



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL**  
**EMPRESA SOCIAL DEL ESTADO**  
**NIT. 891900441-1**



**RESOLUCIONES**

**CÓDIGO: P-GDG 01    VERSIÓN: 2    FECHA: 01/02/2014    TRD: 24-07    PÁGINA: 1 de 3**

**RESOLUCIÓN No.0105 DE 2020**  
**(Enero 24)**

**“POR LA CUAL SE ADOPTAN LOS PLANES EN MATERIA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES VIGENCIA 2020, DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.”**

El Gerente del Hospital Departamental San Rafael de Zarzal Empresa Social del Estado, en uso de sus atribuciones legales, en especial de las conferidas por el Artículo 4 del Decreto No.0139 de 1996 y su concordante el Artículo 2 del Decreto No.2768 del 28 de diciembre de 2012, otorgados por el Gobierno Nacional y demás normas concordantes, y

**CONSIDERANDO:**

1. Que el Decreto No.1413 de 2017, en su artículo 2.2.17.6.6, señala que los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integralidad y disponibilidad de los activos de información.
2. Que en el marco del Decreto 1078 de 2015, contempló en el artículo 2.2.9.1.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI).
3. Que el Decreto 1078 de 2015 contempló en el artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información.
4. Que la Ley 1712 de 2014, formula la metodología para la elaboración del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), cuyo fin es el fortalecimiento de la seguridad de la información y garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la E.S.E., a fin de contribuir al fortalecimiento institucional y consolidar la transparencia, eficacia, acceso y modernización de la información.



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL  
EMPRESA SOCIAL DEL ESTADO  
NIT. 891900441-1**



**RESOLUCIONES**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 2 de 3

**RESOLUCIÓN No.0105 DE 2020  
(Enero 24)**

**“POR LA CUAL SE ADOPTAN LOS PLANES EN MATERIA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES VIGENCIA 2020, DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.”**

5. Que mediante Decreto 415 del 7 de marzo de 2016, se adicionó al Decreto 1083 de 2015, todo lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.
6. Que mediante el Decreto 612 de 4 de abril de 2018, se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

En merito a lo anterior, este Despacho

**RESUELVE:**

**ARTÍCULO PRIMERO:** Adoptar los planes en materia de tecnologías de la información y las comunicaciones vigencia 2020, del Hospital Departamental San Rafael de Zarzal E.S.E., que a continuación se relacionan:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI.
- Plan de Seguridad y Privacidad de la Información.
- Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información.

Los planes institucionales en materia de tecnologías de la información y las comunicaciones aquí adoptados hacen parte integral del presente acto administrativo.

**ARTÍCULO SEGUNDO:** Ordénese la publicación de los planes en materia de Tecnologías de la Información y las Comunicaciones del Hospital Departamental San Rafael de Zarzal E.S.E., para la vigencia 2020, en la página web institucional.

**ARTÍCULO TERCERO.** La presente Resolución rige a partir de la fecha de su expedición y modifica las que le sean contrarias.

**PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE**



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL**  
**EMPRESA SOCIAL DEL ESTADO**  
**NIT. 891900441-1**

**RESOLUCIONES**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 3 de 3



**RESOLUCIÓN No.0105 DE 2020**  
**(Enero 24)**

**“POR LA CUAL SE ADOPTAN LOS PLANES EN MATERIA DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES VIGENCIA 2020, DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.”**

Dada en Zarzal, Valle del Cauca, a los veinticuatro (24) días del mes de enero de dos mil veinte (2020).

  
**Jorge Luis de Jesús Bedoya Hincapié**  
Gerente E.S.E.

*Proyectó: Gloria Maria Trujillo Villada, Subgerente.*  
*Revisó: José Jair Gutiérrez Corrales. Asesor Jurídico.*  
*Aprobó: Jorge Luis de J. Bedoya Hincapié. - Gerente E.S.E.*  
*Transcribió: Elizabeth Valencia A.*



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**

**SISTEMAS DE INFORMACION**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y**  
**PRIVACIDAD DE LA INFORMACION**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 1 de 15



# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**HOSPITAL DEPARTAMENTAL  
SAN RAFAEL DE ZARZAL E.S.E**



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**



**SISTEMAS DE INFORMACION**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y**  
**PRIVACIDAD DE LA INFORMACION**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 2 de 15

## Contenido

1. PRESENTACIÓN .....	3
2. TERMINOS .....	3
3. OBJETIVOS .....	7
Objetivo General .....	7
Objetivos Específicos .....	7
4. PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	8
5. CUMPLIMIENTO DE IMPLEMENTACIÓN .....	9
6. CRONOGRAMA .....	9
DIAGNOSTICO E IDENTIFICACION DE RIESGOS .....	10

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## 1. PRESENTACIÓN

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación del componente de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos de los usuarios, garantizando la seguridad de la información.

## 2. TERMINOS

- **Acceso a la Información Pública** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.
- **Archivo** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).  
Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría Proceso sistemático**, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización Consentimiento previo**, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y</b> <b>PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- **Bases de Datos Personales** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control Las políticas**, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Datos Personales** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y</b> <b>PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- Datos Personales Sensibles** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- Declaración de aplicabilidad** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC27000).
- Derecho a la Intimidad** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- Encargado del Tratamiento de Datos** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- Información Pública Clasificada** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- Información Pública Reservada** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- **Plan de continuidad del negocio** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Responsabilidad Demostrada** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información Preservación** de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- **Titulares de la información** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Trazabilidad** Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

### 3. OBJETIVOS

#### Objetivo General

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el HOSPITAL DEPARTAMENTAL SAN RAFAEL con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

#### Objetivos Específicos

Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en el HOSPITAL DEPARTAMENTAL SAN RAFAEL para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Promover el uso de mejores prácticas de seguridad de la información.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas del Hospital y los centros de salud.
- Optimizar la gestión de la seguridad de la información al interior con los dispositivos de interconexión de redes.

#### RECURSOS

**Humano:** Gerente General, Líderes del Proceso, Profesional 3 Tecnología, Personal Externo

**Físico:** PC y equipos de cómputo y de interconexión de redes de datos.

#### RESPONSABLES

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- Gerente General
- Líderes del Proceso
- Profesional en Tecnología

**METODOLOGÍA DE IMPLEMENTACIÓN** Para llevar a cabo la implementación del Plan de tratamiento de Seguridad y Privacidad de la Información en el HOSPITAL DEPARTAMENTAL SAN RAFAEL y las sedes, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

#### 4. PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

##### ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
4. Valorar del riesgo
5. Realizar Mapas donde se ubican los riesgos
6. Plantear al plan de tratamiento de riesgo aprobado por los líderes

##### DESCRIPCIÓN DEL CICLO DE OPERACIÓN



Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
VALLE DEL CAUCA  
Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y**  
**PRIVACIDAD DE LA INFORMACION**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 9 de 15

## 5. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el FODESEP.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

## 6. CRONOGRAMA

ACTIVIDAD	ENE	FEB	MAR	ABRIL	MAYO	JUNIO	JULIO
1. Realizar Diagnóstico	x	X					
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.			X	X			
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información					X	X	
4. Valorar del riesgo							X
5. Realizar Mapas donde se ubican los riesgos							
6. Plantear al plan de tratamiento de riesgo aprobado por los líderes							

## 7. SEGUIMIENTO y EVALUACIÓN

Se estará pendiente de las revisiones y actualizaciones y de los cambios de cada área



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
 Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y**  
**PRIVACIDAD DE LA INFORMACION**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 10 de 15

