PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD 2024

EMPRESAL SOCIAL DEL ESTADO SAN VICENTE DE PAUL

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD 2024

ESE HOSPITAL SAN VICENTE DE PAUL

INTRODUCION

El plan en cuestión es una herramienta que ayuda a que los procesos críticos de la E.S.E. SAN VICENTE DE PAUL Guatapé, a que continúe funcionando a pesar de una posible falla en los sistemas computarizados. Es decir un plan que le permite seguir operando aunque sea al mínimo.

Las causas pueden ser variadas y pasan por un problema informático, un fallo en la correcta circulación de información o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones.

El hecho de preparar un plan de contingencia no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas con anterioridad y que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

Normalmente, el grado de pérdida causado por una interrupción del servicio está directamente relacionado con el lapso de tiempo en que la interrupción afecta al procesamiento. El plan debería minimizar este tiempo mediante la documentación y priorización de los pasos críticos requeridos para restaurar el procesamiento. La minimización del tiempo de recuperación minimizará las pérdidas.

OBJETIVOS DEL PLAN

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

MARCO LEGAL

Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, articulo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Articulo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Decreto 1537 de 2001, por el cual se reglamenta parcialmente la ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. Cuarto parágrafo. Son objetivos del sistema de control interno (…) definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones… Articulo 3. El rol que deben desempeñar las oficinas de control internos (…) se enmarcan en cinco tópicos (…) valoración de riesgos. Articulo 4. Administración de riesgos. Como parte integral del fortalecimiento de los sistemas de control interno en las entidades publicas (…).

ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN.

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, tres serían las medidas a preparar para ser utilizadas en relación a la cronología del fallo.

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 de el se puedan derivar.

Es un concepto aplicable a cualquier actividad, no sólo a la informática, en la que las personas hagan uso particular o profesional de entornos físicos.

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 una empresa.

La probabilidad de que ocurra un desastre es muy baja, pero si se produce, su impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que, junto con el Centro Alternativo de Proceso de Datos, constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

Son puntos imprescindibles del plan de contingencia:

- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas
- Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.
- Determinar las prioridades del proceso, por días del año, que indiquen cuales son las aplicaciones y sistemas críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer objetivos de recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de desastre y el momento en el que el centro alternativo puede procesar las aplicaciones críticas.
- Asegurar la capacidad de las comunicaciones.
- Asegurar la capacidad de los servidores back-up.

Después

Los contratos de seguros vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades que se puedan derivar para el centro de proceso de datos una vez detectado y corregido el fallo.

CONCEPTOS GENERALES

Usuario
Definido como la persona que tiene cualquier grado de participación con el sistema de información, en cualquiera de sus componentes o actividades (entrada, almacenamiento, procesamiento o salida de información).

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, sea difundidas o transmitidas 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 a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

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.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

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).
Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

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 el intento de obtener de modo no autorizado la información confiada a una computadora.

Ataque Activo
Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ataque Pasivo
Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

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
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

Golpe (Breach)
Es una violación exitosa de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Seguridad Integral de la Información
La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

Con relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

PLAN DE CONTINGENCIA

Operaciones críticas

Se definieron cuales son las operaciones críticas en función a los componentes de los sistemas de información los cuales son: Datos, Aplicaciones, Tecnología Hardware y Software, sistemas de telecomunicaciones, instalaciones y personal.

Riesgos

A continuación se detallan algunos de los riesgos y consecuencias relacionados con un planeamiento de contingencia inadecuado:

- 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.
- A la acción de virus, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A accesos no autorizados, filtrándose datos no autorizados.

- A Fallas en el software
- A problemas con corriente eléctrica
- A perdida de información
- A la violación del sistema de seguridad
- Al daño del sistema de telecomunicaciones
- Al daño de la red de sistemas

Probabilidad de que tenga efecto alguno de los riesgos:

- Al fuego, que puede destruir los equipos y archivos.
    - La institución cuenta con diversos extintores, el personal ha tenido varias capacitaciones sobre uso de los extintores, pero no cuenta con sistemas de aspersión automática.
    - No existen detectores de humo.
- Al robo común, llevándose los equipos y archivos.
    - La institución cuenta con un guardia de seguridad en horario nocturno.
    - El centro de cómputo permanece cerrado.
    - Esta ubicado en un lugar de poca circulación de usuarios.
    - La institución cuenta con circuito cerrado de cámaras.
- Al vandalismo, que dañen los equipos y archivos.
    - Es difícil de que ocurra en la institución, aunque existen áreas de atención al usuario muy expuestas que pueden ser objeto fácil de estas actividades.
    - El área de sistemas esta ubicado en un lugar de poca circulación, el cual está poco expuesto.

