Informático

MINISTERIO DE SALUD

HOSPITAL VICTOR LARCO HERRERA

Dirección General

RESOLUCION DIRECTORAL

N° 324 -2013-DG-HVLH

Magdalena del Mar, 30 de Diciembre 2013.

Visto; la Nota Informativa Nº 128-OEPE/HVLH-2013, emitido por el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico del "Víctor Larco Herrera";

CONSIDERANDO:

Que, mediante Ley N° 27657 – Ley del Ministerio de Salud, en la cual se establece entre uno de los objetivos funcionales, el soporte logístico de bienes, servicios, infraestructura, equipo y mantenimiento, tanto de las dependencias administrativas, como de los establecimientos de salud;

Que, para el cumplimiento de las funciones de ley, es determinante generar un plan estratégico integral, así como los correspondientes Objetivos, Estrategias y Planes que dirijan y orienten el planeamiento institucional, para la prevención, mitigación de riesgos, preparación y atención, que permitan reducir los daños y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales o tecnológicos potencialmente dañinos; para ello la Oficina de Estadística e Informática del Hospital, ha elaborado un Plan de Contingencia Informático para el año 2013, que permitirá recuperar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal informática institucional;

Que, mediante el documento del Visto, el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico del Hospital Víctor Larco Herrera, manifiesta que el Plan de Contingencia Informático para el año 2013, ha sido revisado, evaluado y corregido de acuerdo a la normatividad vigente; por lo que es necesario su aprobación mediante acto resolutivo;

Que, estando a lo propuesto por el Jefe de la Oficina de Estadística e Informática y a lo informado por la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico;

Con el visado del Jefe de la Oficina de Estadística e Informática, de la Jefa de la Oficina de Asesoría Jurídica y del Director de la Oficina Ejecutiva de Planeamiento Estratégico del Hospital "Víctor Larco Herrera" y;

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

SE RESUELVE:

Articulo 1º.- Aprobar, con eficacia anticipada al 02 de enero de 2013 el **PLAN DE CONTINGENCIA INFORMATICO PARA EL AÑO 2013**, del Hospital "Víctor Larco Herrara", que el cual como anexo a fojas nueve (09), forma parte integrante de la presente resolución.

Artículo 2º.- La Oficina de Estadística e Informática del Hospital, es responsable de la difusión, implementación, supervisión y cumplimiento del documento precedente aprobado.

Articulo 3º.- Dejar sin efecto las disposiciones que se opongan a la presente Resolución.

Artículo 4º.- Disponer que la Oficina de Comunicaciones publique la presente Resolución y el documento anexo, en el portal de Internet del Hospital Víctor Larco Herrera.

Regístrese y Comuníquese

Ministerio De Salud
Hospital "Víctor Larco Herrera"
Med. Cristina Eguiguren Li
Directora General
C M P 17899 - R.N.E. 8270

CAEL//MYRV.
Distribución:

- Oficina de Planeamiento Estratégico
- Oficina de Estadística e Informática
- Oficina de Asesoría Jurídica
- Unidades Orgánicas
- Archivo.

HOSPITAL VICTOR LARCO HERRERA

PLAN DE CONTINGENCIA INFORMATICO PARA EL AÑO 2013

I.- INDICE

II.- INTRODUCCIÓN

El Plan de Contingencia es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y de las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución.

Previo a ello se hace un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la entidad. El plan de contingencias deberá ser revisado anualmente. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

El Plan de Contingencia permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada.

En nuestra Institución la Red de Computadoras se encuentra aún en proceso de estructuración, ello 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 sería más grave aún.

El Plan de Contingencia Informático debe contemplar los Planes de Emergencia, Backup, y de Recuperación.

Este Plan permitirá recobrar rápidamente el control y capacidad para procesar la información y restablecer la marcha normal de la informática institucional.

III.- FINALIDAD

Tener un Plan de Contingencias lo más completo y global posible. Definir las normas y procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los Sistemas de Información y Comunicación del Hospital, de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos.

IV.- OBJETIVO GENERALES

Un Plan de Contingencia permite prever los riesgos a los que estará sometido el sistema de información que se va a implementar.

El objetivo es doble: Por un lado, tomar las medidas necesarias para minimizar la probabilidad de que dichos riesgos se conviertan en una realidad y, por otra parte, si esto ocurriera, posibilitar que el sistema pueda responder sin que ello suponga un grave impacto para su integridad.

El presente Plan de Contingencia, involucra a toda la entidad directa o indirectamente.

De este modo, es válido en cuanto se produce con la aprobación de todas las partes implicadas, con la total asunción de responsabilidad que a cada una pudiera corresponderle.

V.- AMBITO DE APLICACIÓN

Hospital Víctor Larco Herrera

VI.- CONTENIDO.

1.- ESQUEMA GENERAL

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los medios de almacenamiento, por lo que en este documento se hará un análisis de los riesgos, ver cómo reducir la posibilidad de su ocurrencia y los procedimientos a seguir en caso que se presentara el problema. Pese a todas las medidas de seguridad puede ocurrir un desastre, por lo tanto es necesario que el Plan de Contingencia incluya un Plan de Recuperación de Desastres, el que tendrá como objetivo, restaurar el servicio en forma rápida y con el menor costo y pérdida posibles.

El esquema del Plan de Contingencias abarca los siguientes aspectos:

a.- Plan de Reducción de riesgos (Plan de Seguridad)

b.- Plan de Recuperación de Desastres

* Actividades Previas al Desastres.
  - -Establecimiento del Plan de Acción.
  - -Formación de Equipos Operativos.
  - -Formación de Equipos de Evaluación (auditoria de cumplimiento)

* Actividades durante el Desastre
  - -Plan de Emergencia
  - -Formación de equipos
  - -Entrenamiento

* Actividades después del Desastre
  - -Evaluación de Daños
  - -Priorización de Actividades del Plan de Acción
  - -Ejecución de Actividades
  - -Evaluación de Resultados
  - -Retroalimentación del Plan de Acción.

2.- ANALISIS DE RIESGOS

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.

El análisis de riesgos supone mas 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 podría. Se ha de tener en cuenta la probabilidad que suceda 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 riesgo supone responder a las preguntas del tipo:

¿Qué puede ir mal?
¿Con que frecuencia puede ocurrir?
¿Cuáles serían sus consecuencias?
¿Qué finalidad tienen las respuestas a tres primeras preguntas?
En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar con mayor fiabilidad posible a las siguientes preguntas:

¿Que se intenta proteger?
¿Cuál es su valor para uno o para la institución?
¿Frente a que se intenta proteger?

¿Cuál es la probabilidad de un ataque?

A continuación se muestra un conjunto de puntaciones que deberán tomar en cuenta el o los responsables de la Oficina de Estadística e Informática juntos 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 autorizaos.
8.- Al robo de datos.
9.- Al fraude desviando o alterando datos de fondos o recaudaciones.

a) Análisis de Fallas de Seguridad

Esto supone estudiar las computadoras, su software, localización y utilización con el objetivo de identificar los resquicios en la seguridad que pudieran suponer un peligro. Por ejemplo, si se instala una computadora personal nueva en una Oficina y este debe tener carpetas o archivos compartidos con sus pares se deberá configurar de tal modo que la seguridad se encuentre garantizada y el acceso debe ser debidamente coordinado entre los usuarios de esta información asumiendo cada uno de ellos la responsabilidad al compartirlas.

3) ALTERNATIVAS DE SOLUCION

a) El Plan de recuperación de Desastres (PRD) informático tendrá los siguientes componentes:

- Emergencia
- Back Up
- Recuperación
- Mantenimiento

b) 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 ella.

c) Designar Personal Responsable.-

Por lo general el responsable de las contingencias puede ser un trabajador de la unidad de Informática y su suplente con conocimiento de Base de Datos y como coordinadores un personal usuario de las Bases de Datos de las Unidades Orgánicas como Logística (Base de Datos SIGA), Economía (Base de Datos SIAF), Personal (Base de Datos Registro de Asistencia), Farmacia (Base de Datos de Farmacia), Central Documentaria (Base de Datos de Registro Documentario).

d) Capacitar en Administración de Sistemas Operativos de Servidores y Administración de Base de Datos al personal de la Unidad de Informática.

e) Preparación de un Plan de Backup.-

Este documento es primordial y necesario para la recuperación. L selección de un BACKUP alternativo requiere una cuidadosa preparación. La Institución debe considera todas las alternativas tecnológicas y de servicio disponibles en el mercado.

f)- El Plan de Recuperación.-

Nuestra Institución debe establecer su capacidad real para recuperar información critica en un periodo de tiempo aceptable. Una parte importante del Plan de Recuperación es el equipo de recuperación.

Es una alternativa recurrir a empresas que ofrezcan servicios de recuperación de información siempre que esta no pueda ser superada por el personal de planta debido a la falta de algún equipo de tecnología inexistente en la institución.

Es importante considerar el tiempo para la aplicación del Plan de Contingencia ya que puede ser necesario uno o dos días hasta que el BACKUP puede re empezar el procesamiento de datos.

g) Imágenes de los Programas.- Sistemas Operativos, aplicaciones y configuraciones son una de las principales medidas a aplicar, de preferencia estas deberán ubicarse en la Unidad D del disco duro y en una unida DVD.