**DIAGNOSTICO E IDENTIFICACION DE RIESGOS**

AREA ASISTENCIAL Y FINANCIERA	RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
✓ Red eléctrica	Cableado mal instalado sin normas
✓ Equipos	Equipos sin polo a tierra
✓ Red de datos	La red inalámbrica
✓ UPS	Regulación de la energía
<b>DATOS LOGICOS</b>	
Claves	Préstamo de claves de acceso al sistema
✓ Red eléctrica	Cableado mal instalado sin normas, tomas de difícil acceso.
✓ Equipos	Equipos sin polo a tierra
✓ Red de datos	La red inalámbrica en áreas neurálgicas como consulta externa, urgencias, cirugía, maternidad y hospitalización
✓ UPS	Regulación de la energía
✓ internet	No se cuenta con un cortafuego para configurar las páginas de internet que se pueden bloquear, este proceso se realiza manual y algunos funcionarios pueden violar esa Seguridad.
Claves	Préstamo de claves de acceso al sistema
Estática	Las torres de los equipos de cómputo se llenan de estática por que se encuentran en el suelo.
PC	Ausencia de equipos de cómputo remanentes para cubrir las necesidades en caso de daños



HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.  
VALLE DEL CAUCA  
Nit: 891900441-1



SISTEMAS DE INFORMACION  
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 1 de 15

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOSPITAL DEPARTAMENTAL  
SAN RAFAEL DE ZARZAL E.S.E

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## INTRODUCCIÓN

Para realizar el Plan de contingencia informático del Hospital Departamental San Rafael de Zarzal se tiene en cuenta la información como uno de los activos más importantes de la empresa, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos como las redes, críticos para la función del Hospital. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Es importante resaltar que para que esta empresa de salud logre sus objetivos, es indispensable el manejo de información, por tanto necesita garantizar tiempos de indisponibilidad mínimos para no originar distorsiones al funcionamiento normal de nuestros servicios a los usuarios de los diferentes municipios y mayores costos de operación ya que de continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar la facturación no solo del hospital sino de los centros de salud que dependen del sistema central, sin información los médicos no podrán ingresar datos a la historia clínica y esto acarrearía problemas de demandas etc, ya que la información nos sirve de control y toma de decisiones para los jefes de área y la alta gerencia. De acuerdo a lo anteriores necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo mejor posible.

La Administración del Hospital Departamental San Rafael de Zarzal E.S.E, depende de los servicios y Aplicaciones que se muestran a continuación. Los mismos son suministrados por la Oficina de Sistemas de Información para apoyar varias de las funciones de diferentes oficinas del área financiera y asistencial.

1. Correo Institucional
2. Página Web del Hospital
3. Acceso al Internet
4. Sistema sihos área financiera y asistencial
5. Dispositivos de interconexión de redes
6. Infraestructura de redes de datos
7. Soporte técnico en Hardware y Software

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

### OBJETIVOS

- ✓ Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- ✓ Garantizar la continuidad de las operaciones de los principales elementos que Componen los Sistemas de Información.
- ✓ Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general

### PLAN DE CONTINGENCIA INFORMATICO Y GESTION DEL RIESGO Y SEGURIDAD DE LA INFORMACION DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL ZARZAL

La protección de la información de una empresa ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático. Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos, dispositivos de interconexión de redes, accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano, naturales y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotajes etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y Capacidades para procesar la información y restablecer la marcha normal del negocio.

### IDENTIFICACION DE MODULOS DEL SISTEMAS

#### SIHOS PRINCIPALES PROCESOS DE SOFTWARE IDENTIFICADOS

#### AREA FINANCIERA

- ✓ Nomina
- ✓ Cartera
- ✓ Presupuesto
- ✓ Tesorería, caja



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- ✓ Activos fijos
- ✓ Contabilidad, cuentas por pagar y por cobrar
- ✓ Inventarios
- ✓ Facturación

#### AREA ASISTENCIAL

- ✓ Historia Clínica
- ✓ Urgencias
- ✓ Triage
- ✓ Promoción y Prevención
- ✓ Consulta externa
- ✓ Consulta especializada
- ✓ Citas
- ✓ Laboratorio Clínico
- ✓ Observación e internación
- ✓ Odontología
- ✓ Procedimientos
- ✓ Terapias física y respiratoria

#### PRINCIPALES PROCESOS DE HARDWARE IDENTIFICADOS

- ✓ Linux centos en el servidor y las estaciones de trabajo windows
- ✓ Correo Electrónico Institucional
- ✓ Internet banda ancha de telefónica 1 mega dedicado, ert son los proveedores del servicio
- ✓ Antivirus nod 32 versión gratuita
- ✓ Herramientas de Microsoft Office.
- ✓ Software Base
- ✓ Mysql
- ✓ Internet explorer versión 8 o 9
- ✓ Backup de la Información
- ✓ Ejecutables de las aplicaciones.

#### RESPALDO DE LA INFORMACIÓN

- ✓ Backup de la Base de Datos sihos
- ✓ Backup de la Plataforma de Aplicaciones (Sistemas)
- ✓ Backup de la WEBSITE
- ✓ Backup del Servidor adicional y los de consulta

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

Metodología aplicada: Para la clasificación de los activos de las Tecnologías de Información del Hospital Departamental San Rafael Zarzal se han considerado Tres criterios:

Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).

Frecuencia del Evento: Puede ser (Nunca, aleatoria, Periódico y continuo)

Impacto: El impacto de un evento: puede ser (Leve, moderado, grave y muy severo).

**Plan de Contingencia:** Son procedimientos que definen como una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en: Leves (Caídas de energía de corta duración, fallas en disco duro, etc.) Severas (Destrucción de equipos, incendios, etc.)

**Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o Daño. Existen distintos tipos de riesgo:

**Riesgos Naturales:** Tales como mal tiempo, terremotos, etc.

**Riesgos Tecnológicos:** tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

**Riesgos Sociales:** como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad.

### ACTIVOS SUSCEPTIBLES DE DAÑO

- ✓ Personal
- ✓ Hardware
- ✓ Software y utilitarios
- ✓ Datos e información
- ✓ Documentación
- ✓ Suministro de energía eléctrica
- ✓ Suministro de telecomunicaciones

### POSIBLES DAÑOS

- ✓ Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- ✓ Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- o borrado físico/lógico de información clave, proceso de información no deseado.
- ✓ Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

#### FUENTES DE DAÑO

- ✓ Acceso no autorizado
- ✓ Ruptura de las claves de acceso a los sistema computacionales
- ✓ Desastres Naturales
- ✓ Movimientos telúricos
- ✓ Inundaciones
- ✓ Fallas en los equipos de soporte causadas por el ambiente la red de energía eléctrica o el no acondicionamiento atmosférico necesario
- ✓ Fallas de Personal Clave, Enfermedad, Accidentes, Renuncias, Abandono De sus puestos de trabajo
- ✓ Fallas de Hardware y en los servidores, red, Switches, cableado, Router, FireWall)

#### CLASES DE RIESGOS

- ✓ Incendio o Fuego
- ✓ Robo común de equipos y archivos
- ✓ Fallo en equipos
- ✓ Equivocaciones
- ✓ Acción de virus informático
- ✓ Fenómenos naturales
- ✓ Accesos no autorizados
- ✓ Ausencia del personal de sistemas
- ✓ Tableros eléctricos destapados

#### MINIMIZACION DEL RIESGO

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo.

