M-407-02

CONTINGENCIA INFORMATICA

ELABORADO POR	REVISADO POR	APROBADO POR
LIDER DEL PROCESO	REPRESENTANTE DE LA DIRECCIÓN	GERENTE GENERAL

INTRODUCCIÓN

Pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos en seguridad afirman "sutilmente" que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", no "por si falla el sistema".

Por tanto, es necesario que el Plan de Contingencias incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo 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 y global posible.

Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

Se entiende por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información".

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

OBJETIVOS

- ✓ Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

- ✓ Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.

- ✓ Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

IDENTIFICACION DE PROCESOS Y SERVICIOS

Principales Procesos de Software Identificados

- Software Integrado IAS
- Software Ventanilla Única
- Software Ofimático (Microsoft Office)
- Software Base de Datos Oracle

Principales servicios que deberán ser restablecidos Y/O recuperados

- Correo Electrónico.
- Internet.
- Antivirus.
- Proxy y/o farewall

Respaldo de la Información

- Backup de la Base de Datos IAS
- Backup de la Información de los Usuarios
- Backup de los dos WEBSITE del Instituto
- Backup de la Intranet
- Backup del Servidor. (Active Directory)

PLAN DE CONTINGENCIA INFORMÁTICO

El Plan está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en prevención de desastres.

Se define la Seguridad de Datos como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o antrópicos. Se ha considerado que para, la información es uno de los activos más importantes, lo cual hace que la protección de esta sea el fundamento más trascendental de este Plan de Contingencia.

En este documento se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y recuperación para enfrentar algún desastre. Por lo cual, se debe tomar como Guía para la definición de los procedimientos de seguridad de la Información.

Actividades Asociadas

Las actividades consideradas en este documento son:

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

ANALISIS DE EVALUACION DE RIESGOS Y ESTRATEGIAS

Metodología aplicada:

Para la clasificación de los activos de las Tecnologías de Información de INFITULUA E.I.C.E. se han considerado cuatro criterios:

- Zona de Riesgo Bajo : donde INFITULUA E.I.C.E. asume el riesgo
- Zona de Riesgo Moderado : donde se procura reducir el riesgo
- Zona de Riesgo Alto : donde se comparte o se transfiere el riesgo
- Zona de Riesgo Extremo : donde INFITULUA E.I.C.E. evita el riesgo

Frecuencia del Evento:

- 0 - 5 cero eventos en cinco años – zona de riesgo bajo
- 1 - 5 un evento en cinco años – zona de riesgo Moderado
- 1 - 2 un evento en dos años - zona de riesgo Moderado
- 1 – 1 un evento en un año - zona de riesgo alto
- 2 – 1 dos eventos en un año - zona de riesgo extremo.

Riesgos Naturales: tales como mal tiempo, terremotos, etc.
Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
Riesgos Sociales: como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la

entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad:

Clases de Riesgos

- Incendio o Fuego
- Robo común de equipos y archivos
- Falla en los equipos
- Equivocaciones
- Acción virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.

ANÁLISIS DE RIESGOS

CAUSA	TIPO DE RIESGO	RIESGO	EFECTO
No se tiene en cuenta el PETI dentro de la elaboración del presupuesto	Tecnológico	Ejecución inoportuna a las políticas que se plantean en el Plan Estratégico de Tecnología e Informática del instituto	Obsolescencia de equipos y vulnerabilidad a ataques informáticos

Falta de coordinación entre sistemas y el mantenimiento general de la empresa	Operativo	No contar con un cronograma de mantenimiento preventivo aprobado	Daño de equipo, reprocesos, perdida de información, demora de procesos
No existe un control de las publicaciones	Imagen	Publicación no veras en la página web del instituto.	Pérdida de imagen y credibilidad
Antivirus desactualizado	Tecnológico	Ataque efectivo de un virus	Perdida de información
Incumplimiento a las políticas de seguridad informática	Tecnológico	Manipulación sin autorización a la base de datos del sistema de información	Daño o perdida de información Detrimento patrimonial
No tener una frecuencia de realización de back ups	Tecnológico	No realizar backups a intervalos planificados	Reprocesos en las actividades
No tener un control a la instalación de software a través de internet	Cumplimiento	Tener software no legalizado en los equipos de cómputo del instituto	Sanciones por derecho de autor

BIENES SUSEPTIBLES DE UN DAÑO

Se puede identificar los siguientes bienes afectos a riesgos:

- Funcionarios
- Hardware
- Software
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

DAÑOS

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos, debido a problemas físicos en las Instalaciones donde se encuentran los bienes, sea por causas naturales o antrópicas.

b) Imposibilidad de acceso a los recursos informáticos, por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de INFITULUA E.I.C.E. y que afecte su patrimonio estratégico Institucional, sea mediante Robo o Infidencia.

