MACROPROCESO: **APOYO**
PROCESO: **SISTEMAS**
SUBPROCESO: **INFORMACION**
PROCEDIMIENTO: **PLAN DE CONTINGENCIA**

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

OBJETIVO: Reducir el riesgo sobre la posibilidad de ocurrencia de siniestro de hardware, software, información y de los equipos periféricos.

¿Qué es un plan de contingencia?

Un plan de contingencia es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

El plan de contingencia propone una serie de procedimientos adicionales al funcionamiento normal de una organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos el equipo informático y la información contenida en los diversos medios de almacenamiento, por lo que en este instructivo se hará un análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas las medidas de seguridad a implementar, puede ocurrir un desastre, por tanto, es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Tipos de fallas a considerar en el Plan de Contingencia:

- Red eléctrica.
- Red de datos.
- Problemas con el servidor.
- Estaciones y periféricos.
- Servicio de Internet.

- ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACION

1. La Seguridad Física

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general.

Medidas a preparar para ser utilizadas en relación a los fallos.

1.2 Antes

El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que dé él se puedan derivar.

- Ubicación del Hospital.
- Ubicación del Área de Sistemas.
- Potencia eléctrica.
- Sistemas contra Incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

1.2 Durante

Se debe de ejecutar un plan de contingencia adecuado. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de la ESE.

Son puntos imprescindibles del plan de contingencia:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.
- Determinar las prioridades del proceso, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Designar entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la capacidad de las comunicaciones.
- Asegurar los back-up de la información.

1.3 Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar los equipos de computo y herramientas tecnológicas una vez detectado y corregido el fallo.

Servidor, equipos de cómputo y demás herramientas tecnológicas: se contrata la cobertura sobre el daño físico con la aseguradora.

Gastos extra: cubre los gastos extra que derivan de la continuidad de las operaciones tras un desastre o daño en el centro de proceso de datos.

Contratos con proveedores y de mantenimiento: proveedores o fabricantes que aseguren la existencia de repuestos, así como garantías de fabricación.

2. Conceptos Generales

- Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

- Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

- Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

- Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.
En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

- Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

- Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

- Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

3. ANALISIS DE RIESGO

El análisis de riesgos supone más que el hecho de observar la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada centro escolar beneficiada con el Proyecto de aulas informáticas.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?
- A continuación se muestra un ejemplo de cómo se realiza una evaluación de riesgos.
- El o los responsables de centro escolar que posee un AI se sentarán para realizar el siguiente conjunto de puntualizaciones:

- ¿A qué riesgos en la seguridad informática se enfrenta la Institución?
- Al fuego, que puede destruir los equipos y archivos.
- Al robo común, llevándose los equipos y archivos.
- Al vandalismo, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.
- A equivocaciones, que dañen los archivos.

Ver Anexo Matriz de Riesgo

4. Fallas Genéricas Funcionales de los Sistemas a tener en Consideración.

Se han encontrado varias fallas comunes a los sistemas de computación, estos incluyen:

- Autentificación. En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

- Cifrado. La lista maestra de contraseñas debe ser almacenada.

- Confianza implícita. Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

- Desconexión de línea. En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control.

- Descuido del operador. Un intruso puede engañar a un operador y hacer que le suministre información.

- Contraseñas. Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos.

- Residuos. A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida antes de liberar o descargar el medio que ocupa (almacenamiento, papel, etc.).

5. Protección del Servidor

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el área de sistemas de la ESE. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro.

PLAN DE ACCION

1. Realizar un inventario de las herramientas informáticas.
Inventario de equipos de cómputo, software y demás equipos informáticos, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, Internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.

2. Identificación de amenazas.
Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc., que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional.

3. Revisar la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las amenazas posibles.

Se debe estar preparado para cualquier percance, verificando que dentro de la ESE Hospital Santa Isabel se cuente con los elementos necesarios para salvaguardar sus activos.

4. Identificar los servicios fundamentales de la ESE Hospital Santa Isabel.
Se deben analizar las funciones y áreas de mayor prioridad de la ESE.

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Menor: Es la que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.
Grave: Es la que causa daños a las instalaciones, pero pueden reiniciar las operaciones en menos de 24 horas.
Crítica: Afecta la operación y a las instalaciones, no es recuperable en corto tiempo y puede suceder por que no existen normas preventivas o bien porque estas no son suficientes o por algún tipo de desastre natural.

Tipos de Contingencias de acuerdo al grado de afectación:
En los enseres.
En los equipos informáticos.
En comunicaciones (Hubs, Routers, nodos, líneas telefónicas).
Información.
Instalaciones físicas.

ETAPAS DE LA METODOLOGIA

1. Establecer un Grupo de Trabajo y definir roles.

Se debe establecer formalmente el Comité del Plan de Contingencia con la siguiente estructura:

Presidente del Grupo
Coordinador General
Coordinador de Sistemas
Coordinador de Soporte
Usuarios

Definición de Roles:

Presidente del Grupo de Trabajo. Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir los comunicados de concientización y solicitud de apoyo a los jefes y/o gerentes de las diferentes áreas involucradas y aprobar su terminación.

Una vez concluida la realización del Plan de Contingencia, el Presidente tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos cada seis meses, en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correcto funcionamiento del Plan de Contingencia Informático, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten.

Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizará las inversiones a realizar así como el fondo de efectivo a asignarse para los gastos necesarios iniciales.
El presidente se mantendrá permanentemente informado respecto de la activación del Plan hasta la declaración de conclusión.

Coordinador General. Tendrá como función principal asegurar que se lleven a cabo todas las fases para la realización del Plan de Contingencia y aprobará junto con el Presidente del Comité la terminación de cada una de las fases y la conclusión del proyecto.

Durante la realización del plan, una de sus actividades principales será la coordinación de la realización de las pruebas del Plan de Contingencia, la aprobación de las ubicaciones alternas que sea necesario definir, la aceptación de los gastos y/o adquisiciones o contratos de servicios que sean necesarios para la realización del plan. Al término de la realización de las pruebas, será el Coordinador General quién dé su visto bueno en la conclusión de éstas y de sus resultados.

Coordinador de Sistemas. Es el responsable de determinar los procedimientos a seguir en caso de que se presente una contingencia que afecte las comunicaciones, Servicios de Internet, Intranet, correo electrónico y red, mantener actualizados dichos procedimientos en el Plan de Contingencia, determinar los requerimientos mínimos necesarios, tanto de equipo como de software, servicios, cuentas de acceso a Internet, enlaces dedicados, dispositivos de comunicación (ruteadores, switchs, antenas etc).

Es el responsable de llevar a cabo el inventario de equipo, software y equipos periféricos, como impresoras, CD Writer, escáners, faxes, copiadoras, etc.; mantener los equipos en óptimas condiciones de funcionamiento; determinar la cantidad mínima necesaria de equipo y sus características para dar continuidad a las operaciones de la ESE; es responsable de elaborar o coordinar con los usuarios los respaldos de información.

Deberá realizar los procedimientos correspondientes para la emisión de los respaldos de cada uno de los servidores o equipos en donde se procese lo enunciado en el párrafo anterior, efectuar y mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático.

En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuere su grado de afectación, es el responsable de restablecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores.

Coordinador de Soporte. Será el responsable de determinar los sistemas Críticos de la ESE, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, pérdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen estos sistemas críticos.

En caso de cambiar a otras instalaciones alternas, el Coordinador de Programación deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los Manuales Técnicos y de Usuario, resguardándolos fuera de las instalaciones para su consulta y utilización al momento de requerirse.

Personal involucrado (Empleados). Al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se estuviera presentado sea grave (incendio, temblor, etc.); posteriormente, y en la medida en que la situación lo permita, deberá ayudar a salvaguardar los bienes de la ESE (el propio inmueble, equipos, documentación importante, etc.).

Con posterioridad a la crisis inicial, deberá apoyar a solicitud del Coordinador de su área y/o del personal clave del Plan de Contingencia, en la toma del inventario de daños, para lo cual deberá seguir las instrucciones generales que indique el propio Plan.

