"PLAN DE CONTINGÉNCIAS DE LOS SISTEMAS INFORMÁTICOS Y DE LA RED LOCAL DEL HOSPITAL DE LA AMISTAD PERU COREA SANTA ROSA II.2 AÑO 2016-2017."

Formulado por:	**Revisado por:**	**Aprobado por:**
Unidad de Estadística e Informática Fecha 20.07.2016	Unidad de Estadística e informática Fecha20.07.2016	Director Ejecutivo. Fecha.

ÍNDICE

Hospital de la Amistad Perú Corea II-2 Santa Rosa Piura
V° B°
DIRECCIÓN

Hospital de la Amistad Perú Corea II-2 Santa Rosa Piura
V° B°
ASESORIA LEGAL

Hospital de la Amistad Perú Corea II-2 Santa Rosa Piura
V° B°
JEFE DE OFICINA
UE

I OBJETIVO

Definir y programar la implementación de las medidas garanticen el funcionamiento continuo de los sistemas del Hospital de la Amistad Perú Corea Santa Rosa II.2. De seguridad informáticos y de Restaurar el sistema en forma eficiente y con el menor costo y pérdidas posibles, en caso se produzca un incidente.

II FINALIDAD

Disponer de un plan que permita atender de manera ordenada y prevista situaciones que pongan en riesgo la operatividad de los Sistemas Informáticos y de Redes en el Hospital de la Amistad Perú Corea Santa Rosa II.2; estableciendo procedimientos que eviten interrupciones en su operación.

III BASE LEGAL

- Directiva Administrativa Nº 088-MINSA/OGEI
- Decreto Legislativo Nº 822- Ley Sobre el Derecho del Autor.
- Ley Nº 28612- Ley que Norma el Uso, Adquisición y Adecuación del Software en la Administración Publica.
- Decreto Supremo Nº 013-2003-PCM.que dicto Medidas para garantizar la legalidad de la adquisición de programas de Software en entidades y dependencias del Sector Publico.
- Decreto Supremo Nº 083-2004-PCM, que aprobó el Texto Único Ordenado de la Ley Nº 26850 – Ley de Contrataciones y Adquisiciones del Estado.
- Decreto Supremo Nº 037-2005-PCM; que modificó el Decreto Supremo Nº 013-2003-PCM; fijando el plazo para que las entidades públicas cumplan con inventarios de software que utilizan.
- Guía de Administración de Software y Licenciamiento INEI-2001.

IV ALCANCE

Esta directiva será administrada por la Unidad de Estadística e Informática (administra, opera y supervisa los sistemas informáticos y de redes de la institución).

V APROBACIÓN, VIGENCIA Y ACTUALIZACIÓN

5.1 APROBACIÓN.

La Directiva de **"Plan de Contingencias de los sistemas informáticos y de la red Local del Hospital de la Amistad Peru Corea Santa Rosa II.2; en el Año 2016";** Contará con la Visacion de Asesoría Legal, Unidad de Estadística e Informática y de Dirección

5.2 VIGENCIA.

La presente directiva entrará en vigencia al día siguiente de su aprobación y se mantendrá en tanto contribuya al cumplimiento eficiente y oportuno de los objetivos y metas de la institución.

VI DISPOSICIONES GENERALES

6.1 El Plan de Contingencia de equipos de cómputo y bienes colaterales considera dos aspectos importantes:

a. Incluye las actividades que se deben realizar y los grupos de trabajo o responsables de operar.

b. El control, referido a las pruebas y verificaciones periódicas sobre la operatividad y actualización del plan de contingencia.

6.2 Forman parte del plan de contingencias: El plan de reducción de riesgos o plan de seguridad y el plan de recuperación de desastres.

6.3 El Plan de Reducción (Plan de Seguridad) 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 más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma

Personalizada para cada organización.

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 puede priorizar los problemas y su coste potencia desarrollando un plan de acción adecuado.

Para cada riesgo, se debe **determinar la probabilidad del factor de riesgo.** Como ejemplo se mencionan algunos factores de riesgo:

1. Factor de riesgo bajo
2. Factor de riesgo muy bajo

3. Factor de riesgo alto

4. Factor de riesgo muy alto

5. Factor de riesgo medio

Luego se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno.
Ejemplo:

TIPO DE RIESGOS FACTOR DE RIESGO

Robo	Alto	Vandalismo	Medio
Fallas en los equipos		Medio	
Acción de virus	Medio		
Equivocaciones		Bajo	
Terremotos		Bajo	
Accesos no autorizados		Bajo	
Robo de datos	Bajo		
Fuego		Bajo	
Fraude		Muy bajo	

6.4 El plan de recuperación de desastres tiene tres fases claramente definidas:
Actividades previas al desastre; Actividades durante el desastre y Actividades después del desastre.

6.5 Las actividades previas al desastre son:

a. <u>Establecimiento del plan de acción, que comprende</u>:

a.1 Sistema de información: son los sistemas producidos en la entidad y que son vitales para el adecuado funcionamiento de la misma.

a.2 Equipos de cómputo: Se cuenta con el inventario actualizado de Hardware y Software, especificación técnica, ubicación física y el área a la que está asignada. Se encuentran etiquetados los computadores de acuerdo a la importancia de su contenido a

fin de tener prioridad en caso de evacuación.

La Oficina de Informática del HISR; es la responsable de identificar las computadoras de acuerdo a su importancia, para lo cual deberá hacer uso del inventario de equipos de informática, el mismo que les proporcionará la información para probables reemplazos de equipos.

a.3 Obtención y almacenamiento de los Respaldos de Información (BACKUPS), que incluye:

- Dos Backups del Sistema Operativo por cada versión.
- Backup del Software Base (paquetes y/o lenguajes de programación con los cuales han sido desarrollados o interactúan los aplicativos institucionales).
- Backup del Software Aplicativo.
- Backup de los Datos.
- Backup del Hardware.
- Procedimiento para los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia.

a.4 Políticas (normas y procedimientos de Backup), que considera:

Determinación de responsabilidades en la obtención del Backup mencionado anteriormente; debiéndose incluir:

- El Backup; se realizará cada tres meses, y en casos muy importantes con carácter mensual (data administrativa y asistencial)
- El Backup; de Data, se realizara en forma diaria de los diferentes sistemas, tanto administrativos como asistenciales. Debiendo detallar como primer dato la Fecha y posteriormente el sistema. Ejmp. 120109_Sismed, 120109_Siga, etc.
- Almacenamiento del Backup en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- El Backup; se realizara en forma diaria uno se custodiara en el servidor de Backup y otro en disco duro portátil. El cual se le asignara a un persona del área de informática.

- Reemplazo del Backup, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas del Backup, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. <u>Formación de equipos operativos</u>,

Mediante la designación del responsable de seguridad de la información en cada área. Las funciones de los responsables serán: Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos. Proporcionar soporte técnico para las copias de respaldo de las aplicaciones. Planificar y establecer los requerimientos de los sistemas operativos en cuanto a los archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas. Supervisar procedimientos de respaldo y restauración. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de respaldos incrementales. Coordinar líneas, terminales, modem y otros para comunicaciones. Establecer procedimientos de seguridad en los sitios de recuperación. Organizar la prueba de hardware y software. Realizar labor de recupero de inventario y seguridad del almacenamiento. Participar en las pruebas y simulacros de desastres.

c. **<u>Formación de equipos de evaluación</u>**:

Para realizar la auditoría de los procedimientos de seguridad; cuyas funciones serán: Revisar la aplicación y cumplimiento de las normas y procedimientos con respecto a Backups, seguridad de equipos y data. Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento. Revisar la correlación entre la relación de sistemas e información necesarios para la buena marcha de la Institución, y los backups realizados. Informar sobre el cumplimiento e incumplimiento de las normas, para las acciones de corrección respectivas.

6.6 Las actividades durante el desastre son:

a. Plan de emergencias: Señalización de los extintores. Cobertores contra el agua

b. Formación de equipos: El personal de la Unidad de Estadística e Informática es el responsable del salvamento de equipos informáticos, de acuerdo a la prioridad del equipo.

c. Entrenamiento: Establecer un programa de prácticas periódicas para el personal, en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le haya asignado en los planes de evacuación de personal o equipos. Para este caso la Oficina de Logística deberá aprovechar las fechas de recarga de los extintores y propiciar charlas con organismos vinculados a siniestros. El personal debe tomar conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y deben asumir con seriedad y responsabilidad los entrenamientos. Los Funcionarios también están en la obligación de participar en los entrenamientos.

6.7 Las actividades después del desastre son:

a. Evaluación de los daños: Inmediatamente después de concluido el siniestro, se deberá evaluar la magnitud del daño producido. Qué sistemas se afectaron; qué equipos están no operativos; cuáles se pueden recuperar y en cuánto tiempo, etc. Comunicar a los organismos con los que se tiene convenio de respaldo a fin de preparar la reposición de equipos

b. Priorizar las actividades del plan de acción.: Si el plan de acción es general y contempla una pérdida total; la evaluación de daños reales y su comparación contra el plan, proporcionará la lista de las actividades a realizar en función de la prioridad. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, a fin de asignarlos en forma temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c. Ejecución de actividades: Conformación de equipos de trabajo para realizar las

actividades previamente establecidas en el plan de acción. Cada uno dh los equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias. El trabajo de recuperación consta de dos etapas: la primera, la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda, volver a contar con los recursos en las cantidades y lugares apropiados, debiendo ser esta etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución o local de respaldo.

d. Evaluación de resultados: Concluida la labor de recuperación del sistema afectada por el siniestro, se debe evaluar objetivamente, todas y cada una de las actividades realizadas, considerándose entre otros aspectos: ¿Qué tan bien se hicieron; qué tiempo demando; qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción; cómo se comportaron los equipos de trabajo. De la Evaluación de resultados y del siniestro en si, deben obtenerse dos tipos de recomendaciones: una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar la pérdida que ocasionó el siniestro.

e. Retroalimentación del plan de acción: Con la evaluación de resultados, debe optimizarse el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. Evaluar cual hubiera sido el costo de no tener un plan de contingencias.

6.8 El riesgo es la probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y periféricos. El análisis supone obtener una evaluación económica del impacto de dichos sucesos negativos. El valor calculado se utiliza para contrastar el costo de la protección de la información con el costo de una nueva producción.

6.9 Se considerarán los siguientes factores de riesgo

Factor de riesgo muy bajo

Factor de riesgo bajo

Factor de riesgo medio

Factor de riesgo alto

Factor de riesgo muy alto

Se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno de ellos contemplados en el numeral 6.12 de la presente Directiva

6.10 El análisis de riesgos supone responder a preguntas y determinar su grado de confiabilidad:

Qué puede ir mal?

Con qué frecuencia puede ocurrir?

Cuáles serían las consecuencias?

6.11 La evaluación de riesgos supone responder a preguntas con la mayor confiabilidad:

Qué se intenta proteger

Cuál es el valor para la organización o para la persona

Frente a qué se intenta proteger

Cuál es la probabilidad de un ataque.

6.12 Los órganos de la institución, sin excepción, están obligados a brindar todo el apoyo necesario a la Unidad de Estadística e Informática.

6.13 El Director, los Jefes de Unidades y/o Área, según sea el caso, designarán a los responsables de cada área usuaria para que brinden apoyo al personal de la Unidad de Estadística e Informática en los siguientes aspectos: prevención de robos, incendios, vandalismo, fallas de equipos.

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

Al fuego, que puede destruir los equipos y archivos:

.- La Institución cuenta con protección contra incendios

.- Se cuenta con sistemas de aspersión automática

.- Diversos extintores

.- Detectores de humo

.- Los empleados están preparados para enfrentar un posible incendio

Al robo común, llevándose los equipos y archivos.

.- En qué tipo de vecindario se encuentra la Institución

.- Hay venta de drogas.

.- Las computadoras se ven desde la calle.

.- Hay personal de seguridad en la Institución

.- Cuántos vigilantes hay.

.- Los vigilantes, están ubicados en zonas estratégicas

Al vandalismo, que dañen los equipos y archivos.

.- Existe la posibilidad qué un ladrón desilusionado o frustrado cause daños

.- Hay la probabilidad qué causen algún otro tipo de daño intencionado

A fallas en los equipos, que dañen los archivos

.- Los equipos tienen mantenimiento continuo por parte de personal calificado

.- Cuáles son las condiciones actuales del hardware

.- Es posible predecir las fallas a que están expuestos los equipos

A equivocaciones, que dañen los archivos.

.- Cuánto saben los empleados de computadoras o redes

.- El que no conocen el manejo de la computadora, sabe a quién pedir ayuda

.- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

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

.- Se prueba software en la oficina sin hacerle un examen previo

.- Está permitido el uso de disquetes en la oficina

.- Todas las máquinas tienen unidades de disquetes

.- Se cuentan con procedimientos contra los virus

A terremotos, que destruyen el equipo y los archivos.

.- La Institución se encuentra en una zona sísmica?

.- El edificio cumple con las normas antisísmicas?

.- Un terremoto, ¿cuánto daño podría causar?

A accesos no autorizados, filtrándose datos no autorizados.

.- Cuánta competencia hay para la Institución

.- Qué probabilidad hay que un extraño intente hacer un acceso no autorizado

.- El MODEM se usa para comunicarse hacia fuera y hacia dentro

.- Se cuenta con Sistemas de Seguridad en el Correo Electrónico o Internet

Al robo de datos, difundiéndose los datos sin cobrarlos.

.- Cuánto valor tienen actualmente las Bases de Datos

.- Cuánta pérdida podría causar en caso de que se hicieran públicas

.- Se ha elaborado una lista de posibles sospechosos que pudieran robar

.- La lista de sospechosos, ¿es amplia o corta?

Al fraude, desviando fondos merced a la computadora

.- Cuántas personas se ocupan de la contabilidad de la Institución

.- El sistema de contabilidad es confiable

.- Los que trabajan en contabilidad, tienen antecedentes laborales, de qué tipo

.- Existe acceso al sistema contable desde otros sistemas o personas.

6.14 La Unidad de Estadística e Informática evaluará las probables fallas en el sistema de seguridad.

6.15 La Dirección General, Direcciones de Línea y Jefes de Oficina, según sea el caso, dispondrán que el personal realice con carácter obligatorio las siguientes acciones de protección de los equipos e información.

Generales: Una copia diaria y mensual de los archivos que son vitales para la Institución, en medio magnético.

Robo común: Cerrar las puertas de entrada y ventanas de cada Oficina. Se cuenta con personal de seguridad en la entrada del local y cerco eléctrico perimétrico

Vandalismo: Cerrar las puertas de ingreso

Falla de los equipos: Tratar con cuidado, realizar el mantenimiento en forma regular, no fumar, debe estar 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.

Equivocaciones: El servidor debe tener buena formación.

Terremoto: Aplicar la protección contra incendio.

Acceso no autorizado: Cerrar la puerta de entrada, la vigilancia debe rondar por todo el perímetro de las Instalaciones del Hospital II-2 Santa Rosa

Robo de datos: Mantener cerrada la puerta principal. Todas las Pc's deben estar bloqueadas con claves de acceso.

Fuego: Colocar extintores en sitios estratégicos y la oficina de Logística debe propender a entrenamiento para el uso de los mismos.

VII DISPOSICIONES ESPECÍFICAS.

7.1 La Unidad de Capacitación y Docencia a través de la Unida de Estadística e Informática es la responsable de formular, programar, realizar, coordinar, ejecutar, evaluar y controlar el Plan de Contingencias de equipos informáticos y periféricos.

7.2 La Unidad de Administración a través de la Oficina de Logística es la responsable del entrenamiento en el uso de extintores, para lo cual deberá programar las fechas en que se realizará tal entrenamiento.

7.3 La Unidad de Administración a través de la Oficina de Logística es la responsable de proporcionar a la Unidad de Estadística e Informática el inventario de equipos informáticos y periféricos debidamente actualizados.

7.4 La Unidad de Estadística e Informática elaborará y ejecutará, dentro de los treinta (30) días calendarios posteriores a la aprobación de la presente Directiva, la encuesta o cuestionario que desarrollará todo el personal de la entidad. El personal institucional está en la obligación, bajo responsabilidad, de desarrollar objetivamente la encuesta o cuestionario que la Unidad de Estadística e Informática le presentará. El desarrollo de la encuesta o cuestionario se desarrollará en un solo acto.

7.6 El Director y Jefes de Unidad/Oficina, según sea el caso, brindarán a su personal las facilidades para el cumplimiento de los objetivos.

7.7 Previo al desarrollo de la encuesta o cuestionario, la Unidad de Estadística e Informática brindará charlas al persona sobre Plan de Contingencia Informático.

VIII DISPOSICIONES COMPLEMENTARIAS

El Plan de Contingencias de equipos informáticos y periféricos tiene la clasificación de prioridad muy alta.

8.2 El jefe de la Unida de Estadística e Informática; es el responsable de velar por el estricto cumplimiento de lo dispuesto en la presente Directiva.

8.3 El personal de la entidad, independientemente de su nivel y cargo forma parte como un todo del plan de contingencias.

8.4 El Jefe de la Unidad de Estadística e Informática; remitirá vía correo electrónico, a cada trabajador, la presente Directiva.

8.5 El personal hará suyo lo establecido en la presente Directiva, bajo responsabilidad.

8.6 El Jefe de la Unidad de Estadística e Informática; bajo responsabilidad informará, dentro los 10 días calendarios posteriores al término de cada mes, a la Jefatura institucional sobre la ejecución del Plan de Contingencias, formulando las recomendaciones a que hubiere lugar.