#### INCENDIO O FUEGO

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Aleatorio

Grado del impacto: Alto

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

Situación Actual	Acción Preventiva
La oficina donde están los servidores cuenta con un extintor, debidamente cargado, se cuenta con un servidor alterno para cualquier eventualidad el servidor cuentas con 2 discos duros de tera para guardar información y otro que maneja el sistema operativo.	Se cumple
Jornadas de capacitación a usuarios sobre manejo de estos	Se cumple con salud ocupacional, pero falta Retroalimentación
<ul style="list-style-type: none"> <li>✓ La información de sihos se guarda en 4 copias de seguridad en el servidor de forma automática en los horarios de 4:40am, 12:40am, 06:40pm, 12:40pm las cuales son copiadas del servidor a diario en la mañana y al medio día en un disco duro externo al servidor. Se guarda una copia mensual, y se guarda una de cada año, en los discos duros del servidor y se van borrando semanalmente para no guardar tanta información. Se tiene un servidor espejo para que cuando este falle el otro empiece a trabajar solo realizándose el cambio de ip activa.</li> <li>✓ Las copias de seguridad de los programas que se consultan ya que fueron dados de baja, estos están ubicados en sistemas y cada programa se encuentra en discos duros de respaldos al igual que en sus respectivas torres en donde fueron instalados.</li> <li>✓ La información de los usuarios cada uno es responsable de sus copias de respaldo pero en su mayoría se les ha hecho copia de seguridad en sistemas.</li> <li>✓ Se tiene copia de seguridad en la nube con Dropbox, diariamente para salva guardar la información en un lugar externo del Hospital Departamental San Rafael.</li> </ul>	Se cumple, falta un disco duro adicional más grande para que toda la información de todas las áreas de servicio se puedan incluir allí, como plan b pero ya se empezó como plan de mejora a subir la información en la nube por dropbox para tenerla en un lugar externo del Hospital.

Para evitar el riesgo de un incendio y se pierda información se envía la información archivo central como plan B alterno a la oficina de sistemas.

Robo Común de Equipos y Archivos Grado de Negatividad: Grave  
 Frecuencia de Evento: Aleatorio Grado de  
 Impacto: Moderado

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

Contamos con un vigilante a las dos entradas principales, este no a todos los revisa.	Se solicita que todo el personal revise sus Dispositivos y aparatos tecnológicos antes de salir del hospital.
Existe en el vigilante una salida de equipos que tiene que hacer firmar cada vez que salga un equipo de la institución	Se realizan rondas periódicas del personal de sistemas para la confrontación de esta carpeta.

### FALLO EN LOS EQUIPOS

Grado de Negatividad: Muy Severo  
 Frecuencia de Evento: Aleatorio  
 Grado del impacto: Alto

Situación Actual	Acción Preventiva
Los fallos de los equipos se deben a problemas eléctricos y bajones de energía	se necesita una planta automática y revisión del sistema eléctrico del hospital, hay muchos bajones de energía.

Por lo anterior se debe tener en cuenta lo siguiente:

### DISPOSITIVOS ELECTRONICOS

- ✓ Todos los equipos de cómputo deben estar protegidos con una ups para evitar daños en su fuente de poder y demás hardware, en el almacén se solicita equipos electrónicos de respaldo para tener como contingencia, en caso de daño.

En caso de daño de la energía se procede a esperar que la planta se encienda, el servidor o el área de sistemas cuenta con una malla a tierra que los protege.

### MANEJO DEL SISTEMA

Grado de Negatividad: Muy Severo  
 Frecuencia de Evento: Aleatorio  
 Grado de Impacto: Alto

Cuando hay manejo del sistema errado somos llamados por las áreas de servicio para su revisión y arreglo si es el caso sino se llama a la empresa proveedora del software Sinergia s.a	Se están haciendo por que se tiene contrato de mantenimiento y actualización.
Se tienen procedimientos cuando el equipo se daña es enviado al almacén con una carta con su diagnóstico respectivo	La carta es enviada y recibida para su posterior dado de baja.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

<p>Cuando hay un daño en el sistema sistemas avisa almacén para que este entregue a las áreas de servicio la papelería necesaria para prestar los servicios</p>	<p>Se tiene la papelería en stop en almacén y se llama a verificar que siempre se tenga, solo se entrega con al autorización del área de sistemas.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------

### ANTIVIRUS INFORMATICO

Grado de Negatividad: Muy Severo  
 Frecuencia de Evento: Aleatorio  
 Grado de Impacto: Alto

<p>El hospital con su técnico vacuna todos los equipos y es indispensable que tenga un antivirus y se actualiza por internet el nod 32</p>	<p>Algunas personas no vacunan las memorias</p>
--------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------

### FENOMENOS NATURALES

Grado de Negatividad: Muy Severo  
 Frecuencia de Evento: Aleatorio  
 Grado de Impacto: Alto

<p>Cuando hay tormentas eléctricas se trata de que el personal apague los equipos y espere a que pase e evento para evitar daños de la información</p>	<p>Algunas personas no atienden al llamado</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------

### ACCESOS NO AUTORIZADOS

Grado de Negatividad: Muy Severo  
 Frecuencia de Evento: Aleatorio  
 Grado de Impacto: Alto

<p>Todos los usuarios del sistema sihos maneja sus usuarios y sus claves respectivamente que son asignadas por sistemas, cuando el personal se retira y se va a vacaciones es informado a sistemas para su inactivación.</p>	<p>Esta acción no es delegada solo tiene permisos el gerente y la administradora del sistema.</p>
<p>Existe un administrador del sistema que hace las funciones.</p>	



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
VALLE DEL CAUCA  
Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 10 de 15

### AUSENCIA DEL PERSONAL DE SISTEMAS

Grado de Negatividad: Muy Severo

Frecuencia de Evento: Aleatorio

Grado de Impacto: Alto

Hay tres personas totalmente capacitadas y con alta experiencia en hardware , software y redes

Siempre debe quedar por lo menos uno en la oficina para dar soporte técnico a los usuarios.

### EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

- ✓ Problemas eléctricos y el evento es daño en los equipos de cómputo, redes, software
- ✓ Puede haber un daño físico en el servidor por daño de disco duro pero se tiene respaldo de otro servidor alternativo.

### RECURSOS DE CONTINGENCIA:

- ✓ Remanente de ups, monitores, teclados, mouse, cartuchos, impresoras etc. Para no parar el servicio en almacén se encuentran o si no se reemplazan por otros de sistemas.
- ✓ Se realiza backup diario de la información
- ✓ Manual de los funcionarios de sistemas
- ✓ Relación de todos los equipos de computo
- ✓ Diagrama lógico de toda la red

### INTERRUPCION DEL FLUJO EELCTRICO DURANTE LA EJECUCION DE LAS ACTIVIDADES

#### Recurso de contingencia: Mantener en buen estado la planta

- ✓ Si hay interrupción de energía se sostendrán con la ups mientras que la planta empieza a funcionar.

### PERDIDA DEL SERIVICO DE INTERNET

- ✓ Se tiene una banda ancha para manejar ip pública para la entrada d los centros de salud.
- ✓ Se tiene otra para el manejo del portal del banco de Bogotá con ip estática
- ✓ Se tiene otra que maneja todos los usuarios

Cuando hay fallo se coge alguna para su restablecimiento o en su defecto se usan modem.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> VALLE DEL CAUCA Nit: 891900441-1				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

**Recurso de contingencia:** software, hardware, redes, servicio de internet.

**DESTRUCCION DEL CENTRO DE CÓMPUTO:**

- ✓ Contar con el inventario de equipos de cómputo.
- ✓ Identificar recursos de hardware y software que se puedan rescatar
- ✓ Salvaguardar los backup de información, que se tienen en dos lugares
- ✓ Buscar un nuevo espacio para el centro de cómputo que será en estadística
- ✓ Presupuestar compra de hardware, software, materiales y contratación de personal.
- ✓ Iniciar con la instalación del nuevo centro d computo
- ✓ Restablecer los backup realizados anteriormente.

