

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – PETIC

ÁREA DE SISTEMAS
E.S.E HOSPITAL SAN RAFAEL

2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	3
3. ALCANCE DEL DOCUMENTO.....	4
4. MARCO NORMATIVO	4
5. RUPTURAS ESTRATÉGICAS	7
6. ANÁLISIS DE LA SITUACIÓN ACTUAL	8
SISTEMAS DE INFORMACIÓN	8
7. POLÍTICAS DE USO DE LOS RECURSOS TECNOLÓGICOS.....	9
8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	10
SISTEMAS DE INFORMACIÓN	11
9. RESPONSABILIDADES DEL TRABAJADOR	13
10. MANTENIMIENTO Y BUEN USO DE LA INFRAESTRUCTURA	14
11. PLAN DE MANTENIMIENTOS	15
CRONOGRAMA DE MANTENIMIENTOS	15
SEGUIMIENTO Y MONITOREO:	15
RIESGOS:	16
12. PROCEDIMIENTO SEGURIDAD DE LA RED INALÁMBRICA:	22
13. ADMINISTRACIÓN DE LA RED	23
14. SEGURIDAD PARA LA RED	23
<i>Redes de datos cableada e inalámbrica</i>	23
15. SEGURIDAD SISTEMA OPERATIVO	23
<i>ANTIVIRUS</i>	23
<i>ENTRADA AL SISTEMA WINDOWS</i>	23
16. SEGURIDAD DEL SISTEMA DE INFORMACIÓN.....	24
17. USO DEL INTERNET.....	24
18. PLAN DE ADQUISICIONES	25
19. PLAN DE COMUNICACIONES DEL PETI.....	25

1. INTRODUCCIÓN

El Plan Estratégico de Tecnología de la E.S.E Hospital San Rafael de Fundación, surge a partir de la voluntad institucional de disminuir la brecha digital y garantizar el pleno ejercicio de los derechos a la información y a las comunicaciones, propiciando la mejora continua en la gestión institucional, basándose para ello en la aplicación de estándares y las mejores prácticas en la implantación de sistemas informáticos. El Plan se enmarca en una serie de acciones encaminadas a optimizar los resultados que son producto de la gestión que el Hospital ha ido promoviendo en los últimos años.

Como consecuencia del avance vertiginoso que han tenido las Tecnologías de la información durante los últimos años, la Entidad, se ha preocupado de potenciar el que hacer administrativo a través de la incorporación de estas tecnologías en sus procesos estratégicos, misionales y de apoyo.

En el buen desarrollo de las estrategias TI y Marcos de referencia de arquitectura empresarial para la gestión de TI en empresas públicas, complementado con la Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI que regula el Ministerio de las Tecnologías de la Información y las comunicaciones, se elabora este documento como propuesta para plan estratégico de las tecnologías de la información y comunicación para el E.S.E HOSPITAL SAN RAFAEL DE FUNDACION en búsqueda de definir lineamientos a seguir en materia de las TI y herramienta que impulsen las metas de la Entidad.

2. OBJETIVOS

Implementar un Gobierno de TI en el E.S.E HOSPITAL SAN RAFAEL DE FUNDACION a través del cual se dirige y controle el uso de las TI.

Fortalecer la gestión del área de Sistemas en la prestación de servicios y soporte tecnológico para cumplir con los objetivos estratégicos de la Entidad.

Optimizar la infraestructura de redes y trato de datos para mejorar los servicios de comunicación de la Entidad.

Mejorar la gestión de la seguridad de la información con base a los modelos normativos que regulan actualmente.

3. ALCANCE DEL DOCUMENTO

El plan estratégico de tecnologías de la información y las comunicaciones – PETI tiene como finalidad apoyar a la alta gerencia a cumplir con sus objetivos estratégicos, dar cubrimiento a todos los dominios del Marco de Referencia de AE, presentar mecanismos que se deben cumplir para proteger las Tecnologías de la Información y comunicación con que cuenta la Entidad para el año en curso.

4. MARCO NORMATIVO

Decreto Nacional 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Concordancias; Decreto 1078 del 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" De acuerdo con su Título I – Objeto, ámbito de aplicación, definiciones, principios y fundamentos. "(...) Artículo 1°. Objeto. Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad. (...) Contando con este objeto la Administración Central debe desarrollar un marco de referencia sobre la Arquitectura Empresarial para así gestionar y promover la armonización de procesos y procedimientos en aras de cumplir con los marcos estratégicos nacionales que aplican para los órdenes territoriales, el presente decreto da la siguiente definición sobre este marco; Artículo 3°. Definiciones. Para la interpretación del presente decreto, las expresiones aquí utilizadas deben ser entendidas con el significado que a continuación se indica: "(...) Marco de Referencia de Arquitectura Empresarial para

