recuperación de desastres en la forma usual, en cooperación con el grupo de operaciones y el sistema de aplicaciones.
- Documentar cada evaluación de recuperación desde la perspectiva de las actividades del grupo de soporte técnico.

10.1.2.2 Coordinador del Grupo

- Coordinador del grupo de Atención a Usuarios.

10.1.2.3 Miembros del Grupo

- Grupo de Soporte de Atención a Usuarios
- Responsable de la operación de programas y comunicaciones.

10.1.3 Grupo de Análisis y Desarrollo

10.1.3.1 Responsabilidades Predesastre

- Establecer procedimientos que permitan las revisiones de todo el software de aplicaciones en producción, para que sea almacenado y copiado rutinariamente en un sitio externo como parte de los procedimientos de backup de la operación del computador.

- Coordinar con los grupos de usuarios para asegurar que sus planes de acción en caso de desastre sean seguros, viables y actualizados con el fin de reflejar las operaciones actuales.
- Mantener una estrategia general, un plan y documentación para la evaluación de las aplicaciones luego de que la recuperación en el centro alterno se halla terminado por parte de los grupos de soporte técnico y de operaciones, pero antes de que los sistemas se coloquen de nuevo en producción.
- Coordinar con el grupo de operaciones el mantenimiento de los proyectos de las aplicaciones y la documentación en el lugar de respaldo.

10.1.3.2 Coordinador del Grupo

- Coordinador del Grupo de Análisis y Desarrollo

10.1.3.3 Miembros del Grupo

- Ingenieros programadores y analistas responsables de la aplicación en etapa de desarrollo y producción según esté establecido.
- Usuario final, responsable de la operación del programa.
- Funcionario Delegado de cada dependencia encargado de la supervisión de la aplicación.

10.2 RECUPERACIÓN DEL DESASTRE: PLAN DE ACCION

El Plan presupone que debe utilizarse un Centro de Cómputo alterno externo al edificio sede de la CONTRALORÍA DE BOGOTÁ D.C., si la emergencia afecta en forma general (en un 60% o más) las instalaciones físicas y técnicas con que se cuenta. Los siguientes procedimientos se circunscriben a dichos hechos o casos.

10.2.1 PRIMERA FASE: Procedimientos Iniciales de Respuesta/Notificación

Los siguientes deben ser los procedimientos a ser implantados en el momento del desastre, procedimientos que deben continuar hasta que se restauren los servicios de procesamiento de datos en el sitio original u otro permanente.

En el caso de incendio, explosión u otro desastre mayor en el Centro de Cómputo, debe implantarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional previa notificación a uno de sus integrantes.

10.2.1.1 Procedimientos de Emergencia en la Sala de Computadores

Si la naturaleza del desastre no da tiempo para apagar y evacuar, la prioridad más alta es la seguridad de las personas. Ellos deben salir inmediatamente del Centro de Cómputo o área afectada. En un caso de éstos, el siguiente paso es notificar inmediatamente al grupo de administración de emergencia (Grupo de Salud Ocupacional o sus delegados).
Si hay tiempo para apagar, se deben realizar las siguientes actividades, en el orden especificado:

a) Inicializar procedimientos de emergencia organizacional estándar (los establecidos por el Grupo de Salud Ocupacional).
b) Ejecutar procedimientos de apagado para los servidores y demás dispositivos del centro de cómputo.
c) Apagar extractores
d) Apagar luces y bajar tacos en las cajas de distribución
e) Notificar al grupo de Administración de Emergencia

10.2.1.2 Grupo de Administración de Emergencia de la Dirección de Informática

Director de Informática
Coordinador Grupo de Análisis y Desarrollo
Coordinador Grupo Línea de Atención a Usuarios
Grupo Centro de Cómputo

10.2.1.3 ARBOL TELEFONICO DE EMERGENCIA

El grupo de emergencia, o su designado, llamará a los líderes de grupo de recuperación de desastre con información actualizada de la situación del desastre, junto con la localización y hora de reunión del Grupo de Administración de Emergencia.

10.2.1.4 Líderes de Grupo

Coordinador del Plan de Contingencias
Grupo de Administración de la Emergencia
Coordinador Centro de Cómputo

Estos líderes de grupo tendrán copias del Plan para el grupo, con la lista de las personas que lo conforman. El líder iniciará un árbol telefónico para contactar todos los miembros del grupo.

El Administrador asumirá la responsabilidad total del grupo de administración de emergencia. El Grupo de Administración de Emergencia hará una apreciación inicial de la extensión del desastre tan rápido como sea posible.

Será decisión del Grupo de Administración de Emergencia, si se inicializa el resto del Plan o no (Si se activa el Centro Alterno o no). Se espera que esto ocurra en un lapso de 4 horas después del desastre.

10.2.2 SEGUNDA FASE: Procedimientos para el proceso de restauración.

Tan pronto como se haya declarado un desastre, los líderes de grupo serán llamados para implantar el Plan a tomar en el desarrollo del Plan de Contingencias.

El grupo de Centro de Cómputo junto con el grupo de atención a usuarios establecerán un centro de control y empezarán la coordinación para la restauración de los sistemas que hayan sido afectados.

10.2.2.1 Acciones

Dentro de las 6 horas siguientes al desastre se debe:

- Notificar a los usuarios la interrupción del servicio.
- Notificar al Centro de Cómputo Alterno, Administrador, Servicios de Soporte, Director y otros.
- Activar el procesamiento manual de las aplicaciones (si es necesario)
- Efectuar una evaluación de daños e identificar el equipo reusable para transferirlo al Centro Alterno.
- Notificar al Proveedor las configuraciones de Hardware y alistar los

requerimientos.
- Notificar a todos los funcionarios de la Dirección de Informática, que están involucrados en el Plan.
- Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
- Inicializar las preparaciones ambientales en el Centro de Cómputo o Centro de Respaldo. (Eléctrica, protección contra incendio, extractores).
- Ordenar los circuitos para comunicación de datos en el Centro Alterno, si es necesario.

Dentro de las 24 horas siguientes al desastre debe:
- Contactar con el proveedor y ordenar el soporte tanto de hardware como de software
- Iniciar y coordinar los procedimientos de preparación del lugar para el Centro Alterno.
- Iniciar el ensamblaje de la documentación y medios magnéticos en el lugar de almacenamiento externo.
- Confirmar el soporte dado por el proveedor.
- Complementar el procesamiento de los reportes seleccionados en el Centro Alterno.

Dentro de los 2 días siguientes al desastre debe:
- Catalogar el despacho de suministros
- Trasladar el personal necesario y/o requerimientos al Centro Alterno
- Completar el ensamblaje de la documentación y los medios magnéticos en el Centro Alterno, coordinando la prestación de los servicios desde el Centro Alterno.

Dentro de los 3 días siguientes al desastre:
- El Centro Alterno debe estar totalmente preparado para operar
- Llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro Alterno.
- Recibir en el Centro Alterno suficientes suministros, muebles y equipo relacionado.
- Determinar el punto inicial de aplicaciones críticas.
- Establecer un catálogo de procesamiento de las aplicaciones críticas.
- Evaluar las líneas de comunicación de datos catalogados para una restauración inicial.

Dentro de los 4 días siguientes al desastre debe:

- Completar la preparación ambiental del Centro Alterno
- Recibir la documentación y el medio magnético de los lugares de almacenamiento en el Centro Alterno.
- Asegurar el ambiente físico en el Centro Alterno y establecer la seguridad de los datos.
- Restablecer los backups de datos de producción de las cintas de backups.
- Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
- Evaluar los sistemas operacionales
- Notificar a los usuarios el estado de la recuperación

Dentro de los cinco días siguientes al desastre:

- Asegurar la operación total de los sistemas críticos.
- Continuar la implantación por fases de la red de comunicación de datos

Dentro de los 28 días siguientes al desastre:

- Restauración completa de la red de comunicación de datos y de las operaciones.

10.2.3 TERCERA FASE: Procesamiento en el Centro de Cómputo Alterno

Las actividades paralelas listadas abajo caracterizan las acciones a tomar durante esta fase. Empiezan cuando los sistemas críticos y las redes de computación son operativas y no se ha podido completar la restauración de los datos del sistema. Esta fase continúa hasta que los servicios de procesamiento de datos son restaurados en el lugar u otro sitio permanente.

En este momento es cuando se debe informar al personal de las actividades que han sucedido y la operabilidad del plan. Los logs de recuperación del desastre se deben recolectar y analizar por parte del Grupo de Administración de Emergencia de la Dirección de Informática. Deben realizarse preparaciones en la marcha para regresar al sitio original o alternativo.

10.2.3.1 Actividades de esta Fase

- Asegurar un medio ambiente físico y restablecer la seguridad en los datos
- Comenzar el procesamiento de transacciones críticas

- Tener todos los recursos en su lugar en el Centro de Cómputo Alterno
- Localizar los procedimientos de backup y almacenamiento
- Obtener una recuperación total
- Distribución del grupo de personal y reportar a la administración

10.2.4 CUARTA FASE: Recuperación en el sitio original o alterno

Mientras que las operaciones se estén ejecutando en el Centro Alterno, se harán planes para la recuperación total en el sitio original. Si hay un desastre mayor, o si está dentro de los planes de la organización, se puede realizar la recuperación en un sitio alterno improvisado. Esta fase es muy similar a la descrita en la fase 3 pero en una localización permanente.

Los siguientes son los componentes procedimentales importantes de las actividades en esta fase:

- Decisiones en el tiempo y equipo de recuperación
- Preparar restauración del lugar
- Desarrollo de los procedimientos de recuperación para la localización permanente.
- Repetir los procedimientos de recuperación
- Asegurar el ambiente físico y establecer la seguridad de los datos
- Montaje de los sistemas
- Evaluación de los sistemas
- Convertir a procesamientos en producción
- Realizar auditoría post-desastre
- Preparar reclamación de los seguros
- Reportar a la administración

10.2.5 QUINTA FASE: Mantenimiento

Parte del mantenimiento del Plan será la Programación de sistemas requeridos para mantener los programas con los cambios sobre el tiempo, del hardware, software y aplicaciones. Esta es obviamente la clave para el futuro exitoso del plan. La actualización de nombres, responsabilidades y números telefónicos de los participantes claves es además críticamente importante. El Plan será auditado para ver que estos detalles sean actualizados rutinariamente en el Plan y en todas sus copias.

11. IMPLEMENTACION DEL PLAN

Para la implementación del Plan, deben estar formalmente documentados, y en operación, los siguientes procedimientos:

- Retención y respaldo de archivos permanente y corriente de cada dependencia, software específico y operativo.
- Recuperación de errores y fallas del sistema
- Seguridad física y lógica
- Mantenimiento preventivo y correctivo de equipos
- Administración de personal en lo referente a las emergencias

En primera instancia, el presente plan debe ser puesto a consideración, revisión y aprobación por parte del Comité de Informática. Seguido, debe ser probado y simulado.

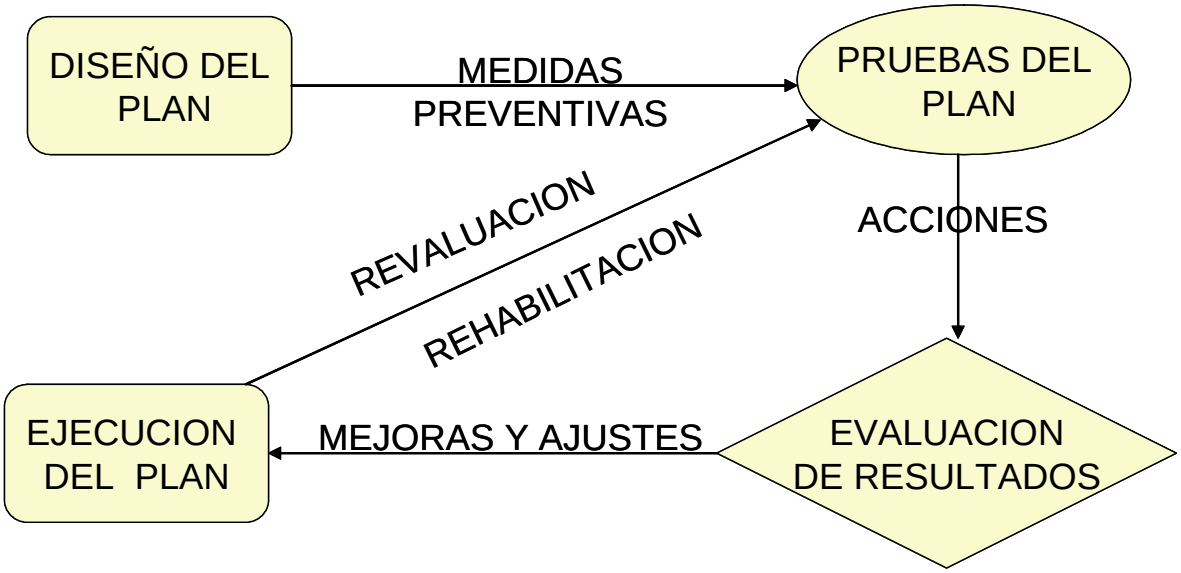
En segunda instancia, desarrollar un programa de entrenamiento a los sujetos y áreas directamente involucradas, aquellas que asumen responsabilidades y funciones dentro del plan.

Finalmente, debe adoptarse a nivel institucional mediante Acto Administrativo, es decir, reglamentado por Resolución emanada del despacho del Contralor Distrital.

Posteriormente, se debe recopilar bimensualmente las modificaciones al plan y realizar actualizaciones periódicas al mismo.

12. PLAN EXPERIMENTAL DE PRUEBAS

El plan de contingencias comprende, finalmente, el desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.



El mayor énfasis será ejercido sobre las pruebas o simulacros, y sobre los eventos posteriores a la emergencia relacionados con el reinicio de las operaciones normales de la Contraloría de Bogotá.
Los siguientes son los objetivos de control y auditoria de las pruebas del plan:

- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.

- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación
- Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias
- Estar preparado para evaluar las necesidades de seguros y reducir al máximo los costos en primas de aseguramiento
- Motivar a los funcionarios involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos inherentes

La Oficina Asesora de Control Interno evaluará que sean definidas las responsabilidades de las pruebas del plan, tales como:
Personal de administración: Grado de participación y compromiso, Niveles jerárquicos de aprobación y Asignación de recursos, capital y tiempo.
Personal del área de informática: Programación, operación y soporte técnico
Grupo de usuarios por segmento operativo
Personal externo: Proveedores, grupos de apoyo internos o externos y centros de recuperación contratados o comprometidos.
La Oficina Asesora de Control Interno conocerá la frecuencia de las pruebas y la periodicidad de cambios en el ambiente informático o cualquier ajuste en el mismo.
La Dirección de Informática y la Oficina Asesora de Control Interno, identificarán y documentarán los diferentes niveles de prueba del plan. Estos pueden ser por segmentos, por áreas relacionadas o a gran escala; éste último, como prueba global del plan, según los lineamientos que establezca el comité directivo. Como métodos de prueba, se sugieren: en papel, real o a gran escala probado por segmento mediante simulacro a criterio del comité directivo con apoyo del grupo de desarrollo; la Oficina Asesora de Control Interno conocerá los períodos de prueba.

12.1 PASOS PARA CONDUCIR LA PRUEBA

El grupo de desarrollo del plan indicará a la Oficina Asesora de Control Interno el esquema ordenado de las pruebas, teniendo en cuenta:
1) Selección del sujeto de la prueba para identificar los aspectos o capítulos del plan que están siendo evaluados
2) Descripción de los objetivos de la prueba y mecanismos de medición del alcance exitoso de los objetivos
3) Reunión con el comité directivo para explicar la prueba y sus objetivos, y obtener como resultado su acuerdo y soporte4) Comunicación formal de una

prueba anunciada, los factores críticos a considerar y el tiempo estimado de la prueba.

5) Consolidación de los resultados de la prueba al final de ésta.
6) Evaluación de resultados: progresos, inconvenientes y logros.
7) Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple (segmento) puede tomarse como referencia para la realización satisfactoria de todos los capítulos del Plan (a gran escala)
8) Generación de recomendaciones para cambios o ajustes, definición de la fecha límite para respuesta y gestión
9) Notificación de los resultados de las pruebas al comité directivo y por su intermedio al nivel directivo de la Contraloría de Bogotá
10) Cambios en documentación o manuales, si es aplicable.

12.2 AREAS O PARTES A PROBAR

- Recuperación del sistema aplicativo individual utilizando archivos y documentación almacenada en el sitio externo
- Habilidad para procesar en modo "degradado" o limitado
- Recarga de los discos del sistema y de los procedimientos de carga y arranque utilizando archivos y documentación almacenada en el sitio externo
- En sitios de procesamiento alterno, solución de diferencias en configuración de equipos
- Disponibilidad de equipos periféricos y de procesamiento
- Disponibilidad de equipos de soporte: aire acondicionado, unidades de potencia no interrumpida de corriente eléctrica
- Disponibilidad de soporte logístico: provisiones, transporte y comunicaciones.
- Evacuación del equipo desde el centro de cómputo de la Entidad, en respuesta a eventos tales como inundación o terrorismo.
- Habilidad de la administración y del comité directivo para determinar la prioridad de sistemas cuando se procesa con recursos computacionales limitados.
- Habilidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la pérdida del personal o turnos primarios.
- Habilidad para adaptar el plan a desastres menores.

- Efectividad de alternativas manuales para aquellos sistemas que confían en esa opción.
- Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
- Habilidad de los usuarios para continuar con las operaciones normales de la entidad para los sistemas clasificados como no críticos.
- Habilidad para establecer contacto en un período definido por emergencia y de manera organizada, con el personal clave o sus designados alternos.
- Nivel de cumplimiento de los estándares normativos aprobados por la entidad.
- Identificación de los recursos utilizados durante la emergencia que son cubiertos por la póliza de seguros.
- Distribución correcta y oportuna de listados, transmisión de datos vía telefónica conmutada, servicios de correo.
- Disponibilidad de formas y cantidad mínima de papelería. Control de formas numeradas o asimilables a títulos valores.
- Adherencia nula, parcial o total a medidas de seguridad durante el período de emergencia.
- Habilidad para ejecutar tareas de evacuación y tratamiento de primeros auxilios.
- Mecanismos para recuperación de información perdida en caso de sistemas en línea.
- Análisis de tiempos y movimientos durante las pruebas.

12.3 PROCESO GENERAL PARA PRUEBA ANUNCIADA

1) Presentación a consideración del comité directivo
2) Procedimiento de comunicación formal
3) Desarrollo de la prueba

12.4 PROCESO GENERAL PARA SIMULACRO

1) Presentación a consideración del comité directivo
2) Desarrollo del simulacro

13. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad de información son la piedra angular de la eficacia de la seguridad de la información, sin una política sobre la cual basar los estándares y procedimientos, las decisiones tomadas serán probablemente inconsistentes y los agujeros de seguridad estarán presentes listos para ser explotados por personas internas y externas a la organización.

Esta es una primera fase en la implementación de políticas, para evaluar su aceptación y cumplimiento en la organización.

13.1 REINICIALIZAR O RESTAURAR SU SISTEMA

Los propietarios de los sistemas de información deben asegurarse de la existencia de un backup completo y que los procedimientos de recuperación de sistemas están en su sitio.

Descripción
Facilita las instalaciones para asegurar que su equipo reinicie exitosamente después de una interrupción voluntaria o involuntaria.

- No tener disponible el sistema después de una interrupción en el proceso normal puede impactar la eficiencia en las operaciones de la entidad.
- Pérdida de información después de una interrupción en el proceso normal, puede interrumpir las operaciones y retrasar los procesos de la entidad.

13.2 PANTALLA SIN INFORMACIÓN VISIBLE

Los usuarios de los computadores de la Contraloría de Bogotá deben asegurarse que su monitor o pantalla se encuentre en blanco, cuando el usuario no la este utilizando.

- Si la pantalla es legible cuando el usuario se encuentra ausente de su escritorio o de su lugar de trabajo, esto podría dar como resultado que la información confidencial (sensible) pueda ser leída por personal no autorizado.

- Cuando el personal puede ver como un sistema confidencial es accesado, esto puede facilitar su premeditación a intentos oportunos para leer y copiar los datos cuando el computador es abandonado aunque sea por un corto periodo.

13.3 MANEJO DE BACKUPS Y PROCEDIMIENTOS DE RECUPERACION

El backup de los archivos de información de la organización y la habilidad para recuperar información es una prioridad alta. La administración es responsable por asegurar que la frecuencia de cada operación de backup y los procedimientos de recuperación se ajusten a las necesidades de la organización.

Los procedimientos usados para iniciar una recuperación deben ser claramente documentados y probados. Si los procedimientos de restauración no han sido probados, una restauración parcial o incompleta puede corromper la integridad del sistema.

Descripción

- Cuando los procedimientos de backups son inadecuados o débiles, la información puede perderse o no estar disponible, lo que compromete la confiabilidad de los procesos de la organización.

- Modificaciones maliciosas, de los resultados de la secuencia diaria del backup dentro de una falla para proteger todos los datos requeridos.

13.4 ARCHIVAR INFORMACIÓN

Los medios de almacenamiento usados para archivar la información deben ser apropiados de acuerdo a las expectativas de vida de la información. El formato en el cual es almacenada la información debe ser cuidadosamente considerado, especialmente cuando los formatos propios están implicados.

Se hace referencia a la información la cual no es requerida en el día a día, pero la cual necesita ser guardada por un cierto periodo y también información la cual debe ser guardada perpetuamente. Los datos que son removidos del procesamiento cotidiano, reducen los niveles de almacenamiento y de recursos de procesamiento.

Las recomendaciones que deben ser consideradas cuando se implemente esta política incluyen lo siguiente:

Las debilidades en la longevidad de los medios usados para archivar, pueden causar fallas en la restauración de los datos cuando eventualmente sean requeridos.

Los datos archivados pueden ser conservados a menudo en un formato del usuario que sea apoyado solamente por los sistemas actuales, asi intentos frustrados de acceso.

13.5 ENVIO DE CORREO ELECTRONICO

El e-mail se debe utilizar solamente para los propósitos institucionales, usándolo en términos que sean consistentes con otras formas de comunicación de la Entidad. Los archivos adjuntos a un e-mail se pueden adjuntar solamente después de confirmar la clasificación de la información que es enviada y después de explorar y verificar que el archivo no posee virus o código malévolo.

Descripción

- El uso de e-mail se ha hecho tan popular hasta el punto donde es obligatorio para todas las compañías ser accesadas a través de este medio. La carencia inherente de seguridad para enviar mensajes, información, archivos o instrucciones aparentemente es ignorado por muchos usuarios que utilizan este servicio.

- Enviar e-mail usando firmas digitales (opcionalmente encriptado) es una forma de asegurar su validez e integridad. El contenido de e-mail recibidos sin autenticación podría ser considerado poco fiable.

    1. La transmisión de un virus puede no solamente causar daño en los equipos sino que puede dañar permanente la reputación de la organización.
    2. Enviar un e-mail vía líneas publicas (por ejemplo internet) puede comprometer la confidencialidad e integridad de la información que está siendo transmitida. Esto es similar a una carta postal porque cualquiera que la pueda abrir, la puede leer.
    3. Archivos confidenciales podrían ser transmitidos por e-mail como adjuntos, rompiendo así la confidencialidad y potencialmente ocasionando pérdidas financieras.
    4. Enviar una copia de archivos a los colegas dentro de la red interna, crea duplicados innecesarios y también compromete la integridad del documento o archivo original.

14. CONCLUSIONES

- En el presente Plan de Contingencias se describen los métodos y procedimientos a seguir en la Contraloría de Bogotá D.C. en caso de presentarse desastres que destruyan, modifiquen o alteren la información y los equipos de computo que la procesan, con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado cumplimiento de sus Objetivos Institucionales.

- Lograr integración interinstitucional, a través de convenios entre las entidades públicas de tal forma que se ofrezca apoyo en sus centros de cómputo principales y alternos con la implementación de aplicaciones de propósito común, compatibles entre sí, garantizando el desempeño y continuidad en cada una de sus funciones.

- Concientizar a los funcionarios de la Entidad acerca de la seguridad de la información, labor que no es sólo de la dirección de Informática, sino que debe comprometer a toda la organización.

- Con el desarrollo de este trabajo en la Contraloría se establecen los perfiles acerca de las labores que ha de cumplir el grupo encargado del seguimiento del Plan de Contingencias.