
PLAN DE
DESARROLLO
2020 - 2024
Plan Estratégico Tecnologías
de la Información y las
Comunicaciones – PETIC
2021
E.S.E HOSPITAL
MARINILLA
¡EL HOSPITAL DE LA GENTE!
hospitalmarinilla
www.hospitalmarinilla.com

PROPOSITO

El plan Estratégico de Tecnología de la Información – PETIC, de nuestra organización permite tener una concepción amplia para manejar el cambio siendo partícipes activos de él, teniendo en cuenta las tendencias tecnológicas del mercado, la infraestructura actual de la organización; permitiendo generar ventajas competitivas, para el mejoramiento de la gestión y el aumento de la productividad.

El Plan Estratégico de Tecnologías de Información - PETIC, tiene como propósito establecer una guía de acción para la administración de las tecnologías de la información y comunicación (TIC), y debe estar alineado a los objetivos corporativos, estrategias y posiciones claras de la empresa en las tres dimensiones de mayor impacto (Recurso Humano, Tecnología y Procesos)

El Plan estratégico de tecnologías de información de la E.S.E Hospital San Juan de Dios de Marinilla, está en línea con el Plan de Desarrollo Institucional del Hospital y con este documento pretendemos definir acciones para realizar a corto y mediano plazo que permitan el crecimiento y la evolución del Hospital en el desarrollo de las TICs.

OBJETIVOS

El Plan Estratégico de Sistemas de Información -PETIC- de la ESE Hospital San Juan de Dios de Marinilla tiene los siguientes objetivos.

GENERAL

El presente plan tiene como objetivo principal alinear e integrar los sistemas de información (SI) y las tecnologías de la información y comunicaciones (TICS) existentes en la organización; evaluando la forma de como beneficiarse de las tecnologías, garantizando la mejora de los servicios; permitiendo que los recursos de tecnología se administren de la mejor manera para que eficiente y efectivamente se cumplan las metas propuestas en los servicios de la Institución.

ESPECIFICOS

- Desarrollar lineamientos para orientar el crecimiento, mantenimiento y fortalecimiento de las TI del hospital.
- Apoyar la toma de decisiones estratégicas y operativas, basadas en datos e información oportuna y confiable.
- Mejorar la seguridad de la información.
- Agilizar los procesos y procedimientos internos del hospital mediante el uso efectivo de las tecnologías de la información.
- Optimizar la facilidad de acceso y respaldo de la información.
- Implementar el programa de seguridad de la información.
- Realizar análisis de riesgos e implementar las medidas correspondientes.

ALCANCE

Este documento describe las estrategias que el Hospital aplicará para los procesos y proyectos, permitiendo el crecimiento y evolución en el desarrollo de los recursos de tecnologías de información y comunicación (TICs) en la institución. Al desarrollar e implementar este PETIC en el hospital, se podrán apropiar y usar eficientemente las tecnologías de información, generando ventajas relacionas con los siguientes aspectos:

Información rápida.
Atención oportuna.
Entrega oportuna de información.
Tecnología actualizada.

JUSTIFICACION

Este documento busca establecer una guía de acción clara y precisa que sirva de base para tomar mejores decisiones buscando el mejor aprovechamiento de la tecnología y el uso óptimo de los recursos de TICs, para apoyar el plan de desarrollo del hospital, mediante la apropiación de los lineamientos, estrategias y proyectos definidos, que garanticen el apoyo al cumplimiento de sus objetivos y funciones, aprovechando de manera efectiva la infraestructura de la entidad. Finalmente, la misión del PETIC es convertirse en la carta de navegación para el futuro desarrollo y modernización tecnológica de la ESE Hospital San Juan de Dios de Marinilla.

NORMATIVIDAD VIGENTE

Decreto 1151 de Abril de 2008 y Manual para la Implementación de la Estrategia de Gobierno en Línea. Por medio del cual se establecen los lineamientos generales de la estrategia de gobierno en línea de la República de Colombia. Se reglamenta parcialmente la Ley 962 de 2005 y se dicta otras disposiciones.

