HOSPITAL NACIONAL DE LA MUJER
"DRA. MARIA ISABEL RODRIGUEZ"

UNIDAD DE INFORMÁTICA

MANUAL SOBRE POLÍTICAS DE SEGURIDAD EN LA UNIDAD DE INFORMÁTICA

SAN SALVADOR, SEPTIEMBRE DE 2016

AUTORIDADES

DIRECTORA : Dra. Adelaida de Lourdes Trejo de Estrada

JEFE DE INFORMÁTICA : Ing. Juan Francisco Cabrera Herrera

AUTORIZADO DIRECTORA:

SAN SALVADOR, SEPTIEMBRE DE 2016

HOSPITAL NACIONAL DE LA MUJER
UNIDAD DE INFORMÁTICA

MANUAL SOBRE POLÍTICAS DE SEGURIDAD EN LA UNIDAD DE INFORMÁTICA

Índice

Págs.

¿Por qué del manual?

El activo más importante que poseen las instituciones actualmente es la información, y por lo tanto deben existir políticas o normas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena, también aquella referente a la aplicación de barreras y procedimientos que resguarden el acceso a los datos.

Objetivo del manual

Presentar los criterios diseñados para salvaguardar el entorno de la Unidad de Informática de eventos accidentales o negligentes que puedan causar daños, pérdidas de información o destrucción, éstos criterios están relacionados con los aspectos lógico y físico.

AMBIENTE FÍSICO

En toda unidad de informática es importante considerar tanto la seguridad física de los equipos como el entorno que los rodea, a fin de contribuir al mantenimiento de éstos.

Sección 1. DE LOS EQUIPOS

a) El mantenimiento y cuidado de los equipos implica la realización de una adecuada limpieza de los mismo tanto externa como interna.
b) Para evitar daños en los discos duros de cada computadora es necesario que éstas cuenten con reguladores de voltaje ya sea propios o compartidos.
c) Para salvaguardar la información en los equipos en caso de situaciones imprevistas. (por Ej. Un corte de energía) es necesario que cuenten con UPS's que le brinden al usuario un tiempo mínimo para almacenar la información.
d) Si el equipo no esta en uso es necesario apagarlo para alargar el tiempo de vida útil de éstos.
e) El servidor de la red de la unidad debe estar en un lugar seguro.
f) Se deben utilizar MEMORIAS USB en buen estado y evitar introducir objetos ajenos a este, en los puerto USB del equipo.

Sección 2. DEL ENTORNO

a) Verificar que el flujo de energía eléctrica sea el adecuado para el funcionamiento de los equipos.
b) La temperatura ambiente en donde se encuentran los equipos debe ser frío tal que contribuya a evitar el sobrecalentamiento de éstos.
c) Verificar que las conexiones de los equipos con los sistemas eléctrico, telefónico u otros sea el correcto, para evitar posibles incidentes perjudiciales a éstos.
d) El Data Center debe tener el sistema de control de incendios.
e) El medio ambiente de la unidad debe estar libre de polvo, suciedad, humedad, pelusas u otros para evitar que estos afecten los puertos USB y los circuitos internos. Por esto es necesario que el área este muy bien aseada.
f) La unidad debe contar con estabilizador de energía para regular los cambios bruscos de flujo así como aquellos cambios imperceptibles.
g) El área de cableado de las computadores debe estar libre de cualquier material que propicie incendios tales como papel, plásticos, aerosoles etc.

AMBIENTE LÓGICO

Seccion1. DE LOS PROGRAMAS DE COMPUTO

a) Cada computadora deberá contener su respectiva licencia de los programas de software que utiliza.
b) Deben realizarse copias de respaldo de la información de carácter institucional, en los sitios designados para ello, a petición de las Jefaturas de Departamentos y/o Servicios que lo soliciten al Jefe de la Unidad de Informatica.
c) Cada equipo debe contar con un software antivirus a fin de que las computadoras no se contaminen de virus.

d) Verificar que los programas de software desarrollados en la unidad estén funcionando correctamente.
e) Cada programa de software desarrollado en la unidad deberá contar con su manual del usuario.

Seccion2. DE LOS USUARIOS

a) Asignar niveles jerárquicos de seguridad para el acceso a la red y en las aplicaciones.
b) Cada usuario debe tener una clave de acceso a la red, para crear dichas claves es necesario tomar en cuenta los siguientes aspectos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
- No usar contraseñas completamente numéricas con algún significado (teléfono, DUI, fecha de nacimiento, patente del automóvil, etc.).
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de 7 caracteres como mínimo.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:

  · Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3.

  · Usar un acrónimo de alguna frase fácil de recordar: A rio Revuelto Ganancia de Pescadores: ArRGdP.

  · Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P

f) Los usuarios pueden cambiar su contraseña en los sistemas informáticos que funcionan dentro de la institución cuando lo deseen.