PLAN DE RECUPERACIÓN Y CONTIGENCIA INFORMATICA

PLAN DE RECUPERACIÓN Y CONTIGENCIA INFORMATICA

Contenido

1.1. Objetivos 2
1.1.2. Objetivos Específicos 2
1.2. Alcance 2
2. MARCO CONCEPTUAL 2
2.1. Definiciones: 2
3. ANALISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS 4
3.1.1. Posibles daños: 5
3.1.2. Fuentes de daño: 5
3.1.3. Clases de riesgo 6
3.2. Factores asociados con la seguridad lógica 6
3.3. Factores asociados con la seguridad técnica integral 6
3.4. Minimizar el Riesgo 6
3.4.1. Incendio o fuego 6
3.4.2. Robo común de equipos y archivos 7
3.4.3. Falla en los equipos 8
3.4.4. Acción de virus informático 9
3.4.5. Terremoto 9
3.4.6. Sabotaje 10
4. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION 11
4.1. Actividades previas al desastre 11
4.2. Falla en las comunicaciones (Teléfono, internet) 11

1.1. Objetivos

1.1.1. Objetivo General

Formular un adecuado Plan de recuperación y contingencia informática, que permita la continuidad en los procedimientos informáticos de la fundación- FUNDACOBA, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la fundación.

1.1.2. Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en la fundación- FUNDACOBA que pueda ser suspendida completa o parcialmente la prestación del servicio.
- Establecer los niveles de complejidad de las fallas del sistema y los posibles tiempos de no disponibilidad de los diferentes softwares.

1.2. Alcance

El Plan de recuperación y contingencia informática Informático está basado en la realidad que manifiesta la fundación- FUNDACOBA, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

2. MARCO CONCEPTUAL

2.1. Definiciones:

AMENAZA: Probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

CONTIGENCIA: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

ELEMENTOS EN RIESGO: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de “0” (no hay daños) a “1” (daño total).

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

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.

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.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Fundación ante la eventualidad que lo afecte de forma parcial o total.

3. ANALISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

3.1. Factores de afectan la seguridad física y la infraestructura Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales como los ataques terroristas. Ambos riesgos tienen su origen de causas externas a la fundación- FUNDACOBA y su grado de previsión es muy mínimo. La probabilidad de origen natural es baja, mientras, que los riesgos artificiales son de probabilidad media.

De igual forma, se encuentran las descargas o cortes eléctricos, los cuales pueden generar interrupción en las labores administrativas que pueden afectar la atención a los usuarios.

Para la clasificación de los activos de la tecnología informática de la institución se han considerado tres criterios:

- Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderado, grave y muy severo).
- Frecuencia del evento: Puede ser (Nunca, aleatorio, periódico o continuo).
- Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de contingencia: Son procedimientos que definen como una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- Leves (caídas de energía de corta duración, fallas en disco duro, equivocaciones, daño de archivos, acceso no autorizado etc.)
- Severas (Destrucción de equipos, incendios, inundaciones, daño de equipo, robos, etc.)

Riesgo: Es la vulnerabilidad de un activo o un bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgos:

- Riesgos Naturales (Mal tiempo, terremoto, inundaciones, etc.)
- Riesgos tecnológicos (Incendios eléctricos, fallas de energía y accidentes de transmisión y transporte).
- Riesgos sociales (Actos terroristas, desordenes, entre otros).

Tipos de contingencias de acuerdo al grado de afectación:

- En el mobiliario
- En el equipo computo en general (Procesadores, unidades de disco, impresoras)
- En comunicaciones (ruteadores, nodos, líneas telefónicas)

3.1.1. Posibles daños:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución fuera de la institución sea mediante robo o infidelidad del personal.

3.1.2. Fuentes de daño:

- Acceso no autorizado.
- Ruptura de las claves de acceso a los sistemas computacionales.
- Desastres naturales (terremotos, inundaciones, falla en los equipos de soportes causados por el ambiente, la red de energía eléctrica o el mal acondicionamiento de los equipos.
- Fallas del personal clave (enfermedad, accidente, renuncias, abandono del puesto de trabajo.)
- Fallas de hardware (fallas en los servidores o falla en el cableado de red, Router, etc.)

3.1.3. Clases de riesgo

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

3.2. Factores asociados con la seguridad lógica

Estos riesgos están asociados con fallas en el funcionamiento de los equipos o de los programas de protección, cuyo deterioro o mal uso pueden generar:

- Daños en Discos duros, controladores de red, etc.
- Fallas en equipos de comunicaciones (switches, Routers)
- Daños graves en los archivos del sistema, por error de Hardware o Software
- Ingreso de virus u otros programas malintencionados que puedan dañar los archivos y los equipos computó.

3.3. Factores asociados con la seguridad técnica integral

Fallas, daños y/o deterioros por mal uso, fallas de mantenimiento y/u obsolescencia para, switch's, dispositivos, backup, Pc, impresoras.

3.4. Minimizar el Riesgo

Corresponde al plan de contingencia informático minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno. Es de tener en cuenta que en lo que respeta a fenómenos naturales, se han presentado últimamente en nuestra región incendios y movimientos telúricos de poca intensidad.

3.4.1. Incendio o fuego

Grado de

negatividad: Muy

Severo Frecuencia

de evento: Aleatorio

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, algunas áreas de la fundación cuenta con un extintor debidamente cargados.	Se cumple

Situación Actual	Acción correctiva
Se ejecutó un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a todo el personal perteneciente a la brigada de emergencia. Lo que es eficaz para enfrentar un incendio y sus efectos.	Se cumple
No se realiza la copia de seguridad diariamente al servidor de Backup.	Realizar copia de seguridad diariamente al servidor de Backup y además realizar Backup del servidor mensual, almacenándolo en donde lo dispongan (CD- ROM, disco duro, base de datos u otros medios de almacenamientos).

Analizando el riesgo de incendio, es necesario almacenar los Backup en lugares donde la acción calorífica de un incendio no alcance los dispositivos de almacenamiento. Por ende, se colocarán en lugares estratégicamente distantes y cercanos a los extintores, para en caso de emergencia sea más fácil controlar el fuego y proteger los dispositivos de almacenamiento.

3.4.2. Robo común de equipos y archivos

Grado de

negatividad:

Grave

Frecuencia de

evento: Aleatorio

Grado de

impacto:

Moderado

Situación Actual	Acción correctiva
Se toma registro de la hora de entrada y salida de las personas particulares que ingresan a la fundación. En caso de que se presente un incidente, se pasará a mirar las cámaras de seguridad.	Se cumple mediante el formato
Autorización escrita firmada por coordinador responsable para salidas de equipos de la fundación.	Se cumple se elabora oficio .
Hurto a mano armada.	Solicitar la colaboración de la Policía Nacional para que realice rondas periódicas por el sector donde se encuentra ubicadas las instalaciones

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado. Tampoco se han reportado casos donde haya habido hurtos de nuestro sistema computo en la fundación, sin embargo, se recomienda siempre estar alerta.

3.4.3. Falla en los equipos

Situación Actual	Acción correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Colocar estabilizadores a todos los equipos de la Fundación.

Analizando el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo a los equipos computo e implementar estabilizadores a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.

3.4.4. Acción de virus informático

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 debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.

Situación Actual	Acción correctiva
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
Los antivirus no se actualizan periódicamente en cada equipo.	El encargado del mantenimiento de equipos instalará y revisara periódicamente que los antivirus de los equipos sigan con la licencia, de lo contrario la tienen que renovar.

Tener actualizado e instalado los antivirus para todos los equipos computo de la Fundación Social y Cultural San Antonio de Padua - FUNPADUA para prevenir daños por causa de un virus informático.

3.4.5. Terremoto

- **Sin Pérdida O Daños Menores De Las Instalaciones:** El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto que provocaría en la fundación o UDS sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.
- **Con Pérdida De Las Instalaciones:** La pérdida de las instalaciones afectaría gravemente a las operaciones de la Fundación o UDS 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.

3.4.6. Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Firma del acuerdo de confidencialidad y seguridad de la información por cada colaborador.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en la fundación

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso de pérdida de la información y confidencialidad de la misma. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Mantener adecuados archivos de reserva (backup)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (Logs) de transacción como medida de seguridad.

4. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

4.1. Actividades previas al desastre

Se considera las 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).

Sistemas de Información: La Entidad cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backup.

Equipos de Cómputo: Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, módems, 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 o buscar información importante.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

4.2. Falla en las comunicaciones (Teléfono, internet)

Ante una falla en las comunicaciones (telefonía fija e internet), se optará por la telefonía móvil, para lo cual se informará el número celular de emergencia a las entidades aseguradoras que con mayor frecuencia tenemos contacto, esta línea la tendría a cargo el recepcionista y los líderes de los procesos.

Para soportar una falla en las comunicaciones, la clínica realizara las siguientes actividades:

- Contar con un celular con minutos permanente en registro y control.

- Entrenar al recepcionista para que pueda brindar la información adecuada ante estos casos.