la gestión de Tecnologías de la Información: Es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de las arquitecturas empresariales, tanto sectoriales como institucionales. El marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información. (...) Contando con este marco para la estructuración del Plan Estratégico de las Tecnologías de la Información y las Comunicaciones el Decreto 2573 de 2014 en su Título II – Componentes, Instrumentos y Responsables que enfatiza sobre los fundamentos principales para desarrollar de manera correcta implementación de la Estrategia de Gobierno en línea, se debe cumplir con los siguientes componentes; Plan Estratégico de Tecnologías de la Información -PETI Página 6 de 58 “(...) Artículo 5°. Componentes. Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea. 1. TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo. 2. TIC para el Gobierno abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones. 3. TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno. 4. Seguridad y privacidad de la Información. Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Parágrafo 1°. TIC para el gobierno abierto comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto, pero no los cubre en su totalidad. Artículo 6°.

Instrumentos. Los instrumentos para la implementación de Plan Estratégico de Tecnologías de la Información -PETI 2016 -2019 Página 7 de 58 "(...) Artículo 9°. Medición y monitoreo. El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno en Línea y de la Dirección de Estándares y Arquitectura de Tecnologías de la Información, diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el Manual de Gobierno en Línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que les sea requerida. Artículo 10. Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos: En conclusión en de vital importancia el cumplimiento del presente decreto por ser el mapa de ruta que las entidades territoriales deben promover en sus administraciones para así aplicar de manera correcta la estrategia nacional de Gobierno en línea, apoyando a la creación de un Estado más eficiente, más transparente y más participativo gracias a las TIC, prestando los mejores servicios en línea al ciudadano, logrando la excelencia en la gestión, empoderando y generando confianza en los ciudadanos e impulsando y facilitando las acciones requeridas para avanzar en los Objetivos de Desarrollo Sostenible -ODS, facilitando el goce efectivo de derechos a través del uso de TIC. Como complemento del Decreto Nacional 2573 de 2014, encontramos el dominio Estrategia TI que tiene como fin apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales, su implementación cuenta con 4 ámbitos de aplicación que servirán como insumo para el correcto formulación, seguimiento y evaluación del Plan Estratégico de las Tecnologías de la Información y las Comunicaciones adoptado por la entidad; Decreto 415 del 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones." En su Artículo 2.2.35.3. Numeral 1 se establece los objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: 1. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la

definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y Plan Estratégico de Tecnologías de la Información -PETI 2016 -2019 Página 8 de 58 servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado. Como conclusión la entidad deberá definir el fortalecimiento institucional a través del uso de las tecnologías de la información y las comunicaciones definiendo mecanismos de implementación y ejecución valederos para las capacidades internas y externas que la entidad contenga para la mejora continua de la prestación del servicio, esto a través de una alta difusión por medios electrónicos con campañas de divulgación de la implementación y la alineación que esta tendrá con el modelo integrado de gestión de la administración mejorando el funcionamiento de los procesos y procedimientos e impulsando la eficacia, la eficiencia y la efectividad a través del ejercicio del principio de transparencia.

5. RUPTURAS ESTRATÉGICAS

Identificando los paradigmas a romper de la Entidad con el fin de realizar una transformación en la gestión de los recursos de TI. Se identifican las siguientes actividades para lograr resultados de impacto:

- Las tecnologías deben ser consideradas de gran importancia para el buen funcionamiento de los servicios de la institución.
- La tecnología debe ser considerada un factor de valor estratégico para la institución pública.
- Necesidad de liderazgo al interior de la institución pública para la gestión de Sistemas de Información, se debe de Contar con una oficina de TI, que haga parte del comité directivo, que gerencia las actividades, los recursos y que se enfoque hacia un servicio de la mejor calidad posible, para los clientes internos y externos.

- Los proyectos de TI son costosos y no siempre es claro su retorno de inversión.
- Hay una amplia brecha entre los directivos y el personal de TI.
- Resolver el dilema entre “desarrollar en casa” vs. “Comprar software comercial”.
- Alinear las soluciones con los procesos, aprovechando las oportunidades de la tecnología, según el costo/beneficio.

6. ANÁLISIS DE LA SITUACIÓN ACTUAL

Este apartado comprende un diagnóstico en cada uno de los dominios del marco de referencia de arquitectura TI, con el fin de determinar el nivel de madurez tecnológico que comprende la entidad en relación con las dimensiones del modelo del marco de referencia, calificando dicho estado de madurez en un rango de alto medio o bajo.

La determinación de los grados de madurez y las deficiencias encontradas establecerán las acciones que se llevarán a cabo para contar con un grado de madurez alto, al finalizar la implementación del modelo y de los proyectos resultantes.

Sistemas de información

Para apoyar los procesos misionales en la organización, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones en todos los aspectos; que garanticen la calidad de la información, dispongan recursos de consulta a los públicos de interés, permitan la generación de transacciones desde los procesos que generan la información siendo fáciles de mantener.

En el Catálogo de Servicios y Catálogo de Software se centralizan todos los servicios ofrecidos por el área de TI, los cuales deben ser conocidos por el personal del proceso, así como por el personal de la organización, con el fin de asegurar el buen entendimiento de dichos servicios.

Entre los Sistemas de Información y Aplicaciones que utiliza el E.S.E. Hospital San Rafael de Fundación se encuentran:

SALUD SYSTEM: Es un software (HIS – Hospital Información System) para la gestión asistencial (Historia Clínica Electrónica), administrativa (facturación, inventarios, caja, citas) y financiera (presupuestos, contabilidad, RIP cxc) de Instituciones Prestadoras de Servicios de Salud.

7. POLÍTICAS DE USO DE LOS RECURSOS TECNOLÓGICOS

Se detallan las políticas para el uso de los recursos tecnológicos de la Entidad:

- Los usuarios no harán parte de los grupos de administrador (ni de server ni locales).
- Se solicitará cambio de contraseñas a los usuarios cada 90 días.
- Se Implementarán cierres automáticos de sesiones abiertas que tengan inactividad de más de 20 minutos, con reinicio de sesión protegido con la contraseña del usuario autenticado.
- Se mantendrán activas las actualizaciones automáticas para poder recibir los parches de seguridad automáticamente cada que estén disponibles.
- El navegador estará configurado para que borre regularmente las cookies.
- Durante los mantenimientos se hará borrado de archivos temporales del sistema operativo y temporales de Internet, descargas e historial de navegación.
- Se implementarán nuevas políticas de navegación con perfiles restringidos, para la activación de permisos especiales se debe hacer el requerimiento a través de la gerencia general.
- Se hará una restricción de funcionalidades de los puertos de acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).
- Se replanteará el acceso a carpetas o recursos compartidos en la red local de acuerdo con las áreas y los diferentes perfiles.
- Se restringe el acceso de los dispositivos móviles a la red corporativa.
- No se proporcionará ningún tipo de acceso a terceros a la red corporativa.
- Restringir el acceso a los usuarios durante sus períodos de vacaciones o

- licencias y darlos de baja en casos de traslado o retiros.
- Llevar un adecuado control en usuarios y perfiles, estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).
 - Cumplir con todas las disposiciones determinadas en el manual.

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Se mantienen las siguientes políticas de seguridad de la información.

- Mantener una infraestructura tecnológica, soportada en plataformas apropiadas, protegiendo los mecanismos de tratamiento, almacenamiento y comunicación de la información.
- Contar con personal competente y comprometido con una cultura de seguridad de la información, generada a través de capacitaciones periódicas al personal, garantizando la aceptación y aplicación de las directrices establecidas.

Así mismo garantiza que:

- La información que se administra internamente, es utilizada con fines empresariales; Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función empresarial; La información digital o digitalizada correspondiente al sistema de información Contable, de Cartera, Facturación e Inventarios y Gestión Humana, las bases de datos de los correos electrónicos corporativos y los archivos ofimáticos de la empresa cuentan con copias de respaldo para garantizar su seguridad.
- Los lugares donde se encuentran ubicados los activos asociados al sistema de procesamiento de la información se consideran áreas de acceso restringido, por tal motivo el ingreso y permanencia a estas áreas es controlado y supervisado por el departamento de sistemas.
- El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la empresa está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre

en cualquiera de las siguientes conductas:

Sistemas de información.

La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Entidad a través del área de sistemas.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios son realizados únicamente por el área de Sistemas.

El área de Sistemas de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios.

Los funcionarios serán conectados a la red de la Entidad con previa solicitud escrita y autorizada por el Líder del área. Los terceros y/o contratistas se conectarán a la red de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, bajo los lineamientos del área de Sistemas, asegurando la legalidad del equipo a través de certificados emitidos por la empresa contratista, de acuerdo con lo definido por el área de sistemas.

Los usuarios que requieren acceder a la infraestructura tecnológica de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas.

Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo con lo definido por el área de sistemas.

La sincronización de dispositivos móviles, tales como smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Entidad, debe ser autorizado de forma explícita por el líder de la dependencia respectiva, en conjunto con el apoyo del área de Sistemas de la Entidad.

Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar, grabar música y/o el uso de redes sociales.

Ningún funcionario contratista o tercero podrá copiar para uso personal archivos o programas de propios del Hospital. A través de las políticas de control de acceso físico y lógico definidas por la Institución, se controla el acceso a cada uno de los ambientes. Adicionalmente, los ambientes de desarrollo, pruebas y producción están totalmente separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

El área de Sistemas debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados.

Igualmente debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

El área de Sistemas debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION.

