RESOLUCIÓN No. 189
(Rionegro, 14 de septiembre de 2018)

"POR MEDIO DE LA CUAL SE ADOPTAN LAS POLÍTICAS DE TECNOLOGÍA DE INFORMACIÓN PARA EL HOSPITAL SAN JUAN DE DIOS E.S.E RIONEGRO"

El Gerente del Hospital San Juan de Dios, Empresa Social del Estado de Rionegro, en uso de sus atribuciones legales y especialmente las conferidas en el artículo 315 Constitucional la Ley 909 de 2004, la Ley 1122 de 2007 y el artículo 91 de la ley 1551 de 2012.

CONSIDERANDO:

Que conforme a lo ordenado en la Ley 1341 de 2009 se hace necesario formular las políticas públicas que regirán las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente la cobertura, la calidad del servicio, el desarrollo de estas tecnologías y el uso eficiente de las redes y del espectro radioeléctrico.

Que la misma Ley 1341 de 2009 expresa que las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

Que el artículo 5° de la citada Ley establece que las entidades del orden nacional y territorial promoverán, coordinarán y ejecutarán planes, programas y proyectos tendientes a garantizar el acceso y uso de la población, de las empresas y las entidades públicas a las Tecnologías de la Información y las Comunicaciones

Que el Ministerio de Comunicaciones a través de su programa Agenda de Conectividad se encarga de impulsar el uso y masificación Tecnologías de la Información y las Comunicaciones (TIC) como herramienta dinamizadora del Desarrollo Social y económico del país.

Que la agenda de conectividad tiene como uno de sus lineamientos estratégicos modernizar la Administración Pública, mediante su estrategia de Gobierno en Línea, para el caso de la Entidades Territoriales, la Agenda de Conectividad ha diseñado el proyecto Gobierno en línea del Orden Territorial.

Que el Gobierno Nacional expidió el Decreto 1151 del 14 de abril de 2008, mediante el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, que son de obligatorio cumplimiento para las entidades que conforman la administración pública en Colombia.

Que, para dar cumplimiento a la normatividad vigente sobre la materia, se hace necesario adoptar las políticas de Tecnologías de la Información y las Comunicaciones para el Hospital San Juan de Dios E.S.E. Rionegro.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar las políticas de Tecnologías de la Información para el Hospital San Juan de Dios E.S.E. Rionegro, insertas en el documento anexo que hace parte integrante de la presente Resolución, para la producción, manejo, protección, intercambio y acceso a la información; integración a los sistemas de información y adopción de estándares en el manejo de tecnologías de información y comunicaciones.

ARTÍCULO SEGUNDO: La presente Resolución y sus anexos serán de obligatorio cumplimiento para todos los empleados del Hospital San Juan de Dios E.S.E. Rionegro.

ARTÍCULO TERCERO: Las políticas de información se regirán por el manual para la implementación del Gobierno en línea, expedido por el Ministerio de Comunicaciones, a través de la Agenda de Conectividad.

ARTÍCULO CUARTO: La presente Resolución y sus anexos podrán ser modificados a solicitud de la Gerencia del Hospital San Juan de Dios E.S.E. Rionegro, o por efecto de la entrada en vigencia de normas que obliguen a su modificación.

ARTÍCULO QUINTO: Teniendo en cuenta que el presente documento se elaboró en forma concertada, y en concordancia con la normatividad legal vigente, puede estar sujeto a modificaciones futuras debido al Mejoramiento Continuo de los procesos del Modelo Integrado de Planeación y Gestión.

ARTÍCULO SEXTO: La presente Resolución rige a partir de su expedición y deroga las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Rionegro, a los catorce (14) días del mes de septiembre de 2018.

LUIS MARÍA OTÁLVARO SÁNCHEZ
Gerente

POLÍTICAS DE TECNOLOGÍA DE INFORMACIÓN

INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado una gran relevancia, más aún con la intervención de herramientas de carácter globalizador como Internet y en particular el acceso a diversos contenidos de información en un sin número de sitios web en los que se puede navegar, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados, llevando a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades. De esta manera, la política de seguridad en informática del Hospital San Juan de Dios E.S.E. Rionegro emerge como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades. El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y mapa de procesos que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

GLOSARIO

Política: Describe la posición de la entidad sobre la seguridad informática; es decir toda persona que ingresa a la institución 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 el presente manual.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos, así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

Dominio: Sistema de denominación de hosts (estaciones de trabajo) en red, está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

Encriptar: Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Firewall: Un cortafuego es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Es un punto de red que actúa como entrada a otra red.

