Ministerio de Salud
Personas que atendemos Personas
Hospital San Juan de Lurigancho

Nº 408 -2013-D-HSJL-DISA-IV-LE

REPUBLICA DEL PERU
MINISTERIO DE SALUD

El presente Documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
MINISTERIO DE SALUD
Disa IV Lima Este
Hospital San Juan de Lurigancho
07 ENE. 2014
Sr. ELOY N. JUMPA ALVARADO
FEDATARIO TITULAR

RESOLUCION DIRECTORAL

San Juan de Lurigancho, 31 de Diciembre del 2013

VISTO:

Informe Nº 033-2013-OPE-HSJL; y

CONSIDERANDO:

Que, la Resolución Jefatural Nº 340-94-INEI aprueba la Directiva Nº 015-94INEI/SII "Normas Técnicas para el Almacenamiento y Respaldo de Información que se procesan en las Entidades del Estado";

Que, la Resolución Ministerial Nº 1942-2002-SA/DM aprueba las "Normas Generales sobre Acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud;

Que, con Resolución Ministerial Nº 1942-2002-SNDM se aprobó la Directiva Nº 001-2002-OGEI "Normas Generales sobre acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud;

Que, la Resolución Jefatural Nº 386-2002-INEI aprueba la Directiva Nº 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de Información procesada por las Entidades de la Administración Pública";

DIRECCIÓN HOSPITAL SAN JUAN DE LURIGANCHO V°B° A. Calero H.

Que, en el Decreto Supremo Nº 013-2003-PCM se dictan Medidas para Garantizar la Legalidad de la Adquisición de Programas de Software en Entidades y Dependencias del Sector Público;

Que, la Resolución Jefatural Nº 053-2003-INEI aprueba la Directiva Nº 004-2003-INEI/DTNP "Norma Técnica para la Implementación del Registro de Recursos Informáticos en las Instituciones de la Administración Pública";

ASESORIA LEGAL Hospital San Juan de Lurigancho V°B° S. ALIAGA

Que, la Directiva Nº 005-2004-PCM/SG "Directiva de Seguridad ante la Presencia de los Virus Informáticos en la Presidencia del Consejo de Ministros;

Que, la Directiva Nº 006-2004-PCM/SG "Plan de Contingencias de los Sistemas Informáticos y de Redes la Presidencia del Consejo de Ministros;

Que, con Resolución Ministerial Nº 224-2004-PCM se aprueba el uso obligatorio del Código de Buenas Prácticas para la Gestión de la Seguridad de la Información;

OFICINA DE ADM. HOSPITAL SAN JUAN DE LURIGANCHO V°B° E. SAAVEDRA M.

Que, con Resolución Ministerial Nº 246-2007-PCM/ONGEI se aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.2da. Edición en todas las entidades integrantes del Sistema Nacional de Informática;

Que, la Oficina de Planeamiento Estratégico del Hospital San Juan de Lurigancho, mediante el documento de visto, solicita aprobar la "**Directiva sobre Políticas de Seguridad Informática**"; mediante acto resolutivo;

Contando con la aprobación y visación de la Sub Dirección, Oficina de Administración y la Coordinación de Asesoría Jurídica;

Estando a las facultades conferidas mediante Resolución Ministerial Nº 449-2010/MINSA, que aprueba el Reglamento de Organización y Funciones del Hospital San Juan de Lurigancho.

A. Calero M.

ASESORIA LEGAL V°B° Hospital San Juan de Lurigancho

S. ALIAGA

SE RESUELVE:

ARTÍCULO 1º.- APROBAR, la **Directiva sobre Políticas de Seguridad Informática del Hospital San Juan de Lurigancho,** que consta de ocho (08) folios, los mismos que forman parte integrante de la presente resolución.

OFICINA DE ADM. V°B° HOSPITAL SAN JUAN DE LURIGANCHO

SAAVEDRA M.

ARTÍCULO 2º.- NOTIFICAR la presente resolución a las instancias administrativas correspondientes e integrantes de la Comisión y Comité técnico constituido.

Regístrese, Comuníquese y Cúmplase

MINISTERIO DE SALUD DISA IV LIMA ESTE SAN JUAN DE LURIGANCHO

DR. FRANKLIN ARTURO SOLIS ARIAS
DIRECTOR
CMP. 20474

FASA/SDAS/GLAV.-
DISTRIBUCION
( ) Dirección.
( ) OCI
( ) Administración.
( ) Asesoría Jurídica.
( ) Planeamiento Estratégico
( ) ARCHIVO.

El presente Documento es "COPIA FIEL DEL ORIGINAL" que he tenido a la vista
MINISTERIO DE SALUD
Disa IV Lima Este
Lurigancho
07 ENE. 2014
Sr. ELOY N. JUMPA ALVARADO
FEDATARIO TITULAR

HOSPITAL SAN JUAN DE LURIGANCHO
V°B°
UNIDAD DE ESTADÍSTICA
E INFORMÁTICA

HOSPITAL SAN JUAN DE LURIGANCHO

DIRECTIVA SOBRE POLÍTICAS DE SEGURIDAD INFORMÁTICA

2013

ÍNDICE

I.	**OBJETIVO**	03
II.	**FINALIDAD**	03
III.	**ALCANCE**	03
IV.	**BASE LEGAL**	03
V.	**DEFINICIONES**	04
VI.	**DISPOSICIONES GENERALES**	05
VII.	**DISPOSICIONES ESPECIFICAS**	06
VIII.	**DISPOSICIONES COMPLEMENTARIAS**	08
IX.	**DISPOSICIONES FINALES**	08

DIRECTIVA SOBRE POLITICAS DE SEGURIDAD DE INFORMACIÓN

HOSPITAL SAN JUAN DE LURIGANCHO V°B° UNIDAD DE ESTADÍSTICA E INFORMÁTICA

I. OBJETIVO

La presente Directiva tiene por objeto preservar la confidencialidad, integridad y disponibilidad oportuna de los activos de tratamiento de la información.

II. FINALIDAD

- Dictar las normas que establecen los Procedimientos para la utilización de los servicios informáticos, así como las medidas para la seguridad informática que deberán cumplir las Unidades orgánicas para evitar el daño, pérdida o mal empleo de la información y material de cómputo del Hospital San Juan de Lurigancho.
- Lograr que los usuarios comprendan la importancia del buen uso de los servicios de información, entendiendo los beneficios que obtienen, así como las consecuencias del no cumplimiento de las normas y recomendaciones.
- Dar cumplimiento a lo dispuesto en el numeral 10.4 del artículo 10º de la Ley No. 29951 - Ley de Presupuesto del Sector Público para el Año Fiscal 2013.

III. ALCANCE

OFICINA DE PLANEAMIENTO ESTRATEGICO V°B° JEFATURA HOSPITAL S.J.L.

La presente Directiva es de aplicación obligatoria en todas las áreas del hospital, en eso incluye servidores y funcionarios, así como para el personal que presta servicios o desempeñe actividades, independientemente del régimen laboral o contratación a la que se encuentre sujeto.

IV. BASE LEGAL

- Ley N° 27657 - Ley del Ministerio de Salud.
- Ley N° 27444 - Ley del Procedimiento Administrativo General.
- Decreto Legislativo N° 604 que aprobó la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Ley Nº 29951 Ley de Presupuesto del Sector Público el Año Fiscal 2013.
- Ley Nº 27815 Código de Ética de la Función Pública.
- R.J. Nº.340-94-INEI, que aprueba la Directiva No.015-94-INEI/SII – Normas Técnicas para el Almacenamiento y Respaldo de la Información que se procesan las entidades del Estado.
- R.M. N° 1942-2002-SA/DM que aprueba las "Normas Generales sobre Acciones de Sistemas de información, Estadística e Informática en el Ministerio de Salud".

- Directiva Nº 005-2004-PCM/SG "Directiva de Seguridad ante la Presencia de los virus Informáticos en la Presidencia del Consejo de Ministros".
- Directiva N° 006-2004-PCM/SG "Plan de Contingencias de los sistemas informáticos y de redes de la Presidencia del Consejo de Ministros" (Resol. de SA Nº 005-2004-PCM).
- Resolución de Contraloría Nº 320-2006-CG Aprueba normas de control interno.
- R.M. Nº 1942-2002-SNDM, que aprobó la Directiva Nº 001-2002-OGEI, "Normas Generales sobre Acciones de Sistemas de Información, Estadística e Informática en el Ministerio de Salud".
- R.J. Nº 053-2003-INEI, que aprobó la Directiva Nº 004-2003-INEI/DNTP, "Norma Técnica para la implementación del registro de recursos informáticos en las Instituciones de la Administración pública".
- R.M. N° 224-2004-PCM, que aprueba el uso obligatorio del Código de Buenas Prácticas para la gestión de la seguridad de la información.
- Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva N°016-2002-INEI/DTNP - Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la administración pública.
- Decreto Supremo N° 013-2003-PCM, por el cual se dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Publico.
- Normas Técnicas de Control Interno, aprobadas por Resolución de Contraloría N° 320-2006-CG.
- Ley Nº 28716 – Ley de Control Interno de las Entidades del Estado.
- R.M. Nº 246-2007-PCM/ONGEI: Que aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición en todas las entidades integrantes del Sistema Nacional de Informática".

V. DEFINICIONES

- **COMPUTADORA PERSONAL O ESTACION DE TRABAJO**: Computadora asignada a los usuarios para el desarrollo exclusivo de las tareas encomendadas por el Hospital San Juan de Lurigancho.
- **SOFTWARE**: Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir la parte intangible o lógica de una computadora.
- **SERVIDOR**: En una red, se denomina servidor a una computadora compartida por múltiples usuarios. Existen servidores de archivos, servidores de impresión, etc. Los Servidores son computadoras de gran potencia que se encuentran a disposición de los usuarios. Cuando los usuarios se intercomunican, en realidad, lo hacen a través de servidores.

- **CORREO ELECTRÓNICO**: El correo electrónico, es el medio por el cual se pueden recibir y enviar información a través de un dispositivo electrónico.
- **USUARIO**: Personal que se encuentra autorizado a utilizar los equipos y sistemas informáticos pertenecientes al Hospital.
- **NAVEGADOR**: Es un programa que provee una interface para acceder y ver archivos en Internet.
- **DOMINIO DE INTERNET**: Es una red de identificación (Ejemplo **@hospitalsjl.gob.pe**) asociada a un grupo de dispositivos o equipos conectados a la red de Internet.

VI. DISPOSICIONES GENERALES

- El usuario que recibe los servicios informáticos solicitados o necesarios para su desempeño, es responsable del cumplimiento de las normas vigentes, del uso adecuado de los equipos de cómputo, del software utilizado, de los datos administrados, así como el cuidado de manuales y otros elementos de soporte que se le entreguen.
- La Unidad de Estadística e Informática del hospital, es la instancia responsable de brindar los servicios informáticos, de aprobar la incorporación de tecnologías de información vinculadas con el desarrollo y operación de los sistemas de información y el mantenimiento de los equipos de cómputo asignados a los usuarios.
- Solicitarán a la Unidad de Estadística e Informática el acceso a las páginas de Internet que se encuentren bloqueadas, cuando por razones del servicio se requiera.
- El personal sin autorización de acceso a medios informáticos, no deberá hacer uso de los mismos.
- Los equipos informáticos deben ser manipulados respetando la normativa establecida por la Unidad de Estadística e Informática.
- Los activos de información deben ser utilizados de acuerdo a lo establecido por los responsables de la información.
- Los usuarios son responsables del cuidado físico y lógico de sus equipos de computo y, por tanto, no deben manipular alimentos, fumar sobre los equipos de computo, instalar software o cualquier otra actividad que pueda dañar los equipos o alterar su correcto funcionamiento, sin la autorización expresa de la Unidad de Estadística e Informática.
- Los usuarios son responsables de las actividades que se realicen con sus accesos, como su identificación de usuario y contraseña a los servicios informáticos. En caso el usuario ceda su acceso al servicio informático a otra persona, seguirá siendo responsable de las actividades que este tercero realice.
- El equipo de computo que es entregado al usuario contiene el software base necesario para satisfacer sus funciones y está instalado de acuerdo al perfil solicitado por su Unidad orgánica. Cualquier necesidad adicional debe ser solicitada formalmente a la Unidad de Estadística e Informática.

- El hospital, a través de la Unidad de Estadística e Informática, es responsable del buen desempeño de los equipos de cómputo y servicios informáticos, brindando el soporte adecuado a las labores de los usuarios de manera eficaz y eficiente.
- El usuario no debe prestar o intercambiar el equipo de cómputo que le ha sido asignado por la institución, bajo responsabilidad.

VII. DISPOSICIONES ESPECÍFICAS

- **Sobre los Equipos de Computo**
  - ✓ El usuario, bajo ninguna circunstancia, debe abrir los equipos de cómputo o periféricos, sacar o cambiar componentes o periféricos de los mismos. Esta acción será reportada por la Unidad de Estadística e Informática a su jefatura inmediata y/o a la Dirección, solicitando la acción disciplinaria correspondiente.
  - ✓ El usuario que requiera otro software adicional al pre-instalado o acceso a un servicio informático en su equipo debe solicitarlo a Unidad de Estadística e Informática.
  - ✓ El usuario es responsable de organizar y mantener en orden la información contenida en el equipo de cómputo que le ha sido asignado por la institución.
  - ✓ El usuario que instale de manera arbitraria software en su equipo de cómputo es responsable del mal funcionamiento del mismo, de los problemas que podrían ocasionar en los demás equipos conectados a la red y de las licencias de software instalado.
  - ✓ El usuario no debe alterar el hardware y software que se encuentra a su disposición, así mismo, no debe cambiar la configuración de los equipos de computo determinada por la Unidad de Estadística e Informática.
  - ✓ El personal de Informática de la Unidad de Estadística e Informática son los autorizados para realizar instalaciones y/o modificaciones a las configuraciones al hardware y software de los equipos de cómputo. Asimismo, son los autorizados para trasladar los equipos de la institución.
  - ✓ El personal de Informática de la Unidad de Estadística e Informática poseerá una 'Clave de Administrador' para poder acceder y/o cambiar las configuraciones de los equipos, ante necesidad justificada, previa solicitud y autorización del responsable del área involucrada.

- **Del Acceso a la Red**
  - ✓ La Unidad de Estadística e Informática proporcionara acceso a Red únicamente a los empleados públicos que indique el jefe del área correspondiente, asignándoles un "nombre de usuario".
  - ✓ El acceso a red y demás servicios informáticos (tales como SIAF, correo

electrónico, internet, etc.) podrán ser eliminados, a pedido del jefe de área o cuando la Unidad de Recursos Humanos comunique el cese de un determinado empleado. Utilizar software de navegación web designado por el Hospital, el que deberá estar configurado con las directivas establecidas por los procedimientos de instalación de software de navegación web.

- **Medidas para garantizar la confidencialidad de las claves o contraseñas:** Los usuarios deberán tener en cuenta los siguientes criterios a fin de elegir adecuadamente las claves de encendido y de acceso a la Red:
  - ✓ Evitar utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres y apellidos (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
  - ✓ Evitar usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I, fecha de nacimiento, etc.).
  - ✓ Las claves más seguras, en cuanto a su confidencialidad, son aquellas que combinan caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

Los usuarios deben tener en cuenta las siguientes recomendaciones:

- ✓ Adoptar las medidas necesarias para evitar que alguna otra persona pueda ver su clave al momento de digitarla ni siquiera el personal de Soporte de la Unidad de Estadística e Informática; si ello ocurriese, es recomendable cambiar la clave.
- ✓ Evitar escribir la clave en un panel o agenda. Se debe procurar memorizarla

Medidas de seguridad durante la ausencia del usuario

- ✓ En caso se requiera acceder a la computadora del usuario ausente, el responsable del área correspondiente, deberá solicitado por escrito o vía correo electrónico a la Unidad de Estadística e Informática. De ser necesario, esta última eliminara las claves de encendido y de acceso a red, asignando nuevas claves, las que serán de conocimiento exclusivo del responsable del área o del empleado público que éste designe, según sea el caso.
- ✓ En el supuesto a que se refiere el numeral anterior, quien posea las claves asumirá en forma personal, la responsabilidad por la confidencialidad de las mismas, así como de las consecuencias derivadas de su uso.
- ✓ A su retorno, el usuario a quien se asigno la respectiva computadora retomara su responsabilidad respecto de la información almacenada y procesada en ella, por lo que deberá modificar la clave de encendido de red y demás servicios informáticos, de ser el caso.

- **Retiro de información y acceso de Terceros**
  - ✓ La información almacenada y procesada mediante los recursos informáticos del hospital, así como los aplicativos desarrollados por este último, le pertenecen a la entidad de manera exclusiva y excluyente. Por tanto, está prohibido el retiro parcial o total de la información, aplicativo o utilidad, almacenado, procesado o desarrollado mediante los recursos informáticos del Hospital.
  - ✓ Está prohibido permitir, a personas ajenas a la institución, el acceso a la información contenida en las computadoras de la institución.

Los usuarios que incumplan las normas establecidas estarán sujetos a suspensiones temporales o definitivas en el uso de los servicios y recursos brindados de acuerdo a la gravedad del caso.

VIII. DISPOSICIONES COMPLEMENTARIAS

- El cumplimiento de la presente Directiva es de responsabilidad de la Unidad de Estadística e Informática en lo que le compete.
- En caso que el usuario deje de laborar, la Unidad de Recursos Humanos deberá notificar a la Unidad de Estadística e Informática, a efectos de eliminar sus cuentas de acceso.

La Unidad de Estadística e Informática es responsable de la difusión de la presente Directiva y de que los usuarios del hospital cumplan con lo dispuesto.

IX. DISPOSICIONES FINALES

- El hospital no se hace responsable por los conceptos emitidos por los usuarios a través de la red o por su uso mal intencionado o ilegal así como por el daño causado a terceros por el uso no apropiado de los servicios habilitados a los usuarios.