PLAN ESTRATEGICO DE TECNOLOGIA DE LA INFORMACION E.S.E. HOSPITAL SAN RAFAEL SAN VICENTE DEL CAGUAN

1 PROPÓSITO DEL DOCUMENTO

El Plan Estratégico de Tecnología de la Información – PETI, tiene como propósito el de establecer una guía de acción clara y precisa para la administración de las Tecnologías de Información y Comunicaciones (TIC) de la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, mediante la formulación de estrategias y proyectos que garantice el apoyo al cumplimiento de sus objetivos y funciones, en línea con el Plan de Gestión Institucional del Hospital.

2 ALCANCE DEL DOCUMENTO

Este documento describe las estrategias y proyectos que ejecutará la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, durante la vigencia 2020 - 2023, en cumplimiento de sus funciones y para el logro de sus objetivos; establece las estrategias que se aplicarán para lograrlo y establece las POLÍTICAS DE LA PLANEACIÓN INFORMÁTICA a desarrollar.

3 BENEFICIOS DE LA PLANEACIÓN Y JUSTIFICACIÓN DEL PETI

El Plan Estratégico de Tecnología de Información - PETI permite a la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, evaluar la forma de como beneficiarse de la tecnología, logrando un esquema de operación integrada, unificada y reconociendo oportunidades de ahorro y consolidación de esfuerzos.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

4 NORMATIVIDAD

NORMA	DESCRIPCION
Directiva Presidencial 02 de 2002	Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
Decreto Nacional 1151 del 14 de abril de 2008 y Manual para la implementación de la Estrategia de Gobierno en Línea de la República de Colombia	por el 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 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
Constitución Política 1991 Articulo 61	El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley
LEY 1438 DE 2011	"Por medio de la 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 del año 2013.
LEY 594 DE 2004	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

CAPITULO 1

PLANEACIÓN ESTRATEGICA E.S.E. HOSPITAL SAN RAFAEL

Identificación y Naturaleza. La Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán es una Entidad del orden Departamental, creada según Resolución No 1518 del 10 de marzo de 1.976 y se constituyó como Empresa Social del Estado a partir del 01 de enero de 2007.

6. MISION

La Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, del municipio de San Vicente del Caguán coordina y ejecuta los servicios de salud, garantizando la prestación completa del primer nivel de complejidad de salud con un eficiente, eficaz y oportuno servicio a todos los habitantes y comunidad en general.

7. VISION

La E.S.E. Hospital San Rafael, será en el año 2020 una empresa que preste un servicio óptimo de salud, sostenible social y financieramente, posicionada como una de las mejores de la región, con estándares de calidad que permitan enfocarse hacia la acreditación de sus servicios.

8. POLITICA DE CALIDAD

La Política de Calidad de la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, se fundamenta en su filosofía organizacional y está enmarcada en la Normatividad y en las siguientes bases conceptuales: Mejoramiento Continuo y Atención Centrada en el Cliente.

“El equipo humano de la E.S.E. Hospital San Rafael; lidera, coordina y ejecuta la prestación de los servicios de salud, a la comunidad de San Vicente del Caguán y su área de influencia, apoyado en sus recursos tecnológicos y teniendo una constante actualización al personal misional y de soporte a fin de extender la cobertura en salud, con un servicio eficiente, eficaz y oportuno.

9. OBJETIVO DE CALIDAD

a) Implementar los programas de capacitación al talento humano en los procesos misionales y de soporte, para mejorar la calidad en la prestación de los servicios.

b) Incrementar la eficiencia y calidad en el desempeño de los procesos, mediante la prestación de servicios de salud con calidad y seguros, que generen desarrollo y competitividad.
c) Aumentar los niveles de satisfacción, oportunidad y calidez en el servicio, mediante el acompañamiento integral que se traduzca en una confianza de nuestros clientes, y un referente como empresa líder en el sector salud.
d) Incrementar la eficiencia y eficacia en la prestación de los servicios de salud.
e) Aumentar la cobertura a través de realización de brigadas de salud.

10. PRINCIPIOS DE CALIDAD

En armonía con su estructura orgánica y funcional, la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, La alta dirección de la Institución, con el fin de conducir a la entidad hacia una mejora en su desempeño, busca la aplicación transversal de los siguientes principios de gestión de la calidad:

a) Enfoque hacia el usuario: "La razón de ser de las entidades es prestar un servicio dirigido a satisfacer a sus clientes; por lo tanto, es fundamental que las entidades comprendan cuales son las necesidades actuales y futuras de los clientes, que cumpla con sus requisitos y que se esfuercen por exceder sus expectativas".

El fin u objeto social de la E.S.E. Hospital San Rafael es la prestación de servicios de salud de baja y mediana complejidad entendidos como un servicio público a cargo del Estado y como parte integrante del Sistema de Seguridad Social en Salud por lo tanto, es fundamental que la institución, identifique cuales son las necesidades actuales y futuras y que cumpla con sus objetivos esforzándose por exceder las expectativas de sus usuarios, mejorando sus condiciones de salud.

b) Liderazgo: "Desarrollar una conciencia hacia la calidad implica que la alta dirección de cada entidad es capaz de lograr la unidad de propósito dentro de ésta, generando y manteniendo un ambiente interno favorable, en el cual los servidores públicos y/o particulares que ejercen funciones públicas puedan llegar a involucrarse totalmente en el logro de los objetivos de la entidad".

La Gerencia ha promovido con gran liderazgo el mejoramiento de la gestión institucional, desde el compromiso personal, y su participación dedicada a la

Implementación del sistema obligatorio de garantía de calidad.

c) Participación activa de los servidores públicos: "Es el compromiso de los servidores públicos que ejercen funciones públicas, en todos los niveles, que permite el logro de los objetivos de la entidad".

La Gerencia de la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán como entidad ha promovido espacios para la participación del personal, a través de capacitaciones específicas para los funcionarios misionales y de apoyo.

d) Enfoque basado en los procesos: "En las entidades existe una red de procesos, para trabajar articuladamente. Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso".

En la Institución, los procesos misionales, así como los procesos de apoyo y direccionamiento estratégico, al trabajar articuladamente en los diferentes servicios, permiten generar un resultado deseado cuando las actividades y los recursos relacionados se gestionan como un proceso.

e) Enfoque del sistema para la gestión: "Identificar, entender, mantener, mejorar y gestionar los procesos interrelacionados como un sistema, contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos".

Esto contribuye a que en la Institución, se evidencien las fallas para realizar los correctivos pertinentes y estructurar un sistema para lograr los objetivos en la forma más eficaz y eficiente.

f) Mejora continua: "La implementación de nuevas alternativas para la prestación de los servicios de salud, es indispensable para lograr el objetivo propuesto y para lograr una balanza entre la eficacia y la eficiencia"

La Administración de la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, mediante la implementación del Sistema Obligatorio de Garantía de Calidad y capacitando al personal, proporciona métodos y herramientas para la mejora continua de desempeño de la organización.

g) Enfoque basado en hechos para la toma de decisiones: "Las decisiones

eficaces se basan en el análisis de datos y la información"

La Gerencia de la Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, con la participación del personal, la oportuna y veraz información realiza seguimiento a la gestión para tomar decisiones acertadamente.

h) Relaciones mutuamente beneficiosas con los proveedores de bienes o Servicios: "Las Instituciones y sus proveedores son interdependientes; y una relación beneficiosa aumenta la capacidad de ambos para crear valor"

La Institución busca una relación contractual equilibrada para la adquisición de bienes y servicios, desarrollando la identificación y selección de los proveedores con una comunicación clara y abierta que conduzca al mejoramiento de la gestión, y el aseguramiento de los productos y/o servicios que se contratan.

i) Coordinación, cooperación y articulación: "El trabajo en equipo, en y entre entidades, es importante para el desarrollo de relaciones que beneficien a sus clientes y que permitan emplear de una manera racional los recursos disponibles".

La Empresa Social del Estado Hospital San Rafael de San Vicente del Caguán, realiza los procesos de coordinación y celebra convenios interadministrativos que contribuyen a la prestación de los servicios de salud, fortaleciendo económicamente la Institución para lograr una atención de manera oportuna y eficaz a sus usuarios.

j) Transparencia: "La gestión de los procesos se fundamenta en las actuaciones y las decisiones claras; por lo tanto, es importante que las entidades garanticen el acceso a la información pertinente de sus procesos facilitando el control social".

Con la creación de la Empresa Social del Estado, se han abierto espacios de participación a la comunidad a través de la oficina de atención al usuario y la conformación de la Asociación de Usuarios del Hospital. El principio va inmerso en todos los procesos, el socializar las decisiones y permitir que estos retroalimenten en la organización, facilita el control social. El Manual de Contratación de la E.S.E., se ajusta a los principios de transparencia consagrados en la Constitución y las leyes.

11. Principios Éticos.

- ✓ Garantizar los mecanismos de participación Ciudadana y Comunitaria
- ✓ Los bienes públicos pertenecen a la sociedad.
- ✓ La contribución al mejoramiento de las condiciones de vida de la población.
- ✓ Servir a la ciudadanía.
- ✓ Rendición de cuentas a la sociedad.

12. Valores Institucionales.

Los valores son un conjunto de preferencias culturales y actitudes psicológicas que estructuran los juicios de los seres humanos. Dentro de los valores definidos por el grupo humano del Hospital San Rafael de San Vicente del Caguán figuran:

- ✓ **Transparencia:** Los funcionarios de la E.S.E. Hospital San Rafael deberán cumplir con los deberes y Obligaciones a los que se han comprometido con la Institución y la Sociedad
- ✓ **Integridad:** La Entidad declara que los principios éticos contenidos en el Código de Ética y Buen Gobierno son el marco de actuación de los servidores, quienes se comprometen a respetarlos y hacerlos cumplir.
- ✓ **Responsabilidad:** Los funcionarios de la E.S.E. Hospital San Rafael, tienen como compromiso realizar sus funciones aportando lo mejor de si mismo con obligación moral por cumplir con el deber asignado con sabiduría, rectitud y oportunidad.
- ✓ **Servicio:** Los funcionarios de la E.S.E. Hospital San Rafael están comprometidos a mejorar la oportunidad en la prestación de los servicios de salud, buscando la satisfacción de los usuarios.
- ✓ **Solidaridad:** Los Funcionarios de la E.S.E. Hospital San Rafael contribuyen a mejorar las condiciones de vida a través de la colaboración y el apoyo mutuo.
- ✓ **Equidad:** La Entidad encamina sus esfuerzos hacia el respeto por los derechos de los demás, dándole aplicación a la normatividad con imparcialidad y justicia.
- ✓ **Lealtad:** Las Funcionarios de la E.S.E. Hospital San Rafael se comprometen en forma absoluta su fidelidad para con la institución ser coherentes con los principios y valores institucionales.
- ✓ **Honestidad**: Los Funcionarios dela E.S.E. Hospital San Rafael se caracterizan por su buena conducta, lealtad a la misión institucional e integridad,

- ✓ **Grupos de Interés**. La E.S.E. Hospital San Rafael reconoce como sus grupos de interés a la Ciudadanía, Contratistas, Proveedores, Gremios Económicos, Organismos Sociales y Sindicales, Organismos de Control, Organizaciones Públicas y Privadas (Entidades Adscritas y Vinculadas, EPS, ARL, Cajas de Compensación Familiar, Comunidad y Agremiaciones, entre otras).

13. ESTRUCTURA GENERAL DEL PLAN ESTRATEGICO.

El Plan Estratégico de la E.S.E. Hospital San Rafael de la vigencia 2017 – 2019 se estructura a partir de la normatividad vigente, la definición de la política general del Hospital y los objetivos estratégicos, cada uno con sus líneas de acción, las cuales se articulan con los planes de acción de las áreas funcionales de la institución.

Dicho plan se hace realidad en el presupuesto de ingresos y gastos de la E.S.E. para dar cumplimiento a los objetivos que dan funcionalidad a la Entidad.

GESTION ADMINISTRATIVA Y FINANCIERA

OBJETIVO 1.

Adquisición de equipos de cómputo.

METAS

- ➢ Actualización de la tecnología.
- ➢ Rapidez en los aplicativos.

ESTRATEGIAS

- ➢ Actualización de la tecnología.
- ➢ Hacer una convocatoria para la presentación de propuestas y ofertas de proveedores.

ACTIVIDADES

- Adquirir equipos de cómputo con sus respectivas licencias.

RESPONSABLES

Gerente, Subgerente Administrativo y Financiero, Ingeniero de sistemas

PLAZO

Mediano

OBJETIVO 2.

Sistematización oficina de archivo.

METAS

- Información veraz y oportuna en los archivos de la E.S.E.
- Seguridad de la información.
- Cumplimiento a la ley 594/2004

ESTRATEGIAS

- Compra de Software.
- Adecuación del área Archivo.
- Compra de PC.
- Capacitación al personal Administrativo del área.

ACTIVIDADES

- Hacer una convocatoria para la presentación de propuestas y ofertas de proveedores.