**PLAN DE RESPALDO Y RECUPERACION DE LA INFORMACION**

El plan de recuperación iniciara con hacer valer la póliza de los activos asegurados, después del desastre se abordara la restauración del centro de datos.

Se definirán las personas responsables de la definición del plan de contingencia.

TECNICO EN ELCTRONICA: Realizara las acciones de equipos

TECNICO EN SISTEMAS: Realizará las acciones de redes

INGENIERO DE SISTEMAS: Realizara las acciones de software, obtención y almacenamiento de los respaldo.

Obtención de ayuda de otros entes: se tiene el proveedor de los sistemas de información como:

Hardware: Impretintas de Zarzal, teléfono 2209749

Software: Empresa Sinergia de Ibagué, teléfonos, 098 2712383

**Actividades después del desastre:**

Se evaluarán los daños los integrantes de la oficina de sistemas y se atenderá como prioridad la facturación y el registro de la historia clínica habilitando el servidor central.

**Priorización de actividades:**

Recuperación y puesta en marcha de los equipos, compra de equipos dañados.

**Ejecución de actividades**

Creación de equipos de trabajo, asignando actividades a las personas que conocen de sistemas del hospital, y cada uno contara con un líder para mirar el avance de los trabajos.

**Evaluación de resultados:**

Se debe verificar que lo realizado se encuentre funcionando correctamente





**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**

**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**



CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 1 de 42

# PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION PETI

HOSPITAL DEPARTAMENTAL  
SAN RAFAEL DE ZARZAL E.S.E

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## Contenido

1.	RESUMEN .....	3
2.	INTRODUCCIÓN .....	3
3.	OBJETIVO .....	3
3.1.	Objetivo Estratégico .....	3
3.2.	Objetivo Específicos .....	3
4.	ALCANCE DEL DOCUMENTO .....	4
5.	MARCO NORMATIVO .....	4
6.	RUPTURAS ESTRATÉGICAS .....	6
7.	ANÁLISIS DE LA SITUACIÓN ACTUAL .....	6
8.	ESTRATEGIA DE TI .....	6
9.	PLANES ESTRATÉGICOS INSTITUCIONALES.....	8
10.	FUNCIONES DEL ÁREA DE SISTEMAS.....	16
11.	MANUAL DE FUNCIONES .....	31
12.	ESTRATEGIA DE SERVICIOS TECNOLOGICOS .....	32

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>					
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>					
	<b>CÓDIGO: P-GDG 01</b>	<b>VERSIÓN: 2</b>	<b>FECHA: 01/02/2014</b>	<b>TRD: 24-07</b>	<b>PÁGINA: 3 de 42</b>	

## 1. RESUMEN

El presente Plan Estratégico de Tecnologías de Información y las Comunicaciones (PETIC), expone la planificación estratégica de las tecnologías de información y las comunicaciones del Hospital Departamental San Rafael, para el periodo comprendido entre los años 2018 al 2019. El PETIC pretende orientar los esfuerzos relacionados con la función de apoyo en Tecnologías de Información y Comunicación al resto de los procesos sustantivos y adjetivos institucionales.

## 2. INTRODUCCIÓN

El área de Sistemas de Información del Hospital Departamental San Rafael, busca definir un norte a seguir en materia de Tecnologías y herramienta que impulse la necesidad de un planteamiento de nuevos horizontes en la gestión de Tecnologías de la información, de esta manera, con el presente documento se inicia un nuevo plan denominado Plan Estratégico de Tecnologías de información y las comunicaciones (PETIC). Con el propósito de mantener este plan ajustado a las necesidades organizacionales el PETIC, será un instrumento sujeto de mejora continua, y por lo tanto, será sometido a revisiones y mejoras en compañía del área de control interno conforme se requiera.

### Misión de TI

“Servir como apoyo a todos los procesos del Hospital Departamental San Rafael, en cuanto al mantenimiento y soporte técnico de los sistemas de Información en funcionamiento y de consulta tantos misionales como de apoyo administrativo, garantizando a los usuarios el acceso a las herramientas informáticas a través de una infraestructura tecnológica adecuada y que cumpla con los requisitos de oportunidad, disponibilidad eficiencia y seguridad”

## 3. OBJETIVO

### 3.1. Objetivo Estratégico

Promover el desarrollo sostenible en la infraestructura tecnológica del Hospital Departamental San Rafael a partir de la modernización de las redes de datos, equipos de cómputo y las comunicaciones, apoyados en el uso estratégico de las TIC, para contribuir en la construcción de un gobierno en línea más eficiente, transparente, participativo, cercano y que genere progreso tanto en la sede principal como en los puestos de salud y veredas.

### 3.2. Objetivo Específicos

- ✓ Implementar un gobierno de las tecnologías de la información y las comunicaciones en el Hospital Departamental San Rafael a través del cual se dirige y controla el uso actual de las tecnologías de la Información.
- ✓ Fortalecer la gestión del área de sistemas en la prestación del servicio a los usuarios tanto internos como externos a través de las tecnologías de la información y la comunicación.
- ✓ Incrementar la calidad y cantidad de los servicios en línea ofrecidos a los ciudadanos.
- ✓ Fortalecimiento de la infraestructura en las redes de datos para mejorar la agilidad del servicio.

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>					
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>					
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	PÁGINA: 4 de 42	

#### 4. ALCANCE DEL DOCUMENTO

El plan estratégico de tecnologías de la información "PETI" se formula con el fin de identificar Las necesidades puntuales del Hospital, y su alcance se basa en la actualización de la infraestructura tecnológica en esta vigencia.

El Plan Estratégico de Tecnologías de la información está comprendido por 5 fases;

**Primera Fase:** Se realiza el análisis del diagnóstico actual del Hospital, a través del cual se revisan el estado actual de cada área tanto en hardware, software, redes, comunicaciones.

**Segunda Fase:** Comprende el análisis del modelo operativo y organizacional de la entidad, las necesidades de información como el software instalado y la alineación de TI con los procesos de las áreas tanto asistenciales como financiera del Hospital Departamental San Rafael y sus sedes, de tal forma que se tenga plena conciencia de los cambios o ajustes que se realicen por área y por sede y así tener claro que necesidades puntuales hay que tener en cuenta para el desarrollo de la estrategia de TI.

**Tercera Fase:** Se desarrolla la estrategia de TI, la cual plantea el modelo de gestión de TI alineado a la estrategia del Hospital y sus sedes y el sector que se desarrolla en los modelos de información, sistemas de información, arquitectura de servicios tecnológicos, Gobierno de TI y modelos de uso y apropiación.

**Cuarta Fase:** Se realiza la planeación con la definición de los lineamientos y actividades estratégicas que salieron de las actividades anteriores, para desarrollar el plan de implementación de la estrategia y se estructura el plan definitivo,

**Quinta Fase:** con la fase anterior será la base para la construcción y lograr los lineamientos que se desarrollan los planes de acción en el corto, mediano y largo plazo y los planes de mejoramiento con actualizaciones anuales y que el área de sistemas estará actualizando según las necesidades de los usuarios y los proyectos que se logren plantear y obtener para el mejoramiento de la infraestructura tecnológica del Hospital y sus sedes ubicadas en el área rural y urbana.

#### 5. MARCO NORMATIVO

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

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

Empresarial para la gestión de Tecnologías de la Información: Es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de las arquitecturas empresariales, tanto sectoriales como institucionales. El marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información. (...) Contando con este marco para la estructuración del Plan Estratégico de las Tecnologías de la Información y las Comunicaciones el Decreto 2573 de 2014 en su Título II – Componentes, Instrumentos y Responsables que enfatiza sobre los fundamentos principales para desarrollar de manera correcta implementación de la Estrategia de Gobierno en línea, se debe cumplir con los siguientes componentes; Plan Estratégico de Tecnologías de la Información -PETI 2016 -2019 Página 6 de 58 "(...) Artículo 5°. Componentes. Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea. 1. TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo. 2. TIC para el Gobierno abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones. 3. TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno. 4. Seguridad y privacidad de la Información. Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Parágrafo 1°. TIC para el gobierno abierto comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto pero no los cubre en su totalidad. Artículo 6°. Instrumentos. Los instrumentos para la implementación de Plan Estratégico de Tecnologías de la Información -PETI 2016 -2019 Página 7 de 58 "(...) Artículo 9°. Medición y monitoreo. El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno en Línea y de la Dirección de Estándares y Arquitectura de Tecnologías de la Información, diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el Manual de Gobierno en Línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que les sea requerida. Artículo 10. Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos: En conclusión es de vital importancia el cumplimiento del presente decreto por ser el mapa de ruta que las entidades territoriales deben promover en sus administraciones para así aplicar de manera correcta la estrategia nacional de Gobierno en línea, apoyando a la creación de un Estado más eficiente, más transparente y más participativo gracias a las TIC, prestando los mejores servicios en línea al ciudadano, logrando la excelencia en la gestión, empoderando y generando confianza en los ciudadanos e impulsando y facilitando las acciones requeridas para avanzar en los Objetivos de Desarrollo Sostenible -ODS, facilitando el goce efectivo de derechos a través del uso de TIC. Como complemento del Decreto Nacional 2573 de 2014, encontramos el dominio Estrategia TI que tiene como fin apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales, su implementación cuenta con 4 ámbitos de aplicación que servirán como insumo para el correcto formulación, seguimiento y evaluación del Plan Estratégico de las Tecnologías de la Información y las Comunicaciones adoptado por la entidad; Decreto 415 del 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones." En su Artículo 2.2.35.3. Numeral 1 se establece los

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	<b>CÓDIGO: P-GDG 01</b>	<b>VERSIÓN: 2</b>	<b>FECHA: 01/02/2014</b>	<b>TRD: 24-07</b>	

objetivos del fortalecimiento institucional. Para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades y organismos a que se refiere el presente decreto, deberán: 1. Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y Plan Estratégico de Tecnologías de la Información -PETI 2016 -2019 Página 8 de 58 servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado. Como conclusión la entidad deberá definir el fortalecimiento institucional a través del uso de las tecnologías de la información y las comunicaciones definiendo mecanismos de implementación y ejecución valederos para las capacidades internas y externas que la entidad contenga para la mejora continua de la prestación del servicio, esto a través de una alta difusión por medios electrónicos con campañas de divulgación de la implementación y la alineación que esta tendrá con el modelo integrado de gestión de la administración mejorando el funcionamiento de los procesos y procedimientos e impulsando la eficacia, la eficiencia y la efectividad a través del ejercicio del principio de transparencia.

## 6. RUPTURAS ESTRATÉGICAS

Las rupturas estratégicas nos permiten identificar los paradigmas a romper de la Institución pública para llevar a cabo la transformación de la gestión de TI, a continuación se listan las siguientes rupturas estratégicas identificadas:

- ✓ La tecnología debe ser considerada un factor de valor estratégico para la institución pública.
- ✓ Necesidad de liderazgo al interior de la institución pública para la gestión de Sistemas de Información, se debe de Contar con una oficina de TI, que haga parte del comité directivo, que gerencia las actividades, los recursos y que se enfoque hacia un servicio de la mejor calidad posible, para los clientes internos y externos.
- ✓ Los proyectos de TI son costosos y no siempre es claro su retorno de inversión.
- ✓ Alinear las soluciones con los procesos, aprovechando las oportunidades de la tecnología, según el costo/beneficio.
- ✓ Los sistemas de información no se integran y no facilitan las acciones coordinadas.
- ✓ Hay una amplia brecha entre los directivos y el personal de TI.
- ✓ Resolver el dilema entre “desarrollar en casa” vs. “Comprar software comercial”.

## 7. ANÁLISIS DE LA SITUACIÓN ACTUAL

En este apartado se describe la situación actual de las Tecnologías de la Información de la institución en relación con los dominios del marco de referencia de Arquitectura Empresarial.

Este análisis debe permitir conocer el estado actual o línea base a partir de la cual se debe partir para proyectar la visión de lo que se espera en materia de gestión de TI en el Hospital Departamental San Rafael y sus sedes ubicadas en el área Rural y Urbana.

## 8. ESTRATEGIA DE TI

El plan nacional de desarrollo para el logro de sus objetivos, plantea como una de sus seis estrategias transversales el buen gobierno. Dichas estrategias trazan los lineamientos de política Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>					
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>					
	<b>CÓDIGO: P-GDG 01</b>	<b>VERSIÓN: 2</b>	<b>FECHA: 01/02/2014</b>	<b>TRD: 24-07</b>	<b>PÁGINA: 7 de 42</b>	

que le permitirán avanzar hacia la construcción de un país en paz, equitativo y educado. La estrategia de buen gobierno está orientada a garantizar la configuración y consolidación de un Estado moderno, más transparente, eficiente, y eficaz. (DNP, 2014 p. 9) Dentro de la estrategia de Buen Gobierno se establece en unos de sus objetivos “mejorar la efectividad de la gestión pública y el servicio al ciudadano nacional y territorial” y una de las acciones ligadas para el cumplimiento de dicho objetivo se destaca:

- ✓ Fomentar la construcción de un Estado más transparente, participativo y colaborativo, involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones. (DNP, 2014 P. 438)
- ✓ Mejorar la infraestructura tecnológica de los sistemas de información que permita fortalecer el acceso a las fuentes de información de los procesos misionales y administrativos de la Función Pública.
- ✓ Brindar alternativas de solución a las principales necesidades de las personas naturales y jurídicas, gracias a la utilización adecuada y estratégica de las TIC para el fortalecimiento de los trámites y servicios que se ponen a su disposición.
- ✓ Formular la política pública, lineamientos y estándares necesarios para garantizar la implementación de la estrategia de Gobierno en Línea.
- ✓ Impulsar la implementación del Marco de Referencia de Arquitectura y de los estándares de seguridad y privacidad de la información con apoyo en soluciones transversales que faciliten y dinamicen la implementación de Gobierno en línea por parte de las entidades públicas. Como parte del diagnóstico del buen gobierno en el literal de gestión pública efectiva, se documenta que se ha avanzado en la implementación del Chief Information Officer (CIO) en las instituciones y de su comunidad de miembros, a través de la formación en liderazgo en el uso de las TIC. Como también en la elaboración de un marco de referencia de arquitectura que plantea los lineamientos, estándares y mejores prácticas que las entidades públicas deberían aplicar para garantizar una efectiva gestión de información y de tecnología. (DNP, 2014 p. 412)
- ✓ En los sistemas de información públicos para la gestión institucional, se presentan retos en materia de interoperabilidad, intercambio y calidad de la información, que limitan la gestión y los procesos de toma de decisión pública. (DNP, 2014 p. 412).

