MANUAL DE IMPLEMENTACIÓN DE POLÍTICAS Y SEGURIDAD TIC HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS

Versión 1

Proceso: Gestión de Seguridad Informática

San Marcos, agosto de 2017

INTRODUCCIÓN

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la ESE Hospital Regional de II Nivel San Marcos una cultura de calidad operando en una forma confiable. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Institución en materia de seguridad.

Las normas y políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios prestados por la red a los usuarios finales. El documento que se presenta como políticas de seguridad, pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la ESE, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias. Toda persona que utilice los servicios que ofrece la red y los dispositivos informáticos, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

Las Políticas y Lineamientos expuestos en este manual, son de obligatorio cumplimiento para el personal de la ESE Hospital Regional Nivel II San Marcos y no podrán ser modificadas sin la autorización del Comité de Gobierno en Línea, por tanto, para cualquier sugerencia de cambio se tramitará a través del Área de Sistemas, quien se encargará de comunicarla al presidente del Comité para su difusión a los demás integrantes

CAPITULO I
ASPECTOS GENERALES DEL MANUAL

OBJETIVOS

Objetivo General
Mantener la integridad, confidencialidad y disponibilidad de la información; preservar la infraestructura tecnológica (equipos de cómputo, de redes, de voz e impresoras) utilizados en la ESE Hospital Regional Nivel II de San Marcos que permiten el diligenciamiento, almacenamiento y disponibilidad de la información.

Objetivos Específicos

- Organizar por capítulos las diferentes políticas que se integran en el manual para que brinden orientación a los usuarios sobre cómo proceder en su uso.
- Socializar las diferentes políticas con los usuarios, logrando la adopción y aplicación de las mismas
- Tener el control de la información de manera íntegra, confidencial y confiable
- Dar el debido manejo a los datos, bienes informáticos (hardware y software) con el fin de minimizar los riesgos en el uso de las tecnologías de información.
- Ofrecer guías mínimas del manejo de protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en la Institución y de esta manera cumplir con normas, leyes y políticas de seguridad informática.

1.2. ALCANCE

Las políticas y medidas establecidas en este manual aplican para todos los usuarios administrativos y asistenciales de planta y contratistas que tengan relación directa con los sistemas o equipos tecnológicos que integran la infraestructura computacional y de telecomunicaciones de la ESE Hospital Regional Nivel II de San Marcos

1.3 REFERENTES NORMATIVOS

- ISO/IEC 27000 - es un vocabulario estándar para el SGSI.
- SO/IEC 27001 - Norma que especifica los requisitos para la implantación del SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
- ISO/IEC 27002 - Information technology - Security techniques - Es el código de buenas prácticas para la gestión de seguridad de la información.
- ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001.
- ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información.
- ISO/IEC 27006:2007 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
- ISO/IEC 27007 - Es una guía para auditar al SGSI
- ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades
- LEY 1273 DE 2009: protección de la información y de los datos
- LEY 1581 DEL 2012: desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
- DECRETO 1377 DE 2013: El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- LEY 603 DE 2000: La Ley 603 de 2000 faculta a la Entidad para realizar verificaciones y enfatiza en la obligación de declarar en los informes de gestión el cumplimiento de las normas que protegen el software

1.4 DEFINICION DE TERMINOS

Las definiciones están relacionadas con las tecnologías de la información y las comunicaciones.

Access Point o Punto de acceso inalámbrico: (WAP o AP por sus siglas en inglés: Wireless Access Point)
En una red de computadores, es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un Access Point también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Administrador de Red: .Es la persona encargada de la administración de la red. Entre sus actividades incluye la administración, mantenimiento y monitoreo de los equipos de comunicaciones y servidores que conforman la red: switches, routers, firewalls, entre otras.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Ancho de banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

Spam: Se denomina spam al correo electrónico no solicitado que se envía por Internet de forma masiva
Antispam: Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados
Virus Informático: Los virus informáticos son programas que se introducen en un ordenador con el propósito de reproducirse a sí mismos e interferir con el harware o el software. Estos virus están programados para ser indetectables y su cometido es el de alterar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo

Antivirus: Los antivirus son programas que se encargan de detectar a los virus, de combatirlos y de erradicarlos de una manera lo más rápida posible. Hay que tener en cuenta que un antivirus es una solución para minimizar los riesgos pero que nunca será una solución definitiva puesto que existen virus que son muy difíciles de detectar. Para ello es muy importante mantener el

antivirus actualizado constantemente para que sea capaz de combatir los que se crean cada día

Base de Datos: (Data Base). Una base de datos es una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

Cifrado: método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Cookies: Las cookies son pequeños archivos que algunos sitios web guardan en tu ordenador. Las cookies almacenan información sobre tí, como nombre de usuario o información de registro, o preferencias de usuario, pero no espían

Copia de seguridad: consiste en guardar en un medio, preferiblemente extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Esta se puede realizar tanto en ordenadores personales como en servidores. Este medio puede ser un disco duro externo, un CD-ROM grabable, cintas de datos (DAT), etc. La copia de seguridad puede realizarse solo de los datos (bases de datos, correo electrónico, carpetas compartidas en un servidor de archivos) pero también de archivos que formen parte del sistema operativo.

Contraseña de Usuario: Una contraseña de usuario o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto

Correo electrónico: (en inglés: e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos

Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.

Firewall: Software o hardware que comprueba la información procedente de la red, bloqueando o permitiendo el paso según esté configurado. Están disponibles en los Sistemas Operativos, Antivirus y Switches.

Hacker: Experto en programación Suele ser un programador, descubren vulnerabilidades, a veces con ánimo constructivo y otras para actividades delictivas.

Dirección IP: es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Modem: Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).

PDF (Portable Document Format): (Formato de Documento Portable) Formato para almacenar documentos, desarrollado por la empresa Adobe Systems, originalmente exclusivo para su programa Acrobat Reader. Actualmente es un formato abierto. La extensión de los archivos de este formato es ".pdf" y además de Acrobat Reader, puede ser leído por otros programas.

Red: Una red informatica, también llamada red de ordenadores, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos, programas, bases de datos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos).

Seguridad Informática: serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos abarca:

- El conjunto de servicios y mecanismos que aseguren la integridad y privacidad de la información que los sistemas manejen.
- El conjunto de servicios, mecanismos y políticas que aseguren que el modo de operación de un sistema sea seguro. El que se especificó en la fase de diseño o el que se configuró en tiempo de administración.
- El conjunto de protocolos y mecanismos que aseguren que la comunicación entre los sistemas esté libre de intrusos.

Sistema de Información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso, desarrollados para cubrir una necesidad u objetivo.

Riesgo informático: es la posibilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generando pérdidas o daños.

Sistema Operativo: Un sistema operativo puede ser definido como un conjunto de programas especialmente hechos para la ejecución de varias tareas, en las que sirve de intermediario entre el usuario y la computadora. Este conjunto de programas que manejan el hardware de una computadora u otro dispositivo electrónico. Provee rutinas básicas para controlar los distintos dispositivos del equipo y permite administrar, escalar y realizar interacción de tareas

Switch: conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro, opera en la capa dos el modelo OSI

TIC: Tecnologías de la Información y las Comunicaciones.

Rootkit: es un conjunto de herramientas usadas por crackers para acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Son difíciles de detectar y eliminar.

Usuario: en informática (user), un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema, además se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados en este.

Usuario final: En informática, el término usuario final designa a la persona o personas que van a manipular de manera directa un producto de software.

Vulnerabilidad: fallo en la programación que permite la infección o el secuestro de nuestra información. Las vulnerabilidades pueden ocasionar lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceda a los datos, lo que se opone a las restricciones específicas de acceso
- Permitir a un atacante suplantar identidad
- Permitir a un atacante realizar una negación de servicio

Web: es un documento electrónico que contiene información, cuyo formato se adapta para estar insertado en la World Wide Web, de manera que los usuarios a nivel mundial puedan entrar a la misma por medio del uso de un navegador,

visualizándola con un dispositivo móvil como un smartphone o un monitor de computadora

World Wide Web: (WWW) o red informática mundial es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de esas páginas usando hiperenlaces.

1.5. CONDICIONES GENERALES

Para la implementación de este Manual, se deben tener en cuenta las siguientes consideraciones

- El Manual deberá estar habilitado para todas las áreas y unidades funcionales del Hospital Regional Nivel II San Marcos, de manera física y/o digital.
- El Manual podrá ajustarse de acuerdo a cambios en las políticas aquí definidas, previa autorización de la gerencia o quien ella designe en concordancia con el área de sistemas

Lineamientos

La Gerencia, el Comité de Gobierno en Línea, el Area de Sistemas y demás dependencias, deben implementa los lineamientos que protejan la operatividad de la plataforma tecnológica disponible para la comunidad institucional, entre los que se destacan:

- Brindar apoyo tecnológico eficiente y oportuno a las diferentes áreas y unidades funcionales del Hospital Regional Nivel II de San marcos.
- Promover la integración de todos los sistemas de información que existan o se adquieran para la ESE.
- Asegurar la conectividad de los equipos, usuarios y servicios, de acuerdo con los estándares técnicos.
- Coordinar con las áreas encargadas del entrenamiento y capacitación de los usuarios institucionales, en el uso y manejo de las herramientas TIC
- Coordinar y controlar con las áreas administrativas encargada de la adquisición de equipos, sistemas, insumos y otros recursos asociados al desarrollo de TIC, se realicen de una manera óptima, con los estándares adecuados. Para garantizar este proceso el área de sistemas debe emitir un concepto técnico respecto a los bienes o servicios adquiridos
- Prestar asistencia técnica eficiente y oportuna que garantice la continuidad en las operaciones de los sistemas informáticos de la ESE

- Minimizar los riesgos inherentes a la seguridad de la información.

CAPÍTULO II

2 POLÍTICAS GENERALES

2.1 Políticas Generales (Usuario Final y Administrador)

1. Los recursos y servicios de Tecnología de Información y Comunicaciones (TIC) suministrados por la ESE Hospital Regional Nivel II San Marcos a las diferentes áreas y unidades funcionales, deberá ser para el estricto uso en actividades propias o directamente relacionadas con las funciones del área en mención .
2. Es responsabilidad de la gerencia del Hospital Regional Nivel II San Marcos garantizar los recursos financieros, materiales y humanos, necesarios para el mantenimiento, operación y la actualización de los recursos, servicios e infraestructura tecnológica de la ESE.
3. Queda prohibido la utilización de servicios TIC provistos por la ESE, a personal ajeno a la comunidad institucional, sin orden escrita de la gerencia o a quien deleguen esa función
4. Los recursos TIC propiedad de terceros que estén conectados a la red informática del Hospital Regional Nivel II de San Marcos, estarán sujetos a las políticas y lineamientos establecidos en este manual.
5. Los usuarios de recursos y servicios TIC de la red informática del Hospital Regional Nivel II de San Marcos, serán responsables del correcto uso (racional, legal y ético), evitando saturación o colapso por rutinas inadecuadas o maliciosas.
6. La asignación de recursos y utilización de los servicios TIC estará sujeto a las capacidades de la infraestructura tecnológica con la que cuenta la ESE.
7. Los proyectos de actualización de la infraestructura tecnológica de la ESE Hospital Regional Nivel II San Marcos para el mejoramiento en la prestación y la utilización de los servicios, estarán sujetos a la disponibilidad y asignación presupuestal para su ejecución.
8. La adquisición de recursos TIC destinada a la dotación de los usuarios que así lo requieran, estará sujeta a la disponibilidad y asignación presupuestal para tal fin.
9. La conexión de estaciones de trabajo, de cualquier tipo, ya sea en una oficina individual o dependencia administrativa, a la red informática del Hospital Regional Nivel II de San Marcos y el acceso a Internet, deberán tramitarse e implementarse a través del Área de Sistemas.
10. La conexión de estaciones de trabajo remotas, solo se autorizan por orden directa de la gerencia.

11. El uso de servicio telefónico, los privilegios y permisos asociados al mismo, quedará sujeto a la aprobación de la Gerencia o las personas que ella autorice para tal fin.
12. Las estaciones de trabajo deberán disponer de un sistema operativo legal que permita el acceso a los recursos de la red e internet con el uso de un nombre de usuario y una contraseña.
13. Todas las estaciones de trabajo deberán disponer de una licencia que permita el uso de cualquier aplicación que así lo amerite.
14. Los servicios y recursos TIC deben ser administrados por personal del área de sistemas, quienes tendrán la responsabilidad de mantener, configurar, modificar, instalar y actualizar los servicios y recursos; siempre alineados con las políticas y lineamientos de la ESE Hospital Regional Nivel II San Marcos emanados de el Área de Sistemas y/o el Comité de Gobierno en Línea

Usuario Final

- Las autorizaciones concedidas a los usuarios para acceder a los recursos de la red y software asistencial y/o administrativo serán individuales y no transferibles.
- Todo servicio tecnológico deberá ser solicitado al Area de Sistemas por parte del jefe de área o unidad funcional correspondiente. Mediante oficio escrito se expondrá el requerimiento
- El usuario deberá acatar los acuerdos y/o compromisos asociados al servicio que utilice.
- La experimentación de nuevos servicios de carácter innovador o de mejora, deberá ser realizada en ambientes de prueba con la finalidad de evitar cualquier impacto negativo sobre el ambiente de producción.
- Para llevar un registro y control de la información de los equipos administrados, se cuenta con inventario tecnológico actualizado

Administrador

- El acceso a los servicios de la red será administrado por el Área de Sistemas en función de las necesidades y prioridades de la ESE y de la disponibilidad de recursos.
- Las competencias y responsabilidades de los encargados de administrar los servicios deberán estar claramente explícitas en la descripción de sus funciones, matriz de responsabilidad, manual de normas y procedimientos internos.

- En los servicios que lo ameriten, se deberá utilizar un nombre de usuario (ID) único que lo vincule con sus acciones.

CAPÍTULO III

POLÍTICAS DE SEGURIDAD DE INFORMATICA

Este documento se constituye en la guía mediante la cual se establece la normatividad, controles y procedimientos que regulen la forma en que la ESE, prevenga, proteja y maneje los riegos de seguridad a los que se enfrentan las tecnologías de la información.

En este sentido, el tipo de información a proteger puede encontrarse, almacenada en bases de datos digitales, trasmitidas por el correo electrónico, medios magnéticos, videos, entre otros que contengan información institucional.

Estas políticas serán revisadas regularmente para actualizarlas de acuerdo a cambios relacionados con la ESE y los ocasionados por la transformación tecnológica.

POLITICAS DE SEGURIDAD FISICA

3.1 Acceso Físico

La ESE Hospital Regional de II Nivel San Marcos, destinarán un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.
Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.
Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un funcionario del área de Sistemas
Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario laboral
El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable o los profesionales del Area de Sistemas, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa de La ESE y al personal de seguridad del edificio

3.2 Protección Física

3.2.1 Rack de Comunicación

El Rack deberá:

- Tener una puerta de acceso de vidrio templado transparente o maya, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la gerencia y el Área de Sistemas
- Recibir limpieza y mantenimiento por lo menos dos veces al año.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Evitar elevadas temperaturas que llegasen a comprometer el buen funcionamiento de los equipos de comunicación y datos.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Contar con algún esquema que asegure la continuidad del servicio.
- Control de humedad
- Prevención y/o detección de incendios
- Sistemas de extinción de incendios

3.2.2 Infraestructura

Las Áreas y Unidades Funcionales deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las existentes.
El resguardo de los equipos de cómputo deberá quedar bajo el área de Sistemas contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos

3.3 Instalaciones de equipos de cómputo

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.

- El Área de Sistemas, deberá contar con un plano actualizado de las instalaciones eléctricas, de comunicaciones y del equipo de red.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

3.4 Control

El Área de Sistemas debe llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.

- Los encargados del área de sistemas son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.
- Recursos Humanos se encargará de reportar al área de sistemas cuando un usuario deje de laborar o de tener una relación con la ESE Hospital Regional san Marcos con el fin de retirar las credenciales de ingreso a los recursos informáticos y supervisar la correcta devolución de los equipos asignados al usuario.
- El usuario, en caso de retiro, deberá tramitar ante el Área de Sistemas la paz y salvo tecnológico correspondiente.

3.5 Respaldos

- Las Bases de Datos de La ESE Hospital Regional San Marcos serán respaldadas diariamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro que permita tener contingencia y continuidad de negocio.
- Se deben implementar servidores de contingencia de Bases de Datos y aplicaciones que garanticen la continuidad de las actividades relacionadas con los sistemas de información en la ESE Hospital Regional Nivel II San Marcos
- Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en unidades de almacenamiento externo.
- El Área de Sistemas no podrá remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter

ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

3.6 Recursos de los usuarios

3.6.1 Uso

- Los usuarios deberán cuidar y hacer un uso adecuado de los recursos de cómputo y Red de La ESE Hospital Regional Nivel II San Marcos, de acuerdo con las políticas que en este documento se mencionan.
- Los usuarios deberán solicitar apoyo al área de Sistemas ante cualquier duda en el manejo de los recursos de cómputo de ESE.
- El correo electrónico no se deberá usar para envío masivo, materiales de usos no institucionales o innecesarios.

3.6.2 Derechos de Autor

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo y demás fuentes que violen la ley de derechos de autor.
Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la ESE Hospital Regional San Marcos bajo ninguna circunstancia sin la autorización escrita. No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que La ESE posee una licencia que cubre dicha instalación.

- No está autorizada la descarga de Internet de programas informáticos no autorizados por La Gerencia o El Área de Sistemas.
- No se tolerará que un empleado cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P) que pueden utilizarse para comercializar trabajos u obras protegidos por los derechos de autor.
- No se tolerará un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Si un usuario desea utilizar programas informáticos autorizados por ESE Hospital regional Nivel II en su hogar, debe consultar con el Área de Sistemas para asegurarse de que ese uso esté permitido por la licencia del autor.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
- Los usuarios que se enteren de cualquier uso inadecuado que se haga en la ESE Hospital Regional Nivel II de San Marcos de los programas informáticos o la documentación vinculada a estos, deberán notificar al Gerente o encargado del área en la que laboran
- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión.
- No se permite la duplicación ilegal de programas informáticos.

Conectividad

3.7 Red

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de ESE entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes o internet

- El Área de Sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la ESE.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de ESE Hospital regional Nivel II de San Marcos y se usarán exclusivamente para actividades relacionadas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles.
- El uso de analizadores de red es permitido única y exclusivamente por el Área de Sistemas para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad.

Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o involucrado dependiendo de las políticas.

3.8 Servidores

3.8.1 Configuración e instalación

El Área de Sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

- Durante la configuración de los servidores el Area de Sisetmas genera las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.
- Los servidores que proporcionen servicios a través de la red e Internet deberán:
  1. Funcionar 24 horas del día los 365 días del año.
  2. Recibir mantenimiento preventivo mínimo dos veces al año

- La información del servidor deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:
  1. Diariamente, información crítica.
  2. Semanalmente, los documentos web.
- Los servicios hacia Internet deben proveerse preferiblemente a través de los servidores con reglas de navegación que incluyan restricciones y protección contra intrusos.

3.8.2 Correo Electrónico

- El área de Sistemas se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico institucional.
- Para efecto de asignarle su cuenta de correo al usuario, el área de Recursos Humanos deberá llenar una solicitud para tal fin y entregarlo al área de Sistemas
- La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres

3.8.3 Bases de Datos

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

3.9 Recursos de Cómputo

3.9.1 Seguridad de cómputo Políticas de Seguridad Informática

- El área de Sistema es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios, la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.
- El área de Sistema debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.
- El área de Sistema es la única autorizada para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

Ingeniero Área de Sistemas

Los Ingenieros de Soporte tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del jefe de área o unidad funcional
- Deben actualizar la información de los recursos de cómputo, cada vez que adquiera e instale equipos o software.
- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red de la ESE Hospital Regional Nivel II San Marcos
- Auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la Gerencia los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

Renovación de equipos

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando un área requiera de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de Sistemas a fin de que se seleccione el equipo adecuado. Sin el visto bueno de Sistemas no debería autorizarse una compra de equipo computacional.

Uso de Servicios de Red

- El área de Sistemas es la responsable de la administración de contraseñas y deberán guardar su confidencialidad
- No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales, excepto por orden expresa de La Gerencia.

3.9.2 Responsabilidades Personales

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su usuario y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su cuenta está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

Uso Apropiado de los Recursos

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

No está permitido:

- El uso de estos recursos para actividades no relacionadas con el propósito de la ESE Hopital Regional Nivel II San Marco, o bien con la extralimitación en su uso.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

CAPITULO IV

4. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

4.1. Infraestructura de la red eléctrica regulada.

La infraestructura de la red eléctrica regulada deberá desarrollarse siguiendo las normas y estándares para este fin, permitiendo la seguridad del recurso humano, tecnológico y documental en la ESE. De la misma manera, deberá asegurar el cableado, la protección de la información y de los equipos en las aéreas administrativas y asistenciales.

Las diferentes áreas institucionales que están reguladas con una infraestructura eléctrica deben cumplir varias responsabilidades para garantizar la protección de la información que manejas y de los equipos, citamos las siguientes:

- Los usuarios de las zonas reguladas eléctricamente deberán verificar que el equipo de cómputo bajo su responsabilidad esté conectado a la toma naranja (CPU y Pantalla).
- Los usuarios deben verificar que las impresoras, ventiladores, radios entre otros que No sean equipos de cómputo No estén conectados a tomas naranja.

- El usuario No deberá conectar multitomas o reguladores a toma naranja para tratar de conectar más equipos.

4.2 Infraestructura de la red de datos.

La ESE Hospital Regional Nivel II San Marcos cuenta con infraestructura de red que comprende el cableado, swiches, routers, unidades inalámbricas. Los dispositivos anteriores permiten la interconexión de equipos (computadores, impresoras) para acceder a servicios como: Internet, interacción entre usuarios a través de sistemas de información entre otros.

El Area de Sistemas es la encargada de garantizar el funcionamiento de estos equipos y servicios, para lo cual realiza verificación permanente de los recursos de red existentes, mejoras que pueda realizarse y servicios externos que puedan ayudar en el soporte y monitoreo.

4.2.1 Centros de cableado

El centro de cableado es el lugar o punto único donde se concentra el cableado de la red local y se conectan los dispositivos que permiten la interconexión para la comunicación interna y hacia internet. En este espacio solo está permitido el acceso al personal de soporte técnico institucional o externos que cumplan una labor contratada, para los diferentes usuarios institucionales está restringido el acceso. Aquí se encuentran dispositivos com: router, transiver y demás que permitan la interconexión para el funcionamiento de la red local.

4.3. Equipos.

4.3.1. Inventario de equipos.

Los equipos de cómputo de la ESE son los activos indispensables para la interacción tecnológica: Para tener un control general se deben relacionar los siguientes registros:

- Usuario responsable del equipo.
- Código de los equipos asignado por el Area de Sistemas.
- Dirección Ip.
- Confirmación hoja de vida
- Descripción general de las características técnicas del equipo (CPU).
- Marca
- Licencia Sistemas Operativo.
- Licencia herramienta ofimática.

- Fecha de adquisición.
- Observaciones generales

4.3.2. Mantenimiento preventivo de equipos.

- Elaborar el cronograma anual para la programación del mantenimiento preventivo de los equipos de cómputo.
- De acuerdo al cronograma, planear semestralmente la realización del mantenimiento preventivo a equipos de cómputo
- Llevar el control del mantenimiento preventivo programado semestralmente.
- Elaborar el registro de equipos y partes para baja por obsolescencia para el servicio, por daños o fallas graves.
- Antes de la ejecución del mantenimiento preventivo, explicar al usuario como elaborar la copia de seguridad de la información de los equipos bajo su responsabilidad.
- Brindar soporte al usuario en el manejo de software legal en el equipo (sistema operativo y herramientas ofimáticas).
- Al entregar el equipo con el mantenimiento preventivo realizado, solicitarle al usuario la verificación del funcionamiento general del equipo, así como de la información.

4.3.3 Seguridad de los equipos: protección contra virus.

Para la instalación de software antivirus, se debe:

- Verificar la capacidad de los equipos de cómputo, antes de la instalación.
- Realizar pruebas de funcionamiento una vez instalado.

4.3.4 Adquisición del software.

Los usuarios y funcionarios que requieran la adquisición de software deberán presentar el requerimiento en la oficina de Almacén e igualmente deberán informar a el Área de Sistemas quien se encargara de evaluar el tipo de software, los requerimientos de instalación, el tipo de licencia, entre otras características que permita analizar la viabilidad de la adquisición.

Por otra parte, si lo que requiere el usuario o empleado es la instalación de software específico individual que sea propiedad de la ESE Hospital Regional Nivel II San Marcos, deberá solicitarlo por escrito a el Área de Sistemas para que sea esta quien verifique la capacidad de la licencia o si debe adquirirse una adicional. Si es software es para trabajo en equipo debe presentar la autorización de administrador de sistema de información.

Sera una falta grave que los usuarios o funcionarios instalen cualquier tipo de software en sus computadoras conectado a la red de la ESE Hospital Regional Nivel II San Marcos y que no esté autorizado previamente por el jefe inmediato y el Area de Sistemas (encargada del control).

4.3.5 Protección y ubicación de los equipos de cómputo.

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Jefe Inmediato (si es cambio de ubicación), Almacén (si es descarga del inventario) y el Área de Sistemas (si involucra actividad técnica), debiéndose solicitar a las mismas por escrito en caso de requerir este servicio.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario de la ESE Hospital Regional Nivel II San Marcos.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas entre otras instaladas y autorizadas en los equipos que utilizan, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.
- Exclusivamente el personal autorizado de el Area de Sistemas de la ESE Hospital Regional Nivel II San Marcos podrá llevar a cabo los servicios y reparaciones a los equipos de cómputo.
- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a mantenimiento o reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de mantenimiento o reparación.
- El usuario deberá dar aviso de inmediato a la Gerencia y almacén en caso de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su responsabilidad.
- El equipo de cómputo o cualquier recurso tecnológico que sufra algún daño por maltrato, descuido o negligencia por parte del usuario comprobada la acción en contra del bien, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

CAPITULO V

5 POLÍTICA DE MANEJO Y CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN.

5.1 Acceso.

La ESE Hospital Regional Nivel II San Marcos prohíbe el acceso no autorizado a los sistemas de información. Ningún usuario o funcionario debe usar el usuario o contraseña de otro, y de la misma manera No podrán dar a conocer su contraseña o, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo única y exclusivamente al personal de soporte de Área de Sistemas.

5.1.1 Privacidad.

La ESE Hospital Regional Nivel II San Marcos no garantiza totalmente la privacidad de los usuarios, aunque los sistemas de información de tipo laboral funcionen correctamente, porque estos pueden ser vulnerados por usuario que pueden revelarlo a otros. Los usuarios deben entender que ningún sistema de información es completamente seguro. Por lo tanto, La ESE implementara todos los recursos, herramientas y acciones encaminadas a proveer un entorno seguro y de privacidad de los sistemas de información.

5.1.2 Seguridad en el correo electrónico.

El propósito de estas políticas es asegurar la privacidad de los mensajes de correo electrónico, el buen uso del sistema y el compromiso inherente de la ESE al suministrar este servicio al personal.

- El personal de la ESE Hospital Regional Nivel II San Marcos no puede emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos institucionales.
- Todos los mensajes de correo electrónico que utilizan los sistemas de información de la ESE Hospital Regional Nivel II San Marcos, deben contener el nombre y apellidos del remitente, su cargo, dirección y número telefónico.
- La creación de correos electrónicos de las dependencias administrativas será genéricas y administradas por seguridad por el jefe del área o la persona que este autorice.
- Un mensaje de correo electrónico debe ser retenido y conservado para futuras referencias si contiene información relevante y de importancia o

si tiene valor como evidencia de una decisión administrativa de la ESE Hospital Regional Nivel II San Marcos

- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página que indique que el mensaje puede contener información confidencial, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo, que puede ser analizado por otras dependencias de la ESE.

La ESE Hospital Regional Nivel II San Marcos debe comunicar a todos los usuarios que los sistemas de correo electrónico, solamente deben ser utilizados para propósitos institucionales, todos los mensajes enviados por correo electrónico constituyen registros de la ESE, quien se reserva el derecho de acceder y revisar cualquiera sin previo aviso y los administradores pueden revisar el correo electrónico del personal para determinar si han roto la seguridad, han violado la política de la ESE Hospital Regional Nivel II San Marcos o han realizado actividades no autorizadas.

Control de Acceso Lógico a Usuarios Externos

- El acceso a los sistemas de información de la ESE Hospital Regional Nivel II San Marcos para personal externo debe ser autorizado por la Gerencia, quien deberá notificarlo por escrito al Área de Sistemas.
- Los usuarios no deben proporcionar información a personal externo, sobre los mecanismos de control de acceso a los sistemas de información institucionales.

5.2 Portal Institucional.

El personal del ESE encargado de la información publicada en la Web será el Área de Sistemas quien debe garantizar la disponibilidad del portal en producción en Internet.

CAPITULO VI
6 POLITICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

La presente política de protección y privacidad de datos personales forma parte de los términos y condiciones que regulan el uso de los datos almacenados de los usuarios internos y externos de la ESE Hospital regional de II Nivel de San Marcos, conforme con la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, donde se establece especial protección al derecho que tienen las personas naturales para autorizar el manejo de la información personal que de ellas es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación.

Acorde con la normatividad citada, el dato personal es cualquier información enlazada que relaciona a una o varias personas naturales que, dependiendo de su nivel de utilización y contacto con la intimidad de las personas, podrá ser público, semiprivado o privado.

Por ello, los datos que tengan el carácter de personal, tales como el nombre, identificación, edad, género, dirección, teléfono y correo electrónico suministrados a la ESE, serán administrados de forma confidencial, con las debidas garantías constitucionales, legales y demás normas aplicables a la protección de datos personales, siendo claro que la ESE Hospital Regional Nivel II San Marcos ha adoptado las medidas necesarias de índole técnica, jurídica y administrativa para garantizar la seguridad de los datos de carácter personal, e impedir su modificación, pérdida, procedimiento o acceso no autorizado.

La ESE Hospital Regional Nivel II San Marcos garantiza que se abstiene de permitir, vender o compartir los datos de carácter personal recolectados, igualmente actualizará, rectificará o eliminará los datos cuando éstos resulten erróneos, inconclusos o hayan dejado de ser obligatorios u oportunos para la finalidad inicial o por expresa solicitud del interesado.

En ejercicio de los derechos de información, actualización y corrección de datos, el titular de la información podrá ejercer su derecho a conocer, actualizar, o modificar los datos personales que haya proporcionado a la entidad, enviando en medio electrónico o físico tal solicitud, indicando su nombre, apellidos y los datos de contacto para recibir comunicaciones.

BIBLIOGRAFIA

- http://www.iso.org/iso/home.html (definicion de norma ISO) consulta y copia de conceptos
- http://www.masadelante.com/faqs/ancho-de-banda
- http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-el-sistema-operativo.php
- http://www.abartiateam.com/antispam-antivirus
- http://www.maestrosdelweb.com/que-son-las-bases-de-datos/
- https://www.ecured.cu/Usuario_(Inform%C3%A1tica)
- http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 (concepto basico de ley 1273 de 2009)
- http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981 (concepto basico de ley 1581 de 2012)
- http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646 (concepto basico decreto1377 de 2013)
- http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960 (concepto basico de LEY 603 DE 2000)

Aprobación del documento				
	Nombre	**Cargo**	**Firma**	**Fecha**
Elaboro	Victor Moreno Perez	Área de Sistemas		23/08/2017
Revisó	Jesús Vergara Barreto	Asesor Jurídico		23/08/2017
Aprobó	Rosalba Lastra Mejía	Gerente		23/08/2017