



Tipo de Documento: MANUAL DE CONTINGENCIAS		Pertenece a: DEPARTAMENTO DE SISTEMAS		Fecha Elaboración AGOSTO 20 DE 2014
Proceso :				Fecha de Revisión SEPTIEMBRE 19 DE 2014
Elaborado por: JORGE RAMOS	Aprobado por: JORGE RAMOS	Autorizado por: JORGE RAMOS	No. Revisión 1	
Código y Título: MGA-004 MANUAL DE CONTINGENCIAS				

MANUAL DE CONTINGENCIAS

INTRODUCCION

Usualmente los controles de operación en el uso de las Tic's aplicados al proceso productivo permitirán elevar el desempeño en los sistemas previniendo fallas tanto de software, como de hardware y también humanas. Razón por la cual es de mucha importancia, mantener un nivel aceptable de operación para el buen funcionamiento de los Centros de Cómputo, parte Productiva y toda la infraestructura administrativa.

Plan de Contingencia

Se puede definir como un conjunto de procedimientos que permitan recuperar el estado normal de funcionamiento de toda la infraestructura informática y así poder prestar un servicio de calidad en el uso de Tic's.

El Plan de Contingencias implica realizar análisis de los posibles riesgos a los cuales se puede estar expuesto, tanto el equipo informático, como toda la información contenida en los diversos medios de almacenamiento.

Pese a todas las medidas de seguridad a implementar, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un *Programa de Recuperación ante Desastres*, el cual tendrá como objetivo principal, la restauración del servicio en forma rápida, eficiente y con el menor costo y pérdidas posibles. Se pueden presentar daños de diferentes niveles, por lo que se hace necesario suponer que el desastre ha sido total, motivo por el cual se debe establecer un *Plan de Contingencias lo más completo posible*.

Fases de un Plan de Contingencias:

- ☐ Plan de Reducción de Riesgos.
- ☐ Plan de Recuperación de Desastres.
- ☐ Actividades Previas al Desastre.
- ☐ Establecimiento del Plan de Acción.
- ☐ Actividades durante el Desastre.



- ☐ Plan de Emergencias.
- ☐ Actividades después del Desastre.
- ☐ Evaluación de Daños.
- ☐ Ejecución de Actividades
- ☐ Evaluación de Resultados.
- ☐ Retroalimentación del Plan de Acción.

Tipos de fallas a considerar en el Plan de Contingencias:

- ☐ Instalaciones eléctricas.
- ☐ Bases de datos y aplicativos.
- ☐ Problemas con el servidor.
- ☐ Estaciones de trabajo y periféricos.
- ☐ Redes e Internet.

Análisis de Riesgos

El análisis de riesgos supone más que el hecho de observar la posibilidad de que ocurran cosas negativas. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado. Teniendo en cuenta la frecuencia con que puede ocurrir un desastre, nivel de daños y las consecuencias generales.

En la fase de evaluación de riesgos se debe priorizar, que se va a proteger, a que se puede enfrentar: terremotos, incendio, inundación, robos, vandalismo, fallas en los equipos, eliminación accidental de archivos, virus. Como también determinar el nivel de riesgo: bajo, muy bajo, medio, alto y muy alto.

Sistema Actual: con el propósito de salvaguardar toda su infraestructura tecnológica e informática de Avícola Triple A S.A.S., debe contemplar los siguientes aspectos en su labor diaria:

- ☐ Hacer copia casi diaria de los archivos que son vitales para la Organización.
- ☐ Control de acceso a las instalaciones de la Organización.
- ☐ Realizar el mantenimiento preventivo de forma regular.
- ☐ Se debe prohibir el ingreso de comidas y bebidas en las Instalaciones informáticas.
- ☐ Mantener estos espacios libres de humo de tabaco, (Prohibido Fumar).
- ☐ Realizar limpieza constante, evitando la acumulación de polvo.
- ☐ Mantener actualizado el programa antivirus.
- ☐ Permitir solo el acceso a las instalaciones informáticas en horarios programados o con la presencia de un supervisor o monitor.

Plan de Recuperación



Es de vital importancia definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre que afecten la infraestructura tecnológica tanto productiva como administrativa.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar y poner en marcha, en el menor tiempo posible el proceso perdido.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. Estos procedimientos estarán a cargo del personal del Departamento de Sistemas.

Las actividades a realizar en un Plan de Recuperación se pueden clasificar en tres etapas:

1. Actividades previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de los activos de la infraestructura tecnológica de la Organización, que nos aseguren un proceso de Recuperación con el menor costo posible.

Establecimiento del Plan de Acción

Equipos de Cómputo: Es necesario realizar un inventario actualizado de los equipos, especificando su contenido (software y licencias).

Respaldos de Información o Backups: Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución del Software y/o Sistemas operativos. Copias del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos), Software de uso diario, herramientas de trabajo, Bases de Datos, Aplicativos.

- ☐ Uso obligatorio de un registro detallado y control de los Backups.
- ☐ Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- ☐ Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar.
- ☐ Pruebas periódicas de los Backups (Restore), verificando su funcionalidad.

2. Actividades durante el Desastre

Una vez presentada la Contingencia, Falla o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

Plan de Emergencias



Se establecen las acciones a realizar cuando se presente una falla o desastre, así como la coordinación y comunicación de las mismas.

Es muy conveniente prever los posibles escenarios de ocurrencia del Siniestro, el cual se puede dar en horario diurno, como nocturno.

El plan debe contemplar la participación y actividades a realizar por todas las personas que se pueden encontrar presentes en el área de ocurrencia, detallando, salidas de emergencia, vías de evacuación, señalización y demarcación de las señales de auxilio (extintores, caja de breakers, linternas y lámparas de mano, números telefónicos de emergencia y nombres de funcionarios a contactar).

Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal, para minimizar costos se puede aprovechar fechas de recarga de extintores, charlas de los proveedores, ARP, etc., (Simulacros).

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen todos los funcionarios, directivos, administrativos y asistenciales.

3. Actividades después del Desastre

Después de ocurrido el Desastre es necesario realizar:

☐ *Evaluación de Daños:* Inmediatamente después de concluido el desastre, de deberá evaluar la magnitud del daño producido, equipos no funcionales, cuales se pueden recuperar y estimación del tiempo.

☐ *Ejecución de Actividades:* La recuperación y puesta en marcha del servicio afectado, se realizara en dos fases, la primera restablecer el servicio usando los recursos propios (Equipos de respaldo) y la segunda con el apoyo de las demás empresas del grupo, proveedores y entes tanto gubernamentales como no gubernamentales .

☐ *Evaluación de Resultados:* Finalizada las fases de recuperación, se debe evaluar objetivamente las actividades realizadas, porcentaje de eficiencia y efectividad, tiempo, inconvenientes, colaboración y apoyo.

☐ *Retroalimentación del Plan de Acción:* Con la evaluación de resultados, se debe actualizar el plan de acción original, mejorando las actividades más complejas y reforzando las que respondieron adecuadamente.

Amenazas



□ *Incendio*: el fuego es una de las principales amenazas y causas de desastre, contra todo tipo de infraestructuras físicas. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los humanos.

□ *Extintores manuales*: Cuando no se cuenta con sistemas automáticos contra incendios, la alternativa más adecuada es la de usar extintores anti fuego, pero se debe tener en cuenta el tipo de material que se está consumiendo por el fuego (papel, madera, plástico, líquidos inflamables). Se recomienda capacitar al personal sobre el manejo adecuado de estos dispositivos y llevar control de las recargas y fechas de caducidad.

□ *Inundaciones*: Daños por agua pueden ocurrir como resultado de goteras y filtraciones del techo, goteras de tuberías o del aire acondicionado cerca a equipos electrónicos.

□ *Terremotos*: Catástrofe natural se pueden presentar en cualquier momento y sin previo aviso, por tanto es de suma importancia incluir en el plan de acción, recomendaciones a seguir, dando prioridad a salvaguardar la vida de los funcionarios de la Organización.

□ *Instalaciones eléctricas*: Para que funcionen adecuadamente, los computadores de escritorio necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible. Por lo general los computadores personales toman la electricidad de los circuitos eléctricos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una corriente alterna (AC), ya que alterna el positivo con el negativo. La mayor parte de los computadores incluyen un elemento denominado fuente de alimentación, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes del equipo informático. Se recomienda tener redes eléctricas reguladas y contar con dispositivos reguladores, estabilizadores de potencia y ups.

□ *Bases de Datos y aplicativos*: La Red de datos es la que permite transmitir información de un computador a otro. La estructura de Red que posee Avícola Triple A S.A.S. es cliente/servidor, por lo que el servidor es uno de los componentes importantes de la Red. El cableado es estructurado y topología es estrella, y también se cuenta con tecnología inalámbrica. El elemento activo de comunicaciones es el switch de datos, conectado a un router, el cual permite trasladar a cada nodo (host) los paquetes de datos para que se intercambie información en toda la Red. Es una Red de Área Local (LAN), lo que limita su



cobertura de servicios estrictamente, sin embargo, a través de los proveedores de servicios (Level3, Claro, Telefónica, Une, Etb), se puede tener acceso a otros sitios como las Oficinas de otras ciudades, las Granjas e Internet. Es por ello, que debe ser de suma importancia el poder detectar las fallas en la red de datos, ya que de esa forma se permitirá prestar en un cien por ciento (100%) de sus recursos disponibles a la Organización.

□ *Cableado estructurado:* El cableado estructurado es la plataforma de comunicaciones en la red que posee Avícola Triple A S.A.S., este cableado usualmente es UTP (cable de par trenzado no apantallado) y su importancia radica que es el medio de transmisión por el cual se transmite la información de un nodo a otro. Es posible que por problemas de cableado, se tengan problemas de conectividad, sin embargo, en la mayoría de casos, el cableado entregado debe estar debidamente certificado por el proveedor y supervisada por el Departamento de Sistemas.

□ *Equipos de comunicación:* El elemento activo de comunicación que se utiliza en la Organización es el switch de datos, el cual es un elemento que permite la transmisión de tramas (paquetes de datos) desde la tarjeta de Red del Transmisor a la tarjeta de Red del Receptor.

Este elemento activo de comunicaciones es de suma importancia, y no debe estar apagado, ya que en ese momento se tendría una caída en la Red de datos. Usualmente estos elementos activos de comunicación son de 8, 16, 24 o 48 puertos, los cuales poseen unos led (indicadores visuales) que señalan el estado de funcionamiento de cada puerto, en el momento en que está activo el puerto, el led del mismo debe estar encendido. Cada puerto conecta a un nodo o computador por lo que una de las formas de detectar que hay falla de comunicación es observar el puerto, obviamente, cada puerto debe estar relacionado con el punto de Red respectivo.

Detección de fallas

□ *Por problemas de energía eléctrica:* Si hay problemas de suministro de fluido eléctrico, posiblemente se apague el elemento activo de comunicaciones, por lo tanto, el resultado será una caída en la red de datos.

□ *Por problemas en el switch de datos:* Si el elemento activo tiene una falla de tipo eléctrico este no encenderá y se tendrá un problema similar al caso anterior.

□ *Por problemas de puerto:* es posible que por alguna variación de voltaje, se queme una cantidad limitada de puertos, se recomienda verificar los led que indican conectividad.

□ *Por problemas en la tarjeta de Red:* puede existir la posibilidad de que la tarjeta de Red este fallando, una forma rápida de verificar su funcionamiento es identificar



si el led de la tarjeta de Red está funcionando, en caso contrario es posible que la NIC no esté operando adecuadamente. Otro caso probable es que este desactivado desde el sistema operativo.

Recomendaciones

□ En el caso de falla en el suministro de energía eléctrica, se recomienda colocar un UPS dedicado para el elemento activo, además, si Avícola Triple A S.A.S. tiene los recursos, se recomienda que la UPS tenga un regulador de voltaje integrado para evitar picos de voltaje.

[illegible]

problemas de switch de datos: Si el responsable del Departamento dectado el puerto esta encendido, si al realizar un ping al Server, este no contesta, entonces, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, si al realizar un ping al Server y este contesta, entonces, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.

Dor problemas de switch de datos: Si el responsable del Departamento dictado el puerto esta encendido, si al realizar un ping al Server, este no contesta, entonces, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, si al realizar un ping al Server y este contesta, entonces, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.

Dor problemas de switch de datos: Si el responsable del Departamento dictado el puerto esta encendido, si al realizar un ping al Server, este no contesta, entonces, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, si al realizar un ping al Server y este contesta, entonces, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.



□ Por problemas en la tarjeta de Red: La tarjeta puede estar deshabilitada desde el Sistema Operativo, será necesario revisar si este está habilitado o no, en el caso que este deshabilitado, habilitarlo inmediatamente desde el sistema operativo. Si está habilitada la tarjeta de red y no hay comunicación, será necesario reinstalar el “driver” de la tarjeta de Red, o revisar si posee dirección Ip, en caso persiste el problema, favor llamar al Departamento de Sistemas *Servidor y Estaciones de trabajo*.

Uno de los elementos importantes en una Red de datos es el Servidor de Aplicaciones, el cual puede ser utilizado como Controlador de Dominio, para uso de la ERP Corporativa, como un servidor de correo, servidor proxy, servidor de Impresoras, de Archivos Compartidos y Backups, como servidor de Seguridad y también como servidor Web.

El servidor puede presentar problemas de configuración (DNS, DHCP, Directorio Activo, IIS), de comunicaciones (protocolos), de hardware (Disco duro, tarjeta de red, motherboard, memoria RAM, fuente de poder, teclado, mouse).

Redes e Internet

El servicio de Redes e Internet permite tener acceso a los otros puntos productivos de la Organización como Granjas, Planta de Alimentos, Oficinas en otras ciudades y también a los recursos de Internet tales como bibliotecas electrónicas, bases de datos, contacto con clientes y proveedores, cursos en línea, correos electrónicos, chat, compartir archivos, videoconferencia.

□ Los componentes del servicio de Datos e Internet: firewall, routers y conectividad dado por el ISP (Telmex), del Directorio activo, DHCP automático.

□ El Router es el elemento activo que permite comunicar la red de datos al servidor de comunicaciones, al proveedor de Internet y a la red de área local (LAN).

ELABORADO POR:

Jorge Ramos Sistemas Avícola Triple A S.A.S.

APROBADO POR: