POLITICA DE SEGURIDAD DE LA INFORMATICA

HOSPITAL RAFAEL PABA MANJARREZ

SAN SEBASTIAN – MAGDALENA

TABLA DE CONTENIDO

1. DECLARACION DE LA POLITICA

a) PROPOSITO

Con la definición de las políticas y estándares de seguridad de la informática se busca establecer en el interior de la Institución una cultura de calidad operando en una forma confiable. De igual manera nos servirá de guía para clasificar, evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades del Hospital Rafael Paba Manjarrez en materia de seguridad de la informática.

b) ALCANCE

La política está dirigida a toda persona que ingresa como usuario del Hospital Rafael Paba Manjarrez para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en la Políticas de Seguridad de la informática.

c) OBJETIVO GENERAL

Establecer medidas y patrones técnicos de administración y organización de las Tecnologías de la Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el proceso de sistemas de información y así dar el debido cumplimiento de los objetivos institucionales.

d) OBJETIVOS ESPECÍFICOS

- 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.

2. REFERENTES NORMATIVOS

- ISO 27000 (TODA LA SERIE)

ISO/IEC 27000 - es un vocabulario estándar para el SGSI.

ISO/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 específica 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 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
- 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 de2012, 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.

3. DEFINICION DE TERMINOS

-PLANES DE CONTINGENCIA : Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

-HARDWARE: se puede definir como el conjunto de los componentes que conforman la parte material (física) de una computadora.

-SOFTWARE: se define como el conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora o de igual manera se define como la parte no tangible dentro de un sistema.

-**CPU:** son las siglas que hace referencia a Central Processing Unit**,** que en español significa **Unidad Central de Procesamiento**, pero a la cual podemos llamar también simplemente**"procesador"**.

-USB: Sigla del inglés universal serial bus, periférico que permite conectar diferentes periféricos a una computadora.

- Backup: Es una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

-FTP: protocolo de red llamado **Protocolo de Transferencia de Archivos** es como su nombre lo indica una de las formas en la cual podemos enviar archivos hacia una Red TCP (siglas en inglés de Transmisión Control Protocol) en la que utilizaremos la clásica arquitectura de Cliente - Servidor para dicha transferencia.

4. SUSTENTO CONCEPTUAL Y TEÓRICO DE LA POLÍTICA

Todo el personal nuevo de la Institución, deberá ser notificado al proceso de sistemas de información, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático. Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática. Todo servidor o funcionario nuevo de la ESE Hospital Rafael Paba Manjarrez, deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se dan a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

SEGURIDAD FISICA Y DEL MEDIO AMBIENTE

Para el acceso a los sitios y áreas restringidas se debe notificar al proceso de sistemas de información para la autorización correspondiente, y así proteger la información y los bienes informáticos. El usuario o funcionario deberán reportar de forma inmediata al procesos de sistemas de información cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio. El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Cualquier persona que tenga acceso a las instalaciones de la ESE Hospital Rafael Paba Manjarrez, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente. Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán ser retirados de las instalaciones de la ESE Hospital Rafael Paba Manjarrez únicamente con la autorización de salida del área de Inventarios, anexando el comunicado de autorización del equipo debidamente firmado por el gestor de sistemas de información. Los Centros de Cómputo del Hospital Rafael Paba Manjarrez son áreas restringidas, por lo que solo el personal autorizado por la Oficina puede acceder a él.

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Oficina de sistemas de información, en caso de requerir este servicio deberá solicitarlo. El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el proceso de sistemas de información. El equipo de cómputo asignado, deberá ser para uso exclusivo para uso de las

Funciones netamente laborales. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos. Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU. Se debe mantener el equipo informático en un lugar limpio y sin humedad. El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar una reubicación de cables con el personal del proceso de sistemas de información. Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al proceso de sistemas de información a través de un plan detallado. Queda terminantemente prohibido que el usuario o funcionario distinto al personal de la sistemas abra o destape los equipos de cómputo. Únicamente el personal autorizado por el proceso de sistemas de información podrá llevar a cabo los servicios y reparaciones al equipo informático. Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

PÉRDIDA DE EQUIPO

El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo. El préstamo de laptops o portátiles tendrá que solicitarse a la Oficina de sistemas de información con el visto bueno del gerente de la Institución o su Jefe inmediato. El servidor o funcionario deberán dar aviso inmediato al proceso de sistemas de información, y a la Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

USO DE DISPOSITIVOS EXTRAÍBLES

El uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos para el manejo y traslado de información o realización de copias de seguridad o Backups deberá ser notificado al proceso de sistemas de información en caso que se trate de información sensible y/o datos de historias clínicas.
Cada gestor o Jefe de Área de la dependencia debe reportar al proceso de sistemas de información el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado con el fin de llevar el control de autorización para realizar dichas tareas de respaldo y/o extracción de información. El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

El funcionario que tengan asignados estos tipos de dispositivos será responsable del buen uso de ellos. Si algún proceso o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el proceso de sistemas de información con el respectivo visto bueno de la subgerencia administrativo y/o asistencial en su defecto de su Jefe inmediato o un superior de la Alta Dirección. Todo funcionario o servidor del Hospital Rafael Paba Manjarrez, deberá reportar a la Oficina el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

DAÑO DEL EQUIPO

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad. El cual será notificado

ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO

Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica del Hospital Rafael Paba Manjarrez. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet. Los usuarios y funcionarios del Hospital que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

El proceso de sistemas de información en cabeza del gestor de Sistemas, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas. Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar a la Sala donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el gestor del proceso y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la gerencia o subgerencia en su defecto, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario de la Oficina de procesos de sistemas de información. Todo equipo informático ingresado al Hospital deberá ser registrado en el libro de visitas o bitácora que maneje el área de vigilancia. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos o en su defecto se realizara en espacios no laborales para no interrumpir las actividades laborales. El gestor de sistemas de información deberá solicitar a la Alta Dirección los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS

Los usuarios de la ESE Hospital Rafael Paba Manjarrez deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial. Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC's) del Hospital Rafael Paba Manjarrez serán registradas y podrán ser objeto de auditoria.

ADQUISICIÓN DE SOFTWARE.

Los usuarios y funcionarios que requieran la instalación de software que no sea propiedad de la ESE Hospital Rafael Paba Manjarrez, deberán justificar su uso y solicitar su autorización por el proceso de sistemas de información con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado. Se considera una falta grave el que los

Usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Hospital Rafael Paba Manjarrez, que no esté autorizado por el proceso de sistemas de información. El proceso de sistemas de información, tiene a su cargo la tarea de informar periódicamente al hospital su política institucional contra la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Emails, Carteleras y Boletines.

El Grupo de Apoyo (Técnicos) de la Oficina de sistemas de información tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Institución. En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

Deben mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados. Cualquier otra petición de software deberá ser tramitada a través del proceso de sistemas de información. Finalmente se procede a actualizar el inventario de licencias de Software cuyo contrato tiene una vigencia anual.

IDENTIFICACIÓN DEL INCIDENTE

El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al proceso de sistemas de información lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las subgerencias administrativas y/o asistenciales, el usuario o funcionario deberá notificar al proceso de sistemas de información. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la ESE debe ser reportado al proceso de sistemas de información.

ADMINISTRACIÓN DE LA RED

Los usuarios de las áreas del Hospital Rafael Paba Manjarrez no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización del procesos de sistemas de información.

USO DEL CORREO ELECTRÓNICO

Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re-direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al de la ESE, a menos que cuente con la autorización del proceso de sistema de información. Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Hospital Rafael Paba Manjarrez. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades. Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico. Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

CONTROLES CONTRA VIRUS O SOFTWARE MALICIOSO

Para revisar si el antivirus se actualiza correctamente, seleccione el icono de su programa antivirus instalado que se encuentra en la barra de herramientas y presione el botón izquierdo del Mouse sobre este, luego en la opción Buscar actualizaciones, el proceso conectado a Internet realiza la actualización en forma automática. Puede que este proceso ponga un poco más lenta a la máquina, pero por ningún motivo interrumpa la actualización. Una vez terminada la actualización el programa le indicará que la base de firmas queda actualizada. En el caso de un equipo de cómputo sin conexión a Internet se haría el proceso de manera manual: Para ello nos ubicamos en un computador con conexión a Internet, repetimos los pasos anteriores para verificar la última actualización, y por medio de Memoria USB el técnico realizara la ejecución de actualización. Para prevenir infecciones por virus informático, los usuarios del Hospital Rafael Paba Manjarrez no deben hacer uso de software que no haya sido proporcionado y validado por el proceso de sistema de información. Los usuarios de la ESE deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el proceso de sistema de información. Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse. Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del proceso de sistemas de información. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al proceso de sistema de información para la revisión y erradicación del virus. El icono del antivirus debe permanecer siempre activo, si usted observa dicho icono inactivo, favor avisar inmediatamente a el proceso de sistemas de información, para que se haga la revisión correspondiente. Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el proceso de sistemas de información en: Antivirus, Outlook, office, Navegadores u otros programas.

CONTROLES PARA LA GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO (BACKUPS)

Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores. Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups. Ya que el software utilizado para las actividades diarias es directamente instalado por el proceso de sistemas de información, este será el único autorizado para la actualización de nuevos ejecutables y será quien revisara que la información que se tenía anteriormente quede almacenada en la maquina antes de la actualización realizada.

PLANES DE CONTINGENCIA ANTE DESASTRE

Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total. El proceso de sistema de información debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre. Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados. Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución. Existencia de documentación de los procedimientos manuales a seguir por los distintos procesos usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos. Existencia de documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros.

INTERNET

El acceso a Internet provisto a los usuarios y funcionarios de la ESE es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas. Usuarios de Internet del Hospital Rafael Paba Manjarrez tienen que reportar todos los incidentes de seguridad informática al proceso de sistemas de información inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática. Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

• Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas en la facturacion, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

•Saben que existe la prohibición de descarga de software sin la autorización del proceso de sistemas de información.

•La utilización de Internet es para el desempeño de sus funciones y cargo en Hospital y no para propósitos personales.

•Cada usuario y funcionario son responsables de la navegación a páginas de internet los cuales por medio de herramientas de filtrado de navegación podrán ser identificados por el " ID " entregado inicialmente por sistema

de información dentro de la red interna de información y a la infraestructura tecnológica del Hospital, por lo que se deberá mantener de forma confidencial.

INFORMACION SENSIBLE Y/O CONFIDENCIAL

Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el proceso de sistemas de información antes de poder usar la infraestructura tecnológica del Hospital Rafael Paba Manjarrez.Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Hospital, a menos que se tenga el visto bueno o la autorización de su Jefe inmediato. Cada usuario que acceda a la infraestructura tecnológica del Hospital debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios. Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

EQUIPO DESATENDIDO

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el proceso de sistemas de información cuando no se encuentren en su lugar de trabajo.

ADMINISTRACIÓN Y USO DE CONTRASEÑAS

La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al proceso de sistema de información para que se le proporcione una nueva contraseña. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizada puedan descubrirlos. Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

CONTROLES PARA OTORGAR, MODIFICAR Y RETIRAR ACCESOS A USUARIOS

Cualquier nuevo rol creado por el proceso de sistemas de información se deberá analizar y concertar con la gerencia.Todo usuario debe quedar registrado en la Base de Datos Usuarios y Roles. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro del sistema de la ESE Hospital Rafael Paba Manjarrez, deberá de venir acompañado del reporte debidamente firmado de lo contrario no se le dará trámite a dicho proceso.

REQUISICIÓN.

El proceso de sistemas de información, en cabeza del gestor o su delegado en caso de ausencia, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

CONTROL DE ACCESOS REMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del proceso de sistema de información.

DERECHOS DE PROPIEDAD INTELECTUAL

Los sistemas desarrollados por personal interno o externo que controle el proceso de sistemas de información son propiedad intelectual de la ESE.

CLÁUSULAS DE CUMPLIMIENTO

El proceso de sistemas de información realizará acciones de verificación del cumplimiento de Políticas de Seguridad Informática. El proceso de sistema de información podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal. Los jefes y responsables de los procesos establecidos en el Hospital deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

VIOLACIONES DE SEGURIDAD INFORMÁTICA

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el proceso de sistema de información. Ningún usuario o funcionario de la ESE debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el proceso de sistema de información. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Hospital.

EQUIPOS EN EL ÁREA ADMINISTRATIVA

El gestor deberá poner a disposición del proceso de sistemas de información, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de

soporte y mantenimiento. El proceso de sistema de información, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos. El proceso de sistemas de información, tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por la Alta dirección o el área usuaria de la licencia, para llevar el control de software instalado, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de los mismos. Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el gestor o Jefe del proceso solicitante, lo cuales serán evaluados por el Proceso de sistemas de información para su autorización e inclusión en el Plan Anual de Presupuesto correspondiente.

Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al proceso de sistemas de información el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.El proceso de sistemas de información deberá elaborar el pase de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico requiera ser trasladado fuera de las instalaciones del Hospital por motivo de garantía, reparación o evento.Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración del proceso de sistema de información para su autorización y visto bueno.

MANUAL DE ACCESO LÓGICO

Cada usuario se responsabilizará por el mecanismo de acceso lógico asignado, esto es su identificador de usuario y contraseña necesarios para acceder a la información e infraestructura de comunicación del Hospital es responsabilidad de cada usuario la confidencialidad de los mismos.

El acceso a la información que fluye dentro de la infraestructura tecnológica del Hospital se otorga en base a las funciones del usuario, se deberán otorgar los permisos mínimos necesarios para el desempeño del cargo o rol.

Todos los usuarios de equipos computacionales son responsables de la confidencialidad del identificador de usuario (ID) y el password o contraseña de su equipo, así como de aplicaciones especiales que requieran el mismo control de acceso lógico.

No está permitido a los usuarios proporcionar información a personal externo sobre los mecanismos de control de acceso a los recursos e infraestructura tecnológica de la Institución, salvo el caso de autorización expresa por la Dirección General de la entidad.

El identificador de usuario dentro de la red es único y personalizado, no está permitido el uso del mismo identificador de usuario por varios miembros del personal. El usuario es responsable de todas las actividades realizadas con su identificador de usuario, por tanto no debe divulgar ni permitir que terceros utilicen su identificador, al igual que está prohibido usar el identificador de usuario de otros.

FUNCIONES ESPECÍFICAS - MANUAL DE ROLES

Para todo el personal integrante del proceso de sistemas de información:

1. Coordinar con el Equipo de Apoyo del proceso de sistemas de información en la definición, factibilidad, especificación y validación de requerimientos.

2. Vigilar la correcta aplicación de los estándares y metodologías de desarrollo de sistemas de información, así como sugerir las mejoras que sean necesarias.

3. Revisar, aprobar y mantener actualizados los manuales de los sistemas, de operación y de usuario, concerniente a los sistemas de información y tecnologías (TIC'S).

4. Elaborar reportes de avance y estrategias de ejecución de los proyectos de desarrollo de sistemas de información.

5. Coordinar con el Equipo de Apoyo del proceso de sistemas de información en la definición, factibilidad, especificación y validación de requerimientos.

6. Vigilar la correcta aplicación de los estándares y metodologías de desarrollo de sistemas de información, así como sugerir las mejoras que sean necesarias.

7. Revisar, aprobar y mantener actualizados los manuales de los sistemas, de operación y de usuario, concerniente a los sistemas de información y tecnologías (TIC'S).

8. Desarrollar e implementar los sistemas de información que requieran las dependencias, de acuerdo a las prioridades establecidas en el plan de necesidades.

9. Efectuar el mantenimiento y actualización de los sistemas de información, analizando los problemas o planteamientos de modificación, garantizando su correcta sincronización.

10. Participar en los procesos de adquisición y pruebas de las soluciones informáticas de terceros. Asimismo, supervisar las actividades realizadas por terceros en el desarrollo e implementación de soluciones informáticas.

11. Apoyar en la capacitación al usuario final y al personal designado de la Sección Soporte a Usuarios, en el adecuado uso de los sistemas de información, proporcionando material de soporte y los medios necesarios para tales fines.

12. Administrar en forma eficiente los recursos asignados a la Oficina, así como el centro de cómputo, velando por la seguridad de accesos y operatividad, y protegiendo la información de ingreso, salida y almacenamiento.

13. Participar en la elaboración de la propuesta del Plan de Actividades de la Oficina, en los planes de contingencia y en la implementación de acciones que minimicen el riesgo de Tecnologías de Información.

14. Verificar que el personal del proceso de sistema de información atienda oportuna y eficientemente los requerimientos de las dependencias, supervisando el cumplimiento de las metodologías, estándares y/o técnicas implementadas en la Sección.

15. Cumplir y hacer cumplir las medidas correctivas recomendadas por los entes de vigilancia y control tanto externo como interno.

16. Atender asuntos relativos al servicio de soporte técnico de primer nivel para la solución de problemas referidos a hardware, Software, comunicaciones y servicios de computación personal, efectuados por el personal de la Oficina y por todas las dependencias institucionales.

17. Participar en los Procesos de Atención de los Problemas y Reclamos.

18. Atender consultas técnicas, operativas y funcionales a los usuarios, incentivándolos en el mejor uso y operación de las tecnologías de información.

19. Representar a la Institución ante los organismos competentes gubernamentales y no gubernamentales.

20. Ejecutar, instalar, configurar, y puesta en línea de los equipos de cómputo y periféricos en las oficinas Administrativas de la Sede Principal y Sedes alternas; cumpliendo con los procedimientos y estándares aprobados.

21. Instalar y diagnosticar los daños del cableado estructurado de la red de las oficinas Administrativas y Sedes alternas.

22. Coordinar y analizar las incidencias y magnitudes de un desastre, determinando prioridades de atención, disminuyendo el nivel de riesgos y traumatismos en la operación.

23. Determinar y gestionar de inmediato las actividades a realizar para generar una solución y puesta en marcha en el menor tiempo posible de todos los sistemas de información colapsados en el desastre.

24. Administración de Fallas (Fault Management): Encargada de detectar, registrar, aislar, notificar y corregir fallas en aquellos equipos que son parte de la red que presenten algún problema que afecte el buen funcionamiento de la red.

25.Administración de la Seguridad (Security Management): Controlar el acceso a los recursos de la red, de acuerdo a las políticas establecidas con el fin de evitar algún abuso y la perdida de la confidencialidad; entre las funciones está identificar los recursos sensibles y críticos de la red, monitorear los accesos.

5. ESTRATEGIA

Una vez publicada la política esta debe ser presentada a todos los funcionarios para evitar sanciones legales en el manejo de la información, la cual es netamente de la institución y por ningún motivo podrá ser tomada como personal. Esta política debe ser entregada a todos los funcionarios que ingresen y así acatar las normas que se contemplan en este documento.

6. LINEAS DE ACCION

Las líneas de acción se conciben como estrategias de orientación y organización de diferentes actividades relacionadas con un campo de acción, de tal forma que se pueda garantizar la integración, articulación y continuidad de información, de manera ordenada, coherente y sistemática. Esta forma de organización enfatiza en la interacción del debido manejo de herramientas y manejo de información. Lo anterior se lograra dando cumplimiento a los estándares y políticas antes mencionadas en este documento y haciendo el uso a partir de la instalación.

7. SEGUIMIENTO Y EVALUACIÓN DE LA POLITICA

El manejo de la información institucional deberá ser entregada una vez culmine su contrato o decida entregar su cargo y esta deberá ser verificada en el Hospital y su seguimiento deberá ser realizado por un ente interno de control quien será la encargada de notificar a gerencia de alguna anomalía encontrada.

a. Metas:

Dar a conocer herramientas el buen manejo del software y alcanzar un alto cumplimiento del manejo de seguridad de la información basados en leyes y reglamentos relacionados en el tema en seguridad de la informática.

Ser pionero en implementación de políticas institucionales en el sector salud

b. Indicadores

Verificación de cumplimiento basados en una escala del 100% en el cual se clasificara de la siguiente manera: 1 a 60% no cumple con estándares básicos de cumplimiento; 61 a 80 cumple con requerimientos básicos pero presenta fallas en la adherencia de la política; 81 a 100 cumple con los requerimientos mínimos leales en cuanto a cumplimiento de seguridad de la información y mínimos en protección físico y lógico.

c. Plan de acción anual

Verificar la adherencia después de publicada y aprobada la política, en los estándares mínimos de verificación expuestos en el documento actual.

5. **BIBLIOGRAFIA** https://www.google.com.co/ (definición de conceptos) consulta

http://www.iso.org/iso/home.html (definicion de norma ISO) consulta y copia de conceptos

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)

http://www.dian.gov.co/descargas/EscritosComunicados/2013/260_Comunicado_de_prensa_31122013.pdf

(Concepto basico de LEY 603 DE 2000)

http://www.mintic.gov.co/portal/604/w3-propertyname-510.html (normatividad (decreto, leyes, circulares y resoluciones))

TABLA DE CONTROL DE CAMBIOS

NO.	FECHA	CAMBIO	RESPONSABLE DEL CAMBIO