Hardware: Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

Malware: Cualquier programa cuyo objetivo sea causar daños a computadoras, sistemas o redes y, por extensión, a sus usuarios.

Servidor: Computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Software: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

OBJETIVOS

OBJETIVO GENERAL

Establecer los lineamientos y directrices generales de seguridad informática, relacionados con el uso de la plataforma tecnológica y la utilización de los servicios informáticos de la Entidad, que debe seguir todo el personal del Hospital San Juan de Dios E.S.E. Rionegro.

OBJETIVOS ESPECÍFICOS

- Definir un marco de referencia para direccionar el actuar del personal en el desarrollo de sus actividades, con miras a unificar la forma de realizar las tareas, propendiendo por el aumento de la productividad y la aplicación de las mejores prácticas de T.I.

- Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Hospital, para alcanzar la misión institucional.

- Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este documento y otras de carácter institucional, legal o emitido por otros órganos del Estado, que guarden relación con normativas aplicables a la materia.

- Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.

- Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.

- Definir las directrices a seguir de los planes de contingencia referente a los eventos adversos.

ALCANCE

Los lineamientos contenidos en el presente documento son de observancia obligatoria para todo el personal que labore en, o para, el Hospital, que por sus funciones tenga acceso a equipos de cómputo, sistemas y aplicaciones, bases de datos, instalaciones del centro de cómputo y en general, a todos los recursos informáticos de la organización.

Establecer un marco de gobierno para que el uso de las TIC de la institución, logre satisfacer las necesidades actuales y futuras derivadas de la estrategia de la Entidad, siguiendo los criterios de innovación, calidad, eficiencia, escalabilidad, y de arquitectura empresarial. Estas políticas son aplicables a todos los colaboradores, consultores, contratistas, terceras partes, que usen las tecnologías de información y la comunicación de la organización.

Supervisión de las políticas
La supervisión del cumplimiento de las "Políticas Generales sobre Tecnologías de Información", queda a cargo del Coordinador y personal de Sistemas; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

Violación a las políticas
La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado al Área de Sistemas correspondiente a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con Talento Humano. Este documento será revisado y/o actualizado por parte del Área de Sistemas, con la finalidad de estarlo mejorando. Estas modificaciones serán aprobadas y comunicadas a través del área de Calidad.

POLÍTICAS DE SEGURIDAD

Uso de computadores y portátiles

- Los computadores del Hospital San Juan de Dios E.S.E. Rionegro, no podrán ser utilizados para visualizar almacenar material no permitido y/o obsceno.

- Los usuarios son responsables de proteger sus contraseñas para poder ingresar a la red del Hospital, según los manuales aplicables de cada sede. Ningún usuario puede acceder a la red con la contraseña o cuenta de otro usuario, en caso de infringir deberá someterse a lo dispuesto en la ley 1341 de 2009 (Se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC).

- El Hospital San Juan de Dios E.S.E. Rionegro, no será responsable por las transacciones financieras electrónicas que realicen los empleados desde el computador asignado o desde cualquier computador que esté disponible para uso público y se encuentre en las instalaciones del Hospital.

- Ningún empleado o contratista del Hospital, o a quien le ha sido asignado un computador, podrá instalar software o hardware que no haya sido aprobado o adquirido por la entidad. Solamente el personal de sistemas o quién sea autorizado por el Área de Sistemas de Información, podrá realizar esta labor.

- El Hospital San Juan de Dios E.S.E. Rionegro, permitirá, en cierto límite, el almacenamiento de información personal en los discos duros de los computadores asignados a cada empleado o contratista, sin embargo, no será responsable de dicha información ni se ejecutarán esfuerzos tendientes a su recuperación.

Restricciones

- Intentar o realizar accesos a cuentas de usuario que no sean las propias (utilizando cualquier protocolo o programa, telnet, ftp (Protocolo de transferencia de archivos), etc.).

- Invadir la privacidad de los demás a través del computador asignado, así como intentar modificar o tener acceso a archivos, contraseñas o datos que pertenecen a otros.

