CIFCO

CEIIIRO IDE CCHNIVENCIONIZ
EI 5AIVAPENI

Plan de contingencia equipo informático

Año 2014

Unidad de Informática

Índice

I.- INTRODUCCIÓN

A medida que las empresas e instituciones se han vuelto cada vez más dependientes de las computadoras y las redes de comunicación de datos para mejorar sus actividades, y mejorar su productividad. El Centro Internacional de Ferias y Convenciones de El Salvador (CIFCO), considera que la información es uno de los patrimonios principales de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las instituciones públicas y privadas, la seguridad del entorno informático (hardware, software, comunicaciones, etc.) se ha convertido en una de las grandes preocupaciones de los profesionales de esta actividad. Esta preocupación debe ser adecuadamente comprendida y compartida por los miembros de la junta directiva, los cuales deben considerar a las inversiones en medidas de seguridad informática, como un gasto necesario, que contribuye a mantener la operatividad y rentabilidad de la Institución.

Esto implica que los responsables del Servicio Informático, deban explicar con la suficiente claridad y con un lenguaje que sea fácil de asimilar, las potenciales consecuencias de una política de seguridad insuficiente o incluso inexistente.

Con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado desempeño de las funciones Institucionales, nos complacemos en presentar el documento "Plan de Contingencias de CIFCO".

El presente documento pretende ayudar a comprender mejor la problemática implícita de los sistemas de información soportados por el computador, de las medidas de seguridad adecuadas, tanto en su número como en su rigor y nivel de aplicación, ya que toda institución debe estar preparada para el caso de ocurrencias imprevistas.

II.- OBJETIVOS

Se tendrá en consideración lo siguiente:

a. Servir como referencia y guía al personal de CIFCO, ante eventos que pudieran comprometer el normal funcionamiento de procesos críticos, estableciendo fases, etapas y responsabilidades mientras dure la contingencia

b. Proteger y conservar los activos de la Institución, de riesgos, de desastres naturales o actos mal intencionados.

c. Evaluación tanto del impacto de los riesgos, como de los costes de las medidas de contingencia, de forma que sólo se invierta lo necesario y con un objetivo claro de rentabilidad.

d. Minimizar el número de decisiones que deben ser tomadas durante la duración de un desastre o suceso de emergencia, de manera que la correcta recuperación de los sistemas y procesos queden totalmente garantizada.

e. Reanudar tan rápidamente como sea posible las funciones más críticas de CIFCO, minimizando el impacto.

f. Minimizar la pérdida económica y de información y en general, preservar la buena imagen institucional de CIFCO.

g. Evitar en la medida de lo posible la dependencia de personas o áreas específicas de CIFCO en el proceso de recuperación.

h. Reparar rápidamente los sistemas y procesos afectados volviendo a la normalidad lo antes posible.

III.- ALCANCE

El presente Plan de Contingencia tiene como alcance a todas las Oficinas del Centro Internacional de Ferias y Convenciones de El Salvador.

V.- DESARROLLO DE LA ESTRUCTURA DEL PLAN DE CONTINGENCIA

El siguiente flujo muestra en detalle las fases y etapas por las que CIFCO atravesará una vez producido el evento que conlleve a aplicar el Plan de Contingencia.

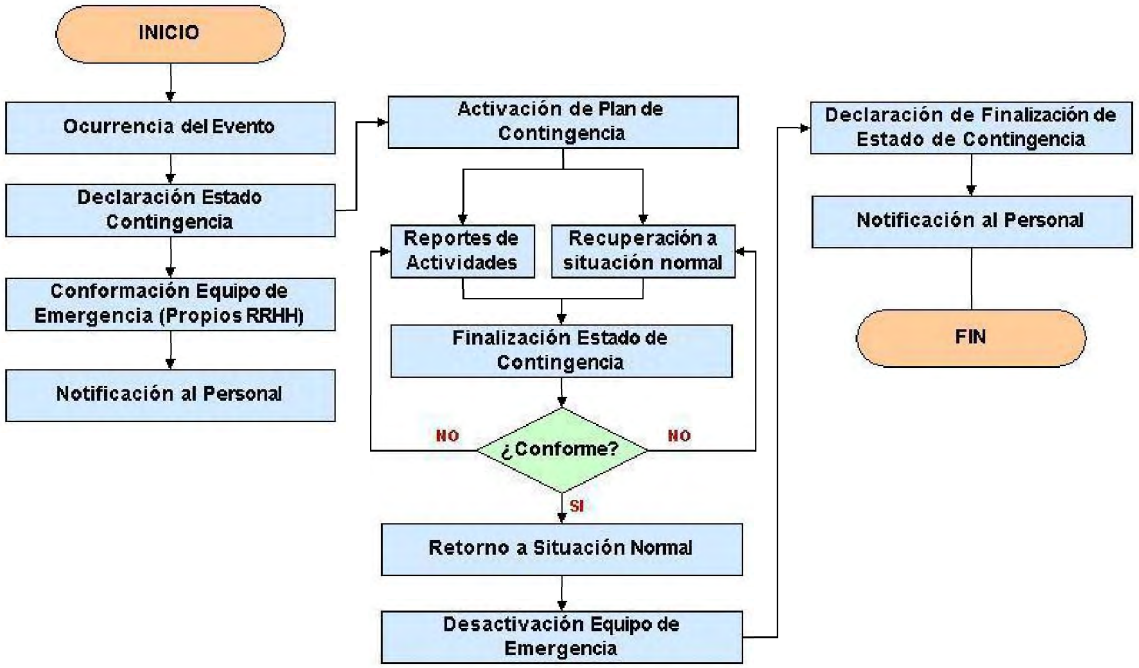


Grafico 01. Pasos a seguir en caso de desastre y activación del Plan de Contingencia

Flujo de proceso:

Ocurrencia del evento: Cuando se suscita un evento al cual se aplicara el plan de contingencia.

Declaración estado de contingencia: Se indica que se aplicara contingencia al evento suscitado.

Conformación equipo de Emergencia Propios RRHH: Definición de la persona/as que atenderán dicho evento.

Notificación al personal: Difusión al personal afectado directa o indirectamente del evento suscitado y estado de la contingencia.

VI Activación del plan de contingencia: Lo que incluye reportes de actividades, recuperación a situación normal, finalización del estado de la contingencia, todo esto dependerá del resultado de revertir los cambios a su situación normal.

Declaración de finalización de estado de contingencia: Determinar la situación bajo control total.

Notificar al personal: Notificar al personal afectado directa o indirectamente, que todo está restablecido.

VI.- IDENTIFICACIÓN DE RIESGOS

En ésta etapa y basándonos en una evaluación cualitativa, se ha realizado un análisis de los diferentes escenarios de riesgo a los cuales estaría expuesta CIFCO.

1. Activos a Proteger.

- La documentación, Base de datos y los sistemas Informáticos con los que cuenta CIFCO.
- Equipos de cómputo y conectividad.
- Software de aplicaciones y copias de respaldo.

2. Riesgos en la Seguridad Informática (equipos y archivos).

- **Incendios.**

A pesar que CIFCO tiene una buena protección contra incendios, y el personal ha sido capacitado y de esta forma se está preparado más sin embargo no se está exento a que suceda una catástrofe de este tipo y que ocasionaría pérdidas totales de información o parciales e irreparables.

- **Robo común.**

A pesar que se tiene un buen control interno relacionado al activo fijo y la seguridad de CIFCO, no se está exento a que los equipos caigan en manos inescrupulosas y pueda suceder un hecho como este y la información quede expuesta

- **Fallas en los equipos.**

Se posee un buen mantenimiento de equipos e instalaciones adecuadas y acondicionadas con buena ventilación, sin embargo no se está exento a que los equipos fallen y que de esta forma pueda haber pérdida de información.