En forma alterna, deberá dar cumplimiento a las instrucciones que se incluyan en el Plan de Contingencia Informático para darle continuidad a las funciones informáticas críticas.

Al declararse concluida la contingencia, deberá participar activamente en la restauración de las actividades normales de la ESE, esto es, apoyar en la movilización de documentación, mobiliario, etc., a las instalaciones originales o al lugar que le sea indicado, hasta la estabilización de las actividades.

Cuando sea necesario, deberá participar en la capacitación del nuevo personal o del personal eventual que hubiera sido necesario contratar.

Roles	Puesto	Encargado
Presidente		
Coordinador General		
Coordinador de Sistemas		
Coordinador de Soporte		
Empleados		

2. Determinar los eventos que pueden afectar adversamente a la ESE Hospital Santa Isabel y su infraestructura, con interrupciones ó desastres en materia informática.

Los desastres y crisis son eventos que pueden inhabilitar a la ESE de proveer normalmente sus servicios a los usuarios internos y la atención al público en General, por lo que deben identificarse, analizar su nivel de riesgo y tomarse las medidas necesarias de prevención.

Identificación de Amenazas:

Terremoto
Incendio
Inundación y humedad
Corte de Energía
Falla de la red de voz y datos
Fallas en Hardware o Software
Sabotaje o daño accidental
Vandalismo y manifestaciones

TERREMOTO

SIN PÉRDIDA O DAÑOS MENORES DEL EDIFICIO: El siniestro puede afectar únicamente parte de la estructura del edificio, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera del edificio; el impacto que provocaría en la ESE sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

CON PÉRDIDA DEL EDIFICIO: La pérdida de las instalaciones afectaría gravemente a las operaciones de la ESE y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

INCENDIO

ÁREAS DE SISTEMAS: Se tiene gran impacto en la información ya que los sistemas utilizados residen en el Servidor y dispositivos de comunicación localizados allí y en caso de sufrir algún daño, se requerirá adquirir un nuevo equipo, así como de instalar nuevamente el sistema, configurar el Servidor y restaurar los respaldos para continuar trabajando.

OTRAS AREAS: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el Área de Sistemas. En el caso de las primeras el impacto que tendría en la ESE es menor, puesto que la información o tiempo de operación que se pierde no tiene gran repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto.

INUNDACIÓN Y HUMEDAD

Puesto que es equipo electrónico el que se maneja dentro de la institución, una inundación severa dañaría los dispositivos irremediablemente deteniendo las operaciones de la misma totalmente.

Un daño grave correspondería a una inundación en el área de sistemas, en tanto que una inundación parcial o limitada a parte de las instalaciones, podría sólo ocasionar un daño medio sí no va seguido de corto circuito.

CORTE DE ENERGÍA

Las operaciones informáticas de la ESE se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido se provocaría un trastorno en las operaciones del día, sin afectar los datos.

Actualmente la ESE cuenta con una planta de energía con capacidad para restablecer la energía inmediatamente después de la perdida de luz en la sede Guamurú; para el caso de la sede CASA no habría energía eléctrica.

Algunos los usuarios cuentan con reguladores para entrar inmediatamente después del corte de energía y evitar daños en los equipos.

FALLAS DE LA RED DE VOZ Y DATOS

RED: Representa la columna vertebral de las operaciones de la ESE, si la red falla en su totalidad, las operaciones se detienen con la consecuente falta del servicio informático.

APLICACIONES: La falla en los sistemas utilizados, representa un impacto medio en las operaciones totales de la ESE, ya que pueden ser reinstalados casi de inmediato.

FALLAS EN HARDWARE O SOFTWARE

Las alteraciones que sufran los servidores tanto en Hardware y Software pueden ser corregidas en la mayoría de los casos, sin embargo si las alteraciones llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

SABOTAJE O DAÑO ACCIDENTAL

La alteración de la información requiere de la restauración de los respaldos y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran reprocesos de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles.

VANDALISMO Y MANIFESTACIONES

Un intento de vandalismo ya sea menor o mayor, podría afectar a los equipos de computo, periféricos y servidor así como las comunicaciones. Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área de sistemas ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado a la ciudadanía.

Actualmente la ESE cuenta con extinguidores de fuego instalados en todas las instalaciones que conforman a la Delegación, dichos extinguidores se les da el mantenimiento adecuado y se encuentran al alcance del personal en caso de suceder incendio.

El área de sistemas no posee detectores de humo ni alarma contra incendio.

3. Procedimiento de Activación de los Dispositivos de Seguridad

EXTINGUIDORES

Los extinguidores tienen la intención de usarse en un tipo en particular de riesgo, así que se debe de poner especial atención en colocarlo cerca del las posibles áreas de riesgo que deben proteger.

TIPOS DE EXTINTORES

	A Agua	AB Agua + Espuma Química	ABC Polvo Químico Seco	BC Dióxido de carbono (CO_2)	ABC Halotron 1	D Polvo Químico D	K Potasio
A Solidos	SI	SI	SI	NO	SI	NO	NO
B Liquidos	NO	SI	SI	SI	SI	NO	NO
C Eléctricos	NO	NO	SI	SI	SI	NO	NO
D Metales	NO	NO	NO	NO	NO	SI	NO
K Grasas	NO	NO	NO	NO	NO	NO	SI

A continuación se describe gráficamente el procedimiento para el uso de extinguidores en caso de incendio:

Es importante que los símbolos de los tipos de incendio ilustrados anteriormente se encuentren especificados en la etiqueta del extinguidor, para que el usuario identifique si el extinguidor a usar es el indicado para el siniestro que se presente.

4. Procedimientos de Respaldo y Recuperación.

Establecer normas de seguridad como son:

Definir los procedimientos que indiquen los pasos a seguir para respaldar la información.

Especificar el lugar donde se encuentran custodiados los respaldos de información o copia de los respaldos, en el interior de la ESE y en un lugar fuera de la esta.

En esta parte, debe incluirse los procedimientos de respaldo y recuperación de la información de los sistemas, así como de los programas o aplicaciones y de los sistemas operativos. Es importante contar con algunos ejemplares del software de los programas comerciales que se utilicen normalmente, como es el Office, CNT, Windows XP, 2003 Server, etc.

Ver anexo: INSTRUCTIVOS COPIAS Y BACKUPS

El Backup de la Base de Datos se realiza 2 veces al día.

Almacenamiento del Backup en condiciones ambientales óptimas, dependiendo del medio magnético empleado.

SERVIDOR		
SERVIDOR WINDOWS	**DIRECCION**	**RUTA**
DCPPAL	192.168.1.10	F:\MSSQL\BACKUP

5. Determinar los tiempos de recuperación y los requerimientos mínimos de recursos.

Para cada una de las fases críticas que se cubrirán con el Plan de Contingencia Informático, se deben determinar los tiempos mínimos requeridos para el establecimiento del plan, esto es, cuánto tiempo debe transcurrir desde el momento en que se inicia o activa el plan, hasta que las actividades, funciones o sistemas se encuentren en operación total o parcialmente.

Es conveniente definir un tiempo aceptable y viable para que la red y la aplicación principal estén nuevamente activas.

Para situaciones críticas:

- Incluir el traslado de los medios de almacenamiento magnético que se encuentren fuera de las instalaciones. 2 Horas
- La copia de los datos a los nuevos medios de almacenamiento magnético y la habilitación de las comunicaciones, servicios de Internet y correo electrónico. 24 Horas
- El personal mínimo requerido para continuar operando. 4 Horas
- Tiempo de restauración de cada uno de los servicios de Red, Comunicaciones, Internet y Correo Electrónico. 24 Horas

El tiempo determinado debe ser conocido y aceptado por todos los usuarios principales que operan los sistemas o cuentan con un equipo crítico.

Para situaciones de bajo riesgo:

- Tiempo de reparación o reposición de una estación de trabajo (PC) 4 Horas
- Tiempo de configuración de las PC. 8 Horas
- Tiempo de respuesta del proveedor para la reparación de los servidores (verificar contratos y garantías). 24 horas
- Tiempos de reparación de fallas eléctricas. 24 Horas

Procedimientos en Caso de daños a Servidor o Equipos de Computo

CASO 1: Error Físico de Disco del Servidor

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a coordinadores de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Enviar el equipo a reparación e instalación.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO 2: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

1. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
2. Ante procesos mayores se congela el proceso.
3. Arroja errores con mapas de direcciones hexadecimales.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la ESE, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a coordinadores de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.