- Utilizar los computadores de la Entidad para Introducir virus computacionales, malware, programas espías o cualquier otro programa diseñado para dañar el equipo o el software utilizado en el hospital o de cualquier manera, arriesgar la seguridad de las computadoras o el sistema de red de la Entidad.

- Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de los usuarios. Excepto cuando el Área de Sistemas para asegurar el correcto funcionamiento así lo requiera.

- Afectar o paralizar algún servicio por la ejecución intento de ejecución de programas indebidos.

- Modificar archivos que no sean propiedad del usuario, aunque se tengan permisos de escritura.

- Acceder, analizar o exportar archivos que sean accesibles a todo el mundo pero que no sean del usuario, salvo que se encuentre en una ubicación que admita su uso público.

- Cambiar la imagen institucional usada en los fondos de pantalla. Impresión de documentos personales en los recursos de la Empresa.

- Uso de los recursos tecnológicos de la empresa por familiares o amigos de los funcionarios, o por personal no autorizado.

Recomendaciones

- No se debe comer o colocar líquidos cerca del computador (CPU, teclado), se pueden producir choques eléctricos y por ende el daño irreparable del mismo.

- Siempre, al final de la jornada, se debe apagar el computador y/o el monitor.

- Se debe apagar el monitor, cuando el usuario se retire de su puesto de trabajo, por periodos de tiempo superiores a una hora.

- El usuario debe cambiar la contraseña regularmente o cuando considere que la misma pudo haber sido copiada.

- Reportar inmediatamente las anomalías detectadas Mantener depurado el correo institucional para evitar el riesgo de no recibir comunicación efectiva.
- La institución se enfocará en la implementación gradual, según la directiva presidencial 04 de abril 3 de 2012 de la política cero papel, a través de crear conciencia en los usuarios.

Consideraciones

- Reparación y mantenimiento de equipos: Los usuarios deben saber que el personal técnico tiene la autoridad para acceder a archivos individuales o datos cada vez que deba realizar un mantenimiento, sin embargo, el personal técnico del Área de Sistemas, no puede exceder su autoridad en ninguna de estas eventualidades, para usar esta información con propósitos diferentes a los de mantenimiento o reparación.

- Respuesta al uso indebido de computadores y sistemas de información: Cuando por alguna causa razonable determinada, se presuma el uso indebido de un computador o portátil, soportado en lo dispuesto en la ley 1341 de 2009, con autorización de la Gerencia el Área de Sistemas de la entidad puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a el(los) involucrado(s) en el incidente, para investigar y aplicar las sanciones a que hubiere lugar. Todos los empleados del Área de Sistemas y a quienes se designe, están en la obligación de monitorear constantemente los computadores y portátiles de la institución a través de los medios correspondientes, para responder oportunamente frente a cualquier acción que atente contra la disponibilidad, seguridad o desempeño correcto de los mismos.

Uso de Software

- Los recursos informáticos están disponibles para fortalecer el flujo de información interna y externa para lograr eficiencia operativa, por lo tanto, estos deberán ser utilizados en las actividades propias del cargo.

- El uso de cualquier tipo de software, es exclusivo para el tiempo en el cual el servidor o servidora forme parte del Hospital San Juan de Dios E.S.E. Rionegro, cuando se desvincule de la institución, se deberá desinstalar cualquier licencia de software que se encuentre en la computadora que él tenga asignada.

- El Hospital San Juan de Dios E.S.E. Rionegro, se reserva el derecho de retirar las licencias de software, en cualquier momento, a aquellos usuarios que hagan uso indebido del software, o que incumplan total o parcialmente estos términos de uso.

- Cualquier información o inquietud de los usuarios con relación a la copia o utilización de un software determinado, deberá solicitarse mediante la plataforma de soporte técnico que se encuentra en la intranet o a través de correo electrónico, enviado al líder de proyecto de soporte del Área de Sistemas de Información.

- Todos los desarrollos propios como: programas, archivos, entre otros y que sean creados en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentren almacenados en los equipos de cómputo, pertenecen al HSJD ESE Rionegro, deberán reportarse y entregarse al área de Sistemas para ser incluidos en el inventario de software de la institución.

- El usuario se obligará a respetar todos los derechos de la propiedad intelectual y a usar el software de forma diligente, correcta, lícita, y en particular, se comprometerá a abstenerse de:
    - Utilizar el software con fines contrarios a la ley y a lo establecido por el Hospital.
    - Copiar, modificar, reproducir o utilizar el software propiedad del Hospital San Juan de Dios E.S.E. Rionegro con fines de lucro.

Asignación cuentas de usuario en los Software de la empresa

Según manual de procesos de informática que se encuentran en la intranet, en los casos que no aplique se procederá de la siguiente manera:

- ✓ La asignación de usuario y contraseña en los diferentes Software de la institución, es única e intransferible, todo lo que se haga con su usuario será responsabilidad del funcionario

- ✓ Una vez asignada la cuenta y la contraseña, la asignación de los permisos a este usuario deberá ser solicitada a los líderes funcionales que se encargan de administrar las autorizaciones de ingreso a los diferentes módulos.

- ✓ Cada usuario que haga uso de los diferentes Software de la institución, deberá tener definido un rol específico según su cargo y perfil profesional y/o funcional

- ✓ Antes de asignar usuario y contraseña a los diferentes funcionarios de la empresa estos deben estar en la base de datos con la información personal requerida por la oficina de Talento Humano.

- ✓ Las claves para el acceso a los aplicativos de reportes a entes de control, deberán ser entregados y custodiados por el área de sistemas.

Seguridad del Hardware

1. Los computadores del hospital son instalados por el Área de sistemas de acuerdo a los requerimientos de las normas para cableado ANSI/TIA-1179ª y en la parte eléctrica se siguen las recomendaciones del código eléctrico colombiano RETIE, garantizando un ambiente seguro, alejados de zonas de humedad y en ubicaciones que cuentan con las instalaciones eléctricas y de red de datos adecuadas.

2. Los equipos de cómputo son para el desarrollo de las actividades institucionales no para otros fines y es responsabilidad del jefe de área o coordinador de servicio velar por su correcto uso.

3. No puede modificarse la ubicación, ni la configuración del hardware y software instalado en los equipos de cómputo por parte de los usuarios sin el acompañamiento del área de sistemas; se ha configurado en el dominio de la red políticas que restringen a los usuarios la modificación de la configuración de los equipos.

4. Se realiza mantenimiento preventivo del 100% de los equipos, de acuerdo al Cronograma de mantenimiento y limpieza de equipos de cómputo, garantizando un mantenimiento anual. Los equipos de cómputo y los servidores del Hospital, cuentan con un circuito de energía regulado con una UPS de 70 KVA y en la sede Gilberto Mejía Mejía 20 KVA.

5. Cualquier falla en los computadores, impresoras o la red de datos debe reportarse inmediatamente al área de sistemas y no tratar de manipular los equipos, ya que podría causar problemas como pérdida de la información o daño del equipo. El área de sistemas registra la solicitud en el reporte de tickets, clasifica la prioridad del evento y asigna un responsable para solucionarlo (Plataforma de soporte técnico que se encuentra en la intranet, reporte de tickets).

6. Todos los equipos de cómputo y equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir el robo. Para ello el hospital protege contra robo los equipos portátiles y algunos de escritorio que se

encuentran en zonas expuesta mediante un sistema de guayas de seguridad con clave y con llaves, Los demás equipos están ubicados en áreas con restricción de acceso físico a personal no autorizado y es responsabilidad del jefe de área velar por su seguridad.

7. Los equipos de cómputo y de red de se encuentran marcados y relacionados en un inventario detallando sus componentes principales como: marca, serial, garantía, ubicación, dirección IP. Los registros de inventario se mantienen actualizados, registrando las novedades de ingresos de equipos nuevos o bajos de inventario cuando se presentan. (Archivo Inventario de equipos).

8. La pérdida o robo de cualquier componente de hardware debe ser reportada inmediatamente al jefe del área, quien informa a la administración para iniciar la investigación respectiva y la afectación de pólizas para la reposición de equipos. El área de sistemas evaluara la alternativa para dar continuidad a los requerimientos del área afectada.

Acceso físico y lógico

1. Antes de conectar equipos de cómputo o algún dispositivo a la red de datos del hospital, el personal de sistemas debe cumplir con el plan de instalación diseñado (archivo procedimiento de instalación de equipos).

2. El hospital tiene implementado el sistema de acceso remoto para funcionarios autorizados y terceros a través de una VPN (Red privada virtual), la cual es validada por las políticas de acceso implementadas en el firewall, lo que garantiza un nivel de seguridad contra acceso no autorizado desde el exterior. (Documento Definición de Políticas Firewall).

3. Todo el intercambio de información desde la institución hacia redes externas o internet y viceversa son validadas por un conjunto de políticas firewall (documento definición de políticas firewall, documentación fortinet).

4. Los aplicativos del sistema Servinte Clinical Suite Enterprise y CNT de la E.S.E. Rionegro y módulos administrativos cuentan con un módulo de administración de privilegios los cuales delimitan la acción de los usuarios en los módulos del sistema. El perfil de los usuarios debe ser definido por los jefes de cada área y ser solicitados a sistemas para la creación y configuración de los usuarios, a través de la plataforma de soporte técnico que se encuentra en la intranet o a través de correo electrónico. (Documento Roles, perfiles y privilegios, Definición de Nombres de Usuario).

5. Cuando los usuarios dejen sus puestos de trabajo deben cerrar la aplicación y la sesión de trabajo, para evitar accesos no autorizados a datos o recursos compartidos del sistema.

6. Los equipos de terceros que ingresan a la institución y deseen tener acceso a recursos como internet, deben solicitar al área de sistemas la configuración para acceso a la red, este acceso se direcciona de acuerdo a las políticas definidas por el área de Sistemas para separar su tráfico de los datos de nuestros equipos y servidores, el usuario asignado al equipo es validado por las políticas del fortinet.

7. Todos los equipos propiedad del hospital como computadores de escritorio, equipos portátiles, impresoras y equipos relacionados con sistemas de información no deben retirarse de las instalaciones físicas por ninguna persona a menos que esté previamente autorizado por escrito bajo la responsabilidad del área de sistemas.

8. Los usuarios del sistema de información no pueden extraer información institucional para usos diferentes a los laborales y siempre deberá estar disponible para la institución cuando se requiera independientemente de la presencia del empleado en la misma.

9. Todos los equipos cuentan con protección de antivirus la cual es actualizada en forma centralizada y automática. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de Sistemas. Los equipos de terceros que usan la red de datos de la E.S.E deben contar con un sistema de antivirus actualizado que será validado previamente por el área de sistemas.

10. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de Sistemas.

11. Todo dispositivo de almacenamiento externo, memorias USB, CD, DVD, debe ser vacunado antes de abrir sus contenidos.

Seguridad del Software y datos

1. Todo el software del hospital está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales. Todos los

originales de instalación deben permanecer bajo seguridad de acceso físico, junto con las claves de instalación y actas de licencias en el área de sistemas y es responsabilidad del jefe del área velar por su correcto uso. Se debe realizar una copia de los medios de instalación y con ellos se realizará la instalación en los equipos, nunca con el original. Esta copia se encuentra en el área de sistemas y es material de trabajo de los auxiliares de sistemas.

Protección contra desastres

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre (cortos circuitos, vandalismo, fuego y otras amenazas, etc.) podrá afectar el nivel de servicio y la imagen del hospital, se debe prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

Planes de emergencia, contingencia y recuperación

El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento que se requiera permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos en un tiempo razonable para cada caso, y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

El mantenimiento del plan de Contingencias y Recuperación General incluye entre otros un proceso estándar que integra los planes de contingencia para computadoras y comunicaciones, así como también el inventario de hardware, software existente y los procesos que corren manualmente mientras dure la contingencia

Indicadores y modalidad de monitoreo

El monitoreo y seguimiento se deberá realizar de manera coordinada con los responsables del área de sistemas o quien haga sus veces, de conformidad con lo establecido en la ley 1341 de 2009 (Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC).

En cuanto a la periodicidad del seguimiento y funcionamiento de la política de seguridad de la información de acuerdo a los procedimientos implementados en el Hospital San Juan de Dios, Ese Rionegro, se realizarán auditorias con personal interno de la institución para la verificación y cumplimiento de objetivos, controles y procedimientos de seguridad de la Información. La Gerencia, Jefes de Oficina, Coordinadores de Área, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad. El Hospital San Juan de Dios, Ese Rionegro asigna un funcionario para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la institución.

El seguimiento se realizará anualmente a la política de seguridad, con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

Bibliografía

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental".