INTRODUCCION

El plan Estratégico de Tecnología de la Información en una Organización es tener una concepción amplia para manejar el cambio y ser partícipes activos de él, teniendo en cuenta las tendencias tecnológicas del mercado, todos los posibles usos de la tecnología informática, la Infraestructura actual de la organización, generándole ventajas competitivas, para el mejoramiento de la gestión y el aumento de la productividad.

Por lo tanto, es importante desarrollar e implementar dentro de la institución el Plan Estratégico de Tecnologías de Información - PETI, en donde debe estar alineado a los objetivos corporativos, con estrategias y posiciones claras de la empresa en las tres dimensiones de mayor impacto (Recurso Humano, Tecnología y Procesos), manteniéndonos preparados a las cambiantes necesidades del entorno en todo lo relacionado a lo comercial, financiero, legislativo y otros factores que amenacen la continuidad permanente y/o obstaculicen el mejoramiento continuo de la empresa.

El Plan estratégico de TI tecnología de información de la ESE, esta alienado con el plan de desarrollo 2020 – 2024.

OBJETIVOS

El Plan Estratégico de Sistemas de Información (PETI) de la ESE Hospital San Roque tiene los siguientes objetivos.

GENERAL

El presente Plan tiene como objetivo principal Alinear e integrar los sistemas de información (SI) y la tecnología de información y comunicaciones (TICS) con la plataforma estratégica y contribuir a disminuir la brecha digital y garantizar 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

- Mejorar la infraestructura Tecnológica y Comunicaciones para el Procesamiento de la información.
- Mejorar la Seguridad de la información.
- Apoyar la toma de decisiones estratégicas y operativas, basadas siempre en datos e información oportuna, pertinente y de calidad
- Automatizar los procesos y procedimientos internos de la entidad contando con las condiciones de infraestructura y servicios tecnológicos requeridos.
- Mantener la tecnología de los canales de comunicación en buenas condiciones.
- Mantener el Hardware en funcionamiento.
- Mantener la conectividad de Internet que se ajuste a las necesidades del hospital en el municipio y en el corregimiento de Mesopotamia.
- Velar porque el software y hardware del Hospital este actualizado y funcionando.
- Implementar el programa de seguridad de la información.
- Realizar análisis de riesgos e implementar las medidas correspondientes.
- Mantener en los procesos de manipulación, captura, control y monitoreo de la información.
- Optimizar la facilidad de acceso y respaldo de la información.

ALCANCE

El presente Plan Estratégico aplica para todos los procesos y proyectos que contribuyen al desarrollo de los recursos de tecnologías de información y comunicación en la Institución. Al desarrollar e implementar este PETI en la entidad, se podrán apropiar y usar eficientemente las tecnologías de información, generando ventajas relacionas con los siguientes aspectos:
Información rápida.
Atención oportuna.
Comunicación asertiva.
Entrega oportuna de información.

JUSTIFICACION

Este documento busca establecer una guía de acción clara y precisa para la administración de las tecnologías de información y comunicaciones, mediante la formulación de estrategias y proyectos que garanticen el apoyo al cumplimiento de sus objetivos y funciones, en línea con el Plan de gestión Institucional de la ESE.

PROPOSITO

El Plan Estratégico de los Sistemas de Información (PETI), tiene como propósito la revisión del estado actual de las Tecnologías de Información y Comunicaciones TIC'S de la ESE Hospital San Roque de La Unión.

DIRECCIONAMIENTO ESTRATEGICO

LINEA ESTRATEGICA

Nos permite evaluar la forma como aprovechamos la tecnología, evaluar las mejores prácticas de las diferentes dependencias (Implementar las formas genéricas del aprendizaje organizacional) y realizar una evaluación.

Es un plan adicional que apoya al hospital en el cumplimiento de sus objetivos estratégicos, sus metas y por tanto hace parte como elemento activo de la plataforma estratégica, permitiendo ponerla en práctica.

NORMATIVIDAD VIGENTE

Decreto 1151 de 04 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.

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.

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 del 30 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

La Empresa Social del Estado Hospital San Roque, brinda servicios de salud de baja complejidad; satisfaciendo las necesidades de la población usuaria, en una infraestructura segura y confortable, con talento humano cálido e idóneo, orientado por los principios organizacionales de compromiso, oportunidad, accesibilidad, cumplimiento, transparencia, competitividad y calidad

VISION

Para el año 2024 seremos la mejor institución prestadora de servicios de salud de baja complejidad del Municipio, a partir del mejoramiento continuo, el funcionamiento de la nueva sede, adquisición de nuevas tecnologías y el reconocimiento de nuestros usuarios por el compromiso e idoneidad del talento humano y la satisfacción de las necesidades en salud de la comunidad.

ESTRATEGIA

Mejorar el sistema de información de la E.S.E.

OBJETIVO ESTRATEGICO

Contar con información oportuna y precisa de todas las áreas de la E.S.E.

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 E.S.E. 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:
El intento o violación de los controles de seguridad establecidos para la protección de los activos informáticos.
El uso sin autorización de los activos informáticos.
El uso no autorizado o impropio de la conexión al sistema.
Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.
El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.
Está prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios.
Está prohibido el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.
El hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos.
Está prohibido retirar de las instalaciones de la E.S.E o áreas bajo su administración o control, cualquier activo informático sin autorización previa.
El Servicio de Internet debe ser utilizado solamente con fines laborales. Se prohíbe toda transmisión de material obsceno o pornográfico, difamatorio, o que constituya una amenaza.
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.
Está prohibido el almacenamiento y reproducción de aplicaciones, programas o archivos de audio o vídeo que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.

El usuario está de acuerdo en aceptar responsabilidad por todas las actividades a realizar con los activos informáticos bajo su responsabilidad y custodia o desde las cuentas asignadas para su acceso a los servicios informáticos.
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.

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 área Administrativa e inventarios, 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, siguiendo el procedimiento "*Inventario y clasificación de activos*".

USO ADECUADO DE LOS ACTIVOS Y RECURSOS DE INFORMACION

Toda la información de la E.S.E, 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 Roque 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 E.S.E.

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 alienados 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, 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 E.S.E.

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 E.S.E, pero únicamente a los funcionarios o terceros autorizados.

CONTROL DE ACCESO

POLÍTICA DE CONTROL DE ACCESO

Los sistemas de información de la E.S.E, 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 E.S.E Hospital San Roque 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.

RED DE COMUNICACIONES

El hospital cuenta con una red tipo estrella, con un centro de datos que se reparte a todas las áreas mediante un canal dedicado para acceso a Internet, el cual es propiedad de la Institución. La señal se reparte a las distintas oficinas mediante cable estructurado tipo 6A, por enlaces de swich punto punto y multipunto mediante canal dedicado. Se cuenta con los elementos necesarios para su conectividad como son Servidores, Swichs, Cableado entre otros.

PLANES DE CONTINGENCIA

El Plan de contingencia informática de la E.S.E. Hospital San Roque, 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.