RESPONSABLES

Gerente, Subgerente Administrativo y Financiero, Ingeniero de sistemas.

PLAZO

Corto

OBJETIVO 3.

Circuito Cerrado de Televisión.

METAS

- Seguridad en la E.S.E.
- Vigilancia en las áreas críticas de la E.S.E..

ESTRATEGIAS

- Compra de Sistema de Tele vigilancia.
- Ampliación de la red se seguridad que se encuentra actualmente.

ACTIVIDADES

- Hacer una convocatoria para la presentación de propuestas y ofertas de proveedores.

RESPONSABLES

Gerente, Subgerente Administrativo y Financiero, Ingeniero de sistemas.

PLAZO

Largo.

CAPITULO 2

MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA OFICINA DE SISTEMAS

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

1. GENERALIDADES

1.1 INTRODUCCIÓN

El documento que a continuación se presenta describe el origen, evolución y logros de la Oficina de Sistemas de la E.S.E. Hospital San Rafael, así como sus objetivos, políticas, estructura organizacional, procesos, estrategias y orientaciones institucionales. La información correspondiente al desarrollo normativo y fundamentación epistemológica, así como la bibliografía se conservan en los documentos de base elaborados por la unidad y que sirvieron de sustento para el presente documento.

1.2 OBJETIVO DEL MANUAL:

Determinar los diferentes procesos y responsables que componen los servicios que presta La E.S.E. Hospital San Rafael respecto a la Oficina de Sistemas.

1.3 ALCANCE DEL MANUAL:

Es el soporte de la Oficina de sistemas en la E.S.E. Hospital San Rafael.

2. PROCEDIMIENTOS DE INFORMÁTICA Y SISTEMAS

2.1

PROCEDIMIENTO DE ADMINISTRACIÓN DE CENTRO DE DATOS Y SEGURIDAD INFORMATICA:

2.1.1 CENTRO DE DATOS Y SEGURIDAD INFORMATICA:

2.1.1.1 DESARROLLO DE LAS ACTIVIDADES:

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
		MONITOREO DE RECURSOS: Se realiza un monitoreo del desempeño de las particiones y discos en cada uno de los servidores, verificando la velocidad de lectura y escritura, tiempo de acceso y capacidad usada. Se realiza un monitoreo del desempeño de la CPU, verificando el porcentaje de consumo del sistema y las aplicaciones. Se realiza un monitoreo de los tiempos de respuesta de la interfaces del servidor, también se verifica el ancho de banda consumido por el mismo.

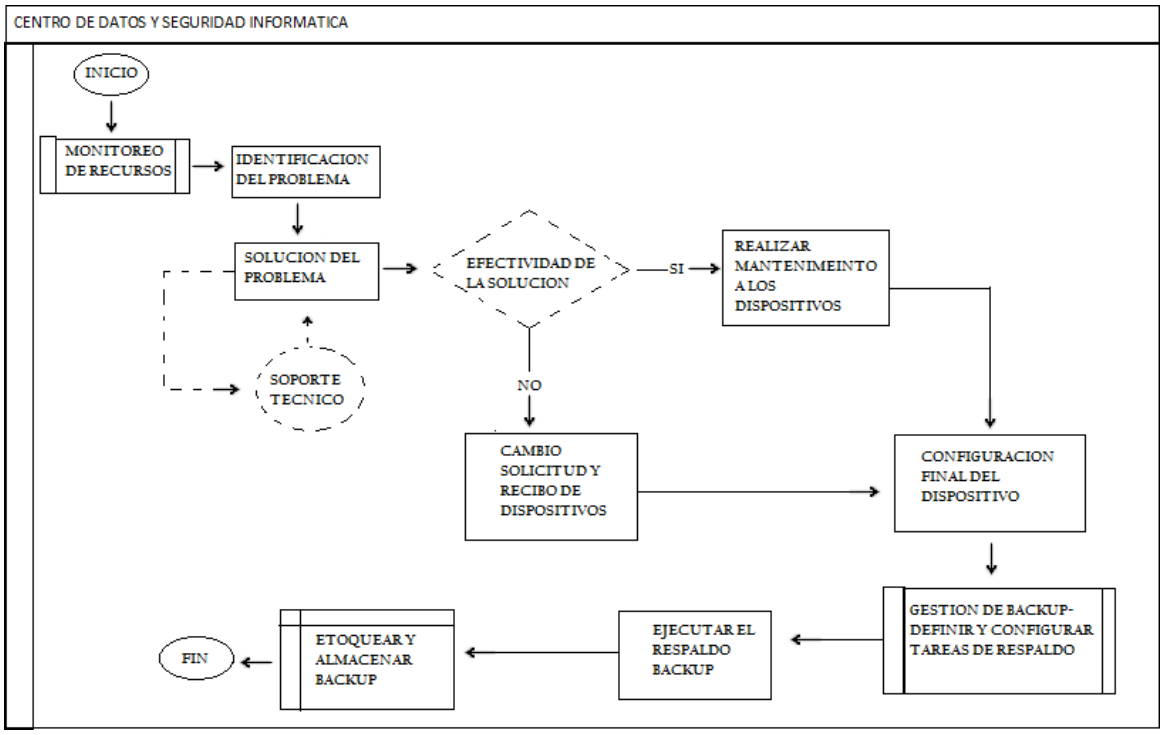
1	Ingeniero de Sistemas	Se realiza una revisión de los diferentes archivos de logs del servidor para determinar si en el hardware o software se presentan anomalías. Se realiza una revisión de los enlaces de datos (Internet e Intranet) y los equipos de red (swiches y enrutadores) para detectar posibles fallas o la no disponibilidad operativa de los mismos. Si los problemas en los discos, la CPU, interfaces de red, equipos de red, enlaces, telefonía y los logs persisten se pasa a la siguiente actividad para su identificación. **IDENTIFICACIÓN DEL PROBLEMA:** Para los discos: Se verifica que la aplicación no esté generando problema sobre la lectura o escritura del disco. Se verifica que el disco o partición no esté presentado fallos físicos. Se verifica que el disco no esté ocupado al 100% de su capacidad. Para la CPU: Se identifica el proceso o procesos que estén generando los mayores consumos de CPU y se verifica si es correcto o no el valor presentado. Nota: el valor de uso de CPU varía de acuerdo con el tipo de aplicación.
2	Ingeniero de Sistemas	Para interfaces de red: Se verifica el consumo de ancho de banda, teniendo en cuenta el tipo de tráfico (HTTP, SMTP, FTP, STREAMING, recursos compartidos, entre otros) que se genere. Dependiendo de este tipo de tráfico se verifica si hay algún problema en los dispositivos de red o si algún equipo o aplicativo está haciendo uso indebido del ancho de banda. Para equipos de red: Se localiza el equipo de red afectado acudiendo al mapa de distribución de equipos y a la herramienta de monitoreo. Se detecta la falla en el equipo o puerto. Para enlaces de red: Se establece el alcance del corte en el servicio ya sea en la red de campus o en la red de Internet, para lo cual se acude al estado de los enlaces (herramienta de monitoreo). Para logs:

		Se identifica el tipo de mensaje reportado, el cual permite establecer sobre qué dispositivo o aplicación se está presentando la anomalía.
3	Ingeniero de Sistemas	**SOLUCIÓN DEL PROBLEMA:** Se realizan las correcciones necesarias para el correcto funcionamiento de los dispositivos: discos, CPU, equipos de red, enlaces, interfaces de red, cables y logs. Nota: En algunas ocasiones los problemas presentados en las interfaces de red se deben a clientes de la intranet; para su solución se pasa para soporte técnico para que programar el servicio, revisar y corregir el problema presentado por el cliente. **CAMBIO, SOLICITUD Y RECIBO DE DISPOSITIVOS:** En caso de falla de algún dispositivo se verifica si puede ser sustituido por algún otro que se encuentre en el stock de la Oficina de Sistemas o si este tiene garantía. Si el dispositivo tiene garantía se verifica que el proceso a seguir con el proveedor.
4	Ingeniero de Sistemas	Si la garantía está vigente se contacta telefónicamente al proveedor del servidor para que diagnostique y sustituya el dispositivo. Cuando el dispositivo (servidor, planta, extensión, equipo de red) o componente no posee contrato se contacta al proveedor para que diagnostique y envié una cotización que incluya el costo de mantenimiento y del dispositivo. Estas cotizaciones se envían a la Oficina de Administración con el concepto técnico, la solicitud de orden de compra y el Certificado de disponibilidad Presupuestal. Se recibe el dispositivo y la salida de almacén, por parte de la Oficina de Almacén. En el momento en que se realiza la instalación por parte del proveedor, se hace un seguimiento a la instalación y posteriormente se verifica el correcto funcionamiento del mismo. Con aprobación del Ingeniero de Sistemas, se envía un oficio a la Oficina de Administración indicando la entrega a satisfacción por parte del proveedor.
5	Ingeniero de Sistemas	**REALIZAR MANTENIMIENTO A LOS DISPOSITIVOS:** Se hace limpieza y se corren diagnósticos a los dispositivos. (dispositivos y servidores) Se realiza la afinación del servidor, configurando los parámetros óptimos para tener el mejor desempeño del servidor. Se realiza la eliminación de los archivos de logs o

		respaldos temporales que ya no son necesarios.
6	Ingeniero de Sistemas	**CONFIGURACIÓN FINAL DEL DISPOSITIVO:** Se hacen pruebas de funcionamientos a cada dispositivo, red o servidor; y se deja en estado funcional. Se realiza configuraciones a nivel de firewall local, permisos de lectura, ejecución y escritura sobre dispositivos y servidores para aumentar la seguridad. Se verifica que los parches de seguridad de dispositivos y servidores para que estén actualizados. Se verifica periódicamente que la información de los respaldos en cuanto a consistencia y disponibilidad en caso de que necesite ser recuperado. **GESTIÓN DE BACK UP - DEFINIR Y CONFIGURAR TAREAS DE RESPALDO:** Los respaldos de datos pueden ser respaldos lógicos o respaldos en frío.
7	Ingeniero de Sistemas	Respaldo en frío : Previo acuerdo con el usuario funcional, se define día y hora de ejecución de este respaldo (Horario Nocturno). Nota para base de datos: Se le debe recordar al usuario funcional que éste respaldo implica suspender el servicio de la base de datos. Configurar base de datos en modo archivelog. Identificar los archivos que componen la base de datos. Respaldo Lógico: Se construye un script que especifica los datos a respaldar, nombre del archivo a generar, el nombre del archivo log, el tipo de respaldo y las fechas del respaldo.
8	Ingeniero de Sistemas	**EJECUTAR EL RESPALDO – BACK UP:** Si el respaldo es lógico: Se emplea la utilidad para programar tareas del sistema operativo (cron), se programa la ejecución del script de respaldo automáticamente. Si el respaldo es en frío para base de datos: En las fechas previamente pactadas, se baja en modo normal la base de datos y se copian con comandos del sistema operativo los archivos que componen la base de datos (30 días). Se copian diariamente los archivos tipo archivelog. Si el respaldo es en frío para sistema operativo: En las fechas previamente pactadas, se copian los respaldos del sistema operativo, los archivos que componen las diferentes aplicaciones o servicios a

		respaldar.
9	Ingeniero de Sistemas	**ETIQUETAR Y ALMACENAR – BACK UP:** Se verifica como fueron ejecutados cada uno de los scripts de respaldo consultando los archivos tipo log. Si fue exitoso: Se procede a copiar los archivos en disco, medios magnéticos y guardarlos debidamente marcados en la caja de seguridad, Centro de datos y copia externa. Si no fue exitoso: Se notifica vía correo electrónico, al profesional responsable del servicio respaldado. Se concerta con él una posible solución o si es del caso se regresa nuevamente a la actividad •Se hace el respectivo registro en el formato backups para respaldos. •Se almacena en caja de seguridad.

2.1.1.2FLUJOGRAMA:



Calle 5 No 3-38 Telefono (8) 4644101 Fax (8) 4644912
www.hospitalsanrafael.gov.co
info@hospitalsanrafael.gov.co / sistemas@hospitalsanrafael.gov.co
San Vicente del Caguán Caquetá Colombia

2.1.2GESTIÓN DE BACKUPS DE SERVIDORES:

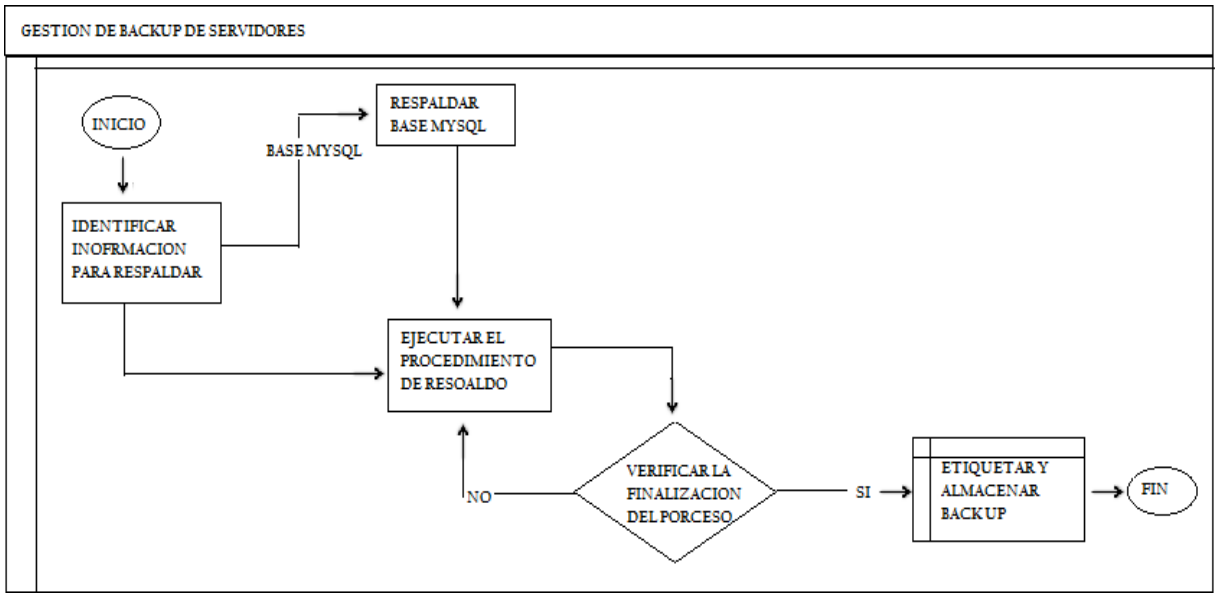
Este procedimiento respalda la información de los aplicativos institucionales que están bajo la responsabilidad de la Oficina de Sistemas, conforme a las políticas de seguridad establecidas por éste y garantiza la disponibilidad de los datos en el momento en que se requieran.

2.1.2.1DESARROLLO DE LAS ACTIVIDADES:

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
1	Ingeniero de Sistemas	**IDENTIFICAR INFORMACIÓN PARA RESPALDAR:** El tipo de información se identifica por: -Servidor. En este caso, se identifican los archivos o particiones que se van a respaldar. Se continúa con la Actividad 3. -Aplicación. En este caso se identifica si es la aplicación o los datos de la aplicación son los que se van a respaldar. -Si el respaldo es de aplicación, se continúa con la actividad 3. -Si el respaldo es de bases MySQL, se continúa con la actividad 2. Si se trata de otro tipo de base de datos, es preciso consultar la Guía de administración Centro de Datos y Seguridad Informática
2	Ingeniero de Sistemas	**RESPALDAR BASES MYSQL:** Bases MySQL. Se respaldan diariamente mediante la herramienta de backup de MySQL Administrador. Nota: Este respaldo se realiza en disco duro o medios magnéticos. Fin de procedimiento.
3	Ingeniero de Sistemas	**EJECUTAR EL PROCEDIMIENTO DE RESPALDO:** Se ejecuta el respaldo de la información a través de los siguientes comandos: Para respaldar servidores se utiliza una conexión en forma remota protocolo ssh y los archivos son extraídos mediante el uso de protocolo ssh.

4	Ingeniero de Sistemas	**ETIQUETAR Y ALMACENAR:** Se especifica a que servidor o aplicación se le realizó el backup con la fecha en que se realizó. Almacenar en gavetas.

2.1.2.2FLUJOGRAMA:



2.2

PROCEDIMIENTO DE ADMINISTRACIÓN DEL PORTAL INSTITUCIONAL:

2.2.1ADMINISTRACIÓN DEL SERVIDOR Y DE LA PLATAFORMA DEL PORTAL

INSTITUCIONAL:

2.2.1.1POLITICAS, NORMAS Y MEDIDAS DE

SEGUIRIDAD TIPO DE INFORMACIÓN

- Lenguajes de programación para subir páginas web al servidor, esto es: HTML, HTML5, XHTML, CSS, CSS3, PHP y JAVA
- Información sobre eventos, publicaciones, boletines, etc., que hagan referencia a la E.S.E. Hospital San Rafael.

El contenido.

- Cualquier contenido, vínculo, imagen u otro que afecte la imagen y los intereses de la E.S.E. (Éstos serán retirados del servidor web sin aviso a la dependencia).
- Los documentos que se suban al servidor (deberán ser norma de gestión de calidad) en formato PDF.
- No se permitirán archivos ejecutables .EXE
- Todos los contenidos o publicaciones que contengan información referente a la E.S.E. (eventos, proyectos, evaluaciones, formularios, páginas web), deberán ser enviadas a los correos institucionales de sistemas@hospitalsanrafael.gov.co o info@hospitalsanrafael.gov.co además aprobadas por la Oficina de Sistemas y Gerencia.

PLANTILLA PUBLICACIÓN DE CONTENIDOS

- Todas las publicaciones de información general que se realicen en el portal web institucional o intranet deberán tener la plantilla institucional vigente. Sin embargo, es posible utilizar una diferente siempre y cuando sea para la promoción de un evento o convenio, presentaciones en flash, o consulta de base de datos.

LOGOTIPOS, MARCAS, IMÁGENES Y ANIMACIONES

- Los logotipos y marcas serán los aprobados por el Gobierno del Departamento y la Gerencia de la E.S.E.

Web o Intranet.

- Las imágenes que se publiquen deben ser de autoría de la E.S.E.. Cuando se publique una imagen que no pertenezca a la E.S.E. se deben escribir los respectivos derechos de autor o del sitio web de donde se obtuvo la imagen.
- El formato para imágenes podrá ser: JPG, GIF o PNG
- El formato para animaciones será: SWF
- El formato para video podrá ser FLV o se pueden utilizar videos embebidos de YouTube de la cuenta institucional

TAMAÑO DE LOS ARCHIVOS

- Los archivos que se publiquen en el servidor web no podrán superar los 10 MB;
- Se permite realizar vínculos a otros sitios web de la E.S.E. o ajenos a ella. Sin embargo, estos vínculos deben ser de páginas que contengan información importante para la E.S.E. y que no desvíen los intereses institucionales y administrativos de la misma (MISIÓN y VISIÓN)

REDES SOCIALES (Facebook, YouTube, Flicker, Twitter, etc)

- Las redes sociales oficiales de la E.S.E. serán administradas por la Oficina de Sistemas.

SEGURIDAD Y PERMISOS SOBRE EL SERVIDOR WEB

- El responsable de la administración de los usuarios y claves será el Ingeniero de sistemas.
- La Oficina de Sistemas es el único ente autorizado para cambiar contraseñas, nombres de usuario, dar de alta o de baja a un usuario.

RESPALDO Y BACKUPS DE INFORMACIÓN

- La Oficina de Sistemas tiene una política de backups propia para el servidor web de la E.S.E., no obstante cada área o departamento es responsable de hacer copias de su información.

PROGRAMACIÓN Y BASES DE DATOS

- Todos los sitios web deberán ser programados en los lenguajes PHP o JAVA; no se permiten páginas sobre tecnologías .NET o ASP u otros que necesiten de servidores en Windows.
- Las bases de datos son administradas exclusivamente por la Oficina de Sistemas.
- Para las áreas que realicen programación con bases de datos deberán crearlas localmente en un equipo y enviarlas a la Oficina de sistemas, indicando para qué va a ser utilizada la base de datos.
- Las bases de datos permitidas en el servidor web serán en MySQL.
- La programación deberá estar orientado a garantizar la optimización de las bases de datos de tal manera que éstas no afecten el rendimiento del servidor web. En caso de que una base de datos sea muy robusta o demasiado grande y consuma recursos del servidor, será retirada la publicación y se informará al área que realizó la programación.

SANCIONES

- Las sanciones pueden resultar en la suspensión temporal de la sección o la cancelación definitiva de su espacio.

PUBLICACIONES EN LA PÁGINA PRINCIPAL DEL SITIO WEB

- La Oficina de Sistemas es el único ente que podrá publicar información en este espacio del sitio web de la E.S.E. y panel de noticias.
- Si alguna unidad necesita publicar información en este espacio deberá enviar la solicitud al correo sistemas@hospitalsanrafael.gov.co adjuntando el respectivo archivo o información a publicar.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

2.2.2CONTROL DEL CORREO INSTITUCIONAL:

NORMAS Y DEBERES:

- La identificación de los servicios informáticos es única y exclusivamente para uso personal, para actividades netamente institucionales y deberá ser empleada únicamente por la persona a quien le fue asignada. El correo es de uso personal e intransferible.
- Es deber de cada usuario asegurarse de cerrar la sesión de trabajo una vez finalice la utilización de todos los servicios a fin de que nadie más pueda utilizar su identificación. El olvidar esta tarea puede acarrear graves consecuencias para el usuario, que van desde la posibilidad de pérdida de información y el envío de correos a su nombre, hasta el uso inadecuado, por parte de otras personas, de los recursos que le fueron asignados.
- Si un usuario encuentra abierta la identificación de otra persona es su deber cerrarla y por ningún motivo deberá hacer uso de ella.
- Toda comunicación oficial entre funcionarios, asistenciales y administrativos de la E.S.E. se deberá realizar a través del correo institucional con dominio www.hospitalsanrafael.gov.co. Según corresponda.
- El usuario será el único responsable del perjuicio que pueda llegar a ocasionarle el no poder enviar ni recibir mensajes y archivos de correos electrónicos en caso de que el espacio que se le haya asignado este agotado.
- La E.S.E., en caso de uso no permitido del correo electrónico, suministrará la información del usuario a la entidad que lo requiera para algún tipo de investigación por uso no apropiado del servicio, esto sin que ella sea parte de la investigación, ya que simplemente es la entidad que ofrece el servicio.
- El usuario de correo de la E.S.E. debe revisar con frecuencia el buzón de su cuenta de correo.
- No se debe realizar envío de correos tipo cadena o forwards con información que no pertenezca al área de salud o institucional.

2.2.3POLÍTICAS DE USO:

- La E.S.E. Hospital San Rafael está bajo las políticas del proveedor que suministra el servicio de correo

(Google) citados en el siguiente link:

https://www.google.com/a/hospitalsanrafael.gov.co/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/a/hospitalsanrafael.gov.co

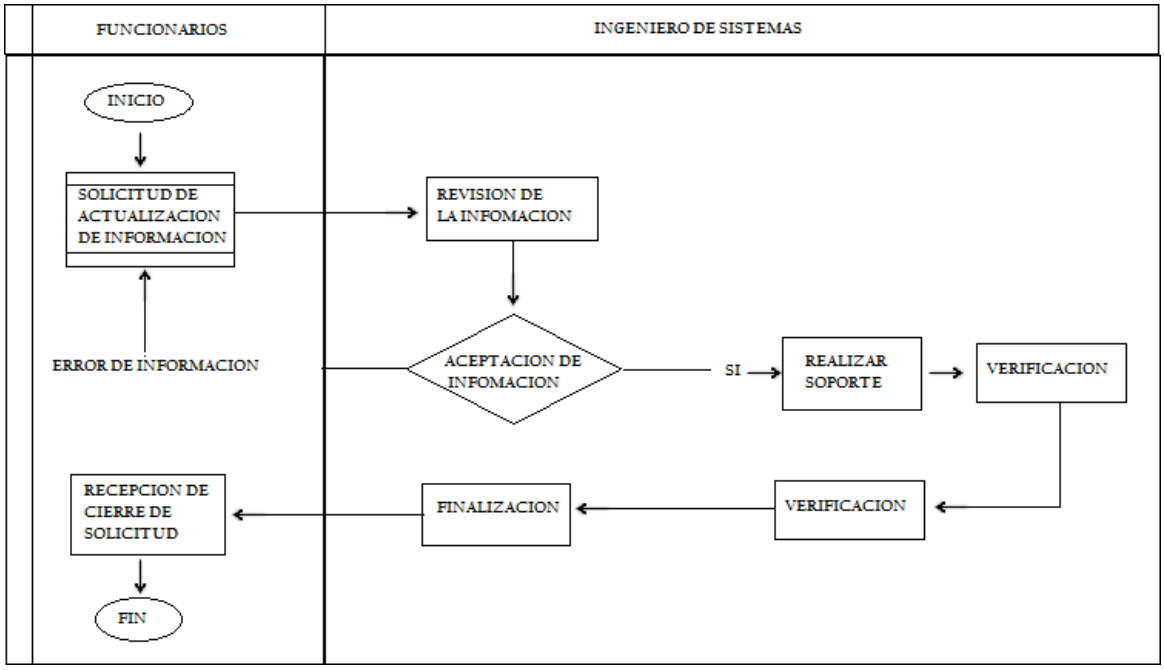
- Cada buzón de correo tendrá una capacidad de acuerdo a lo que designe el proveedor del servicio de correo electrónico.
- La E.S.E. no se hace responsable por el contenido de texto, sonido, video o cualquier otro que el usuario envíe o reciba usando el correo electrónico institucional.
- En el momento en que el usuario deje de ser Funcionario de la E.S.E., se cancelará en forma inmediata el servicio de Correo Electrónico; la E.S.E. no se hace responsable de pérdidas de información por este proceso. En caso de reingreso, la E.S.E. no puede asegurar la disponibilidad del mismo nombre de usuario ni mucho menos del backup de los archivos del periodo anterior.
- Mantener y ejecutar funciones de administración para eliminar aquellos mensajes que no requieran estar almacenados con el fin de mantener espacio disponible tanto para enviar como para recibir nuevos mensajes.
- Utilizar destinatarios precisos para evitar los mensajes en cadenas o series.
- Solicitar en la Oficina de Sistemas de la E.S.E. ayuda para el envío de correo masivo con el fin de evitar el SPAM.
- Solicitar o enviar correo de acuerdo con la cuota de almacenamiento asignada por la E.S.E. con el fin de evitar devoluciones de correos.
- Es deber de los usuarios, cada vez que se identifiquen con una cuenta de correo Institucional, velar porque no se comprometa la buena imagen de la E.S.E.
- El usuario se compromete a indemnizar y a exonerar a la E.S.E. y a sus funcionarios de cualquier reclamo o demanda, incluyendo honorarios razonables de los abogados, hecho por una tercera parte y derivados del contenido que el usuario presente, anuncie o transmita por medio del Servicio, su uso y conexión al mismo, su violación de los certificados de seguridad, o su violación de los derechos de terceros.
- El usuario debe respetar y acatar las políticas de uso que entregue el proveedor de servicios de correo electrónico a la E.S.E.
- A quienes incumplan con alguna de las políticas y normas establecidas, le podrán ser suspendidos los servicios de forma parcial o total dependiendo de la gravedad de la falta, y se le podrán aplicar las debidas sanciones.

