PAG WEB

MINISTERIO DE SALUD

Dirección General

RESOLUCION DIRECTORAL

N°010 -2019-DG-HVLH

Magdalena del Mar, 18 de Enero del 2019

Visto; la Nota Informativa N° 722-2018-OEI-HVLH-MINSA, emitida por el Jefe de la Oficina de Estadística e Informática del Hospital Víctor Larco Herrera;

CONSIDERANDO:

Que, la Ley 28551 Ley que establece la obligación de elaborar y presentar Planes de Contingencia; dispone que todas las personas naturales y jurídicas de derecho privado o público que conducen y/o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle;

Que, el artículo 2° de la acotada norma legal, establece que los planes son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos;

Que, mediante Resolución Ministerial N° 431-2015/MINSA de fecha 09 de Julio del 2015, se aprobó el documento técnico "Política de Seguridad de la Información del Ministerio de Salud MINSA", con la finalidad de mantener la continuidad de las operaciones del Ministerio de Salud , en relación a los sistemas de información seguros, minimizando sus riesgos y maximizando los niveles de satisfacción de los usuarios; siendo su objetivo de establecer los principios para la implementación del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud;

Que, mediante documento del visto, el Jefe de la Oficina de Estadística e Informática, da cuenta sobre la necesidad de contar con un Plan de Contingencia Informático que tiene como finalidad definir las normas y procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los Sistemas de Información y Comunicación del Hospital Víctor Larco Herrera, de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos;

Que, mediante Nota Informativa N° 005-2019-OEPE/HVLH, de fecha 07 de Enero del 2019 el Director de la Oficina Ejecutiva de Planeamiento Estratégico del Hospital Víctor Larco Herrera, manifiesta que el Plan de Contingencia Informático del Hospital Víctor Larco Herrera, para los años 2018 – 2019, ha sido revisado, el mismo que cumple con las "Normas para la Elaboración de Documentos Normativos del Ministerio de Salud" aprobado por Resolución Ministerial N° 850-2016/MINSA;

Que siendo ello así, resulta necesario aprobar el Plan de Contingencia Informático, por convenir a los intereses funcionales institucionales que permitan un mejor cumplimiento de los fines y objetivos de la institución, resulta necesario formalizar su aprobación, mediante la emisión del correspondiente acto de administración;

Estando a lo informado por el Jefe de la Oficina de Estadística e Informática del Hospital Víctor Larco Herrera; y,

Con el visto bueno de la Directora de la Oficina Ejecutiva de Administración, del Director de la Oficina de Planeamiento Estratégico, y de la Jefa de la Oficina de Asesoría Jurídica; y,

De conformidad con las atribuciones señaladas en 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 el Documento Técnico Denominado: **"PLAN DE CONTINGENCIA INFORMATICO"** del Hospital Víctor Larco Herrera, para el Año 2019; el mismo que en documento adjunto a folios trece (13) forma parte integrante de la presente Resolución Directoral.

Artículo 2º.- Encargar a la Oficina de Estadística e Informática del Hospital "Víctor Larco Herrera", la difusión, implementación, supervisión y cumplimiento en su integridad del referido Plan.

Artículo 3°.- Dejar sin efecto la Resolución Directoral N° 058-2016-DG-HVLH, que aprueba el Pal de Contingencia Informático del Hospital Víctor Larco Herrera.

Artículo 4º.- Dispóngase la publicación de la presente resolución en el portal institucional del Hospital Víctor Larco Herrera (www.larcoherrera.gob.pe).

Regístrese y Comuníquese

Ministerio de Salud
Hospital Victor Larco Herrera

Med. Elizabeth M. Rivera Chávez
Directora General
C.M.P. 24232 R.N.E. 10693

EMRCH/GMRR/MYRV.
Distribución:

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

HOSPITAL VICTOR LARCO HERRERA

PLAN DE CONTINGENCIA INFORMATICO
HOSPITAL VICTOR LARCO HERRERA

AÑO 2019

I. INDICE

Página

Contenido

PLAN DE CONTINGENCIA INFORMATICO HOSPITAL VICTOR LARCO HERRERA, PARA EL AÑO 2019.

II. INTRODUCCION

El Plan de Contingencia Informático, constituye un instrumento de gestión, para el buen manejo de las Tecnologías de la Información y de las Comunicaciones (TIC). El Plan en si expresa las medidas técnicas humanas y organizativas necesarias para garantizar la continuidad de la operatividad y funcionalidad asistenciales, así como administrativas de nuestra Institución.

Previo a ello se hace un análisis de riesgos donde entre otras amenazas se identifican las que afectan a la comunidad de la operatividad de la entidad. El Plan de Contingencias será revisado anualmente. Así mismo es revisado y/o 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 el Parque Informático (Red de Computadoras y otros equipos informáticos y servicios) se encuentra aún en proceso de estructuración, ello implica que los responsables de los servicios informáticos expliquen a los usuarios finales, con propiedad y suficiente claridad los potenciales riesgos y las consecuencias de una política de seguridad a fin de evitar en todo lo posible los graves riesgos que implican.

El Plan de Contingencia Informático debe contemplar los Planes de Emergencia, Backup (respaldo de la información digital) y de rápida Recuperación de la misma.

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

Es esencial "tomar conciencia real del valor de la seguridad informática". En la actualidad, el constante desarrollo tecnológico lleva a las organizaciones a enfrentar amenazas que en muchas ocasiones ni siquiera saben que existen, pero que pueden afectar los datos de sus organizaciones, clientes e incluso incapacitarlos para trabajar.

"Las buenas prácticas están muy bien definidas formalmente, podemos tener normativas, ISOS, políticas definidas de seguridad, pero se tendría que resumir las prácticas en tres conceptos básicos:

- **La primera es la formación**, porque, aunque tengamos una guía de actuación, el personal interno tiene que ser sensibilizado sobre cómo manejar los datos, esto incluye a los directores y/o jefes, a los técnicos y al usuario final.
- **El segundo concepto sería el asesoramiento**, porque estamos sustituyendo plataformas, implementado tecnologías, por lo que necesitamos en ocasiones asesores que nos digan dónde aparecen huecos y fallas.
- **El tercer eje sería el reciclaje**, necesitamos técnicos, personal que esté al día con lo que pasa en el exterior con el objetivo de que el personal y la entidad no queden obsoletos frente a la vigencia tecnológica.

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 GENERAL

Un Plan de Contingencia permite prever los riesgos a los que estarán sometido y/o expuesto los sistemas de información implementada y/o los que se van 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 pueda corresponderle.

V. BASE LEGAL.

- Ley Nº 25323, que crea el Sistema Nacional de Archivos.
- Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto Supremo Nº 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
- Ley Nº 27269, Ley de Firmas y Certificados Digitales.
- Ley Nº 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
- Ley N ° 30096, Ley de Delitos Informáticos.
- Ley Nº 30276, Ley que modifica el Decreto Legislativo 822, Ley sobre el Derecho de Autor.
- Decreto Legislativo Nº 822, Ley sobre el Derecho de Autor, y sus respectivas modificatorias.
- **Resolución Ministerial Nº 119-2018-PCM "Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública" 08-05-2018.**
- Decreto Supremo Nº 013-2003-PCM, que dicta medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del sector público.
- Decreto Supremo Nº 024-2006-PCM que aprueba el Reglamento de la Ley Nº 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
- Decreto Supremo Nº 052-2008-PCM, que aprueba el Reglamento de la Ley Nº 27269 modificada por Ley Nº 27310, Ley de Firmas y Certificados Digitales.
- Resolución Ministerial Nº 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública.

- Resolución Ministerial Nº 381-2008-PCM, que aprueba los lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.
- Resolución Ministerial Nº 004-2016-PCM, que aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2º edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Ley Nº 26842, Ley General de Salud.
- Ley Nº 29414, Ley que establece los Derechos de las Personas Usuarias de los Servicios de Salud.
- Decreto Supremo Nº 016-2002-SA, que aprueba el Reglamento de la Ley Nº 27604, Ley que modifica la Ley General de Salud, respecto de la obligación de los establecimientos de salud a dar atención médica en casos de emergencias y partos.
- Resolución Ministerial Nº 529-2006/MINSA, que aprueba la NTS Nº 043-MINSA/DGSP-V.01 "Norma Técnica de Salud para la Atención Integral de salud de las Personas Adultas Mayores".
- Resolución Ministerial Nº 626-2006/MINSA, que aprueba la NTS Nº 046-MINSA/DGSP-V.01 "Norma Técnica de Salud para la Atención Integral de Salud de la Etapa de Vida Adulto Mujer y Varón"
- Resolución Ministerial Nº 431-2015/MINSA, que aprueba el Documento Técnico "Políticas de Seguridad de la Información del Ministerio de Salud"
- Resolución Ministerial Nº 214-2018/MINSA Aprobar la NTS Nº139-MINSA/2018/DGAIN: "Norma Técnica de Salud para la Gestión de la Historia Clínica", que en documento adjunto forma parte integrante de la presente Resolución Ministerial y su modificatoria Resolución Ministerial Nº 265-2018//MINSA.
- Resolución Ministerial Nº 120-2017/MINSA "Aprueba la Directiva Administrativa Nº 230 — MINSA/2017/OGTI, "Directiva Administrativa que establece los estándares y criterios técnicos para el desarrollo de los sistemas de información en salud", que en documento adjunto forma parte integrante de la presente Resolución Ministerial.
- Ley Nº 30024, Ley que crea el Registro Nacional de Historias Clínicas Electrónicas.
- Decreto Legislativo Nº 1306, Decreto Legislativo que Optimiza Procesos Vinculados al Registro Nacional de Historias Clínicas Electrónicas.
- Decreto Supremo Nº 024-2005-SA, que aprueba las Identificaciones Estándar de Datos en Salud.
- Resolución Ministerial Nº 751-2004-SA/MINSA, que aprueba la NT Nº 018-MINSA/DGSP-V.01: "Norma Técnica del Sistema de Referencia y Contrarreferencia de los Establecimientos del Ministerio de Salud.
- Decreto Supremo Nº 039-2015-SA, que aprueba el Reglamento de la Ley que crea el Registro Nacional de Historias Clínicas Electrónicas.
- Resolución Ministerial Nº 058-2017/MINSA Aprobar la Directiva Administrativa Nº 226-MINSA/2017/OGTI "Directiva Administrativa para la gestión de los Certificados Digitales y el Uso de la Firma Digital en el Ministerio de Salud.
- Resolución Ministerial No. 461-2008/MINSA, que aprueba la Directiva Administrativa No.134-MINSA/OGEI para el "Uso Racional de Recursos Informáticos y de Comunicaciones en las Direcciones de Salud y sus Establecimientos'.
- Resolución Ministerial No. 971-2006/MINSA, que aprueba la directiva Administrativa No.100-MINSA/OGEI "Directiva Administrativa para el Correcto Uso de Equipos de Cómputo y Servicios Informáticos en el Ministerio de Salud"

- Resolución Ministerial No. 520-2006/MINSA, que aprobó les "Lineamientos de Política de Seguridad de la información".
- **Resolución Ministerial Nº 132-2005/MINSA "Aprueban Reglamento de Organización y Funciones del Hospital Víctor Larco Herrera"**
- Resolución Jefatural Nº 199-2003-INEI que aprueba la Directiva sobre "Normas Técnicas para la administración del software libre en los servicios informáticos de la Administración Pública"
- Resolución Nº 0791-2015/CDA-INDECOPI, que aprueba lineamientos complementados de la Comisión de Derecho de Autor sobre el Uso Legal de los Programas de Ordenador (Software)
- Resolución Nº 0121-1998/ODA-INDECOPI, que aprueba lineamientos de la Oficina de Derechos de Autor sobre uso legal de los programas de ordenador (software)
- Ley Nº 27444 Ley del Procedimiento Administrativo General.
- Decreto Ley Nº 19414, que declara de utilidad pública la defensa, conservación e incremento del Patrimonio Documental de la Nación.
- Decreto Legislativo Nº 681, que regula el uso de Tecnologías Avanzadas en materia de Archivo.
- Decreto Supremo Nº 009-92-JUS, Reglamento del Decreto Legislativo Nº 681, sobre el uso de tecnologías de avanzada en materia de archivos de las empresas.

VI. AMBITO DE APLICACIÓN

Hospital Víctor Larco Herrera.

VII. CONTENIDO

1. ESQUEMA GENERAL

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los 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 presentará el problema. Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto, es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el que tendrá como objetivo, restaurar el Servicio en forma rápida y con el menor costo y lo las pérdidas posibles.

El esquema del Plan de Contingencias abarcará los siguientes aspectos:

a. Plan de Reducción de Riesgos (Plan de Seguridad).
b. Plan de Recuperación de Desastres.

- Actividades Previas al Desastre.
  - Establecimiento del Plan de Acción.
  - Formación de Equipos Operativos.
  - Formación de Equipos de Evaluación (auditoria de cumplimiento de procedimientos de Seguridad).
- Actividades durante el Desastre.
  - Plan de Emergencias.
  - Formación de Equipos.
  - Entrenamiento.

- Actividades después del Desastre.
    - Evaluación de Daños.
    - Priorización de Actividades del Plan de Acción señaladas en 2.i.i
    - Ejecución de Actividades
    - Evaluación de Resultados.

2. ANALISIS DE RIESGOS

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

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 como resultado de una contingencia. 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 indicaciones que deberán tomar en cuenta los responsables de la Oficina de Estadística e Informática, su Unidad Funcional de Informática y su Unidad Funcional de Estadística (protección de la información digital del SIHE y de otros aplicativos como Sistema TUPA, Bases de datos Excel de Egresos, Hospitalización, ingresos, emergencia, consulta externa hoja HIS, otro tipo de información digital) en conjunto con los responsables de todas las áreas usuarias administrativas y asistenciales de la Institución:

¿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 digitales y físicos.
4. A fallas en los equipos, que dañen los archivos digitales y físicos.
5. A equivocaciones, que dañen los archivos digitales y físicos.
6. A la acción de virus informático, que dañen los equipos y archivos digitales.
7. A accesos a los equipos y/o información digital no autorizados, filtrándose datos no autorizados.
8. Al robo de datos.
9. Al fraude digital, desviando fondos merced a la computadora.
10. A la falta de protección de datos personales, de la historia clínica.

3. ANALISIS DE FALLAS EN LA SEGURIDAD

Esto supone estudiar las computadoras, su software, hardware, localización y utilización con el objetivo de identificar los resquicios (posible abertura pequeña o estrecha) 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.

4. 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, otros aplicativos digitales que utilicen actualmente), Oficina de Personal (Base de

Datos Registro de Asistencia y Remuneraciones), Farmacia (Base de Datos de Farmacia de todos sus aplicativos digitales), Central Documentaria (Base de Datos de Registro Documentario), Oficina de Estadistica (Bases de datos del SIHE, Hojas de Cálculo Excel, Egresos, Consultas Externas, Ingresos a Hospitalización, Emergencia, Movimiento de Historias Clínicas, TUPA, documentación digital en procesadores de texto en formato Word, Unidad de Referencia y Contra referencia, (bases de datos FUAS, y demás aplicativos informáticos establecidos por el SIS), Oficina de Planeamiento Estratégico (base de datos del Módulo de Presupuesto Público), y en general toda Oficina y/o Servicio que almacene información digital oficial de toda índole inherente a su funciones propias establecidos en sus manuales de gestión respectivas de cada Oficina y/o Servicio.

d. **Capacitación:** la capacitación debe realizarse en Administración de Sistemas Operativos de Servidores y Administración de Base de Datos al personal de la Unidad de Informática y también a capacitaciones a nivel usuario a manera de conocimiento general.

e. **Preparación de un Plan de Backup. -**

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

f. **El Plan de Recuperación. -**

Nuestra Institución 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 gestión de la recuperación de información (recursos humanos debidamente capacitados y disponer con los materiales y equipamiento adecuado para lograr la recuperación de información).

Es una alternativa recurrir a empresas por servicios de terceros que ofrezcan servicios de recuperación de información digital; siempre que esta no pueda ser superada por el personal de la Unidad Funcional de Informática, 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 reiniciar el procesamiento de datos, y de esta manera la institución pueda reiniciar y continuar con sus labores en los sistemas y aplicativos que corresponda a cada área.

g. **Imágenes de los Programas Informáticos**. - 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, puede ser en una unida DVD, en una unidad de Disco Duro Externo y/o si existiera la posibilidad en algún tipo de alojamiento en las nubes digitales (gestión de almacenamiento de nuestra información institucional en espacios rentados en servidores de gran capacidad).

   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, y otros aplicativos dispuestos por el MINSA, así como las claves de los sistemas operativos, de la página web institucional, 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.

5. PROTECCIONES ACTUALES

- Se hace una copia mensual y de ser posible en forma diaria, de los archivos digitales de mayor importancia y por prioridades, estas copias de respaldo al ser recuperadas permitirán continuar con el normal funcionamiento de los sistemas institucionales, luego de la contingencia.
- Robo Común, se cierran las puertas y ventanas con candados y chapas de seguridad. Falla de los equipos, se realiza et 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, salvo con autorización estrictamente evaluado por el equipo de técnicos de Informática en coordinación con las Jefaturas y los usuarios de las estaciones de trabajo.
- Equivocaciones, los usuarios finales tienen una regular formación en el uso de los equipos de cómputo, pero en algunos casos excepcionales, si existiera desconocimiento del uso de algún equipo de cómputo o programa informático, se debe comunicar al personal de la Unidad Funcional de Informática para el apoyo técnico requerido.
- 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 usuarios y claves de acceso son responsables del uso de estas mismas.
- 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 a cargo de la empresa proveedora del servicio quienes reportaran a la Unidad Funcional de Informática señalando la Dirección IP que hace uso indiscriminado del servicio de Internet a fin de tomar las medidas del caso.

VIII. ANEXOS

1. CRITERIOS SOBRE SISTEMAS DE INFORMACION EN INTERNET.

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información y las comunicaciones TIC. 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 línea 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 está influidas por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la validez de los documentos puede existir la posibilidad de ser negado, o los datos personales pueden ser recolectados de forma ilícita por terceros ajenos a la información. 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 (gobierno digital) 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, pues esto constituiría un grave riesgo en el normal funcionamiento de nuestros servidores de red de computadoras.

2. ANEXO COMPLEMENTARIO

La Oficina de Estadística e Informática, ha solicitado autorización, para publicar en el Portal Institucional un "AVISO DE SINCERAMIENTO" con respecto a la aplicación de la Resolución Ministerial Nº 119-2018-PCM "Disponen la creación de un **Comité de Gobierno Digital en cada entidad de la Administración Pública**" 08-05-2018, en la sección de DISPOSICIÓN COMPLEMENTARIA DEROGATORIA Única. Déjese sin efecto la Resolución Ministerial Nº 061-2011-PCM "Aprueba los lineamientos que establecen el contenido mínimo del Plan Estratégico de Gobierno Electrónico" PETI y la Resolución Ministerial Nº 019-2011-PCM "Apruébese la "Formulación y Evaluación del Plan Operativo Informático (POI) de las entidades de la Administración Pública" y su Guía de Elaboración Aprobar como actividad permanente la "Formulación y Evaluación del Plan y todas aquellas disposiciones, que se opongan a esta.

En ese sentido el Hospital Víctor Larco Herrera, ha elaborado el presente plan de contingencia informática, por ser de necesidad actual en nuestra Institución, dejando en claro que estas dos Resoluciones Ministeriales de la Presidencia del Consejo de Ministros han sido derogadas en este año 2018.

El objetivo del Aviso de Sinceramiento está referido a socializar la necesidad de comunicar a la comunidad hospitalaria, autoridades internas y autoridades

externas que el tema de los Planes Informáticos algunos de ellos se encuentran en proceso de elaboración, dado a la complejidad que estos significan su culminación.

IX. BIBLIOGRAFIA

1. Plan Estratégico de Tecnologías de Información de SERVIR (PETI 2016-2021) Resumen Ejecutivo.
2. Plan de Contingencias de los Sistemas Informáticos y de Redes de la presidencia del Consejo de Ministros actual.
3. Técnicas de Seguridad Informática Software Libre – Alejandra Stolk – año 2013
4. Guía práctica para el Desarrollo de un Plan de Contingencia de los Sistemas de Información INEI
5. Publicación de la Secretaría de Gobierno Digital Presidencia del Consejo de Ministros año 2018.

X. 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 adicionan les 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.