PLAN DE CONTINGENCIA
DE INFORMÁTICA
de
Empresa_X

Preparado por

Hernán Moraga Müller

(E-Consulting Ltda.)

Introducción

Este manual es una guía, según los estándares de planes de contingencia informático, para que cada Gerente de Departamento de Empresa_X (en adelante E_X) defina y documente un Informe de Trabajo derivados de la definición del Plan de Contingencia de Informático.

El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes de su Departamento asociados con la plataforma tecnológica.

Entenderemos como infraestructura informática al hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio bajo su responsabilidad.

Entendemos también como procedimientos relevantes a la infraestructura informática a todas aquellas tareas que su personal realiza frecuentemente cuando interactúa con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

Un Plan de Contengencia considera una "Planificación de la Contingencia" así como un conjunto de "Actividades" las que buscan definir y cumplir metas que permitan a cada Departamento de E_X controlar el riesgo asociado a una contingencia.

Como Administrador Usted deberá leer acabadamente este instructivo, así como generar un "Plan de Trabajo para el Plan de Contingencia de IT" que involucre a los actores relevantes. Este plan de trabajo considera evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos. Naturalmente, en la generación del Plan de Trabajo de su Departamento es recomendable trabajar con sus reportes clave a fin de que sus recomendaciones cuenten con una base operativa sólida.

La Administración de E_X ya ha definido el Plan de Trabajo de Administración para el Plan de Contingencia de IT, en donde Usted es un miembro importante del Comité de Recuperación frente a desastres. Este comité se activará frente a una Contingencia, según la convocación del Gte. de Administración y Finanzas.

Sugerimos que su plan de trabajo respectivo, se genere como "una respuesta" a cada uno de los puntos que contiene esta Guía de Plan de Contingencia de E_X.

Agradecemos la diligencia que invertirá en este aspecto tan importante del manejo de contingencias informáticas, el que sabemos valorará en la eventualidad de una contingencia mayor.

1. Planificación de Contingencia

El Plan está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en prevision de desastres.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. Se ha considerado que para la compañía, la seguridad es un elemento básico para garantizar su supervivencia y entregar el mejor Servicio a sus Clientes, y por lo tanto, considera a la Información como uno de los activos más importantes de la Organización, lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia.

En este documento se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y recuperacion para enfrentar algún desastre. Por lo cual, se debe tomar como Guía para la definición de los procedimientos de seguridad de la Información que cada Departamento de la firma debe definir.

1.1 Actividades Asociadas

Las actividades consideradas en este documento son :

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

2. Análisis de Riesgos

Para realizar un análisis de los riegos, se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la compañía, y su importancia dentro del mecanismo de funcionamiento.

Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

2.1. Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal
b) Hardware
c) Software y utilitarios
d) Datos e información
e) Documentación
f) Suministro de energía eléctrica
g) Suministro de telecomunicaciones

2.2. Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, 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, llámese por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
c) Divulgacion de información a instancias fuera de la Compañía y que afecte su patrimonio estratégico Comercial y/o Institucional, sea mediante Robo o Infidencia.

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 se pierden en el acontecimiento.

Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

2.4. Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía asociadas al Centro de Operaciones Computacionales de E_X son:

Acceso no autorizado

Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).

Ruptura de las claves de acceso a los sistema computacionales

a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

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

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 causados por falla en los suministros de agua.
c) Fallas en los equipos de soporte:
- Por fallas causadas por la agresividad del ambiente
- Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por parte de la Compañía.
- Por fallas de los equipos de acondicionamiento atmosféricos necesarios para una adecuada operación de los equipos computacionales más sensibles.
- Por fallas de la comunicación.
- Por fallas en el tendido físico de la red local.
- Fallas en las telecomunicaciones con la fuerza de venta.
- Fallas en las telecomunicaciones con instalaciones externas.
- Por fallas de Central Telefónica.
- Por fallas de líneas de fax.

Fallas 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) Gerencia, supervisores de Red.
c) Administración de Ventas.
d) Personal de Administración de Bodegas-Despachos.

Pudiendo existir los siguientes inconvenientes:

a) Enfermedad.
b) Accidentes.
c) Renuncias.
d) Abandono de sus puestos de trabajo.
e) Otros imponderables.

Fallas de Hardware

a) Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.
b) Falla en el hardware de Red:
- Falla en los Switches.
- Falla en el cableado de la Red.

c) Falla en el Router.
d) Falla en el FireWall.

