PLAN DE CONTINGENCIA BASES DE DATOS

Introducción

Varias de las operaciones que se realizan a diario en una empresa o ente publica dependen de la eficacia y eficiencia de los servicios informáticos, por lo que si sucede un desastre informático la productividad y continuidad es fuertemente afectada.

Se podría definir como un desastre informático lo que provoca la interrupción y paralización de las actividades y/o procesos más esenciales y que puedan afectar los servicios. Tras un suceso de este tipo, se deben tener un conjunto de acciones con base en los recursos necesarios, con el fin de recuperarse en el menor tiempo y costo posible. Para ello, son necesarios sistemas y servicios que ayuden a recuperar información técnica, organizativa y de funcionamiento básica.

La buena aplicación de estos servicios y soluciones de continuidad y recuperación, están pensados para garantizar la disponibilidad de los procesos esenciales. Aunque las pérdidas por un desastre informático puedan ser muy importantes, cada vez son mayores los avances tecnológicos que permiten y hacen posible la recuperación en muy poco tiempo y a unos costos razonables, siendo sus ciclos de implantación cada vez más cortos. Sin embargo, más allá de la recuperación son necesarios servicios de continuidad del negocio que ayuden a evolucionar al sistema de un negocio.

1. Plan de Contingencia

El objetivo de un plan de contingencia para las Tecnologías de Información y Comunicación es definir las acciones a realizar para proporcionar continuidad y recuperación en los servicios, dentro de los parámetros que permitan los recursos disponibles. El plan de contingencia constará de dos fases principales, la primera mostrará las amenazas con posibilidad de ocurrencia alta y que son críticas para la continuidad de operación de los servicios informáticos y la segunda definirá las acciones a seguir para la recuperación de las operaciones.

1.1 Actividades Asociadas

Las actividades consideradas en este documento son:

- Análisis de Riesgos
- Medidas Preventivas
- Previsión de Desastres
- Plan de Respaldo
- Plan de Recuperación

2. Análisis de Riesgos

De acuerdo a las operaciones de los bienes y servicios que proporciona, se han identificado los siguientes problemas críticos:

- Falla en comunicación a Internet
- Falla en comunicación entre inmuebles
- Falla en el suministro de energía
- Falla en hardware y/o software de servidores
- Falla en aplicaciones
- Virus Informático

2.1 Bienes susceptibles de daño

La infraestructura, aplicaciones e información vulnerable:

Información

- Bases de datos de aplicaciones en servidores
- Configuración de usuarios de correo electrónico en servidor

2.2 Daño Dentro de los posibles daños se pueden contemplar:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, ya sea por causas naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, como cambios de claves de acceso, eliminación o borrado físico / lógico de información.

2.3 Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que pierden en el acontecimiento.

2.4 Fuentes de daño

Las amenazas que pudieran tener los bienes y servicios son:

Hackeo

Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

Virus Informático

Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso.

Falla en infraestructura

• Falla en servidor de aplicaciones y datos, tanto en su(s) discos(s) duro(s) como en el procesador central

• Falla en elementos activos o cableado de red

• Falla en Router o Firewall

Falla de Software

Falla en el sistema operativo o cualquier software instalado en los servidores que de soporte a la operación de los servicios.

Errores Humanos (Falla de personal clave)

Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de los sistemas de Información:

a) Personal de Informática

b) Soporte Técnico

c) Usuarios de Sistemas

Críticos Pudiendo existir los siguientes inconvenientes:

a) Enfermedad o accidentes

b) Renuncias

c) Otros imponderables

Desastres Naturales

a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).

b) Inundaciones causadas por falla en los suministros de agua.

c) Fallas en los equipos de soporte:

- Por causas de agresividad en el ambiente
- Por fallas de la red de energía pública por diferentes razones
- Por fallas en los equipos de acondicionamiento atmosférico necesarios para una adecuada operación de los equipos computacionales más sensibles
- Por fallas en el tendido físico de la red local
- Por fallas en el conmutador telefónico

Proveedores con Fallas Técnicas

Servicios contratados con terceros, con ocurrencia de fallas por diferentes razones ajenas al manejo por parte del Instituto.

Errores en Bases de Datos

Estas deben considerarse como parte de la infraestructura tecnológica, ya que los manejadores de bases de datos son el soporte para manejo de información en los sistemas.

2.5 Expectativa de Daños

La expectativa de daños debe de ser la mínima, sin embargo en caso de una contingencia siempre existirá la posibilidad de que estos se presenten, por lo que a continuación se presenta una tabla con la posibilidad de ocurrencia de las amenazas consideradas.

Amenaza	Posibilidad de ocurrencia
Hackeo	Baja
Virus informático	Alta
Falla en infraestructura	Alta
Falla de software en equipos	Alta
Errores humanos	Media
Proveedores con fallas técnicas	Media
Errores en bases de datos	Baja
Desastres naturales	Baja

3. Medidas Preventivas

3.1Control de Acceso

a) Acceso físico de personas no autorizadas.

El acceso físico a los diferentes sitios que se encuentran se encuentran restringidos por puertas con seguridad, a las cuales solo el personal de la Subdirección de Informática tendrá acceso, esto con la finalidad de evitar cualquier fallo ocasionado por personal ajeno a ésta.

La clave de acceso para puertas con seguridad por contraseña, deberá de ser cambiada periódicamente. En estas puestas todo el personal de la Subdirección de Informática tiene acceso.

b) Acceso a la Red de PC's y Servidores.

Tanto el acceso a red de pc's y servidores, se encontrará controlado por un controlador de dominio el cual determinará los equipos pertenecientes a la red; así como usuarios y contraseñas, brindando diferentes niveles de seguridad.

Cabe mencionar que a los servidores Primary Domain Controller y Sencondary Domain Controller sólo tendrá acceso la Jefatura de Departamento de Servicios Web y la Subdirección de Informática. Para el caso del Servidores de aplicaciones Lando y Ewok el acceso sólo lo tendrá la Jefatura de Desarrollo de Sistemas Administrativos y la Subdirección de Informática.

Como medida preventiva, se solicita el cambio de la contraseña de acceso a todos los usuarios de forma periódica.

c) Acceso restringido a las librerías, programas, y datos.

Parte del control de usuarios por medio del controlador de dominio, es poder determinar a que tiene acceso un usuario o no, así como las capacidades de estos para instalar programas, librerías o acceso a ciertas carpetas dentro de los equipos o servidores.

3.2Respaldos

4. Previsión de Desastres

La previsión de desastres sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en los sitio de cómputo y comunicaciones, en la medida de que no haya situaciones que generen la interrupción del proceso de operación normal; así como el de respaldo, al tener claro los lugares de resguardo, vías de escape y de las ubicaciones de los archivos, diskettes, discos con información vital de respaldo de aquellos que se encuentre aún en las instalaciones del Instituto.

4.1Adecuado Soporte de Utilitarios

Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos:

a) Unidades de Respaldo de Energía – Este equipo deberá recibir cuando menos 3 servicios de mantenimiento preventivo al año, esto para su correcto funcionamiento.

El mantenimiento será dado por la empresa contratada para realizar dicho servicio, dejando un reporte o bitácora de servicio.

b) Antenas de Comunicación – El equipo de comunicaciones punto a punto deberá de recibir cuando menos 3 servicios de mantenimiento preventivo al año, con la finalidad de asegurar su correcto funcionamiento, además de realizar ajustes en el envío y recepción de señal.

El mantenimiento será dado por la empresa contratada para realizar dicho servicio, dejando un reporte o bitácora de servicio.

4.2Seguridad Física del Personal

Como medida de seguridad física del personal, se deberán seguir las establecidas por la unidad de protección civil del Instituto.

4.3Seguridad de la Información

Esta parte refiere al acceso a información contenida en los diversos sistemas de información, la cual deberá está protegida por claves de acceso; así como un adecuado seguimiento al plan de respaldo.

5. Plan de Respaldo

Como parte importante de un Plan de Contingencia Informático se encuentra el Plan de Respaldo, el cual nos permite saber el proceso para la generación de los diferentes respaldos, ya sea de bases de datos, aplicaciones o configuraciones y nos proporcionará la medida de la pérdida de información relevante para dar continuidad a la operación de los sistemas de información institucionales.

5.1.2 Respaldo de Sistemas y Aplicaciones

Debido a la importancia de los sistemas y aplicaciones institucionales, es necesario realizar un proceso de respaldo que asegure que en caso de contingencia sea posible restaurar éstos para su funcionamiento. Por lo cual en este documento se explica el proceso de respaldo de los sistemas y aplicaciones.

En el Instituto se manejan sistemas y aplicaciones basados en un esquema de cliente / servidor. Por lo cual los datos se respaldan independientemente de la aplicación. Caso excepcional el Sistema WINSIAF desarrollado por MW Software, en el cual se respalda la aplicación y datos al mismo tiempo debido a las herramientas con las que fue desarrollado.

5.1.2.1 Respaldo de Datos

En el Instituto Nacional de las Mujeres todos los sistemas y aplicaciones de manejo de información cuentan con una base de datos para cada uno de ellos respectivamente. Estas bases de datos están soportadas por un Motor de Bases de Datos Microsoft SQL Server 2000.

El proceso de respaldo de las bases de datos dentro del SQL Server se trata de un plan de mantenimiento el cual se puede programar, determinando la periodicidad en horas, días, etc. De la misma forma, se puede determinar la ubicación donde se guardará el respaldo resultante. Cabe mencionar que al tratarse de un plan de mantenimiento se nos preguntará sobre optimizaciones, comprobaciones de integridad, etc., puntos que no trataremos en este documento.

5.1.2.3 Tablas de Respaldos

Respaldo de Datos				
Sistema/Aplicación	Servidor	Plan de Mantenimiento	Base	Programación
Evaluación de Competencias	Lando	competencias	competencias	Semanal: domingo, 4 a.m.
Requerimiento de Eventos	Lando	eventos	eventos	Semanal: domingo, martes, jueves, 2 a.m.
Mensajería Presidencia	Lando	mensajeriapres	mensajería	Semanal: lunes, miércoles, viernes, 2 a.m.
Sistema Programático para PNUD	Lando	PNUD	pnud	Semanal: martes y jueves, 2 a.m.
Sistema Programático 2005	Lando	Poa	Poa	Semanal: sábado, 3 a.m.
Sistema Programático 2006	Lando	Poa2006	Poa2006	Semanal: sábado 4 a.m.
Sistema Programático 2007	Lando	Poa07	Poa07	Semanal: sábado 4:30 a.m.
Winsiaf	Lando	Winsiaf	Winsiaf	Cada 12 hrs.
Sistema Programático 2008	Lando	Poa08	Poa08	Diariamente a las 5:00 a.m.

5.1.3.4.2 Base de Datos

La información de los huellómetros es almacenada en el manejador de base de datos Microsoft Access. En esta base de datos se almacenan el nombre, el número de empleado(a) y la huella digital del personal, así como la configuración para cada tipo de horario y los registros de entrada y salida del personal, entre otra información.

El Instituto tiene dos bases de datos una para el inmueble de Insurgentes y otra para el de AEO. Al tener únicamente una base de datos, los tiempos de respuesta para el registro de huellas del inmueble contrario a donde se tiene almacenada la base de datos, son muy prolongados.

La base de datos del inmueble de Insurgentes se llama BDmaestra.mdb y es la que funge como base maestra, la del inmueble de AEO se llama BDesclava.mdb, y como su nombre lo indica depende de la maestra. Para el correcto funcionamiento de la aplicación, se requiere que la carpeta donde se encuentran almacenadas las bases de datos se encuentre compartida para la Subdirección de Personal, para la Subdirección de Informática y para el huellómetro contrario.

Ambas bases de datos deben ser replicadas para que contengan la misma información, ya que los registros de entradas y salidas son independientes a ambos inmuebles y los registros de nuevo personal son almacenados en la base de datos maestra. Por lo que si no se replican no podrán generarse los reportes que conjuntan los registros de todo el personal y no podrán ser registradas las entradas y salidas del personal nuevo del inmueble de AEO.

Para realizar la réplica se deberá ejecutar el programa de Replicar verificando que los nombres de las bases de datos coincidan con la maestra y la esclava. Al finalizar deberá indicar el número de registros replicados.

El programa de replica realiza la copia de aquellos registros de entradas y salidas de la base de datos esclava que no se encuentran en la maestra, para posteriormente copiar toda la base de datos maestra en la esclava.

El programa se ejecuta manualmente, ya que no fue elaborado para trabajar automáticamente. La Dirección de Recursos Humanos realiza esta actividad periódicamente.

Al realizar la réplica, ambas bases de datos se bloquean, por lo que se recomienda realizarla cuando no existan entradas o salidas de los inmuebles. En su defecto, la Dirección de Recursos Humanos deberá solicitar a la Subdirección de Informática desactivar los huellómetros temporalmente para realizar la réplica, eliminando así posibles errores.

5.1.3.4.3 Respaldo

El respaldo de ambas bases de datos se realiza diariamente entre las 3:27am y 3:50am. Para programar la actividad automática se utilizó la herramienta Abakt, en la que se configura cual será el directorio a respaldar (c:\archivos de programa\ControlDePersonal\BD o c:\archivos de programa\ControlDePersonal\BaseDatos), en que formato 'HM-BAK-['yyyy'- 'mm'-'dd']'.zip o 'HE-BAK-['yyyy'-'mm'-'dd']'.zip y en que equipo. El respaldo se realiza en el directorio Huellómetro del servidor Ewok. De esta herramienta se genera un archivo .abp que se incluirá en una tarea programada de Windows.

Posteriormente se automatizó con una tarea programada de Windows, indicando la siguiente ruta de ejecución de respaldo:

"C:\Archivos de programa\Abakt\Abakt.exe" -b -x -m "C:\Archivos de Programa\ControlDePersonal\ScriptBackup\BackUpHuellometro.abp".

6. Plan de Recuperación

6.1Objetivos

Los objetivos del plan de recuperación son:

• Determinación de los procedimientos para respaldar las aplicaciones y datos

• Planificar la reactivación de la operación interrumpida producida por un desastre de los sistemas prioritarios

• Permanente mantenimiento y supervisión de los servicios, sistemas y aplicaciones

• Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre

6.2Alcance

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal de los sitios de cómputo y telecomunicaciones, basándose en los planes de emergencia y de respaldo.

La responsabilidad sobre el Plan de Recuperación es la Dirección de Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, comunicaciones y suministros.

6.3Activación

Decisión

Queda a juicio de la Dirección General de Administración y Finanzas determinar la activación del Plan de Contingencia.

Duración estimada

Dependiendo de la situación, se determinará la duración estimada de la interrupción del servicio.

Responsables

• Orden de Ejecución del Plan – Dirección General de Administración y Finanzas

• Supervisión General del Plan – Dirección de Administración

• Supervisión del Plan de Recuperación – Subdirección de Informática

• Tareas de Recuperación – Personal de tareas afines Aplicación del Plan El plan se aplicará en caso de que se suspenda el servicio por más de 48 hrs.

8.1 Acciones de recuperación

Las acciones de recuperación serán diseñadas para cada uno de los impactos mostrados anteriormente, definiendo asimismo los responsables de dichas actividades.

PLAN