Estadística

MINISTERIO DE SALUD
INSTITUTO DE GESTIÓN DE SERVICIOS DE SALUD
HOSPITALNACIONAL SERGIO E. BERNALES

Nº 213 -2015-DG-HNSEB

RESOLUCIÓN DIRECTORAL

Comas, 02 de Junio de 2015

Visto el Memorando N° 151-2015-OEI-HNSEB de fecha 06 de mayo de 2015 del Jefe de la Oficina de Estadística e Informática del Hospital Nacional Sergio E. Bernales.

CONSIDERANDO:

Que, mediante Memorando N° 151-2015-OEI-HNSEB de fecha 06 de mayo de 2015, el Jefe de la Oficina de Estadística e Informática del Hospital Nacional Sergio E. Bernales, remite a la Dirección Ejecutiva de Administración el Proyecto de Directiva N° 002-2015-OEI-HNSEB - "Directiva de Protección de datos personales del Hospital Sergio E. Bernales" para su evaluación y aprobación;

Que, la Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento aprobado mediante Decreto Supremo N° 03-2013-JUS, tienen por objeto garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2, numeral 6 de la Constitución Política del Estado, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ellas se reconocen;

Que, el artículo 3 de la Ley N° 29733, Ley de Protección de Datos Personales, señala que "La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional";

Que, el Hospital Sergio E. Bernales no cuenta con una directiva específica que regule los mecanismos y procedimientos tendientes a garantizar una protección adecuada de datos personales;

Que, es importante establecer medidas organizativas y técnicas para determinar las condiciones y medidas de seguridad apropiadas para el manejo y tratamiento de datos personales;

Con el visado del Director Ejecutivo de Planeamiento Estratégico, del Director Ejecutivo de Administración, del Jefe de la Oficina de Estadística e Informática, y del Jefe de la Oficina de Asesoría Jurídica;

En uso de las atribuciones conferidas por el Reglamento de Organización y Funciones del Hospital Nacional Sergio E. Bernales, aprobado por la Resolución Ministerial N° 795-2003-SA/DM y sus modificatorias mediante Resolución Ministerial N° 512-2004-MINSA, Resolución Ministerial N° 343-2007-MINSA y Resolución Ministerial N° 124-2008-MINSA;

SE RESUELVE:

ARTÍCULO 1°.- APROBAR la Directiva N° 002-2015-OEI-HNSEB - "Directiva de Protección de datos personales del Hospital Sergio E. Bernales".

ARTÍCULO 2°.- Publíquese la presente Resolución en el Portal de Transparencia del Hospital Nacional Sergio E. Bernales.

ARTÍCULO 3°.-DISPONER que la Oficina de Comunicaciones se encargue de la publicación de la presente resolución en el Portal Institucional

Regístrese y Comuníquese.

MINISTERIO DE SALUD
INSTITUTO DE GESTION DE SERVICIOS DE SALUD
HOSPITAL NACIONAL SERGIO E. BERNALES
Mg. Jaime A. Arévalo Torres
DIRECTOR GENERAL
C.M.P. N° 23086

JAAT/rasl

( ) Dirección General
( ) Dirección Adjunta
( ) Oficina Ejecutiva de Administración
( ) Oficina de Asesoría Jurídica
( ) Oficina de Estadística e Informática
( ) Archivo

DIRECTIVA ADMINISTRATIVA N° 002-2015-OEI-HSEB

DIRECTIVA DE PROTECCIÓN DE DATOS PERSONALES DEL HOSPITAL SERGIO E. BERNALES

I. FINALIDAD

Dar a conocer las políticas y estándares de Seguridad que deben conocer y tomar en cuenta los usuarios y responsables de Base de datos personales para el manejo y trato de los datos personales contenidos en banco de datos personales del Hospital E. Sergio Bernales.

II. OBJETIVO:

2.1. OBJETIVO GENERAL

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales y su manejo por área responsable del Hospital Sergio E. Bernales.

2.2. OBJETIVO ESPECIFICO

- Determinar las condiciones de seguridad en el tratamiento de datos personales.
- Determinar las medidas organizativas y técnicas a cumplir por los responsables del banco de datos personales.
- Establecer las medidas de seguridad apropiadas para el manejo y conservación de base de datos los datos personales en el Hospital Sergio E. Bernales.

III. AMBITO DE ABLICACION

La presente directiva es de aplicación permanente y de cumplimiento obligatorio para todas las áreas responsables de su jurisdicción, así como los órganos de línea, de asesoramiento y apoyo, del Hospital Sergio E. Bernales.

IV. BASE LEGAL

- RM N° 795-2003/SA/DM-Aprueba el Reglamento de Organización y funciones del Hospital Sergio E. Bernales, modificado por la RD N° 512-2004-MINSA

- Resolución Suprema N° 016-2003-SA-Aprueba el cuadro para Asignación de Personal del Hospital Segio E. Bernales, modificada por la RD N° 366-2004-SA-DE-HSEB-OEPE.
- Directiva N° 007-95-INEI/SJI "recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- Ley N° 29733, Ley de Protección de Datos Personales
- Decreto Supremo 003-2013-JUS, aprueba el Reglamento de Ley N° 29733 Ley de Protección de Datos Personales.
- Resolución Ministerial N° 246-2007-PCM, aprueba la Norma Técnica Peruana "NTP ISO/IEC 17799:2007 EDI, Técnicas de seguridad, Código de Buenas Prácticas para la gestión de seguridad de la información 2ª Edición.
- Resolución Ministerial 129-2012-PCM aprueba el uso obligatorio de la norma técnica peruana "NTP-ISO/IEC 27001:2008 EDI Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información en todas las entidades integrantes del Sistema Nacional de Informática.
- Manual de Organización de Funciones para el área de estadística.

V. DISPOSICIONES GENERALES

5.1. DEFINICIONES OPERATIVAS

1. **Datos Personales:** Son cualquier información que permite identificar a una persona.

2. **Datos Sensibles:** Son los constituidos a datos biométricos, referidos a origen racial y étnico, ingresos económicos, convicciones políticas, religiosas, filosóficas, morales y con relación a salud y vida sexual.

3. **Base de Datos Personales:** Conjunto organizado de datos personales, automatizado o no, independiente del soporte que se encuentren, sea físico, magnético, digital, óptico u otros.

4. **Responsable de seguridad:** Rol asignado a una persona que coordina y controla la implementación de las medidas de seguridad en un banco de datos personales.

5. **Usuarios de Sistemas de Información:** Persona natural que tiene acceso a un sistema de información que realiza tratamientos de datos personales. Puede ser el administrador del sistema, administrador de banco de datos, operadores, personal de soporte o el responsable de los datos personales.

6. **Autorización:** Función que permite otorgar acceso de uso de determinados recursos de las base de datos personales.

7. **Archivo:** Sinónimo de fichero y esencia del almacenamiento informático/físico.

8. **Contraseña o password:** Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

9. **Equipos informáticos y comunicación:** Servidores de Red, estaciones de trabajo, impresoras y equipos de comunicaciones (swiches, hub, routers, etc.).

10. **Protección:** Mecanismo de control contra posibles acciones no autorizadas que brinda el sistema informático.

11. **Respaldo:** Se refiere a una copia extra, de un archivo o base de datos.

12. **Seguridad:** Medidas de resguardo contra el acceso no autorizado a los datos personales.

13. **HNSEB:** Hospital Nacional Sergio E. Bernales

14. **OEI:** Oficina de estadística e Informática

VI. DISPOSICIONES ESPECIFICAS.-

El Hospital Segio E. Bernales dispone de Bases de Datos Personales de nivel Complejo con las siguientes características:

- Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un (1) año.
- Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas y/o departamentos del Hospital Sergio E. Bernales).
- Incluye Datos Personales sensibles.
- Las Oficinas Responsables son las que alberga dichos datos Personales en sus instalaciones.

DE LAS ÁREAS RESPONSABLES DE BASE DE DATOS PERSONALES

Artículo 1.- Las Oficinas y/o áreas responsables de Base de datos personales deben de implementar la estructura de roles y responsabilidades del personal que interactúa con los mismos para sobre guardar la integridad de los datos a Proteger.

Artículo 2.- Designar a un Delegado por cada base de Datos Personales, quien se encargara del control de acceso, administración y supervisión.

Artículo 3.- Las Oficinas Responsables de Base de Datos Personales deben de llevar control y registro de los operadores con acceso al banco de datos personales.

Artículo 4.- El Delegado de cada Base de Datos Personal debe generar un registro de revisión que evidencie la realización de dicha revisión, en el cual se debe incluir la fecha de la revisión, usuarios y medios supervisados, así como observaciones de ser el caso.

Artículo 5.- Cualquier anomalía identificada dentro de la supervisión tiene que ser reportado al titular de la Base de Datos y seguir los procedimientos según Art. 21°.

Artículo 6.- Las Oficinas Responsables de la Base de datos Personales deben de brindar capacitaciones, conciencia y entrenamiento en datos personales a los usuarios de sistemas de Información.

Artículo 7.- Las Oficinas Responsables deben de implementar un registro de accesos a banco de datos Personales el cual debe de contener:

- Fecha y Hora del Acceso
- Personas y/o personas que realizaron el acceso
- Identificador del titular de los datos personales
- Motivo de Acceso

Artículo 8.- Para el Proceso de Obtención de Datos Personales se debe de contar con autorización y/o consentimientos para el tratamiento de datos personales, para su registro y preservación.

Artículo 9.- Para el Personal que interactúa con los Datos Personales se debe de Celebrar contratos de confidencialidad para el tratamiento de datos personales con el personal relacionado (interno y/o externo).

Artículo 10.- Revisar periódicamente las medidas de seguridad implementadas con una frecuencia mínima de cada 3 meses.

PARA EL TRASLADO DE DATOS PERSONALES ENTRE OFICINAS y/o DEPARTAMENTOS.

Artículo 11.-Los datos personales en soporte físico deben ser contenidos en un contenedor que evite su acceso y legibilidad así como mecanismos de verificación y no vulneración del contenedor.

Artículo 12.-Para los Datos contenidos en Soporte Informático deben ser transportados previa encriptación (compresión con clave y/o medio para cifrado).

ELIMINACION DE INFORMACION DE MEDIOS INFORMATICOS REMOVIBLES

Artículo 13.-Cuando se requiera eliminar la información contenida en un medio removible informático se debe de utilizar mecanismos de eliminación total de la información (formateo y desfragmentación) para asegurar el borrado total de la información y la no recuperación.

Artículo 14.- Solo personal autorizado por la oficina responsable de la base de datos personal puede ser quien elimine esta información.

COPIA DE SEGURIDAD O REPRODUCCION

Artículo 15.- Cuando sea necesario sacar reproducciones y/o para sobre guardar la integridad de la base de datos, la oficina responsable de base de datos personales debe designar a un personal que ejecute dicha función.
Implementar las siguientes medidas para confidencialidad de datos:

- Utilización de equipos autorizados (fotocopiadoras, escáner, etc)
- Supervisar el proceso de copia y reproducción de documentos, por ningún motivo se puede dejar desatendido este acto.
- Retirar los documentos originales y las copias inmediatamente después de finalizada la copia o reproducción.

Artículo 16.- Las copias de seguridad y/o reproducciones de los documentos tienen que ser registradas indicando como mínimo:

- Nombre de la Persona que solicita la copia.
- Nombre de la persona autorizada a realizar las copias
- Descripción de los datos personales copiados
- Número de copias
- Motivo
- Nombre de la persona que recibe la copia.

- Lugar de destino
- Periodo de validez de la copia

Artículo 17.- Las copias o reproducciones de los documentos deben tener una marca que indique el periodo de valides de las mismas

PARA LAS COPIAS DE RESPALDO:

Artículo 18.- La generación de las copias de respaldo de la Base de Datos Personales, será con frecuencia: diaria, semanal, mensual y anual (según criterio del responsable de la Base de Datos Personales).

- Copias semanales 4 copias por mes ejecutándose cada último día hábil de cada semana,
- Copia Mensual 12 copias por año ejecutándose cada último día hábil de cada semana
- Copia Anual 1 copias por año ejecutándose cada último día hábil de cada año.
- Las copias de respaldo anual obtenido, quedan de forma permanente pasando a conformar los archivos históricos

La copia de seguridad debe ser comprimida y/o encriptada para su seguridad.

Artículo 19.-La información que se procesa periódicamente, se almacenara por periodos, entendiéndose por periodo, al tiempo (mensual, bimensual, trimestral, semestral o anual) que transcurre para que se ejecute el procesamiento de la información.

La Identificación de la operación (ID-OPE) cuya estructura es:

- TC-dm-aaaa /x
- TC : indica que es una copia (Semanal "S", mensual "M", anual "A")
- dm : fecha de grabacion
- Aaaa : año de la grabación.
- x : 1 (primera copia) / 2 (segunda copia).

Artículo 20.-Realizar un proceso de restauración de la DATA contenida en la copia de respaldo, con una frecuencia de cada 3 meses para comprobar que las copias se encuentran en buen estado así mismo documentar dicho proceso.

Artículo 21.-Realizar pruebas semestrales para verificar la integridad de los datos Personales de las bases de datos y se deben documentar los resultados indicando:

- Fecha y hora de la prueba
- Nombre de la persona que realizo la prueba
- Banco de datos personales recuperado
- Archivo recuperado y fecha de datos recuperados
- Tiempo de recuperación
- Acciones tomadas en caso de pruebas insatisfactorias

SOBRE INCIDENTES DE SEGURIDAD

Artículo 22.-Deben ser registrados los incidentes de seguridad relacionados con los bancos de datos personales contando con la siguiente información de ser el caso:

- Fecha y hora del incidente
- Nombre de la persona que lo reporta
- Naturaleza del incidente
- Datos personales comprometidos
- Nombres de las personas involucradas en la resolución del incidente.
- Consecuencias del incidente
- Medidas correctivas implementadas
- Recomendaciones para el titular de datos personales (si Aplica)
- Recuperación de datos
- En caso de haber realizado recuperación de datos, se debe registrar:
- Nombre de la persona que realizo la recuperación
- Descripción y fecha de los datos restaurados
- Descripción de los datos restaurados en forma manual (si Aplica)

Artículo 23.- Al generarse algún hecho fortuito o no autorizado, al verse afectado los derechos patrimoniales o morales y comprobarse el hecho, el titular de la base de datos personales tiene que informar al titular de los datos personales. La siguiente información:

- Naturaleza del incidente
- Datos Personales comprometidos
- Recomendaciones al titular de datos personales
- Medidas correctivas implementadas.

PARA BASES DE DATOS PERSONALES QUE SE REALIZAN CON MEDIOS INFORMÁTICOS:

Artículo 24.- Controlar la Asignación y el uso de las contraseñas de los usuarios de los sistemas de información:

- Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas
- Permitir el Cambio del Usuario cuando lo considere o solicitarlo al área responsable.
- La generación de las contraseñas deben contener al menos 8 dígitos y que sean alfanuméricos (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial, para aumentar la fuerza de la misma.

Artículo 25.- La oficina Responsable de la Base de Datos Personal debe solicitar o generar el acceso a los usuarios según el perfil designado brindando únicamente los privilegios necesarios para su correcto desempeño. Para lo cual ser debe de restringir el acceso a recursos que su función no corresponda.

BASE DE DATOS PERSONALES PROTECCIÓN FÍSICA

Artículo 26.- El ambiente externo de resguardo y custodia de archivos de información histórica, deberá contar como mínimo, con una copia de respaldo

mensual, una copia de respaldo anual, así como la documentación necesaria que permita su adecuada administración.

Artículo 27.- Los medios magnéticos donde está grabada la información deben recibir mantenimiento de limpieza cada tres meses como mínimo, así como también con unidades o dispositivos de lectura/grabación a fin de garantizar la buena grabación y conservación de la información. También aplica para los equipos que interactúan con las bases de datos y los equipos para sacar las copias de seguridad.

Artículo 28.- Las Base de Datos Personales que contengan datos sensibles deben de ubicarse en un ambiente aislado protegido por cerradura o similar, en el cual el mecanismo de acceso recae en el Delegado de la Base de Datos.

Artículo 29.- De encontrarse en un medio informático los equipos para su almacenaje deben recibir mantenimiento preventivo y correctivo. Así también los espacios físicos de almacenaje de medios físicos (formularios, documentos, etc).

Artículo 30.- Los equipos que deben interactúen con el tratamiento de datos personales deben contar con software de protección de código malicioso (antivirus).

Artículo 31.- Los titulares de los datos Personales que se encuentran inmersos en las Base de Datos Personales del Hospital Sergio E. Bernales, tienen la completa facultad de:

- Acceder a la información que sobre si mismos sea objeto de tratamiento en banco de datos personales del Hospital Sergio E. Bernales.
- Rectificar (actualización e inclusión) modificación de datos personales.
- Cancelar y/o revocar el consentimiento de sus datos Personales.
- Oposición por un motivo legítimo y fundado, referido a una situación personal concreta, figurar en banco de datos o tratamiento de sus datos personales.