PLAN DE CONTINGENCIA
Y
RECUPERACION DE DESASTRES

BOGOTA, Agosto 2012.

ASPECTOS GENERALES

Definición

El proceso de contingencia está compuesto por un grupo de actividades que se ejecutan cuando se presenta una interrupción de la operación diaria o inconsistencias en los procesos normales. Estas actividades deben llevarse a cabo de manera inmediata para lograr retornar a la operación normal del sistema en el menor tiempo posible.

1.1 Objetivo

Establecer un procedimiento que permita garantizar la continuidad de la operación del sistema, determinar el nivel de aseguramiento del mismo, asegurando la recuperación de información con una mínima perdida de datos y de esta manera, mantener sin alteraciones las operaciones realizadas sobre el sistema cuando se presenten condiciones de falla.

1.2 Identificación de Puntos Críticos:

1.2.1 Equipos de Cómputo

1.2.1.1 Servidores de información:

Transborder cuenta con diez servidores en donde se almacena la información de los usuarios, y las aplicaciones:

Nombre del servidor:	SERVERDB1
Procesador:	Intel(R) Xeon(TM) CPU 3.06GHz [1 core(s) x86]
Memoria:	3072
Disco Duro:	250 GB de almacenamiento en Raid 5
Sistema Operativo:	W2K3 Server Standard Edition

Nombre del servidor:	SERVAPPS
Procesador:	Quad-Core AMD Opteron(tm) Processor 2378 [4 core(s) x64]
Memoria:	49152
Disco Duro:	1.5 TB de almacenamiento en Raid 5
Sistema Operativo:	W2K8 Enterprise Edition

Nombre del servidor:	MUISCA
Procesador:	Intel(R) Xeon(R) CPU 3065 @ 2.33GHz [1 core(s) x86]
Memoria:	4096
Disco Duro:	500 GB de almacenamiento en Raid 1

Sistema Operativo:	W2K3 Server Standard Edition 32-bit (420-2965)

Nombre del servidor:	SERVAV
Procesador:	Intel(R) Xeon(TM) CPU 3.06GHz [1 core(s) x86]
Memoria:	4GB DDR SDRAM 266MHZ (4X1GB) PowerEdge
Disco Duro:	250 GB de almacenamiento en Raid 5
Sistema Operativo:	W2K3 Server Standard Edition

Nombre del servidor:	SERVDC1
Procesador:	Intel(R) Xeon(TM) CPU 3.00GHz [1 core(s) x64]
Memoria:	8GB
Disco Duro:	560 GB de almacenamiento en Raid 5
Sistema Operativo:	W2K8 Server Enterprise Edition 32-bit (420-2965)

Nombre del servidor:	SERVBES
Procesador:	Intel(R) Pentium(R) D CPU 3.00GHz [1 core(s) x86]
Memoria:	1024
Disco Duro:	80 GB de almacenamiento en Raid 1
Sistema Operativo:	W2K3 Server Standard Edition

Nombre del servidor:	SERVNSFLS
Procesador:	Intel(R) Xeon(TM) CPU 3.00GHz [1 core(s) x86]
Memoria:	4GB
Disco Duro:	200 GB de almacenamiento en Raid 5
Sistema Operativo:	W2K3 Server Standard Edition 32-bit (420-2965)

Nombre del servidor:	SERVER2
Procesador:	Quad-Core AMD Opteron(tm) Processor 2378 [4 core(s) x64]
Memoria:	49152
Disco Duro:	1.5 TB de almacenamiento en Raid 5
Sistema Operativo:	W2K8 Server Enterprise Edition

Nombre del servidor:	STORAGE
Procesador:	Intel XEON
Memoria:	12GB

Disco Duro:	6 TB de almacenamiento en Raid 5
Sistema Operativo:	Windows Server Storage Edition

Nombre del servidor:	MUISCA2
Procesador:	Intel(R) Xeon(R) CPU E5630 @ 2.53GHz [1 core(s) x86]
Memoria:	65536
Disco Duro:	1.2 TB de almacenamiento en Raid 5
Sistema Operativo:	W2K8 Server enterprise Edition

En el servidor SERVERDB1 se encuentran alojados los siguientes Servicios de Red:

- Unidades de red.
- Bases de datos SQL

En el servidor SERVAPPS se encuentran alojados los siguientes Servicios de Red:

- Lotus Domino Aplicaciones
- Unidades de red

En el servidor MUISCA se encuentran alojados los siguientes Servicios de Red:

- Citrix

En el servidor SERVAV se encuentran alojados los siguientes Servicios de Red:

- Consola Antivirus
- Bases de datos SQL

En el servidor ServDC1 se encuentran alojados los siguientes Servicios de Red:

- Active Directory
- DNS
- Unidades de red

En el servidor SERVBES se encuentran alojados los siguientes Servicios de Red:

- Servidor black berry

En el servidor SERVNSFLS se encuentran alojados los siguientes Servicios de Red:

- Active Directory
- DNS
- Unidades de red

En el servidor SERVER2 se encuentran alojados los siguientes Servicios de Red:

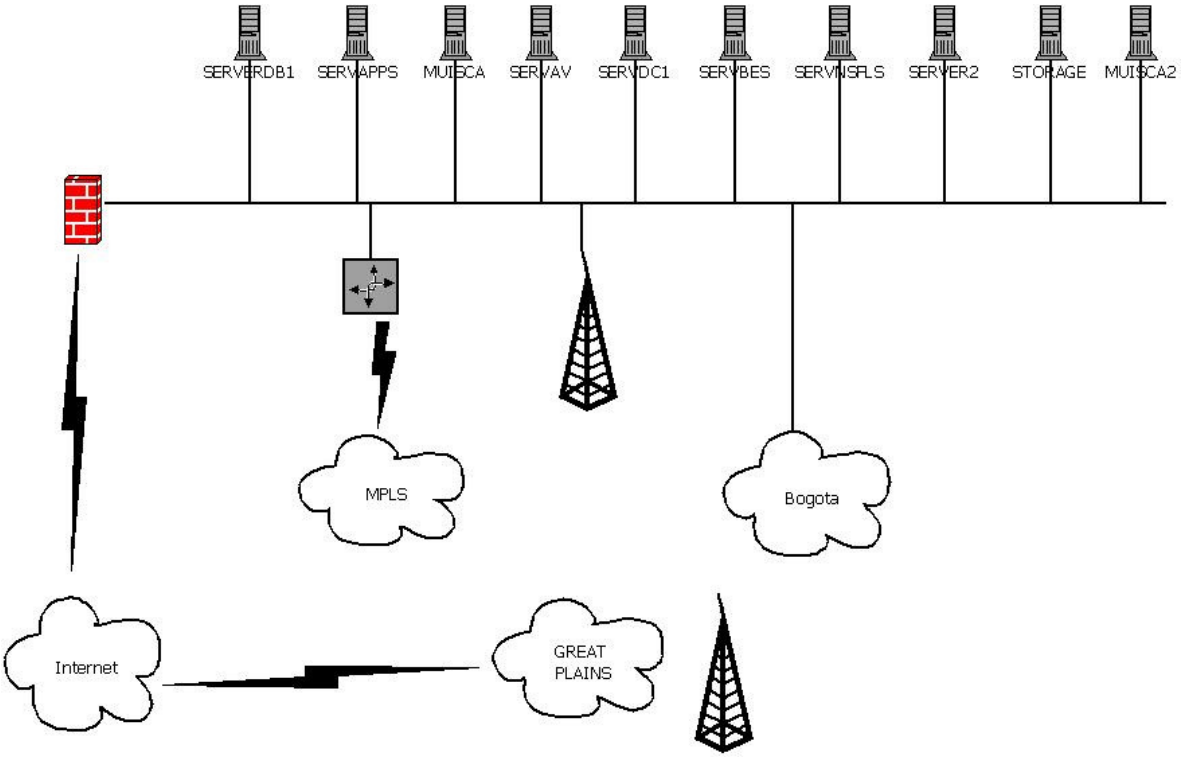
- Lotus Domino Correo

En el servidor STORAGE se encuentran alojados los siguientes Servicios de Red:

- Unidades de red
- Backup Historico

En el servidor MUISCA2 se encuentran alojados los siguientes Servicios de Red:

- Citrix



1.2.1.2 Unidad de Tape Backup

Con el objetivo de contar con copias de seguridad de la información almacenada en los servidores se tiene habilitado el servicio de snapshot el cual crea instantáneas tres veces al dia de la información de los discos, adicional a esto se tiene esquema de copias diarias almacenadas en cintas LTO3, en esquema de cinta diaria

con rotación cada tres semanas, copia semanal con rotación anual, y copia anual definitiva, dichas copias son enviadas a transarchivos para su almacenamiento.

1.2.2 Comunicaciones:

Para accesar al toda la infraestructura de la compañía, transborder cuenta con los siguientes canales de comunicación, adicionalmente se cuenta con tres canales para el acceso a internet.

Configuración Canales de Comunicación

Tipo	Origen	Destino	IP	Proveedor
Canal MPLS	Bogota	Cali	192.168.100.10-192.168.102.1	Telmex
Canal MPLS	Bogota	Buenaventuta	192.168.100.10-192.168.103.1	Telmex
Canal MPLS	Bogota	Cartagena	192.168.100.10-192.168.104.1	Telmex
Canal MPLS	Bogota	Barranquilla	192.168.100.10-192.168.105.1	Telmex
Canal MPLS	Bogota	Medellin	192.168.100.10-192.168.106.1	Telmex
Canal dedicado	Bogota	Diveo Data center	192.168.100.9	DIVEO
Canal ADSL	Bogota	Internet	192.168.100.115	ETB
Canal dedicado	Bogota	Internet	192.168.100.2	Telmex

1.2.3 Centro de Cómputo

Los servidores y equipos de comunicaciones de transborder se encuentran alojados en la Cr 7 # 17-51 oficina 1102, en el cuarto identificado como “centro de computo”

Dentro de sus principales características se encuentran:

- Control de acceso mediante llave
- reguladores eléctricos.
- 1 UPS de 10 KVA.
- Sistema de refrigeracion.

1.3 DETERMINACION DE RIESGOS POTENCIALES:

Con el objetivo fundamental de cumplir con todos los aspectos necesarios para garantizar el correcto funcionamiento de la infraestructura a nivel físico (hardware) y lógico (software), es conveniente asumir que existe alguna probabilidad que en su momento pueda llegar a fallar alguno de los componentes del sistema.

Las posibles fallas identificadas son las siguientes:

- Errores físicos: falla de hardware que afecta a los equipos alojados en el centro de tecnología.
- Factores externos: desastre natural (incendio, inundación, terremoto) o acto terrorista que afecta al centro de cómputo.

- Errores lógicos: borrado de un programa o archivo que afecte el normal funcionamiento de algún área de transborder.

- Comunicaciones: fallas que impidan conexión a la base de datos a través del canal de comunicaciones.

2. CONTROLES PREVENTIVOS

Las siguientes actividades comprenden los controles que se llevan a cabo para evitar la ocurrencia de situaciones de emergencia ó que estas puedan ser atendidas y corregidas lo más pronto posible en caso de presentarse.

2.1 Estrategia y Procedimientos de Backup

Las copias o Backups de información deben generarse siguiendo pautas claras y oportunas que permitan contribuir a una recuperación de datos en un espacio de tiempo lo más corto posible.

Los Backups a nivel de base de datos se realizan diariamente, un total semanal, y un total mensual, los cuales son monitoreados a diario por el administrador de infraestructura, quien determina si un backup fue exitoso o no dependiendo de código de retorno suministrado por la herramienta que realiza directamente esta operación.

Los Backup diarios se realizan de la siguiente manera:

- ✓ Se genera backup diario a las 10:00 pm
- ✓ Adicionalmente se genera una copia semanal que se almacena en dos cintas LTO3.

2.2 Almacenamiento externo de cintas

Todos los Miercoles y viernes, Transborder envía las cintas usadas de cada semana a transarchivos, empresa especializada en Custodia de medios; de tal manera que en el evento de necesitar cintas con los Backups de la semana anterior haya disponibilidad casi inmediata de las mismas.

2.2.1 Sincronización del tiempo

Todos los servidores y equipos de computo de Transborder utilizan la misma hora en su reloj interno, para ello se deben sincronizar contra el servidor NTP (Network Time Protocol), que esta habilitado para tal fin (192.168.100.99).

Es función del administrador de infraestructura mantener el servidor NTP disponible y con la hora oficial para los sistemas de información y equipos de comunicaciones de transborder.

2.2.2 Autenticación

Todo acceso a la red de Transborder será validado, autenticado y verificado a través del servicio de directorio activo (active Directory)

El servicio de login no excluye la autenticación que de los usuarios se debe hacer para la utilización de algún servicio y/o aplicación de las áreas de negocios.

Cada usuario que accede a la red tendrá un perfil definido de acuerdo a la solicitud de creación de usuario dada por el gerente de cada area en conjunto con el área de tecnologia, este perfil le permite únicamente tener acceso a los servicios que este usuario necesita.

2.2.3 Políticas de manejo de antivirus

Toda la información está expuesta a virus a diario, si no se cuenta con los medios apropiados para evitar y atacar dichos virus es probable perder la información, por tal razón Transborder ha adquirido y ha instalado en todos los computadores el Antivirus de Mcafee.

2.2.3.1 Objetivo

Minimizar y en lo posible evitar la de perdida de información y /o alteraciones de los sistemas de información de la compañía.

2.2.3.2 Políticas

- El antivirus de la compañía es Mcafee
- Todos los equipos deben tener instalado y activado el antivirus.
- No está permitido instalar un antivirus diferente a Mcafee.
- Es responsabilidad del Administrador de infraestructura tener la última versión disponible para que los usuarios puedan actualizar el antivirus.
- Es responsabilidad del usuario verificar por lo menos una vez a la semana que su equipo este libre de virus.
- Es responsabilidad del usuario el verificar todos los archivos y correos que recibe con archivos, que puedan tener posibles virus.
- Es responsabilidad del administrador de infraestructura, el tener los servidores con las últimas versiones de antivirus instaladas.
- Es deber del usuario reportar anomalías que se presenten en sus equipos y que posiblemente puedan ser virus.
- El incumplimiento de las políticas establecidas por parte de los funcionarios, será motivo de sanciones de acuerdo a la falta y especificadas en la Política siguiente.

2.2.3.3 Procedimiento

- El Administrador de infraestructura verificara que se halla descargado la última versión de la actualización para que sea instalada en las maquinas de Transborder.
- Actualiza el antivirus: El usuario revisará por lo menos una vez a la semana que la definición de virus se ha actualizado.
- Error: Si aparece algún tipo de error el usuario informará al Administrador Red Interna dicho error.
- Resuelve problema, actualiza: El Administrador de infraestructura resuelve el problema y actualiza el equipo.

La política de antivirus permite que automáticamente, estaciones y servidores que previamente se han configurado bajo la consola administrativa de Mcafee se actualicen a una hora exacta con la misma versión de actualización.

Si alguna máquina no se encuentra conectada a esta consola, se debe descargar manualmente la versión y hacer la respectiva actualización manualmente.

2.3 Otras Políticas

Todos los servidores de Transborder están ubicados en la Cr 7 # 17 – 51 piso 11

Todos los servidores que no estén siendo utilizados deben permanecer bloqueados con contraseña que impida el acceso a un tercero no autorizado.

2.4 Centro de Cómputo

Los servidores de Transborder están alojados en el centro de cómputo, el cual nos permite garantizar para las plataformas allí instaladas las condiciones que a continuación se relacionan:

2.4.1 Refrigeración:

El centro de cómputo cuenta con un equipo de refrigeración de 36000 BTU

2.4.2 UPS:

Contamos con 1 UPS de 10 KVA, y con baterías que para esta carga pueden dar hasta 30 minutos de soporte.

2.4.3 Control de acceso al centro de cómputo:

- Disponemos de un control de acceso por llave al centro de cómputo.
- Existen únicamente tres llaves de acceso.

2.4.4 Control de incendio:

- Un extintor fuera del centro de cómputo.

DESARROLLO DEL PLAN DE CONTINGENCIA

2.5 Descripción del Plan de Contingencia

Con el fin de garantizar la continuidad del negocio, se tienen definidas las siguientes contingencias de primer nivel que permitirán migrar la información de manera rápida, segura y eficiente:

- Debido a que la primera instancia de almacenamiento de las copias de seguridad, la constituyen los discos duros de cada máquina, se cuenta con un backup de primera mano en caso de daño de la base de datos, respaldado por la información que se baja a cinta.

- Cada servidor de Transborder cuenta con un arreglo de discos Raid 5 que nos garantizarán el normal funcionamiento de cada máquina en caso de falla de uno de los discos duros.

- Como contingencia del canal de acceso a internet, se ha instalado un canal dedicado con un proveedor de ancho de banda diferente al que suministra el servicio principal, lo que garantiza que en caso de que el proveedor principal tenga problemas en uno de sus nodos, estos no afecten al proveedor del canal de contingencia.

2.6 Procedimientos de Contingencia

2.6.1 Equipos de Cómputo

2.6.1.1 Escenario 1 - Daño de parte con redundancia

2.6.1.1.1 Criterios para Invocar el Plan

Se han identificado problemas de hardware en el sistema, bien sea por los logs monitoreados por el Administrador de infraestructura. El daño detectado en este caso corresponde a una de las partes que poseen redundancia (disco duro, fuente de poder).

2.6.1.1.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Se detecta el daño en una de las partes que poseen redundancia en el servidor (Fuente, Disco Duro) y deja funcionando a la otra sin interrumpir la operación normal	(El computador lo detecta automáticamente)	Inmediato (La operación no se detiene)
2. Se detecta el tipo de falla a través de los logs del sistema o de los monitoreos diarios realizados a los servidores.	Administrador de infraestructura	20 minutos
3. Si la parte afectada posee redundancia basada en el otro servidor (unidad de 3½, unidad de tape, unidad de CD, etc.) se debe compartir, redireccionar o configurar las partes del servidor que no ha presentado fallas, con el servidor que tiene la parte defectuosa, con el fin de prestar un apoyo temporalmente mientras se corrige el problema.	Administrador de infraestructura	30 minutos

2.6.1.1.3 Monitoreo del Plan

Se realizan chequeos y revisiones del correcto funcionamiento del servidor afectado en lapsos muy cortos de tiempo, con el fin de constatar que la parte redundante trabaja correctamente después de haber entrado en producción sin tener en el momento de activación de la contingencia su igual de respaldo.
Se hará seguimiento presencial al cambio de la parte afectada.

2.6.1.1.4 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer la parte que presentó la falla. Puede ser de pocas horas en caso de existir en las instalaciones del proveedor de la máquina en Bogotá D.C. o de días en caso que se requiera importar.

2.6.1.1.5 Retorno a Operación Normal

En términos generales, la operación se mantiene normal por no haber interrupción del servicio, sin embargo se trabaja bajo un riesgo que requiere ser mitigado.

Actividad	Responsable	Tiempo Estimado
1. Se hace contacto con soporte técnico del distribuidor para intentar buscar posibles soluciones y las causas del inconveniente.	Administrador de infraestructura	2 Horas
2. Se crea un requerimiento de compra de la pieza de hardware dañada y para solicitar soporte técnico por parte del distribuidor en caso de no contar con garantía.	Administrador de infraestructura	30 Minutos
3. Se programa en horas no hábiles de servicio el reemplazo de la pieza de tal manera de impactar lo menos posible el normal funcionamiento del Transborder.	Administrador de infraestructura	Depende si hay existencia de la parte o si requiere ser importada
4. Se coordina la visita de la persona de soporte del fabricante para efectuar el cambio de la parte dañada por el reemplazo en horas no hábiles de servicio, en caso de tener que reiniciar el servidor.	Administrador de infraestructura	Depende si hay existencia de la parte o si requiere ser importada
5. El técnico enviado por Dell reemplaza la parte averiada por la nueva.	Soporte fabricante	24 – 48 horas
6. Se realizan las revisiones manuales o a nivel de Sistema Operativo necesarias para verificar que la parte reemplazada si queda en correcto funcionamiento.	Administrador de infraestructura	1 Hora
7. Se restablece el servicio de manera normal en los servidores.	Administrador de infraestructura	20 minutos

2.6.1.2 Escenario 2 - Daño en archivos alojados en los servidores.

2.6.1.2.1 Criterios para Invocar el Plan

- Se ha detectado corrupción en alguno de los archivos almacenados en los servidores del Transborder

2.6.1.2.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Se genera un requerimiento de soporte técnico en refiriendo el archivo que se encuentra dañado, su ubicación y la ultima fecha en la que se acceso de manera correcta.	Usuario Final	10 minutos
2. Se solicita la cinta a transarchivos	Administrador de infraestructura	1 dia
3. En el servidor SERVAPPS se inserta la cinta inmediatamente anterior a la fecha remitida en el numeral 1.	Administrador de infraestructura	20 minutos
4. Usando Backup EXEC se examina el contenido de dicha cinta y se restaura en la ubicación original el (los) archivos solicitados en el numeral 1.	Administrador de infraestructura	10 minutos
5. Se informa al usuario final la disponibilidad del archivo solicitado.	Administrador de infraestructura	20 minutos

2.6.1.2.3 Monitoreo del Plan

- Se verificará constantemente el estado de progreso o avance del proceso de restauración de los archivos.
- Se constatará el correcto funcionamiento del sistema luego de restaurados los archivos.

2.6.1.2.4 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer el (los) archivos dañados. Puede ser de pocas horas en caso que el medio de almacenamiento este en transborder o días en caso que se deba solicitar a transarchivos.

2.6.1.2.5 Retorno a Operación Normal

Actividad	Responsable	Tiempo Estimado
1. Inmediato tras la confirmación del usuario final.	Usuario final	10 minutos

2.6.1.3 Escenario 3 - Daño en Servidor de Correo Lotus.

2.6.1.3.1 Criterios para Invocar el Plan

- El Sistema de Correo Lotus no responde y se ha detectado un fallo de hardware que impide su reparación inmediata.

2.6.1.3.2 Plan de Contingencia (opción 1)

Actividad	Responsable	Tiempo Estimado
1. Se inicia sesión como usuario Administrador en el servidor ServDC1 (192.168.100.80).	Administrador de infraestructura.	10 minutos
2. Se restaura la copia de seguridad de la fecha inmediatamente anterior del servidor server2 y se ubica en el directorio e:\Lotus de dicho servidor.	Administrador de infraestructura.	5 horas
3. Se Desinstala AD del servidor SERVDC1.	Administrador de infraestructura.	20 minutos
4. Se cambia el nombre del servidor SERVDC1 Por SERVER2 y se cambia su IP.	Administrador de infraestructura.	20 minutos
5. Se instala Lotus Domino.	Administrador de infraestructura.	30 Minutos
6. Se Inicia el servicio.	Administrador de infraestructura.	20 Minutos

2.6.1.3.3 Monitoreo del Plan

- Se verificará constantemente el estado de progreso o avance del proceso de restauración del backup.
- Se constatará el correcto funcionamiento del sistema luego de restauradas las copias de seguridad.

2.6.1.3.4 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer la parte que presentó la falla. Puede ser de pocas horas en caso de existir en las instalaciones del proveedor de la máquina en Bogotá D.C. o de días en caso que se requiera importar.

2.6.1.3.5 Retorno a Operación Normal

Inmediato tras verificar que los usuarios tienen acceso al servicio de correo electrónico, se requiere posteriormente retornar a la maquina original pues las especificaciones de hardware y software no son similares. El servidor de correo original será remitido al Administrador de infraestructura.
para verificar el cambio de la pieza de hardware que origino el fallo.

2.6.1.4 Escenario 4 - Daño en servidor Lotus de aplicaciones

2.6.1.4.1 Criterios para Invocar el Plan

- El Sistema de Aplicaciones Lotus no responde y se ha detectado un fallo a nivel de hardware que impide su restauración inmediata.

2.6.1.4.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
7. Se inicia sesión como usuario Administrador en el servidor ServDC1 (192.168.100.80).	Administrador de infraestructura.	10 minutos
8. Se restaura la copia de seguridad de la fecha inmediatamente anterior del servidor server2 y se ubica en el directorio G:\Lotus de dicho servidor.	Administrador de infraestructura.	5 horas
9. Se Desinstala AD del servidor SERVDC1.	Administrador de infraestructura.	20 minutos
10. Se cambia el nombre del servidor SERVDC1 Por SERVAPPS y se cambia su IP.	Administrador de infraestructura.	20 minutos
11. Se instala Lotus Domino.	Administrador de infraestructura.	30 Minutos
12. Se Inicia el servicio.	Administrador de infraestructura.	20 Minutos

2.6.1.4.3 Monitoreo del Plan

- Se verificará constantemente el estado de progreso o avance del proceso de restauración de la base de datos.
- Se constatará el correcto funcionamiento del sistema luego de restauradas las bases de datos.

2.6.1.4.4 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer las partes que presentaron fallas. Puede ser de pocas horas en caso de existir en las instalaciones del proveedor de la máquina en Bogotá D.C. o de días en caso que se requieran importar.

2.6.1.4.5 Retorno a Operación Normal

Inmediato tras verificar que los usuarios tienen acceso al servicio de correo electrónico, se requiere posteriormente retornar a la maquina original pues las especificaciones de hardware y software no son

similares. El servidor de correo original será remitido al Administrador de infraestructura para verificar el cambio de la pieza de hardware que origino el fallo.

Escenario 5 - Daño en servidor DNS

2.6.1.4.6 Criterios para Invocar el Plan

- El Sistema de resolución de nombres de dominio DNS se ha detenido abruptamente y / o no responde.

2.6.1.4.7 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Se detecta el daño en uno de los servidores DNS y queda funcionando el otro sin interrumpir la operación normal.	Administrador de infraestructura.	10 minutos
2. Se detecta el tipo de falla a través de los logs del sistema o de los monitoreos diarios realizados a los servidores.	Administrador de infraestructura.	20 minutos

2.6.1.4.8 Monitoreo del Plan

Se realizan chequeos y revisiones del correcto funcionamiento del servicio DNS en lapsos muy cortos de tiempo, con el fin de constatar que el servidor redundante trabaja correctamente después de haber entrado en producción sin tener en el momento de activación de la contingencia su igual de respaldo.

2.6.1.4.9 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer las partes que presentaron fallas. Puede ser de pocas horas en caso de existir en las instalaciones del proveedor de la máquina en Bogotá D.C. o de días en caso que se requieran importar.

2.6.1.4.10 Retorno a Operación Normal

Inmediato tras verificar que los usuarios tienen acceso al servicio de resolución de nombres de dominio.

Escenario 6 - Daño en servicio de autenticación Active Directory

2.6.1.4.11 Criterios para Invocar el Plan

- El Sistema de autenticación del dominio AD se ha detenido abruptamente y / o no responde.

2.6.1.4.12 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Se detecta el daño en uno de los servidores Controladores de dominio y queda funcionando el otro sin interrumpir la operación normal.	Sistema Operativo	Inmediato
2. Se detecta el tipo de falla a través de los logs del sistema o de los monitoreos diarios realizados a los servidores.	Administrador de infraestructura.	20 minutos

2.6.1.4.13 Monitoreo del Plan

Se realizan chequeos y revisiones del correcto funcionamiento de Active Directory en lapsos muy cortos de tiempo, con el fin de constatar que el servidor redundante trabaja correctamente después de haber entrado en producción sin tener en el momento de activación de la contingencia su igual de respaldo.

2.6.1.4.14 Duración de la Contingencia

La duración de la contingencia será igual al tiempo que se requiera para reponer las partes que presentaron fallas. Puede ser de pocas horas en caso de existir en las instalaciones del proveedor de la máquina en Bogotá D.C. o de días en caso que se requieran importar.

2.6.1.4.15 Retorno a Operación Normal

Inmediato tras verificar que los usuarios tienen acceso al servicio de autenticación.

2.6.2 COMUNICACIONES

2.6.2.1 Escenario 7-Falla en canal de comunicaciones red MPLS

2.6.2.1.1 Criterios para Invocar el Plan

- No se puede entablar comunicación entre el Bogota y alguna (s) sucursal por posibles caídas de los canales de comunicación.
- Intermitencia en la comunicación entre Bogota y alguna (S) sucursales. que provoca constantes interrupciones en el acceso al sistema de información.

2.6.2.1.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Se genera un ticket en e-care informando la caída del canal.	Administrador de infraestructura.	5 minutos
2. Mediante programas de monitoreo, se revisa el estado de los canales administrados por TELMEX. para identificar el posible problema.	TELMEX	Por determinar
3. NO HAY CONTINGENCIA		

2.6.2.1.3 Monitoreo del Plan

2.6.2.1.4 Duración de la Contingencia

Depende del nivel de la complejidad del daño presentado, pero inicialmente se estima que puede durar entre 5 y 24 horas.

2.6.2.1.5 Retorno a Operación Normal

Actividad	Responsable	Tiempo Estimado
1. Telmex confirma que el servicio se encuentra de nuevo funcionando	Especialista en Comunicaciones/ Soporte Telmex	Depende de lo critico del daño Entre 5 y 24 horas

2.6.2.1.6 **CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN**

- ✓ El hardware afectado ha sido reparado y se ha comprobado su correcto funcionamiento.
- ✓ El software afectado ha sido reparado, reemplazado y/o actualizado y se ha comprobado y verificado su correcto funcionamiento.
- ✓ Los datos afectados han sido recuperados y se ha comprobado su disponibilidad e integridad.
- ✓ Se ha restablecido de manera satisfactoria el funcionamiento de los canales de comunicación.
- ✓ Se ha restablecido de manera satisfactoria el fluido eléctrico y el funcionamiento de las líneas telefónicas

2.6.2.2 Escenario 8-Falla Acceso a Internet

2.6.2.2.1 Criterios para Invocar el Plan

- No se puede entablar comunicación entre el Transborder e Internet por posibles caídas del Firewall.
- Intermitencia en el acceso a internet.
- Caída de uno de los proveedores de acceso a Internet.

2.6.2.2.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Mediante requerimiento se informa la no disponibilidad del servicio de Internet.	Usuario Final	10 minutos
2. Mediante herramientas del protocolo TCP IP (ping, tracert, traceroute, dig, nslookup, etc.), se revisa el estado de los canales provistos para el acceso a Internet para identificar el posible problema.	Administrador de Infraestructura	10 minutos
3. Si se presenta alguna anomalía en el servicio, se realiza contacto con Telmex para confirmar alguna posible falla en el servicio por ellos prestado.	Administrador de Infraestructura	10 minutos
4. Se cambia el Gateway del servidor de correo electronico, para recibir y enviar correo por el otro canal (DIVEO) los apuntamientos DNS ya están realizados.	Administrador de Infraestructura	10 minutos
5. Si Telmex confirma errores presentados en la comunicación entre Transborder e Internet, se realizan diversos análisis tendientes a encontrar una causa posible.	Administrador de Infraestructura /Soporte Telmex	30 minutos
6. Si la solución no se da en un tiempo prudente se procede a realizar el cambio de proveedor de		

Actividad	Responsable	Tiempo Estimado
canal por ETB utilizando herramientas propias para este fin, con esto se asegura una corrección en la comunicación temporalmente mientras se corrigen los problemas presentados.	Administrador de Infraestructura	10 minutos
7. Se informa a Gerencia de Tecnologia la contingencia adoptada.	Administrador de Infraestructura	5 minutos
8. Se prueba el correcto funcionamiento del Acceso a Internet.	Usuarios finales	5 minutos

2.6.2.2.3 Monitoreo del Plan

- Se realizarán controles de chequeo sobre los paquetes transmitidos a través del medio contingente.
- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre la solución propuesta por el proveedor de ancho de banda que presentó el inconveniente.

2.6.2.2.4 Duración de la Contingencia

Depende del nivel de la complejidad del daño presentado, pero inicialmente se estima que puede durar entre 1 y 8 horas.

2.6.2.2.5 Retorno a Operación Normal

Actividad	Responsable	Tiempo Estimado
1. Telmex confirma que el servicio se encuentra de nuevo funcionando.	Especialista en Comunicaciones/ Soporte Telmex	Depende de lo critico del daño Entre 1 hora y 8 horas
2. Transborder se modifican las tablas de enrutamiento para usar el canal principal	Administrador de Infraestructura	10 Minutos

2.6.2.2.6 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

- ✓ Se ha restablecido de manera satisfactoria el funcionamiento de los canales de comunicación.

2.6.2.3 Escenario 9-Falla en el FIREWALL

2.6.2.3.1 Criterios para Invocar el Plan

- No se puede entablar comunicación entre Transborder y otras redes por posibles caídas del Firewall.
- Intermitencia en el acceso a otras redes.

2.6.2.3.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Mediante requerimiento se informa la no disponibilidad de los servicios de otras redes.	Usuario Final	10 minutos
2. Mediante herramientas del protocolo TCP IP (ping, tracert, traceroute, dig, nslookup, etc.), se revisa el estado de los canales provistos para el acceso a Internet para identificar el posible problema.	Administrador de Infraestructura	10 minutos
3. Si se presenta alguna anomalía en los canales de comunicación, se debe observar el escenario correspondiente, si se determina que es el firewall se continua con este procedimiento.	Administrador de Infraestructura	10 minutos
4. Se Informa a Lock-net, de la falla presentada	Administrador de Infraestructura	10 Minutos
5. NO HAY CONTINGENCIA POR PARTE DE LOCK-NET		
6. Se conecta el equipo Linux 192.168.100.1, y se adicionan las ips publicas de Transborder a la tarjeta WAN y se adicionala ip 192.168.100.2 a la tarjeta LAN.	Administrador de Infraestructura	10 Minutos
7. Con el usario root Se ejecuta el script /root/fw2	Administrador de infraestructura	5 Minutos
8. Se realiazn pruebas de envio y recepción de correo, y acceso a internet	Administrador de Infraestructura	15 Minutos

2.6.2.3.3 Monitoreo del Plan

- Se realizarán controles de chequeo sobre los paquetes transmitidos a través del medio contingente.

- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre la solución propuesta por el proveedor que presentó el inconveniente (Lock-net).

2.6.2.3.4 Duración de la Contingencia

Depende del nivel de la complejidad del daño presentado, pero inicialmente se estima que puede durar entre 1 y 8 horas.

2.6.2.3.5 Retorno a Operación Normal

Actividad	Responsable	Tiempo Estimado
1. LockNet repara el firewall	Lock-net	Por estimar
2. Gerencia de Tecnologia, autoriza la puesta en producción del firewall administrador por Lock-net.	Gerencia deTecnologia	10 Minutos
3. Se retiran las direcciones IP publicas de la tarjeta WAN y la IP 192.168.100.2 ed firewall contingente	Administrador de Infraestructura	15 Minutos
4. Se pone en producción el firewall principal	Lock-net/Administrador de Infraestructura	15 Minutos

2.6.2.3.6 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

✓ Se ha restablecido de manera satisfactoria el funcionamiento del Firewall Principal.

2.6.2.4 Escenario 10-Falla en un Switch

2.6.2.4.1 Criterios para Invocar el Plan

- No se puede entablar comunicación entre algunos equipos de Transborder debido a falla en alguno de los Switch de la red.
- Intermitencia en el acceso a otras redes.

2.6.2.4.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Mediante requerimiento, o vía telefónica se informa la no disponibilidad de los servicios de red.	Usuario Final	10 minutos
2. Mediante herramientas del protocolo TCP IP (ping, tracert, traceroute, dig, nslookup, etc.), se revisa el estado de los dispositivos	Administrador de Infraestructura	

Actividad	Responsable	Tiempo Estimado
de comunicación de la red del Transborder.		10 minutos
3. Si se presenta alguna anomalía en los canales de comunicación, se debe observar el escenario correspondiente, si se determina que es el Switch se continua con este procedimiento.	Administrador de Infraestructura	10 minutos
4. Se dispone de un Switch de reserva en la Gerencia de Tecnologia, a este se deberán conectar todos los puntos de red que estuviesen conectados al Switch averiado.	Administrador de Infraestructura	10 – 30 Minutos

2.6.2.4.3 Monitoreo del Plan

- Se realizarán controles de chequeo sobre los paquetes transmitidos a través del medio contingente.
- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre la solución propuesta por el proveedor de ancho de banda que presentó el inconveniente.

2.6.2.4.4 Duración de la Contingencia

Depende del tiempo en que tome adquirir un nuevo Switch.

2.6.2.4.5 Retorno a Operación Normal

Inmediato, tras reemplazar el Switch ya no hay contingencia.

2.6.2.4.6 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

- ✓ Se ha reemplazado de manera satisfactoria el Switch.

2.6.2.5 Escenario 11-Falla en el CCTV

2.6.2.5.1 Criterios para Invocar el Plan

- No se puede entablar comunicación entre el circuito cerrado de televisión y los equipos autorizados para su monitoreo debido a falla en el servidor cámaras.

2.6.2.5.2 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Mediante requerimiento, o vía telefónica la gerencia de tecnologia informan la no disponibilidad del circuito cerrado de televisión.	Gerencia de tecnologia	10 minutos
2. Mediante herramientas de diagnostico del sistema operativo, se determina la causa el problema.	Administrador de Infraestructura	30 minutos
3. Si se debe a una falla de software, se debe reinstalar el sistema operativo y el software base. Si se debe a una falla de hardware se debe identificar la pieza, generar requerimiento al área administrativa para la adquisición de la misma	Administrador de Infraestructura	1 – 48 Horas
4. Se verifica que el CCTV funcione adecuadamente	Administrador de Infraestructura	10 – 30 Minutos

2.6.2.5.3 Monitoreo del Plan

- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre la adquisición de la parte averiada.

2.6.2.5.4 Duración de la Contingencia

Depende del tiempo en que tome adquirir el hardware en mal funcionamiento.

2.6.2.5.5 Retorno a Operación Normal

2.6.2.5.6 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

- ✓ Se ha reiniciado de manera satisfactoria el servicio de CCTV.

Escenario 12 No hay acceso a las instalaciones de Transborder

2.6.2.5.7 Criterios para Invocar el Plan

- No se puede Ingresar a las instalaciones de transborder, por asonadas, acto terrorista, bloqueo judicial, orden policial, manifestación, desordenes de orden publico, etc.
- No hay ninguna afectación eléctrica en el edificio Cr 7 # 17-51

2.6.2.5.8 Plan de Contingencia

Actividad	Responsable	Tiempo Estimado
1. Mediante Comunicación telefónica (celular), se informa a los gerentes que no es posible accesar a las instalaciones de transborder	Cualquier empleado de Transborder	10 minutos
2. El Gerente que se entera en el numeral 1, informa a los demás de dicha situacion	Gerente respectivo	10 minutos
3. Se solicitan certificados VPN temporales, para las areas que asi lo requieran, con un máximo de 2 certificados por area.	Administrador de Infraestructura	1 Horas
4. Se Instala y configura OPEN VPN en equipos de los usuarios asignados, para que se puedan conectar via VPN.	Administrador de Infraestructura / Coordinador de Soporte Tecnico	30 – 60 Minutos

2.6.2.5.9 Monitoreo del Plan

- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre la novedad de acceso a las instalaciones.

2.6.2.5.10 Duración de la Contingencia

Indeterminado.

2.6.2.5.11 Retorno a Operación Normal

Tiempo Indeterminado.

2.6.2.5.12 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

- ✓ Se ha levantado la restricción de acceso a las instalaciones de transborder.

2.6.2.6 Escenario 13-Destruccion de las instalaciones de transborder

2.6.2.6.1 Criterios para Invocar el Plan

- Las instalaciones de Transborder se encuentran destruidas, debido a catástrofe natural (inundación, terremoto. Incendio) o acto terrorista.
- Todos los servicios de red se encuentran afectados.

2.6.2.6.2 Plan de Contingencia

Se replica via DFS diariamente los archivos entre el servidor principal y su espejo, el cual esta ubicado en la ciudad de Medellin (debe considerarse un dia adicional que tomaria que alguien de tecnología llegue a Medellin para restaurar algún archivo no considerado inicialmente en el plan de contingencia).

Aproximadamente se puede restablecer en 3 Horas

Actividad	Responsable	Tiempo Estimado
1. Si la catástrofe se presenta en horario laboral debe primar el plan de evacuación de transborder y el del edificio. Una vez se encuentren a salvo todo el recurso humano se pasa al numeral 2.	TODOS	20 minutos
2. Se genera Un ticket en E-care para redireccionar los registros DNS de Transborder y Transtainer para la nueva dirección IP.	Administrador de Infraestructura	4 Horas
3. Se realizan pruebas de envio y recepción de correo electrónico.	Administrador de Infraestructura	1 Hora
4. Se continua según lo indicado en el escenario No acceso al edificio.	TODOS	

2.6.2.6.3 Monitoreo del Plan

- Para todos los casos se hará seguimiento telefónico o por correo electrónico del estado en que se encuentre el restablecimiento de los servicios de red..

2.6.2.6.4 Duración de la Contingencia

Indeterminado.

2.6.2.6.5 Retorno a Operación Normal

Tiempo Indeterminado, se debe crear una nueva red de datos.

2.6.2.6.6 CRITERIOS PARA RETORNAR AL MODO NORMAL DE OPERACIÓN

- ✓ Se ha construido una nueva sede para transborder y se han instalado todos los servicios de infraestructura.

3 PRUEBAS Y ENTRENAMIENTO

Para tener planes de contingencia exitosos, estos deben ser probados regularmente, y en lo posible en sistemas de pruebas para no afectar el Up-time de sistemas productivos acordados con el cliente.

3.1 Pruebas

- ✓ Se han probado con éxito los planes de contingencia que hacen referencia a daño en parte redundante, daño en uno de los servidores de producción, daño en ambos servidores de producción, daño en servidor de pruebas y restauración de Backups. Estas últimas de han realizado de manera constante en los servidores de desarrollos y prueba, bien sea para atender los requerimientos de Transborder o por necesidad real y no se ha presentado pérdida de información con respecto a la última copia generada.

- ✓ Se han probado con éxito los planes de contingencia que hacen referencia a fallas de hardware en unidades de backup.

- ✓ Los canales instalados en las oficinas del cliente, han sido debidamente configurados juntamente con información necesaria y probados para garantizar su correcto funcionamiento en caso de falla de los canales o del router.

Es necesario aplicar un registro de cambios que permita determinar qué, quién y cuándo se han hecho cambios este documento, para ello se debe diligenciar la siguiente tabla:

REGISTRO DE CAMBIOS			
Página	**Tema**	**Fecha del cambio**	**Cambio**