Se logrará una gestión pública efectiva y orientada al servicio al ciudadano, en el nivel internacional, nacional y territorial, a través de la modernización de la infraestructura administrativa pública, los modelos de gestión, entre ellos el de talento humano, el jurídico público, y el documental, la innovación social y el uso de herramientas tecnológicas. Además, se logrará la efectividad, transparencia y oportunidad en los procesos de contratación pública, un modelo distinto de gobierno de las empresas estatales y una gestión inmobiliaria especializada. Parte de estos avances y retos se evidencian en el decreto 415, donde se define la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones emitido por el departamento administrativo de la función pública en el 2016.

#### **Plan de desarrollo municipal**

[http://camaratulua.org/area\\_influencia/zarzal/plan-de-desarrollo-municipal-zarzal-2016-2019/](http://camaratulua.org/area_influencia/zarzal/plan-de-desarrollo-municipal-zarzal-2016-2019/)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

### Plan de desarrollo del Departamento del Valle del Cauca 2016-2019. "El Valle está en Vos"

Bajo el acuerdo sostenido entre el asesor de informática y telemática de la alcaldía de Cali y el secretario TIC de la gobernación de valle del cauca.

Alineando las metas que tenían propuestas se decidió priorizar y trabajar articuladamente en los siguientes proyectos:

- 1) Zonas Wifi.
- 2) Trámites en línea.
- 3) Apropiación en ViveLab
- 4) Resultado del ejercicio se anexa documento con las 21 metas que se aprobaron el el Plan de Desarrollo Departamental y acta de reunión.

## 9. PLANES ESTRATÉGICOS INSTITUCIONALES.

### POLITICA DE CERO PAPEL

1. Los retiros de los empleados o novedades se realicen la solicitud a sistemas por correo electrónico
2. En urgencias solo se debe imprimir la epicrisis o resumen de la historia.
3. Todos los documentos internos deben ser enviados por correos electrónicos solo se radican los documentos externo

### POLITICA ANTITRAMITE

1. En el área de siau la persona encargada de triage y consulta externa deberá entregarle el tike para que el médico le explique al usuario su fórmula medica

Anexo carpeta TIC: carta enviada el 10 de octubre de 2014

2. La oficina de siau debe verificar la tramitología que tienen los pacientes con la autorizaciones, lo que se quiere es que la oficina de siau tramite las autorizaciones de las entidades y que se llame desde allí, se haga el trámite de las ordenes medicas ante las EPS, en donde doña Rubiela le entrega los anexos a siau y sea esa la oficina que haga las llamadas, siau solicita que se les abra una línea telefónica para realizar las llamadas.

En el área de estadística se va a imprimir la historia clínica completa para que el usuario no tenga que voltear tanto para un servicio.

### POLITICAS DE COMPRA DE EQUIPOS DE CÓMPUTO

Con el fin de garantizar la adecuada gestión de los computadores de escritorio y portátiles, el **HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL** realizará procesos de compra institucional de equipos al año. Al inicio de cada año se debe comunicar a la gerencia, las cantidades y referencias



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

de equipos que desean adquirir, los cuales serán entregados a las dependencias. Estas compras buscan satisfacer las siguientes necesidades del HOSPITAL.

1. Renovación de los computadores de escritorio y portátiles que no cumplen su función o presenten lentitud a los procesos para lo que fueron designados.
2. Asignación de equipos nuevos, por crecimiento de la planta de personal de las unidades.

Únicamente se aprobarán compras de computadores de escritorio o portátiles, por fuera de la compra institucional de la del HOSPITAL SAN RAFAEL DE ZARZAL, en los siguientes casos:

1. Para satisfacer los crecimientos no planeados de la planta de personal de las unidades.
2. Para reemplazar un computador que presenta daño irreparable no cubierto por la garantía del equipo y el equipo anterior es dado de baja. (Es necesario adjuntar el reporte técnico de la DEPENDENCIA DE SISTEMAS).

#### ANALISIS COSTO BENEFICIO

Se define y se evalúa la necesidad del usuario con las siguientes preguntas:

- ✓ Para qué se necesita el equipo?
- ✓ Cuanto uso le va a dar al computador diario?
- ✓ ¿Cuál es la potencia del procesador?
- ✓ La capacidad de la memoria
- ✓ Puedo expandir la memoria del computador que quiero comprar?
- ✓ Clonado o de marca?
- ✓ Computador Portátil o de mesa

**EI HOSPITAL SAN RAFAEL DE ZARZAL**, por intermedio de la DEPENDENCIA DE SISTEMAS, seleccionará un fabricante y los modelos de los equipos, para que sean seleccionados por las unidades que deseen adquirirlos.

Con el fin de garantizar la adecuada planeación, la DEPENDENCIA DE SISTEMAS, en conjunto enviará las diferentes unidades el listado de los equipos que deben incluir en el proceso de planeación presupuestal.

Las excepciones a estas reglas deberán ser sometidas al Comité de Compras del **EI HOSPITAL SAN RAFAEL DE ZARZAL** y para su evaluación, es requisito que cumplan con los lineamientos antes descritos.

#### POLITICAS DE USO DE LOS RECURSOS TECNOLOGICOS

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	



El Hospital Departamental San Rafael, provee a sus colaboradores un sistema informático y el equipamiento correspondiente para el cumplimiento de las tareas a su cargo. En consecuencia, el acceso al sistema informático y al uso de internet o de intranet provisto por el hospital posee las características de una herramienta de trabajo.

Se encuentra prohibido a todo el personal y se considera uso indebido del sistema informático de la Empresa:

1. Utilizar para fines personales y/o extra laborales el sistema informático y el equipamiento puesto a su disposición.
2. Utilizar programas sin el soporte legal, ni licencia correspondiente o incorporar a su computadora programas no adquirido legalmente por la Empresa.
3. Incorporar programas sin autorización previa escrita del Hospital, y/o con contenidos no correspondientes al sistema informático de la Empresa.
4. Vulnerar de cualquier forma y con cualquier medio la confidencialidad de la información existente en el sistema del Hospital.
5. Extraer copias de la información de cualquier tipo que obra en el sistema del hospital sin previa autorización escrita.
6. Enviar e-mails y/o "chatear" por motivos ajenos al Hospital y a sus tareas, ya sea con terceros (incluyendo amigos o familiares) o con personal de la Empresa.
7. La asignación de una clave personal de acceso al trabajador no le otorga derecho alguno a la utilización privada del sistema informático o al correo asignado para su puesto. En consecuencia, respecto de la correspondencia electrónica, se prohíbe el envío o recepción de e-mails por cuestiones personales.
8. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe monitorear que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

9. Todo el personal tendrán una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo, sólo son para uso interno, no tienen la capacidad de enviar correos públicos.

### **Sobre la seguridad de la información**

10. Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.

11. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.

12. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información. 13. Todos los equipos asignados a los conectores/gestores tendrán deshabilitados los accesos a puertos USB, CD o Diskettes. Esta medida tiene 3 objetivos:

Evitar ataques de virus en los equipos y el servidor.

Evitar extracciones no autorizadas.

Evitar la carga de archivos ajenos a la labor de gestión.

14. Los equipos autorizados para el uso de dispositivos de almacenamiento externos están supervisados por coordinación y por el área de sistemas, para la entrada y salida de información.

15. A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

Actualizar su base de firmas de virus (actualización de la lista de amenazas) Búsqueda de virus (análisis del equipo)

Eliminación de virus si fue detectado.

En caso autorizado de memorias USB y discos, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

### **Sobre el mantenimiento y buen uso de la infraestructura**

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

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

18. Si se presentara una suspensión de servicio eléctrico y el servidor solo se sostuviera con el no-break, se tendrán que apagar primero todos los equipos de la hospital y posteriormente el

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>					
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>					
	<b>CÓDIGO: P-GDG 01</b>	<b>VERSIÓN: 2</b>	<b>FECHA: 01/02/2014</b>	<b>TRD: 24-07</b>	<b>PÁGINA: 12 de 42</b>	

servidor.

19. El servidor y la máquina principal del área administrativa deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías.

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

21. Periódicamente, por espacio de 6 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas. Previo a una programación el usuario deberá entregar el equipo para su limpieza en el horario programado.

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

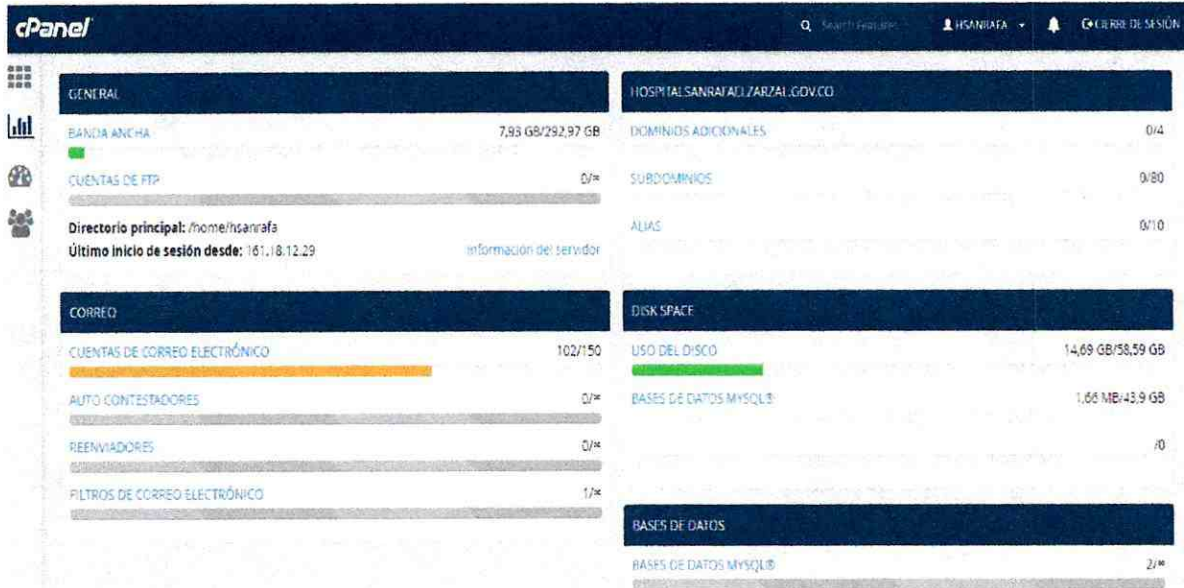
La desobediencia de cualquiera de estas normas será considerada como grave incumplimiento laboral.

#### **Uso y apropiación de la tecnología**

El siguiente punto tiene como propósito diagnosticar el uso y apropiación de TIC, concepto importante que radica en que los usuarios promuevan e intercambien información, recursos y posibilidades de comunicación e interacción, utilizando los aplicativos y sistemas de información para la consolidación de una administración más eficiente, tecnológica y rápida en la operación de sus procesos.

Estadísticas de uso del aplicativo web:

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	<b>CÓDIGO: P-GDG 01</b>	<b>VERSIÓN: 2</b>	<b>FECHA: 01/02/2014</b>	<b>TRD: 24-07</b>	



**GENERAL**

BANDA ANCHA: 7,93 GB/292,97 GB

CUENTAS DE FTP: 0/∞

Directorio principal: /home/hsanrafa

Último inicio de sesión desde: 161.18.12.29

**CORREO**

CUENTAS DE CORREO ELECTRÓNICO: 102/150

AUTO CONTESTADORES: 0/∞

REENVIADORES: 0/∞

FILTROS DE CORREO ELECTRÓNICO: 1/∞

**HOSPITALSANRAFAEL.ZARZAL.GOV.CO**

DOMINIOS ADICIONALES: 0/4

SUBDOMINIOS: 0/80

ALIAS: 0/10

**DISK SPACE**

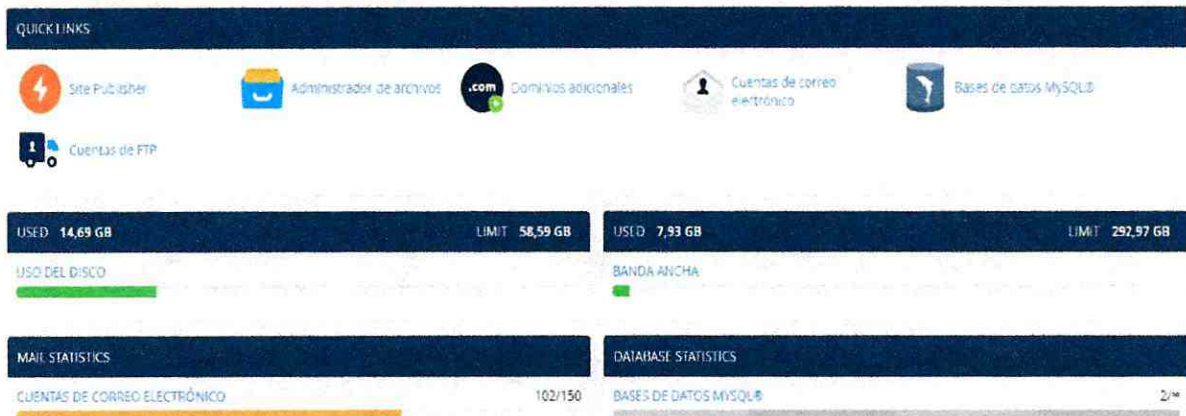
USO DEL DISCO: 14,69 GB/58,59 GB

BASES DE DATOS MYSQL: 1,66 MB/43,9 GB

**BASES DE DATOS**

BASES DE DATOS MYSQL: 2/∞

## USO DE LAS CUENTAS DE CORREO



**QUICK LINKS**

- Site Publisher
- Administrador de archivos
- Compuhos adicionales
- Cuentas de correo electrónico
- Base de datos MySQL
- Cuentas de FTP