2.2.3.1ESARROLLO DE LAS ACTIVIDADES CORREO INSTITUCIONAL

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
1	Funcionarios de la E.S.E.	SOLICITUD DE ACTUALIZACIÓN DE INFORMACIÓN: Se recibe la solicitud de creación de correo, cambio de contraseña o soporte, a través del correo electrónico o mediante oficio a la oficina de sistemas.
2	Ingeniero de Sistemas	REVISIÓN DE LA INFORMACIÓN: Se revisa que los datos enviados correspondan a la persona que solicita el soporte, de acuerdo con los datos que se indican cuando un usuario solicita crear correo o solicita algún soporte.
3	Ingeniero de Sistemas	ERROR EN INFORMACION: Si la información no corresponde o no está completa se envía un correo a quien la envió para que realice los respectivos ajustes
4	Ingeniero de Sistemas	REALIZAR SOPORTE: Se accede al servidor de correos de la E.S.E. y se realiza la creación del correo, el soporte, de acuerdo con los datos que se indican cuando un usuario solicita crear correo o solicita algún soporte.
5	Ingeniero de Sistemas	VERIFICACIÓN: Se verifica que los datos creados o modificados que funcionen adecuadamente
6	Ingeniero de Sistemas	FINALIZACIÓN: Se da respuesta al usuario a través del correo electrónico sobre la creación de la cuenta o los cambios realizados de acuerdo con la solicitud recibida. Se le envían las instrucciones necesarias para acceder y las consideraciones que debe tener en cuenta en el uso del correo.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

2.2.3.2FLUJOGRAMA



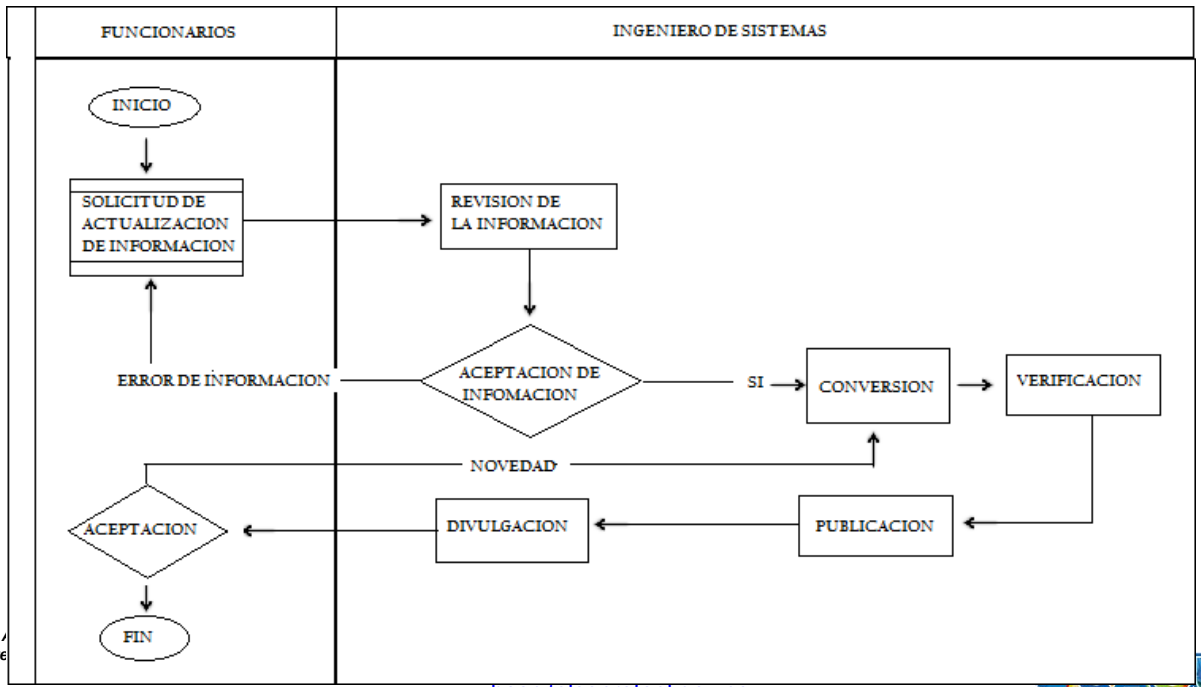
2.2.4CREACIÓN Y ACTUALIZACIÓN DEL PORTAL INSTITUCIONAL

2.2.4.1DESARROLLO DE LAS ACTIVIDADES

No	RESPONSABLE	DESCRIPCIÓN DE LAS ACTIVIDADES
1	Jefes de área e Ingeniero de Sistemas	RECEPCIÓN DE INFORMACIÓN: Recibir la información para publicar en los sitios web de la E.S.E. a través de solicitud escrita (memorando) o virtual (correo electrónico).
2	Ingeniero de sistemas	REVISIÓN: Revisar que la información haya llegado en su totalidad y que corresponda a lo que se solicita publicar. ERROR EN INFORMACIÓN: Si la información no corresponde o no está completa se envía un correo a quien la envió para que realice los respectivos ajustes.
3	Ingeniero de Sistemas	CONVERSIÓN: Se realiza la conversión del documento enviado al sistema de archivos del espacio virtual en donde vaya a ser publicada la información. De igual manera se realiza la edición de imágenes si la publicación lo

		amerita
4	Ingeniero de Sistemas	VERIFICACIÓN: Se verifica en varios ambientes virtuales y navegadores (según corresponda) que la publicación sea correcta y funcione adecuadamente en el espacio virtual en donde se ha publicado la información enviada
5	Ingeniero de Sistemas	PUBLICACIÓN: Se realiza la publicación de la información en el espacio virtual que corresponda
6	Ingeniero de Sistemas	DIVULGACIÓN: Se informa a través del correo electrónico institucional o memorando u otro medio, si fuese necesario, que sea realizada la publicación de la información solicitada
7	Gerencia y Subgerencias	ACEPTACIÓN: La Gerencia y Subgerencias revisan la información para cambio o novedad sobre la divulgación realizada.
8	Ingeniero de Sistemas	ARCHIVO DE COPIA Archivo de una copia de los memorandos o correos que indican el momento en el que el trabajo fue publicado en el portal web de E.S.E..

2.2.4.2FLUJOGRAMA



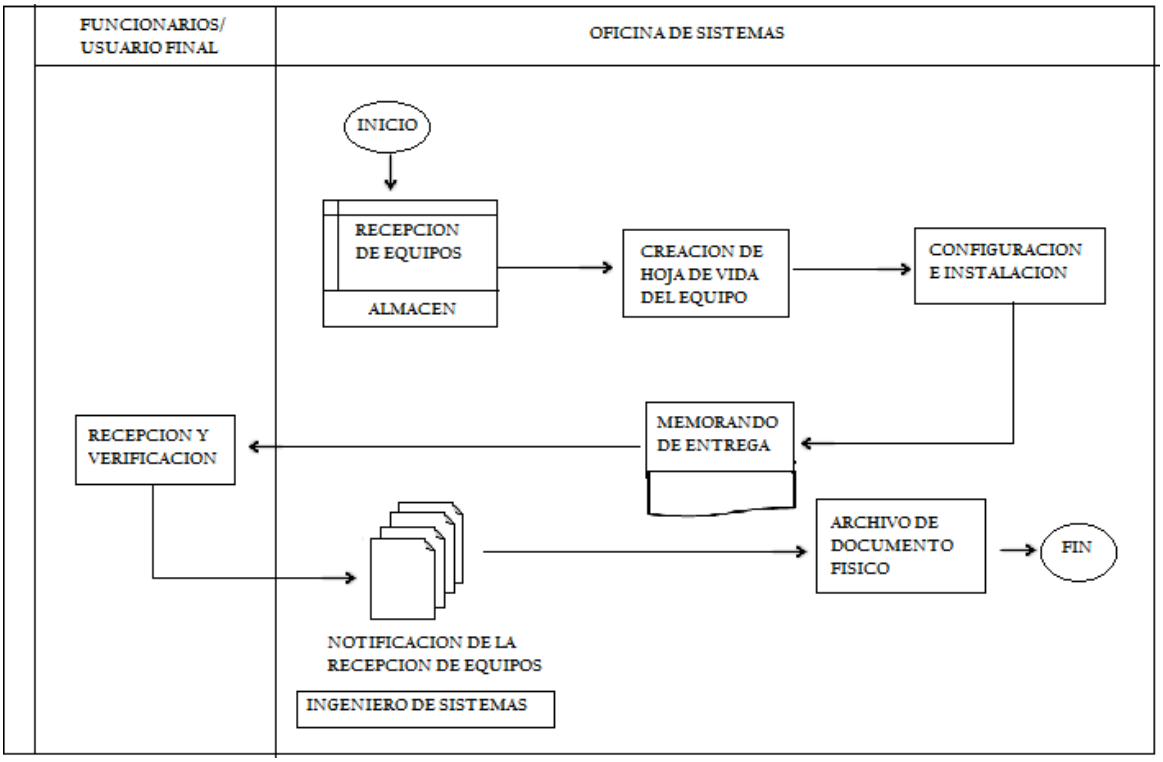
2.3PROCEDIMIENTO DE SOPORTE TECNICO:

2.3.1RECEPCION Y ASIGNACION DE EQUIPOS:

2.3.1.1DESARROLLO DE ACTIVIDADES:

No	RESPONSABLE	DESCRIPCION DE ACTIIVDADES
1	Ingeniero de Sistemas	RECEPCION DE EQUIPOS: Recibe los equipos solicitados y verifica que correspondan al pedido aprobada por el Almacén.
2	Ingeniero de Sistemas	CREACIÓN DE HOJA DE VIDA DEL EQUIPO: se crea la hoja de vida respectiva para el control de inventario tecnológico a partir de la información enviada por Almacén.
3	Ingeniero de Sistemas	CONFIGURACIÓN E INSTALACIÓN: Configuración e instalación de equipos y entrega a usuarios
4	Ingeniero de Sistemas	MEMORANDO DE ENTREGA: El ingeniero elabora el memorando de entrega, con la información pertinente del equipo.
5	Usuario final (Funcionarios)	RECEPCION Y VERIFICACION: Recibe y firma la remisión de entrega de los equipos a satisfacción.
6	Ingeniero de Sistemas	NOTIFICACION DE LA RECEPCION DE EQUIPOS: Escaneo de copia de memorando firmada y envió del archivo digital a Almacén.
7	Ingeniero de Sistemas	ARCHIVO DE DOCUMENTO FISICO: Se encarga de archivar la copia de memorando físico en el archivo de la Oficina.

2.3.1.2FLUJOGRAMA



2.3.2 MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE:

Esta actividad se desarrolla de acuerdo con la elaboración previa de un cronograma, el cual se socializa a través de correo electrónico a todos los funcionarios de la E.S.E.. Las evidencias quedan registradas en la Hoja de Vida de cada uno de los Equipos de Cómputo.

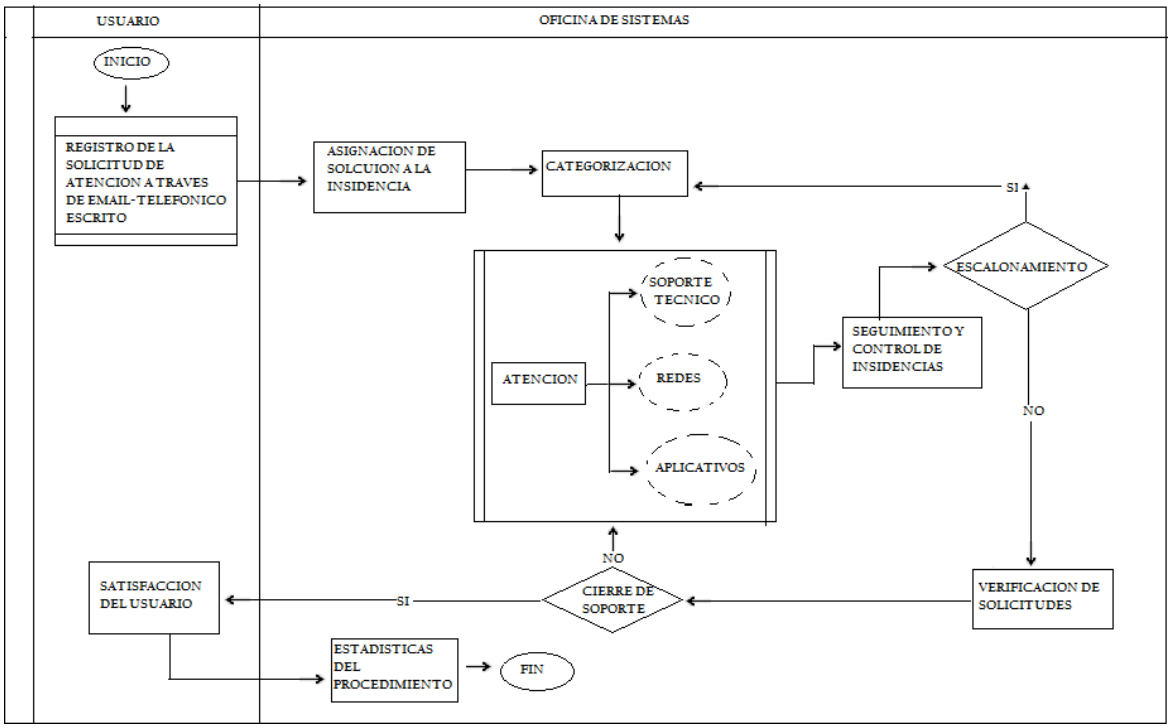
2.3.3 PROCEDIMIENTO SERVICIO MESA DE AYUDA

2.3.3.1 DESARROLLO DE ACTIVIDADES:

No	RESPONSABLE	DESCRIPCION DE ACTIIVDADES
1	Usuario Final /Funcionario	REGISTRO DE LA SOLICITUD DE ATENCIÓN A TRAVÉS DEL CORREO ELECTRONICO, LLAMADA TELEFONICA O SOLICITUD DE SOPORTE Comunicación con el ingeniero de sistemas. Realiza el reporte del incidente o problema. Recibe confirmación del registro de la incidencia.

2	Ingeniero de Sistemas	CATEGORIZACIÓN: Se categoriza la incidencia
3	Ingeniero de Sistemas	ASIGNACIÓN PARA SOLUCIONAR LA INCIDENCIA: El Ingeniero coordina a través del sistema de Mantenimiento la asignación de tareas. ATENCIÓN: Los incidentes o problemas serán atendidos en orden de llegada a la Oficina de sistemas y se asignan de acuerdo al tipo de incidente:
4	Ingeniero de Sistemas	DESPLAZAMIENTO A SITIO: Se desplaza a sitio y evalúa el incidente o problema. REVISIÓN Y SOLUCION: Ejecuta las acciones técnicas pertinentes para dar solución al incidente o problema. (Manteniendo correctivo, traslado de equipos y realización de pruebas de funcionamiento.) CIERRE SOPORTE: Desde sitio, si el incidente fue solucionado el técnico comunica vía telefónica al usuario. Si por el contrario es necesario escalar el incidente, se reporta a Almacén.
5	Ingeniero de Sistemas	SEGUIMIENTO Y CONTROL INCIDENCIAS: Realiza seguimiento desde el ingreso hasta el final del requerimiento.
6	Ingeniero de Sistemas	ESCALAMIENTO: Se notifica vía correo electrónico al Jefe de área y a Almacén el incidente o problema a escalar
7	Ingeniero de Sistemas	VERIFICACION DE SOLICITUDES: Verifica los seguimientos de cada solicitud
8	Ingeniero de Sistemas	CIERRE DE SOPORTE: Vía telefónica se valida el cierre del soporte mediante el concepto del usuario expresado en el seguimiento de verificación del servicio a través de la Oficina de Sistemas.
9	Ingeniero de Sistemas	SATISFACCIÓN DEL USUARIO: Se solicita a los usuarios la calificación en la encuesta de satisfacción del servicio

2.3.3.2FLUJOGRAMA



2.3.3.3GENERACION DE BACKUP DE PC:

Cada proceso y/o dependencia de la E.S.E. es responsable de su propia información. La oficina de Sistemas realiza Back up de la información a los computadores del personal administrativo y asistenciales de acuerdo a la solicitud realizada.

2.4

PROCEDIMIENTO CONTROL DE LICENCIAMIENTO ESPECIALIZADO:

Las licencias se encuentran en la oficina de Sistemas, y se lleva el control en

Almacén. 2.5

PROCEDIMIENTO ADMINISTRACION DE LOS SISTEMAS DE INFORMACION:

2.5.1AFINAMIENTO Y MONITOREO BASE DE DATOS:

- Responsabilidades del Afinamiento y Monitoreo de la Base de Datos:
- Monitorear las bases de datos

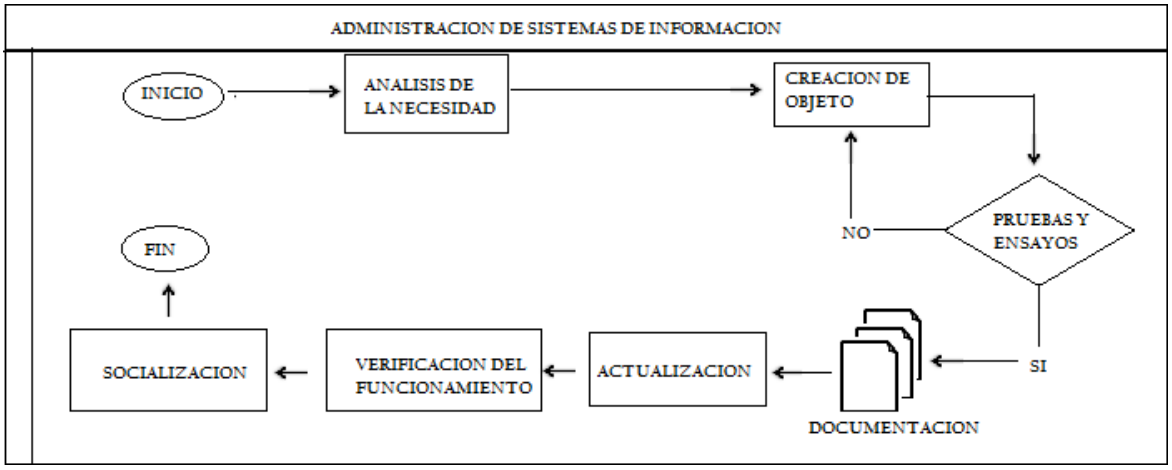
- Verificar el espacio libre de almacenamiento
- Revisar los archivos de registro (log's) de errores generados por el Sistema de Gestión de Bases de Datos
- Aplicar los ajustes necesarios para garantizar el funcionamiento de las bases de datos
- Monitorear las sentencias que se están ejecutando en base de datos
- Optimizar el desempeño de respuesta de las consultas bases de datos
- Mejorar la parametrización de la base de datos
- Depuración de archivos de log's y mantenimiento a la estructura del Sistema de Gestión de Bases de Datos.

2.5.2 ACTUALIZACION DE OBJETOS EN BASE DE DATOS Y CODIGO FUENTE EN APLICACIONES.

2.5.2.1 DESARROLLO DE ACTIVIDADES:

No	RESPONSABLE	DESCRIPCION DE ACTIIVDADES
1	Ingeniero de Sistemas	ANALISIS DE NECESIDAD: Análisis de la necesidad de los usuarios o del sistema
2	Ingeniero de Sistemas	CREACION DE OBJETO: Crear el objeto que soluciona el inconveniente.
3	Ingeniero de Sistemas	PRUEBAS Y ENSAYOS: Realizar las respectivas pruebas (que cumpla el objetivo)
4	Ingeniero de Sistemas	DOCUMENTACION: Documentar el código del objeto. Recepción de los archivos enviados por los programadores.
5	Ingeniero de Sistemas	ACTUALIZACION: Actualizar los archivos correspondientes. En caso de ser archivos nuevos se agregan al proyecto. Compilar el proyecto. Verificar errores de compilación.
6	Ingeniero de Sistemas	VERIFICACION DEL FUNCIONAMIENTO: Verificar el buen funcionamiento y servicio de los cambios realizados en el sistema de información.
7	Ingeniero de Sistemas	SOCIALIZACION: Se comunica a las partes interesadas y afectadas a través del correo institucional.

2.5.2.2FLUJOGRAMA



2.6

PROCEDIMIENTO CONECTIVIDAD Y REDES:

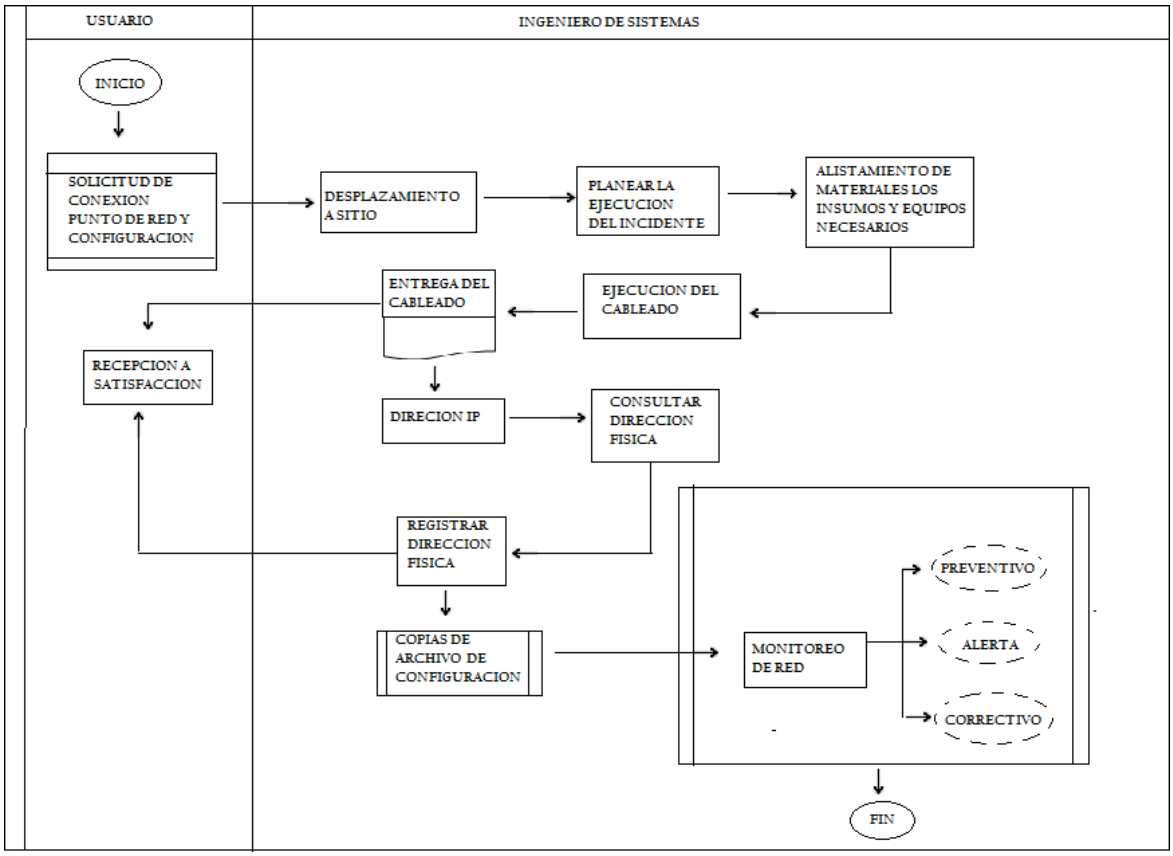
2.6.1PUNTOS DE CONEXIÓN FISICOSA LA RED (CABLEADO ESTRUCTURADO) CONFIGURACIÓN:

2.6.1.1DESARROLLO DE ACTIVIDADES:

No	RESPONSABLE	DESCRIPCION DE ACTIIVDADES
1	Usuario	SOLICITUD DE CONEXIÓN PUNTO DE RED Y CONFIGURACIÓN: Envía la solicitud a la Oficina de Sistemas tanto de implementación de establecer un punto. Para el caso de configuración de IP se pasa al paso No. 7 directamente.
2	Ingeniero de Sistemas	DESPLAZAMIENTO A SITIO: Desplazamiento a sitio para verificar, identificar y clasificar el tipo de incidente
3	Ingeniero de Sistemas	PLANEAR LA EJECUCIÓN DEL INCIDENTE: Se planifica la intervención para dar solución al incidente.
4	Ingeniero de Sistemas/Almacén	ALISTAMIENTO DE MATERIALES LOS INSUMOS Y EQUIPOS NECESARIOS: Se alista las herramientas, el material, los insumos y los equipos necesarios para el cableado, en caso de hacer falta algo, se debe realizar el pedido

5	Ingeniero de Sistemas	EJECUCIÓN DEL CABLEADO: Se desplaza al sitio donde se debe ejecutar la solución bajo los estándares de calidad (ISO/IEC 11801, ANSI/TIA/EIA 568-B, ANSI/EIA/TIA 569-A, ANSI/TIA/EIA 606-A). Que obedece a las normas de cableado estructurado
6	Usuario	ENTREGA DEL CABLEADO: Se diligencia el formato de entrega a satisfacción con el visto bueno del jefe de área.
7	Ingeniero de Sistemas	DIRECCIÓN IP: Se conecta al servidor DHCP por medio de un explorador web a través de una conexión segura (HTTPS) y se valida el usuario para permitir el ingreso al servidor.
8	Ingeniero de Sistemas	CONSULTAR DIRECCIÓN FÍSICA: Se debe verificar por medio de una búsqueda que la dirección física (MAC) y el nombre del host (equipo), no se encuentren registradas anteriormente para evitar duplicidad impidiendo errores en el registro.
9	Ingeniero de Sistemas	REGISTRAR DIRECCIÓN FÍSICA: Se ubica el segmento al que pertenece la IP dentro del archivo de configuración del servidor y se agrega la dirección física en una dirección IP libre, se aplican y guardan cambios.
10	Usuario	RECIBIDO DE DIRECCIÓN IP: Utilización de la dirección IP solicitada.

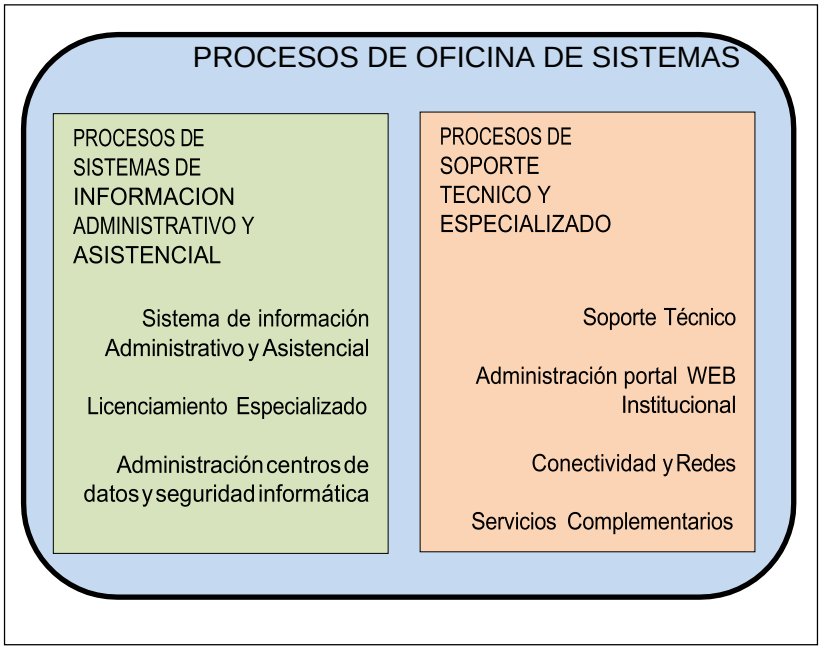
2.6.1.2 FLUJOGRAMA



3. CONTROL DE CAMBIOS:

Emisión inicial

Se establecieron los procesos de acuerdo a su evolución y mejora en la estandarización de cada uno de ellos y su paso a paso al interior de los procedimientos que a continuación se presentan.



CAPITULO 3

MANUAL DE POLITICAS, PROCEDIMIENTOS Y REGLAMENTO DEL AREA DE SISTEMAS DE LA E.S.E. HOSPITAL SAN RAFAEL DE SAN VICENTE DEL CAGUAN

1. ***DISPOSICIONES GENERALES***

1.1 AMBITO DE APLICACIONES Y FINES.

Las políticas de seguridad en cómputo tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes de telemática [voz y datos]) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de computo de la E.S.E. Hospital San Rafael.

La E.S.E. Hospital San Rafael a través de la oficina de sistemas es quien dará a conocer estas políticas de seguridad internamente.

1.2 DEFINICIONES

- **ABD:** Administrador de Base de Datos.
- **EHSR:** E.S.E. Hospital San Rafael
- **BD**: Base de datos.
- **AV**: Antivirus.
- **CONTRASEÑA:** Conjunto de caracteres que permiten el acceso a un usuario a un recurso informático (password)
- **RECURSO INFORMÁTICO**: Cualquier componente físico de un sistema de información.
  RED: Equipos de cómputo, sistemas de información y redes de telemática de la EHSR.
- **SII:** Sistema Integral de Información de la EHSR.
- **SITE**: Espacio designado en la entidad a los equipos de telecomunicaciones y servidores.
- **USUARIO:** cualquier persona (empleado o no) que haga uso de las tecnologías de la información proporcionadas por la EHSR.
- **VIRUS INFORMÁTICO:** programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento,

así como destrucción de daros, reducción del desempeño de la maquina o equipo de cómputo.

2. POLITICAS DE SEGURIDAD FISICA

2.1 ACCESO FISICO

- Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.

- El acceso de terceras personas deben ser identificadas plenamente, controlado y vigilado durante el acceso.
- Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas o con el debido permiso del responsable del área de sistemas.

- El personal autorizado para mover, cambiar o extraer equipos de cómputo de la EHSR es el responsable del área de sistemas, el cual notificara al área de Almacén para el debido descargue de los formatos de Entrada/Salida de materiales.

2.2 ROBO DE EQUIPO

- A partir de los procedimientos definidos por la EHSR, el área de almacén el definirá el procedimiento para inventario físico, firmas de resguardo para préstamo y usos dedicados de equipos de tecnología de información.

- El resguardo y/o responsabilidad de los equipos de comunicaciones deberá quedar asignado a la persona que lo usa o administra, permitiendo conocer siempre la ubicación física de los equipos.

- El centro de servidores, así como las áreas que cuentes con equipos de misión crítica deberán contar con vigilancia e ingresar solo personal autorizado.

2.3 PROTECCION FISICA

El SITE de la EHSR debe:

- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Ser un área restringida
- Estar libre de contacto de las instalaciones eléctricas en mal estado
- Contar por lo menos con dos extintores de incendio adecuado y cercano al centro de telecomunicaciones.
- El site deberá seguir los estándares vigentes para una protección adecuada de los equipos de telecomunicaciones so servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas del Site deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Cada vez que se requiera conectar equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.
- Contar con algún esquema que asegure la continuidad del servicio.
- Se deberá tener fácil acceso a los procedimientos de contingencias.

2.4 RESPALDOS

- Las Base de Datos de la EHSR serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Los respaldos de la ehsr deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

3. POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED DE LA EHSR

3.1 DE LA RED

- La Red de la EHSR tiene como propósito principal servir en la transformación e intercambio de información dentro de la entidad entre usuarios, técnicos, departamentos, oficinas.

- Si una aplicación en la red es coherente con los propósitos de la Red de la EHSR, entonces significa que las actividades necesarias para esa aplicación serán consistentes con los propósitos de la unidad de TIC.

- La Oficina de Sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

- No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus superiores correspondientes.

- No se permite el uso de los servicios de la red cuando no cumplan con los quehaceres propios de la institución.

- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la EHSR y se usarán exclusivamente para actividades relacionadas con la Institución.

- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

- El uso de analizadores de red es permitido única y exclusivamente por el personal de Sistemas, para monitorear la funcionalidad de la Red de la EHSR, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normas de La Oficina de Sistemas de la EHSR.

- No se permitirá el uso de analizadores para monitorear o censar redes ajenas a la EHSR y no se deberán realizar análisis de la Red de la EHSR desde equipos externos a la entidad.

- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de la normas de La Oficina de Sistemas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

3.2 DEL ÁREA DE SISTEMAS

- La Oficina de Sistemas debe llevar un control total y Sistematizado de los recursos de cómputo.

- El área de sistemas son los responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

- Los Jefes de Área deberán reportar a la oficina de sistemas cuando un usuario deje de laborar o de tener una relación con la empresa.

- Si un usuario o departamento viola las políticas vigentes de uso aceptable de la Red de la EHSR, los administradores de la Red lo aislará de la misma.

- Para reforzar la seguridad de la información de los usuarios, bajo su criterio, deberá hacer respaldos de la información en sus discos duros o solicitarla a la oficina de sistemas; dependiendo de la importancia y frecuencia del cambio de la misma.

- Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

4. POLÍTICAS DE USO ACEPTABLE DE LOS USUARIOS

4.1 LOS RECURSOS DE CÓMPUTO EMPLEADOS POR EL USUARIO:

- Deberán ser afines al trabajo desarrollado.
- No deberán ser proporcionados a personas ajenas.
- No deberán ser utilizados para fines personales.

- Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

- El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, ect).

- Para reforzar la seguridad de la información de su cuenta, el usuario –conforme su criterio- deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los usuarios

- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un manifiesto donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de la EHSR, de acuerdo con las políticas que en este documento se mencionan.

- Los usuarios deberán solicitar apoyo al Oficina de Sistemas ante cualquier duda en el manejo de los recursos de cómputo de la institución.

4.2 DE LOS SERVIDORES DE LA RED DE EHSR.

- La Oficina de Sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

- La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de la Oficina de Sistemas.

- Durante la configuración del servidor la Oficina de Sistemas deben normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

- Los servidores que proporcionen servicios a través de la RED e Internet deberán:

a) Funcionar 24 horas del día los 365 días del año.
b) Recibir mantenimiento preventivo máximo dos veces al año
c) Recibir mantenimiento semestral que incluya depuración de bitácoras.
d) Recibir mantenimiento anual que incluya la revisión de su configuración.
e) Ser monitoreados por La Oficina de Sistemas de la entidad y por el Centro

de Operaciones de la Red de la EHSR.

- La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

a) Diariamente, información crítica.
b) Semanalmente, los correos y los documentos web.
c) Mensualmente, configuración del servidor.

- Los servicios institucionales hacia Internet sólo podrán proveerse a través de los servidores autorizados por la Oficina de Sistemas.

- La oficina de Sistemas se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.

- Para efecto de asignarle su cuenta de correo al usuario, éste deberá llenar una solicitud en formato libre y entregarlo al área de sistemas, con su firma y la del Jefe de área.

- Una cuenta deberá estar conformada por el nombre del área y su contraseña asignada. La sintaxis de la cuenta de correo será: area@hospitalsanrafael.gov.co y no deberá contener alias.

- La cuenta será activada en el momento en que el usuario se prE.S.E.nte en la oficina de sistemas, para teclear y verificar de manera personal su contraseña de acceso.

- Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones:

a) Acceso restringido.
b) Temperatura adecuada al equipo.
c) Protección contra descargas eléctricas.
d) Mobiliario adecuado que garantice la seguridad de los equipos.

- En caso de olvido de la contraseña por parte del usuario, podrá apoyarse con el área de sistemas para el cambio de contraseña.

4.3 DE LOS SISTEMAS INSTITUCIONALES DE INFORMACIÓN

- El Ingeniero de Sistemas tendrá acceso a la información de la Base de Datos únicamente para:

a) La realización de los respaldos de la BD.

b) Solucionar problemas que el usuario no pueda resolver.
c) Diagnóstico o monitoreo.

- El Ingeniero de Sistemas no deberá eliminar ninguna información del sistema,
- a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

- El Ingeniero de Sistemas es el encargado de asignar las cuentas a los usuarios para el uso. Para tal efecto será necesario seguir el procedimiento determinado para tal efecto.

- Las contraseñas serán asignadas por el Ingeniero de Sistemas en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Ingeniero de Sistemas para reasignarle su contraseña.

5. POLÍTICAS DE SEGURIDAD LÓGICA PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO

5.1 ÁREA DE SEGURIDAD EN CÓMPUTO

- La Oficina de Sistemas es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

- La Oficina de Sistemas debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

- La Oficina de Sistemas es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

5.2 ADMINISTRADORES DE TECNOLOGÍAS DE INFORMACIÓN

- La Oficina de Sistemas debe cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito por las Gerencias en los siguientes casos:

a) Si la cuenta no se está utilizando con fines institucionales.
b) Si pone en peligro el buen funcionamiento de los sistemas.
c) Si se sospecha de algún intruso utilizando una cuenta ajena.

- La Oficina de Sistemas deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

- La Oficina de Sistemas deberá utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

- La Oficina de Sistemas deberá realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

- La Oficina de Sistemas debe actualizar la información de los recursos de cómputo de la entidad, cada vez que adquiera e instale equipo o software.

- La Oficina de Sistemas debe registrar cada máquina en el inventario de control de equipo de cómputo y red de la entidad.

- La Oficina de Sistemas debe auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

- La oficina de sistemas debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

- Es responsabilidad de La Oficina de Sistemas revisar periódicamente las bitácoras de los sistemas a su cargo.

- la oficina de sistemas reportará a la Dirección los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

5.3 RENOVACIÓN DE EQUIPO

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta a la oficina de sistemas a fin de que se seleccione el equipo adecuado. Sin el Visto Bueno de La Oficina de Sistemas no podrá liberarse una requisición de compra de TIC o de equipo.

6. POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DE SERVICIOS DE RED

6.1 SERVICIOS EN LAS GERENCIAS Y EDIFICIOS

- Los Jefes de área definirán los servicios de Internet a ofrecer a los usuarios y se coordinará con La Oficina de Sistemas para su otorgamiento y configuración.

- Los Jefes de área pueden utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización de La Oficina de Sistemas.

- La Oficina de Sistemas es el responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

- Los Jefes de área deberán notificar a La Oficina de Sistemas cuando un usuario deje de prestar sus servicios a la empresa.

- La Oficina de Sistemas realizará las siguientes actividades en los servidores de la empresa:

a) Respaldo de información conforme a los procedimientos indicados por el centro de operaciones.
b) Revisión de bitácoras y reporte cualquier eventualidad al Centro de Operaciones de la RED.
c) Implementar de forma inmediata las recomendaciones de seguridad proporcionados y reportar a la Dirección posibles faltas a las políticas de seguridad en cómputo.
d) Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
e) Calendarizar y organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

- La Oficina de Sistemas es el único autorizado para asignar las cuentas a los usuarios con previa anuencia de Los Jefes de área.

- La Oficina de Sistemas aislará cualquier servidor de red, notificando a la gerencia y áreas de la entidad, en las condiciones siguientes:

a) Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
b) Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
c) Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
d) Si se detectan accesos no autorizados que comprometan la integridad de la
e) información.
f) Si se viola las políticas de uso de los servidores.
g) Si se reporta un tráfico adicional que comprometa a la red de la Entidad.

6.2 USO DE LOS SERVICIOS DE RED POR LOS USUARIOS

- El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.

- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de La Oficina de Sistemas, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

a) Cuando ésta sea una contraseña débil o de fácil acceso.
b) Cuando crea que ha sido violada la contraseña de alguna manera.

- El usuario deberá notificar a la oficina de sistemas en los siguientes casos:

a) Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
b) Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

- Si un usuario viola las políticas de uso de los servidores, La Oficina de Sistemas podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a la gerencia correspondiente.

7. POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DEL ANTIVIRUS INSTITUCIONAL

7.1 ANTIVIRUS DE LA RED

- Deberán ser utilizadas en la implementación y administración de la Solución Antivirus, todos los equipos de cómputo de la EHSR.

Periódicamente se hará el rastreo en los equipos de cómputo de la EHSR, y se realizará la actualización de las firmas antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

7.2 POLÍTICAS ANTIVIRUS.

- La Oficina de Sistemas será el responsable de:
a) Implementar la Solución Antivirus en las computadoras de la entidad.
b) Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente. Configurar el analizador de red para la detección de virus.

- El administrador de la Red aislará el equipo o red, notificando a la Gerencia correspondiente, en las condiciones siguientes:
a) Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros Equipos y redes.
b) Si el usuario viola las políticas antivirus.
c) Cada vez que los usuarios requieran hacer uso de discos, USB's, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de Sistemas de EHSR.

- En caso de contingencia con virus La Oficina de Sistemas deberá seguir el procedimiento establecido.

7.3 USO DEL ANTIVIRUS POR LOS USUARIOS

- El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.

- El usuario que cuente con una computadora con recursos limitados, contará con la versión ligera de la Solución Antivirus Institucional.

- El usuario deberá comunicarse con La Oficina de Sistemas en caso de problemas de virus para buscar la solución.

- El usuario será notificado por La Oficina de Sistemas en los siguientes casos:

a) Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
b) Cuando sus archivos resulten con daños irreparables por causa de virus.
c) Cuando viole las políticas antivirus.

8. POLÍTICAS DE OPERACIÓN DE LOS CENTROS DE CÓMPUTO

- La Oficina de Sistemas podrá ofrecer servicios de cómputo, soporte técnico y servicios audiovisuales en las salas de juntas de la entidad.

- La administración de los servicios de la Red deberá llevarse a través de métodos Automatomatizados de La Oficina de Sistemas.

- La oficina de sistemas deberán verificar el grado de seguridad del software adquirido e instalado en los equipos.
-
- Se podrá dar asesoría siempre y cuando no entorpezca las acciones de mayor relevancia.
- El personal de informática dará soporte técnico únicamente al equipo de cómputo de la entidad.

- La instalación de Software específico deberá ser realizada en conjunto y común acuerdo del usuario que lo solicite y La Oficina de Sistemas.

CAPITULO 4

PLAN DE CONTINGENCIA INFORMATICO
E.S.E. HOSPITAL SAN RAFAEL

1. OBJETIVOS

1.1 GENERAL

Definir las acciones y procedimientos necesarios para garantizar la rápida y oportuna recuperación y puesta en operación de los sistemas y servicios informáticos que apoyan el cumplimiento de la misión de la entidad y los procesos administrativos críticos, frente a la posible ocurrencia de un incidente de seguridad que comprometa total o parcialmente la prestación de los servicios informáticos de la E.S.E. Hospital San Rafael

1.2. ESPECÍFICOS

- Asignar las responsabilidades al recurso humano identificado y debidamente capacitado en cada uno de los procedimientos necesarios para ejecutar el plan de contingencia, garantizando la restauración de la operación informática en el tiempo requerido.

- Disponer de procesos y procedimientos claros para atender cualquier evento de seguridad que afecte la disponibilidad de los recursos informáticos críticos, para garantizar la continuidad de los servicios informáticos.

- Realizar simulacros de restauración que garanticen el éxito de los procesos y procedimientos contenidos en el plan de contingencias, aumentando niveles de confiabilidad y disponibilidad de los sistemas y servicios informáticos de la E.S.E. Hospital San Rafael

2. ALCANCE

El plan de contingencia informático cubre específicamente los eventos o incidentes de seguridad que comprometan total o parcialmente la operación informática de la entidad, estableciendo los procedimientos necesarios para restablecer la prestación de los servicios informáticos de forma eficaz y oportuna.

3. DEFINICIONES

- Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

- Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

- Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

- Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de las salvaguardas, o de una situación desconocida previamente que puede ser pertinente a la seguridad.

- Incidente de seguridad: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio, y amenazar la seguridad de la información.

- Sistemas y servicios informáticos de la entidad: Correo, Bases de datos, Internet, Directorio Activo (Claves de acceso), Sistemas operativos (Windows XP, Windows 7, Windows Server, Linux).

- Firewall: Dispositivo de seguridad perimetral entre redes para evitar que los intrusos puedan acceder a información institucional confidencial, a través de la aplicación de políticas que permiten o no el acceso a los sistemas y servicios informáticos de la entidad, de acuerdo a los roles y responsabilidades de los usuarios.

4. DIAGNÓSTICO DE SITUACIÓN ACTUAL

- Diagnostico Infraestructura

Actualmente La E.S.E. Hospital San Rafael no cuenta con un procedimiento alternativo que muestre un modelo vigente de relevamiento de la infraestructura tecnológica en caso de materialización de un incidente de seguridad que comprometa total o parcialmente la operación informática.

Las bases de datos de los aplicativos, tanto la administrativa como la de facturación, cuentan con un sistema de respaldo automático, incremental, diario,

semanal, mensual y anual, en medio magnético, en cumplimiento del documento institucional vigente referente a la gestión de Backup's, control implementado que minimiza el riesgo de pérdida de información en caso de la materialización de riesgos informáticos.

5. ANALISIS Y VALORACION DE RIESGOS

- Determinación de áreas de riesgo

Los riesgos derivados del uso de las tecnologías de información y comunicaciones como una de una de las principales herramientas de apoyo al cumplimiento de la misión de La E.S.E. Hospital San Rafael, se centran en la infraestructura tecnológica que soporta la operación informática de la entidad principalmente en tres áreas: bases de datos, servicios de información y administrativos y seguridad informática (comunicaciones), cercanamente interrelacionadas.

Las bases de datos están alojadas en los servidores ubicados en el centro de cómputo de servidores en el nivel central en La E.S.E. Hospital San Rafael, el cual no cuenta con un esquema de alta disponibilidad en cuanto a suministro eléctrico.

Con base en el conocimiento de la Oficina de Sistemas de La E.S.E. Hospital San Rafael en el mantenimiento preventivo y correctivo de administración de los sistemas y servicios informáticos, y desarrollo del Sistema de Gestión de Seguridad de la Información, se realiza la identificación de los riesgos que pueden comprometer total o parcialmente el funcionamiento de los activos de tecnologías de la información y comunicaciones de La E.S.E. Hospital San Rafael.

Tabla No. 1
Riesgos Informáticos

AMENAZA	VULNERABILIDAD
Medio ambiente e infraestructura	Controles de acceso a centro de datos inadecuados
	Suministro eléctrico inestable
	Desastres naturales
	Desastres ocasionados por el hombre
	Inadecuado sistema de prevención de atención de desastres
Recurso Humano	Contratación inadecuada
	Ausentismo
	Roles y responsabilidades inadecuados Falta de conciencia alrededor de la seguridad informática
	Falta de capacitación
	Falta de procedimientos oficiales
	Desastres ocasionados por el hombre
Software (Malware)	Falta de conciencia alrededor de la seguridad informática
	Software malicioso
	Exposición de contraseñas de acceso a servicios informáticos
	Falta de documentación
Hardware	Daño
	Degradación
	Plan de mantenimiento preventivo inapropiado
	Suministro eléctrico inestable
Comunicaciones	Falta de esquemas de alta disponibilidad (respaldo)
	Administración de red inadecuada
Datos (Información)	Inadecuada clasificación de activos
	Software malicioso
	Protección inadecuada de bases de datos
	Falta de plan de procedimientos y software de respaldo

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

6. SISTEMAS Y SERVICIOS INFORMATICOS CRÍTICOS

Los riesgos derivados del uso de Tecnologías de información y comunicaciones que pueden afectar total o parcialmente el correcto funcionamiento de los sistemas y servicios informáticos de La E.S.E. Hospital San Rafael, hacen necesario la identificación de los procesos Críticos al interior de la entidad, a fin de contar con procedimientos alternos que garanticen la continuidad en su operación informática.

7. DEFINICIÓN DE LOS PROCEDIMIENTOS DE RECUPERACIÓN

Para la definición de los procedimientos a seguir al identificar situaciones de falla, se requiere la ejecución de actividades tales como la creación de grupos responsables del plan de contingencia por cada área, definir los procesos y pasos a seguir en caso de la presencia identificada de los riesgos detectados, definir los medios o alternativas de respaldo y por último definir el plan retorno que facilite el normal funcionamiento de la operación informática de La E.S.E. Hospital San Rafael

- Creación de Grupos

✓ Grupo Coordinador

Es el Grupo encargado de coordinar todas las actividades propias del plan de contingencia así como los otros grupos, este grupo es el responsable de que la solución de la eventualidad y/o emergencia tenga el mayor éxito posible y está conformado por:

- Profesional Universitario - Ingeniero de Sistemas
- Gerente
-

El grupo coordinador es responsable de las siguientes funciones:

- Definir lineamientos del plan de contingencia para el área de Sistemas.
- Orientar y evaluar el desarrollo del plan.
- Efectuar seguimiento y controlar costos del desarrollo, implantación y mantenimiento del plan.

✓ Grupo de recuperación de servicios informáticos.

Conformado por los Coordinadores de cada área de La E.S.E. Hospital San Rafael, quienes harán la selección del recurso humano conformado por funcionarios, contratistas y proveedores que sean requeridos para apoyar la ejecución del Plan y tomar las medidas necesarias según sea el caso de acuerdo a los procesos que realicen en desarrollo de las labores contractuales.

Este grupo tiene las siguientes funciones:

Efectuar cada una de las actividades definidas en el plan de contingencia
Diseñar planes de entrenamiento para los funcionarios, contratistas y proveedores
Diseñar cronogramas y apoyar logísticamente
Mantener actualizado el plan de contingencia.