- **Equivocaciones.**

El nivel de preparación del empleado para afrontar una equivocación.

- **Acción de virus.**

En CIFCO se posee un excelente antivirus, sin embargo jamás se está exento de una infección de virus y que pueda ocasionar daños en el software y archivos de

los equipos.

- **Terremotos.**

Ninguna institución está exenta a un desastre natural de esta magnitud, por lo cual se debe poseer algún tipo de medida para el resguardo de la información.

- **Inundaciones.**

Un incremento en las precipitaciones pluviales hiciera que las alcantarillas se colapsen provocando el deterioro de la infraestructura de la oficina, así como la documentación, y el adecuado ambiente de trabajo para el personal.

- **Fallo en el suministro eléctrico.**

Provocado por la discontinuidad en el servicio de energía eléctrica para el uso de los equipos.

- **Falla total o parcial del cableado.** ocasiona pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.

- **A la falla de Software**

Se produce debido a que no se hicieron las pruebas y la validación correspondiente del software para su utilización en implementaciones nuevas o de terceros (no diseñadas en CIFCO).

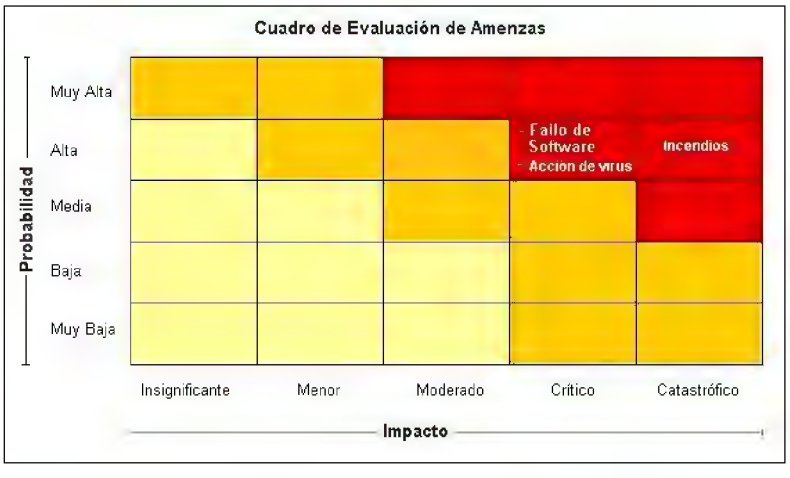
3. Probabilidad de Ocurrencia de Riesgos

TIPOS DE RIESGO	PROBABILIDAD
Fallo de Software	Alta
Acción de virus	Alta
Incendios	Alta
Fallas en los equipos	Media
Fraude	Media
Equivocaciones	Baja
Fallo en el suministro eléctrico	Baja
Fallo en el Cableado	Baja
Robo de datos	Baja
Robo común	Baja
Terremotos	Baja
Inundaciones	Muy baja

VII.- EVALUACIÓN DE RIESGOS

El análisis de riesgos es un proceso formal por el cual la organización toma conciencia de cuáles son sus activos de información, de cuál es el valor de la pérdida de uno de sus atributos (confidencialidad, integridad o disponibilidad), de cómo estos activos están amenazados y de su vulnerabilidad.

El presente Plan en base a una previa identificación de riegos, considerará sólo aquellos riesgos con mayor probabilidad de ocurrencia (muy alta y alta).



Resumen de Riesgos

Riesgo	Consecuencia	Medidas de Control
Fallo de Software	Retraso en los procesos y en la atención.	Activar Plan de Contingencia: Fallo de Software
Acción de virus	Interrupción del Servidor de Datos e Internet y de la atención.	Activar Plan de Contingencia: Acción de virus.
Incendios	Interrupción del Servidor de Datos e Internet y de la atención.	Activar Plan de Contingencia: Incendios.

La columna *Medidas de Control* nos muestra un rumbo de lo que hacer en caso se produzca alguno de los eventos mencionados. Posteriormente se detallará las características de cada una de ellas.

VIII.- ASIGNACIÓN DE PRIORIDADES A LAS APLICACIONES O PROCESOS

8.1. Fallo de Software

Es factible que durante la operativa diaria, se presenten problemas o desperfectos en el software base o en el software aplicativo, los cuales pueden manifestarse a consecuencia de situaciones no contempladas en el desarrollo de los mismos, o por requerimientos de nuevas personalizaciones, originando la no atención a los clientes.

(1) Presentado el problema el Jefe de Informática deberá declarar el estado de Contingencia, comunicar al personal a su cargo sobre tal hecho, formar el equipo de emergencia y reportarlo a Dirección Ejecutiva y Presidencia.

(2) El departamento de Informática, deberá disponer de los backups o versiones anteriores del software.

(3) Una vez reparado el software se procede a actualizar las computadoras con la versión actualizada. El equipo de emergencia debe realizar las pruebas correspondientes y dar su visto bueno.

(4) Una vez solucionado el problema, el departamento de Informática deberá declarar finalizado el estado de contingencia para el retorno a las actividades normales, se desactivará el equipo de emergencias y se

notificará sobre el retorno a la normalidad.

8.2 Acción de Virus

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

(1) Presentado el problema el jefe de informática evaluará si es necesario declarar el estado de Contingencia en caso que se encuentre en la ejecución de un proceso crítico, si es así comunicará al personal a su cargo sobre tal hecho, formará el equipo de emergencia y lo reportará a dirección ejecutiva y presidencia.

(2) El equipo de emergencia, bajo la supervisión del jefe de informática, realizará una investigación del hecho, para detectar cómo es que los equipos de cómputo se han infectado y proponer una nueva medida preventiva para este caso.

(3) 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 el equipo de emergencia retirarla del ingreso al sistema y proceder a su revisión.

(4) El equipo de emergencia deberá hacer una evaluación general de todos los equipos de cómputo para detectar posibles amenazas de este tipo con la utilización de un antivirus.

(5) El equipo de emergencia en su proceso de evaluación encontrara virus, deberá 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 al término del escaneado. Finalizado el escaneado, reconstruir el Master Boot del disco duro.

(6) Si el virus causó suficiente daño como para evitar que los equipos de cómputo operen normalmente, el equipo de emergencia deberá proceder a formatear el equipo, instalando el mismo software base y operacional. A si como los backups de la Base de Datos.

(7) Una vez terminada la evaluación, el equipo de emergencia deberá colocar en funcionamiento los equipos evaluados, asegurarse de la devolución de los equipos de cómputo prestados (si es que esto haya ocurrido) y notificar los hechos y presentar sus observaciones a dirección ejecutiva y presidencia. Propondrá medidas que eviten futuros hechos similares (como por ejemplo la obtención de un antivirus potente y de su constante actualización).

(8) Una vez solucionado el problema, el jefe de informática levantará el estado de Contingencia, notificará al personal involucrado.

8.3 Incendios

El fuego es un elemento comprendido dentro de las principales amenazas contra la

seguridad. El fuego está considerado como problema crítico en CIFCO, por varias razones: primero, porque el local está lleno de material inflamable como papel, cajas, etc. El hardware y el cableado son también fuentes vulnerables de serios incendios.

El fuego es considerado el principal enemigo del computador ya que puede destruir fácilmente los ficheros de información y programas. Además de la pérdida de ficheros o del equipo, el fuego puede causar otras pérdidas no cubiertas por el seguro. La más importante es la pérdida del "momento del negocio". Un contratiempo de semanas o meses causa irreparables daños a cualquier organización, aunque lograra situarse en las condiciones originales.

A continuación presentaremos algunos elementos en la lucha contra este tipo de amenaza.

- **MENOR MAGNITUD:**

(1) Tomar la voz de alerta y avisar a las personas presentes.

(2) Solicitar con serenidad y seguridad, que se realice la salida de todas las personas, siguiendo las rutas de evacuación señalizadas.

(3) Comprobar si alguno de los presentes tiene alguna incapacidad física o mental que le impida realizar una adecuada evacuación, para tener especial interés en ayudarlo a lograr el objetivo de salida.

(4) La persona encargada de portar el extintor, se dirigirá al lugar en el que este se encuentre y procederá a aplicarlo en la zona donde se haya producido el incendio.

(5) Una vez ubicado en la zona de la emergencia, se procederá a romper el sello de plástico del extintor o a romper el sello de seguridad que pudiera existir.

(6) Apuntar la boquilla del extintor hacia la zona de la base del fuego.

(7) Siempre se deberá operar el extintor a favor del viento. Nunca en contra de él, ya que el operador podría verse impregnado de la sustancia extintora.

(8) El extintor se deberá utilizar a una distancia de 2 a 3 metros del fuego. La sustancia nitrogenada que se encuentra en su interior, alcanza una acción de hasta 3 a 5 m. al momento en que el extintor es usado.

(9) Presionar firmemente la manija de descarga de la sustancia que se encuentra dentro del extintor.

(10) Mover la boquilla del extintor en forma de abanico hasta extinguir el fuego.

(11) Una vez usado el extintor, dejarlo echado en el suelo en señal que se encuentra descargado.

(12) Inmediatamente después de superado el incendio, proceder a realizar la recarga del extintor y volverlo a colocar en su respectiva ubicación.

(13) Se deberá tener siempre presente que luego de cualquier prueba o del uso del

extintor, la sustancia de su interior pierde potencia y por ende deberá ser recargado en lugares de confianza.

- **MAYOR MAGNITUD:**

(1) Ante todo, se recomienda conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

(2) El Equipo de Emergencia debe tratar en lo posible de trasladar los servidores fuera del Local de CIFCO, desalojando en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

(3) A su vez se comunicará a al personal de vigilancia para solicitar el apoyo de los bomberos y emergencia del hospital más cercano.

(4) Una vez solucionado el problema, se deberá declarar el estado de emergencia haciendo una evaluación de los daños producidos por el incendio, e informar a dirección ejecutiva y presidencia para su pronta normalidad del desarrollo de los procesos.

IX.- IMPLEMENTACION DEL PLAN (ACCIONES CORRECTIVAS Y PREVENTIVAS)

- **Los que afectan a la seguridad del edificio.** Preparar extinguidores, organizar las señales de evacuación, preparar bombas de extracción de agua, generadores eléctricos, etc.
- **Los que afectan la integridad de los datos.** Instalar: firewalls, antivirus, etc.
- **Topología de Red.** Preparar planos de la topología, tener equipos de repuestos de la red, herramientas necesarias todo esto en lugar de fácil acceso.
- **Copias de Seguridad:** Se realizarán de la siguiente manera:

De forma periódica la información, es decir la base de datos de la empresa, es copia en un disco extraíble. Esto permite salvar la información, en caso de ruptura parcial o total, de uno o ambos servidores, o de la propia base de datos.

La restauración de la información, disminuye los tiempos de inactividad, en caso de rupturas parciales o totales de uno o ambos servidores o de las bases de datos, dado a que se cargaría el CD-ROM con el backup del día, o del mes (según corresponda) y se instalarían nuevamente los sistemas operativos en los terminales y de red, para levantar la contingencia.

X.- RECOMENDACIONES

- Se recomienda brindar un mantenimiento de forma periódica a este plan.
- Se recomiendan capacitaciones al personal de informática en relación a seguridad informática con el fin de implementar nuevas estrategias en dicho plan.
- Se recomienda la evaluación de otro tipo de tecnologías para realizar respaldos de forma eficiente y eficaz.