ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

INSTITUTO PARA LA ECONOMIA SOCIAL

IPES

Plan de Contingencia de TI

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

PROCESO DE GESTION DE LA SEGURIDAD DE LA INFORMACION Y RECURSOS TECNOLOGICOS

Bogotá D.C. Noviembre de 2017

Elaboró:	Reviso:	Aprobó:
John Jair Garzón	Clarisa Díaz García	Clarisa Díaz García
Profesional	Subdirector de Diseño y Análisis Estratégico	Subdirector de Diseño y Análisis Estratégico

Contenido

1 Introducción 6

2 Descripción general del plan de contingencia 8

2.1 Requerimientos estatutarios 8

2.1.1 Ley 87 de 1993 8

2.1.2 MECI 1000:2005 8

2.1.3 Sistema de gestión de calidad NTC-GP 1000 9

2.1.4 Resolución 305 de la Comisión Distrital de Sistemas 9

2.1.5 Directiva 02 de 2004 Comisión Distrital de Sistemas : políticas generales de tecnología de información y comunicaciones aplicables a las entidades del distrito capital 10

2.2 Política de contingencia 10

2.2.1 Comunicación de la política de contingencia 10

2.3 Objetivos 10

2.4 Supuestos 11

2.5 Administración del plan de contingencia 11

2.5.1 Descripción general de sistemas de información y tecnología críticos para IPES 11

2.5.2 Roles involucrados en la estrategia de contingencia del IPES 12

2.5.3 Identificación de roles y responsabilidades del plan de contingencia 13

2.6 Mantenimiento del plan de contingencia 17

2.6.1 Revisión y actualización del plan 17

2.6.2 Coordinación con terceros interesados 18

2.6.3 Distribución del plan 18

2.6.4 Registro de cambios 18

3 Análisis de impacto al negocio 20

3.1 Propósito y etapas del BIA 20

3.2 Identificación de procesos y sistemas críticos 20

3.3 Identificación de impactos y valoración de tiempo no disponible 22

3.4 Identificación de impactos por servicios 23

3.5 Identificación de tiempos y objetivos de recuperación 24
3.6 Recursos tecnológicos por servicio 24
3.7 Prioridades de recuperación 27
3.8 Escenarios de riesgo 27
3.8.1 Escenarios de riesgo generales 28
3.8.2 Escenarios de riesgo asociados a pérdida de disponibilidad 28
3.8.3 Escenarios de riesgo asociados a la pérdida de integridad 29
4 Controles preventivos 30
4.1 Capacidad de la UPS. 30
4.2 Capacidad de los sistemas de refrigeración. 30
4.3 Sistema de extinción de incendio 31
4.4 Sistemas de monitoreo de capacidad de servidor. 31
4.5 Sistemas de monitoreo de aplicación 31
4.6 Sistemas de monitoreo de base de datos 31
4.7 Sistemas de almacenamiento de copias de respaldo 31
4.8 Sistema de almacenamiento de copia de respaldo en sitio remoto 32
4.9 Periodicidad del respaldo de datos 32
4.10 Sistemas de protección de la seguridad de la información 32
5 Definición de las estrategias de contingencia 34
5.1 Uso de site alterno 34
5.1.1 Centro alterno en acuerdo con otra entidad 34
5.1.2 Centro alterno contratado 34
5.1.3 Identificación de equipos 34
5.1.4 Acuerdos con proveedores 35
5.1.5 Arquitectura de contingencia 35
6 Fases del plan de contingencia 37
6.1 Fase de notificación y activación 37
6.2 Identificación de incidentes 37

6.3 Criterios para activación del plan de contingencia 37
6.3.1 Daños en componentes de tecnología 38
6.4 Procedimientos de notificación 38
6.4.1 Notificación telefónica 40
6.4.2 Notificación vía correo electrónico 40
6.4.3 Notificación por mensaje de texto 40
6.5 Fase de recuperación 41
6.5.1 Estrategias de recuperación 41
6.5.2 Verificación de funcionamiento de aplicaciones críticas 44
6.5.3 Aprovisionamiento de puestos de trabajo para personal de misión crítica 44
6.5.4 Verificación de funcionamiento de puestos de trabajo 44
6.5.5 Aprovisionamiento de servicio de impresión de contingencia 44
6.5.6 Aprovisionamiento de servicio telefónico de contingencia 45
6.5.7 Procedimientos de recuperación 45
6.6 Escalamiento 45
6.7 Fase de restablecimiento de servicios 46
6.7.1 Criterios para finalizar las acciones de contingencia 46
6.7.2 Ejecución de procesos concurrentes entre infraestructura de contingencia e infraestructura normal de tecnología 46
6.7.3 Restablecimiento de sistemas críticos 47
6.7.4 Prueba de sistemas restablecidos 48
6.7.5 Pruebas de sistemas de información después de restaurar backup 48
6.7.6 Notificaciones 48
6.7.7 Limpieza y desmonte de la infraestructura de contingencia 49
6.7.8 Almacenamiento de datos del site alterno 49
6.7.9 Documentación 49
7 Pruebas, entrenamiento y simulación 50
7.1 Plan de pruebas 50

7.1.1 Sensibilización 50
7.1.2 Instrucción formal del plan 50
7.1.3 Revisión de escritorio 50
7.1.4 Recorrido guiado por el plan 51
7.1.5 Simulación 51
7.1.6 Ejercicio de actividad crítica 51
7.1.7 Restauración de datos en equipo alterno 51
7.1.8 Prueba completa del plan de contingencia 52
7.2 Entrenamiento de personal 52
7.2.1 Conceptos de continuidad de negocio 52
7.2.2 Procedimientos básicos de apoyo al plan de contingencia del IPES 52
7.2.3 Procedimientos técnicos del plan de contingencia 52
8 Anexos 54
8.1 Formato de reporte de valoración de incidente 54
8.2 Procedimientos de restablecimiento de servicios 56
8.3 Formato diario de revisión de servicios de tecnología 58
8.4 Registros de las cintas que se utilizan para los Backups 72

1 Introducción

El Instituto para la Economía Social **-** IPES tiene por objeto promover, coordinar y ejecutar políticas, programas y proyectos de desarrollo económico del Distrito a través de diferentes estrategias en sectores sociales informales, encaminadas al fortalecimiento de las competencias productivas, empresariales y comerciales, la formación del capital humano, el apoyo a proyectos productivos de la micro, pequeña y mediana empresa y la administración de las plazas de mercado, en coordinación con el plan de abastecimiento de alimentos, generando esquemas de mejoramiento de calidad de vida.[1]

1.1. Misión

Aportar al desarrollo económico de la ciudad mediante la oferta de alternativas de generación de ingresos a la población de la economía informal que ejerce sus actividades en el espacio público, enfocadas a la formación, el emprendimiento, el fortalecimiento empresarial y la gestión de plataformas comerciales competitivas; así como administrar y desarrollar acciones de fortalecimiento del Sistema Distrital de Plazas de Mercado

1.2. Visión

En el 2025 seremos reconocidos como una entidad que contribuye al mejoramiento de las condiciones de vida de los actores de la economía informal, a través de alternativas productivas, competitivas, sostenibles y generadoras de ingresos que propendan por su inserción en los circuitos de mercado formal y por el posicionamiento de las plazas de mercado como lugares de encuentro ciudadano, de abastecimiento de productos de calidad y precios competitivos, así como referentes turísticos y gastronómicos del país.

Con el propósito de mejorar continuamente su capacidad institucional, se ha definido el siguiente plan de contingencia de tecnologías de información y comunicaciones TIC`s, que permita una pronta recuperación en caso materializarse uno o más incidentes de seguridad de la información que comprometan la continuidad y disponibilidad de los sistemas y servicios informáticos y de red que soportan sus funciones misionales, administrativas y de gestión.

[1] DE-010 PLAN ESTRATEGICO 2016-2020

El plan de contingencia se ha estructurado en las siguientes secciones:

- **Capítulo 1**: Descripción general del plan de contingencia: Contienen la descripción general del plan, sus componentes, esquema de mantenimiento.

- **Capítulo 2:** Análisis de impacto al negocio: Identificación de los procesos críticos de tecnología, que apoyan el cumplimiento de la misión del IPES.

- **Capítulo 3**: Controles: Identificación de los controles de tecnología esenciales para el buen funcionamiento del plan de contingencia.

- **Capítulo 4:** Estrategia de contingencia: Esquema general de la estrategia de contingencia para el mantenimiento de los servicios misionales.

- **Capítulo 5:** Fases del plan de contingencia: Como se debe activar el plan, que actividades se deben ejecutar en contingencia, como se debe notificar el avance de las actividades de contingencia y como se debe volver a condiciones normales la infraestructura de IT.

- **Capítulo 6:** Pruebas, entrenamiento: Esta sección describe las actividades que se deben realizar para mantener actualizado el plan de contingencia.

2 Desarrollo

2.1 Capítulo 1: Descripción general del plan de contingencia

2.1.1 Requerimientos estatutarios

El plan de contingencia del IPES se desarrolla para brindar confianza a los interesados en que los servicios informáticos misionales, administrativos y de gestión y la plataforma tecnológica que los soporta, contarán con estrategias claramente definidas para mitigar los riesgos, sus causas y consecuencias, que pueden afectar la normal operación informática institucional. Normativamente el plan se soporta en los siguientes aspectos:

- **Ley 87 de 1993,** promulga el modelo de control interno para las entidades del estado en la cual "se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones". En particular el artículo 2do de la ley 87 que establece:

  ARTÍCULO 2o. OBJETIVOS DEL SISTEMA DE CONTROL INTERNO. Atendiendo los principios constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientarán al logro de los siguientes objetivos fundamentales:
  a) Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten;
  e) Asegurar la oportunidad y confiabilidad de la información y de sus registros;
  f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos;

2.1.2 MECI 1000:2005

El modelo estándar de control Interno MECI 1000:2005 plantea una serie de componentes que guardan estrecha relación con el establecimiento de mecanismos que garantice la continuidad en el cumplimiento de la función misional y la disponibilidad de la información.

2.2 Objetivos de Control Estratégico

Diseñar los procedimientos necesarios, que permitan a la Entidad Pública cumplir la misión para la cual fue creada y proteger los recursos que se encuentren bajo su custodia, buscando administrar en forma diligente los posibles riesgos que se puedan generar.

2.3 Objetivos de Control de Ejecución.

Constituyen objetivos de Control de Ejecución de la Entidad Pública los siguientes:

a) Determinar los procedimientos de prevención, detección y corrección que permitan

mantener las funciones, operaciones y actividades institucionales en armonía con los principios de eficacia, eficiencia y economía.

2.4 Objetivos de Control de Evaluación. Constituyen objetivos de Control de

Evaluación de la Entidad Pública los siguientes:

d) Propiciar el mejoramiento continuo del Control y de la Gestión de la

Entidad, así como de su capacidad para responder efectivamente a los diferentes grupos de interés

3.3.2 Planes de Mejoramiento por Procesos. Elemento de Control, que contiene los planes administrativos con las acciones de mejoramiento que a nivel de los procesos y de las áreas responsables dentro de la Organización Pública, deben adelantarse para fortalecer su desempeño y funcionamiento, en procura de las metas y resultados que garantizan el cumplimiento de los objetivos de la Entidad en su conjunto.

2.1.3 Sistema de gestión de calidad NTC-GP 1000

A nivel del sistema de gestión de calidad para la administración pública, los siguientes requerimientos soportan el establecimiento de un plan de contingencia.

"6.3 INFRAESTRUCTURA
La entidad debe determinar, proporcionar y mantener la infraestructura necesaria para lograr la conformidad con los requisitos del producto y/o servicio. La infraestructura incluye, cuando sea aplicable:
a) edificios, espacio de trabajo y servicios asociados,
b) equipo para los procesos, (tanto hardware como software), y
c) servicios de apoyo (tales como transporte o comunicación)."

2.1.4 Resolución 305 de la Comisión Distrital de Sistemas

ARTÍCULO 18. PLANES DE CONTINGENCIA. Los Jefes de las áreas de informática de las entidades, organismos y órganos de control del Distrito Capital deben formular "Planes de Contingencia" que garanticen la continuidad de las operaciones ante una situación crítica que pueda amenazar, parcial o totalmente, la prestación de servicios.

PARÁGRAFO 1º. El Plan de contingencia que se adopte debe ser formulado conforme a una metodología específica para tal fin, contemplar todos los tipos de riesgo posibles para la entidad, establecer el plan de manejo del riesgo y los planes de acción específicos en cada caso, ser avalado por la Alta Dirección, socializado en todos los niveles de la organización estableciendo las responsabilidades correspondientes y revisado periódicamente de acuerdo con el "Plan Estratégico de Sistemas de Información" y con cambios en las condiciones operativas de la entidad.

PARÁGRAFO 2º. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben estimular la creación de una Cultura de Seguridad de la información para

garantizar la "adecuada implementación del Plan de Contingencia".

2.1.5 Directiva 02 de 2004 Comisión Distrital de Sistemas : políticas generales de tecnología de información y comunicaciones aplicables a las entidades del distrito capital

"4.3.2 Formulación de la política

Las áreas de informática de las entidades del Distrito deberán formular Planes de Contingencia que garanticen la continuidad de las operaciones ante una situación crítica que pueda amenazar, parcial o totalmente, la prestación de servicios."

2.2 Política de contingencia

El INSTITUTO PARA LA ECONOMIA SOCIAL establecerá, mantendrá, implementará, operará, realizará seguimiento, revisará, mantendrá y mejorará un plan de contingencia de tecnología para mitigar los riesgos que afecten a sus componentes críticos de Tecnología de Información y Comunicación para brindar confianza suficiente a todos los interesados de que su servicios misionales se mantienen en niveles de funcionamiento que no afecten el cumplimiento de la misión de la Entidad

EL IPES documenta, revisa y actualiza periódicamente los procedimientos necesarios para garantizar el correcto funcionamiento del plan de contingencia, así como las responsabilidades y roles para el mantenimiento y operación del mismo. Todo el personal con funciones o relación con el plan de contingencia ser capacitado de acuerdo con sus responsabilidades específicas.

Periódicamente el IPES realiza pruebas del plan de contingencia para identificar oportunidades de mejoras o debilidades a corregir.

2.2.1 Comunicación de la política de contingencia

La política de contingencia debe ser comunicada formalmente a todos los funcionarios, contratistas y partes interesadas del IPES. La política de contingencia forma parte integral de las políticas de seguridad de la información del IPES y debe ser conocida, aceptada y aplicada por todo el personal del IPES.

2.3 Objetivos

Son objetivos del plan de contingencia del IPES:

- Brindar confianza a todos los interesados de que el IPES cuenta con estrategias, planes y recursos para garantizar la continuidad de sus servicios de información y tecnología
- Contar con un conjunto de procedimientos claros para el restablecimiento de los servicios de tecnología que soportan la función misional en caso de no disponibilidad de los mismos.

- Establecer una línea base para el desarrollo de una cultura de la seguridad de la información en los funcionarios y contratistas de la entidad.

2.4 Supuestos

El cumplimiento de los siguientes supuestos es fundamental para que el plan de contingencia cumpla con sus objetivos:

- El plan de contingencia se construye con el aporte técnico, administrativo y estratégico del personal dueño de procesos misionales del IPES.
- El plan de contingencia cuenta con la aprobación y soporte del nivel directivo del IPES.
- El plan de contingencia recibe los recursos necesarios para mantenerse actualizado y operativo.
- El plan de contingencia se somete a pruebas mínimo una vez al año.
- El personal del IPES es capacitado periódicamente en los procedimientos del plan.

2.5 Administración del plan de contingencia

2.5.1 Descripción general de sistemas de información y tecnología críticos para IPES

En la actualidad el IPES soporta tecnológicamente en sistemas de información y servicios a la red. a Continuación se relacionan los principales sistemas de información y servicios que soportan la operación misional del IPES. La descripción detallada y configuraciones especificas de cada sistema y servicio se encuentran documentados en manuales técnicos que gestiona la oficina de sistemas.
HEMI: Constituye el sistema de información misional de la Entidad.
SIAFI: Es el sistema de información que soporta las funciones financieras y administrativas de la Entidad
Servicios de correo electrónico: Es el sistema que permite la comunicación de las actividades realizadas por los diferentes procesos misionales de la entidad, a la vez que es el medio de comunicación primario de los funcionarios y contratistas de IPES.
Almacenamiento de archivos: Mediante el uso de almacenamiento compartido en la NAS, referenciado internamente dentro de las estaciones de trabajo de IPES como el Drive U:, se permite el almacenamiento de la información resultante de las diferentes actividades realizadas por los funcionarios y contratistas del IPES.

Los anteriores sistemas y servicios, dependen de diversos componentes que son críticos para su correcto funcionamiento, entre ellos:
Almacenamiento compartido:

Sistema de almacenamiento NAS
Controlador de Dominio Active Directory
Red Lan

Servicio de correo electrónico:
Almacenamiento local de la estación de trabajo
Controlador de Dominio Active Directory
Servidor de correo electrónico

Sistema de información SIAFI
Servidor de aplicación
Servidor de base de datos
Red Lan
Controlador de dominio Active Directory

Sistema de información HEMI
Servidor de aplicación
Servidor de base de datos
Controlador de dominio Active Directory
Portal de Internet

Cualquiera de los servicios antes descritos depende para su uso de estación de trabajo y conectividad LAN hacia los servidores que soportan el servicio

Finalmente la prestación de los servicios críticos de información y tecnología dependen de infraestructura básica de energía eléctrica, conectividad hacia Internet.

2.5.2 Roles involucrados en la estrategia de contingencia del IPES

Todo el personal del IPES tiene relación con el plan de contingencia, ya que las funciones de la entidad dependen de una u otra forma de su talento humano y sin la activa participación de funcionarios y contratistas, los servicios de información y tecnología no pueden cumplir por si solos la misión del IPES.

Para definir una estructura formal de roles y responsabilidad para la administración de plan de contingencia de tecnología se documentan a continuación los principales roles y cargos tienen especiales responsabilidades dentro del plan. Para obtener una descripción detallada de las responsabilidades de estos roles se debe consultar a sección “Identificación de roles y responsabilidades” dentro de este mismo plan.

- Director General del IPES
- Asesor de control interno
- Subdirector Administrativo y Financiero
- Jefe de Oficina de sistemas
- Rol Coordinador de plan de contingencia
- Rol Administrador de red

- Rol Administradores de bases de datos
- Rol Administrador de servidores

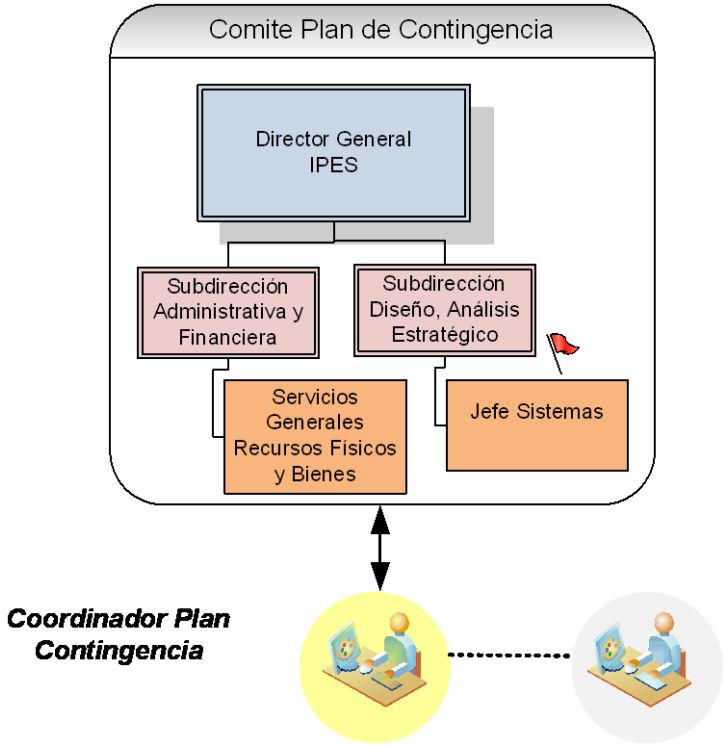
2.5.3 Identificación de roles y responsabilidades del plan de contingencia

Comité de plan de contingencia

El comité de contingencia es una instancia temporal dentro del IPES cuya función es revisar a intervalos planificados la vigencia y pertinencia de las estrategias de contingencia de información y tecnología del IPES. El comité se reúne en las mismas sesiones del comité de sistemas del IPES y discute los aspectos específicos de la estrategia de contingencia del IPES

El comité es el encargado de aprobar la política de contingencia y aprobar el plan de contingencia y sus actualizaciones. El comité está conformado por las siguientes personas, pero puede citar para aspectos particulares a quienes considere necesarios para el desarrollo de los planes de contingencia de tecnología de la Entidad:

- Director General del IPES o su representante. Quién es la persona que preside el comité.
- Subdirector administrativo y financiero o su representante.
- Subdirector de Diseño y Análisis estratégico o su representante.
- Jefe de oficina de sistemas.
- Representante de la oficina de control interno quién participa con voz pero sin voto en la sesiones del comité de contingencia



Dentro de las tareas del comité están la de nombrar un coordinador del plan de contingencia y definir el rol la persona responsable de emitir la orden de inicio del plan de contingencia.

Responsable de inicio del plan de contingencia.
Es la persona nombrada por el comité del plan de contingencia para evaluar la necesidad de iniciar el plan de contingencia, dentro de sus responsabilidades están evaluar el impacto de la situación que está afectando a la Entidad a nivel de servicios de información y tecnología.

El responsable del inicio del plan de contingencia debe evaluar

1) Si el evento es un incidente que puede ser tratado por los procesos de atención de incidentes y problemas, en caso contrario,

2) Determinar si el evento ha recibido la calificación de problema y ya se debe realizar un escalamiento a proveedores o fabricantes de los componentes afectados

3) En caso de que el evento calificado como problema no haya sido resuelto en el tiempo máximo definido en los acuerdo de niveles de servicio con proveedores o fabricantes se debe determinar la necesidad de activar el plan de contingencia y

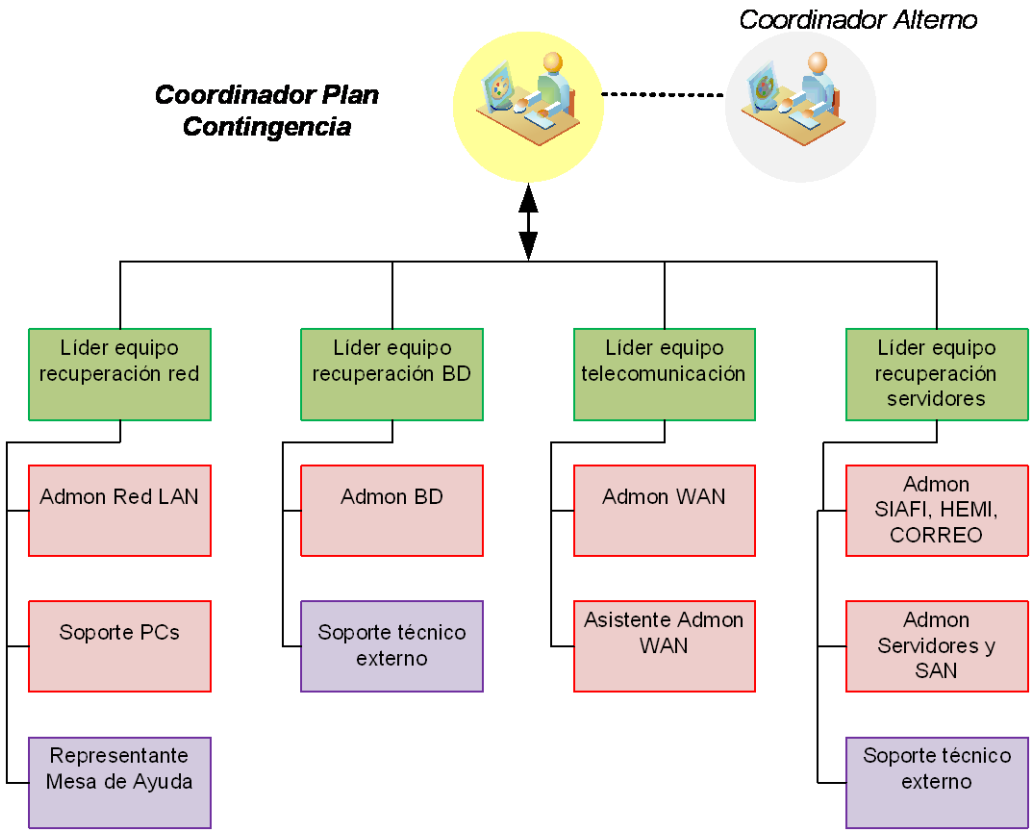
proceder a la realización de todas las acciones definidas de acuerdo con el escenario identificado.

Una vez se ha tomado la determinación de activar el plan de contingencia de IT, el coordinador del plan debe comunicar a la Dirección General de IPES la necesidad de informar a los diferentes subdirectores que la plataforma de Información y tecnología ha entrado en contingencia y que deben activar sus planes específicos de continuidad de negocio.

Una vez se activa el plan de contingencia, el coordinador debe realizar el reporte de evento y comunicar el hecho a los líderes operativos del plan de contingencia y a los integrantes del comité del plan de contingencia

El coordinador del plan de contingencia será el único responsable de coordinar las comunicaciones entre los líderes operativos y el comité del plan de contingencia.

Rol propuesto: Jefe del área de sistemas del IPES



Coordinador de plan de contingencia y coordinador alterno.
Persona nombrada por el comité del plan de contingencia y encargada de realizar el reporte de incidente y comunicar el hecho a los líderes operativos del plan de contingencia y a los integrantes del comité del plan de contingencia.

Es el responsable de coordinar las comunicaciones entre los líderes operativos y el comité del plan de contingencia y sus decisiones estratégicas y administrativas, ver figura árbol de notificación.

Administrador de red.
Persona encargada de hacer la valoración del incidente y coordinar las actividades de contingencia de acuerdo al documento plan de contingencia conducente a la recuperación de los elementos y actividades que tienen que ver con la red de área local (LAN). Las personas que pertenecen a este equipo de contingencia son:

- Administrador de red LAN (equipos activos, cableado estructurado, energía, Aiea acondicionado).
- Encargado del soporte de computadores personales y portátiles.
- Encargado de la mesa de ayuda. Quién recibirá y clasificará todas las notificaciones que se pueden recibir por el incidente a través de la mesa de ayuda.

Administradores de base de datos.
Persona encargada de hacer la valoración del incidente y coordinar las actividades de contingencia de acuerdo al documento plan de contingencia conducente a la recuperación de los elementos de software y actividades que tienen que ver con las bases de datos. Las personas que pertenecen a este equipo de contingencia son:

- Administrador base de datos Oracle.
- Administrador base de datos SQL.
- Soporte técnico externo o de fabricante.

Líder equipo de telecomunicaciones.
Persona encargada de hacer la valoración del incidente y coordinar las actividades de contingencia de acuerdo al documento plan de contingencia conducente a la recuperación de los elementos y actividades que tienen que ver con la red de área extensa (WAN), internet y equipos de seguridad perimetral. Las personas que

pertenecen a este equipo de contingencia son:

- Administrador de servicios de Internet y equipos de seguridad perimetral.

Administrador de servidores.
Persona encargada de hacer la valoración del incidente y coordinar las actividades de contingencia de acuerdo al documento plan de contingencia conducente a la recuperación de los elementos y actividades que tienen que ver con los servidores. Las personas que pertenecen a este equipo de contingencia son:

- Administrador de servidores de Sistema de Información HEMI.
- Administrador de servidores de Sistema de Información SIAFI
- Administradores de servidores de servicios básicos de red
- Controlador de dominio
- Sistema de almacenamiento NAS
- Servicios de Correo electrónico
- Soporte técnico externo o de fabricante.

2.6 Mantenimiento del plan de contingencia

2.6.1 Revisión y actualización del plan

El plan de contingencia de IT se debe revisar a intervalos planificados, mínimo una vez al año. La revisión del plan de contingencia es una de las actividades que se debe incluir en la revisión del Sistema Integrado de gestión del IPES. Las entradas que se deben revisar respecto al Plan de contingencia incluyen:

- Resultados de auditorías al cumplimiento del plan de contingencia
- Retroalimentación de partes interesadas como Comisión Distrital de Sistemas, Secretaria de Hacienda, Proveedores relacionados con el plan de contingencia, oficina de control interno entre otros

- Técnicas, productos o herramientas que se puedan utilizar para mejorar el plan de contingencia
- Cambios internos o externos que puedan afectar al plan de contingencia
- Resultados de las pruebas que se realicen al plan de contingencia
- Lecciones aprendidas de incidentes que afectaron la disponibilidad de servicios o la efectividad del plan de contingencia
- Resultados de las actividades de capacitación y toma de conciencia del plan de contingencia.

2.6.2 Coordinación con terceros interesados

Con el fin de que el plan de contingencia sea efectivo y las actividades que dependen de actores externos sean comunicadas en forma oportuna y precisa a esos terceros, se deben realizar sesiones de trabajo con proveedores de equipos, servicios, hardware, software o sistemas de información que estén a cargo del soporte o mantenimiento de los elementos de tecnología que están cubiertos por el alcance del plan de contingencia. En la sección “Identificación de recursos esenciales” se encuentra una lista de todos los recursos que conforman el plan de contingencia, incluidos terceros y personal necesario para la activación del plan de contingencia.

Además de los proveedores de servicios de tecnología, el plan debe ser socializado con entes de control distrital con el fin de recibir retroalimentación respecto a los compromisos del IPES respecto a la continuidad de los servicios que soportan la operación misional y de los niveles de apoyo técnico o administrativo que se requieren de esas partes interesadas en caso de requerirse la activación del plan de contingencia.

2.6.3 Distribución del plan

El plan de contingencia debe ser distribuido siguiendo los procedimientos del sistema integrado de gestión del IPES y las versiones más recientes siempre deben estar disponibles para los debidamente autorizados. Debido a que el plan de contingencia contiene información de carácter sensitivo del IPES, su divulgación debe ser controlada siguiendo las políticas de seguridad de la información. Una copia actualizada del plan debe permanecer fuera de las instalaciones del IPES en caso de que se requiera su consulta desde lugares diferentes a la sede principal del IPES. Se prefiere que el plan se mantenga en formato electrónico lo que facilita su actualización y control de distribución mediante clave de acceso. En los casos en que se deba activar el plan de contingencia, se preferirá dotar a cada responsable del plan de una copia impresa del mismo.

2.6.4 Registro de cambios

Todos los cambios al plan de contingencia deben ser documentados. Los cambios al plan se deben controlar mediante el procedimiento de control de documentos del

sistema integrado de gestión del IPES. La versión actualizada del plan de contingencia debe ser distribuida a las partes interesadas.

3 Análisis de impacto al negocio

Está sección del plan de contingencia contiene el análisis de impacto al negocio para el área de sistemas del IPES, esta sección del documento forma parte del proceso de planificación de la contingencia para los sistemas de información crítica del IPES.

3.1 Propósito y etapas del BIA

El propósito del BIA es identificar y priorizar los componentes de los sistemas de información, correlacionarlos con los procesos misionales que los soportan y de esta forma caracterizar el impacto que sobre estos procesos se presenta en caso de que no estén disponibles. El BIA está compuesto por:

Identificación de los procesos misionales y criticidad de recuperación.

En primera instancia se identifican los procesos misionales que son soportados por sistemas, el impacto que sobre los procesos genera la suspensión de los sistemas y el tiempo estimado de suspensión. El tiempo de suspensión debe reflejar el máximo tiempo que la entidad puede soportar la suspensión de servicios sin incumplir su función misional.

Identificación de requerimientos de recursos

La identificación realista de los esfuerzos necesarios para recuperar los sistemas implica una evaluación detallada de los recursos necesarios para reactivar los procesos misionales y la identificación de las interdependencias entre recursos y sistemas. Algunos de los elementos que se deben considerar incluyen: personal, instalaciones, equipos, software, archivos de datos, componentes de los sistemas y registros vitales.

Identificación de las prioridades de recuperación de recursos y sistemas

Basados en los resultados de la identificación de requerimientos se verifican las dependencias entre los sistemas y los procesos críticos de la entidad para determinar las prioridades de recuperación para establecer la secuencia de recuperación de las actividades y recursos.

Este documento se usa como entrada para construir el plan de contingencia de los procesos críticos. Este BIA puede ser usado como entrada a planes de recuperación ante desastres y los procedimientos de a respuesta a incidentes de seguridad de la información.

3.2 Identificación de procesos y sistemas críticos

Para formular el BIA del IPES se realizó un inventario de los procesos críticos y se determinaron los siguientes parámetros:

- **Periodicidad de entrega:** corresponde a la periodicidad en el tiempo de como cada proceso debe entregar resultados. Los parámetros de periodicidad definidos son: Diariamente, Semanalmente, Quincenalmente,

Mensualmente, Bimensualmente, Trimestralmente, Semestralmente, Anualmente

- **Evaluación de Tiempo de interrupción no programada:** Este parámetro se utiliza para establecer cuál sería el tiempo máximo que un proceso crítico puede soportar una suspensión del sistema de información. Los posibles valores son:
  7: No se puede esperar, el proceso nunca se puede detenerse,
  6: Puede esperar pero solo máximo 1 a 2 horas
  5: Puede esperar entre 3 y 5 horas
  4: Puede esperar hasta 1 día (8 horas)
  3: Puede esperar entre 2 y 3 días
  2: Puede esperar entre 4 y 5 días
  1: puede esperar más de 5 días

Nombre del servicio	**Periodicidad de entrega** (día, semanal, quincena, mes, bimensual, trimestral, semestral, anual)	**Tiempo de interrupción no programa tolerable** (Ver Evaluación de Tiempo de interrupción no programada)	**Descripción del servicio**
Sistema de información HEMI	El servicio se presta diariamente, el sistema de información HEMI funciona en modalidad 7x24	De acuerdo con la dinámica de utilización de los servicios de HEMI el tiempo máximo previsto para interrupción no programa de servicio HEMI está en 1 día (8 horas)	Sistema de información misional
SIAFI	El servicio se presta diariamente, el sistema de información SIAFI Se utiliza en modalidad 5 x 8 y en casos especiales sábado y domingos	El sistema de información SIAFI tiene fechas críticas de prestación de servicio que determinan diferentes tiempos de interrupción no programada. (ver tiempos de entrega de resultados de módulos SIAFI)	Sistema de información Financiero Administrativo
Almacenamiento compartido	El servicio se presta diariamente, la operación del servicio es 7x24 pero los usuarios solo tienen acceso al servicio desde las instalaciones de la red LAN de IPES	El servicio de almacenamiento de archivos en drive U mantiene una réplica de los archivos almacenados en los computadores personales de los usuarios. En términos generales el de espera no programado está entre 3 y 5 horas	Permite el almacenamiento de archivos en drive compartido U:
Correo electrónico	El servicio se presta diariamente, la operación del servicio es 7x24 los usuarios pueden tener acceso al servicio desde las instalaciones de la red LAN de IPES, el almacenamiento de los buzones de correo se realiza en la estación de trabajo de cada usuario.	El servicio de correo electrónico depende de la conectividad a Internet, los usuarios almacenan sus correos en la estación de trabajo con lo cual es posible trabajar fuera de línea está entre 1 y 2 horas	Permite el envió y recepción de correos electrónicos.

Tiempos de entrega de resultados de módulos principales de SIAFI

SIAFI es el sistema de información financiera del IPES, el sistema se basa en el sistema de información SICAPITAL de la Secretaria de Hacienda Distrital, los tiempos de entrega crítica de información de SIAFI se relacionan a continuación

Nombre del Proceso	**Periodicidad de entrega de resultados del proceso**	**Tiempo de interrupción NO programada**	**Descripción del proceso** (qué hace el proceso)
operación y gestión de tesorería (OPGET)	mensualmente. se tiene plazo para ejecutar el proceso asociado a OPGET hasta máximo 7 días hábiles antes de que termine el mes.	se puede esperar hasta 2 días sin sistema. siempre que la interrupción no se presente en la fechas crítica de ejecución de OPGET.	OPGET es el sistema operación y gestión de tesorería. automatiza las gestiones de recaudo, pagaduría, planeación financiera de la dirección distrital de tesorería. incluye módulos de ingresos, egresos y conciliaciones bancarias.
presupuesto distrital PREDIS	anualmente el último día hábil de cada año se deben entregar los resultados de PREDIS.	en un escenario en que falle PREDIS al final de año, máximo se puede esperar hasta el 3er día hábil del nuevo año para poder suministrar los resultados de PREDIS	PREDIS es el sistema de presupuesto distrital. apoya el proceso de programación, ejecución, control y seguimiento del presupuesto distrital.

3.3 Identificación de impactos y valoración de tiempo no disponible

Las siguientes categorías representan las áreas de mayor importancia que se deben evaluar por el impacto de incidentes en los procesos críticos.

- **Impacto Financiero**: Impactos relacionados con pérdida económica o multas. En el caso de las entidades del gobierno, el impacto financiero por pérdidas económicas siempre es severo.
- **Impacto Operacional**: Incumplimiento en los plazos para cumplir compromisos de la entidad. Capacidad para cumplir los compromisos misionales:

> *La misión del IPES es crear, promover y **ejecutar estrategias** de apoyo a la economía popular y de fortalecimiento económico de las personas, unidades domésticas y productivas, y grupos poblacionales que la integran, para contribuir a transformar el modelo de ciudad vigente, superar las diferentes formas vigentes de segregación urbana, adaptar la ciudad al cambio climático, mejorar la calidad de vida de la población y construir la paz.*

Criterios para cálculo de impactos de los eventos

Criterio	Impacto Severo (5)	Impacto Alto (3)	Impacto moderado (1)
Financiero	No es admisible ninguna clase de pérdida económica	No aplica	No aplica

Criterio	Impacto Severo (5)	Impacto Alto (3)	Impacto moderado (1)
Operacional (oportunidad para el cumplimiento de compromisos)	No se cumple el compromiso en ningún plazo. Es decir no se hace el trabajo	El compromiso no se cumple en la fecha establecida, se cumple en otra fecha y la entidad queda obligada a elaborar un plan de mejora para resolver el no cumplimiento	El compromiso no se cumple en la fecha definida, se cumple en fecha posterior pero no se requiere un plan de mejora para resolver el no cumplimiento
Satisfacción de interesados (ciudadano, otras entidades, entes de control	No se puede cumplir la misión institucional	Se cumple en forma parcial la misión institucional	Se cumple la misión institucional con variaciones que no afectan a los interesados

3.4 Identificación de impactos por servicios

El impacto a nivel de servicios permite determinar que puede ocurrir a nivel financiero e impacto operacional en caso de no disponibilidad de alguno de los servicios considerados como críticos para el cumplimiento de la función misional.

Proceso	**Impacto financiero**	**Impacto operacional**		**Impacto global**
		Oportunidad (cumplir en los plazos)	Satisfacción (cumplir el alcance)	
HEMI	No aplica, HEMI no soporta obligaciones financieras en el IPES	(1) Impacto moderado. La entidad registra sus compromisos y tareas en el sistema HEMI, pero como el procesamiento se puede hacer fuera de línea con lo cual el cumplimiento de las obligaciones en cuanto a función misional se puede cumplir en caso de falla de HEMI	(3) Impacto Alto La entidad cumple con sus funciones de manera continua aún sin acceso a HEMI. A nivel de entes de control y partes interesadas en el cumplimiento de la función de IPES se necesita la entrega de información consistente por lo que el uso de HEMI en fundamental para presentar informes unificados de operación de la Entidad	(4)
(SIAFI) OPGET	(5) Impacto severo No es admisible ninguna clase de pérdida económica	(5) impacto severo No se cumple en compromiso en ningún plazo. Es decir no se hace el trabajo	(3) impacto alto Se cumple en forma parcial la misión institucional	13
(SIAFI) PREDIS	(5) No es admisible ninguna clase de pérdida económica	(5) impacto severo No se cumple en compromiso en ningún plazo. Es decir no se hace el trabajo	(5) impacto severo No se puede cumplir la misión institucional	15

Proceso	Impacto financiero	Impacto operacional		Impacto global
		Oportunidad (cumplir en los plazos)	Satisfacción (cumplir el alcance)	
Almacenamiento compartido	No aplica el almacenamiento compartido no soporta operaciones financieras	(5) impacto severo La disponibilidad de la información para toma de decisiones y presentación de informes es fundamental para el cumplimiento de la misión, cuando no existe acceso al drive compartido se debe recurrir a los archivos locales almacenados en las estaciones de trabajo	(5) impacto severo Los usuarios del servicio depende de su información almacenada para la realización de sus trabajos, pero puede operar con las replicas de información que almacenan en sus estaciones de trabajo local	10
Correo electrónico	No aplica el almacenamiento compartido no soporta operaciones financieras	(5) impacto severo La interrupción de los servicios de correo electrónico implica la ausencia de comunicación entre actividades y procesos de la entidad	(3) Impacto alto La comunicación con las partes interesadas se demora y se pueden presentar no cumplimientos en compromisos de entrega de información.	8

3.5 Identificación de tiempos y objetivos de recuperación

MTD: En la columna MTD (Máximo tiempo tolerable de interrupción) se registra el tiempo máximo que se puede tolerar si servicio
RTO: Es el tiempo máximo disponible para la restauración de los sistemas que soportan el servicio antes de que se presenten impactos inaceptables para el IPES, el RTO no puede ser mayor al MTD.
RPO: Es la periodicidad del backup que se realiza al servicio

Nombre del Proceso	MTD Máximo tiempo tolerable de interrupción	RTO Tiempo objetivo de recuperación	RPO Punto Objetivo de recuperación
HEMI	1 día	2 horas	Diario
SIAFI	Hasta 1 día cuando no se está en fecha crítica o de entrega de información En fechas críticas de entrega de información el sistema el MTD no debe superar las 2 horas	1 día	Diario
Almacenamiento compartido	Hasta 1 día	1 día	Diario
Correo electrónico	Hasta 1 día	2 horas	Diario

3.6 Recursos tecnológicos por servicio

A continuación se detallan los recursos tecnológicos que soportan los servicios identificados como críticos.

Servidores y Maquinas virtuales

SRV2K8IPES01

- SRV2K8IPES07: E:\AD\ActiveDirectory
- SRV2K8IPES16: G:\CORREO\CORREO
- SRV2K8IPES15: G:\OCS
- SRV2K8IPES10: G:\PRINT2\PRINT2
- SRV2K8IPES13: G:\SQLSERVER
- Zimbra: E:\ZIMBRAFIN

SRV2K8IPES02

- SRV2K8IPES11: G:\BDAD2
- SRV2K8IPES03: G:\HEMI\HEMI6
- SRV2K8IPES14: E:\HEMI\HEMIPRUEBAS
- SRV2K8IPES05: E:\INTRAPORTAL
- SRV2K8IPES04: G:\PRINT3

Virtualización de los servidores

SERVIDOR	SERVICIOS
SERVIDOR 1 192.168.0.17 5 máquinas virtuales	**Servidor 1.1 192.168.0.20** - Consola de Administración Kaspersky - Sistema de Información administrativo y financiero SIAFI**(replica contingencia)** - Unidad compartida para SIAFI (T) **(replica aplicativo contingencia)** - Unidad compartida del Sistema Integrado de Gestión (X) - Servidor de impresoras **(replica contingencia)** - Administrador de licencia de Autocad **Servidor 1.2 (HEMI) 192.168.0.14** - Servidor web - Internet Information Services (**IIS)** - HEMI - HEMIPRUEBAS - REPORTES **Servidor 1.3 (Portal) 192.168.0.19** - Servidor Apache - Servidor MySQLMyadmin - Portal IPES - Navicat **Servidor 1.4 192.168.0.6 (directorio activo secundario y nombres de dominio secundario)** - Active Directory (Backup) - DNS (Backup) - Terminal server (pruebas) **Servidor 1.5 (Hemi pruebas) 192.168.0.24** - Servidor web - Internet InformationServices (IIS) - HEMI
SERVIDOR 2 **5 máquinas virtuales** **192.168.0.18**	- Servidor 2.1 (directorio activo primario y nombres de dominio primario) 192.168.0.15 - Directorio Activo (Principal) - DNS (Principal) - Servidor 2.2 (Correo Institucional) 192.168.0.13 - Zimbra (servidor de correo) - Servidor 2.3 (Aplicativo SIAFI) 192.168.0.16 - Aplicativo SIAFI - Administrador impresión - Servidor 2.4 (Motor SQL) 192.168.0.23

	- SQL server 2005 - Bases HEMI, Cartera, Digiturno, PIVOC - **Servidor 2.5 (ZIMBRA 2) 192.168.0.x**

DISTRIBUCIÓN GENERAL DE SERVICIOS Y SERVIDORES:

SERVIDOR	SERVICIOS
SERVIDOR 1	-Router cisco
SERVIDOR 2 192.168.0.11	-Proxy - PFSENSE
SERVIDOR 3 192.168.0.12	-File server (Servidor de archivos en un 90% - mybook unidad f) - Motor de BD SQL Server 2005(Cartera, Digiturno, Hemi, Hemipruebas,escalera,PIVOC 3.0,Web IPes, reportingservices) - Sistema de Información Pivoc - Sistema de Información Cartera - DHCP - WSUS - Carpetas compartidas de capacitación, contabilidad, emprendimiento, ACI, presupuesto. - Administrador Data Protector Express HP
SERVIDOR 4 192.168.0.63	- Servidor Tom Cat de nómina SIAFI - Conexión remota con proveedores de SIAFI
SERVIDOR 5 192.168.2.15	- Misión Bogotá - Directorio Activo - DNS - Fileserver - Impresoras - DHCP
SERVIDOR 6 192.168.0.9 win2003	- Planta Telefónica -One Box
SERVIDOR 7 192.168.0.10	- Planta Telefónica - Linux
SERVIDOR 8 192.168.2.11	- Proxy - PFSENSE Firewall - Snort (IPS) - Filtrado de contenidos (SquidGuard)
SERVIDOR 9 192.168.0.3	- NAS -Fileserver - Unidades U - Videos y software - SIAFI - Administrador Data Protector Express HP - Discos iscii presentaron 17 -18
SERVIDOR 10 192.168.0.7	- UTM - Firewall - Antibot - Antivirus - URL filtering - DLP - IPS - VPN - Antispam - Mobile Access

	- QoS - NAT - Identity awareness - Aplication control - ISP Redundacy -Proxy
SERVIDOR 11 192.168.0.28	- Intranet - Linux redhat - Lampp - PHP - Apache -Mysql -Myadmin - GLPI
SERVIDOR 12 10.232.30.31	-Alfresco

3.7 Prioridades de recuperación

La siguiente tabla registra las prioridades de recuperación de las funcionalidades del IPES en caso de un incidente mayor, los resultados se baNAS en los impactos financieros y operacionales derivados de una falla en los servicios analizados

Componente	Descripción técnica
SIAFI	Sistema de información Financiero administrativo. En caso de falla mayor en los sistemas de información, la prioridad es recuperar este sistema debido a que su falla implica NASciones para la entidad.
Almacenamiento compartido	Segunda prioridad de recuperación, la no disponibilidad de la información afecta directamente la función misional de la Entidad.
Correo electrónico	Debido a la dependencia de los servicios de correo para la comunicación misional el servicio de correo debe ser recuperado con la misma prioridad que el almacenamiento compartido
HEMI	La naturaleza del IPES implica el cumplimiento de estrategias que no son actividades de realización inmediata, el sistema de información HEMI permite el registro de las acciones para el cumplimiento de la Misión. En caso de fallas simultáneas en varios servicios críticos es prioritario recuperar los sistemas financieros, sistemas de almacenamiento de información, sistema de comunicación vía correo y finalmente el sistema HEMI que dada su infraestructura redundante tiene capacidad para recuperación inmediata.

3.8 Escenarios de riesgo

La activación del plan de contingencia debe considerar los efectos que para los procesos misionales de la entidad tendrían la ocurrencia de riesgos cuyas consecuencias sean: Pérdida de disponibilidad en la prestación del servicio o pérdida de la integridad de la información que ponga en riesgo la capacidad operacional de la entidad para cumplir su función misional. Las combinaciones de amenazas (causas) y consecuencias (perdida de disponibilidad e integridad) generan los escenarios de riesgo bajo los cuales el comité de contingencia debe determinar si se autoriza o no la activación del plan de contingencia.

Dentro del análisis de riesgos de seguridad de la información se pueden encontrar información detallada sobre las estrategias para mitigar las vulnerabilidades y

controles que se pueden aplicar para reducir el impacto o probabilidad de ocurrencia de los riesgos que activarían el plan de contingencia.
Todos los incidentes de seguridad de la información deben ser manejados inicialmente por el procedimiento de gestión de incidentes de seguridad de la información. En ese procedimiento se definen los parámetros iníciales para la atención de los incidentes.
En los casos en los que el incidente de seguridad ya no puede manejarse por los procedimientos normales de la mesa de ayuda, se debe proceder al escalamiento del incidente al coordinador del plan de contingencia quién debe seguir los pasos de notificación y evaluación del incidente para tramitar la autorización de activación del plan de contingencia ante la persona o personas responsables de esta acción.

3.8.1 Escenarios de riesgo generales

A partir de los resultados del análisis de impacto al negocio, se describen a continuación los escenarios de riesgos generales que pueden afectar al sistema y cuyas consecuencias generarían perdida de disponibilidad de servicios con la consecuente necesidad de activación del plan de contingencia.

- Cuando se presenta una falla en la energía comercial del edificio y las baterías que soportan la UPS se descargan, y ante el hecho de que no hay una planta eléctrica, los equipos que soportan los sistemas de información del IPES fallan.
- Debido a una ausencia o falta de mantenimiento en los equipos de energía o en los equipos activos de comunicaciones, los equipos dentro de los datacenter que soportan los sistemas de información del IPES pueden fallar.
- Debido a una ausencia o falta de mantenimiento en los servidores, los sistemas de información del IPES pueden funcionar mal o fallar.
- Cuando no se cuenta con sistemas centralizados de monitoreo y alarma, se presentan fallas en los equipos o en los servicios informáticos del IPES, por lo que no se tiene una respuesta rápida a los eventos y se presentan pérdidas en la efectividad para el cumplimiento de las funciones de la organización.

3.8.2 Escenarios de riesgo asociados a pérdida de disponibilidad

Dentro de las amenazas estudiadas en el análisis de riesgos del sistema de gestión de seguridad de la información del IPES que podrían generar perdida de disponibilidad de los servicios, se tienen los siguientes escenarios de riesgos:

- Cuando no se realizan análisis periódicos de riesgos o no están en constante supervisión y actualización las políticas de seguridad de los equipos de seguridad perimetral, se pueden tener ataques por denegación de servicios
- Debido a una ausencia o falta de mantenimiento en los servidores y en las bases de datos de los sistemas de información del IPES, se puede presentar un mal funcionamiento en la bases de datos.
- Se puede presentar robo de información debido a un acceso no autorizado a una aplicación, ya que no existe un procedimiento formal para desvinculación

o eliminación de usuarios.

- Debido a la humedad, polución y otros factores, y ante la ausencia de espacios físicos adecuados para almacenamiento de documentos, se pueden perder o destruir registros o documentos importantes para la entidad.
- Debido al uso de tecnología ineficiente para gestión de archivos, y la no aplicación de procedimientos de gestión documental, se puede presentar daño o pérdida de registros y documentos.
- Puede haber un abuso de derechos o accesos no autorizados, debido a una inadecuada asignación de permisos en la información que se encuentra compartida con lo que se perdería la integridad, confidencialidad y disponibilidad de la información.
- Debido a que no se tiene una práctica adecuada para el backup de los buzones de correo, se pueden perder los datos de los usuarios.

3.8.3 Escenarios de riesgo asociados a la pérdida de integridad

Las amenazas asociadas a la pérdida de integridad de los sistemas de información pueden derivar en los siguientes escenarios de riesgos:

- Se puede presentar un tratamiento deficiente de la información por falta de disponibilidad de personal debido a la alta rotación de funcionarios.
- Puede haber un abuso de derechos o accesos no autorizados, debido a una inadecuada asignación de permisos en la información que se encuentra compartida con lo que se perdería la integridad, confidencialidad y disponibilidad de la información.
- Hay un error en el uso de los sistemas y los procesos debido a un procedimiento inadecuado de inducción del personal, con lo que se puede presentar una manipulación o procesamiento inadecuado de la información, lo que puede derivar en una corrupción de datos no intencional.
- Debido a que no se tiene cifrado para el tráfico de datos, se puede presentar un cambio fraudulento de datos, lo que puede causar una pérdida de la integridad de los datos.

4 Controles preventivos

En esta sección e describirán los mecanismos de control que se tienen implementados en el IPES para mitigar los impactos de incidentes que afecten la disponibilidad de los servicios de información y tecnología identificados como críticos.

4.1 Capacidad de la UPS.

El IPES cuenta con UPS, una para los servidores y otra para los computadores personales conectados al circuito regulado del cableado estructurado. En caso de una falla de energía, los UPS suministraran potencia por un período de tiempo limitado por la autonomía de las UPS dependiendo de la capacidad de las baterías. En caso de un corte de energía mayor al 30% del tiempo de autonomía real del UPS de servidores y equipos activos deberían iniciarse las labores de bajado de servicios y apagado sincronizado, labor que en lo posible debe hacerse de forma automática ya que el corte se puede presentar en horario donde no hay personal de atención de equipos. En el caso de los Computadores personales el personal del IPES debería iniciar de inmediato el proceso de apagado de los equipos.

De acuerdo a lo anterior, en los mantenimientos preventivos de las UPS, deben hacerse pruebas de funcionamiento de UPS y medición de autonomía de baterías para conocer la capacidad real de tiempo con que se cuenta en caso de falla de energía comercial. Para las baterías las pruebas mínimas de autonomía deben realizarse por lo menos una vez por semestre.

Otra de las tareas a ejecutar es la de realizar un estudio de cargas teórico y real de los equipos que son alimentados por las UPS y actualizarlo de acuerdo a los cambios como instalación de nuevos equipos, retiro de equipos o potenciación de equipos o cambio de partes, esto con el fin de mantener actualizado los requerimientos de potencia de equipos informáticos.

4.2 Capacidad de los sistemas de refrigeración.

El Datacenter del IPES, cuenta con un aire acondicionado. En la actualidad la sensación térmica es suficiente para el correcto funcionamiento de los equipos.

Considerando que a la fecha no se cuenta con registros de mediciones de temperatura y humedad del aire por medio de termómetros e higrómetros que permitan alarmar el sistema y dar orden de apagado de servidores en caso que se presenten temperaturas perjudiciales para los equipos. Es necesario realizar verificaciones diarias de las condiciones ambientales del data center.

De acuerdo a lo anterior se debe formular un proyecto para la instalación equipos medidores de temperatura y humedad integrados al monitoreo del sistema, así mismo se debe hacer un estudio de cargas de temperaturas de equipos y mantenerlo actualizado de acuerdo a la instalación o retiro de equipos.

4.3 Sistema de extinción de incendio

El IPES no cuenta con un sistema de extinción de incendios. En la actualidad solo se cuenta con extintores manuales los cuales son de utilidad solo en el momento que haya personal en caso de que se presente un incidente de fuego y no cuando están desatendidos como es en las noches. Es necesario realizar verificaciones periódicas de las condiciones ambientales del data center y formular un proyecto de implementación de un sistema de protección contra incendios en el Datacenter.
Por lo anterior se debe implementar un sistema de extinción de incendio automático con supervisión integrada al sistema de monitoreo general, con un programa de mantenimiento periódico.

4.4 Sistemas de monitoreo de capacidad de servidor.

En la actualidad el IPES no cuenta con sistemas de gestión de monitoreo centralizado de capacidad de los servidores que permitan medir el uso de CPU, Memoria y Disco Duro. Las herramientas de monitoreo de los recursos de tecnología (incluidas variables fundamentales del servidor y ancho de banda de canales), son necesarias para establecer comportamientos de los recursos de tecnología y predecir incidentes. El Monitoreo de la capacidad de servidores es una medida preventiva frente a incidentes de seguridad de la información.

4.5 Sistemas de monitoreo de aplicación

En la actualidad no se cuenta con herramientas centralizadas de monitoreo de las aplicaciones. Una de las oportunidades de mejora para el plan de contingencia incluye la implantación de herramientas de supervisión que permitan identificar comportamientos anómalos en las aplicaciones y así prevenir incidentes

4.6 Sistemas de monitoreo de base de datos

En la actualidad no se cuenta con herramientas centralizadas de monitoreo base de datos. Una de las oportunidades de mejora para el plan de contingencia incluye la implantación de herramientas de supervisión de bases de datos que permitan identificar comportamientos anómalos y así prevenir incidentes. La segunda estrategia que es prioritaria para mejorar los tiempos de recuperación es fortalecer las capacidades internas para la administración de bases de datos (DBA) que permitan realizar actividades de afinamiento, supervisión y recuperación de bases de datos.

4.7 Sistemas de almacenamiento de copias de respaldo

La infraestructura actual de respaldo de los sistemas misionales del IPES se fundamenta en el uso de una NAS. El esquema de respaldo debe adoptar esquemas formales de pruebas de restauración de información y su aplicabilidad en caso de contingencia.

4.8 Sistema de almacenamiento de copia de respaldo en sitio remoto

Se tiene un servicio para guardar los respaldos fuera de las instalaciones del IPES, es necesario mantener la continuidad del contrato para mitigar los riesgos de fallas mayores en la infraestructura física y tecnológica de la sede principal que obliguen al uso de las copias de información almacenada en sitio remoto..

4.9 Periodicidad del respaldo de datos

De acuerdo con el resultado del BIA, la periodicidad del respaldo de datos para los diferentes sistemas de información críticos del IPES debería mantenerse en los niveles actuales:

Nombre del Proceso	**RPO** Punto Objetivo de recuperación
HEMI	Diario
SIAFI	Diario
Almacenamiento compartido	Diario
Correo electrónico	Diario

Aunque el análisis de las funciones misionales indica que los servicios de réplica de información almacenada en las estaciones de trabajo y la NAS es una medida efectiva en caso de incidentes en las estaciones de trabajo o incluso en la misma NAS, es necesario verificar periódicamente las políticas sobre el uso del recurso compartido de almacenamiento para evitar consumos de recursos de almacenamiento con archivos que no formen parte de la función misional del IPES (música, vídeos, presentaciones que no son institucionales y demás información personal no autorizada formalmente)

4.10 Sistemas de protección de la seguridad de la información

Los resultados del análisis de brecha del sistema de gestión de seguridad de la información del IPES indican que los puntos de vulnerabilidad más delicados de los sistemas son:

- Ausencia de procesos formales de toma de conciencia en seguridad de la información: Para mitigar incidentes generados por amenazas externas como denegación de servicio e infiltración es necesario promover la cultura de uso seguro de los sistemas de información.
- Procedimiento de control de cambios al software: Para fortalecer el control de cambios al software y reducir la posibilidad de errores en la actualización de funcionalidades se debe seguir un procedimiento de control de cambios de software.
- Almacenamiento de código de fuente: Siguiendo las recomendaciones de la norma de gestión de seguridad de la información, el código fuente de las aplicaciones de misión crítica debe ser respaldado siguiendo las buenas prácticas de la industria.

- Controles de auditoría: Todas las aplicaciones misionales deben ser sometidas al menos una vez al año a auditorias de sistemas y auditorias de seguridad de la información siguiendo las recomendaciones del sistema de gestión de seguridad de la información y el área de control interno.
- Cuando falla un sistema de información o un servicio informático, y no se tiene un sistema centralizado de monitoreo que alerte a una persona de contacto de la falla, puede pasar bastante tiempo hasta que la persona que administra el servicio se entere de la falla y la repare.
- Se presente un evento o incidente de seguridad de la información y no existe un procedimiento formal para comunicarlo o reportarlo, puede pasar que se acumulen eventos que degraden la seguridad de la información de la entidad.
- Si no se tiene un procedimiento documentado de control de cambios y se tenga que hacer un mantenimiento o un cambio que involucre algún activo de seguridad de la información, puede pasar que la actividad no culmine con los resultados esperados y pueda comprometer la seguridad de otros activos.
- Por un daño en el disco duro o un malware que contamino un PC, el usuario puede perder los datos de su buzón de correo.
- Se puede presentar robo de información debido a un acceso no autorizado a una aplicación, ya que no existe un procedimiento formal para desvinculación o eliminación de usuarios.

La implementación de las acciones de mitigación de estas vulnerabilidades reduciría la posibilidad de ocurrencia de incidentes de seguridad de la información que impliquen la activación del plan de contingencia.

5 Definición de las estrategias de contingencia

5.1 Uso de site alterno

Escenario: No se puede usar la sede principal del IPES y el centro de cómputo no es apto para correr las aplicaciones.

Alternativa: Centro alterno en instalaciones del IPES diferente a la sede principal

En la actualidad el IPES no cuenta con un SITE alterno para restablecer los sistemas de información en caso de falla total del centro de cómputo de la sede principal. Debido a que el BIA identificó que los tiempos máximos de restablecimiento de los servicios en fecha crítica son de 2 días la estrategia de contingencia en caso de falla del centro de cómputo principal es:

Nombre del servicio	Estrategia de Site Alterno
Sistema de información HEMI	Uso de sede Barichara para instalar un servidor de contingencia para que los usuarios responsables de actualizar información directamente en el servidor, las conexiones desde Internet en este esquema de contingencia no son viables.
SIAFI	El establecimiento de un acuerdo con la Secretaria de Hacienda para desplazar a dos funcionarios responsables de registrar la información vital de SIAFI directamente en la secretaria de Hacienda. La estrategia se activaría solo en fallas que se presenten en fechas críticas de entrega de información
Almacenamiento compartido	Aunque es factible la reinstalación del servidor en donde se almacenaban los datos del Drive U antes de la instalación de la NAS, los usuarios cuentan con copias de su datos en los computadores personales, la relación de Beneficio/Complejidad de la estrategia no viabiliza el plan
Correo electrónico	Aunque es factible instalar un servidor de correo en sede alterna, los usuarios cuentan con sus buzones de correo en los computadores personales, la relación de Beneficio/Complejidad de la estrategia no viabiliza el plan y es más factible esperar al restablecimiento de los servicios

5.1.1 Centro alterno en acuerdo con otra entidad

Esta estrategia se aplicaría en caso de que el IPES establezca acuerdo para reubicación de sus sistemas de información en el centro de cómputo de otra entidad, la estrategia depende de los acuerdos establecidos. Para los efectos del presente plan de contingencia no se cuenta con acuerdos con otra entidad.

5.1.2 Centro alterno contratado

Esta estrategia se aplicaría en caso de que el IPES contara con contrato para uso de site alterno con un proveedor de servicios de tecnología. Para los efectos del presente plan de contingencia no se cuenta con acuerdos con proveedor externo.

5.1.3 Identificación de equipos

Los siguientes equipos son esenciales para la operación del plan de contingencia. Los equipos se aprovisionan de acuerdo con la evaluación que se realice durante la fase de evaluación y activación del plan de contingencia.

- Servidores
- Unidades de respaldo/restauración de cintas
- Switches
- Fuentes de SIAFI
- Fuentes de sistema operacional
- Copias de respaldo de imágenes de los servidores virtuales
- Fuentes de motor de base de datos
- Última copia de respaldo de base de datos de SIAFI
- Última copia de respaldo de base de datos de HEMI
- Estaciones de trabajo de usuario final

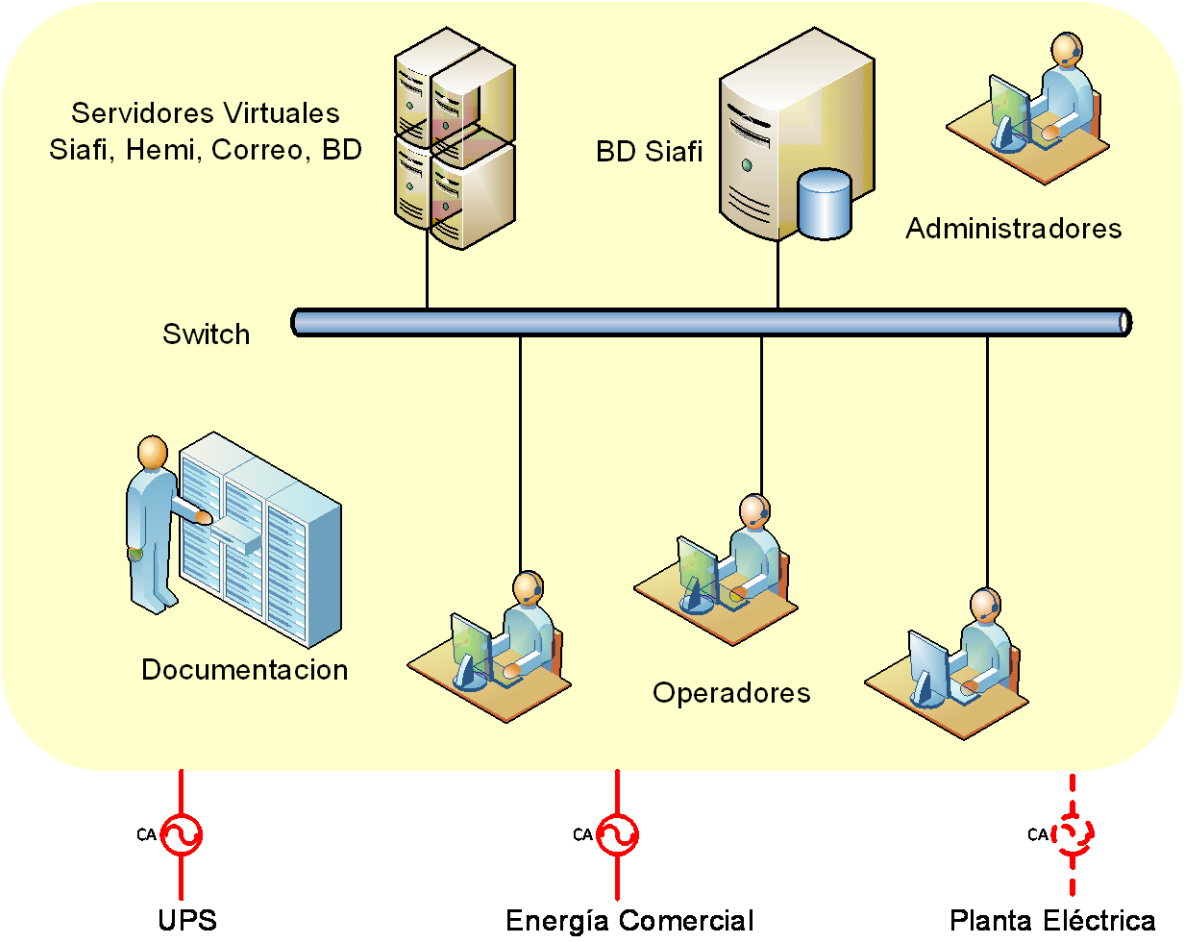
5.1.4 Acuerdos con proveedores

Los siguientes acuerdos para apoyo son esenciales para la correcta operación del plan de contingencia.

- Soporte de hardware de servidores
- Soporte de sistema operacional de servidor
- Soporte de aplicación SIAFI
- Soporte de hardware y software de Switches
- Soporte de hardware y software de NAS
- Acuerdos para cargue de datos en secretaria de hacienda
- Acuerdos con proveedor de acceso a Internet (ETB)

5.1.5 Arquitectura de contingencia

La siguiente gráfica muestra la arquitectura básica de contingencia que se debe implementar para brindar continuidad a los servicios de misión crítica del IPES a un grupo seleccionado y esencial de líderes de los procesos misionales.


Servidores Virtuales
Siafi, Hemi, Correo, BD
BD Siafi
Administradores
Switch
Documentacion
Operadores
CA
UPS
CA
Energía Comercial
CA
Planta Eléctrica

6 Fases del plan de contingencia

6.1 Fase de notificación y activación

A continuación se relacionan las fechas críticas dentro del año en las que los procesos misionales del IPES requieren disponibilidad de los sistemas de información. Durante esas fechas se debe reforzar la aplicación de los controles preventivos, verificación del correcto funcionamiento de aplicaciones e infraestructura de Información y Tecnología. Uno de los criterios fundamentales para activar el plan de contingencia es la ocurrencia de incidentes durante esas fechas.

Sistema o Servicio de Información y tecnología	Fechas críticas dentro del año
HEMI	[Por definir]
SIAFI	7 hábiles antes del fin de cada mes Todo el mes de diciembre
Almacenamiento compartido	Diario
Correo electrónico	Diario

6.2 Identificación de incidentes

El grupo de sistemas del IPES debe seguir los procedimientos de gestión de incidentes de tecnología y gestión de incidentes de seguridad. En el caso del procedimiento de gestión de incidentes cuando se realice un escalamiento de segundo nivel al grupo de especialistas y no se obtenga solución al incidente se debe iniciar un proceso de evaluación de activación del plan de contingencia.

La evaluación de la necesidad de activar el plan de contingencia estará a cargo del responsable de iniciar el plan de contingencia que haya nombrado el comité de contingencia, en este caso el Jefe de Sistemas. En la sección Criterios de activación del plan de contingencia se describen los parámetros mínimos a evaluar para determinar que se debería activar el plan de contingencia.

En el caso de los incidentes de seguridad de la información, la evaluación de la necesidad de activar el plan de contingencia se debe realizar tan pronto como se identifica la ocurrencia de un incidente de seguridad de la información que genera no disponibilidad de servicios de misión crítica. El procedimiento de gestión de incidentes de seguridad de la información establece los mecanismos para iniciar las actividades de recuperación y restablecimiento de servicios.

6.3 Criterios para activación del plan de contingencia

El responsable de activación del plan de contingencia debe considerar los siguientes parámetros para ordenar la activación del plan de contingencia.

En caso de que algunas de las siguientes condiciones se presente, se debería activar el plan de contingencia sobre el sistema afectado.

6.3.1 Daños en componentes de tecnología

Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Evento	Descripción
Indisponibilidad total de componentes de tecnología que soportan las aplicaciones críticas	El diagnóstico del procedimiento de gestión de incidentes o el procedimiento de gestión de incidentes de seguridad de la información demuestra un daño total o parcial físico en uno o varios de los componentes de tecnología de información y comunicaciones que soportan uno o varios de los sistemas de información críticos y que impide la prestación de servicios misionales.

Criticidad del sistema afectado

Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Evento	Descripción
Ocurrencia de incidente sobre un sistema de información crítico en fecha crítica	Cuando se identifique un incidente de seguridad de la información o incidente de tecnología que afecta un sistema de información crítico y además el incidente se presenta en una de las fechas críticas para el sistema.

Duración del incidente

Se activa el plan de contingencia cuando se presenten eventos en los componentes de tecnología si:

Evento	Descripción
La duración del incidente supera el tiempo disponible para restablecer los servicios y se entra en fecha crítica de operación de los servicios.	Cuando se esté atendiendo un incidente de tecnología o de seguridad de la información y el tiempo empleado para resolver el incidente empiece a consumir tiempo de las fechas críticas de operación de los sistemas críticos

6.4 Procedimientos de notificación

Para efectos de notificación de la ocurrencia de un incidente de tecnología o un incidente de seguridad de la información, se deben seguir los procedimientos respectivos. Como resultado de los procedimientos antes mencionados se generan reportes que deben ser remitidos al coordinador del plan de contingencia para que se diligencie el formato de reporte de incidente y valoración de incidente. A continuación se relacionan los mecanismos y árbol de notificación.

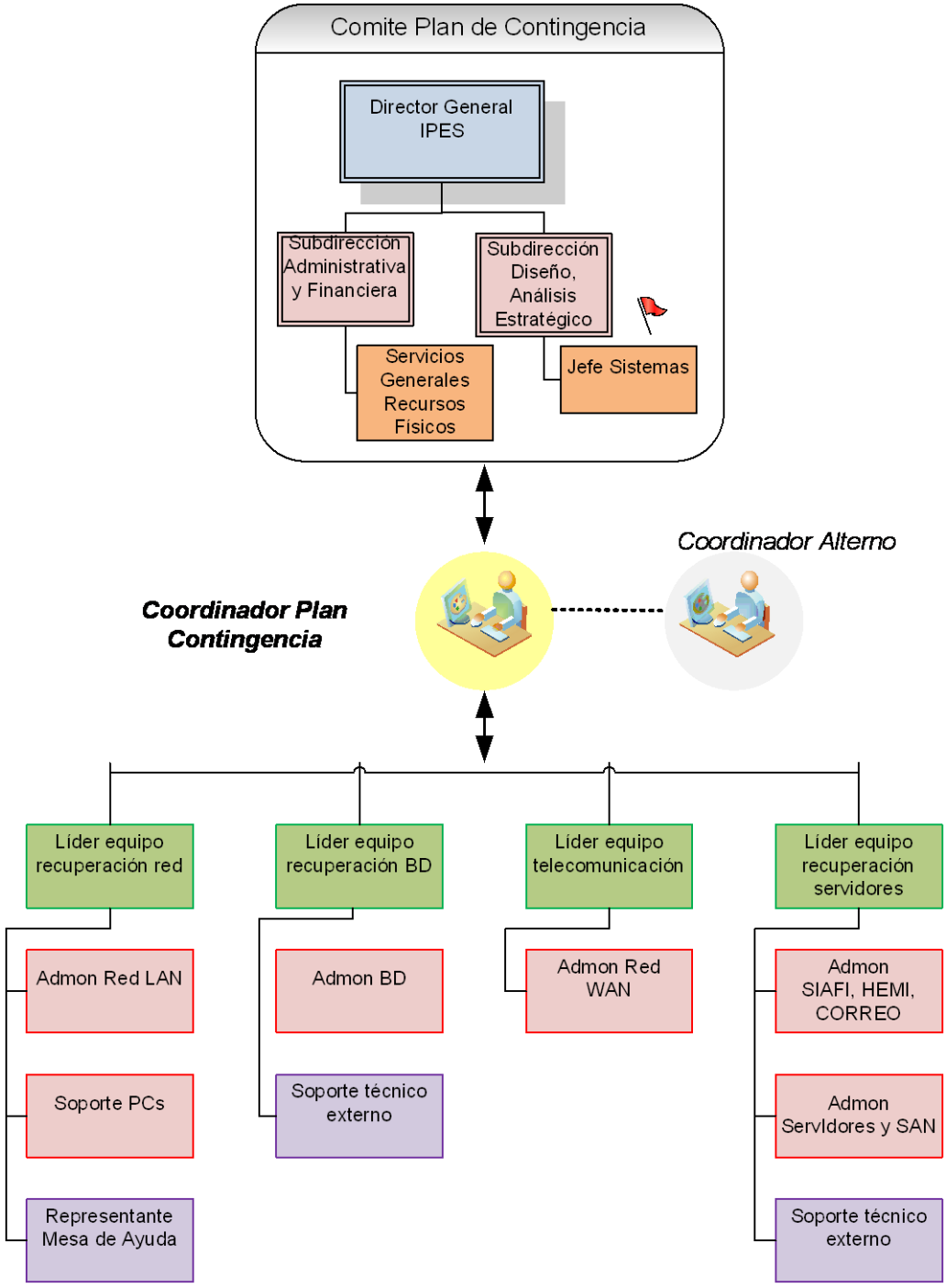


Ilustración 1 Árbol de notificación

6.4.1 Notificación telefónica

La primera notificación del incidente se debe realizar vía teléfono en caso de que no se pueda hacer personalmente. A continuación se tiene la lista de contactos para notificación

Contacto	Celular	Dirección casa	Teléfono Casa	Debe realizar notificación a:
Jefe de sistemas				Director IPES y Comité de plan de contingencia
Administrador LAN				Jefe de sistemas IPES (coordinador de plan de contingencia)
Administradores sistemas de información				Jefe de sistemas IPES (coordinador de plan de contingencia)
Administrados de sistema de Almacenamiento y Servidores				Jefe de sistemas IPES (coordinador de plan de contingencia)

6.4.2 Notificación vía correo electrónico

Una vez se complete la notificación telefónica y si existe servicio de correo electrónico, se debe proceder a remitir el formato de reporte y valoración de incidente al personal que forma parte del plan de contingencia.

Contacto	Email	Debe continuar notificación con:
Jefe de sistemas		Director IPES y Comité de plan de contingencia
Administrador LAN		Jefe de sistemas IPES (coordinador de plan de contingencia)
Administradores sistemas de información		Jefe de sistemas IPES (coordinador de plan de contingencia)
Administrados de sistema de Almacenamiento y Servidores		Jefe de sistemas IPES (coordinador de plan de contingencia)

6.4.3 Notificación por mensaje de texto

Considerando que puede no existir el servicio de correo electrónico o los puntos de contacto responsables de actividades del plan de contingencia no son ubicados por correo electrónico, se debe continuar con la notificación vía mensaje SMS de la

existencia de un incidente que requiere valoración de activación del plan de contingencia. El árbol de notificaciones a seguir es:

Contacto	Celular	Pin Blackberry (en caso de existir)
Jefe de sistemas		
Administrador LAN		
Administradores sistemas de información		
Administrados de sistema de Almacenamiento y Servidores		

6.5 Fase de recuperación

La fase de recuperación de servicios en la infraestructura de contingencia depende del resultado de la valoración del incidente por parte del grupo de contingencia. A continuación se detalla una secuencia de recuperación que supone una pérdida total de disponibilidad de servicios de infraestructura. El coordinador del plan de contingencia y los líderes de infraestructura deben valorar la extensión del incidente para identificar que grupos de actividades se deben aplicar para recuperar los servicios de misión crítica en situación de contingencia.

6.5.1 Estrategias de recuperación

Recuperación en sitio alterno

Si el incidente afecta el centro de cómputo principal pero es viable seguir trabajando desde la sede misma sede se debe proceder reubicar los servidores que sean factibles de mover a un sitio predefinido dentro de la sede principal de IPES, las prioridad de recuperación en estos casos es el sistema de almacenamiento, la operación de SIAFI debe trasladarse a las instalaciones de la Secretaria de Hacienda mediante el desplazamiento de los funcionarios responsables de las funciones críticas de SIAFI, los archivos vitales y los certificados digitales asignados al IPES.

Los servicios de Correo y HEMI serán las prioridades subsecuentes y su restauración en sitio alterno dentro del IPES dependerá de la disponibilidad de energía eléctrica y espacio físico.

Si el incidente afecta todo el edificio principal del IPES es necesario definir un plan de recuperación ante desastres.[2]

Aprovisionamiento de servicios de energía
Si el incidente afecta el suministro de energía eléctrica del centro de computo, y ha sido necesaria la activación del plan de contingencia dentro del edificio del IPES se debe hace uso de los servicios de la UPS mientras que la afectación no ponga en riesgo la operación de los equipos y sea necesario apagar las máquinas y esperar al retorno del fluido eléctrico.

.

Aprovisionamiento de servicios de conectividad LAN
En los casos en los que el incidente afecta solo los equipos de conectividad de los servidores:

- Switch para conexión de servidores o switch de core/distribución:

  Se debe verificar el resultado de la valoración de incidente y si el resultado indica que no están disponibles los switches, la solución de contingencia implica reemplazar switch afectado por un switch de contingencia que debe ser configurado con una copia de respaldo de la configuración del switch que falló en el caso de ser de iguales características.

- Firewall

  La no disponibilidad del firewall impide la conexión entre el sistema SIAFI del IPES y la secretaria de hacienda. En la eventualidad en que falle el firewall se debe proceder a generar los datos misionales críticos de SIAFI, grabar los datos o transacciones en un medio removible (esta operación implica apoyo del administrador de SIAFI para apoyar a los usuarios de los procesos misionales) y desplazarse físicamente a la sede de la secretaría de hacienda para cargar los datos. En el caso de acceso a las aplicaciones de registro de contratos como: contratos.gov.co, portal de contratación a la vista, el acceso se puede realizar mediante conexión inalámbrica con modem USB el cual se puede gestionar con ETB o mediante desplazamiento físico a un centro de servicios de acceso a Internet (centro interactivo de ETB) para cumplir las actividades.

Aprovisionamiento de servidor
Si el incidente implica falla de un servidor o servidores que soportan los procesos misionales críticos del IPES se debe informar a los responsables de los procesos misionales para que activen sus planes de continuidad de negocio en forma manual,

[2] El plan de recuperación ante desastres es un plan de alcance mayor al plan de contingencia. El plan de recuperación ante desastres cubre los planes de emergencia, los planes de continuidad de cada proceso misional y las actividades de contingencia.

mientras que se configura un nuevo servidor virtual y se restablece el servicio. Para el caso del sistema de información HEMI se cuenta con configuración redundante que mitiga la afectación en caso de falla de alguno de los servidores (Aplicación o Base de datos). En el caso del servidor SIAFI si el daño es físico es necesario el reemplazo del servidor por un equipo diferente lo que implicaría tiempos de restablecimiento de servicios superiores a los admitidos por el BIA y es necesario activar la contingencia mediante operación en puesto de trabajo gestionado con la secretaria de Hacienda Distrital.

Aprovisionamiento de sistema operacional

Cuando la valoración del incidente indique que se ha presentado una falla que implica la no disponibilidad total del sistema operacional del servidor o servidores que soportan las aplicaciones misionales se debe notificar a los dueños de los procesos misionales para que inicien sus procedimientos de continuidad de negocio en forma manual. Una vez notificada la necesidad de plan de continuidad manual se debe iniciar las tareas de restauración de las imágenes de los servidores virtuales afectados. En el caso de SIAFI se debe proceder a la reinstalación del sistema operacional y restablecimiento de la base de datos, situación que implicaría tiempos de restablecimiento de servicios superiores a los admitidos por el BIA y es necesario activar la contingencia mediante operación en puesto de trabajo gestionado con la secretaria de Hacienda Distrital .

Aprovisionamiento de canales de comunicaciones.

En la eventualidad en que falle el acceso con la secretaria de hacienda o con Internet, se puede activar el uso de un canal ADSL disponible con ETB, pero con capacidad limitada, la prioridad será el restablecimiento de servicios fundamentales sobre el sistema SIAFI. Ante falla de la contingencia con conexión ADSL, se debe proceder a generar los datos misionales críticos de SIAFI, grabar los datos o transacciones en un medio removible (esta operación implica apoyo del administrador de SIAFI para apoyar a los usuarios de los procesos misionales) y desplazarse físicamente a la sede de la secretaría de hacienda para cargar los datos.

En el caso de los servicios de correo electrónico las fallas en los canales de comunicación deben ser escalada al proveedor del acceso a Internet (ETB) , los tiempos máximos tolerables de no disponibilidad del servicio de acceso a Internet permiten que se haga uso del escalamiento al proveedor de servicios.

Aprovisionamiento de motor de base de datos

Cuando el resultado de la valoración del incidente indique que el binario del motor de la base de datos que soporta las aplicaciones misionales no está disponible y no puede ser recuperado por los procedimientos de gestión de incidentes o problemas,

se debe proceder a la recuperación del binario mediante reinstalación del motor de la base de datos y la recuperación de la copia más reciente del backup de base de datos. En el caso de SIAFI la actividad implica el apoyo del proveedor de servicios de soporte a la base de datos Oracle. En el caso de HEMI, el esquema de contingencia permite dar continuidad a los servicios en caso de falla de una de las maquinas mediante la activación de la máquina de contingencia. El tiempo de restablecimiento del servicio de HEMI está dentro de los tiempos del BIA.

Recuperación de backup más reciente de base de datos y aplicaciones
El restablecimiento del backup de base de datos se ordena cuando la valoración del incidente determina que se existe una falla en los datos de la base de datos que no se puede recuperar mediante los procedimientos de gestión de incidentes o problemas, o que el tiempo de recuperación de los datos mediante estos procedimientos excede los tiempos máximos tolerables de no disponibilidad definidos en el BIA.

6.5.2 Verificación de funcionamiento de aplicaciones críticas

Una vez aplicado el procedimiento de contingencia para el componente o componentes que fallen se debe seguir el protocolo de verificación de correcto funcionamiento de aplicaciones que se encuentra anexo a este plan.

6.5.3 Aprovisionamiento de puestos de trabajo para personal de misión crítica

En caso de requerirse estaciones de trabajo para los líderes de los procesos misionales críticos, la prioridad de selección de estaciones se ajustará la disponibilidad a los siguientes criterios:

- En primera instancia la estación de trabajo asignada al usuario.
- En segunda instancia una estación de trabajo portátil de la misma área del usuario líder.
- En tercera instancia una estación de trabajo portátil de otra área del IPES.
- En última instancia una estación de trabajo alquilada o aprovisionada por un proveedor externo.

6.5.4 Verificación de funcionamiento de puestos de trabajo

Una vez aplicado el procedimiento de contingencia para las estaciones de trabajo se debe seguir el protocolo de verificación de correcto funcionamiento de estaciones de trabajo que se encuentra anexo a este plan.

6.5.5 Aprovisionamiento de servicio de impresión de contingencia

En caso de activación del plan de contingencia, el aprovisionamiento de servicios de impresión tiene baja prioridad, bajo circunstancias de fuerza mayor que impliquen la generación de informes, el servicio se aprovisionará mediante impresoras

departamentales habilitadas específicamente para tal fin. La impresión se coordinará con el apoyo de los administradores de las aplicaciones y se prestará únicamente a los procesos misionales críticos.

6.5.6 Aprovisionamiento de servicio telefónico de contingencia

En caso de activación del plan de contingencia, el aprovisionamiento de servicios de telefonía tiene baja prioridad, los líderes de proceso crítico se comunicaran mediante medios como teléfono celular o correo electrónico si está disponible.

6.5.7 Procedimientos de recuperación

Los anexos del plan de contingencia detallan los siguientes procedimientos de restablecimiento de servicios en situación de contingencia:

- Aprovisionamiento de servicios de energía: uso de la UPS
- Aprovisionamiento de servicios de conectividad LAN: acceso a canal ADLS o en caso de afectación del switch de core la configuración de switch nuevo.
- Aprovisionamiento de sistema operacional: reinstalación de sistema operacional de servidores.
- Aprovisionamiento de motor de base de datos: Reinstalación de motores de base datos
- Recuperación de backup más reciente de base de datos y aplicaciones: restauración de copia de base de datos
- Aprovisionamiento de puestos de trabajo para personal de misión crítica: instalación de herramientas de trabajo esenciales para estación de trabajo

6.6 Escalamiento

Los siguientes puntos de contacto se utilizarán durante la ejecución del plan de contingencia para resolver situaciones específicas de reconfiguración de servicios o instalación de componentes de información y tecnología:

Componente	Proveedor/Contacto	Teléfono/E-mail/Móvil
Servidores		
Sistemas operacionales		
Motor de base de datos		
Aplicación SIAFI		
Aplicación HEMI		

Servicios de correo electrónico		
Sistema de almacenamiento NAS		
Canales de comunicación internet		
Switches		
Firewall		

6.7 Fase de restablecimiento de servicios

6.7.1 Criterios para finalizar las acciones de contingencia

De acuerdo con las estimaciones del análisis de impacto, lo sistemas críticos identificados podrían operar bajo la infraestructura de contingencia durante un plazo no superior a dos (2) semanas, pasado ese tiempo es necesario contar con la infraestructura completa de información y tecnología del IPES. Los pasos que se describen a continuación detallan las actividades que se deben ejecutar para retornar la operación normal de sistemas de información después de la activación del plan de contingencia. Las condiciones para el restablecimiento de los servicios a condición normal deben ser evaluadas por el responsable de contingencia del IPES, en este caso particular se trata del jefe de sistemas del IPES quien determinara la viabilidad para reactivar los sistemas de información después de la contingencia teniendo en consideración los siguientes aspectos:

Condiciones a considerar para finalizar el plan de contingencia y volver a la operación normal de servicios y sistemas de información
1) El incidente que obligó a la activación del plan de contingencia haya sido completamente controlado
2) Los sistemas de información afectados se haya restablecido exitosamente
3) El comité de contingencia apruebe el retorno a condiciones normales de operación

6.7.2 Ejecución de procesos concurrentes entre infraestructura de contingencia e infraestructura normal de tecnología

Debido a que la estrategia de contingencia definida para los sistemas de información de naturaleza crítica consiste en el uso de instalaciones propias del IPES y equipos de contingencia, la ejecución concurrente de dos versiones o dos instancias de los sistemas de información (el de contingencia y el oficial) se descarta por las siguientes consideraciones

1. Los tiempos de restablecimiento de los sistemas de información críticos a lo

sumó tomarían 1 días y el tiempo máximo MTD para los procesos es superior a 1 día , con lo cual el tiempo se cuenta con holgura para recuperación de servicios.

2. En caso de ejecutarse más de una copia de los sistemas de información críticos, el proceso de sincronización de las bases de datos y los registros entre los dos sistemas es más complejo que simplemente tomar un respaldo a las bases de datos del sistema de contingencia y restablecer los datos (se excluyen binarios y aplicaciones), en el sistema oficial
3. Bajo las condiciones más críticas de ausencia total de los sistemas de información, los sistemas que soportan los procesos misionales críticos tienen la posibilidad de operación manual, por lo que intentar correr simultáneamente dos versiones de los sistemas es innecesario y haría que los tiempos de restablecimiento a operación normal se prolonguen innecesariamente.

6.7.3 Restablecimiento de sistemas críticos

El proceso de restablecimiento de sistemas a condiciones normales se debe realizar siguiendo las etapas que se describen a continuación:

1 Confirmar con el coordinador de plan de contingencia que el incidente que afecto a los sistemas de información ha sido resuelto, que se ha corrido las pruebas de correcto funcionamiento de los sistemas de información y todo funciona de acuerdo con los parámetros de operación normal.

2 Informar al personal de contingencia que los sistemas de información ya fueron restablecidos y que la infraestructura de contingencia se va a deshabilitar, para realizar respaldo de los datos registrados en contingencia y restaurar los datos en los sistemas de información normales.

3 Cuando se confirme con el personal de contingencia que ha cerrado las operaciones o transacciones que realizaron en la plataforma de contingencia, se debe proceder a realizar un respaldo de datos y cerrar los sistemas de contingencia

Advertencia.

Para preservar la consistencia de bases de datos y registros, NO se deben tener simultáneamente activos a los usuarios el sistema de contingencia y el sistema normal.

El sistema normal, solamente se debe activar a todos los usuarios cuando se restaure el backup en los sistemas normales y los líderes de proceso hayan verificado que las transacciones que se aplicaron en contingencia están disponibles en el sistema normal.

Los sistemas de contingencia no se desmontan hasta que se corran las pruebas de correcto funcionamiento de los sistemas de información normales

6.7.4 Prueba de sistemas restablecidos

Pruebas previas al restablecimiento de backup

Los líderes de cada plataforma, debe ejecutar pruebas internas de correcto funcionamiento de los componentes de sistemas de información, las pruebas y sus resultados se deben registrar en los formatos anexos en este plan.

6.7.5 Pruebas de sistemas de información después de restaurar backup

Una vez que los lideres técnicos hayan verificado el correcto funcionamiento de los componentes de IT (servidor, bases de datos, comunicaciones), se debe proceder a restaurar el backup de datos del sistema de contingencia y llamar a los líderes de proceso para que corran pruebas de correcto funcionamiento de los sistemas de información (SIAFI, HEMI). Las pruebas y resultados se registran en los formatos de pruebas anexos a este plan.

Cuando los líderes de proceso, certifiquen que la aplicación y los datos funcionan de acuerdo con las condiciones normales de operación, se puede autorizar el apagado de la infraestructura de contingencia e iniciar los procesos de restablecimiento de servicios en condición normal.

6.7.6 Notificaciones

Cuando los sistemas de información críticos hayan sido restablecidos, se debe informar al responsable de contingencia (jefe de sistemas) para que se proceda a la notificación de fin de contingencia al comité de contingencia, quienes formalmente autorizaran a las diferentes áreas del IPES para que puedan volver a utilizar los sistemas de información. El esquema de notificación de usuarios se realizara empleando los medios de comunicación disponibles después de la contingencia: notificación personal, teléfono, mensajes SMS, Correo electrónico.

6.7.7 Limpieza y desmonte de la infraestructura de contingencia

Al finalizar la contingencia y cuando el responsable de contingencia, (jefe de sistemas) autorice el desmonte de la infraestructura de contingencia, se debe proceder a desmontar los equipos empleados en la contingencia. En caso de haber usado equipos en préstamo o convenio se procede a su embalaje y coordinación de devolución sus dueños. Todo equipo de contingencia debe ser inventariado para generar un acta de devolución. El acta de devolución debe describir estado en que se devuelven los equipos. Incluso en los casos en que sean equipos de reserva del IPES se debe documentar su estado final.

6.7.8 Almacenamiento de datos del site alterno

Los datos respaldados del site alterno y que fueron restaurados en los sistemas normales, se deben marcar y de preferencia enviar a centro de almacenamiento alterno. Los sistemas restablecidos seguirán sus esquemas definidos de respaldo en operación normal.

6.7.9 Documentación

Una vez se restablezcan los sistemas de información a sus condiciones normales, se debe iniciar el proceso de documentación formal del incidente. La documentación del incidente se realiza siguiendo las actividades descritas en el procedimiento de gestión de incidentes de seguridad de la información y la guía para atención de incidentes de seguridad de la información.

7 Pruebas, entrenamiento y simulación

7.1 Plan de pruebas

Con el fin de garantizar el correcto funcionamiento del plan de contingencia, se deben realizar pruebas regulares del mismo. Los mecanismos que se deben emplear para la prueba del plan de contingencia incluyen: ejercicio del plan de contingencia, auditoría y autoevaluación. A continuación se detallan los tipos de pruebas que se pueden realizar al plan de contingencia.

7.1.1 Sensibilización

Tipo de prueba	Divulgación y sensibilización del Plan de contingencia
Nivel de complejidad	SIMPLE
Proceso de ejecución	Conferencia de explicación de la estrategia general de contingencia con evaluación escrita de los conceptos presentados
Variaciones	Realizar la capacitación vía web
Frecuencia	Mínimo una vez al año o cuando se presenten cambios que afecten el entorno o condiciones bajo las cuales fue planificado el plan de contingencia

7.1.2 Instrucción formal del plan

Tipo de prueba	Instrucción formal del plan
Nivel de complejidad	MEDIA
Proceso de ejecución	Entrenamiento formal de cada rol del plan de contingencia con evaluación de conocimientos de las funciones de cada rol.
Variaciones	No aplica.
Frecuencia	Mínimo una vez al año o cuando se presenten cambios que afecten el entorno o condiciones bajo las cuales fue planificado el plan de contingencia.

7.1.3 Revisión de escritorio

Tipo de prueba	Revisión de escritorio.
Nivel de complejidad	SIMPLE
Proceso de ejecución	Revisión detallada de todos los documentos del Plan de contingencia. La revisión debe ser realizada por los responsables de cada una de las secciones del plan de contingencia. Se debe revisar la documentación de procedimientos que acompañan el plan de contingencia. Los resultados de la revisión permiten ajustar el documento de plan de contingencia.
Variaciones	Auditoría realizada al plan por un representante de control interno. Actualización del plan por parte de un responsable del plan.
Frecuencia	Mínimo una vez al año o cuando se presenten cambios que afecten el entorno o condiciones bajo las cuales fue planificado el plan de contingencia.

7.1.4 Recorrido guiado por el plan

Tipo de prueba	Recorrido al plan
Nivel de complejidad	Mediano
Proceso de ejecución	Se toma el plan de contingencia y se revisan las actividades que deben ejecutar los responsables de las diferentes actividades. Cada participante lee la actividad a su cargo y sin realizar ejecución de la tarea simula su ejecución en el lugar y empleando los recurso definidos para la actividad. Ejemplo. Tomar el árbol de notificación, llamar al primer punto de notificación (verificar nombre, teléfono) informarle que se está realizando un ejercicio de recorrido de plan de contingencia, informarle que debe continuar con el árbol de notificación definido. Anotar resultados pertinentes del ejercicio: teléfonos no actualizados, nombres responsables no actualizados, inconsistencias en el árbol de notificación. En el caso de actividades técnicas, ubicar los elementos técnicos como servidores, switches o cintas de respaldo, leer las acciones de plan y verificar que las actividades se podrán ejecutar. Validar que se conocen comando y pasos definidos en el plan de contingencia.
Variaciones	Realizar el trabajo de recorrido del plan activando a varios participantes la vez.
Frecuencia	Al menos una vez al año.

7.1.5 Simulación

Tipo de prueba	Simulación
Nivel de complejidad	Mediano
Proceso de ejecución	Tomar el plan de contingencia y en la modalidad de simulación ejecutar un subconjunto de las actividades definidas en el plan: Probar todo el árbol de notificación, probar la restauración de datos. Las actividades a verificar no son de carácter crítico y no deben impactar la operación normal del IPES. La situación es la simulación de un escenario artificial para verificar que las actividades del plan se pueden ejecutar.
Variaciones	Realizar la simulación activando más de un grupo de trabajo.
Frecuencia	Al menos una vez al año, ideal dos veces al año.

7.1.6 Ejercicio de actividad crítica

Tipo de prueba	Ejercicio de actividad crítica
Nivel de complejidad	Mediano
Proceso de ejecución	Seleccionar **una** actividad crítica y una fecha que no impacte la operación del IPES para esa actividad. Bajo condiciones controladas verificar la posibilidad de ejecutar las actividades de contingencia, verificar si es realizar las actividades de SIAFI desde la secretaria de Hacienda
Variaciones	Ejecutar las actividades de contingencia por más de un día en la sede alterna
Frecuencia	Al menos una vez al año o máximo cada dos años.

7.1.7 Restauración de datos en equipo alterno

Tipo de prueba	Restauración de datos en equipo alterno
Nivel de complejidad	Medio/Complejo
Proceso de ejecución	Realizar la restauración de los sistemas críticos HEMI, Correo en servidor virtual, aislado del ambiente de producción para certificar que las copias de respaldo operan correctamente.
Variaciones	No aplica
Frecuencia	Al menos dos vez al año

7.1.8 Prueba completa del plan de contingencia

Tipo de prueba	Prueba completa del Plan de contingencia.
Nivel de complejidad	Complejo.
Proceso de ejecución	Activar todo el plan de contingencia y operar en sede alterna. Solo aplicable para SIAFI y para acceso desde Barichara a servicios de almacenamiento o correo
Variaciones	No aplica.
Frecuencia	Al menos una vez al año o máximo cada dos años.

7.2 Entrenamiento de personal

El éxito en la operación y funcionamiento del plan de contingencia del IPES depende de que todo el personal con funciones asignadas en el plan participe en un programa de sensibilización y capacitación en los procedimientos del plan de contingencia. A continuación se describen los aspectos del programa de capacitación en el plan de contingencia

7.2.1 Conceptos de continuidad de negocio

Dirigido a: Todo el personal del IPES
Duración: 4 horas
Temario:

- Conceptos relacionados con continuidad de negocio: BCP, DRP, Plan de contingencia
- Razones para la implementación de un plan de continuidad
- Concepto de BIA: Análisis de impacto al negocio
- Análisis y gestión de riesgos
- Estrategias para implementar la continuidad de negocio

7.2.2 Procedimientos básicos de apoyo al plan de contingencia del IPES

Dirigido a: Personal con funciones operativas durante la ejecución del plan de contingencia

Duración: 8 horas
Temario

- Procedimiento de gestión de incidentes de tecnología
- Procedimiento de gestión de problemas de tecnología
- Procedimiento de gestión de incidentes de seguridad de la información
- Procedimiento de operación del plan de contingencia

7.2.3 Procedimientos técnicos del plan de contingencia

Dirigido a: Personal con funciones técnicas de recuperación de servicios de misión crítica

Duración: (depende de cada módulo)

Temario

- Configuración de switch nuevo para soporte de LAN (2 a 4 horas)
- Reinstalación de sistema operacional de servidores (8 a 16 horas)
- Reinstalación de motores de base datos (8 a 16 horas)
- Restauración de copia de base de datos (2 a 4 horas)
- Instalación de herramientas de trabajo esenciales para estación de trabajo (8 a 16 horas)
- Reinstalación de aplicaciones mediante restauración de imagenes de servidores virtuales (4 a 6 horas)

8 Anexos

8.1 Formato de reporte de valoración de incidente

REPORTE DEL INCIDENTE (dd/mm/aa/hh:mm) :	
Naturaleza del Incidente. (Daño físico, Interrupción servicio, Daños lógicos)	Causas Conocidas del incidente
Detalles sobre tipo de respuesta y recuperación requerido.	Sitio, Fecha y Hora Reunión del Informativo de reporte de incidente
Instrucciones para preparación de la reubicación de sistemas (si aplica)	Instrucciones para completar notificaciones
Elaboró.	Aprobó.
VALORACION DEL INCIDENTE (dd/mm/aa/hh:mm) :	
Causa de la interrupción	Efectos potenciales sobre otros sistemas
Diagnóstico situación actual de infraestructura (datacenter, potencia, telecomunicaciones, Aire Acondicionado.)	Tipo de daño (agua, fuego, calor, fuente eléctrica, impacto físico)

Tiempo estimado para restaurar servicios	Elementos a reemplazar (hardware, software)
Inventario y estado de los diferentes componentes (funcional, no funcional, parcial)	
Elaboró.	Aprobó.

8.2 Procedimientos de restablecimiento de servicios

Los diferentes procesos de restablecimiento de servicios se encuentran desarrollados a través de diferentes videos en su totalidad son 158 videos, ubicados en el servidor NAS al que tiene acceso todos los integrantes del área de sistemas.

Correo

Se cuenta con snapshots a diario de las diferentes máquinas virtuales donde se ejecutan los diferentes servicios (correo, SIAFI, HEMI, Directorio Activo) en un fallo critico se propone revertir por medio de los snapshots. Mensualmente se genera un export de las maquinas virtuales que sirve como respaldo en caso de no lograr revertir el fallo con los snapshots.

El registro de la información se encuentra en las maquinas, el servicio de correo, en este momento no se cuenta con un respaldo del histórico de la información de los PST de correo.

La estructura propuesta para el backup de los .pst, generando una replicación de los .pst del cliente a su U y sacar el backup de la U.

Directorio Activo

Se cuenta con dos backup en línea uno en a misma sede y el otro se encuentra en Barichara, por medio de una replicación del principal a los dos backup.

Se cuenta con dos servidores iguales para la virtualización que se mantienen sincronizados.

SIAFI

La base de datos tiene un propio backup de ORACLE por medio de RMAN, y es pasado a cinta todos los viernes. Los sábados se hace un export de la base de datos y se pasa a cinta.

La base de datos se encuentra en un servidor físico no en maquina virtual, el aplicativo que se está en producción se encuentra en la NAS.

La restauración de SIAFI se debe realizar manual, no cuenta con replicación, la restauración se debe realizar de forma manual, restaurando los backups diarios.

HEMI

Cuenta con un servidor Web que se encuentra en una maquina virtual y la base de datos en un servidor DHSP, administra el WSUS que servicios como los file servers.

En la eventualidad de un fallo, se realiza un diagnóstico para determinar si el fallo es en el servidor Web o en la base de datos o en el aplicativo como tal.

Drive U

Se realiza backup de la información colgada por los usuarios en su unidad de U. La información se encuentra en la NAS.

El backup se realiza semanal de todas las U y en cada no de los clientes se mantiene un backup.

Se quiere modificar las políticas de backup, para que se puedan realizar de forma incrementales o diferenciales diariamente.

Existe un grado de confianza pues es un dispositivo nuevo, y existe las contingencias en los RAID y los backup.

8.3 Formato diario de revisión de servicios de tecnología

RESPONSABLE VERIFICACIÓN: JOHN JAIR GARZÓN DELGADO
FECHA: 19/06/2013
HORA: 7:02

Servicio de correo electrónico institucional: Diagnóstico de recepción y envío de correos electrónicos:		
Interno – Interno	(•) SI	( ) NO
Interno – Externo	(•) SI	( ) NO
Externo - Interno	(•) SI	( ) NO
Servicio de Internet: Navegación a Internet		
NAVEGACIÓN	(•) SI	( ) NO
Servidor de Archivos: Funcionamiento de unidad de red		
FILESERVER	(•) SI	( ) NO
Servidor de Antivirus: administrador, actualizaciones y tareas funcionando		
CONSOLA ANTIVIRUS	(•) SI	( ) NO
TELEFONÍA	(•) SI	( ) NO
SIAFI	(•) SI	( ) NO
PORTAL	(•) SI	( ) NO
INTERNET	(•) SI	( ) NO
HEMI	(•) SI	( ) NO

SERVIDOR IMPRESIÓN	SI	NO
COMPARTIDOS	SI	NO
ZONA S	SI	NO
ZONA U	SI	NO
REPLICACIÓN DNS	SI	NO
AGENTE SQL	SI	NO
DIGITURNO	SI	NO
AGENTE SQL SERVER	SI	NO
CARTERA	SI	NO
PIVOC	SI	NO
LICENCIA AUTOCAD	SI	NO
PING SERVER 0.9	SI	NO
0.10	SI	NO
0.7	SI	NO
0.63	SI	NO
0.17	SI	NO
0.18	SI	NO
0.13	SI	NO
0.14	SI	NO
0.19	SI	NO
0.20	SI	NO
2.2	SI	NO

	0.186	SI	NO

Instantáneas en 17 (Solo debe quedar una instantánea al finalizar la jornada):

	BDAD2	SI	NO
	HEMI6	SI	NO
HEMIPRUEBAS		SI	NO
	PORTAL3	SI	NO
	PRINT3	SI	NO

Instantáneas en 18 (Solo debe quedar una instantánea al finalizar la jornada):

ActiveDirectory		SI	NO
	PRINT2	SI	NO
	ZIMBRA2	SI	NO
	CORREO	SI	NO

Sellos colocados o removidos:

Lugar	Número de sello
Data Center	
Laboratorio	
Gabinete de elementos	n/a
Coordinación	

Ping a servidores

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

U:\>ping 192.168.0.9

Haciendo ping a 192.168.0.9 con 32 bytes de datos:
Respuesta desde 192.168.0.9: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.9: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.9: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.9: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.9:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.10

Haciendo ping a 192.168.0.10 con 32 bytes de datos:
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.10: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.7

Haciendo ping a 192.168.0.7 con 32 bytes de datos:
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.7: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.63

Haciendo ping a 192.168.0.63 con 32 bytes de datos:
Respuesta desde 192.168.0.63: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.63: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.63: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.63: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.63:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.17

Haciendo ping a 192.168.0.17 con 32 bytes de datos:
Respuesta desde 192.168.0.17: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.17: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.17: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.17: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.17:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.18

Haciendo ping a 192.168.0.18 con 32 bytes de datos:
Respuesta desde 192.168.0.18: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.18: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.18: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.18: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.18:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.13

Haciendo ping a 192.168.0.13 con 32 bytes de datos:
Respuesta desde 192.168.0.13: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.0.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.13: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.13: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.13:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 0ms

U:\>ping 192.168.0.14

Haciendo ping a 192.168.0.14 con 32 bytes de datos:
Respuesta desde 192.168.0.14: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.14: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.14: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.14: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.14:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.19

Haciendo ping a 192.168.0.19 con 32 bytes de datos:
Respuesta desde 192.168.0.19: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.19: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.19: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.19: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.19:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.0.20

Haciendo ping a 192.168.0.20 con 32 bytes de datos:
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.20:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

U:\>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:
Respuesta desde 192.168.2.2: bytes=32 tiempo=6ms TTL=253
Respuesta desde 192.168.2.2: bytes=32 tiempo=5ms TTL=253
Respuesta desde 192.168.2.2: bytes=32 tiempo=6ms TTL=253
Respuesta desde 192.168.2.2: bytes=32 tiempo=5ms TTL=253

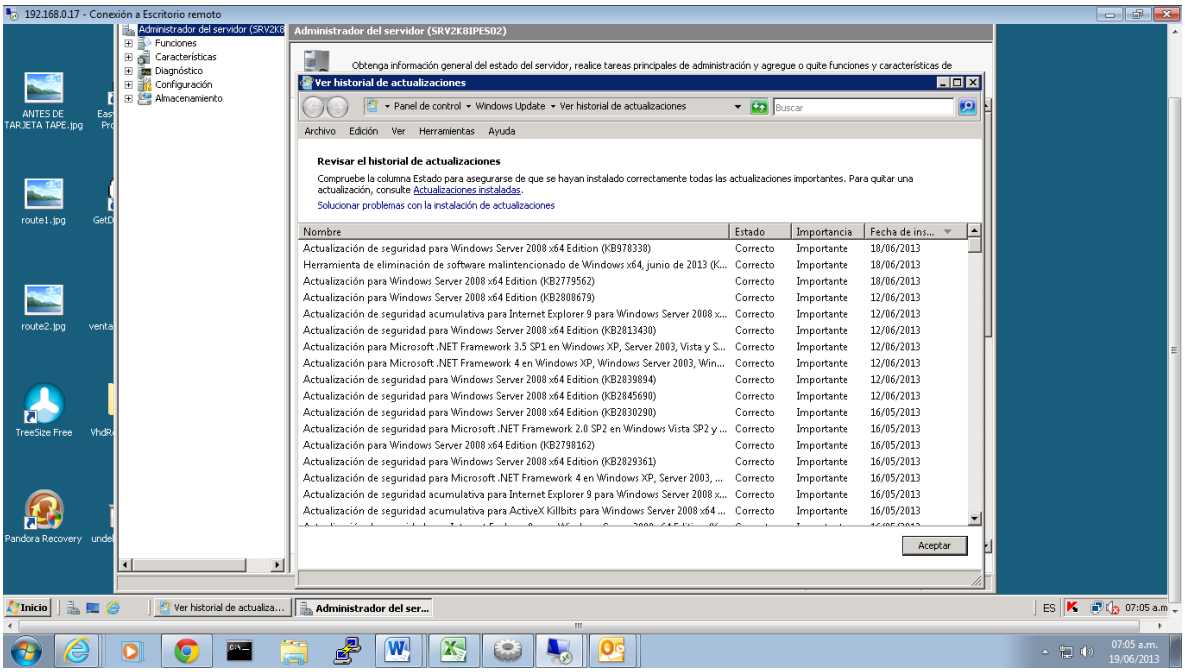
Estadísticas de ping para 192.168.2.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 5ms, Máximo = 6ms, Media = 5ms

U:\>ping 192.168.0.186

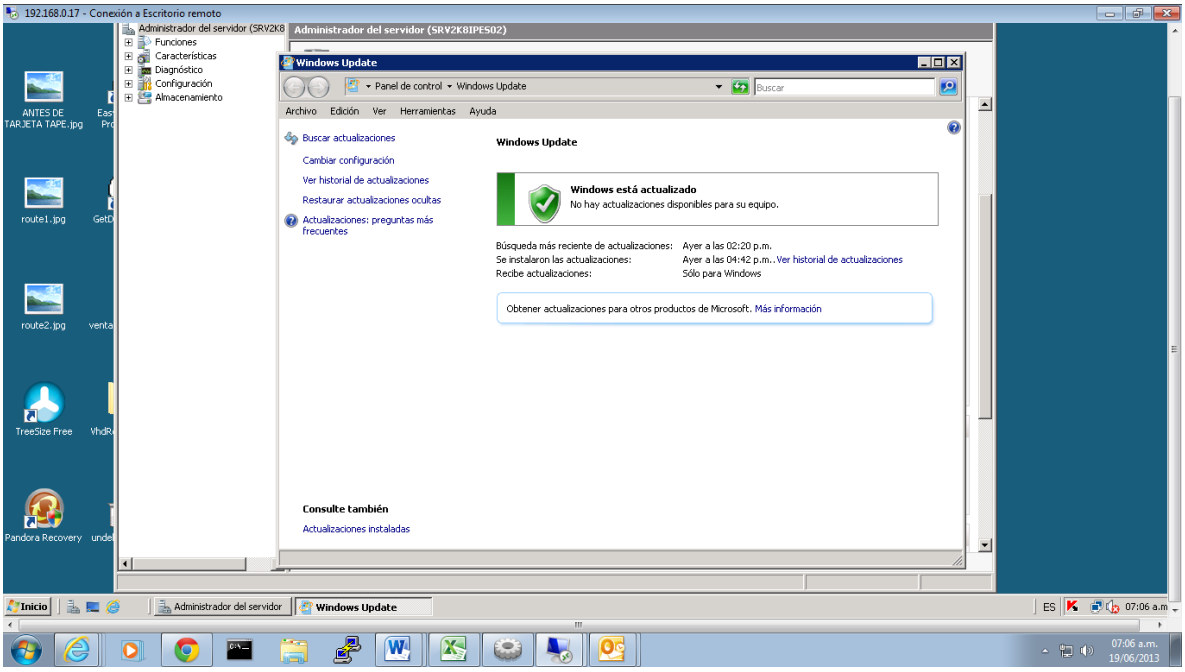
Haciendo ping a 192.168.0.186 con 32 bytes de datos:
Respuesta desde 192.168.0.186: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.186: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.186: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.186: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.186:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

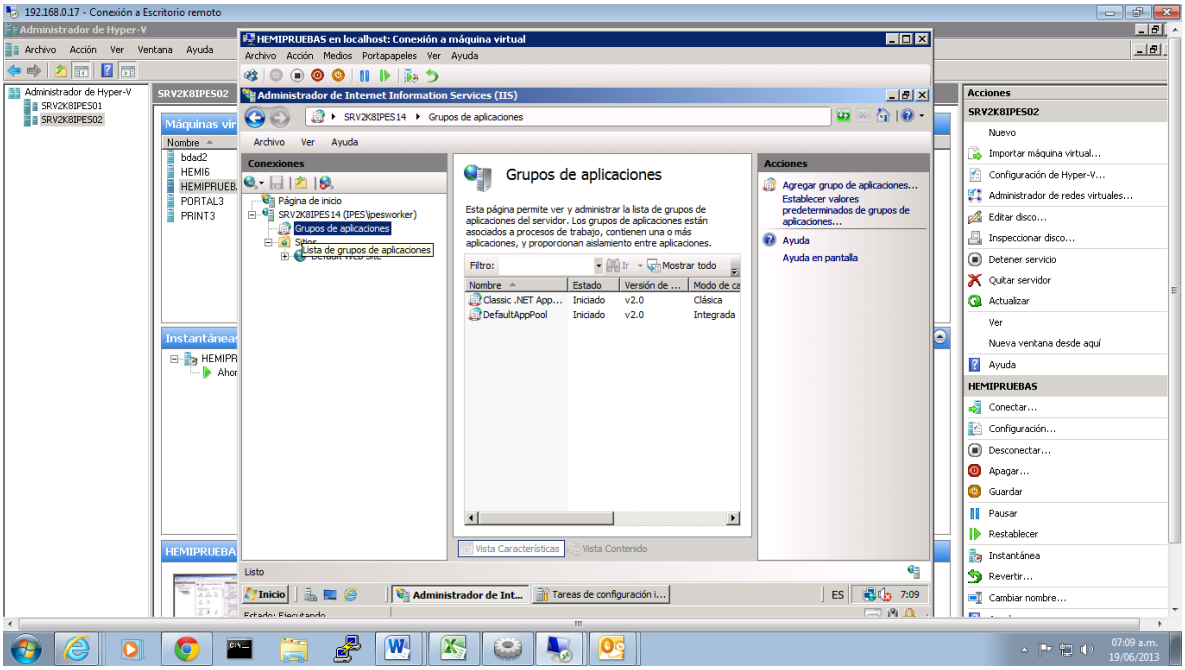
U:\>



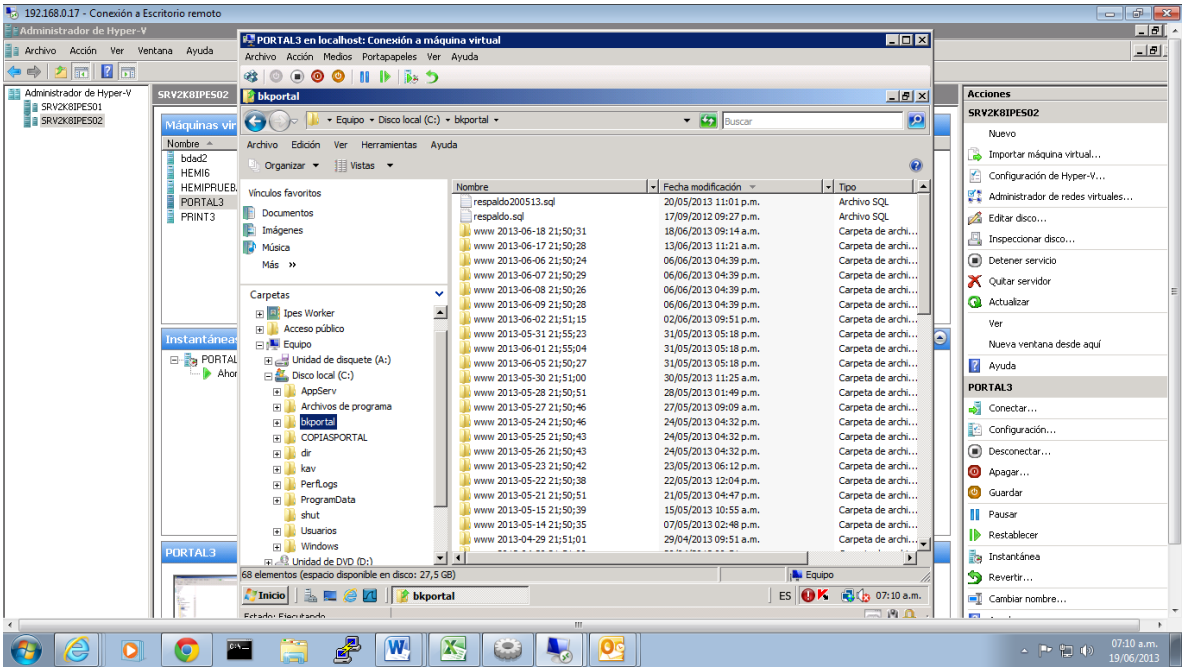
Updates satisfactorios 17



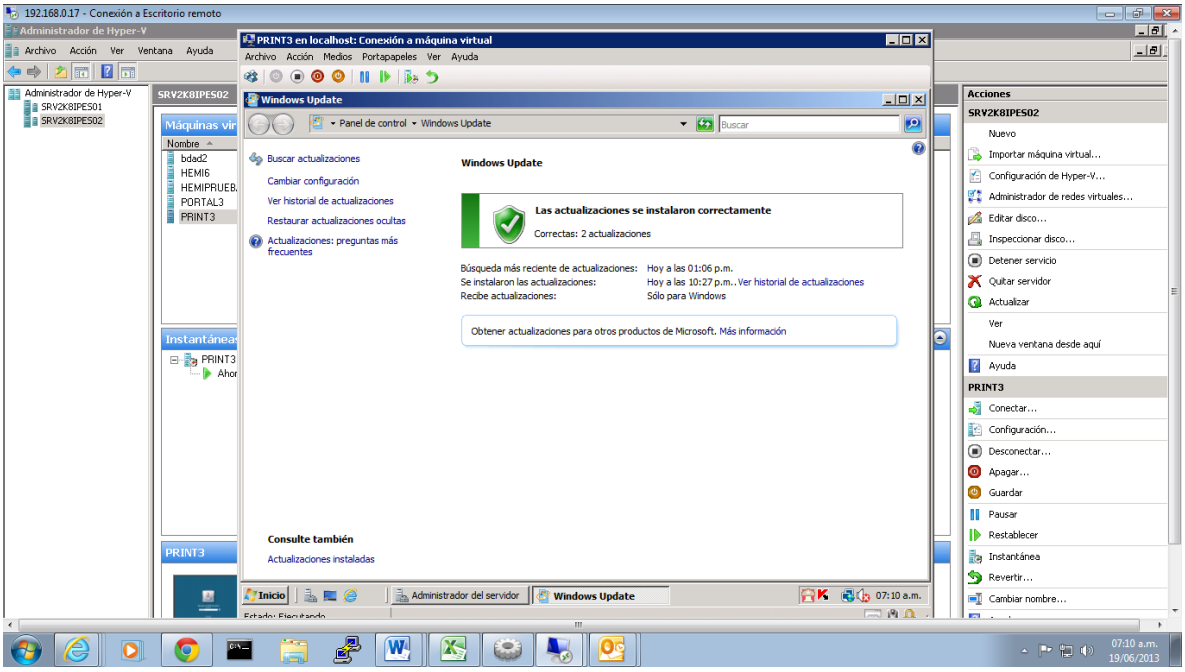
Servicios de IIS

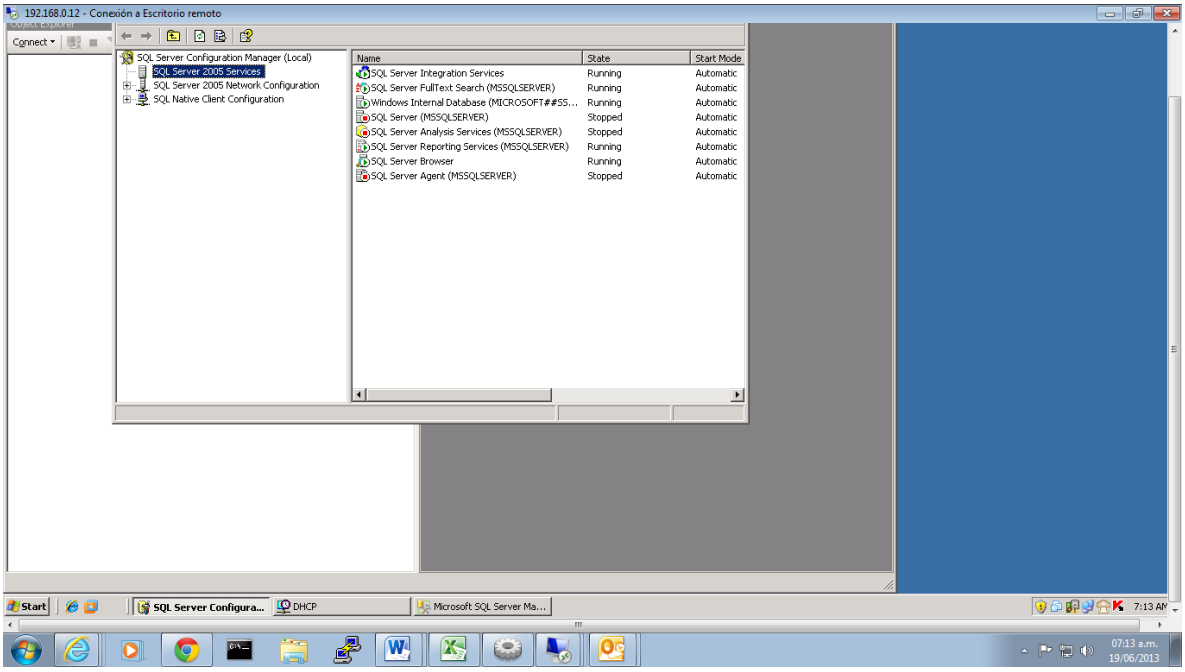


Backup Portal satisfactorio

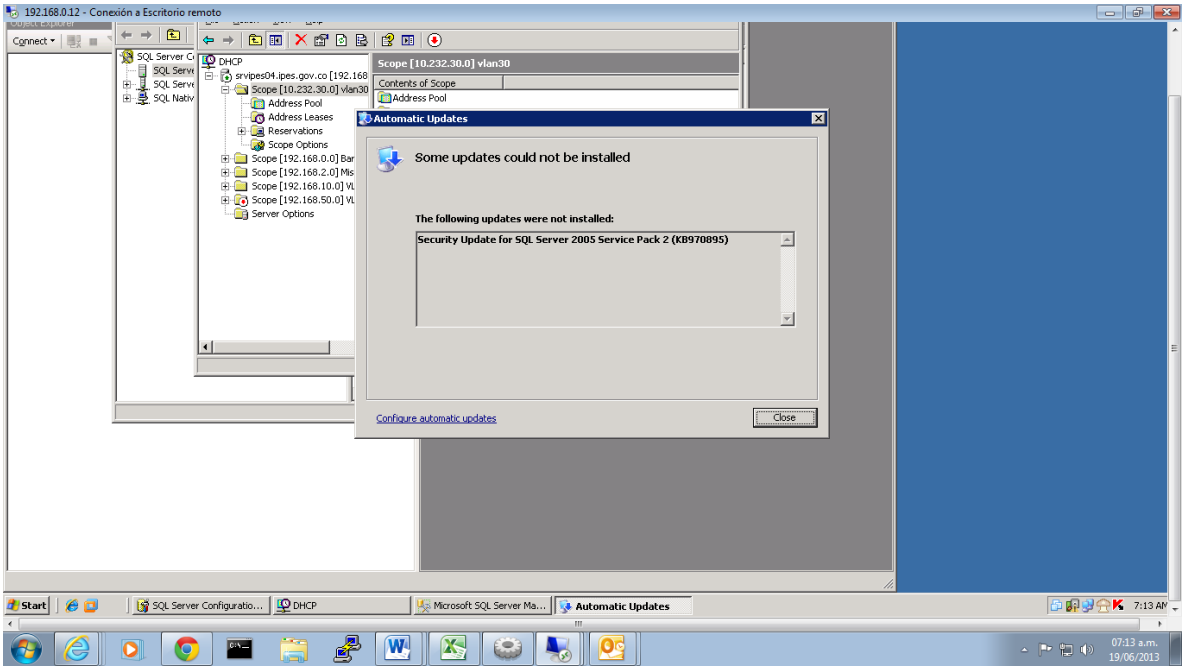


Updates instaladas en .20

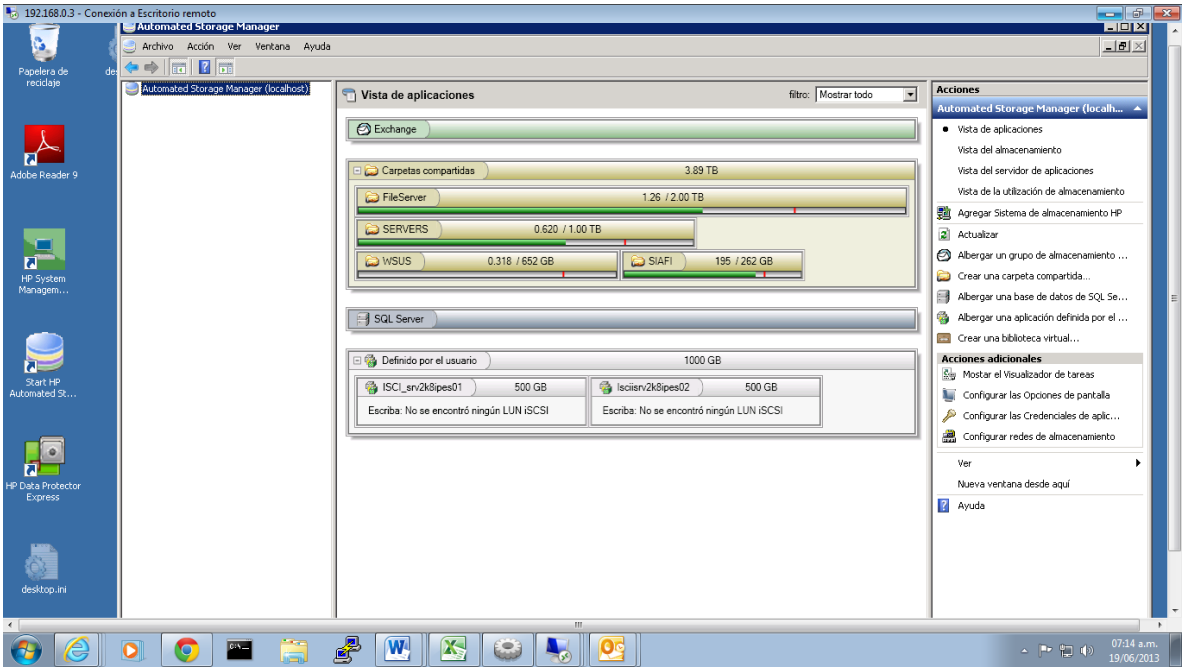


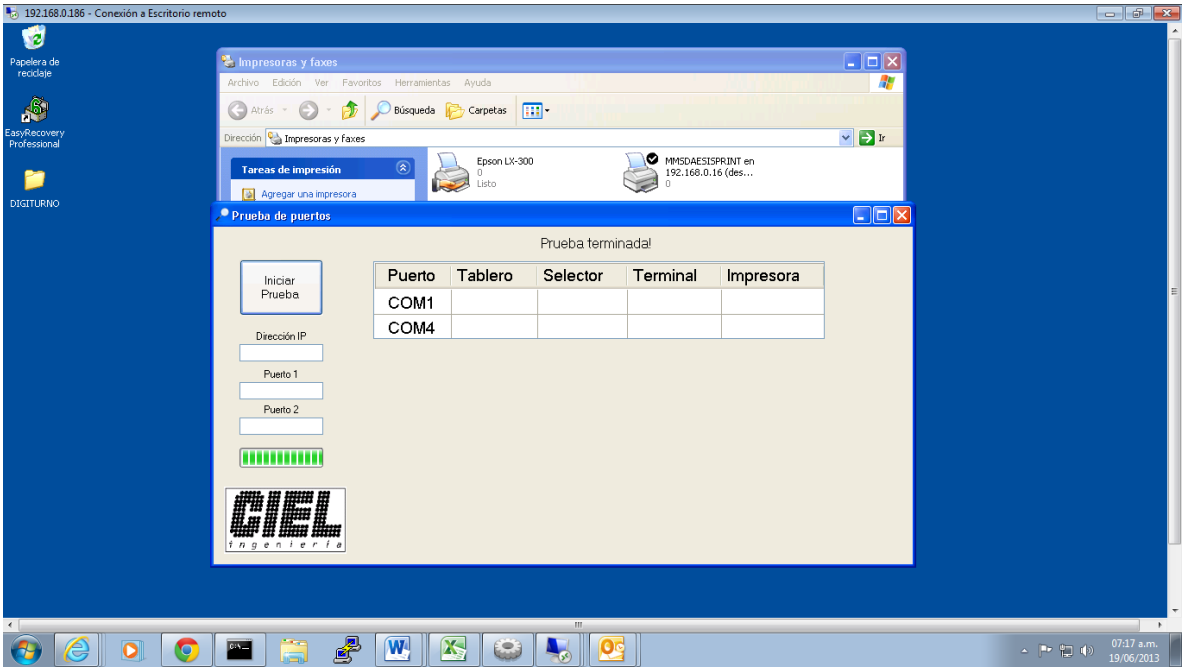


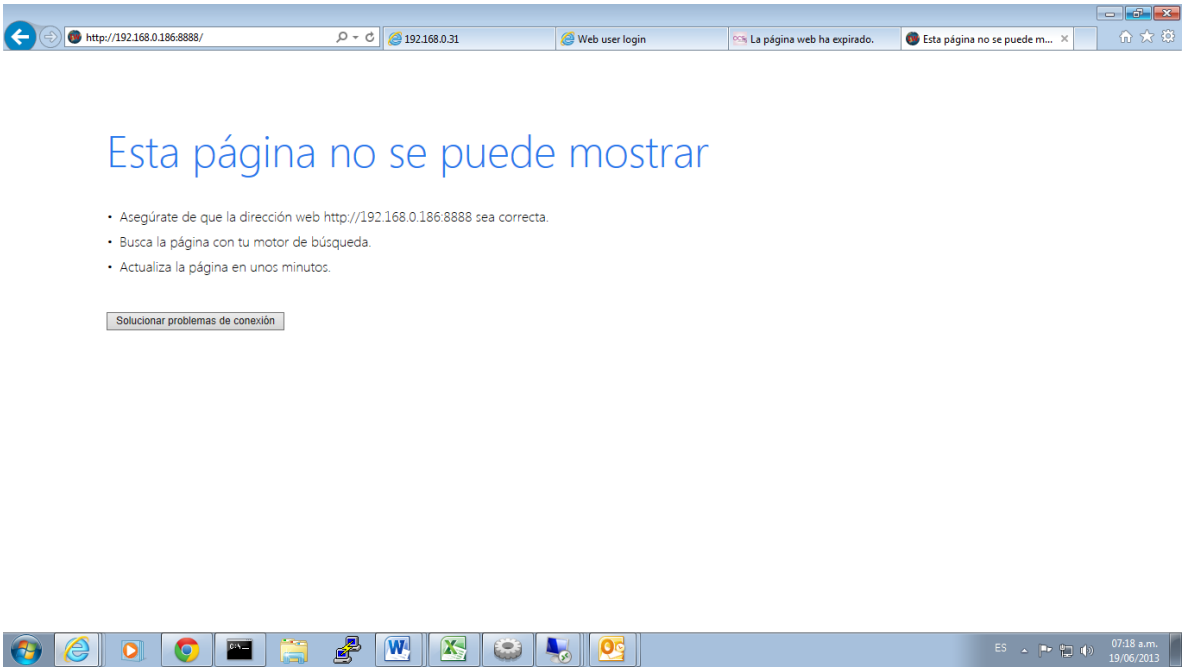
Update SQL server



Almacenamiento NAS

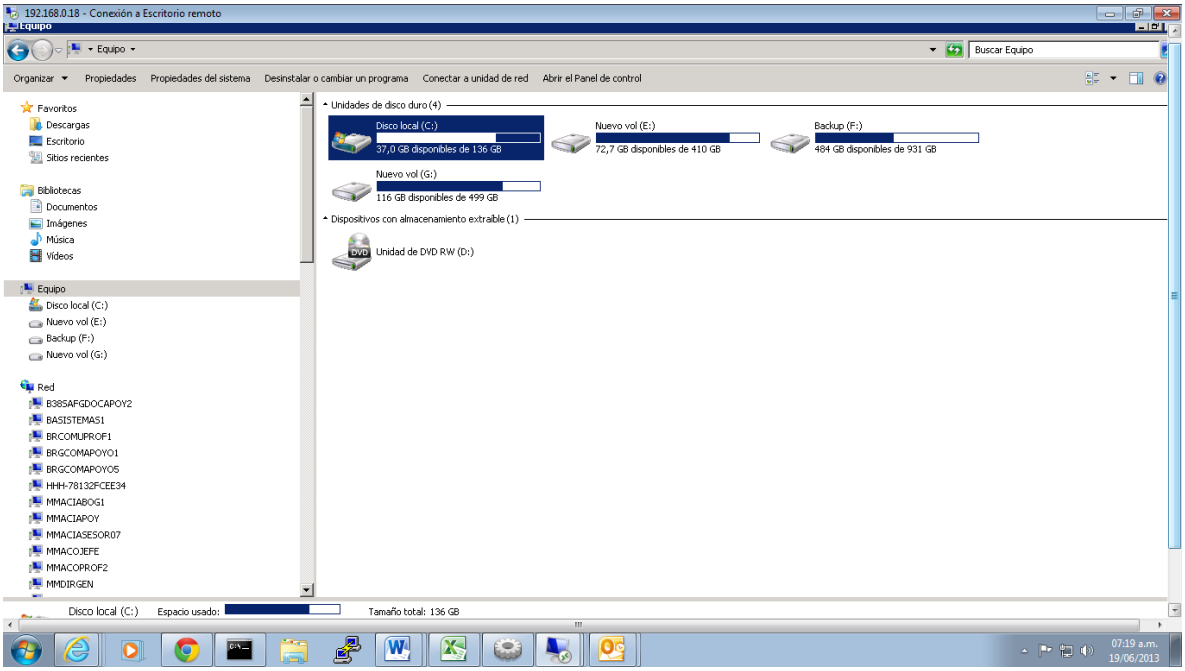

192.168.0.3 - Conexión a Escritorio remoto
Automated Storage Manager
Archivo Acción Ver Ventana Ayuda
Automated Storage Manager (localhost)
Vista de aplicaciones
filtro: Mostrar todo
Exchange
Carpetas compartidas 3.89 TB
FileServer 1.26 / 2.00 TB
SERVERS 0.620 / 1.00 TB
WSUS 0.318 / 652 GB
SIAFI 195 / 262 GB
SQL Server
Definido por el usuario 1000 GB
ISCI_srv2k8ipes01 500 GB
Escriba: No se encontró ningún LUN iSCSI
Isciisrv2k8ipes02 500 GB
Escriba: No se encontró ningún LUN iSCSI
Acciones
Acciones adicionales
Papelera de reciclaje
Adobe Reader 9
HP System Managem...
Start HP Automated St...
HP Data Protector Express
desktop.ini


192.168.0.186 - Conexión a Escritorio remoto
Papelera de reciclaje
EasyRecovery Professional
DIGITURNO
Impresoras y faxes
Tareas de impresión
Agregar una impresora
Epson LX-300
Listo
Prueba de puertos
Prueba terminada!
Iniciar Prueba
Dirección IP
Puerto 1
Puerto 2
Puerto Tablero Selector Terminal Impresora
COM1
COM4
CIEL ingeniería

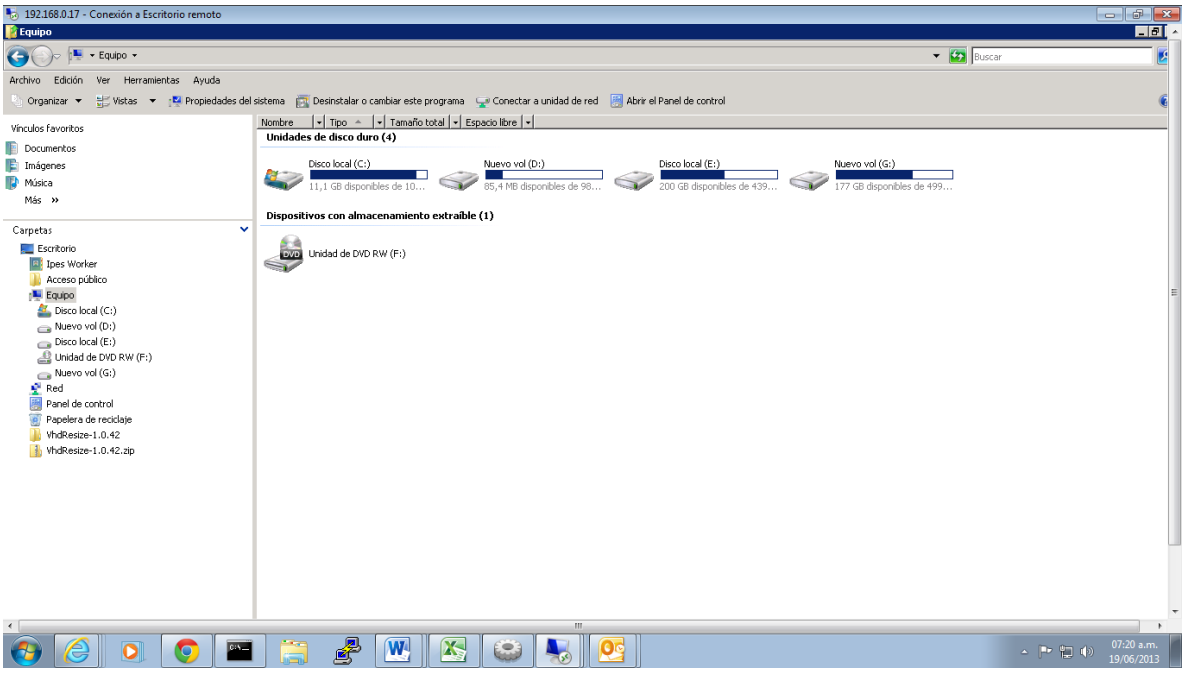


DIGITURNO PRESENTA CAIDA DE SERVICIO WEB

Almacenamiento Host de virtualización 18



Almacenamiento Host de virtualización 17



8.4 Registros de las cintas que se utilizan para los Backups

CINTA	FECHA	Información
SIAFI1	27/06/2013	RMAN de Oracle
SIAFI9	27/06/2013	Full de Base de Datos SIAFI
IPES810	27/06/2013	Unidades U
IPES811	27/06/2013	Unidades U
IPES812	27/06/2013	Unidades U
IPES828	27/06/2013	Backups servidores, Bases de Datos y configuración
IPES829	27/06/2013	Backups servidores, Bases de Datos y configuración
IPES830	27/06/2013	Backups servidores, Bases de Datos y configuración
SIAFI2	04/07/2013	RMAN de Oracle
SIAFI10	04/07/2013	Full de Base de Datos SIAFI
IPES813	04/07/2013	Unidades U
IPES814	04/07/2013	Unidades U
IPES815	04/07/2013	Unidades U
IPES831	04/07/2013	Backups servidores, Bases de Datos y configuración
IPES809	04/07/2013	Backups servidores, Bases de Datos y configuración
SIAFI3	11/07/2013	RMAN de Oracle
SIAFI11	11/07/2013	Full de Base de Datos SIAFI
IPES816	11/07/2013	Unidades U
IPES817	11/07/2013	Unidades U
IPES818	11/07/2013	Unidades U
IPES822	11/07/2013	Backups servidores, Bases de Datos y configuración
IPES823	11/07/2013	Backups servidores, Bases de Datos y configuración
IPES824	11/07/2013	Backups servidores, Bases de Datos y configuración
SIAFI4	18/07/2013	RMAN de Oracle
SIAFI12	18/07/2013	Full de Base de Datos SIAFI
IPES819	18/07/2013	Unidades U
IPES820	18/07/2013	Unidades U
IPES821	18/07/2013	Unidades U

CINTA	FECHA	Información
IPES825	18/07/2013	Backups servidores, Bases de Datos y configuración
IPES826	18/07/2013	Backups servidores, Bases de Datos y configuración
IPES827	18/07/2013	Backups servidores, Bases de Datos y configuración
SIAFI1	25/07/2013	RMAN de Oracle
SIAFI5	25/07/2013	Full de Base de Datos SIAFI
IPES810	25/07/2013	Unidades U
IPES811	25/07/2013	Unidades U
IPES812	25/07/2013	Unidades U
IPES828	25/07/2013	Backups servidores, Bases de Datos y configuración
IPES829	25/07/2013	Backups servidores, Bases de Datos y configuración
IPES830	25/07/2013	Backups servidores, Bases de Datos y configuración
SIAFI2	01/08/2013	RMAN de Oracle
SIAFI6	01/08/2013	Full de Base de Datos SIAFI
IPES813	01/08/2013	Unidades U
IPES814	01/08/2013	Unidades U
IPES815	01/08/2013	Unidades U
IPES831	01/08/2013	Backups servidores, Bases de Datos y configuración
IPES809	01/08/2013	Backups servidores, Bases de Datos y configuración