ESCUELA MILITAR DE INGENIERÍA
MCAL. ANTONIO JOSÉ DE SUCRE
BOLIVIA

MANUALES DE CONTINGENCIAS

DISEÑO DEL CENTRO DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA BAJO ESTÁNDARES INTERNACIONALES.

CASO: DIRECCIÓN NACIONAL DE INFORMÁTICA – ESCUELA MILITAR DE INGENIERÍA.

ERICK ROLANDO PALENQUE RIOS

LA PAZ, 2016

ÍNDICE DE CONTENIDO

Pag.

MANUAL DE CONTINGENCIAS CSIRT-EMI

1.1 INTRODUCCIÓN

En nuestra época, llamada la era contemporánea y también la edad de la informática o cibernética, se ha hecho imprescindible que todo tipo de negocio cuente con computadoras y sistemas de información, ya que sin ellos el proceso del negocio se volvería muy complejo por los requerimientos modernos de agilidad y confiabilidad de la información.

Por ningún motivo, la Escuela Militar de Ingeniería se encuentra ajena a este tipo de realidad, es más, por su naturaleza, está en la obligación de contar con herramientas capaces de ofrecer la seguridad que necesita la información académica y administrativa de esta casa de estudios superiores.

La realidad expuesta determina que la institución tenga en la actualidad montada una estructura informática que contiene elementos físicos (Servidor, terminales, U.P.S.s, impresoras, módems, tipología de red con sus componentes) y elementos lógicos (programas de aplicación administrativos y financieros). Estos componentes exigen una serie de cuidados y medidas destinados a ofrecer la seguridad necesaria en su uso y por lo tanto de la información que procesan.

El plan de contingencias es una estrategia constituida por un conjunto de recursos ideados con el propósito de servir de respaldo, contando con una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios efectuados por una paralización total de la capacidad operativa de la institución.

El presente manual debe constituirse en la lectura básica de todo el personal de la Escuela Militar de Ingeniería y su observancia y cumplimiento es responsabilidad de los órganos de la Dirección.

1.2 OBJETIVO DEL MANUAL.

Este manual tiene el objetivo de normar los procedimientos a emplear en el Centro de Respuesta a Incidentes de Seguridad Informatica, para poder Proteger los activos de información críticos de la Escuela Militar de Ingeniería y promover el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad a los diferentes Departamentos y/o secciones de esta Casa de estudios Superiores.

Este documento contiene, todos los procedimientos y responsabilidades necesarios para garantizar el buen funcionamiento de la estructura informática de la Escuela Militar de Ingeniería, estableciendo normas procedimentales que definen la forma en la que se debe mantener (seguridad) y corregir errores y problemas (contingencias).

1.3 DEFINICIÓN DE TERMINOLOGÍA

Para la buena comprensión del manual, es necesario definir algunos términos que usaremos con frecuencia a través del desarrollo de los temas.

RED DE COMPUTADORAS: Es un conjunto finito de computadoras interconectadas con el fin de aprovechar recursos como: información de proceso común, impresoras, comunicaciones, etc.

SERVIDOR: Es la computadora principal de la red de datos. Se encarga de almacenar y distribuir en forma coherente y sincronizada la información requerida por todos y cada uno de los usuarios; también es la que contiene el sistema operativo de red.

SERVIDOR DE ARCHIVOS: Es la computadora principal o secundaria de una red de datos. Se encarga de almacenar la información de los diferentes usuarios y puede o no tener un sistema operativo de red diferente al servidor principal

SISTEMA OPERATIVO DE RED: Es el conjunto de programas encargado de administrar la operación del Servidor principal en todas sus actividades, que en forma enunciativa y no limitativa son: Almacenar la información y distribuirla según

requerimiento de los usuarios de la red, administrar los usuarios en aspectos como la distribución de derechos de acceso, reconocer la distribución de los recursos compartidos, etc.

U.P.S (Uninterrumpible Power Suply ó Fuente de Poder Ininterrumpida): Es un equipo que funciona en base a baterías acumuladoras de energía, que permite mantener la alimentación de la energía eléctrica a los equipos que se le conectan en caso de interrupción de la fuente externa.

HUB: Aparato distribuidor de los paquetes de señales de la red. A este dispositivo se conectan los servidores y las terminales, encargándose de mandar la señal a la terminal que corresponde y pasar la que proviene de estas últimas al primero indicando de quién procede. Se utiliza en tipologías estrella.

TOPOLOGÍA ESTRELLA, CABLE MULTIPAR (de 6 u 8 hilos), CONECTORES R.J-45: Conjunto de accesorios necesarios para lograr conectar una red de computadoras a través de cable multipar a velocidades que oscilan entre 2 y 100 Mega bits por segundo. Las condiciones de seguridad en la transmisión de datos de este tipo de red son bastante superiores a las del tipo bus, por lo que se la utiliza entre los HUBs y las terminales, aunque se debe renunciar, en algunos casos, a la velocidad, ya que es un poco más lenta en su respuesta.