Incendios

2.5. Expectativa Anual de Daños

Para las pérdidas de información, se deben tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha sea menor o igual al necesario para la reposición del equipamiento que lo soporta.

3. Medidas Preventivas

3.1. Control de Accesos

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

a) Acceso físico de personas no autorizadas.
b) Acceso a la Red de PC's y Servidor.
c) Acceso restringuido a las librerías, programas, y datos.

3.2. Respaldos

En el punto Nro. 5 se describirá el alcance de esta importante medida preventiva.

4. Previsión de desastres Naturales

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Computación Central, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, el tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, diskettes, discos con información vital de respaldo de aquellos que se encuentren aun en las instalaciones de la compañía.

Adecuado 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:

a) UPS ..... de respaldo de actual servidor de Red o de estaciones críticas
b) UPS ..... de respaldo switches y/o HUB's

Seguridad Física del Personal

Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización de los softwares y elementos de soporte relevantes. Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

Seguridad de la Información

La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

5. Plan de Respaldo

El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o reestablecimiento. Todos los nuevos diseños de Sistemas, Proyectos o ambientes, tendrán sus propios Planes de Respaldo.

Respaldo de datos Vitales

Identificar las áreas para realizar respaldos:

a) Sistemas en Red.
b) Sistemas no conectados a Red.
c) Sitio WEB.

6. Plan de Recuperación

Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

1) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.
2) Planificar la reactivación dentro de las 12 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
3) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
4) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal del centro de procesamiento de la información, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputos y de los demás niveles.

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

Activacion del Plan

Decisión

Queda a juicio del Gerente de Administración y Finanzas determinar la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

Duración estimada

Los supervisores de cada area determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

Responsabilidades

* Orden de Ejecución del Plan : Gerencia de Admin. & Finanzas.
* Supervisión General de Plan : Empresa en convenio para Recuperación.
* Supervisión del Plan de Rec. : Supervisor(es) de Área(s).
* Abastecimiento (HW, SW) : Asistente de Administración.
* Tareas de Recuperación : Personal de tareas afines.

Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables).

Consideraciones Adicionales

1. **Plan debe ser probado una vez al año**

   Frente a la contingencia, se notifica al Gte. de Administración y Finanzas, quien evalúa en terreno el desastre, y estima tiempo de paro de operaciones mientras se reestablecen las operaciones.

   Si el tiempo estimado es mayor a 48 horas de iterrupción de operaciones en cualquier día salvo el fin de mes, en cuyo caso el tiempo estimado es mayor a 24 horas, entonces convoca al comité de Recurperación, compuesto por:

   * Supervisor de Plataforma : Empresa en convenio para Recuperación.
   * Supervisión del Plan de Rec. : Supervisor(es) de Área(s).
   * Abastecimiento (HW, SW) : Asistente de Administración.
   * Tareas de Recuperación : Personal de tareas afines.

   El comité determinará el lugar donde se instalará el sistema alternativo (red y servidor alquilado), pudiendo ser en las mismas premisas de E_X si las condiciones lo permiten, o en las premisas de la empresa con convenio recíproco de "Plan de Contingencia", si se contara con ella.

   Cada supervisor de área, tomará nota de las condiciones de la nueva plataforma operativa (sus capacidades y limitaciones, tanto en funcionalidad como en velocidad), e informará a su personal para operar de acuerdo a estas restricciones, durante el tiempo que se vuelve a reestabler el nivel de operaciones normales, tal como se experimenta durante el simulacro anual.

   El Gte. de Administración y Finanzas activará el contrato de Recuperación con la empresa respectiva, y dará instrucción a la Asistente de Administración para que emita una OC abierta para cubrir el arriendo o compra de HW o SW requerido para la instalación temporal de Servidor/red, así como para el Servidor/Red en proceso de restauración.

   Cada Gerente o Jefe con personal a cargo que esté involucrado en las tareas normales de la operación de E_X, designará según lo instruya el Gerente de Administración y Finanzas al personal necesario, a tareas afines.

2. **Todos los miembros del comité de recuperación deben estar informados y entrenados**, así como poseer una copia del Plan de Contingencia.

3. **Una copia del plan debería mantenerse almacenado off-site**, junto con los respaldos.

4. **Iniciación del Plan**

   - Gerencia de Administración y Finanzas debería ser notificada

   - Gerencia de Administración y Finazas contactará los equipos de recuperación

   - Cuartel General de Recuperación in-site a definir

   - Cuartel General de Recuperación Off-site a definir