9. RESPONSABILIDADES DEL TRABAJADOR

Se detallan las responsabilidades que recaerán sobre el trabajador:

- Suministrar la información a quien no tiene derecho a conocerla.
- Usar la información con el fin de obtener beneficio propio o de terceros.
- Ocultar la información maliciosamente causando cualquier perjuicio.
- Hacer pública la información sin la debida autorización.
- Hurtar software de propiedad de, o licenciado a nombre del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, [copia o reproducción entre usuarios finales].
- Realizar copias no autorizadas de software de propiedad o licenciado a nombre del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, dentro y fuera de sus instalaciones.
- Falsificar y duplicar formatos o productos informáticos de propiedad del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION.
- Descargar software, a través de Internet sin la debida autorización.
- Intentar modificar, reubicar o sustraer equipos de cómputo o periféricos, software y/o información sin la debida autorización.
- Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Utilizar la infraestructura tecnológica del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, [computadores, software, información o redes] para acceder a recursos externos con propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Aduñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
- Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Lanzar cualquier tipo de virus, gusano, troyano o programa de computador cuya intención sea hostil o destructiva. Véase DOCUMENTO PROTECCIÓN CONTRA SOFTWARE MALICIOSOS.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un recurso del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION.

- Descargar o reproducir material multimedia [imágenes, audio, video y animaciones] sin la autorización del Coordinador del área de Informática.
- Uso personal de cualquier recurso informático del E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material pornográfico.
- Violar cualquier Ley o Regulación nacional respecto al uso de sistemas de información.
- Los activos de hardware que hayan sido asignados a un usuario para ser utilizados como herramientas en la ejecución de sus funciones laborales y/o contractuales, serán devueltos, luego de la culminación de estas.
- Se prohíbe la tenencia o ingesta de alimentos y/o bebidas en los puestos de trabajo, al igual que el fumar cerca de equipos de cómputo, equipos de red y/o equipos de protección eléctrica.
- No se apilan documentos sobre los equipos de cómputo, dispositivos electrónicos como impresoras, faxes, escáneres y/o dispositivos de regulación eléctrica, como tampoco se obstruyen las rejillas de ventilación de estos equipos para evitar la generación y/o propagación de incendios.
- Se prohíbe la utilización de medios personales de almacenamiento de información como memorias USB, discos duros externos, CDs y disquetes, entre otros, en los equipos de cómputo de la empresa.

10. MANTENIMIENTO Y BUEN USO DE LA INFRAESTRUCTURA

Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.

Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.

Una vez al año se realizará una revisión en la red para detectar desperfectos y dar así mantenimiento.

Periódicamente, por espacio de 4 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas. Previo a

una programación el usuario deberá entregar el equipo para su limpieza en el horario programado.

Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoría interna.

La desobediencia de cualquiera de estas normas será considerada como grave incumplimiento laboral.

11. PLAN DE MANTENIMIENTOS

Para la realización del plan de mantenimiento de los servicios tecnológicos de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION, se tuvo en cuenta la guía de servicios tecnológicos del Marco de Referencia de Arquitectura Empresarial de MinTIC. Los tipos de mantenimiento que se brinda desde el Área de Sistemas son los siguientes:

Cronograma de Mantenimientos

En los anexos se encuentra el cronograma general de mantenimientos preventivos para los servicios tecnológicos de la E.S.E. HOSPITAL SAN RAFAEL DE FUNDACIÓN en la vigencia 2023.

Seguimiento y Monitoreo:

El cronograma de mantenimientos se ejecutará en el lugar de trabajo, y se acordará con el usuario la realización de este, para no afectar las actividades diarias de los usuarios.

El técnico reportara al coordinador de infraestructura el respectivo informe correspondiente al mantenimiento, para después realizar acciones que permitan mejorar y el plan de acción correspondiente.

Riesgos:

Algunos de los riesgos que se pueden presentar en la ejecución del plan de mantenimientos son:

- Falta de herramientas como repuestos para cambio durante el mantenimiento.
- Disponibilidad de recursos humanos para la realización del mantenimiento.
- Incumplimiento en los tiempos de respuesta.
- Sucesos imprevistos ajenos a la Entidad (Por ejemplo: problemas del servicio de energía).
- Reporte a destiempo de las fallas por parte de los usuarios.

PROGRAMACIÓN DE MANTENIMIENTO PREVENTIVO

No. ROTULO	MARCA Y MODELO	SERIAL	AREA	Fecha Programada	Fecha Programada	Fecha Programada	Observaciones
0675	HP ALL IN ONE 20-c200-LA	8CC8380KJ4	ADMISION URGENCIAS	1/04/2023	1/08/2023	1/12/2023	
0736	HP ALL IN ONE C0391A	8CC0121JS1	ADMISION URGENCIAS	1/04/2023	1/08/2023	1/12/2023	
0008	HP ALL IN ONE 20-C218LA	8CC8080LZD	ALMACEN	1/04/2023	1/08/2023	1/12/2023	
0684	HP ALL IN ONE 20-c200-LA	8CC8301781	AUDITORIA	1/04/2023	1/08/2023	1/12/2023	
1248	HP ALL IN ONE C0391A	8CC0114C00	AUDITORIA	1/04/2023	1/08/2023	1/12/2023	
1251	HP ALL IN ONE C0391A	8CC0121JHQ	AUDITORIA	1/04/2023	1/08/2023	1/12/2023	
1262	HP ALL IN ONE C0391A	8CC0114BY7	AUDITORIA	1/04/2023	1/08/2023	1/12/2023	
1255	HP ALL IN ONE C0391A	8CC0121J53	AUDITORIA	1/04/2023	1/08/2023	1/12/2023	
0587	HP ALL IN ONE 20-c200 LA	8CC8380KMF	AUTORIZACIÓN	2/04/2023	2/08/2023	2/12/2023	
0585	HP ALL IN ONE 20-C215LA	8CC84700H1J	AUTORIZACIÓN	2/04/2023	2/08/2023	2/12/2023	
0567	HP ALL IN ONE 20-C218LA	8CC8080LYW	CAJA VENTANILLA	2/04/2023	2/08/2023	2/12/2023	
0572	HP ALL IN ONE 20-c200 LA	8CC7660FYY	CALL CENTER	2/04/2023	2/08/2023	2/12/2023	
1382	TORRE DELL VOSTRO 3681	BM2TB93	CALL CENTER	2/04/2023	2/08/2023	2/12/2023	
1177	MICRO TORRE HG00941	00138967	CALL CENTER	2/04/2023	2/08/2023	2/12/2023	
1194	HP PRO ONE 20-c200la	8CC8380KJ2	CARTERA	2/04/2023	2/08/2023	2/12/2023	
0683	HP ALL IN ONE 20-c200-LA	8CC830175Y	CARTERA	2/04/2023	2/08/2023	2/12/2023	
1200	LENOVO ALL IN ONE	YJ00B0LU	CARTERA	2/04/2023	2/08/2023	2/12/2023	
1195	HP ALL IN ONE C0391A	8CC8301754	CARTERA	2/04/2023	2/08/2023	2/12/2023	

0667	HP ALL IN ONE 20-C217LA	8CC8220QT6	CONSULTA EXTERNA MESÓN	4/04/2023	3/08/2023	3/12/2023	
0184	COMPAQ ALL IN ONE 18	5CM2500KMX	CONSULTA EXTERNA MESÓN	4/04/2023	3/08/2023	3/12/2023	
0324	HP ALL IN ONE C0391A	8CC0121JRS	CONSULTA GINECOLOGIA	4/04/2023	3/08/2023	3/12/2023	
0974	HP ALL IN ONE 20-C200la	8CC8380KDS	CONSULTORIO URGENCIAS	4/04/2023	3/08/2023	3/12/2023	
0633	HP PRO ONE 400 G4 20.0	8CC89430BFG	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
0373	HP PRO ONE 400 G4 20.0	8CC9430BMW	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
1197	HP ALL IN ONE C0391A	8CC0121JPR	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
0374	HP ALL IN ONE C0391A	8CC0121JQ1	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
0244	TORRE HP 260-A 100B LA	CNV7240SZN	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
0132	HP ALL IN ONE 20-c200-LA	8CC83017RZ	CONTABILIDAD	4/04/2023	3/08/2023	3/12/2023	
0198	LENOVO ALL IN ONE F0BB00ALLX	MP10UY06	CONTRATACIÓN	4/04/2023	3/08/2023	3/12/2023	
0103	HP ALL IN ONE C0391A	8CC02133Z3	CONTRATACIÓN	4/04/2023	3/08/2023	3/12/2023	
0098	HP ALL IN ONE C0391A	8CC0121IJC	CONTRATACIÓN	4/04/2023	3/08/2023	3/12/2023	
0090	HP PRO ALL IN ONE 400 G4	8CG9430BF7	CONTRATACIÓN	4/04/2023	3/08/2023	3/12/2023	
1076	TORRE DELL VOSTRO 3681	CM2TB93	CONTRATACIÓN	4/04/2023	3/08/2023	3/12/2023	
0348	HP 3000 SFF	MXL0460CZZ	CONTROL INTERNO	5/04/2023	4/08/2023	5/12/2023	
0342	HP ALL IN ONE C0391A	8CC0121JS6	CONTROL INTERNO	5/04/2023	4/08/2023	5/12/2023	
0078	HP ALL IN ONE C0391A	8CC0121IJM	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
1181	MICRO TORRE HG00941	00139204	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
1187	MICRO TORRE HG00941	00139205	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
1344	TORRE DELL VOSTRO 3681	9M2TB93	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
N/A	HP ALL IN ONE 20R5155LA	3CR62204MB	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
0076	HP PRO ALL IN ONE 400 G4	8CG9430BMT	COOR. MEDICA	5/04/2023	4/08/2023	5/12/2023	
0175	MICRO TORRE HG00941	00139206	COORDINACIÓN DE ENFERMERÍA	5/04/2023	4/08/2023	5/12/2023	
0066	LENOVO 9486 A15	LKLHVPR	ESTADISTICAS	5/04/2023	4/08/2023	5/12/2023	
0290	HP ALL IN ONE C0391A	8CC80121JS5	ESTADISTICAS	5/04/2023	4/08/2023	5/12/2023	
1206	HP ALL IN ONE 20-C217la	8CC9295MFN	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	

Calle 16 N° 53 - 46 Salida a Valledupar
 Teléfono: 4140124
 Código Postal: 472020

📍 ESE Hospital San Rafael Fundación
 📱 @EESANRAFAEL
 🌐 esehospitalsanrafael



0141	HP ALL IN ONE 20-c200-LA	8CC8080LVW	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1218	LENOVO ALL IN ONE PO-CL	Y100BOX6	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
0727	COMPAQ ALL IN ONE 18	5CM2500KXV	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1028	HP PRO ONE 400 G4 20.0	8CG9430BF5	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
0127	COMPAQ ALL IN ONE 18-2001 LA	5CM2500KXG	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
0275	MICRO TORRE HG00941	00139203	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1215	HP ALL IN ONE C0391A	8CC0114C1R	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1054	TORRE DELL VOSTRO 3681	3N2TB93	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
0136	HP ALL IN ONE C0391A	8CC0114C0Z	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1091	TORRE DELL VOSTRO 3681	892KF73	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1210	HP ALL IN ONE C0391A	8CC0121JRQ	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1058	TORRE DELL VOSTRO 3681	2N2TB93	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
1225	HP ALL IN ONE C0391A	8CC0114C21	FAC. CASA ADMINISTRATIVA	6/04/2023	5/08/2023	6/12/2023	
0556	HP ALL IN ONE 20-C217la	8CC9071X2H	FAC. CONSULTA EXTERNA	6/04/2023	5/08/2023	6/12/2023	
0554	HP ALL IN ONE C0391A	8CC0114C39	FAC. CONSULTA EXTERNA	6/04/2023	5/08/2023	6/12/2023	
1061	TORRE DELL VOSTRO 3681	CL2TB93	FAC. CONSULTA EXTERNA	6/04/2023	5/08/2023	6/12/2023	
1294	TORRE DELL VOSTRO 3681	J65KF73	FAC. CONSULTA EXTERNA	6/04/2023	5/08/2023	6/12/2023	
0207	LENOVO ALL IN ONE FO8800LALLX	MP10UXNE	FARMACIA	7/04/2023	6/08/2023	7/12/2023	
N/A	HP ALL IN ONE C0391A	8CC0121JTV	FARMACIA	7/04/2023	6/08/2023	7/12/2023	
0299	COMPAQ ALL IN ONE 18-2001LA	5CM2500KXY	FISIOTERAPIA	7/04/2023	6/08/2023	7/12/2023	
1071	TORRE DELL VOSTRO 3681	HM2TB93	GERENCIA GENERAL	7/04/2023	6/08/2023	7/12/2023	
0235	HP ALL IN ONE C1106LA	8CC0320TNT	GERENCIA GENERAL	7/04/2023	6/08/2023	7/12/2023	
0068	COMPAQ ALL IN ONE 18	SC2500KYT	HOSPITALIZACIÓN	7/04/2023	6/08/2023	7/12/2023	
1773	TORRE DELL VOSTRO 3681	8M2TB93	HOSPITALIZACIÓN	7/04/2023	6/08/2023	7/12/2023	
0846	COMPAQ ALL IN ONE 18-2001 LA	5CM2500KZB	HOSPITALIZACION	7/04/2023	6/08/2023	7/12/2023	
0745	HP ALL IN ONE 20-c200 LA	8CC8380KJK	HOSPITALIZACION	7/04/2023	6/08/2023	7/12/2023	
0810	LENOVO ALL IN ONE FOD8004GLD	YJ00PH7V	HOSPITALIZACION	7/04/2023	6/08/2023	7/12/2023	

Calle 16 N° 53 - 46 Salida a Valledupar
 Teléfono: 4140124
 Código Postal: 472020

