RESUMEN DEL DOCUMETO

TITULO DEL DOCUMENTO

PLAN DE CONTINGENCIAS

SISTEMA DE SEGUIMIENTO Y CONTROL DE TRANSPORTACION

Autor del Documento:

Ing. Tomas Trejo/Carlos Diosdado

Aprobación del Documento:

Ing. Gustavo Licona Jiménez

Nota

Es responsabilidad del usuario de este documento para verificar que es la edición más actual. Cualquier documento impreso del sistema de control de documentos es una copia no controlada.

Historial de Cambios

Numero de Edición	Razón y Descripción de Cambio	Paginas Afectadas	Fecha de Actualización
1	• Edición del Documento	Todas	05/Marzo/2014
	•		

INDICE

1 INTRODUCCION

Este manual es una guía de plan de contingencia, para un Informe de Trabajos derivados de eventualidades las cuales pongan fuera de servicio el sistema de seguimiento y control de transportación.

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 nuestra responsabilidad.

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

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

2 OBJETIVO

El plan de contingencia establecerá un procedimiento escrito que indique las acciones principales para afrontar efectivamente una emergencia afín de reducir significativamente el impacto negativo.

3 ALCANCE

Sera aplicable a todo el personal involucrado en la operación del proyecto este alcance comprende desde el momento de la notificación de una emergencia hasta que está controlada.

4 NIVEL DE ESCALACION

En canso de alguna contingencia se deberá revisar la tabla anexa para hacer la escalación y reportar la situación o problema para buscar una solución.

PUESTO	NOMBRE	TELEFONO	CORREO
Supervisor Logística CTS-Transportes	Carlos Diosdado	(044)55 4762-7867 Nextel: 4598-9431 Id:62*12*71311	karloetienne@yahoo.com.mx
Gerente de Logística e Instalación Empresarial SA de CV	Tomas Trejo	55 5482-0935 Nextel: 4598-9432 Id: 62*12*52487	tom.trejo@logisticacts.com.mx

5 PLANIFICACION 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.

5.1 Actividades Asociadas

Las actividades consideradas en este documento son:

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

6 ANALISIS 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.

6.1. 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

6.2. 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) Divulgación de información a instancias fuera de la compañía y que afecte su patrimonio estratégico Comercial y/o Institucional, sea mediante robo o incidencia.

6.3. 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.

6.4. 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 **Logística e Instalación Empresarial S.A de C.V.** 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 al sistema computacionales
a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacional en uso (Virus, sabotaje).
b) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

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/Oficinas Pudiendo existir los siguientes inconvenientes:

1. Enfermedad.
2. Renuncias.
3. Vacaciones

Solución a estos inconvenientes:

Problema	Solución
Enfermedad o Accidente	Se deberá tener al personal capacitado y disponible para transmitir los conocimientos y así suplir y realizar momentáneamente las actividades del personal enfermo hasta su mejora.
Renuncias	En caso de alguna renuncia se deberá tener al personal capacitado y disponible para suplir esta ausencia para lo antes posible empezar a capacitar una nueva contratación.
Vacaciones	El personal deberá avisar con anticipación para hacerle saber a sus compañeros y transmitirles los conocimientos pertinentes para suplirlo y cubrir esa ausencia hasta su regreso.

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.
-Falla en el Router.
-Falla en el FireWall.

c) Incendios

6.5. 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.

7 MEDIDAS PREVENTIVAS

7.1. 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 restringido a las librerías, programas, y datos.

7.2. Respaldos

En el punto Nro. 9 se describirá el alcance de esta importante medida preventiva

8 PREVENCION DEL SISTEMA EN CASO 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.

9 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

Respaldo de datos Vitales
Identificar las áreas para realizar respaldos:

a) Sistemas en Red.
b) Sitio WEB.
c) Base de Datos
d) Documentación Impresa Física, (Esta se tiene resguardo en archivo muerto en Alcatel–Lucent, así mismo en CSL en su servidor de respaldo de escaneo.)

10 Plan de Recuperación

El Plan de recuperación se manejara de la siguiente manera en caso de un siniestro, teniendo un respaldo alterno.

Hosting México

Problema	Solución
Falla en Servicio	El sistema entrara automáticamente a un servidor de respaldo, alojado en el site de Logística e Instalación Empresarial SA de CV

Servidor de Respaldo

Problema	Solución
Falla en Servidor de Respaldo	1. Si se ha solucionado el problema en hosting México se realiza un interchange entre los servicios. 2. En caso contrario se levantara un servidor virtual alterno para levantar servicios WEB y cargar respaldo de BD y Sistema (El cual se ejecuta todos los viernes 00:00:00)
Falla en IP Fija	Se tendrá una IP Fija de respaldo la cual en caso de falla se re direccionara a esta.