CAPITULO 5

POLITICAS DE ACTIVACION E INACTIVACION

DE CUENTAS DE USUARIO

Según registra el manual de políticas, procedimientos y reglamento del área de sistemas de la E.S.E. Hospital San Rafael, existen unos parámetros para la activación y desactivación de cuentas de usuarios para el manejo de las plataformas, sistemas operativos, software y correos electrónicos institucionales; mencionados a continuación:

- La oficina de Sistemas se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
- Para efecto de asignarle su cuenta de correo al usuario, éste deberá llenar una solicitud en formato libre y entregarlo al área de sistemas, con su firma y la del Jefe de área.
- Una cuenta deberá estar conformada por el nombre del área y su contraseña asignada. La sintaxis de la cuenta de correo será: nombrearea@hospitalsanrafael.gov.co y no deberá contener alias.
- La cuenta será activada en el momento en que el usuario se presente en la oficina de sistemas, para teclear y verificar de manera personal su contraseña de acceso.
- Las contraseñas serán asignadas por el Ingeniero de Sistemas en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.
- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Ingeniero de Sistemas para reasignarle su contraseña.
- La Oficina de Sistemas debe cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito por las Gerencias en los siguientes casos:

- Si la cuenta no se está utilizando con fines institucionales.
- Si pone en peligro el buen funcionamiento de los sistemas.
- Si se sospecha de algún intruso utilizando una cuenta ajena.

- Los Coordinadores de área deberán reportar a la oficina de sistemas cuando un usuario deje de laborar o de tener una relación con la empresa.

- La Oficina de Sistemas es el responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de La Oficina de Sistemas, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

- Cuando ésta sea una contraseña débil o de fácil acceso.
- Cuando crea que ha sido violada la contraseña de alguna manera.

- El usuario deberá notificar a la oficina de sistemas en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

Los funcionarios a activar cuentas según los Aplicativos activos son:

SISTEMA DE INFORMACION	AREA	DEPENDENCIA	USUARIO	MODULO	ROL
HASSQL	ADMINISTRATIVA	Subgerencia administrativa y financiera	Subgerente	Presupuesto	Ingresos y Gastos
			Aux. Administrativo	Presupuesto	CDP-RP
		Contabilidad	Coordinadora Financiera	Contabilidad	Administrador
				Presupuesto	
				Nomina	
				Almacén e Inventarios	
			Aux. Administrativo	Contabilidad	Registros
				Nomina	Interfaces
		Recursos Humanos	Aux. Administrativo	Nomina	Nomina
		Suministros	Aux. Administrativo	Almacén e inventarios	Entradas-Salidas e Inventarios

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

		Pagaduría	Aux. administrativo	Contabilidad	Comprobantes
	ASISTENCIAL	Farmacia	Regente	Almacén e inventarios	Salidas
	SISTEMAS	Sistemas	Profesional Universitario-Ing de	Contabilidad Presupuesto Nomina Almacén e Inventarios	Administrador
CADUCEOS	FACTURACION	Técnico Supervisor	Tec. Administrativo	Facturación Validador Rips CPSS Reportes	Supervisión, Contratos, Anulación y Validación
		Cajas de Facturación	Aux. administrativos	Facturación	Facturador – Digitador –Agenda
		Estadística	Aux. administrativo	Facturación Validación Reportes	Digitador
	SIAU	Trabajo Social	Trabajadora Social	Facturación	Agenda
	ASISTENCIAL	Farmacia	Tec. Regente Farmacia	Farmacia	Digitador-Evaluador
		Consulta Externa -Urgencias –UBA-Sala de Partos – Hospitalización –Laboratorio Clínico	Profesionales de la Salud-	Historia Clínica	Médico Odontólogo Bacteriólogo Psicólogo Enfermeras
		Hospitalización - Sala de Partos - Urgencias -UBA	Auxiliares área de la Salud-	Historia Clínica	Auxiliares de Enfermería
		Consulta Externa - UBA	Tec. Higienista Oral	Historia Clínica	Higiene Oral
		Coordinación Resolutiva	Coordinación Resolutiva	Historia Clínica	Verificador Digitador Medico
		Subgerencia Servicios de Salud	Subgerente Servicios de Salud	Historia Clínica	Verificador
	FACTURACION	Tec. Administrativo	Tec. Administrativo	Historia Clínica	Verificador
	SISTEMAS	Sistemas	Profesional Universitario-Ing de sistemas	Facturación CPSS Reportes Validación Rips 4505 EMS Depurador Farmacia Historia Clínica	Administrador
ANTRO	PYP	Crecimiento y Desarrollo	Aux. de la Salud	Antro Antro Plus	Digitador

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

Los funcionarios a activar cuentas de correo electrónico son:

- Coordinadores de área
- Dependencias que manejen información interinstitucional.

No se permite generar contraseña a los equipos de cómputo sin previo aviso al área de sistemas.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

CAPITULO 6

REGLAMENTO DE LOS CENTROS DE CÓMPUTO

INTRODUCCIÓN

Con el objeto de proporcionar un buen servicio y adecuado manejo de los equipos existentes, La Oficina de Sistemas ha elaborado el presente reglamento.

Objetivo: Proporcionar servicios de cómputo integral y eficiente para los empleados de la EHSR.

GENERALES

1. Únicamente pueden ser usuarios de los recursos de TIC:
a) Los empleados de la entidad.
b) Las personas externas previa firma de convenio o autorización de un mando superior.

2. El Personal de La Oficina de Sistemas estará disponible para contingencias mayores o críticas las 24 horas del día durante los 365 días del año.

3. Para tener derecho a los servicios:
a) Se atenderán las peticiones de los usuarios asignándole el equipo que cubra las expectativas avanzadas para desarrollar sus actividades, las cuales podrán ser de manera individual o por grupo.
b) En caso de:
c) Solicitud de soporte Individual: El usuario deberá utilizar el sistema de Soporte Informático, que para tal efecto estará disponible en todos los equipo de la red.
d) Solicitud de soporte para eventos especiales: Las realizará en forma de e-mail el Coordinador de área correspondiente señalando el detalle del soporte y con un mínimo de 24 horas previo al evento.

4. Tiempo de respuesta a solicitudes de soporte:
Las Solicitudes de soporte individual serán atendidas, sin ninguna excepción, el mismo día que se realicen, siempre y cuando sean en horas de oficina.

5. Cancelación de solicitudes de soporte:

El personal de informática en común acuerdo con el usuario podrá cancelar una solicitud que no proceda, señalando la causa en el cuerpo de la misma.

6. Servicios:

a) Los usuarios deberán respetar las especificaciones que los equipos tengan con respecto al software instalado en general.
b) El equipo de cómputo asignado, son de uso exclusivo para un usuario
c) Los usuarios solo podrán utilizar el equipo de cómputo que les sea asignado. En caso que éste tenga alguna anomalía, deberán reportarlo mediante el sistema de soporte, para que se le corrija la anomalía.
d) El usuario que requiera el uso de software especial que no se encuentre instalado o provisto de manera institucional, deberá solicitarlo a La Oficina de Sistemas, previa justificación que la sustente.
e) Los usuarios deberán contar con sus discos de trabajo para efectuar los respaldos de su información.

7. La instalación y desinstalación de programas es facultad exclusiva del personal de Informática, si el resguardatario del equipo instala un programa sin previa autorización, cualquier consecuencia por dicha instalación será responsabilidad del usuario.

8. Derechos de autor.

Queda estrictamente prohibido inspeccionar, copiar y almacenar software que viole la ley de derechos de autor.

9. La Oficina de Sistemas no se hace responsable de la información de los usuarios almacenada en los discos duros de los equipos de cómputo.

10. El Departamento de Informática se rE.S.E.rva el derecho de cancelar el servicio total de la TIC en caso de una emergencia mayor.

11. Equipo ajeno a la institución:

El usuario que requiera conectar equipos personales a la red o periféricos a las computadoras, deberán contar con la autorización correspondiente de La Oficina de Sistemas, y no será responsabilidad de esta, si el equipo sufre un daño o contaminación por virus. En caso de que un usuario, sin autorización, conecte un equipo o periférico personal al sistema de red de la entidad y este ocasione un daño o contaminación de virus, será total responsabilidad del usuario y se aplicaran las sanciones correspondientes.

DERECHOS Y ATRIBUCIONES

1. Son derechos de los usuarios de los recursos de TIC:

a) Hacer uso de los servicios de cómputo proporcionados por la entidad
b) Reservar el equipo de cómputo para su uso.
c) Solicitar una cuenta personalizada a La Oficina de Sistemas.
d) Respaldar información en su cuenta personalizada y/o unidades extraíbles.
e) Disponer del equipo de cómputo durante el tiempo establecido por la entidad.
f) Recibir la capacitación requerida de los programas alojados en su equipo en la fecha y horario que estipule La Oficina de Sistemas.
g) Recibir este reglamento

2. Son derechos de los usuarios Jefes de área:

a) Determinar a qué empleados de su área se le proporcionará servicios de navegación en Internet y las paginas habilitadas.
b) Determinar a qué usuario de su área se le proporcionará servicio de mensajería instantánea.

3. Son atribuciones de La Oficina de Sistemas:

a) Presupuestar los recursos de TIC
b) Determinar las configuraciones y alcances de los equipos y software de la entidad
c) Hacer estudios previos sobre todos los equipos, sistemas, refacciones y servicios relacionados con la TIC
d) Determinar la distribución de los equipos en función a las cargas de trabajo

OBLIGACIONES

Son obligaciones del usuario de los recursos de TIC:

a) Cuidar su equipo de no sufrir daño físico.
b) Notificar a La Oficina de Sistemas cualquier anomalía en su equipo y/o programas de cómputo.
c) Vacunar sus discos y cuidar que no contaminen el sistema de red de la entidad.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

d) Cerrar correctamente su sesión como usuario de la red.
e) Limpiar y acomodar su área de trabajo al término de su sesión y apagar el equipo de cómputo (CPU, Monitor, Periféricos, Reguladores y Fuentes de Poder).

RESTRICCIONES

Queda estrictamente prohibido al usuario:

a) Consumir alimentos, bebidas, fumar y tirar basura, mientras esta usando la computadora.
b) Conectar cualquier equipo ajeno a la empresa sin autorización.
c) Transferir su cuenta asignada por La Oficina de Sistemas.
d) Modificar los parámetros de configuración de hardware y software instalado.
e) Mover el equipo de cómputo y cambiar los cables de conexión a la red.
f) Conectarse a equipos no autorizados.
g) Realizar trabajos con fines de lucro.
h) Utilizar cualquier tipo de juego.
i) Utilizar programas de plática en línea (chat's) sin autorización.
j) Utilizar la infraestructura de la entidad para lanzar virus.
k) Utilizar la infraestructura de la entidad para realizar ataques internos o externos.
l) Introducir cualquier objeto que genere o emita magnetismo o electromagnetismo.
m) Acceder a información que pueda dañar la imagen de la Entidad: faltas a la moral y a las buenas costumbres.
n) Ingresar a las áreas exclusivas del personal del Centro de Cómputo.

SANCIONES

Las sanciones a que están sujetos los usuarios por incumplimiento de sus obligaciones e incurrir en las restricciones señaladas, son las siguientes:

a) Llamada de atención de manera verbal o escrita.
b) Suspensión temporal de los servicios de la Red.
c) Suspensión definitiva de los servicios de la Red.
d) Reposición o pago de los bienes extraviados, destruidos o deteriorados.
e) Sanciones disciplinarias de acuerdo a la ley 734 de 2012 de ser necesario.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

Anexo Recomendaciones para Centros de Cómputo

Recomendaciones de uso para el Equipo Multimedia y Equipo de Cómputo.

1. Usarse en áreas con aire acondicionado
2. Conectarse a tomas de corriente regulada, si están disponibles.
3. Mantenerse alejados de alimentos y bebidas.
4. No forzar las conexiones de los dispositivos de los equipos (éstos sólo pueden
5. conectarse de una forma).
6. Ubicar los equipos de tal forma que el calor generado por éstos no incida sobre
7. equipos de cómputo.
8. No mover ni golpear los equipos cuando están encendidos.
9. Poner los equipos en modo de reposo (stand-by) durante al menos 5 minutos antes de apagarlos de manera definitiva.
10. Al terminar, enrollar los cables y acomodarlos para un transporte seguro. Sin embargo, los cables no deben enrollarse con radios de curvatura muy pequeños, ya que pueden fracturarse.
11. No colocar los proyectores o cañones sobre computadoras portátiles ya que la pantalla líquida puede dañarse.
12. Evitar dejar sin vigilancia los equipos.

De las Impresiones

Impresión de trabajos.

1. Para impresiones de “trabajo” se utilizarán hojas recicladas.
2. Cada Jefe de área solicitará el papel de impresión y será responsable de su buen uso.
3. Solo se utilizará tonners, cintas y tintas originales.
4. No se imprimirán trabajos con fines de lucro ni aquellos que no tengan relación con la Entidad.

Imprevistos
Los casos no previstos en este reglamento serán resueltos por La Oficina de Sistemas y la Gerencia de la entidad.

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas

Vigencia

Este Plan Estratégico de Tecnología de la Información – PETI de la Empresa Social del Estado de San Vicente del Caguán, rige a partir de su firma y con vigencia de 4 años 2020-2023.

MARLON MAURICIO MARROQUIN GONZALES
Gerente

JOHANA ANDREA OBREGON ENCISO
M.P. N° 70255205193TLM
Profesional Universitario Ingeniera de Sistemas

Elaboro: Johana Andrea Obregón E.
Ingeniera de Sistemas