PRIORIDADES

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en el acontecimiento.

Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre, para este caso son los servidores de aplicaciones, Dominio y Proxy.

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de INFITULUA E.I.C.E. asociadas al Centro de Operaciones Computacionales son: *Acceso no autorizado:* Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).

Ruptura de las claves de acceso al sistema de información.

a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

b) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

Desastres locales y/o Naturales

a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte y/o de operación.

b) Inundaciones causadas por falla en los suministros de agua.

c) Fallas en los equipos por causas no antrópicas

- Por fallas causadas por la agresividad del ambiente
- Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por parte de INFITULUA E.I.C.E..
- Por fallas de la comunicación.
- Por fallas en el tendido físico de la red local.
- Fallas en las telecomunicaciones con instalaciones externas.
- Por fallas de Central Telefónica.
- Por fallas de líneas de fax e Internet.

Fallas de Hardware

a) Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) Como en el procesador central.

b) Falla en el hardware de Red:

- Falla en los Switches.
- Falla en el cableado de la Red.

d) Falla en el Router.

e) Falla en el FireWall.

MINIMIZACION DEL RIESGO

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo. Es de tener en cuenta que en lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

INCENDIO O FUEGO

Grado de impacto alto

Situación Actual	Acción Correctiva
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso cuenta con un extintor debidamente cargado.	Se cumple
No se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios nuevos, lo que no es eficaz para enfrentar un incendio y sus efectos	Realizar capacitación para el manejo de extintores y primeros auxilios.
El servidor realiza backups de la	Se cumple

información diariamente, y existe otras copia de respaldo.	

Analizando el riesgo de incendio, permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, Discos duros. Para la mejor protección de la información INFITULUA E.I.C.E. ha comprendido la importancia de guardar su información en la nube.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca de las posibles áreas de riesgo que se debe proteger.

ROBO DE EQUIPOS Y ARCHIVOS
Grado de impacto Moderado

Situación Actual	Acción Correctiva
INFITULUA E.I.C.E. no cuenta con servicio de vigilante y las personas particulares que ingresan a la entidad, no son registradas.	Recomendar a la administración un servicio de vigilancia con funciones de registro y control de activos fijos de la Institución
Autorización escrita firmada por el responsable de almacén y funcionario responsable, para la salida de equipos de la Entidad.	Se cumple, por medio del formato F-405-04 ENTRADA Y SALIDA DE ACTIVOS

Por la situación de orden público en todo el país existe la posibilidad de robo a mano armada en las instalaciones del Instituto.	Se cumple, se solicita acompañamiento de la policía nacional y de una empresa privada de vigilancia privada.

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización de los administradores y/o el Técnico de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado.

Falla en los Equipos
Grado de Impacto: Grave

Situación Actual	Acción Correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Se cumple se realizan mantenimientos preventivo de equipos por lo menos dos veces al año. Ver el formato F-405-01 CRONOGRAMA DE MANTENIMIENTOS y se verifica en la hoja de vida de cada equipo de computo. Ver formato f-407-05 HOJA DE VIDA DE EQUIPO.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Se cumple se cuenta con un contrato de mantenimiento preventivo de impresoras y correctivo de equipos de computo, en caso de requerir remplazo de piezas y se cuenta con repuestos de

	quipos que están para dar de baja.
Cada Unidad Administrativa se une a la red eléctrica a través de dos UPS , la falta de energía en éstos, origina la ausencia de uso de los servicios de red	Se cumple. Las UPS se encuentran protegidos en un lugar de acceso restringido y son manipulados solo por el técnico de sistemas.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple: se tienen 2 UPS con capacidad de hasta 2 horas de duración, a estas UPS se les hace mantenimiento 2 veces al año y se la cambian baterías cada 2 años.

Teniendo en cuenta la importancia del fluido eléctrico para el funcionamiento de la entidad, 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 provocaría un trastorno en las operaciones del día, sin afectar los datos. El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales de escritorio, necesitan de una fuente se alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico.

Equivocaciones manejo del sistema

Grado de Impacto: Moderado

Situación Actual	Acción Correctiva
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Se cumple: Realizar instrucción inicial en el ambiente de trabajo presentando el Manual M-407-01 POLITICAS DE SEGURIDAD INFORMÁTICA, establecidas para manejo de sistemas.
Algunas veces el usuario que tiene conocimiento en informática intenta navegar por sistemas que no están dentro de su función diaria.	Se cumple: El técnico de sistemas debe asignar permisos y privilegios a cada usuario de acuerdo a sus funciones. Por medio de Active Directory u funciones propias en programas con funciones específicas.
La entrega de inventario es realizada por el área de almacén no se realiza de forma mancomunada con la unidad administrativa de sistemas.	El área de almacén debe entregar inventario junto con el técnico de sistemas en lo referente a equipos de cómputo.
Se presentan equivocaciones en el manejo de información debido a que no existen políticas de informática claras y precisas.	Definir políticas de informática claras y precisas, las cuales se deben comunicar a los funcionarios al igual que cualquier modificación a las mismas.

Acción de Virus Informático

Grado de Impacto: Grave

Situación Actual	Acción Correctiva
Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración.	Se cumple: Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple
Se tiene acceso restringido al servidor, únicamente es el administrador de la red el encargado de cambiar configuraciones y anexar nuevos equipos.	Antes de logear una maquina a la red, se debe comprobar la existencia de virus en la misma.
Por medio del correo electrónico se obtienen virus constantemente.	Se cumple: Crear un correo institucional para cada funcionario, de forma que únicamente se reciba información de importancia para la entidad.
Los antivirus no se actualizan periódicamente en cada equipo.	Se cumple: el antivirus se actualiza automáticamente todos los días

Los Virus informáticos han evolucionado de tal manera que hoy en día todos conocemos la importancia de tener un programa Antivirus en el computador y aun más importante es su actualización. Si tenemos un antivirus instalado pero no lo hemos actualizado, seguramente será capaz de encontrar los virus que intenten entrar en nuestros sistemas pero no será capaz de hacer nada con ellos, dado que esta información está contenida en las definiciones de virus. La actualización del Patrón de Definiciones de virus es vital y debe de hacerse como mínimo una vez al día. Otra de las piezas esenciales del Antivirus, el motor, también debe de actualizarse regularmente dado que los nuevos virus requieren en muchos casos nuevos motores de escaneo para poder detectarlos, por lo que la actualización del motor también es tarea obligada.

Fenómenos Naturales
Grado de Impacto: Grave

Situación Actual	Acción Correctiva
En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención.
Aunque existen épocas de lluvia fuertes, las instalaciones del Instituto están debidamente protegidas.	Tomar medidas de prevención
Los servidores principales se encuentran en un ambiente libre de filtraciones.	Ante la mínima filtración se debe informar de inmediato a la dirección, para realizar el respectivo mantenimiento preventivo.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos necesarios en la sala de Computación, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

Accesos No Autorizados
Grado de Impacto: Grave

Situación Actual	Acción Correctiva
Se controla el acceso al sistema de red mediante la definición de un administrador con su respectiva clave.	Se cumple
La asignación de usuario se realiza a discrecionalidad del técnico de sistemas y se solicita por medio de un formato con firma de la Directora Financiera y Administrativa	Se cumple: formato F-407-06
la Dirección Financiera y Administrativa comunica a la Unidad Administrativa de sistemas, cuando un funcionario sale a vacaciones o se retira de la entidad a fin de desactivar ese usuario.	Se cumple: formato F-407-06

Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software.
No se cancelan los usuarios del personal que se retira de la entidad de forma inmediata, recurriendo en algunos casos a utilizar la contraseña del funcionario ausente.	Tan pronto se informe que un funcionario se retira definitivamente se debe cancelar este usuario.

Todos los usuarios sin excepción tienen un “login” o un nombre de cuenta de usuario y una clave de acceso a la red. Además están registrados en el servidor de Active Directory a través del cual se otorga los permisos debidamente asignados por el responsable de área. Cada usuario es responsable de salir de su acceso cuando finalice su trabajo, también existe una política o GPO de bloqueo de maquina por tiempo superior a 5 minutos de no uso.

Ausencia del personal de sistemas
Grado de Impacto: Grave

Situación Actual	Acción Correctiva
En la INFITULUA E.I.C.E. existe un único funcionario con autorización para administrar el sistema.	Es importante autorizar un administrador del sistema alterno, en caso de que falte el funcionario de sistemas no se paralice la entidad.
El funcionario de sistemas es la única	Se cumple: se creo el formato F-407-08

persona con claves de acceso al sistema, conocedor del manejo de la red y los sistemas de información.	cambio de contraseñas de altos privilegios y todos los procesos de sistemas están debidamente documentados.

MEDIDAS PREVENTIVAS

Control de Accesos

Medidas para controlar los diferentes accesos a los activos computacionales:

- Acceso físico de personas no autorizadas.
- Acceso a la Red de PC's y Servidor.
- Acceso restringido a las librerías, programas, y datos.

BACKUPS

Referirse a instructivo I-407-01 copias de Seguridad

Adecuado Soporte de Hardware

Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos a:

a) UPS de respaldo de actual servidor de Red y/o de estaciones de trabajo

b) UPS de respaldo switches y/o HUB's

Seguridad Física de los Servidores Públicos.

Se deberá tomar las medidas para recomendar, incentivar y lograr que los funcionarios compartan sus conocimientos con sus colegas, en lo referente a la utilización de los software y elementos de soporte relevantes. Cada vez que una persona queda encargada de la Unidad Administrativa de un compañero deberá llenar el formato F-407-06 SOLICITUD DE ACCESO, para que el Técnico Administrativo de Sistemas, de los permisos necesarios en los servidores y programas y así desarrollar las funciones pertinentes.

Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

Seguridad de la Información

La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de Backup adecuado. (Formato F-407-03_Control_de_Copias_de_Seguridad).

EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

Cuando se efectúa un riesgo, este puede producir un Evento, por tanto a continuación se describen los eventos a considerar dentro del Plan de Contingencia.

• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht. • Fallas Punto Pacht Panel. • Fallas Punto de Red.	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR
• Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco • Computador de Escritorio funciona como Servidor	FALLAS EN EL EQUIPO SERVIDOR
• Incapacidad • Accidente • Renuncia Intempestiva	AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE TECNOLOGÍA DE LA INFORMACIÓN.
• Corte General del Fluido eléctrico	INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
• Falla de equipos de comunicación: SWITCH,	PERDIDA DE SERVICIO DE INTERNET

• Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet.	
• Incendio • Sabotaje • Corto Circuito • Terremoto	INDISPONIBILIDAD DEL CENTRO DE COMPUTO (DESTRUCCIÓN DE LA SALA DE SERVIDORES)
• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht. • Fallas Punto Pacht Panel. • Fallas Punto de Red.	NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR

No hay comunicación entre cliente – servidor Principal de INFITULUA E.I.C.E.

1. Requerimiento del usuario, que no cuenta con acceso a la red.
2. El técnico de sistemas procederá a identificar el problema.
3. Si se constata problema con el Pacht Panel, realizar cambio del mismo.
4. Si no se resuelve el problema proceder a constatar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma.
5. Si persiste el problema revisar los puntos de red, utilizando el diagrama lógico.
6. Testear el cable UTP. Si existe daño, realizar el cambio del cable.
7. Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones

8. Recuperación del sistema de red para el usuario.

Recursos de Contingencia

- Componentes de Remplazo:
- Diagrama Logico de la red

Falla del Servidor

Puede producir Pérdida de Hardware y Software, Perdida del proceso automático de Backup y restore e Interrupción de las operaciones. A continuación se describen algunas causas del fallo en un Servidor:

Error Físico de Disco de un 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 Unidades Administrativas.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
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.

Error de Memoria RAM

En este caso se dan los siguientes síntomas:

• El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

• Ante procesos mayores se congela el proceso.
• Arroja errores con mapas de direcciones hexadecimales.
• Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Error de Tarjeta(s) Controladora(s) de Disco

Para los errores de cambio de Memoria RAM o Tarjeta Controladora de disco se deben tomar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la pieza a cambiar.
4. Retirar la pieza con sospecha de deterioro y tener a la mano otra igual o similar.

5. Retirar la conexión de red del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, 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.

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

Error Lógico 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 falla en el servidor de los sistemas computacionales de la INFITULUA E.I.C.E.; se debe tener en cuenta:

- Verificar el suministro de energía eléctrica.
- Deshabilitar el ingreso de usuarios al sistema. 14 de diciembre de 2010

- Realizar backup de archivos contenidos en el servidor, a excepción de la carpeta raíz.
- Cargar un Portatil que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.
- Al término de la operación de reparación 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 una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

Recursos de Contingencia

- Componente de Remplazo (Memoria, Disco Duro, etc.).
- Backup diario de información del servidor

Ausencia parcial o permanente del personal de la unidad de tecnología de la información.