3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
6. Realizar pruebas locales, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO 3: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a coordinadores de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar, en el caso de no tenerla enviar el equipo para el cambio de las tarjetas.
5. Retirar la conexión del servidor con la red, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO 4: Caso de Incendio Total

En el momento que se dé aviso de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

6. Ante todo, se recomienda conservar la serenidad, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
7. En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el
8. tiempo lo permite) de "Salir de Red y Apagar Computador",
9. Apagar el Servidor
10. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO 5: Caso de Inundación

- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
- Mover los equipos de cómputo a partes altas.

CASO 6: Caso de Fallas de Fluido Eléctrico

- Si fuera corto circuito, la UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.

- Cuando falle el fluido eléctrico se encenderá la planta que se encuentra en la sede Guamurú para contrarrestar la falta de energía.

- Cuando el fluido eléctrico de la calle se ha restablecido se desconectara la planta.

ERROR LOGICO DE DATOS

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de BD, una vez mostrado el prompt de Dos, cargar el sistema operativo.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Copiar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá Copiarlo también.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de base de datos no reconocidas como tal, se debe recuperar con las copias de seguridad.

Al concluirse la reparación del equipo, se regresara a servicio el servidor reparado, buscando realizar esto durante la noche o en un fin de semana, con el objeto de no entorpecer las actividades normales del personal usuario.

Descompostura o falla en Equipo de Comunicaciones. Se deberá sustituir de inmediato con equipo que se tenga disponible para estos casos, o en su defecto adquirir de urgencia el servicio con el proveedor especializado.
Falla de cableado. Para reparaciones mínimas la Sistemas lo realizará máximo en 8 hrs. Para efectuar el recableado o sustitución del tramo de cable dañado,

es importante remitirse a la garantía con el proveedor que realizó el cableado.

Falla de tarjeta de red de estación de trabajo. Sustitución inmediata con tarjetas nuevas, lo que no debe tardar más de 4 hrs.

Falla en Router. Se deberá sustituir de inmediato con equipo que se tenga disponible para estos casos, o en su defecto adquirir de urgencia el servicio con el proveedor especializado.

Falla de enlaces. Se deberá solicitar al proveedor la restauración del servicio, el cual por lo regular tarda 24 horas en restablecerse, a menos de que se trate de daño mayor, el cual puede tardar aproximadamente 48 horas.

Ver Anexo: Hoja de Vida de equipos
Inventario General

FALLAS DE INTERNET

Cuando se trate de fallas de acceso en Internet causadas por el proveedor del servicio (Edatel), se deberá tener comunicación con el personal de soporte de cuenta para realizar el reporte del daño y para establecer el tiempo en el que se estará sin servicio.

La red Internet de EDATEL es una red de alta capacidad, redundante, altamente eficiente y capaz de ofrecer una cobertura a nivel nacional, formada por enrutadores dedicados exclusivamente para este fin.

VIRUS

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor y equipos internos de computo:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe, com, ovl, nlm, etc.) serán reemplazados del diskett original de instalación o del backup.

- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar el programa.

REQUERIMIENTOS MINIMOS SOFTWARE

Los Equipos de Cómputo para los usuarios y para personal de la ESE que operara en las instalaciones alternas, deberá contar con la siguiente configuración mínima.

XP o Superior
Office 2003 o Superior
Antivirus Symantec Corporativo
Explorador de Internet

Impresoras: Equipos con Powersafe, Ecoprint e impresión laser.

Red:

Cableado estructurado nivel 5E interconectado mediante Switchs

Salida a Internet por medio de la Red

Software CNT Sistemas de Información con permisos según cargo

CONCLUSION

La ESE tendrá que realizar paralelamente un plan de contingencia por cada área.

Adicionalmente al plan de contingencias se debe desarrollar pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.