- A fallas en los equipos, que dañen los archivos.

    - A los equipos se les realiza mantenimiento preventivo y correctivo con dos visitas al año, el hardware actual en un 30% aproximadamente esta pendiente de actualización o reposición por equipos nuevos ya que su tecnología no satisface los requerimiento del software aplicativo y del de uso general.

- A equivocaciones, que dañen los archivos.

    - El personal administrativo en su mayoría es empírico en el manejo de sistemas por lo tanto su uso se limita a las aplicaciones especificas de la empresa, por lo anterior se tienen programadas capacitaciones para reforzar la utilización de la tecnología informática.

    - El sistema actual de la empresa corre en ambiente cliente servidor proporcionando seguridad dependiendo de los permisos que se asignen por modulo y adicionalmente a este existen permisos por pantallas y acciones con lo cual se limita la acción que pueda poner inestable el sistema.

- A la acción de virus, que dañen los equipos y archivos.

    - El hospital tiene licencia de antivirus hasta Mayo del año 2024, el cual se actualiza por Internet diariamente, y tiene soporte permanentemente por la empresa la cual esta ubicada en la ciudad de Bogotá permitiéndole de esta forma estar libre de virus.

- A terremotos, que destruyen equipos y los archivos.

    - El edificio no cumple con las medidas antisísmicas.

- A accesos no autorizados, filtrándose datos no autorizados.

    - El hospital cuenta con un sistema cliente servidor que le permita autorizar accesos dependiendo de la función que realice el usuario.

- A Fallas en el software
    - La falla del software está dada por la actualización, la cual en su mayoría presenta problemas de desarrollo, lo que ocasiona retrocesos de la información y atrasos en la puesta en marcha de los aplicativos.
- A problemas con corriente eléctrica
    - El Hospital cuenta con una planta eléctrica, así como con UPS para la mayoría de las estaciones de trabajo que le permiten seguir funcionando por algunos minutos mientras se estabiliza la corriente eléctrica.
- A pérdida de información
    - La E.S.E. realiza copias de seguridad diariamente, de todo el sistema de los módulos del software; se realiza una copia mensual después de realizar el cierre del respectivo mes.
- A la violación del sistema de seguridad
    - El sistema cuenta con un log de transacciones que le permite verificar las transacciones que están realizando los usuarios.
- Al daño del sistema de telecomunicaciones
    - La pérdida de las telecomunicaciones es una amenaza externa y su resolución depende de la empresa externa con la cual se tiene el contrato de telefonía y de internet.
- Al daño de la red de sistemas
    - Se programaron visitas de mantenimiento preventivo que garanticen el adecuado funcionamiento de la red de sistemas.

La orientación principal de un plan de contingencia es la **continuidad de las operaciones** de la empresa, no sólo de sus sistemas de información.

Definición de los niveles mínimos de servicio.
Funcionamiento del sistema de información las 24 horas del día, los 365 días del año.

Identificación de las alternativas de solución.

Daño lógico de los archivos de base de datos

- Mantenimiento de copia de seguridad diariamente.
- Almacenamiento de las copias de seguridad en un lugar adecuado tanto interna como fuera del hospital.

- Daño físico del Disco Duro
  - Efectuar en forma periódica revisiones de la superficie del disco.
  - Realizar mantenimiento preventivo dos veces al año.
  - Mantener un adecuado sistema de corriente regulada que permita mantener el fluido eléctrico constante y sin variaciones significativas que afecten el sistema.
  - Mantener el sistema de espejo (Adquision de Discos duros) y compra de servidores.
  - Mantener un disco duro disponible para entrar a operar en un momento dado.
- Perdida de Información
  - Realizar copias de seguridad, evaluar la integridad de los datos.
- Ataque de Virus
  - Mantener el antivirus actualizado, los parches del sistema operativo, administrador de bases de datos.
  - Realizar verificaciones periódicas a todas las unidades del sistema en busca de virus.
  - Mantener utilidades que permitan bloquear accesos no autorizados
- Problemas con corriente eléctrica
  - Garantizar el adecuado funcionamiento de la UPS, en los servidores, así como la oportunidad en el encendido de la planta eléctrica.
  - Realizar visitas de mantenimiento preventivo del cableado eléctrico y de datos que permita garantizar el suministro de corriente eléctrica y el transporte de datos, imagen y

sonido sin ningún contratiempo.

