PLAN DE CONTINGENCIA INFORMATICA

Son los procedimientos alternativos a la operación normal en la organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo de las operaciones, estando preparándonos para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

VENTAJAS POTENCIALES

El hecho de tener estructurado el plan de contingencias para el área de T.I tiene algunas ventajas potenciales que ayudan a prevenir o a disminuir el impacto de los siniestros. Algunas de estas ventajas permiten:

• Determinar acciones preventivas que reduzcan el grado de vulnerabilidad; por el conocimiento que se tiene de los sistemas automatizados de información.
• Cuantificar los riesgos potenciales a que están expuestos los sistemas de información.
• Facilitar la oportuna toma de decisiones ante anomalías o fallas.
• Contribuir a generar una cultura de seguridad y control en el área de T.I, haciendo énfasis en el manejo de la información.
• Asegurar la estabilidad operativa y de la organización, frente a la evidencia de un siniestro.
• Medir el grado de seguridad en los sistemas de información de la compañía

EL PLAN SE HA ESTRUCTURADO EN TRES GRANDES FASES:

1) Fase de Mitigación:
La Contraloría, asegura la conservación de su información vital y determina donde procesar sus trabajos críticos de procesamiento de datos, sistemas o aplicaciones automáticas críticas, en caso de falla de sus equipos o de los mismos aplicativos.
2) Fase de Emergencia:
Contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia.
3) Fase de Recuperación:
Permite restablecer las condiciones originales y operación normal de los sistemas de información en su conjunto.

Los cuales implican el desarrollo de las siguientes Etapas:

1) Revisión: comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones de la misma.
2) Valuación del impacto por interrupción del servicio: comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las

operaciones. Esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla el análisis de riesgos.
3) Implementación: se realizan actividades específicas para la reducción y eliminación de riesgos que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.

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 previsión 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 recuperación 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 compañía debe definir.

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.

Bienes susceptibles de un daño
a) Personal
b) Hardware

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

Daños

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) Divulgación de información a instancias fuera de la Compañía y que afecte su patrimonio estratégico comercial y/o Institucional, sea mediante Robo o Infidencia.

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.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía asociadas al área de T.I:

Acceso no autorizado:
a) Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
b) Ruptura de las claves de acceso al sistema computacionales.
c) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).
d) 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.

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.

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
a) Expectativa Anual de Daños
Para las pérdidas de información, se deben tomar las medidas de precaución 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

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 restringido a las librerías, programas, y datos.

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 el área de T.I, 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, 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.

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 del software 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 restablecimiento. 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

a) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.
b) Planificar la reactivación dentro de las 2 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
c) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
d) 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.

7. Otros Planes de Contingencia

a) Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la compañía, ante el evento de un incidente o catástrofe parcial y/o total.
b) El área de T.I debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre.
c) Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.
d) Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.
e) Existencia de documentación de los procedimientos manuales a seguir por las distintas áreas usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos.
f) Existencia de documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros.
g) Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta, capitalizando los resultados de la pruebas para el afinamiento del plan.
h) Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.
i) Disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.