DISCO DURO ó HARD DRIVE: Medio de almacenamiento masivo que se utiliza en la actualidad en todas las computadoras existentes. En este dispositivo se almacenan todos los datos que se procesa

1.4 ALCANCE DEL MANUAL

El manual se centra básicamente en la descripción de los procedimientos estándar necesarios para realizar el objetivo descrito en párrafos anteriores.

Los responsables de aplicar y hacer aplicar todas y cada una de las recomendaciones son:

- ✓ Rector
- ✓ Director de la Unidad Académica
- ✓ Director Nacional de Informatica
- ✓ Jefes de Departamento de la DNI.
- ✓ Usuarios

2.1 POLÍTICAS GENERALES DE PROTECCIÓN Y SEGURIDAD.

2.1.1 Proteger la instalación de personas no autorizadas.

- ✓ Definir procedimientos adecuados con la finalidad de minimizar las acciones aleatorias e incrementar los aspectos de seguridad, de forma tal que los eventos que pudieran ocasionar los terceros sean reducidos al mínimo

- ✓ Proteger el sistema con palabras clave para el ingreso a equipos y a la red.

2.1.2 Contar con Software de Base de Probada Calidad, Original y Respaldo con un Contrato de Mantenimiento.

Verificar el buen funcionamiento del software de base y los sistemas y subsistemas que se manejan, en lo posible desarrollar localmente, o en su defecto, con un servicio de soporte y mantenimiento. En este sentido se debe contar con un contrato que asegure los servicios.

2.1.3 Contar con Hardware de Alta Confianza.

Adquirir equipos de marca reconocida que garanticen la mejor calidad de la operación. (Fundamentarse en rigurosos controles de calidad)

2.1.4 Contar con Equipos de Alta Disponibilidad.

Alta disponibilidad: es la propiedad que tiene un sistema de mantener su operación ante contingencias. Es decir, permite la operación continúa del sistema, independientemente de las posibles fallas del Servidor, los datos o desperfectos de la red. Se recomienda un

servidor de respaldo y un equipo configurado para funcionar con el sistema financiero y la red.

2.1.5 Contar con Software y Hardware de plataforma abierta.

Se debe tener cuidado tanto en el software de cómo en el hardware que los productos sean compatibles y en la medida de lo posible de plataforma abierta, es decir, puedan aceptar componentes de diferentes fabricantes para construir el todo y que el software sea compatible bajo cualquier sistema operativo o entorno de funcionamiento

- ✓ Contar con ambientes para el área del Centro de Respuestas a Incidentes de Seguridad Informática.

- ✓ El área de Centro de Respuestas a Incidentes de Seguridad Informática, estará instalado de tal forma que las computadoras principales están en un sitio separado y resguardado

- ✓ El área del Centro de Respuestas a Incidentes de Seguridad Informática tiene la obligación de tener un extinguidor de incendios en el lugar

- ✓ El área del Centro de Respuestas a Incidentes de Seguridad Informática debe contar con gabinetes de cableado y paneles de distribución

- ✓ El área del Centro de Respuestas a Incidentes de Seguridad Informática debe contar con paneles de distribución de la energía eléctrica con UPS.

2.1.6 Contar con una Red Eléctrica Adecuada y Moderna.

Se cuenta con un circuito eléctrico aterrado diferenciado para equipos de computación en toda la institución, en las secciones con mas de tres equipos se cuenta con protección global con UPS, de tal forma que cuando haya cualquier desperfecto eléctrico, la red eléctrica se corte inmediatamente para minimizar problemas que pueda acarrear a siniestros

3.1 SITUACIONES CONTROLABLES.

Las situaciones controlables a través de este manual provienen de dos tipos de agentes, descritos a continuación.

3.1.1 Agentes Externos.

Agentes externos son aquellos en los cuáles no tiene ninguna injerencia las acciones de la Escuela Militar de Ingeniería ni de su personal. Son hechos generados en fuentes ajenas a nosotros y que nada o casi nada podemos hacer para evitar que sucedan.

Los agentes externos que pueden influir en el buen desenvolvimiento de la actividad académica y administrativa de la estructura informática de la Escuela Militar de Ingeniería son los siguientes:

3.1.1.1 Cortes de Energía Eléctrica

Una de las causas más comunes que existe dentro de la gama de posibilidades de agentes externos y de hecho una de las más peligrosas.

Los peligros que puede traer van desde la simple molestia por interrumpir las actividades de los usuarios, continuando por la pérdida de información en línea, hasta llegar a daños irreparables tanto en la información, como en los medios de almacenamiento.

Normas Preventiva

Como seguridad para el hecho es imprescindible el uso de U.P.S.s, ya sean centrales (una para todos los equipos) o individuales (una por equipo).

Que Hacer en Caso de Corte de Energía Eléctrica.

- Apagar los equipos conectados a la UPS, dejando encendidos los estrictamente necesarios para la atención al cliente

- Si el corte de energía se prolonga por un tiempo considerable:

  - ✓ Comunicar a todas las secciones que se apagará el Servidor
  - ✓ Apagar el Servidor
  - ✓ Instruir la puesta en OF del Switch de los cortapicos de todos los equipos de la institución

Una vez Restablecida la Energía Eléctrica, se Debe:

- ✓ Verificar la integridad física de terminales, servidor, UPS, estabilizadores, impresoras y demás componentes físicos
- ✓ En caso de daño de algún componente, acudir a los distribuidores oficiales, para la reparación o sustitución del mismo.
- ✓ Reiniciar el sistema de acuerdo al procedimiento de inicio de sistema

3.1.1.2 Descargas Eléctricas.

Este tipo de hecho es de los más raros, pero también de los más peligrosos que pueden ocurrir. Está ocasionado, ya sea por rayos o carga estática fuerte en el medio.

El alcance de los daños que puede causar es amplio:

Quemado de tarjetas de comunicación.

Quemado de tarjetas madres.

Quemado de monitores

Quemado de cables

Explosiones y/o fuego.

Pérdida de discos duros.

Pérdida de datos.

Normas Preventivas.

Las normas de seguridad exigen contar imprescindiblemente con un Sistema Eléctrico Aterrado. Es muy importante que el Sistema de Tierra esté bien calculado para la carga de energía que se utiliza, ya que sino, es posible que funcione más bien como conducto de energía externa.

Que hacer en caso de Descargas Eléctricas?

- ✓ Informar a los usuarios que se realizará la desconexión del servidor
- ✓ Desconectar el servidor
- ✓ Instruir la desconexión de los equipos de la red de alimentación eléctrica.
- ✓ Esperar para proceder al encendido de todos lo equipos, luego de la finalización de la tormenta eléctrica.

3.1.1.3 Incendios.

El término es explícito por sí mismo. Los daños que puede causar varían en función a la exposición que hayan tenido los equipos al calor.

Normas Preventivas

- ✓ La existencia de extinguidores adecuados es obligatoria para poder actuar lo más rápido posible en la contención del fuego, más aún, cuando a veces es difícil conseguir asistencia inmediata por parte de los bomberos.
- ✓ Es posible, que si el incendio fuera masivo, no quede ni una sola copia de seguridad de la información confiable en la Institución, para lo cuál es aconsejable, almacenar las copias mensuales, semestrales y anuales en cajas

de seguridad de otras Instituciones especializadas.

Que Hacer en Caso de Incendios?

- ✓ Recurrir al extinguidor de fuego más cercano y proceder de acuerdo al procedimiento para manejo de extinguidores

- ✓ Verificar los daños ocasionados y proceder de acuerdo a lo siguiente:

    - Si existen daños graves en los Servidores Principales, será necesario restaurar las últimas copias de seguridad de forma inmediata de acuerdo al procedimiento de restauración de backups.

    - Si se hubieran realizado transacciones posteriores a la última copia de seguridad, reconstruir la base de datos, tomando como referencia la documentación existente.

    - En el caso de una leve y breve exposición, es posible que no hayan mayores problemas, salvo el reemplazo de los cables de comunicación;

    - En casos extremos resultará en la pérdida irreparable de toda la infraestructura informática de la Institución. En este caso se deberá recurrir a la implementación de un nuevos servidores y la restauración de la última copia de seguridad existente

3.1.1.4 Inundaciones.

Otra contingencia proveniente de agentes externos a la Institución, son las Inundaciones. Producidas ya sea por fuertes lluvias o fallas en las redes de distribución o drenaje.

Normas Preventivas

- ✓ La estructura del o los edificios debe estar diseñada para evitar la acumulación de líquidos.

- ✓ Se debe revisar periódicamente la red interna de agua y drenaje para evitar tapaduras, fugas, etc.

- ✓ Es posible, si la inundación fuera masiva, no quede ni una sola copia de seguridad confiable en la Institución, para lo cuál es aconsejable, almacenar las copias mensuales semestrales y anuales en cajas de seguridad de otras Instituciones especializadas.

Que Hacer en Caso de Inundaciones.

- Escurrir el o los ambientes afectados

- Dejar secar todos los equipos sin encenderlos.

- ✓ Sin embargo, es posible que debido a la humedad hayan habido cortes en los circuitos de energía que hayan ocasionado problemas parecidos a los que ocurren cuando hay Cortes Abruptos de Energía o Descargas Eléctricas. En caso de detectarse el problema cuando está apareciendo:

  - Se deberán apagar de todos los equipos eléctricos y electrónicos

  - Proceder a desconectarlos de las tomas de corriente en forma inmediata.

- ✓ Verificar los daños ocasionados y proceder de acuerdo a lo siguiente:

  - Si existen daños graves en el Servidor Principal, será necesario restaurar la última copia de seguridad de forma inmediata de acuerdo al procedimiento de restauración de backups.

  - Si se hubieran realizado transacciones posteriores a las últimas copias de seguridad, reconstruir la base de datos, tomando como referencia la documentación existente.

- ✓ En casos extremos resultará en la pérdida irreparable de toda la infraestructura informática de la Institución. En este caso se deberá recurrir a la implementación

de nuevos servidores y la restauración de las últimas copias de seguridad existente.

3.1.1.5 Robo y Violencia.

Nunca existe seguridad plena de que un robo no pueda ocurrir. Las computadoras son artículos bastante codiciados por los ladrones, por lo que, adicionalmente a un robo de dinero, es muy factible que se lleven computadoras. Dentro de este contexto, puede desaparecer hasta el Servidor. Por motivos ajenos a la lógica, también es factible que puedan existir daños a causa de golpes infringidos contra el equipamiento. Donde si podrán existir daños de diversa índole. Los daños que puede causar este tipo de circunstancias, se reducen, principalmente, a la pérdida de información y/o daños materiales en computadoras y cables.

Normas Preventivas.

Las normas preventivas que se pueden mencionar giran alrededor de contar con edificios diseñados para ofrecer la mayor seguridad posible

- ✓ Contar con guardia permanente
- ✓ Asegurar todas las instalaciones, incluidos todos los equipos.
- ✓ Es posible, si el robo fuera masivo o dirigido a eliminar información, no quede ni una sola copia confiable en la Institución, para lo cual es aconsejable, almacenar las copias mensuales, semestrales y anuales en cajas de seguridad de otras Instituciones especializadas.

Que Hacer en Caso de Robo y Violencia

- ✓ Efectuar un análisis para determinar el alcance real de los daños.
- ✓ Si existen problemas en los medios de almacenamiento o en partes físicas, éstos deben ser reemplazados, sin arriesgarse a mantenerlos, ya que en la mayoría de los casos, se vuelven inestables.

- ✓ Si la información fuera afectada, inmediatamente se procederá a restaurar la última copia de seguridad disponible.

- ✓ Si se hubieran realizado transacciones posteriores a la última copia de seguridad, reconstruir la base de datos, tomando como referencia la documentación existente.

3.1.1.6 Interrupción en el Servicio de Comunicaciones.

La interrupción del servicio de comunicaciones puede ocasionarnos serios problemas ocasionando la no emisión y/o recepción de información.

La información no emitida

- ✓ Cartas
- ✓ Fax
- ✓ Transacciones
- ✓ Notas
- ✓ Disposiciones

La información no recibida:

- ✓ Cartas
- ✓ Circulares
- ✓ Reportes
- ✓ Informes
- ✓ Actualizaciones de Software

Sin embargo también podría afectar el servicio prestado al cliente con nuestra unidad de servicios.

Normas Preventivas

Para el caso de la suspensión de atención al cliente, es aconsejable tener un Centro de Procesamiento de Datos Alternativo.

Que Hacer en Caso de Interrupción de Comunicaciones.

- ✓ Consultar la causa de la falla con la institución y en caso necesario solicitar una Carta en la que se explique los motivos, tiempos y duración de la suspensión

- ✓ Si la suspensión del servicio se prolonga mas allá del plazo establecido para el envío de información explicando la razón de no enviar adjuntando en lo posible la carta de la institución proveedora

- ✓ Si el problema fuera interno, solicitar servicio técnico para la revisión de las conexiones

3.1.2 Agentes Internos.

Existen una serie de posibles causas generadas dentro la misma institución, que son capaces de crear dificultades o contingencias.

Para una mejor comprensión, las dividiremos en dos grandes grupos, las de origen en elementos físicos (hardware) y en los lógicos (software). Sin embargo, antes, queremos hacer referencia a una excepción en estos dos grupos. Una contingencia de origen interno que es bastante peligrosa para la Institución en general:

Motivos Físicos.

Describiremos los más importantes sucesos que pueden ocurrir por elementos físicos relacionados a la operación informática:

3.1.2.1 Corte de Conexión de Red

Un problema bastante común, generado por la interrupción de la comunicación una terminal y el Servidor a través de la interrupción de la conexión del cable de la red local o de la línea en la comunicación remota.

Los problemas que traerá serán la interrupción de la ejecución de los programas que estaba corriendo la terminal, con la inminente pérdida de los datos que se estaban procesando.

Las causas de esta contingencia pueden ser que:

- ✓ Alguien haya pateado el cable.
- ✓ Se haya pisado el cable.
- ✓ El cable se haya cortado físicamente.
- ✓ Una fuente de energía aledaña al cable haya generado una campo de impedancia haya interferido la comunicación.
- ✓ Otros que por su acción no permitan el paso de la energía a través del cable.

Normas Preventivas

- ✓ Proteger todos los tramos de cable, especialmente aquellos que estén al paso de las personas y/o objetos
- ✓ Asegurarse que no existan ningún tipo de fuentes de energía cercanos al cable
- ✓ Proteger los racks de distribución de red

Que Hacer en Caso de Cortes de Conexión

- ✓ Si existen problemas en los tramos de cable, éstos deben ser reemplazados, sin arriesgarse a mantenerlos, ya que en la mayoría de los casos, se vuelven inestables o inservibles.
- ✓ Verificar que el Switch esté encendido
- ✓ Verificar las conexiones de cable de red en el Switch
- ✓ Verificar la conexión del cable de red en la roseta
- ✓ Reconfigurar la tarjeta de red

- ✓ Reiniciar el equipo

3.1.2.2 Bloqueo del Servidor.

Dentro de los problemas de operación de las computadoras integrantes de la red, dividiremos aquellos que ocurren específicamente en el Servidor de Archivos y las Terminales, ya que cada uno de ellos tiene tratamientos diferentes en relación a la importancia de los equipos.

Normas Preventivas

- ✓ Contar con un servicio de mantenimiento preventivo de hardware y software por espacios semestrales con instituciones especializadas

- ✓ Capacitar al personal del área de Servidores.

Que Hacer en Caso de Bloqueo del Servidor

- ✓ Si no enciende, poner el switch en Apagado y revisar las conexiones internas y externas, luego encenderlo

- ✓ Si enciende y el sistema operativo no sube, solicitar asistencia técnica para solucionar el problema

- ✓ Si se agotaron las acciones recomendadas, elaborar el informe a Dirección solicitando la Asistencia por técnicos especializados.

- ✓ Iniciar actividades con el servidor auxiliar.

- ✓ Configurar en las terminales el emulador con la dirección IP del Servidor Auxiliar.

3.2.2.3 Fallas Técnicas en el Servidor

- ✓ **Daño en la Tarjeta de Red:** Es factible que la tarjeta de red que posee el Servidor de Archivos se haya dañado por motivos inherentes a picos fuertes de energía, fallas de fabricación, etc.

Los efectos (en orden de mayor a menor) de esas causas son: La imposibilidad de comunicarse a través de las terminales conectadas a esa(s) tarjeta(s), cortes repentinos en la comunicación y pérdida de datos.

- ✓ **Daño en el C.P.U:** Es factible que la tarjeta madre del equipo, ó los procesadores, periféricos, etc. que posee el Servidor de Archivos se haya(n) dañado por motivos inherentes a picos fuertes de energía, fallas de fabricación, vibraciones, etc,

Los efectos (en orden de mayor a menor) de esas causas son:

- ✓ La imposibilidad de arrancar el equipo
- ✓ Fallas en la comunicación a las terminales conectadas al Servidor de Archivos
- ✓ Cortes repentinos durante el trabajo
- ✓ Reportes del BIOS de errores
- ✓ Aparición de resultados absurdos en los cálculos
- ✓ Desaparición inexplicada de datos, etc.

Normas Preventivas

- ✓ Asegurarse que la alimentación de energía al Servidor de Archivos sea constante y estabilizada
- ✓ Que la calidad de la tarjeta de red esté garantizada.
- ✓ Que la calidad de los componentes internos esté garantizada.
- ✓ Que la seguridad que se establezca en torno al ambiente físico donde se encuentre el Servidor de Archivos sea la debida.
- ✓ Evitar fuentes magnéticas importantes en las cercanías del equipo.

- ✓ Proteger toda la red con una buena instalación de U.P.S.s y tierra.

- ✓ Contar con servicio de mantenimiento preventivo y correctivo de hardware con instituciones especializadas por espacios semestrales.

- ✓ Mantener un ambiente acondicionado.

- ✓ Es aconsejable, almacenar las copias mensuales, semestrales y anuales en cajas de seguridad de otras Instituciones especializadas.

Que Hacer en Caso de Fallas Técnicas en el Servidor.

- ✓ Habilitar el servidor de respaldo existente con la última copia de seguridad disponible siguiendo el procedimiento de restauración de Backup

- ✓ Si se habrían realizado transacciones posteriores a la copia de seguridad, no quedará otra opción que introducir todas las operaciones faltantes hasta ponerse al día y cuadrar entre todas las áreas relacionadas.

- ✓ Solicitar asistencia técnica especializada para el mantenimiento correctivo

- ✓ Si existen problemas en los componentes, éstos deben ser reemplazados, sin arriesgarse a mantenerlos, ya que en la mayoría de los casos, se vuelven inestables o inservibles.

3.2.2.4 Problemas Específicos en las Terminales.

Toda falla en u equipo terminal ocasionara la interrupción en las actividades diarias y por tanto en el atención del socio, es menester mencionar que estas son las que en mayor probabilidad ocurren.

3.2.2.5 Fallas técnicas internas.

Fallas de Hardware

- ✓ Daño en la Tarjeta de Red

- ✓ Daño en el C.P.U
- ✓ Daño en Puertos COM
- ✓ Daño en puertos USB
- ✓ Daño en puertos LPT
- ✓ Daños en los Cooler de las fuentes de poder y/o microprocesadores

Es factible que los componentes como tarjeta madre del equipo, el procesador, tarjetas de red, periféricos, etc. que posee la Terminal se haya(n) dañado por motivos inherentes a picos fuertes de energía, fallas de fabricación, vibraciones, etc.

Los efectos (en orden de mayor a menor) de esas causas son:

- ✓ La imposibilidad de comunicarse al Servidor de Archivos
- ✓ Cortes repentinos en la comunicación
- ✓ Pérdida de datos.
- ✓ Cortes repentinos durante el trabajo
- ✓ Reporte del BIOS de errores
- ✓ Aparición de resultados absurdos en los cálculos
- ✓ Desaparición inexplicada de datos
- ✓ Cuelgues constantes
- ✓ Imposibilidad de seguir trabajando, etc.

Normas Preventivas

- ✓ Asegurarse que la alimentación de energía a la Terminal sea constante y estabilizada

- ✓ Que la calidad de los componentes esté garantizada
- ✓ Que la seguridad que se establezca en torno al ambiente físico donde se encuentre sea la debida.
- ✓ Evitar fuentes magnéticas importantes en las cercanías del equipo

- ✓ Protegerlo con una buena instalación de U.P.S.s y tierra.
- ✓ Mantenimientos preventivos periódicos.

Que Hacer en Caso de Fallas Técnicas de Hardware

- ✓ Análisis previo determinar el alcance real de los daños
- ✓ Detectar el componente que produce el error
- ✓ Si existen problemas en los componentes, éstos deben ser reemplazados, sin arriesgarse a mantenerlos, ya que en la mayoría de los casos, se vuelven inestables o inservibles.
- ✓ Instalar y configurar el componente dañado
- ✓ Si no es posible reparar el equipo solicitar asistencia a técnicos especializados, para la realización del mantenimiento correctivo.

Fallas de Software

Es factible que los programas instalados en un equipo terminal tanto software de base (sistema operativo), software de ofimática u otros que posee la Terminal se haya(n) dañado por motivos relacionados a:

- ✓ La terminal no haya sido apagada de la forma correcta.
- ✓ Constantemente se hayan presentado cuelgues del equipo.

Normas Preventivas

- ✓ Capacitar al personal acerca del manejo adecuado del equipo.
- ✓ Mantenimiento preventivo de software.

Que Hacer en Caso de Fallas de Software

- ✓ Proceder a la ejecución de alguna herramienta de diagnóstico, como por ejemplo programa Norton Utilities, en la opción System Check.
- ✓ Luego de la revisión por el programa, ejecutar la opción Repair All
- ✓ Si la falla persiste, desinstalar la aplicación de software con problemas y

proceder a la reinstalación.

3.2.2.6 Problemas en los Switch.

Es probable que en cualquier momento inesperado, algunas terminales no puedan conectarse al servidor o entre si y exista la imposibilidad de trabajar con el sistema o de compartir recursos y no exista razón aparente para esta incomunicación,

Normas Preventivas

- ✓ Proteger los racks donde se encuentran instalados los Switch
- ✓ Asegurarse que la alimentación de energía a la Terminal sea constante y estabilizada.
- ✓ Protegerlos con una buena instalación de UPS y tierra.

Que Hacer en Caso de Problemas en los Switch

Una vez efectuadas la revisión en el equipo terminal, cables y conexiones queda revisar las conexiones en el Switch y se pueden intentar las siguientes acciones:

- ✓ Revisar la conexión del Patch Panel al Switch y o cambiar de posición el Patch Cord

- ✓ Si no existieran lugares disponibles, entonces será necesario, ya sea cambiar el Switch o aumentar uno para que se pueda utilizar adicionalmente, para lo que no será necesario aumentar otra tarjeta de comunicación el Sevidor de Archivos, debido a que todos los Switch tienen un puerto para realizar UpLink con otro Switch.

- ✓ Si ninguna de las terminales se puede comunicar y ya se ha revisado que la alimentación de energía al Switch es correcta, se deberá revisar, en primera, instancia la comunicación del Switch con el Servidor de archivos, porque podría ser que lo que esté mal sea el cable de conexión o la tarjeta de red del Servidor.

Sin embargo, si esto también está bien, entonces lo más lógico sea que se haya quemado el Switch. Para esto la única solución viable es cambiarlo por otro capaz de efectuar el mismo trabajo del anterior.

Motivos Lógicos.

Al igual que para el caso anterior, es posible encontrar una variedad de posibilidades que pueden ocasionar también otra variedad de problemas, causados por irregularidades en la parte lógica del equipo. A continuación, describiremos las más representativas:

Problemas Específicos del Servidor

El Servidor, por sí mismo puede sufrir una serie de daños en la parte lógica, así:

3.2.2.7 Mala Configuración en el BIOS

Es muy posible que la computadora en cuestión esté mal configurada en su registro de arranque, es decir que la información que recibe el procesador sobre los periféricos conectados, el control de interrupciones, administración de energía, distribución de recursos, etc. esté mal; ya sea porque el que configuró el equipo lo hizo mal o que la pila de soporte de la tarjeta madre se haya agotado.

Los efectos que se observarán pueden ser: que arranque el equipo reportando errores en el arranque, los que deberán anotarse para proceder a solucionarlos; o sencillamente que no arranque.

Que Hacer en Caso de Mala Configuración del BIOS

- ✓ Habilitar el Servidor Auxiliar restaurando la última copia de seguridad
- ✓ Revisar la configuración contrastando los manuales y configurar el equipo de acuerdo a las especificaciones del fabricante y tomando en cuenta todos los recursos con los que cuenta el equipo

- ✓ Si los problemas se repiten aún después de configurado, entonces significará que la pila de soporte se ha agotado; entonces, antes de intentar de nuevo, se tendrá que cambiar la pila.

- ✓ Si la computadora no arranca, lo más aconsejable es llamar a técnicos calificados (por Ej. los proveedores) para que procedan a solucionar el inconveniente. Sin embargo, si se tiene conocimientos suficientes, es posible que sacando la pila de soporte del BIOS de la tarjeta madre por veinticuatro horas y reemplazándola por una nueva se pueda hacer arrancar el equipo para poder después configurarlo. Si esto fallara, entonces no quedará alternativa que llamar al servicio técnico.

3.2.2.8 Daños en el Disco Duro

Uno de los medios que más trabaja y por lo tanto está expuesto a daños es el disco duro, que se constituye en el medio de almacenamiento más usado dentro de la computadora, por ser el más rápido y efectivo.

Dentro de los problemas más usuales que podemos tener dentro el servidor de la red están los siguientes:

- ✓ Daños en las particiones: El disco duro (o los discos) del Servidor, tienen varias porciones que reciben el nombre de particiones, desde la primaria o de arranque hasta varias otras dependiendo de la cantidad de sistemas operativos presentes o unidades lógicas definidas. Una partición contiene información de su tamaño, el tipo de organización que deben mantener sus archivos, el sistema operativo al que responden, etc. Es decir, información que será utilizada para que esa partición sea reconocida por el equipo y por el sistema operativo que la creó. Cuando se pierde esa información, el sistema operativo no reconoce la existencia de la partición y es posible perder grandes cantidades de datos y causar daños irreparables en la información almacenada. Normalmente los problemas de particiones ocurren ante cortes de luz, picos de energía, vibraciones fuertes, etc.

- ✓ Errores en la superficie del disco: Otro de los problemas usuales dentro de la operación de los discos duros son los errores en la superficie.

Se producen por cortes de luz que hacen que las cabezas de lectura escritura del disco caigan sobre la superficie produciendo rayas que dañan en forma definitiva el disco; aunque también los picos de energía fuertes pueden provocarlos.

Estos errores físicos no son recuperables y toda la información que esté contenida en los sectores y pistas afectadas no podrá ser recuperada.

Normas Preventivas.

Que Hacer en Caso de Daños en el Disco Duro

- ✓ Habilitar el servidor Auxiliar con la última copia de seguridad

- ✓ Solicitar asistencia técnica para la reparación de la falla

3.2.2.9 Problemas Específicos de las Terminales.

Las Terminales también pueden tener sus problemas específicos:

Errores en la Configuración del BIOS

Es muy posible que la computadora en cuestión esté mal configurada en su registro de arranque, ya sea porque el que configuró el equipo lo hizo mal, se modificó la configuración ó que la pila de soporte de la tarjeta madre se haya agotado.

Los efectos que se observarán pueden ser: que arranque el equipo reportando errores en el arranque, los que deberán anotarse para proceder a solucionarlos; o sencillamente que no arranque.

Que Hacer en Caso de Mala Configuración del BIOS

- ✓ Encender el equipo y presionar la tecla SUP o DEL para ingresar al BIOS

- ✓ Se procederá a configurar el equipo de acuerdo a las especificaciones del fabricante y tomando en cuenta todos los recursos con los que cuenta el equipo.

- ✓ Sin embargo, si los problemas se repiten aún después de configurado, entonces significará que la pila de soporte se ha agotado; entonces, antes de intentar de nuevo, se tendrá que cambiar la pila.

- ✓ Si la computadora no arranca, lo más aconsejable es llamar a técnicos calificados para que procedan a solucionar el inconveniente. La falla podría ser ocasionada por fallas en componentes internos.

3.2.2.10 Daños en el Disco Duro

En el caso de las terminales, los discos duros se utilizan para almacenar la información de los trabajos locales del usuario, también para almacenar los sistemas de aplicación personal y los programas de comunicación con el o Servidor.

Dentro de los problemas más usuales que podemos tener dentro de las terminales están los siguientes:

Daños en las particiones: El disco duro (o los disco) de la Terminal, tiene varias porciones que reciben el nombre de particiones, desde la primaria o de arranque hasta varias otras dependiendo de la cantidad de sistemas operativos presentes o unidades lógicas definidas. Normalmente, los sistemas operativos tienen utilitarios capaces de resolver problemas relativos a las particiones de los discos duros (por Ej. el FDISK.EXE del D.O.S. o el Windows).

Los que deben ser utilizados para resolver este tipo de problemas a tiempo. Generalmente los problemas de particiones ocurren ante cortes de luz, picos de energía, vibraciones fuertes, etc.

Errores en la superficie del disco: Otro de los problemas usuales dentro de la operación de los discos duros son los errores en la superficie. Se producen por cortes de luz que hacen que las cabezas de lectura escritura del disco caigan sobre la superficie

produciendo rayas que dañan en forma definitiva el disco; aunque también los picos de energía fuertes pueden provocarlos.

El mismo efecto de sectores dañados se puede obtener por problemas en la asignación de espacio en la tabla de localización de archivos (F.A.T.) y por problemas lógicos en la grabación de los datos; en estos casos, es posible recuperar mayor cantidad de información a través de utilitarios disponibles, ya sea en el sistema operativo o de terceros.

Normas Preventivas

Realizar periódicamente un escaneo del disco duro.

Limpieza de archivos

Desfragmentación del disco duro

Que Hacer en Caso de Daños en el Disco Duro

- ✓ Actualización del firmware
- ✓ Cambiar la tableta PCB de un disco duro defectuoso
- ✓ Cambiar los diodos TVS o fusibles de un disco duro defectuoso

3.2.2.11 Existencia de Virus Informáticos.

El problema de los virus informáticos nació muy temprano en la década de los 80, expandiéndose dentro el ámbito de las computadoras personales a partir de 1986. Un virus no es otra cosa que un programa escrito por algún programador que tiene características especiales.

Las dos características principales de un virus son:

- ✓ La capacidad de reproducirse (copiarse) a otros programas o medios de almacenamiento

- ✓ La capacidad de causar desórdenes dentro de la ejecución regular de los sistemas.

El que se encuentre presente un virus involucra una serie de desastres y consecuencias dependiendo el tipo que se haya detectado.

Los daños que se pueden encontrar varían entre una simple molestia en la pantalla hasta la desaparición de toda la información almacenada en los discos, ya sean discos duros y otro tipo de medios.

Normas Preventivas

- ✓ Instalar en cada terminal software de protección antivirus
- ✓ Capacitar al Personal en el manejo del software de antivirus
- ✓ Actualizar periódicamente el software antivirus
- ✓ Restringir el uso de medios extraíbles de fuente externa a la institución (u otro tipo de medios de almacenamiento), sin que hayan sido revisados por el antivirus para comprobar que se encuentran libres de infección

Que Hacer en Caso de Existencia de Virus

Las medidas correctivas para eliminar las infecciones también son varias y dependen del alcance de los daños que ha provocado el o los virus presentes.

- ✓ Aislar la terminal infectada del resto de la red.
- ✓ Intentar ejecutar las opciones de detección y eliminación de los programas antivirus con los que se cuente (siempre de última generación), normalmente este tipo de sistemas darán todas las instrucciones pertinentes para llegar a eliminar los tipos de virus presentes.
- ✓ Si mediante este método no se puede, entonces la siguiente medida es radical e

involucra el formateo de la unidad de almacenamiento (disco duro u otro) y reinstalación del sistema operativo y los paquetes de aplicación

- ✓ El proceso de detección y eliminación de virus, una vez que se ha detectado la presencia, se debe realizar sobre todos los medios de almacenamiento que se hayan utilizado y tengan posibilidades de haberse infectado.

CONCLUSIONES

Como se ha visto a lo largo de las páginas que anteceden, existen circunstancias que provocan problemas dentro de la estructura informática de la Institución. Felizmente, el tiempo y la tecnología nos han enseñado a lidiar con muchas de ellas.

Debemos tener presente siempre las normas de seguridad para prevenir acciones por razones fortuitas o de negligencia, que puedan venir de dentro o fuera de la Institución.

Esperamos que el contenido de este Manual de Contingencias provea al lector de suficientes elementos para poder hacer frente a los problemas más frecuentes que se pueden encontrar, sin esperar que sea una Biblia metodológica, sino más bien, una guía de consulta.