Las imágenes permitirán restauración de sistemas operativos, aplicaciones y configuración de los equipos en un tiempo aproximado de 45 minutos en una estación de trabajo sin considerar los archivos propios del usuario. Otra de las ventajas es que mediante las imágenes se podrá hacer las restauraciones en el lugar de trabajo del usuario, esto no incluye cuando el disco presente una falla física como daño en sus pistas o circuitos quemados.

h) Plan de Mantenimiento.-

Cualquier cambio necesario debe ser integrado dentro del plan previamente documentado. Se debe contar con un Plan de acción para incorporar e implementar dichos cambios de forma fehaciente para asegurar incluso mayor protección frente a un desastre.

i) Las Claves de Acceso.-

Las Claves de acceso de los programas, sistemas gubernamentales como SIGA, SIAF así como las claves de los sistemas operativos, de la página web deberán ser de conocimiento de la Dirección Ejecutiva de Administración y Oficina de Estadística e Informática mediante sobre lacrado bajo responsabilidad funcional, estas solo serán utilizadas en caso de contingencia

j) Beneficios de un Plan de Contingencia 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 a poder recuperar de la forma más rápida posible sus capacidades de procesamiento de información crítica y poder proveer a sus usuarios servicios eficientes y eficaces.

4.- PROTECCIONES ACTUALES

- Se hace una copa mensual de los archivos de mayor importancia para el funcionamiento de los sistemas institucionales.
- Robo Común, se cierran las puertas y ventanas con candados y chapas de seguridad. Falla de los equipos, se realiza el mantenimiento de forma regular, los usuarios no fuman en sus escritorios.
- Daño por virus informático, todos los equipos cuentan con software antivirus adquirido legalmente por la institución, estos están interconectados con un servidor de antivirus que permite su actualización en forma diaria. Está prohibida la descarga de software, juegos, música y videos por internet a fin de evitar el filtro de virus.
- Equivocaciones, los usuarios finales tienen una regular formación pero en caso de desconocimiento comunican al personal de la Unidad de Informática para el apoyo técnico.
- Acceso No Autorizado, los usuarios que no cuentan con acceso a los sistemas institucionales están prohibidos de intentar vulnerar el acceso así como los que cuentan con sus claves son responsables del uso de estas.
- Las Oficinas cuentan con extinguidores recargados permanentemente ubicados en lugares estratégicos para su fácil acceso.
- Firewall, la Institución cuenta con un sistema de filtro a páginas prohibidas, el control está en manos de la empresa proveedora del servicio quienes reportan a la Unidad de Informática señalando la Dirección IP que hace uso indiscriminado del servicio de Internet a fin de tomar las medidas del caso.

VII ANEXOS

CRITERIOS SOBRE SISTEMAS DE INFORMACION EN INTERNET

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información. Es suficiente comprobar cómo la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras, como el comercio electrónico o la interacción con las administraciones públicas.

Los recientes avances en las telecomunicaciones y en la computación en red han proporcionado la aparición de canales rápidos para la propagación de datos a través de sistemas digitales. Las redes abiertas están siendo utilizadas cada vez más como una plataforma para la comunicación en nuestra sociedad, pues permiten rápidos y eficientes intercambios de información con un bajo coste económico asociado y con una fácil accesibilidad.

El desarrollo actual y las perspectivas de futuro de las "superautopistas de datos" y de una infraestructura global de información, es decir, de Internet y de la World Wide Web (WWW), crean toda una variedad de nuevas posibilidades. Sin embargo, la realización efectiva de tales posibilidades están influidas por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la validez de los documentos se puede negar, o los datos personales pueden ser recolectados de forma ilícita. Como resultado, el atractivo y ventajas ofrecidas por la comunicación electrónica, tanto en el desarrollo de oportunidades comerciales entre organizaciones privadas como en las interrelaciones entre las organizaciones públicas y los ciudadanos, no pueden ser explotadas en su totalidad.

Es por esto tener en cuenta dentro de nuestro plan de contingencia la operatividad de un firewall para impedir el acceso a usuarios del exterior que no tengan autorización, ya que esto podría ser perjudicial para el servicio de nuestros servidores de red.

VIII BIBLIOGRAFIA

1.- Plan de Contingencia Informático y Seguridad en la Información

Universidad de Piura – 2009

2.- Guía practica para el Desarrollo de un Plan de Contingencia de los Sistemas de Información.

INEI 2001

3.- Los 27 Controles Criticos de la Seguridad Informática

Sergio Castro Reynoso

IX GLOSARIO DE TERMINOS

Antivirus.- En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos

Backup.- Es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Base de Datos.- es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Data Center.- Un Data Center es, tal y como su nombre indica, un "centro de datos" o "Centro de Proceso de Datos" (CPD).

Hardware.- se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Software.- Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Virus Informático.- Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.