- Violación del sistema de seguridad del software
    - Establecer políticas de seguridad que permitan mantener control de los usuarios que tienen acceso a la red, así como de los permisos.
    - Implementar como política el cambio de clave periódica (cada 30 días) de los usuarios tanto para ingresar a la red como para usar el software.
    - Establecer como política de sistemas, a implementación de claves alfanuméricas de mínimo ocho (8) caracteres.
- Caída de la red
    - Establecer planes de mantenimiento preventivo, como medidas de control, para garantizar el adecuado funcionamiento de la red.
- Sustracción de servidores.
    - Mantener la oficina de sistemas cerrada con seguro, no permitir la entrada de personal no autorizado en ella.
    - Instalación de alarmas en la oficina de sistemas.
- Problemas de software.
    - Realizar contratos periódicos con la empresa desarrolladora del software para mantener actualizado el sistema, así como garantizar el soporte técnico requerido para subsanar los problemas técnicos que se puedan presentar.

Costes estimados: El costo del plan de contingencia esta dado por el mantenimiento preventivo y correctivo, el licenciamiento del software antivirus, las copias de seguridad (Tape backup), el costo del almacenamiento de las copias de seguridad.

Mantenimiento preventivo

- Dos (2) mantenimientos preventivos al año (Junio-Diciembre) al hardware, software y la red de datos.
-

- Actualización de antivirus EsetNod 32.

Recursos necesarios: Discos duros externos, CD-DVD RW, Software antivirus, personal calificado para realizar el mantenimiento preventivo y correctivo.

DETERMINACIÓN DE NECESIDADES DE SOPORTE

Evaluación de proveedores de servicios

El proveedor de hardware para las estaciones de trabajo tiene una respuesta aceptable en un rango de 8 horas, con lo cual no se afecta el sistema.

Para los servidores se cuenta con varios proveedores, sin embargo para las partes específicas de estas maquinas, existen algunos repuestos que deben ser pedidos a Bogota, con una demora de 24 a 48 horas aproximadamente.

ESTRATEGIAS DE EMERGENCIAS

Acción: Utilizar medios de almacenamiento externo (CD y discos externos) para guardar la información para las siguientes contingencias:

- Perdida de información
- Daño lógico de los archivos de base de datos
- Daño físico del Disco Duro

Observación: La copia de la base de datos se realizara diariamente asi:

Copia en disco duro (servidor) completa a las 12:00 am.
Copia en disco duro externo completa a las 12:00 am.
Copia en disco duro (servidor) completa: a las 06:00 pm.

Cada mes se generara una copia de toda la información de los aplicativos de historia clínica, Paisoft, Datalab y archivos administrativos.

Acción: Ejecutar utilidades de revisión de discos duros periódicamente para las siguientes contingencias.

- Pérdida de información
- Daño físico del Disco Duro

Acción: Tener un disco duro alterno para las siguientes contingencias

- Perdida de información
- Daño físico del Disco Duro
- Daño lógico de los archivos de base de datos

Acción: Contar con UPS para los servidores y aplicaciones críticas como el digitalizador de imágenes para las siguientes contingencias:

- Problemas con corriente eléctrica.

Acción: Mantener un software antivirus actualizado, así como las actualizaciones del sistemas operativo, programa de correo electrónico, navegador de internet.

- Problemas con Virus

Acción: Administrar los accesos al personal de la institución a través de claves, que sólo permita el ingreso a los aplicativos que necesite para su desempeño, y el cambio periódico de las claves de accesos para evitar fraudes.
Limitar los recursos compartidos, y establecer una clave por cada recurso compartido.

- Seguridad del sistema

Acción: realizar chequeos periódicos de la red para evitar caídas de puntos de red, bloqueos, sobrecarga del sistema.

- Caída de la red.

COMPONENTES DEL PLAN

Recurso Humano: Ingeniero de Sistemas
Recurso de hardware: Disco duro, medios externos (CD), Discos duros externos, UPS, escaneadores de red, ponchadora para RJ45.
Recurso de software: Programa de copias de seguridad, Utilidades de desfragmentación, escaneo de discos y revisión de discos, antivirus, actualización de software, herramientas para la supervisión de la red.
Documentación: Manual del administrador del sistema.
Capacitación: Las capacitaciones del software de historia clínica y módulos administrativos se implementaran en la medida que vayan llegando usuarios de sistema nuevos a la institución.

Capacitación al personal en operación de Software de oficina y Sistemas operativos.

ACTIVIDADES

ACTIVIDADES	INDICADORES		
	NOMBRE DEL INDICADOR	FORMULA	META
• Utilizar medios de almacenamiento externo (CD y discos externos) para guardar la información • Ejecutar utilidades de revisión de discos duros periódicamente ○ Tener un disco duro alterno ○ Contar con UPS para los servidores y aplicaciones críticas ○ Administrar los accesos al personal de la institución a través de claves ○ Limitar los recursos compartidos, y establecer una clave por cada recurso compartido.	Proporción de actividades ejecutadas	Total de actividades ejecutadas acorde al plan/ total de actividades proyectadas	90%