1. Directriz del Gerente (escrita o Email) para que el Administrador alterno se encargue del centro de cómputo de INFITULUA E.I.C.E. especificando el periodo de asignación.
2. Obtener la relación de los Sistemas de Información con los que cuenta INFITULUA E.I.C.E., detallando usuarios, en que equipos se encuentran instalados y su utilidad.
3. Conocer la ubicación de los backups de información.
4. Contar con el diagrama lógico de red actualizado.

Recursos de Contingencia

Manual de funciones actualizado del Técnico de Sistemas.

Relación de los sistemas de información.

Diagrama lógico de la Red INFITULUA E.I.C.E. actualizado.

Interrupción del fluido eléctrico durante la ejecución de los procesos.

1. Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que la UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones, para que no corten bruscamente el proceso que tienen en el momento del apagón.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de UPS a corriente normal (Corriente brindad por la empresa electrica).

Recursos de contingencia

Asegurar que el estado de las baterías del UPS, se encuentren siempre cargadas.

Perdida de servicio internet

1. Realizar pruebas para identificar posible problema dentro de la entidad
2. Si se evidencia problema en el hardware, se procederá a cambiar el componente
3. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor

4. Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
5. Es necesario registrar la avería para llevar un historial que servirá de guía para futuros daños.
6. Realizar pruebas de operatividad del servicio.
7. Servicio de internet activo.

Recursos de Contingencia

- Hardware
- Router
- Software
- Herramientas de Internet.

Destruccion del Centro de Cómputo

1. Contar con el inventario total de sistemas actualizado.
2. Identificar recursos de hardware y software que se puedan rescatar.
3. Salvaguardar los backups de información realizados.
4. Identificar un nuevo espacio para restaurar el Centro de Cómputo.
5. Presupuestar la adquisición de software, hardware, materiales, personal y transporte.
6. Adquisición de recursos de software, hardware, materiales y contratación de personal.
7. Iniciar con la instalación y configuración del nuevo centro de cómputo.
8. Reestablecer los buckups realizados a los sistemas.

PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros. El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

- ✓ Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.
- ✓ Planificar la reactivación dentro de las 12 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
- ✓ Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
- ✓ Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal del centro de procesamiento de la información, basándose en los planes de respaldo.

La responsabilidad sobre el Plan de Recuperación es del técnico administrativo de sistemas, el cual debe considerar la combinación de todo el personal, equipos, datos, sistemas, comunicaciones y suministros.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto se definen los siguientes responsables:

Técnico Administrativo de Sistemas: Sera responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.

Directora Financiera y Administrativa: Verificara la labor realizada por el Técnico Administrativo de Sistemas

Control Interno: Evaluara la ejecución de acciones correctivas a fin de minimizar los riesgos.

- Un Plan de Recuperación de Desastres se clasifica en tres etapas:

Actividades Previas al Desastre.

Actividades Durante el Desastre.
Actividades Después del Desastre.

Actividades previas al desastre

Se considera las actividades de actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a:

Sistemas e Información
Equipos de Cómputo
Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a. Sistemas de Información

La Entidad deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas.

b. Equipos de Cómputo

Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional). Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).

- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

c. Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

- Copia de seguridad del Software Integrado IAS
- Copia de seguridad información de usuarios
- Copia de seguridad del Active Directory del servidor
- Copia de seguridad de las páginas web de INFITULUA E.I.C.E.(EXTERNO lo hace el servidor de Hosting COLNODO)
- Copia de seguridad de la página intranet

Actividades durante el Desastre (PLAN DE EMERGENCIAS)

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

PLAN DE EMERGENCIAS

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

a. Buscar Ayuda de Otros Entes

Es de tener en cuenta que solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro causen más daños o destrucciones.

- Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda.

- Todo el personal debe conocer la localización de vías de Escape o Salida: Deben estar señalizadas las vías de escape o salida.

- Instruir al personal de la entidad respecto a evacuación ante sismos, a través de simulacros, esto se realiza acorde a losprogramas de seguridad organizadas por Defensa Civil a nivel local u otros entes.

- Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad

b. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades.

d. Entrenamiento

Se debe establecer un programa de practicas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a

los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr 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 los Directivos y Ejecutivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a. Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de INFITULUA E.I.C.E. se debe atender los procesos de Contabilidad, Tesorería, Presupuesto, Ventanilla Única y demás Sistemas de Información primordiales para el funcionamiento de la Entidad, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b. Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de

nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de actividades implica la colaboración de todos los funcionarios, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones.

Los trabajos de recuperación se iniciaran con la restauración del servicio usando los recursos de la institución, teniendo en cuenta que en la evaluación de daños se contempló y gestiono la adquisición de accesorios dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

e. Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse dos tipos de recomendaciones, una la

retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

f. Retroalimentación de Actividades

Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

Activación del Plan

Decisión

Queda a juicio del Técnico Administrativo de sistemas determinar la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas.

Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 24 horas.

PLAN DE ACCIÓN EN EL PEOR DE LOS ESCENARIOS.

Antes de la activación del plan, según ente manual, debieron crearse una serie de copias de seguridad de todos los funcionarios (toda la información debe estar almacenada sobre la carpeta “Mis Documentos” de cada computador), están copias estarán almacenadas en internet, en el momento contamos con dos sitios que son:

Core FTP con HOST 200.25.22.107 Usuario: sistemas@infitulua .gov.co Clave ***** a cargo del encargado de sistemas.

Y el programa OWNCLOUD (www.owncloud.org) que se acede de la siguiente manera URL: http://archivos.infitulua.gov.co/ Usuario: AdminInfiTulua ontraseña: AdminInfiTulua/66sd&.

Una vez cumplido con todo el plan preventivo, ejecutamos los siguientes pasos:

1. Ubicar una ubicación física (casa, local, etc.) adecuada, que posea los servicios públicos de energía, agua e internet banda ancha, como mínimo. Esta búsqueda estará a cargo del gerente y la Dirección Financiera y Administrativa.
2. Se conseguirán 6 computadores, para reiniciar las tareas básicas del instituto estos estarán distribuidos así:

    - Uno actuara como servidor provisional
    - Uno para contabilidad
    - Uno para tesorería
    - Uno para cartera
    - Uno para jurídica
    - Uno para recepción y Unidad de correspondencia. (Ventanilla Única)

Estas Unidades administrativas, son primordiales en el inicio del funcionamiento de las labores después se irán restaurando las otras Unidades Administrativas según las necesidades.

3. Se debe crear una red de trabajo entre estos seis equipos y el grupo de trabajo se llamara INFITULUA E.I.C.E., no se creará el dominio ya que es una medida transitoria, mientras se evalúan los daños y se espera indicaciones de gerencia.
4. En el computador que actuará como servidor provisional, se le instalará el programa integrado IAS, FileZilla Client y los demás programas que se le instalará a los ordenadores tipo clientes, después se restaurará la última copia de seguridad del programa IAS como los archivos del Técnico Administrativo de Sistemas.
5. En los equipos restantes se instalara los programas:
    - Microsoft Office
    - Adobe Reader X
    - Win Rarr o Win Zip ó 7zip según las licencias que se tengan
    - Google Chrome
    - Google Talk
    - IAS versión cliente
6. Una vez terminada la configuración básica de trabajo, se configurarán otros equipos dependiendo de las directrices de Gerencia y Dirección Financiera, como también de los recursos tecnológicos que se tengan en el momento (impresoras, scanner, etc.).
7. Se esperaran, informes ó directrices de gerencia para hacer una restauración total del sistema una vez terminada la eventualidad que nos llevó a aplicar este plan de contingencia.

CONCLUSIONES

El presente Plan de contingencias y Seguridad en Información de INFITULUA E.I.C.E., tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información. Este Plan está sujeto a la infraestructura física y las funciones que realiza el Área de Sistemas.

El Plan de Contingencia, es un conjunto de procedimientos alternativos al orden normal de una empresa, cuyo fin es permitir su funcionamiento continuo, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo. Que una Entidad prepare su Plan de Contingencia, supone un avance a la hora de contrarrestar cualquier eventualidad, que puedan acarrear importantes pérdidas y llegado el caso no solo materiales sino personales y de información.

Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Minimización de riesgos, Identificación de posibles eventos para el Plan de Contingencia, Establecimiento del Plan de Recuperación y Respaldo, Plan de Emergencias y Verificación e implementación del plan.

No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Centro de Cómputo.

Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de INFITULUA E.I.C.E..

Adicionalmente al plan de contingencias se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados.

Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento.

Cuando el administrador de la red se encuentre ausente se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la Entidad no se vea interrumpida.

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. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere ala distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

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. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son

primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

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.

Incidente o Evento
Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido