MINISTERIO DE SALUD

Dirección General

HOSPITAL "VÍCTOR LARCO HERRERA"
OFICINA DE COMUNICACIONES
18 JUN. 2009
RECIBIDO
Por..... Hora.....13:04

RESOLUCION DIRECTORAL

N° 115 -DG-HVLH-2009

Magdalena del Mar, 03 de Junio del 2009

VISTO, el Memorando Nº 040-SDG-HVLH-2009, emitido por el Sub Director General del Hospital "Víctor Larco Herrera" quien solicita aprobación del Plan de Contingencia Año 2009,

CONSIDERANDO:

Que, la Institución, cuenta con equipos informáticos y periféricos necesarios para el desarrollo de sus actividades, los mismos que son susceptibles de ***siniestros;***

Que la Oficina de Estadística e Informática ha elaborado un Plan de Contingencia Informático correspondiente al año 2009, que norma las acciones y procedimientos que permite reducir y eliminar el riesgo de ***siniestros*** *siendo necesario aprobar dicho documento mediante Resolución Directoral;*

Estando a la propuesta por la Dirección de Estadística e Informática y con la aprobación de la Sub Dirección General y con el Visado de la Oficina de Asesoría Jurídica;

De conformidad con el literal c) del articulo 11º del Reglamento de Organización y Funciones del Hospital "Víctor Larco Herrera" aprobado por Resolución Ministerial Nº 132-2005/MINSA;

SE RESUELVE:

Artículo 1º.- *APROBAR, el* ***PLAN DE CONTINGENCIA INFORMATICO AÑO 2009*** *del Hospital "Víctor Larco Herrera", cuyo texto forma parte integrante de la presente Resolución.*

Artículo 2º.- *Encargar a la Dirección de Estadística e Informática la formulación, programación coordinación, ejecución y control del Plan de Contingencia de los Equipos Informáticos del Hospital "Víctor Larco Herrera".*

Artículo 3º.- *Encargar a la Oficina de Comunicaciones la publicación de la presente Resolución y el Plan de Contingencia Informático 2009, en el Portal de Internet del Hospital "Víctor Larco Herrera".*

Regístrese y comuníquese

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"

Dra. Cristina Eguiguren Li
Directora General
CMP. 17899 RNE. 8270

CAEL/AESG/msm

PLAN DE CONTINGENCIA INFORMATICO AÑO 2009

HOSPITAL VICTOR LARCO HERRERA

MINISTERIO DE SALUD HOSPITAL VICTOR LARCO HERRERA OF. ESTADISTICA E INFORMATICA

PLAN DE CONTINGENCIA INFORMATICO HOSPITAL VICTOR LARCO HERRERA 2009

PRESENTACIÓN

El Hospital Víctor Larco Herrera, es la entidad Decana de la Psiquiatría Latinoamericana, por ello es una fuente importante de información no solo científica y como una gran institución también de información administrativa.

Consideramos a la información como patrimonio de toda institución a pesar que es un Bien no tangible, pero tan importante como el equipo mas costoso de toda institución.

A medida que la tecnología ha ido evolucionando y con ella, la envergadura de los sistemas de información de las instituciones estatales y particulares, la seguridad del entorno informático (hardware, software, comunicaciones, etc) se ha convertido en una de las grandes preocupaciones de los, profesionales de estas ramas y personal en general.

Día a día el personal de informática se encuentra con dificultades nuevas tanto internas como externas, vale decir se puede uno encontrar con un usuario que guarda información relevante en una carpeta oculta dentro de un directorio designado para el sistema (ejem. Directorio Windows) y al restaurar el sistema operativo esta se pierde, o a los diarios ataques de virus, malwares, gusanos, troyanos etc. Que vulneran la información.

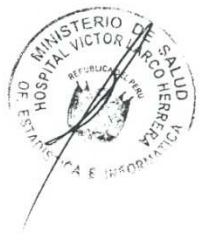
Es muy importante para el personal del área de informática que esta preocupación sea comprendida claramente por las autoridades del hospital.

Esto implica que los responsables de los servicios informáticos expliquen con propiedad y suficiente claridad, las potenciales consecuencias de una política de seguridad ineficiente o carente de ella, lo que seria mas grave aun.

El Plan de Contingencia Informático debe contemplar los planes de emergencia, backup, recuperación comprobación.

Este plan permitirá recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal informática institucional.

El área de redes ofrece este proyecto de Plan de Contingencia poniéndola a disposición de la Oficina de estadística e Informática así como todas las unidades orgánicas de la Institución.



Plan de Contingencia Informático

Para proteger información vital ante la posible pérdida, destrucción, robo y otras amenazas el Hospital debe preparar un completo plan de contingencia informático. Un Plan de Recuperación de Desastres (DRP) informático debe tener los siguientes componentes:

- Emergencia
- Back-Up
- Recuperación
- Simulación
- Mantenimiento

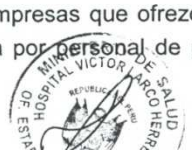
El plan de "emergencia" indica las acciones que deben tomarse inmediatamente tras el desastre. Un importante aspecto de este plan es el diagrama de organización de la contingencia, para ello se deberá nombrar **personal responsable de la contingencia** así como **un coordinador de contingencia**.

1.- Designar Personal Responsable.-
Por lo general los responsable de las contingencias pueden ser uno o dos trabajadores del área de Informática con conocimiento de Bases de datos y como coordinadores de la contingencia un personal usuario de las principales Bases de datos de la institución SIGA (Logística), SIAF (Economía) y de la Historia Clínica Electrónica.

2.- Preparación de un plan de "backup".
Este documento es un elemento primordial y necesario para la recuperación. La selección de un backup alternativo requiere una cuidadosa preparación. El Hospital debe considerar todas las alternativas tecnológicas y de servicios disponibles en el mercado.

3.- **El Plan de "recuperación".**
El Hospital debe establecer su capacidad real para recuperar información crítica en un periodo de tiempo aceptable. Una parte importante del plan de recuperación es el equipo de recuperación.

Se debe contar además con una base de datos de empresas que ofrezcan servicios ante una situación crítica que no pueda ser superada por personal de planta por la falta de algún equipo de tecnología avanzada.



También es importante contemplar la indisponibilidad de parte del personal informático. Incluso con el plan de contingencia más elaborado, pueden ser necesarios uno o dos días hasta que el centro de backup pueda empezar cualquier tipo de procesamiento de datos.

3.1 .- Imágenes de los Sistemas Operativos, aplicaciones y configuración.- Una de als principales medidas que se vienen implementando es la creación de Archivos imágenes de los computadores en esos archivos (que se dejan en la Unidad D del disco duro y el CDs).

Estas imágenes permitirán la restauración de los sistemas operativos, aplicaciones, información y configuración en un tiempo aproximado de 30 minutos de ser el caso de una estación de trabajo. Otra ventaja de la elaboración de archivos imágenes es que la restauración se podrá realizar sin mover el equipo de su modulo. (solo en el caso de fallas lógicas en los sistemas operativos o aplicaciones).

Este retraso requiere que el Hospital centre sus esfuerzos en ejecutar esos procesos informatizados de gestión esenciales para la supervivencia de la organización.

Como consecuencia, el equipo de recuperación debe establecer prioridades claras sobre que tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa de cuales de los procesos son críticos y cuales son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión, ese tipo de decisiones se realizan de forma más simple teniendo en cuenta los centros de trabajo alternativos, planes de trabajo, instalaciones de backup, necesidades de software, necesidades de personal, seguridad y requerimientos de documentación.

5.- Plan de "Mantenimiento"

Cualquier cambio necesario debe ser integrado dentro del plan previamente documentado. Debe prepararse un plan de acción, para incorporar e implementar dichos cambios de forma fehaciente para asegurar incluso mayor protección frente a los desastres.

6. De las Claves de Acceso.- Las Claves de acceso de los programas, sistemas estatales (SIAF, SIGA, RECAVE, SISMED, etc. Etc.), así como las claves de los Sistemas Operativos, claves de firewall, clave del Acceso al Servidor de la Pagina Web, otros; deberán hacer de conocimiento al Área Técnica (Oficina de Estadística e Informática) bajo responsabilidad funcional, las misma que solo serán utilizadas en casos de cualquier contingencia, de igual modo estas claves de acceso también deberán ser entregadas a la Dirección General en Sobre cerrado y debidamente lacrado.

Beneficios de un Plan de Contingencias Informático.

El plan de contingencia informático se considera como un control correctivo. No se trata por tanto de prevenir o detectar posibles desastres, sino de limitar las pérdidas ocasionadas por desastres comunes.

La existencia de un plan de contingencia habilita a las instituciones para poder recuperar de la forma más rápida posible sus capacidades de procesamiento de información crítica para su supervivencia y poder proveer productos y servicios a sus clientes eficiente y eficazmente.

ESQUEMA GENERAL

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en este documento se hará un análisis de los riesgos, ver cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema. Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan
de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio 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 posible.

Haciendo un esquema, el Plan de Contingencias abarcará los siguientes aspectos:

1.- Plan de Reducción de Riesgos (Plan de Seguridad).

2.- Plan de Recuperación de Desastres.

2.1.- Actividades Previas al Desastre.

2.1.1.- Establecimiento del Plan de Acción.

2.1.2.- Formación de Equipos Operativos.

2.1.3.- Formación de Equipos de Evaluación (auditoria de cumplimiento de procedimientos de Seguridad).

2.2.- Actividades durante el Desastre.

2.2.1.- Plan de Emergencias.

2.2.2.- Formación de Equipos.

2.2.3.- Entrenamiento.

2.3.- Actividades después del Desastre.

2.3.1.- Evaluación de Daños.

2.3.2.- Priorización de Actividades del Plan de Acción señaladas en 2.1.1

2.3.3.- Ejecución de Actividades

2.3.4.- Evaluación de Resultados.

2.3.5.- Retroalimentación del Plan de Acción.

4. PLAN DE RIESGOS (PLAN DE SEGURIDAD)

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

4.1 ANALISIS DE RIESGOS

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado. El análisis de riesgos supone responder a preguntas del tipo:
¿Qué puede ir mal?

¿Con qué frecuencia puede ocurrir?

¿Cuáles serían sus consecuencias?

¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

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

¿Qué se intenta proteger?

¿Cuál es su valor para uno o para la institución?

¿Frente a qué se intenta proteger?

¿Cuál es la probabilidad de un ataque?

A continuación se muestra un conjunto de puntualizaciones que deberán tomar en cuenta el o los responsables de la oficina de Estadística e Informática junto con los responsables de las áreas usuarias:

¿A qué riesgos en la seguridad informática se enfrenta la Institución?

1. Al fuego, que puede destruir los equipos y archivos.
2. Al robo común, llevándose los equipos y archivos.
3. Al descuido o indiferencia, que dañen los equipos y archivos.
4. A fallas en los equipos, que dañen los archivos.
5. A equivocaciones, que dañen los archivos.
6. A la acción de virus, que dañen los equipos y archivos.
7. A accesos no autorizados, filtrándose datos no autorizados.
8. Al robo de datos, difundiéndose los datos sin cobrarlos.
9. Al fraude, desviando fondos merced a la computadora.

4.2 ANALISIS DE FALLAS EN LA SEGURIDAD

Esto supone estudiar las computadoras, su software, localización y utilización con el objeto de identificar los resquicios en la seguridad que pudieran suponer un peligro. Por ejemplo, si se instala una computadora personal nueva, para recibir informes de inventario desde otras PCs vía MODEM situados en lugares remotos, y debido a que el MODEM se ha de configurar para que pueda recibir datos, sea abierto una vía de acceso al sistema informático. Habrá que tomar medidas de seguridad para protegerlo, como puede ser la validación de las clave de acceso.

4.3 PROTECCIONES ACTUALES

- Generales, se hace una copia ínterdiaria de los archivos que son vitales para la Institución.
- Robo común, se cierran las puertas de entrada y ventanas.

- Falla de los equipos, se tratan con cuidado, se realiza el mantenimiento de forma regular, no se permite fumar, está previsto el préstamo de otros equipos.

- Daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus. Los programas de dominio público y de uso compartido (Shareware), sólo se usan si proceden de una fuente fiable. Está prohibido la descargas de juegos software y música por Internet según como se aprecia en el documento de normatividad informática debido a que de esa manera se pueden filtrar los virus.

- Equivocaciones, los usuarios finales tienen una regular formación pero en caso de desconocimiento procuran llamar a personal capacitado para absolución de dudas.

- Acceso no autorizado, se cierra la puerta de entrada. Algunas computadoras disponen de llave de bloqueo del teclado. Varias computadoras tienen acceso bajo clave.

- Robo de datos, se cierra la puerta principal. Algunas computadoras disponen de llave de bloqueo del teclado, las claves de acceso a los servidores de información están al alcance de varios usuarios?

- El jefe coordina constantemente con el Área de Informática a fin de cambiar las claves de Acceso? Ejemplo: sistema SIAF, SIGA, etc.

- Fuego, en la actualidad se encuentra instalado Sistemas contra incendios, extinguidotes, en sitios estratégicos y se brinda entrenamiento en el manejo de los sistemas o extinguidotes al personal, en forma periódica

Pre Operatividad del Plan de Contingencia Informático

Acciones	Responsables
Conocimiento del Plan de Mantenimiento Preventivo de Equipos Informáticos	Oficina Ejecutiva de Administración Oficina de Estadística e Informática Area de Informática Soporte Técnico Area de Redes Todos los Usuarios de la Institución.
Conformación de un Equipo o Comité Tecnico con Personal que participará, antes, durante y despues de la Prueba y Monitoreo en casos de Emergencia.	Oficina Ejecutiva de Administración Oficina de Estadística e Informática Oficina de Servicios Generales Area de Informática Soporte Técnico Area de Redes Todos los Usuarios de la Institución.
Identificacion, Analisis y Selección de las Zonas Criticas, en caso de una emergencia por desastres. Especificar los escenarios donde ocurriran los problemas	Oficina Ejecutiva de Administración Oficina de Estadistica e Informatica Administrador de Redes Soporte Tecnico Todos los Usuarios
Lista de los recursos que serán utilizados, para las Operaciones en casos de emergencia por desastres	Oficina Ejecutiva de Administración Oficina de Logistica Oficina de Estadística e Informática Administrador de Redes Personal de Soporte Técnico.
Preparar la lista de personas, dependencias del Hospital Victor Larco Herrera y/o Organizaciones Externas para comunicarse (elaborar un directorio telefónico)	Oficina Ejecutiva de Administración Oficina de Estadística e Informática Central Telefonica Administrador de Redes Personal de Soporte Técnico. Todos los Usuarios
Pruebas y monitoreo, como funcionaría el Plan de Contingecia, en los casos/eventos reales en una emergencia.	Oficina Ejecutiva de Administración Oficina de Estadística e Informática Central Telefonica Administrador de Redes Personal de Soporte Técnico. Todos los Usuarios
Recuperacion del Sistema de Informacion, recuperacion de datos y retorno a la Normalidad, despues de la Emergencia.	Equipo o Comité Técnico
Evaluacion de la Ejecución del Plan de Mantenimiento Preventivo de Equipos de cómputo.	Oficina Ejecutiva de Administración Director de la Oficina de Estadística e Informática. Administrador de Redes Soporte Técnico
Informe Final Anual, de la Ejecución y Evaluacion del Plan	Director de la Oficina de Estadística e Informática.
Publicación en el portal Institucional, del Plan de Mantenimiento Preventivo, su Ejecución, y Evaluación, según corresponda.	Dirección General Oficina de Relaciones Publicas Director de la Oficina de Estadística e Informática. Responsable de la Actualizacion del Portal Institucional.

MINISTERIO DE SALUD
HOSPITAL VICTOR LARCO HERRERA
OF. ESTADISTICA E INFORMATICA