 ESE Hospital San Rafael Fundación
 @EESANRAFAEL
 esehospitalsanrafael



Hospitales
y Médico
en Tu Casa

0861	HP ALL IN ONE C0391A	8CC0222QQM	HOSPITALIZACIÓN PEDIATRIA	7/04/2023	6/08/2023	7/12/2023	
0699	COMPAQ ALL IN ONE 18-2001 LA	5CM2500KXZ	HOSPITALIZACIÓN PEDIATRIA	7/04/2023	6/08/2023	7/12/2023	
0135	HP ALL IN ONE 20-c200 LA	8CC8191NLR	LABORATORIO	7/04/2023	6/08/2023	7/12/2023	
0495	HP ALL IN ONE 20-C217LA	8CC9295MBZ	LABORATORIO	7/04/2023	6/08/2023	7/12/2023	
0521	HP ALL IN ONE 20-C218LA	8CC8080LHT	LABORATORIO	7/04/2023	6/08/2023	7/12/2023	
0476	HP ALL IN ONE C0391A	8CC01148XZ	LABORATORIO	7/04/2023	6/08/2023	7/12/2023	
0561	COMPAQ ALL IN ONE 18-2001 LA	5CM2500KZM	MATERNIDAD	8/04/2023	8/08/2023	8/12/2023	
0666	HP ALL IN ONE 20-C200LA	8CC8380KHT	MEDICINA FAMILIAR	8/04/2023	8/08/2023	8/12/2023	
0506	HP ALL IN ONE 20-c218 LA	8CC8080LCM	MEDICINA INTERNA	8/04/2023	8/08/2023	8/12/2023	
1093	COIN PORTATIL	LUMI142G202007000601	MISION MEDICA	8/04/2023	8/08/2023	8/12/2023	
N/A	LENOVO PORTATIL	PF28QFGF	MISION MEDICA	8/04/2023	8/08/2023	8/12/2023	
N/A	LENOVO PORTATIL	PF28R588	MISION MEDICA	8/04/2023	8/08/2023	8/12/2023	
0834	COMPAQ ALL IN ONE 20-c217 LA	8CC9295M4F	OBS. GINECOLOGIA	8/04/2023	8/08/2023	8/12/2023	
0572	HP SLIM LINE 260-A100BLA DTPTC LTNA	CNV7230N44	OBS. GINECOLOGIA	8/04/2023	8/08/2023	8/12/2023	
0782	COMPAQ ALL IN ONE 18-2001LA	5CM2500KZD	ORTOPEDIA CONS. EXTERNA	8/04/2023	8/08/2023	8/12/2023	
0396	HP ALL IN ONE C0391A	8CC0114C01	PEDIATRIA CONS. EXTERNA	8/04/2023	8/08/2023	8/12/2023	
N/A	HP ALL IN ONE 20-C218LA	8CC8080LX8	RAYOS X	8/04/2023	8/08/2023	8/12/2023	
0802	HP ALL IN ONE 20-C217la	8CC9295MG4	REFERENCIA	8/04/2023	8/08/2023	8/12/2023	
1075	TORRE DELL VOSTRO 3681	5N2TB93	REFERENCIA	8/04/2023	8/08/2023	8/12/2023	
0812	LENOVO ALL IN ONE	YJ00NXBC	REFERENCIA	8/04/2023	8/08/2023	8/12/2023	
0581	HP ALL IN ONE C0391A	8CC02133XD	REFERENCIA	8/04/2023	8/08/2023	8/12/2023	
0070	COMPAQ ALL IN ONE 18	5CN2500KPS	SIAU	9/04/2023	9/08/2023	9/12/2023	
0357	TORRE DELL VOSTRO 3681	572KF73	SISTEMAS	9/04/2023	9/08/2023	9/12/2023	
0634	HP PRO ONE 400 G4 20.0	8CG9430BF6	SISTEMAS	9/04/2023	9/08/2023	9/12/2023	
0369	HP ALL IN ONE C0391A	8CC0320TMQ	SISTEMAS	9/04/2023	9/08/2023	9/12/2023	
0366	SERVIDOR HP PROLIANT M110 GEN 9	MX26220037	SISTEMAS	9/04/2023	9/08/2023	9/12/2023	

Calle 16 N° 53 - 46 Salida a Valledupar
 Teléfono: 4140124
 Código Postal: 472020

 ESE Hospital San Rafael Fundación
 @EESANRAFAEL
 esehospitalsanrafael



Hospitales
y Médico
en Tu Casa

0741	HP DESTOKP 260-A 100 BLA "CPU"	CNV7230NY3	STAND CIRUGIA	9/04/2023	9/08/2023	9/12/2023	
0207	COMPAQ ALL IN ONE 18	5CM2500KXS	STAND CIRUGIA	9/04/2023	9/08/2023	9/12/2023	
6890	TORRE CLON	N/A	STAND CIRUGIA	9/04/2023	9/08/2023	9/12/2023	
0735	HP ALL IN ONE 20-c200 LA	8CC8380KMS	STAND URGENCIAS	9/04/2023	9/08/2023	9/12/2023	
0812	LENOVO ALL IN ONE	YJ006FQX	STAND URGENCIAS	9/04/2023	9/08/2023	9/12/2023	
0781	COMPAQ ALL IN ONE 18	5CM2500MHC	STAND URGENCIAS	9/04/2023	9/08/2023	9/12/2023	
0201	HP ALL IN ONE C0391A	8CC0121JRL	TALENTO HUMANO	9/04/2023	9/08/2023	9/12/2023	
0190	HP ALL IN ONE C0391A	8CC0114C31	TALENTO HUMANO	9/04/2023	9/08/2023	9/12/2023	
0093	HP ALL IN ONE 20-C200LA	8CC8380KJ1	TALENTO HUMANO	9/04/2023	9/08/2023	9/12/2023	
1097	TORRE DELL VOSTRO 3681	1M2TB93	TALENTO HUMANO	9/04/2023	9/08/2023	9/12/2023	
1357	HP ALL IN ONE 20-c200-LA	8CC9295MFQ	VACUNACIÓN	9/04/2023	9/08/2023	9/12/2023	

Calle 16 N° 5ª - 46 Salida a Valledupar
 Teléfono: 4140124
 Código Postal: 472020

 ESE Hospital San Rafael Fundación
 @EESANRAFAEL
 esehospitalsanrafael



Hospitales
y Médico
en Tu Casa



PROCEDIMIENTO PARA LA ACTUALIZACIÓN DEL SITIO WEB CON BASE GOBIERNO EN LÍNEA (TIC).

Desarrollo del Sitio web:

EL ingeniero de sistemas del Hospital actualiza e implementa el sitio web, el cual es alimentado con la información de todas las áreas de servicio del hospital tanto financiera como asistencial.

Procedimiento:

Cada jefe de área y la gerencia envían la información pertinente a lo que se requiere subir teniendo en cuenta la normatividad de ley del **Ministerio de las TIC** y bajo los lineamientos de **Gobierno En Línea**, regidos por los siguientes reglamentos.

Decreto 1151 abril 14 de 2008: Por el cual se establecen los lineamientos generales de la estrategia del gobierno en Línea de la República de Colombia, se reglamenta parcialmente la ley 962 de 2005 y se dictan otras disposiciones.

Ley 1712 del 6 de marzo de 2014: "por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

DECRETO 2693 de 2012- gobierno en línea ETAPAS Y COMPONENTES DE LA POLÍTICA ANTITRÁMITES Y DE GOBIERNO EN LÍNEA.

12. PROCEDIMIENTO SEGURIDAD DE LA RED INALÁMBRICA:

Para la red inalámbrica se tiene la seguridad por registro de ip, registro de mac, y se tiene clave de acceso, no podrá entrar a la red inalámbrica e internet ningún equipo de cómputo o móvil que llegue al hospital y quiera acceder a menos que llegue a sistema.

13. ADMINISTRACIÓN DE LA RED

Los usuarios de las áreas del hospital 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 del hospital, sin la autorización del área de sistemas.

14. SEGURIDAD PARA LA RED

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el área de sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del hospital, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Redes de datos cableada e inalámbrica: Para la red inalámbrica y cableada se tiene un archivo con las direcciones ip en donde antes de la asignación de un equipo a un usuario se verifica que no esté repetida y que pueda ser asignada.

15. SEGURIDAD SISTEMA OPERATIVO

ANTIVIRUS: Todos los equipos antes de trabajar con ellos el usuario se les instalan un antivirus debidamente licenciado con el que cuenta la entidad.

ENTRADA AL SISTEMA WINDOWS: Cada usuario nuevo en el sistema de cómputo debe entrar con la clave al sistema operativo por una cuenta local nadie excepto los de sistemas pueden entrar a instalar o a modificar programas sin previa autorización.

16. SEGURIDAD DEL SISTEMA DE INFORMACIÓN

Solo el sistema de información es modificado por los jefes de área los cuales tienen el permiso previamente asignado en su módulo, la clave máster solo la tiene el ingeniero de sistemas hace las modificaciones respectivas al sistema si hay un contrato de actualización que lo respalde, o por un correo electrónico que sirva como respaldo para cualquier reclamo.

17. USO DEL INTERNET

El acceso a Internet provisto a los usuarios y funcionarios de Hospital es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Hospital, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de sistemas.

Los usuarios de Internet del Hospital tienen que reportar todos los incidentes de seguridad informática al área de sistemas 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, 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 área de sistemas. La utilización de Internet es para el desempeño de sus funciones y cargo en el Hospital y no para propósitos personales.

18. PLAN DE ADQUISICIONES

Se detalla un plan de adquisición de equipos para el E.S.E. HOSPITAL SAN RAFAEL DE FUNDACION.

Elemento	Detalle	Cantidad
ANTIVIRUS	KASPERSKY ANTIVIRUS	130
NAS DE ALMACENAMIENTO		1
IMPRESORA	LASER MULTIFUNCIONAL	4
	TINTA MULTIFUNCIONAL	4
COMPUTADORES	ALL IN ONE y PORTATIL	15
SWITCH	24 PUERTOS BASE 1000	2
ACCES POINT		2
BLOWER	SOPLADOR - ASPIRADOR	1

19. PLAN DE COMUNICACIONES DEL PETI

En las actividades de comunicación y sensibilización del PETI en la institución, el área de Sistemas hará la divulgación por medio de los correos institucionales y reuniones de socialización con la alta gerencia, también por correo con el personal administrativo sobre los procesos de implementación de gobierno y mejoras continuas.