Ley 872 de 2003. Con esta Ley se ordena la creación del Sistema de Gestión de Calidad (SGC) en las instituciones del Estado, como una herramienta para la gestión sistemática y transparente, que permita dirigir y evaluar el desempeño institucional en términos de calidad y satisfacción social con la prestación de los servicios, enmarcada en los planes estratégicos y de desarrollo que el sector Estatal debe cumplir para ejercer su función social.

Decreto 2693 de 2012. Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 61 de la constitución Política de 1991. El Estado protegerá la propiedad intelectual por el tiempo y formalidades que establezcan a Ley.

Ley 1341 de Julio de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y organización de las tecnologías de la información y comunicaciones.

Decreto 235 de Enero de 2010. Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Ley 1438 de 2011. Por medio del cual se reforma el sistema general de Seguridad Social en Salud y se dictan otras disposiciones. Parágrafo “transitorio” del Artículo 112 “La historia clínica única electrónica será de obligatoria aplicación antes del 31 de Diciembre de 2013.

Ley 594 de 2004. Por medio de la cual se dictan la Ley General de Archivo y se dictan otras disposiciones.

NTC-ISO/IEC 27002. Establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información.

NTC-ISO/IEC 27001. Señala los requerimientos del Sistema de Gestión de Seguridad de la Información.

PLATAFORMA ESTRATEGICA DE LA E.S.E

MISION

Somos una IPS de primer nivel de atención prestadora de servicios de salud, humanizados, en condiciones de seguridad, oportunidad, centrados en el usuario y la familia que buscamos permanecer en el mercado, auto sostenernos y responder a las necesidades de los usuarios mediante la optimización de los recursos, con un talento humano idóneo, competente, con infraestructura y tecnología adecuada, disponible; lo hacemos posible trabajando en equipo, con sentido de pertenencia, compromiso y calidad para la generación de una cultura de autocuidado, e impacto positivo en el perfil epidemiológico de la comunidad".

VISION

En el 2021 seremos referente en el sector como una IPS que presta servicios con calidad, humanizados y en condiciones de seguridad, con un talento humano fortalecido, competente y comprometido, con infraestructura y tecnología adecuada, financieramente sostenible, orientada al mejoramiento continuo, que promueve estilos de vida saludable, bajo un modelo de atención integral al alcance de todos que contribuya al bienestar, la satisfacción de los clientes, usuarios y sus familias.

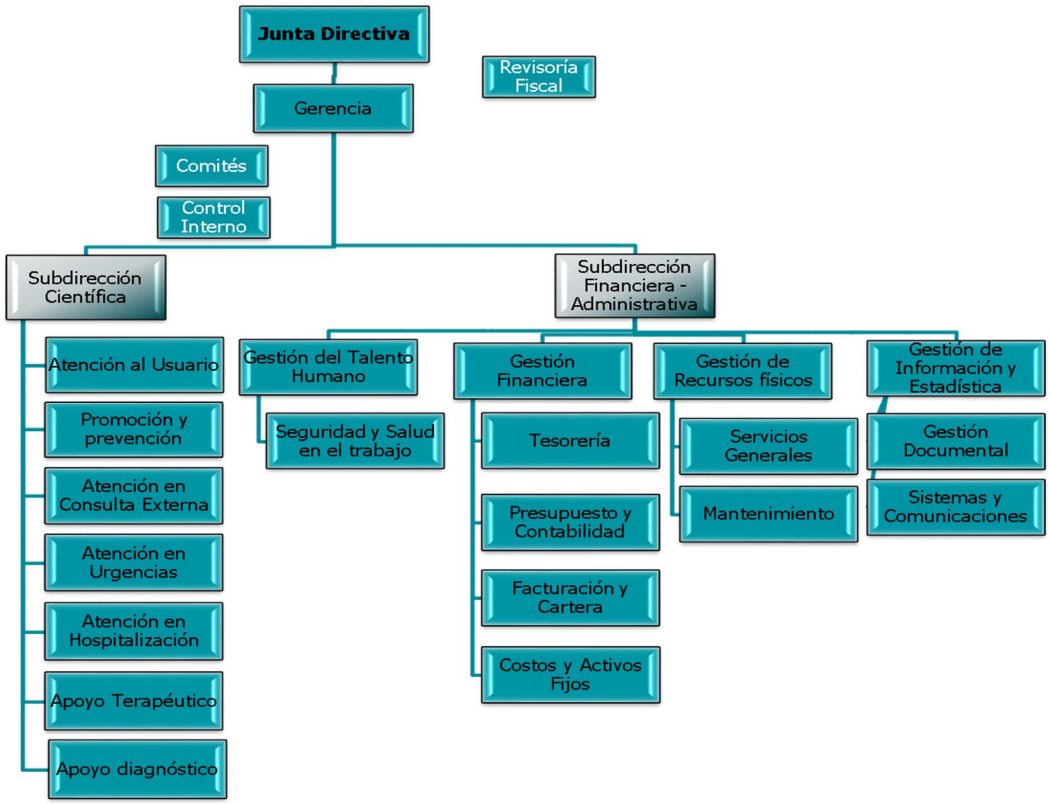
VALORES

- Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.
- Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.
- Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
- Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.
- Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.
- Transparencia: Siendo creíbles, inspirando confianza, siendo capaces de explicar claramente el porqué de nuestro actuar, Dónde no tiene oportunidad la mentira ni personal ni institucional.

PRINCIPIOS

- Calidad: Haciendo las cosas bien desde el principio, para el caso nuestro brindar la atención que nos solicitan con amabilidad, respeto, oportunidad, aplicando los conocimientos técnicos y/o profesionales, además de los que nos provee la experiencia en forma óptima, proyectando una excelente imagen personal e institucional, pensando siempre que el usuario que tenemos al frente podría ser la persona más querida para nosotros y nos agradaría que saliera de nuestra empresa totalmente satisfecho.
- Compromiso: Es aquel que generamos cuando tenemos un alto sentido de pertenencia. Nos implica velar por la satisfacción de cada uno de los usuarios internos y externos, desde nuestro quehacer o fuera de él, con el aporte que cada uno puede brindar para generar una excelente atención, va más allá del "Hacer lo que me toca". Incluimos el cumplimiento de los deberes como funcionarios y como miembros de una sociedad con nuestro entorno.
- Solidaridad: Siendo sensibles frente a la situación de los que nos rodean, con responsabilidad, trabajando unidos por superar las dificultades, en procura de metas comunes, Dónde todos nos beneficiamos, superando los individualismos y/o intereses particulares, dentro de las posibilidades empresariales.

ESTRUCTURA ORGANICA



PLATAFORMA ESTRETIGA DEL AREA GESTION DE INFORMACION

MISION

La misión del área Gestión de Información de la ESE Hospital San Juan de Dios de Marinilla, es la de apoyar la buena prestación de los servicios, planear, desarrollar, implantar y mantener los Servicios de Tecnologías de Información en los niveles operativo, administrativo y estratégico, dentro de los criterios de adecuación tecnológica que sirvan de apoyo al crecimiento, organización y proyección de la institución.

VISION

En el año 2022 la plataforma, los procesos y procedimientos de la ESE Hospital San Juan de Dios de Marinilla, estarán a la vanguardia, actualizados, estables y confiables en todo lo referente a las TICs, permitiendo a todos los actores la integración de procesos, la disminución de trámites y la disposición de toda la información de manera unificada, permitiendo al hospital ser referente en la región.

ESTRATEGIAS

La estrategia busca que la ESE Hospital San Juan de Dios de Marinilla

- Cumpla con las metas de Plan de desarrollo.
- Garantizar un buen servicio a los ciudadanos y servidores públicos.
- Optimización de los procesos de la entidad.
- Aprovechamiento de los recursos tecnológicos en forma eficiente y eficaz.
- Apoyo en la toma de decisiones.
- Promover el uso y apropiación de los recursos tecnológicos.
- Garantizar la seguridad y privacidad de la información
- Promover la cultura informática en el Hospital
- Identificar los Activos de Información con el fin de fortalecer la integración de sistemas y bases de datos del Hospital, para tener como meta final, un Sistema Integral de Información.

POLITICAS INFORMATICAS

En el área de Gestión de Información de la ESE Hospital San Juan de Dios de Marinilla, se establecen las siguientes políticas en cuanto a relación de cada usuario, equipos y seguridad de la información.

ADMINISTRACION Y SUMINISTRO DE INFORMACION INSTITUCIONAL

- Quienes laboran en el Hospital son responsables de velar por la integridad, veracidad, seguridad, confidencialidad y disponibilidad de la información.
- Quienes laboran en el Hospital deben vigilar que la información sea, generada, operada, modificada, almacenada, conservada, accedida, divulgada o destruida, de acuerdo con las normas y reglamentos de la Empresa.

- La información confidencial ha de emplearse de manera acorde con su naturaleza y carácter; en consecuencia, quienes laboran en el Hospital, no podrán utilizarla para beneficio propio o de terceros.
- Quienes laboran en el Hospital evitarán cualquier tipo de comunicación informal que afecte a la Institución o a la dignidad de las personas.
- La custodia de la información de los usuarios es responsabilidad de quienes laboran en el Hospital en general.
- Quienes laboran en el Hospital deben emplear la información que conozcan en ejercicio de sus cargos, funciones o responsabilidades, exclusivamente para usos relacionados directamente con el cumplimiento de esas funciones, excepto cuando requiera ser suministrada a los entes gubernamentales de control y a las instancias que legalmente tengan derecho siempre y cuando busquen acceder a ella a través de los conductos regulares.
- Con excepción de la Gerencia, quienes laboran en el Hospital no podrán hacer cualquier tipo de comentario o revelar información a los medios de comunicación como prensa, radio, televisión o cualquier otro medio masivo de comunicación, a menos que exista autorización previa y escrita de la misma Gerencia.

POLÍTICA DE SEGURIDAD DE LA INFORMACION

REGULACION

Las políticas contenidas en este documento deberán ser conocidas, aceptadas y cumplidas por todos los colaboradores de la ESE Hospital San Juan de Dios de Marinilla. El incumplimiento de las mismas se considerará un incidente de seguridad que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios de acuerdo al manual y/o política de confidencialidad de la E.S.E.

POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACION

El uso aceptable de los activos informáticos de la E.S.E, implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estándares establecidos para garantizar la seguridad informática y el buen uso de los mismos, así como de los compromisos y responsabilidades adquiridas.

Los siguientes se consideran actos de obligatorio cumplimiento para el uso de los activos informáticos y están expresamente prohibidos así:

Políticas de Seguridad:

- Conocer y aplicar las políticas y procedimientos apropiados con relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial del Hospital a personas no autorizadas.

- No permitir y no facilitar el uso de los sistemas informáticos del Hospital a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, servidores) para otras actividades que no estén directamente relacionadas con el trabajo.
- Proteger meticulosamente su contraseña, por ningún motivo revelársela a nadie y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta (mínimo 8 dígitos) y que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos d del Hospital y en tal sentido deben usarse en las horas no laborables.
- Está prohibido el intento o el hecho de agregar, remover o modificar información identificadora o de contenido en la red, que engañe o confunda al sistema o al usuario destinatario o suplante a otro usuario utilizando su información identificadora.
- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.
- Los equipos del Hospital sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas.
- No se permite fumar, comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos del medioambiente (polvo, incendio, agua, etc.).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- No pueden moverse los equipos o reubicarlos sin permiso. Para cambiar de lugar y/o llevar un equipo fuera de alguna sede del Hospital, se requiere del Área de sistemas.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente a la administración o Directivos del Hospital.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar. Ejemplo: un mensaje de correo electrónico cuyo objetivo es transmitir o comunicar información confidencial.
- No se debe llevar al sitio de trabajo computadores portátiles (Laptops, NoteBooks, tablet) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Hospital está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (CD, USB, etc.), el software o los datos residentes en las computadoras del Hospital, sin la aprobación previa.
- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Área de Sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.

- Para prevenir demandas legales o la introducción de virus informáticos, no debe instalarse software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución freeware o shareware, a menos que haya sido previamente aprobado por el Área de Sistemas.
- No deben usarse usb u otros medios de almacenamiento en cualquier computadora a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial del Hospital.
- La información almacenada en los puestos de trabajo por cada usuario es responsabilidad de cada uno, de esta información no se genera copia de seguridad.
- Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden Público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en Internet, y el respeto por los derechos de terceras personas.

Políticas de Contraseñas y el control de acceso:

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas del Hospital, pudiendo ser causal incluso de despido.

Políticas para uso de Cuentas usuarios:

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse una cuenta a personas que no sean empleados del Hospital a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que la Gerencia determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- Cuando un empleado es despedido o renuncia al Hospital, debe desactivarse sus cuentas (Sistema de información CNT, chat interno, turneros) antes de firmar el paz y salvo de retiro.

REVISION INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACION

El área de Sistemas será responsable de garantizar que se realicen revisiones periódicas al Sistema de Gestión de Seguridad de la Información, para verificar su vigencia, su correcto funcionamiento y su efectividad.

GESTION DE ACTIVOS DE INFORMACION

INVENTARIO DE ACTIVOS DE INFORMACION

El responsable de Activos Fijos, mantendrá un inventario actualizado de los activos informáticos, donde se registrarán y controlarán, desde su ingreso a la institución hasta el momento que se requiera prescindir de los mismos.

USO ADECUADO DE LOS ACTIVOS Y RECURSOS DE INFORMACION

Toda la información de la ESE, será procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se garanticen los criterios de confidencialidad, integridad y disponibilidad.

USO DE INTERNET

Dado que Internet es una herramienta de trabajo que ofrece múltiples sitios y páginas Web para investigar y aprender, y que además permite navegar en muchos otros sitios no relacionados con las actividades propias de la E.S.E, se controlará, verificará y monitoreará el uso adecuado este recurso, considerando para todos los casos las restricciones definidas en las siguientes políticas:

- No se permitirá el acceso a páginas relacionadas con pornografía, música, videos, concursos, entre otros.
- No se permitirá la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
- No se permitirá el intercambio no autorizado de información de propiedad de la E.S.E de sus usuarios y/o de sus funcionarios, con terceros.
- Cada uno de los funcionarios será responsable de dar un uso adecuado de este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

CORREO ELECTRONICO

La ESE Hospital San Juan de Dios asignará una cuenta de correo electrónico institucional como herramienta de trabajo para cada una de las áreas o dependencias, la cual será usada para el desempeño de las funciones asignadas.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la ESE Hospital San Juan de Dios de Marinilla.

SEGURIDAD DE LOS EQUIPOS

La infraestructura de procesamiento de información (equipos de hardware, software, elementos de red y comunicaciones, instalaciones físicas) deberá contar con las medidas de protección eléctricas y de comunicaciones para evitar daños a la información procesada. Se deberán instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Los dispositivos y mecanismos de protección estarán alineados con los resultados del análisis de riesgos. Así mismo, se protegerá la disponibilidad e integridad de la infraestructura de procesamiento de información mediante acciones de mantenimiento y soporte.

ELIMINACION Y/O REUTILIZACION SEGURA DE EQUIPOS

Cuando un equipo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información de la organización que allí se encuentre almacenada. Luego el equipo deberá ser sometido a un proceso de eliminación segura de la información sensible almacenada y del software instalado, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

ADMINISTRACION DE OPERACIONES Y COMUNICACIONES

PROCEDIMIENTOS Y RESPONSABILIDADES

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados (reportes-hoja de vida), con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica Cada procedimiento tendrá un responsable para su definición y mantenimiento.

PROTECCIÓN CONTRA CODIGO MALICIOSO

La infraestructura de procesamiento de información contará con sistema de detección de intrusos, sistema anti-spam y sistemas de control de navegación (UTM), con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de la ESE Hospital San Juan de Dios.

COPIAS DE RESPALDO

La información contenida en los servidores se respaldará de forma periódica y automática, es decir se harán copia de respaldo y backup de información y se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

Para garantizar que la información de los usuarios sea respaldada, es responsabilidad de cada uno mantener copia de la información de su estación de trabajo en medio externo.

CONTROLES DE RED

Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos de acuerdo a los resultados del análisis de riesgos sobre los activos de información. El acceso remoto a la red de datos se permitirá para acceder a recursos de la ESE, pero únicamente a los funcionarios o terceros autorizados.

CONTROL DE ACCESO

POLÍTICA DE CONTROL DE ACCESO

Los sistemas de información de la ESE, contarán con mecanismos de identificación de usuarios y procedimientos para la autenticación y el control de acceso a los mismos.

El acceso a los activos de información estará permitido únicamente a los usuarios autorizados, por esta razón, todo funcionario tendrá asignado un identificador único de usuario, el cual deberá utilizar durante el proceso de autenticación, previo al acceso de los activos de información autorizados según su perfil (Rol).

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la Infraestructura de Procesamiento, sea por Internet, o por otro medio, siempre estará autenticado.

ADMINISTRACION DE CONTRASEÑAS DE USUARIOS

Los usuarios deberán seguir las siguientes políticas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados.

- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- Las contraseñas no se deberán escribir en ningún medio, excepto cuando son entregadas en custodia de acuerdo al procedimiento.
- Reportar cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.
- Las contraseñas se deberán cambiar según los requerimientos de la infraestructura de procesamiento de información.

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Los usuarios deberán bloquear su estación cada vez que se retiren de su sitio de trabajo y sólo se podrán desbloquear con la contraseña del usuario. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo. Los usuarios deberán retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. Así mismo, no se deberá reutilizar papel que contenga información confidencial.

INVENTARIO DE EQUIPOS INFORMATICOS Y SISTEMAS OPERATIVOS

La ESE Hospital San Juan de Dios cuenta con una cantidad suficiente de equipos informáticos, los cuales cubren cada una de las necesidades en las diferentes dependencias de la empresa, estos son utilizados para llevar a cabo todos los procesos de manera más organizada y a la vez se logra tener toda la información sistematizada. Para esto se tendrá hoja de vida de cada computador donde se registra las especificaciones técnicas, sistema operativo, software instalado, fechas de los mantenimientos realizados, cambio de piezas.

PLANES DE CONTINGENCIA

El Plan de contingencia informática de la ESE Hospital San Juan de Dios de Marinilla, lleva plasmado un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance del presente Plan guarda la relación con la infraestructura informática, así como los procedimientos relevantes asociados con la plataforma tecnológica.

Este Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, y así establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

OBJETIVO DEL PLAN DE CONTINGENCIA

Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

- Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones de la entidad.
- Proteger la propiedad de la entidad y otros activos.
- Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o posibles fallas ocasionadas.
- Proteger al sistema de información de pérdidas irreparables de información procesada.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y/o infraestructura informática.
- Alcanzar una alta disponibilidad, es decir, impedir que se produzcan fallas en los sistemas, que dificulten el normal funcionamiento de nuestra Institución.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información y/o infraestructura informática.

CULTURA INFORMÁTICA

Con el fin de crear una Cultura Informática al interior del Hospital, se desarrollaran campañas de divulgación y motivación para que los funcionarios actúen con sentido de pertenencia y se logre un aprovechamiento de los recursos tecnológicos.

Políticas Generales sobre Cultura Informática

El Hospital adoptará las políticas de seguridad informática y las pondrá en práctica a través de procesos de socialización a todos los funcionarios de la Institución.

Para lograr una efectividad en la seguridad de información, es necesario contar con el esfuerzo de equipo, se requiere la participación de forma activa, de cualquier funcionario que tenga interacción con la información o los sistemas de información del Hospital. Todos los funcionarios de la entidad, deben cumplir con las Políticas de Seguridad de Información y más que eso, desempeñar un papel proactivo para su protección y divulgación de estas políticas.

Los usuarios son responsables de familiarizarse y cumplir con las políticas de seguridad de información, las dudas que puedan surgir alrededor de éstas deben ser consultadas con el Profesional de Sistemas del Hospital. En forma periódica el área de Sistemas del Hospital, debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad.