Radio Televisión Nacional de Colombia
RTVC

Plan de recuperación, reanudación y contingencia informática de **rtvc**

Índice

I. RIESGOS IDENTIFICADOS Y RELACIONADOS A LOS SISTEMAS DE INFORMACIÓN

Se define como riesgo una situación la cual, si ocurrieran, afectaría de forma negativa el desarrollo normal de actividades dependientes de tecnologías de información y comunicación. Por su nivel de criticidad deben ser previstos antes de su ocurrencia.

El Plan de Contingencia se diseña con el objetivo de reaccionar ante la ocurrencia de dichos riesgos y en el caso que se lleve en ejecución dicho Plan, se debe soportar en el Plan de Recuperación y Reanudación que garantice la continuidad del negocio de nuestra entidad. El Plan de recuperación de desastres es diseñado con el objetivo de reaccionar en el caso que un desastre impida prestar los servicios por daños físicos resultantes de este hecho.

Los riesgos tienen un conjunto de componentes a considerar: el evento de riesgo como tal, su probabilidad de ocurrencia y la gravedad del impacto de los efectos en caso que ocurriera.

Se definirán los riesgos según sus particularidades en las siguientes categorías:

- Riesgo de hardware e infraestructura y comunicaciones (HARDWARE)
- Riesgos por software de terceros (SOFTWARE)
- Riesgo de información (INFORMACIÓN)
- Riesgo provenientes de usuarios (USUARIOS)

En la Tabla 1, se sintetizan los riesgos identificados, de los cuales se entregan respuesta en el presente plan de contingencia.

Radio Televisión Nacional de Colombia
RTVC

Id. Riesgo	Categoría	Riesgo	Probabilidad de ocurrencia	Gravedad del impacto
HARD01	HARDWARE	Inundación	Baja	Alta
HARD02	HARDWARE	Incendio	Baja	Alta
HARD03	HARDWARE	Corte de energía eléctrica	Media	Media
HARD04	HARDWARE	Robo de equipos o cualquier elemento de la infraestructura	Baja	Alta
SOFT01	SOFTWARE	Virus informáticos	Media	Media
USUA01	USUARIOS	Ataques de confidencialidad de parte de los usuarios de rtvc para acceder a información a la cual no tienen permisos	Baja	Alta
HARD05	HARDWARE	Problemas de comunicación de los equipos clientes con los servidores	Media	Alta
HARD06	HARDWARE	Problemas de cableado eléctrico de las estaciones de trabajo	Baja	Baja
HARD07	INFORMACIÓN	Problemas con recursos compartidos de la red	Media	Media
SOFT02	SOFTWARE	Caída de las bases de datos	Baja	Alta
HARD08	HARDWARE	Falla mecánica en un equipo servidor	Baja	Alta
SOFT03	SOFTWARE	Caída del servicio que presta un servidor	Baja	Baja
HARD09	HARDWARE	Pérdida total del servidor	Baja	Alta
HARD10	HARDWARE	Pérdida de las estaciones de trabajo por daños irreparables	Media	Baja
USUA02	USUARIOS	Hackeo de cuentas de dominio	Baja	Media
SOFT03	SOFTWARE	Borrado de información en los servidores	Media	Alta
SOFT04	SOFTWARE	Hackeo de los sitios web de la entidad	Media	Alta
HARD11	HARDWARE	Problemas de acceso inalámbrico a la red LAN de rtvc.	Alta	Media

SOFT05	SOFTWARE	Spamming al servidor de correo	Baja	Baja
HARD12	HARDWARE	Daño en una impresora de la entidad	Baja	Baja
HARD13	HARDWARE	Daño en el enrutador de salida a Internet	Baja	Alta
HARD14	HARDWARE	Daño en dispositivos de comunicaciones de la infraestructura de red	Baja	Media
USUA03	USUARIOS	Borrado de información por personal que ya no trabaja en la entidad desde sus perfiles de usuario	Baja	Media
USUA04	USUARIOS	Usuarios con privilegios instala software no licenciado	Media	Alta
USUA05	USUARIOS	Ataques a sitios externos a través de máquinas de la entidad	Baja	Alta
USUA06	USUARIOS	Notificación tardía de cierre de cuenta a usuarios que ya no trabajan para la entidad que conlleva a pérdida de datos o ataques de disponibilidad de los servicio	Media	Alta
HARD15	HARDWARE	Atentados terroristas	Baja	Alta
HARD16	HARDWARE	Terremotos	Baja	Alta
HARD17	HARDWARE	Daño en el cableado estructurado	Media	Alta
USUA07	USUARIOS	Problemas de manejo de contraseñas por falta de comprensión de la importancia de la confidencialidad de las contraseñas.	Media	Media
SOFT05	SOFTWARE	Problemas de planeación al momento de la contratación que no permite garantizar los elementos informáticos adecuados según el área de desempeño.	Media	Media

Radio Televisión Nacional de Colombia
RTVC

II. PLAN DE RECUPERACIÓN DE DESASTRES DE RTVC

1. Introducción

El Plan de recuperación de desastres, acompañado de los servicios de contingencia y del personal de rtvc asignados para tal fin, descritos en este documento, aseguran que un ambiente de cómputo efectivo esté disponible dentro del plazo estipulado siguiente a la notificación por parte de un representante o personal autorizado que informe un desastre en la entidad.

Este documento permite garantizar la continuidad del negocio después de la ocurrencia de eventos que afecten las operaciones. Este objetivo se alcanza por medio de la habilidad de planear, prevenir y recuperarse ante la ocurrencia de un evento de dicha naturaleza.

2. Plan de recuperación de desastres

Este plan consiste en la habilidad de continuar operando después de la ocurrencia de un evento con la capacidad de interrumpir las operaciones. Los sistemas tolerantes a desastres se diseñan para permitir que las operaciones continúen durante el periodo de reconstrucción posterior al evento del desastre.

El sitio de respaldo alterno es vital para **rtvc** ya que este se utilizaría en forma inmediata en caso de presentarse inconvenientes de tipo desastre total o parcial, este sitio puede ser cualquier sitio alterno que cuente con una conexión de Internet y equipos servidores con sistema operativo *Windows 2003 Server Standard* y *Linux Ubuntu Hardy Heron*, allí se trasladaría el personal de

informática o quienes en su momento sean los encargados de realizar la reanudación de las operaciones informáticas.

Se deben tener en cuenta los siguientes aspectos para la restauración de desastres:
2.1 Contar con los sistemas informáticos, de comunicaciones de infraestructura que provean la plataforma tecnológica sobre los que funcionan los sistemas y la información de la entidad.
2.2 Contar con los programas y archivos (instaladores), contraseñas, manuales de instalación y configuración.
2.3 Contar con la información (bases de datos y documentos) a restaurar los cuales deben ser poder ser recuperados a través de los backup locales y/o backup remotos.
2.4 Contar con un plan de recuperación de desastres.

3. Los eventos que denotan posibles desastres

Los eventos que denotan posibles desastres identificados en **rtvc** se relacionan con cortes de energía, desastres naturales (temblores, rayos, inundaciones), daños de hardware (fallos de discos duros, main board, memorias, fuentes de poder, dispositivos de conectividad), virus, intrusiones no autorizadas, errores de operación, desconfiguración o fallos de software. Para ello **rtvc** cuenta con los siguientes planes para cada caso:

3.1 Plan de recuperación en caso de fallo de energía eléctrica

rtvc por la misma función que cumple de emisión en radio y televisión las 24 horas del día, posee UPS´s de tipo corriente regulada que suministra constantemente corriente tanto a equipos de cómputo como a los equipos que se utilizan para la emisión de la programación y en caso de que la falla en el fluido eléctrico sobrepase el tiempo de carga de las UPS´s. Se poseen plantas eléctricas que se activarían por el personal encargado de Servicios Generales o la persona encargada en el momento de presentarse el imprevisto (estas personas activan las plantas eléctricas previstas para estos casos).

3.2. Plan en caso daño virus o intrusiones no autorizadas

Los equipos de **rtvc** en la actualidad tienen instalada la suite de Avira Security Management Center, compuesta a su vez por el *"Avira Security Management Center Frontend"* la cual permite administrar y gestionar de forma centralizada todos los equipos que pertenecen a rtvc.

También se encuentra compuesta por un servidor de actualizaciones, que consiste en un repositorio debidamente configurado que gestiona las descargas "*on line"* de los últimos paquetes, programado de tal forma que se ejecute cada (1) hora y éste a su vez actualiza cada (3) tres horas a todos los equipos incluyendo estaciones de trabajo, servidores y portátiles que en ese momento se encuentren en producción. Este método permite un ahorro considerable de canal y tiempo de actualización sobre los equipos clientes.

Adicionalmente se encuentra instalado un dispositivo de hardware Firewall, para seguridad perimetral JUNIPER SSG-140, basado en tecnología UTM *"Unified Thread Management"* la cual integra una solución Antivirus, Antispam, Anti Adware, AntiKeylogger, Web Filtering, IPS (*Deep Inspection*), Este conjunto de herramientas adicionales inspecciona todos los paquetes y protocolos POP3, HTTP, SMTP, IMAP, FTP, IM, antes de ingresar a la LAN de rtvc, ofreciendo así mayor protección y previniendo cualquier tipo de ataque.

4. Responsables dentro del plan de recuperación

Son aquellas personas en la organización que tienen la autoridad para declarar un desastre y por ende, colocar el plan en efecto. **rtvc** cuenta con una división llamada Subgerencia de Soporte Corporativo y en cabeza del Subgerente Corporativo que es la persona líder encargada de coordinar todas las áreas que tienen que ver con el suministro, mantenimiento, adecuación y protección de las locaciones y equipos, a ella pertenece la Jefatura de Informática, que es el área a la cual nos estamos refiriendo en este caso, estas dos dependencias son las encargadas de acuerdo a las circunstancias que se estén presentando para iniciar el proceso de acuerdo al tipo de desastre y/o amenaza que se esté viviendo.

En caso de que se deba evacuar **la oficina de informática de rtvc** de las instalaciones actuales por circunstancias ajenas, puede desplazarse a cualquier oficina del edificio que cuente con alimentación eléctrica regulada y conectividad que le permitirá interconectar los equipos que cubran la contingencia para restaurar los aplicativos e información para darle continuidad a las operaciones urgentes o prioritarias de la entidad, también allí se desplazaría el personal de informática para iniciar las labores de restauración de los aplicativos si fuere el caso junto con el personal contratista de los aplicativos que se encuentran instalados en **rtvc**. A estas instalaciones se llevarían los equipos necesarios para la restauración de los backups de aplicativos, estos dispositivos son las cintas donde se almacena la información y la unidad de backup.

4.1 Responsables dentro del plan de recuperación

Papeles y responsabilidades de todo el personal clave con respecto a llevar a cabo el plan (definir roles y responsables)

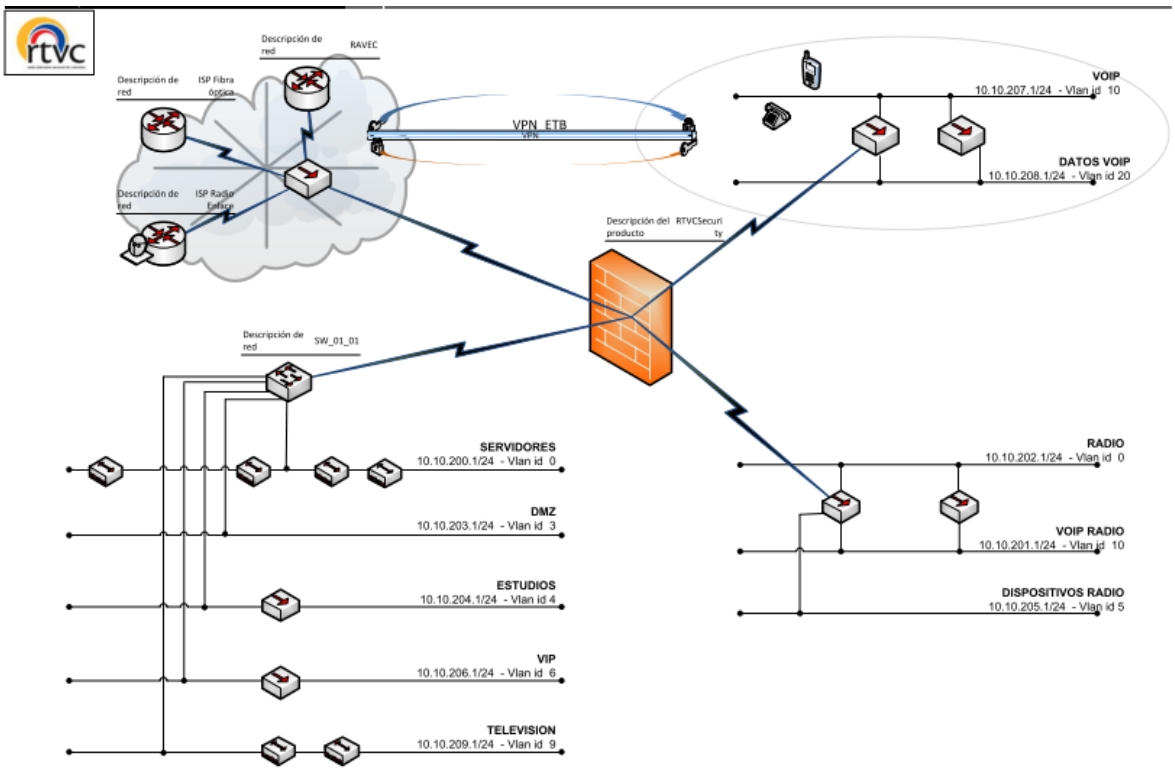
- **Jefe de informática**, es el encargado de planear, dirigir, controlar, instalar y configurar los sistemas y delegar las labores que se deriven según el caso presentado durante el desastre.
- **Personal de soporte técnico informático**, es la persona encargada de instalar, configurar y poner en marcha todos los equipos que se requieren para reiniciar la producción, a su vez colabora con los proveedores externos para facilitarles las labores que competan a cada uno de ellos y,
- **Servicios Generales**, son los encargados de proveer toda la infraestructura eléctrica, tomas, extensiones, teléfonos al personal que lo requiera en el sitio alterno.

5. Inventario y recursos necesarios para el plan de recuperación de desastres

Corresponde a las necesidades requeridas para restaurar los sistemas en producción.

5.1 Diagrama lógico de la red

Corresponde a una visión general de la arquitectura de red implementada en rtvc, este diagrama se encuentra en la ruta *"\\10.10.2000.5\documentacion$\2012\red\Mapa red.pdf".*



Inventario de Equipos RTVC que deberían ser puestos en producción prioritariamente
Este es el inventario de los equipos y usuarios a los cuales se les debe preparar equipos para continuar con las funciones pertenecientes a RTVC

5.2 Inventario de equipos

rtvc cuenta con (5) cinco servidores, de los cuales se mantiene actualizada su hoja de vida y se puede encontrar sobre la unidad documentación o através del software de control de inventarios Discovery.

Allí se especifica el rol asignado a cada uno de los servidores y sus características con los servicios ofrecidos.

6. Disponibilidad del Hardware y Software

El plan de recuperación de desastres debe incluir métodos para conseguir el hardware y software necesarios para las operaciones en el sitio de respaldo. Un sitio de respaldo manejado profesionalmente quizás ya tenga todo lo que usted necesita (o quizás tenga que organizar la adquisición y entrega de materiales especializados que el sitio no tiene disponibles); por otro lado, un sitio de respaldo frío implica que se tienen identificadas las fuentes para cada ítem requerido. A menudo las organizaciones trabajan directamente con los fabricantes para establecer acuerdos para la entrega inmediata de hardware y/o software en el evento de un desastre.

7. Disponibilidad de los respaldos

Cuando se declara un desastre, es necesario notificarlo a la empresa que maneja el almacenamiento fuera de sitio por dos razones:
· Para enviar los últimos respaldos al sitio de respaldo.

· Para coordinar entregas de respaldos regulares, al sitio de respaldo.

8. Conectividad de red al sitio de respaldo

Un centro de datos no es de mucha ayuda si se encuentra desconectado del resto de la organización que está sirviendo. Dependiendo del plan de recuperación de desastres y de la naturaleza del mismo, su comunidad de usuarios puede estar ubicada a kilómetros de distancia del sitio de respaldo. En estos casos, una buena conectividad es vital para restaurar la producción.

Otro tipo de conectividad a tener en mente es la conectividad telefónica. Debe asegurarse de que existen suficientes líneas telefónicas disponibles para manejar todas las comunicaciones verbales con sus usuarios. Lo que antes podía ser un grito por encima de la pared de un cubículo ahora implica una conversación telefónica de larga distancia; por lo tanto, se deben contemplar cómo va a ser la comunicación telefónica de la que pudiera parecer necesaria en un principio.

9. Personal del sitio de respaldo

El problema sobre conseguir el personal para su sitio de respaldo es multidimensional.

Un aspecto del problema es determinar el personal requerido para poner a funcionar el centro de datos de respaldo por el tiempo que sea necesario. Mientras que un equipo esquelético puede mantener las cosas en funcionamiento por un corto período de tiempo, a medida que el desastre se extiende se necesitará más y más gente para continuar el esfuerzo necesario para funcionar bajo las circunstancias extraordinarias que rodean un desastre.

Esto implica asegurarse de que el personal tiene tiempo suficiente para descansar y posiblemente viajar de regreso a sus hogares. Si el desastre fuese tan extendido que afecte también los hogares y familias de la gente, se necesitará tiempo adicional para permitirles manejar su propia recuperación de desastre. Se necesita alojamiento temporal cerca del sitio de respaldo, junto con el transporte requerido para movilizar a la gente entre el sitio de respaldo y su alojamiento.

A menudo un plan de recuperación de desastres incluye que trabaje en el sitio un personal representativo de todas las partes de la comunidad de usuarios de la organización. Esto depende en la habilidad para operar con un centro de datos remoto. Si los usuarios representantes deben trabajar en el sitio de respaldo, también deben estar disponibles facilidades similares para ellos.
rtvc en caso de presentarse un evento que denote un posible desastre como Terremotos, Cortes de energía, daños de hardware, virus, intrusiones no autorizadas, desconfiguración o fallo de

software etc. Posee para ello planes alternos que se colocarían en marcha de acuerdo al evento inesperado que se presente.

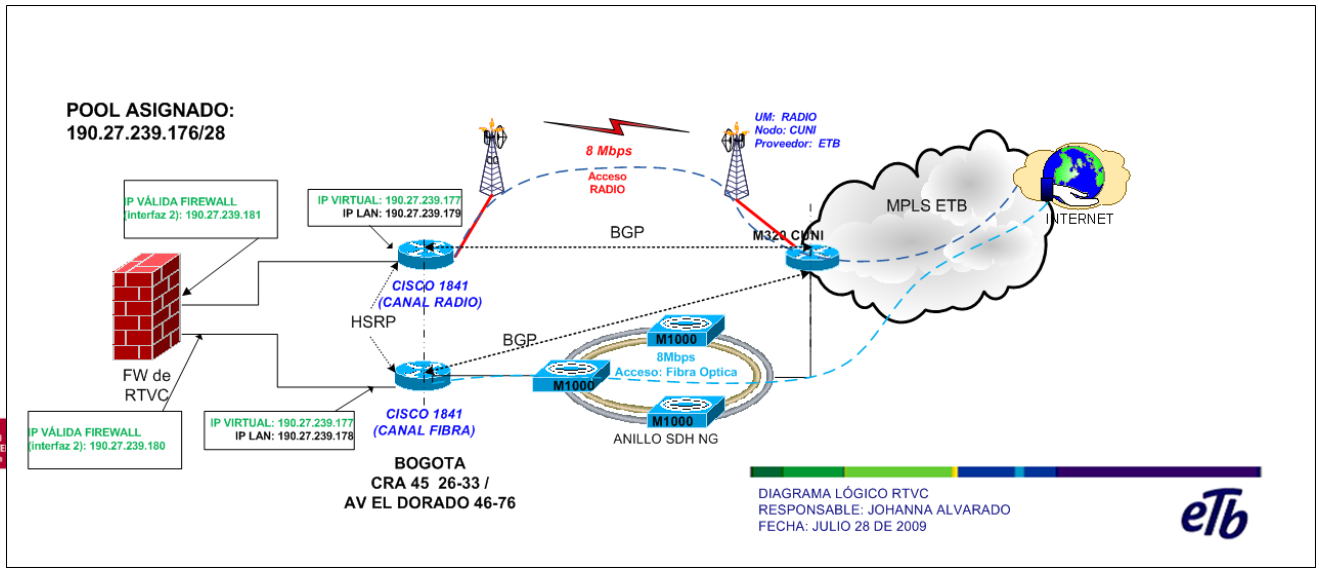
III. PLAN DE CONTINGENCIA

Un plan de contingencia que especifica los medios para manejar eventos externos que puedan tener serio impacto en la organización.

1. Plan en caso de fallo del servicio del proveedor de Internet (ISP)

Actualmente ETB provee a toda la entidad de conectividad a Internet con una conexión ***Activo/Pasivo*** de 20 Mbps a través de dos medios físicos diferentes el primero es a través de Fibra óptica la cual permite un optimo desempeño y rendimiento sobre el canal y el segundo es con un radio enlace.

Mediante el protocolo de comunicación *bgp* "***Border Gateway Protocol",*** en caso que se presente algún fallo, automáticamente al cabo de 10 segundos se activa el otro medio de transmisión que es radio enlace, que provee el mismo rendimiento y permite continuidad en las comunicaciones, teniendo en cuenta también que los dispositivos de comunicación son diferentes tenemos dos alternativas de continuidad en la conectividad para respaldar las actividades del negocio ofrecidas por un mismo proveedor, como se describe en el siguiente diagrama lógico de la red hacia rtvc.



2. Plan en caso de fallo de energía eléctrica

rtvc por su naturaleza y funciones de mantener permanentemente transmisiones de radio y televisión permanente posee UPS´s de tipo corriente regulada que suministra constantemente corriente tanto a equipos de computo como a los equipos que se utilizan para la emisión de la programación y en caso de que la falla en el fluido eléctrico sobrepase el tiempo de carga de las UPS´s, se poseen plantas eléctricas que se activarían por el personal encargado de Servicios generales o la persona encargada en el momento de presentarse el imprevisto estas personas activan las plantas eléctricas previstas para estos casos.

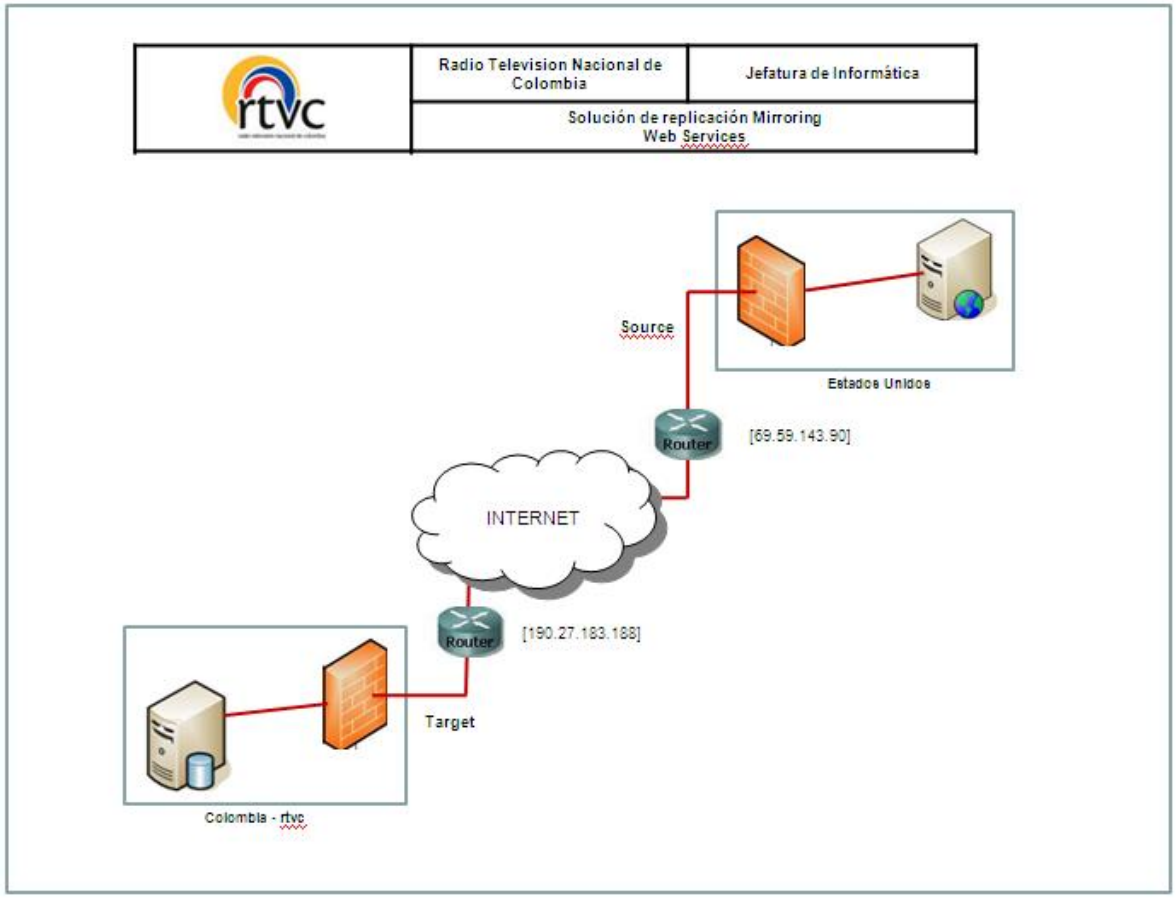
3. Plan en caso de fallo del proveedor de servicios WEB

La infraestructura tecnológica **WEB** de **rtvc** actualmente esta soportada bajo un esquema de recuperación y copia de los datos del ambiente productivo, que se realiza de manera permanente en rtvc. Consiste en un "*Mirror*" o copia remota mantenida en tal forma que permita la continuidad de los servicios ofrecidos de cada una de las páginas web (*www.rtvc.gov.co*, *www.institucional.gov.co*, *www.senalcolombia.gov.co*, *www.radionacionaldecolombia.gov.co*, *www.radionica.gov.co*, *www.bicentenario.gov.co*) en caso de la pérdida del servicio en el Datacenter de ServePath ubicado en Estados Unidos – San Francisco CA donde esta alojado el servidor dedicado para los sitios web de rtvc.

Mirroring es una solución para replicar datos de un sitio primario (o local) a un sitio alterno (o remoto) entre servidores a través de una red de datos LAN o WAN.
Ofrece además un mínimo impacto en los recursos de redes y comunicaciones existentes.

Modo de operación: monitorea cualquier cambio a los archivos de datos críticos definidos en la maquina fuente y envía los cambios a la máquina destino. Replicando únicamente los cambios de los archivos en vez de copiar todo nuevamente, permitiendo utilizar los recursos eficientemente. Captura los cambios que son escritos en la fuente y los envía al destino continuamente. La replicación mantiene al destino actualizado y sincronizado con la fuente.

En términos de recursos de red y tiempo, replicar los cambios es un método más eficiente de mantener una copia de los datos en tiempo real que copiar un archivo completo que ha sido cambiado.



4. Plan en caso de Desastre Natural (Incendio, Inundación, Terremoto)

En los equipos y servidores que se designen y que servirían para reiniciar temporalmente las labores de los usuarios. En caso de requerir específicamente restaurar el sistema de información financiero y administrativo "SEVEN", **rtvc** deberá solicitar los archivos instaladores y programas de forma de poder dejar funcional el sistema en los equipos adquiridos para cubrir la contingencia y procederá a recuperar los backup de información del sistema del lugar de resguardo local (caja fuerte del 3o piso) de **rtvc** y/o del sistema de backup remoto.

5. Plan en caso de falla por servidor

Este Plan consiste en los procesos que se deben desarrollar en el caso que exista alguna falla que impida que un servidor continúe operando sus servicios normalmente. La información documentada que se menciona en las actividades también se encuentra debidamente replicada en las copias de seguridad externa, para los casos en que la eventualidad impida el acceso a los servidores que contienen la información.

A continuación se exponen las actividades a realizar en caso de fallas por cada servidor:

5.1. Servidor 1(DC, DNS, File System, Printers)

Proceso-Tiempo estipulado	Responsable	Actividad
TOLERANCIA A FALLOS	Administrador	Gracias a que el servidor cuenta con una tarjeta Smart Array (para servidores HP), se configuró un arreglo de discos por Hardware en Raid 5 que garantiza tolerancia permanente a fallas de disco
INSTALACION SISTEMA OPERATIVO 01:30:00	Administrador Servidores – Personal Soporte técnico	TENER DOCUMENTACION Tener a la mano la documentación, Hoja de vida y software correspondiente al servidor INSTALACION DE SISTEMA OPERATIVO Tener en cuenta la información que se encuentra documentado en la H.V. ubicada en la unidad *"W:documentación\Hojas de vida servidores\Servidor1.docx"*
INSTALACION ACTUALIZACIONES Y ANTIVIRUS 00:20:00	Administrador Servidores – Personal Soporte técnico	INSTALAR ACTUALIZACIONES INSTALAR ANTIVIRUS Ir a la ruta para encontrar los instaladores: \\10.10.200.5\software$\Antivirus\Avira\cliente\agent_en.exe \\10.10.200.5\software$\Antivirus\Avira\cliente\antivir_profesional_es.exe Documentación de instalación: w:\\AVIRA_2009\capacitacion.ppt
INSTALACION	Administrador	Referirse al manual de instalación ubicado en la ruta

DC[1]	Servidores	*"W:documentación\documentacion tecnica\server1\manual dc, DNS.doc"*
INSTALACION DNS	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\server1\manual dc, DNS.doc"*
INSTALACION FILE SYSTEM	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\server1\manual dc, DNS.doc"*
INSTALACION PRINTERS	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\server1\manual dc, DNS.doc"*
RESTAURACION BASE DE DATOS ACTIVE DIRECTORY	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\server1\manual dc, DNS.doc"*

[1] DC son las siglas de Domain Controller, Controlador de Dominio.

5.2. Servidor 2(Sistema Administrativo y Financiero Seven)

Proceso-Tiempo estipulado	Responsable	Actividad
INSTALACION SISTEMA OPERATIVO 01:30:00	Administrador Servidores	TENER DOCUMENTACION Tener a la mano la documentación, Hoja de vida y software correspondiente al servidor INSTALACION DE SISTEMA OPERATIVO Tener en cuenta la información que se encuentra documentado en la H.V. ubicada en la unidad *"W:documentación\Hojas de vida servidores\Servidor2.docx"*
INSTALACION ACTUALIZACIONES Y ANTIVIRUS	Administrador Servidores	INSTALAR ANTIVIRUS Y ACTUALIZACIONES w:\\2009\AVIRA_2009\capacitacion.ppt
INSTALACION SEVEN	Administrador Servidores Soporte Digitalware	Referirse al manual de instalación ubicado en la ruta: *"W:documentación\documentacion tecnica\DIGITALWARE\ documentos_seven_julio_2009 \manual de instalación seven ERP"* Una vez instalado SEVEN se debe tener en cuenta que es una aplicación que requiere de actualizaciones en forma periódica y dichas actualizaciones no se encuentran en los medios de instalación. SEVEN está dividido en cuatro partes las cuales interactúan unas con otras; una primera parte son los archivos ejecutables o *.exe estos se encuentran la partición F:\seven\modulo\submodulo\bin

		Ej. F:\seven\modfinan\cn_conta\bin La segunda son los archivos con extensión *.ocx y *.htm estos se encuentran en F:\inetpud\wwwroot\seven\modulo\cn_conta ej. F:\inetpud\wwwroot\seven\modfinan\cn_conta *La tercera son las plantillas para los reportes, estos archivos tiene la extensión *.rpt y se encuentran en la ruta F:\inetpud\wwwroot\seven\Rpt* Por último, la base de datos la cual se encuentra en la ruta G:\datos \SEVEN Para cualquier cambio de servidor o actualización se deben modificar o actualizar estas carpetas. En este caso se recomienda que servidor de contingencia se llame de la misma forma (servidor2), ya que de lo contrario se deberá editar algunos archivos de sistema y cambiar rutas de búsqueda, lo que ocasionaría retraso en la puesta en marcha. En una migración o restauración de esta aplicación se debe tener copia la cual se debe reescribir las carpetas de la siguiente forma: Es recomendable crear las particiones F:\ G:\ en el servidor ya que se minimiza el riesgo de daño o pérdida por fallas de sistema operativo. La carpeta SEVEN en F:\seven; se debe copiar toda esta carpeta y reemplazarla en el servidor de contingencia en la misma ubicación La carpeta wwwroot en F:\inetput\wwwroot; se deben copiar en el servidor de contingencia con la misma estructura se debe tener cuidado con la carpeta rpt ya ella aloja todas las plantillas para los reportes y está en F:\inetpud\wwwroot\seven\rpt.
RESTAURACION BASE DE DATOS	Administrador Servidores	La base de datos se encuentra en G:\datos\SEVEN. Esta base de datos utiliza el motor SQL 2000. El traslado de esta base de datos se puede realizar copiando el

	Soporte Digitalware	archivo seven_Data.MDF alojado en la ruta anterior teniendo el servicio de SQL cerrado y la restauración se debe hacer copiando este archivo (Base de datos de SEVEN) en un lugar seguro del servidor de contingencia con el Administrador Corporativo de SQL se adjunta la base de datos SEVEN dando la ubicación donde se guardó la base de datos

5.3. Servidor 3 (Sistema de Help Desk, Backup Exec)

Proceso-Tiempo estipulado	Responsable	Procedimiento
INSTALACION SISTEMA OPERATIVO 01:30:00	Administrador Servidores	TENER DOCUMENTACION Tener a la mano la documentación, Hoja de vida y software correspondiente al servidor INSTALACION DE SISTEMA OPERATIVO Tener en cuenta la información que se encuentra documentado en la H.V. ubicada en la unidad *"W:documentación\2012\Hojas de vida servidores\Servidor3.docx"*
INSTALACION ACTUALIZACIONES Y ANTIVIRUS	Administrador Servidores	INSTALAR ANTIVIRUS Y ACTUALIZACIONES w:\\2009\AVIRA_2009\capacitacion.ppt
INSTALACION DISCOVERY	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *W:\2009\DISCOVERY_2009\MANUAL DE INSTALACION SERVIDOR DE DISCOVERY* Los desarrollos y consultas se guardan en la carpeta c:\Archivos de

		Programas\Leverit\software, por esta razón es necesario recuperar la carpeta Leverit con toda su estructura.
RESTAURACION BASE DE DATOS DISCOVERY 00:15:00	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *W:\2009\DISCOVERY_2009\MANUAL DE INSTALACION SERVIDOR DE DISCOVERY - Pagina 31*
INSTALACION BACKUP EXEC 01:30:00	Administrador Servidores Soporte backup Exec	Referirse al manual de instalación ubicado en la ruta *W:\2009\BACKUP EXEC\Manual de instalacion Backup Exec*

5.4. Servidor 4(Sistema de Fonoteca Mandarín, SAN y Centro de Emisión)

Proceso-Tiempo estipulado	Responsable	Procedimiento
TOLERANCIA A FALLOS	Administrador	Gracias a que el servidor cuenta con una tarjeta para Raid se configuró un arreglo de discos por Hardware en Raid 5 que garantiza tolerancia permanente fallas de disco. Se debe tener en cuenta la configuración de las particiones documentadas en: "*W:documentación\2012\Hojas de vida servidores\Servidor4.docx*"
INSTALACION SISTEMA OPERATIVO 01:30:00	Administrador Servidores	TENER DOCUMENTACION Tener a la mano la documentación, Hoja de vida y software correspondiente al servidor INSTALACION DE SISTEMA OPERATIVO Tener en cuenta la información que se encuentra documentado en la H.V. ubicada en la unidad "*W:documentación\Hojas de vida servidores\Servidor4.docx*"

INSTALACION ACTUALIZACIONES Y ANTIVIRUS	Administrador Servidores	INSTALAR ANTIVIRUS Y ACTUALIZACIONES w:\\2009\AVIRA_2009\capacitacion.ppt
INSTALACION MANDARIN	Administrador Servidores Soporte Mandarin	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\MANDARIN\guia del usuario.pdf"*
INSTALACION SOFTWARE CENTRO DE EMISION	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica \software emision\manuales \manual técnico.doc"*

5.5. Servidor 5 (Sistema de Gestión Documental Orfeo)

Proceso-Tiempo estipulado	Responsable	Procedimiento
INSTALACION SISTEMA OPERATIVO 01:30:00	Administrador Servidores	TENER DOCUMENTACION Tener a la mano la documentación, Hoja de vida y software correspondiente al servidor INSTALACION DE SISTEMA OPERATIVO Tener en cuenta la información que se encuentra documentado en la H.V. ubicada en la unidad

		"W:documentación\Hojas de vida servidores\Servidor5.docx" Página 12
INSTALACION ACTUALIZACIONES	Administrador Servidores	EJECUCION DE GPUPDATE Y GPUPGRADE
INSTALACION SERVIDOR FTP	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 19*
INSTALACION SERVIDOR WEB	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 19*
INSTALACION SOFTWARE MONITOREO	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 33*
RESTAURACION BD	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 26*
RESTAURACION APLICACIÓN WEB	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 24*
RESTAURACION BODEGA	Administrador Servidores	Referirse al manual de instalación ubicado en la ruta *"W:documentación\documentacion tecnica\ORFEO \manuales\manual tecnico.dot" Página 24*

6. Manual Plan en caso de ataques de hacker o virus informáticos

6.1. Ataques por intrusiones no autorizadas

Generar a través de las herramientas dispuestas, los logs del tráfico para determinar los puertos, origen y destino de los paquetes que se transmiten a través de la red.

Teniendo esta información se deben activar las funcionalidades necesarias como Antiphising o Antispy, Attack denegation of service, etc.

Activar únicamente los puertos requeridos para la continuidad de los servicios de rtvc.

Establecer los niveles de seguridad adecuados para cada equipo de acuerdo a su perfil.

6.2. Virus informáticos

La centralización de los mecanismos de defensa permite que en dado caso si existe un ataque por virus, la persona que administra estas herramientas envíe y replique a través de la red las actualizaciones necesarias para aplicarse sobre los equipos, incluyendo también políticas y configuraciones necesarias para evitar el contagio, lo anterior corresponde al primer paso de ejecución.

El segundo paso corresponde a un análisis detallado del ataque, para posteriormente comunicarse con el proveedor o la empresa de seguridad informática que presta el servicio de soporte sobre la herramienta de antivirus con la que cuenta actualmente rtvc, la cual hará la toma de las muestras y el seguimiento del caso.

El tercer paso corresponde a un aislamiento de las maquinas infectadas, evitando así una propagación que detenga la continuidad en la producción.

IV. Plan de Recuperación y reanudación

El Plan de Contingencia nos garantiza la respuesta para el momento que se declaran las emergencias. Una vez resuelta la emergencia, se disparan otra serie de procedimientos que vuelven la operación a su normalidad, los cuales están contemplados en el Plan de Recuperación y Reanudación.

El Plan de Recuperación y Reanudación tiene como objetivo tratar de alcanzar una disponibilidad de 99.99% para la infraestructura crítica, lo que implica que el sistema siempre estará disponible: el Plan de reanudación especifica los medios para mantener los servicios críticos en la ubicación de la crisis y el plan de recuperación especifica los medios para recuperar las funciones del negocio en una ubicación alterna.

A continuación se exponen las medidas a tomar para la reanudación de los servicios, expuestas en el Manual de Restauración de las copias de seguridad o backups en las cuales se contemplan los procedimientos de restauración de los backups tanto en los servidores como en las estaciones de trabajo, la restauración del sistema operativo en servidores y estaciones de trabajo, el manual de instalación del aplicativo SEVEN y se finaliza haciendo una revisión a los riesgos identificados y relacionados a los Sistemas de Información de rtvc y las recomendaciones del caso.

1. Restauración de copias de seguridad (servidores y PC)

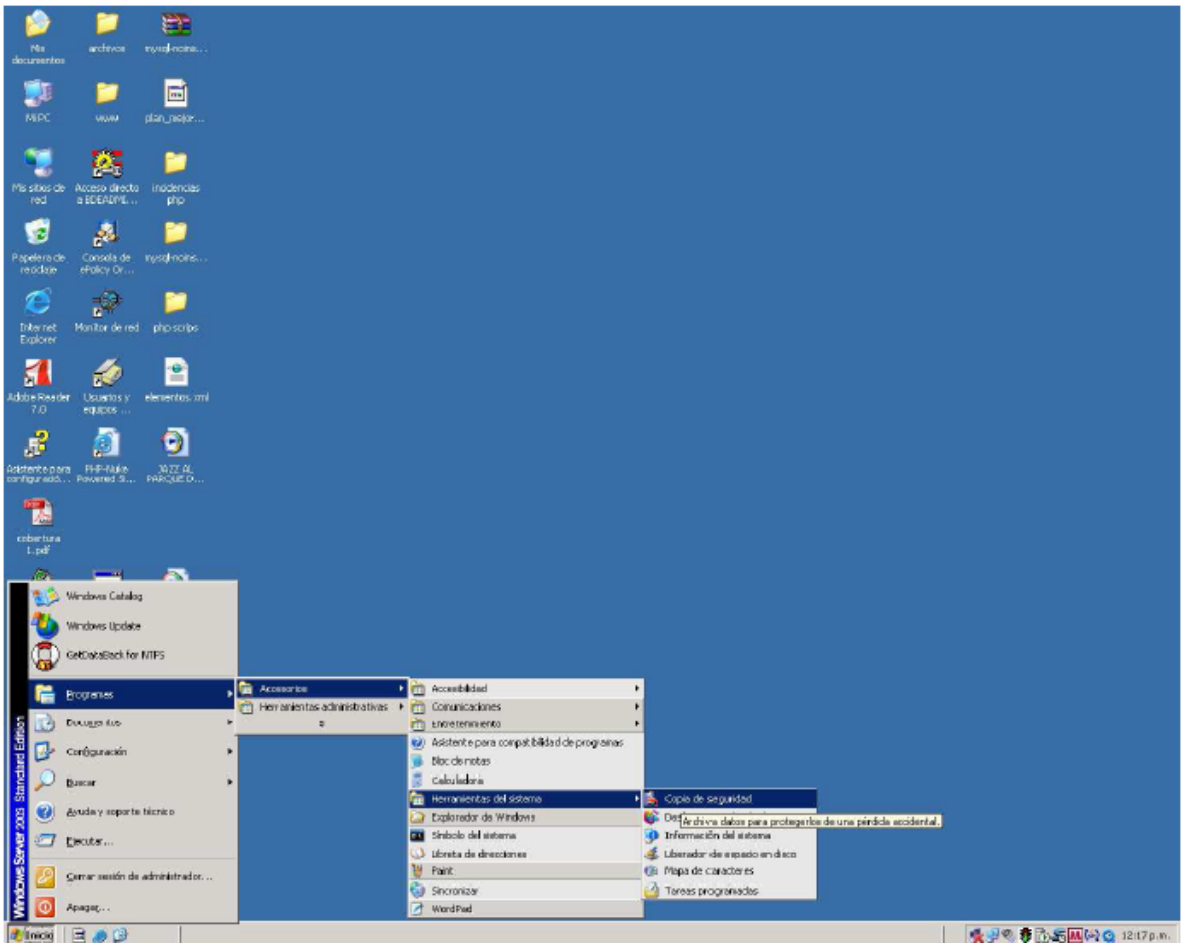
El Plan de Recuperación y Restauración fue diseñado con el objetivo de ser el referente en el momento de realizar las tareas de restauración de las copias de seguridad realizada sobre los servidores y las estaciones de trabajo de los usuarios. En este capítulo contiene las tareas a realizar para poder recuperar exitosamente la información y la reanudación inmediata de las actividades después de la presentación de un evento excepcional.

1.1 Restauración de backups en servidor

1.1.1 Restauración de backups en servidores Windows

Para realizar la restauración de backups en un servidor con Windows NT 4.0, 2000 o 2003 Server, se deben seguir los pasos descritos a continuación:

- Debe loguearse al servidor con el usuario administrador
- Ir por Inicio-Programas-Accesorios-Herramientas del Sistema-Copia de Seguridad:



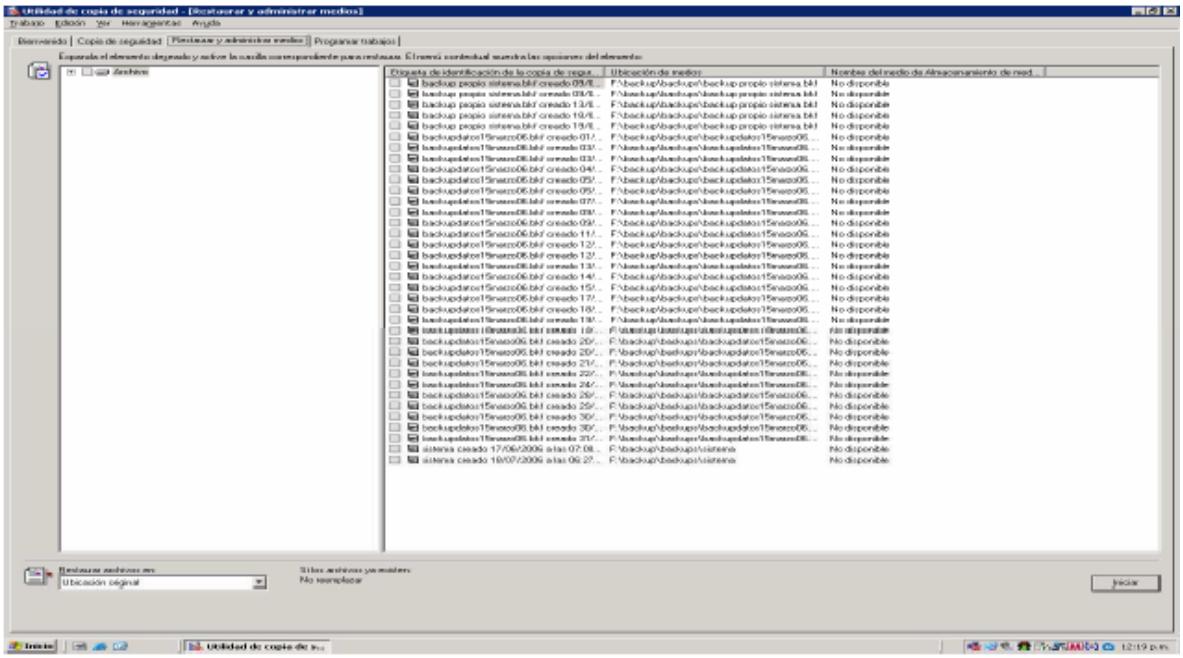
Luego de haber seleccionado los archivos o carpetas y el lugar de destino, se da clic en Iniciar, allí se mostrará una pantalla de información del tiempo y los archivos que se van restaurando. Al terminar este proceso, la restauración genera un archivo de datos de todos los eventos realizados.

En este caso nos muestra la cantidad de archivos y tiempo utilizado y si se presentó algún error. Posteriormente se oprime el botón de Cerrar y se Finaliza el programa.

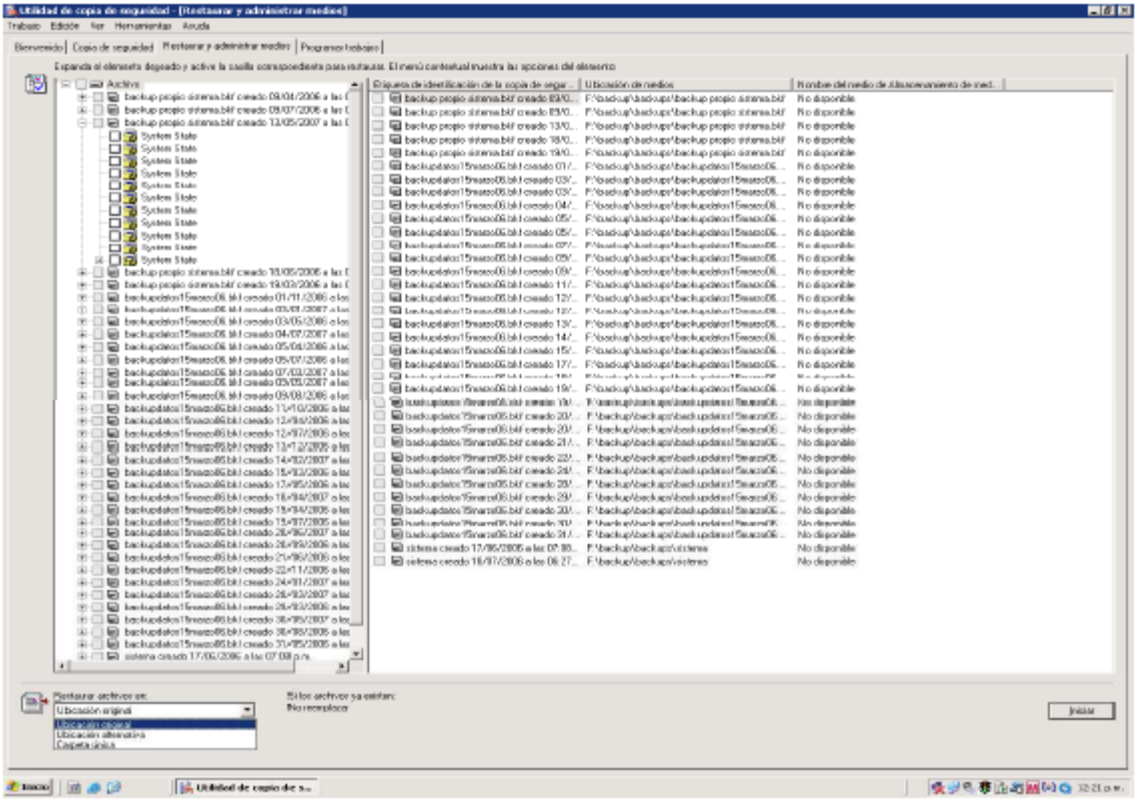
1.1.2 Restauración de backups en servidor de producción SERVIDOR 2

Se realiza la restauración siguiendo los pasos de restauración de servidor expuestos en el numeral 1.1.1 del Plan de Reanudación, seleccionando como medio Cinta.

Se da clic en la pestaña “Restaurar medios” y aparece los tipos de medios, del cual se selecciona cinta de 4mm.



Se selecciona el nombre de la cinta en el panel izquierdo y aparecen los catálogos que se encuentren grabados, en el panel de lectura izquierdo y se selecciona la fecha más reciente del medio insertado en la unidad. Luego en la pestaña marcada como “Restaurar archivos en ”, se selecciona la ubicación donde se van a restaurar los datos, como se muestra en la figura,



En este momento se da clic en “Iniciar”, evento por el cual se despliega una pantalla de información del tiempo y los archivos que se van restaurando. Al terminar esta tarea, se genera un archivo de datos de los eventos realizados donde incluye la cantidad de archivos y el tiempo que tardó la restauración y en el caso de presentarse errores, muestra un log de errores. Una vez revisada dicha información se da clic en Cerrar y se finaliza el programa.

Después de realizada la restauración, se debe adjuntar la base de datos, ingresando al programa SQL Server, dando clic derecho sobre el nombre del servidor (SERVIDOR 2), se indica la ruta donde se encuentra la base de datos y el aplicativo genera el nombre de la base de datos que se adjuntó. En el caso de este servidor aparecerá SEVEN.

Luego se debe ir a cada uno de los equipos que ingresan al aplicativo y el acceso directo para ingreso al aplicativo.

1.1.3 SERVERPRU

Por ser un servidor de Windows, los pasos a seguir son idénticos a los expuestos en el ítem anterior, usando el backup del servidor de producción, por ser éste una imagen del SERVIDOR2. En la contingencia que el servidor2 no pueda ser accedido por fallos graves, se habilita este servidor y el único cambio se realizará en las estaciones de trabajo, donde se cambia el nombre "SERVIDOR2" por "SERVERPRU".

1.2 Restauración de sistema operativo en servidor

Para restaurar el sistema operativo en un servidor se debe tener en cuenta los siguientes eventos:

1. Si la falla es por daño físico del disco duro y no se posee configuración RAID.
2. Si la falla es por daño de algún archivo de Windows que impide que este arranque.

Caso 1. Si la falla es por daño físico del disco duro y no se posee configuración RAID, se deben seguir los siguientes pasos:

- Configurar la unidad de CDROM como primer dispositivo de arranque.
- Colocar el CD del sistema operativo del servidor
- La instalación se inicia con la copia de algunos archivos que se necesiten para poder verificar los discos duros y formatearlos.
- Al realizar la verificación de los discos duros, el instalador pide la creación de una partición primaria donde se alojará el sistema de inicio del sistema operativo. Se recomienda una partición mínima de 30 Gigas para el sistema operativo y los aplicativos que se instalarán. Se instalarán los aplicativos que estén documentados en la hoja de vida de ese servidor.
- Los datos siguientes que solicita el instalador son los datos de usuario, la licencia (ver hoja de vida del servidor), la configuración del servidor, la dirección IP (ver la hoja de vida del servidor) que usará el equipo.
- Es importante que la instalación se configure de acuerdo a los datos que aparecen en las hojas de vida de los servidores, las cuales se realizaron con este objetivo principal.

Caso2. Si la falla es por daño de algún archivo de Windows que impide que este arranque, la tareas a realizar son:

- Configurar la unidad de CDROM como primer dispositivo de arranque.
- Colocar el CD del sistema operativo del servidor

- La instalación se inicia con la copia de algunos archivos que se necesiten para poder verificar los discos duros.
- Al realizar la verificación de los discos duros, aparece una pantalla indicando si se desea realizar una instalación nueva o reparar una ya existente. Se selecciona la opción "Reparar".
- Al seleccionar esta opción, la instalación realiza la copia de los archivos que encuentra dañados o eliminados. Es importante resalta que este procedimiento no altera ni borra ningún archivo o aplicativo instalado antes del daño.

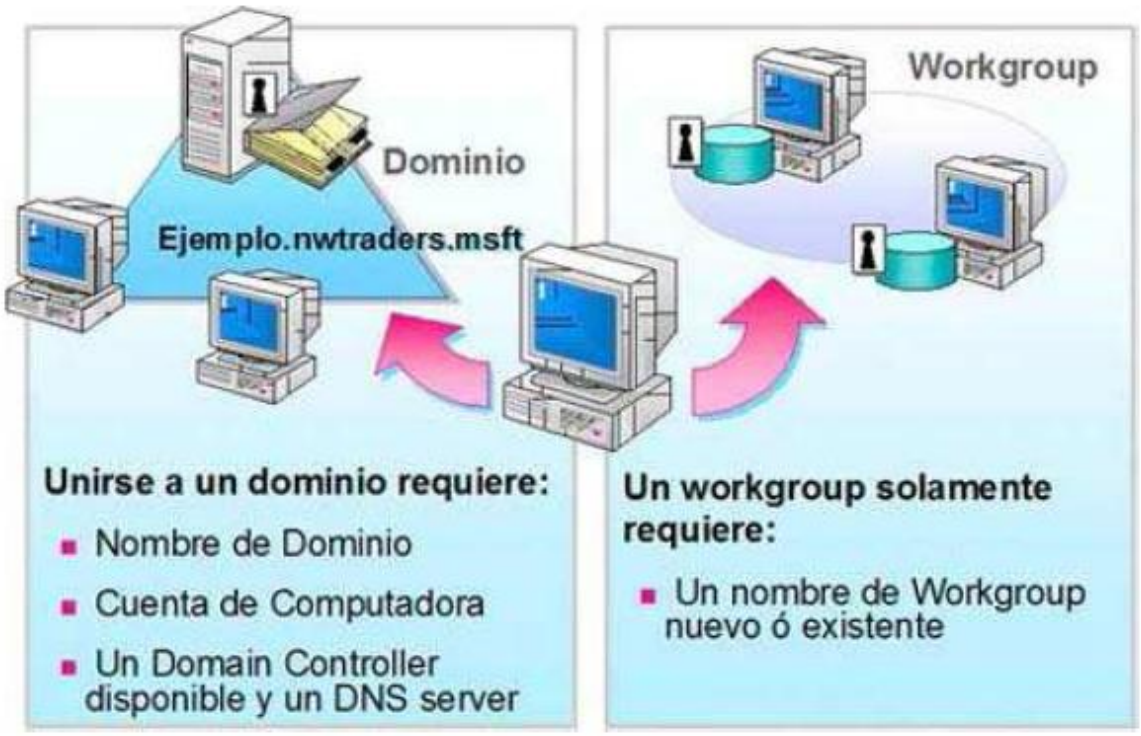
1.2.1. Instalación de servidores Microsoft Windows Server 2003

Existen cuatro servidores que cuentan con este sistema operativo: SERVIDOR1, SERVIDOR2, SERVIDOR 3 Y SERVIDOR4, todos debidamente licenciados. El original de los medio se encuentra en la caja fuerte del segundo piso y una copia en poder de soporte técnico de la Jefatura de Informática.

Para realizar una instalación nueva, se ingresa el CD de instalación y se reinicia desde la unidad de CD, ante lo cual se visualizará el Asistente para Instalación de Windows Server 2003:

- Se selecciona la primera opción “Install” y el instalador le solicitará los sistemas de archivos que se usarán en las particiones creadas. Se revisa de la Hoja de vida del servidora para verificar cuántas particiones y qué sistema de archivos tiene cada una y se configura de acuerdo a esa información.
- Posteriormente se selecciona el Modo de licenciamiento, del cual se debe tener en cuenta que hay una MOLP[2] de dos servidores: y los dos adicionales se configuran como servidores independientes.
- Se determina la pertenencia al dominio de la entidad: RTVC

[2] MOLP son las siglas de Microsoft Open License Program.



1.3 Restauración de sistema operativo y aplicaciones en un PC

Según la notificación sobre los respaldos de información, la única información de los equipos de cómputo que será amparada por las rutinas automáticas de Backup será la que se guarde dentro de la carpeta compartida de cada dependencia, que no se verá afectada en caso de fallos en el equipo de trabajo del usuario.

En el caso de daño del sistema operativo, se restaurará la imagen o copia espejo de la estación de trabajo, la cual es generada de la siguiente manera: Una vez instalado el software en una estación de trabajo: sistema operativo, herramientas de de Ofimática, todas las actualizaciones críticas, fuentes de Orfeo, service pack de las aplicaciones hasta el momento de la instalación, fuentes necesarias de Seven, aplicativos necesarios para el trabajo en general de todos los usuarios como Acrobat reader, descompresor, drivers de los equipos, los instaladores del antivirus, el software Roxio para el uso de las unidades de CD quemadoras, los navegadores Internet Explorer y Mozilla Firefox actualizados, se genera una copia espejo con el software Acronis True Image. El nombre de

la copia guardada se asigna en función del mes y el año. Por ejemplo la copia imagen del mes de noviembre de 2009 es “noviembre2009.tib”.

La copia es almacenada en una unidad de disco duro externa, proceso que dura en promedio 50 minutos y depende de la velocidad del equipo. Estas copias se actualizan cada tres meses.

La restauración del sistema operativo y esta copia espejo por tanto, se realiza con el mismo software, en su funcionalidad de restauración. Una vez restaurada la copia espejo, se procede a:

- Ingresar al dominio, dando el nombre de acuerdo a su funcionalidad
- Instalar el antivirus, con el motor de búsqueda y la última base actualizada.
- Se instalan las aplicaciones críticas del momento de la copia al momento de la restauración
- Se instala el Service Desk para los requerimientos que se hace a Soporte.
- Se instala el software específico de acuerdo a las funciones que cumplirá la estación de trabajo, previa revisión de licenciamiento.