**USO DEL DISCO**

USED: 14,69 GB | LIMIT: 58,59 GB

**BANDA ANCHA**

USED: 7,93 GB | LIMIT: 292,97 GB

**MAIL STATISTICS**

CUENTAS DE CORREO ELECTRÓNICO: 102/150

**DATABASE STATISTICS**

BASES DE DATOS MYSQL: 2/∞

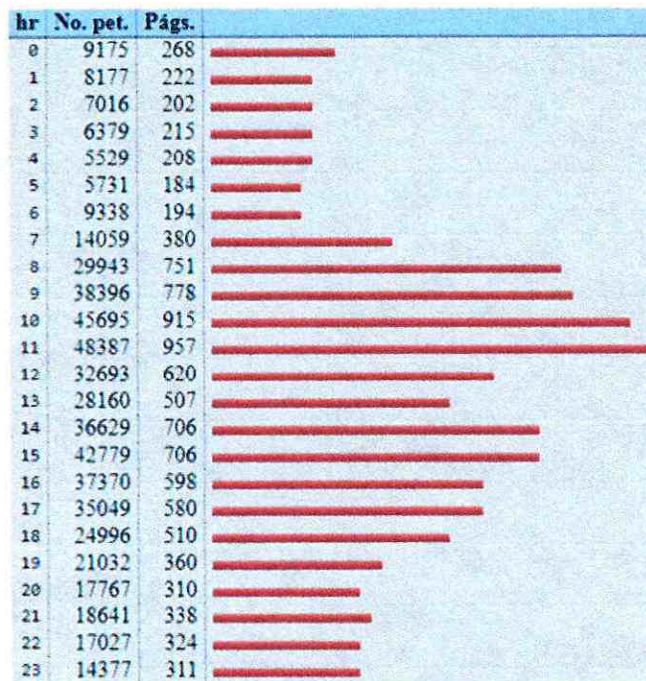




## Resumen horario

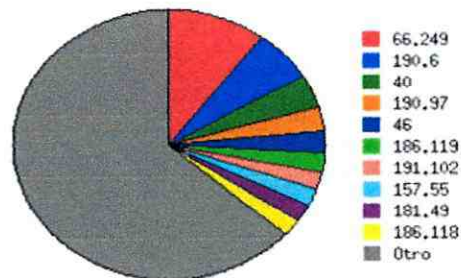
(Ir a: [Arriba](#) | [Resumen general](#) | [Informe mensual](#) | [Resumen diario](#) | [Resumen horario](#) | [Informes](#) | [Buscadas](#) | [Informe de navegadores](#) | [Resumen de navegadores](#) | [Informe de Sistemas Operativos](#))

Cada unidad (■) representa 25 peticiones por páginas o fracción.



## Informe de organización

(Ir a: [Arriba](#) | [Resumen general](#) | [Informe mensual](#) | [Resumen diario](#) | [R](#) | [Buscadas](#) | [Informe de navegadores](#) | [Resumen de navegadores](#) | [Inform](#))



Las áreas están dibujadas por número de peticiones.



HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.  
VALLE DEL CAUCA  
Nit: 891900441-1

SISTEMAS DE INFORMACION  
PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION  
PETI



CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 16 de 42

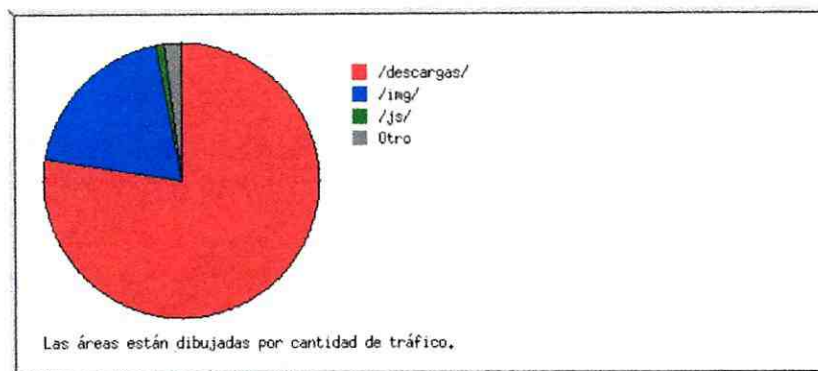
## Informe de remitentes redireccionados

(Ir a: [Arriba](#) | [Resumen general](#) | [Informe mensual](#) | [Resumen diario](#) | [Resumen horario](#) | [Informe de dominios](#) | [Informe de Búsquedas](#) | [Informe de navegadores](#) | [Resumen de navegadores](#) | [Informe de Sistemas Operativos](#) | [Informe de códigos](#))



## Informe de Directorios

(Ir a: [Arriba](#) | [Resumen general](#) | [Informe mensual](#) | [Resumen diario](#) | [Resumen horario](#) | [Informe de dominios](#) | [Informe de Búsquedas](#) | [Informe de navegadores](#) | [Resumen de navegadores](#) | [Informe de Sistemas Operativos](#) | [Informe de códigos](#))



## 10. FUNCIONES DEL ÁREA DE SISTEMAS

### Administración de cuentas de usuario administración y uso de contraseñas

- ✓ Para la creación de las contraseñas en el sistema la política es que cada contraseña se cree el usuario con la primera letra del nombre, seguido del primer apellido, y la contraseña asignada son los 4 últimos números de la cedula, la cual debe ser cambiada por el usuario en el mismo momento en que este entre al sistema sihos.
- ✓ La asignación de contraseñas debe ser realizada de forma individual lo que el uso de contraseñas compartidas está prohibido,
- ✓ Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al área de sistemas para que se le proporcione una nueva contraseña o en su defecto usted podrá



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

cambiarla por el mismo aplicativo.

- ✓ Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- ✓ Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar.
- ✓ Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- ✓ Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.
- ✓ Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

**RESPONSABLE:** Ingeniero de sistemas

#### **Procedimiento para la actualización del sitio web con base gobierno en línea (tic) y la participación en la red social facebook**

##### **Desarrollo del Sitio web:**

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

##### **Procedimiento:**

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

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

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

##### **DECRETO 2693 de 2012- gobierno en línea**

##### **ETAPAS Y COMPONENTES DE LA POLÍTICA ANTITRÁMITES Y DE GOBIERNO EN LÍNEA**

El dominio registrado para entrar al sitio web es: [www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
Facebook

Lo que se publica como noticia principal en el sitio web, es lo que se sube al Facebook del hospital el oficial para mantener actualizado a otros tipos de usuarios, correo electrónico como lo encuentran  
Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585  
[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[hospitalsanrafaelzarzal@telecom.com.co](mailto:hospitalsanrafaelzarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

es: facebook@hospitalsanrafaelzarzal.gov.co

**Responsable del desarrollo, actualización, implementación de los sitios del hospital es:**

Ingeniero de Sistemas

**Procedimiento para la administración de cuentas de usuario:**

Para acceder al sistema sihos debe pasar por la agremiación o si es rural por la oficina de personal en donde es allí donde definen al área de sistemas que usuario se creara en el sistema sihos, luego se le da un usuario y una contraseña para y si es médico o asistencial debe entregar al área de sistemas la firma con el sello para subirlo al sistema.

Cada novedad de los usuarios del sistema como vacaciones, permisos, licencias, retiros etc, debe ser reportada por la agremiación o por la oficina de personal por escrito o por correo electrónico, con el fin de realizarse el cambio respectivo.

**RESPONSABLE:** Ingeniero de sistemas

**Las cuentas de usuario y su aprobación:**

Se solicita por correo electrónico la oficina de agremiación y talento humano verifica que si se realice la modificación y su inactivación si es el caso.

- ✓ **RESPONSABLE DE LOS DATOS INTERNOS:** Ingeniero de Sistemas revisa periódicamente las cuentas y verifica los retiros y las actualizaciones del sistema que no tengan inconvenientes los usuarios.
- ✓ **RESPONSABLE DEL SISTEMA SIHOS:** Empresa Sinergia encargado del soporte y actualización de la información.

**LICENCIAMIENTO DE SOFTWARE**

Como política de seguridad se tiene establecido en el Reglamento de Uso de las áreas funcionales, la prohibición de instalar software y programas no autorizados y sin licencia. El área de sistemas realiza trimestralmente el mantenimiento preventivo un inventario físico de los programas y software instalados en cada uno de los computadores de la Institución.

**MODIFICACION DEL SISTEMA**

**Responsable del cierre de historias clínicas:** los médicos del hospital, son los encargados del cierre y su verificación.

**Responsable de abrir historias clínicas:** Las jefes de enfermeras y la ingeniera de sistemas, con el nombre de la admisión y una descripción que informe por qué se va abrir.

**RESPONSABLE:** Ingeniero de sistemas, jefes de enfermeras

**ADMINISTRACIÓN DE PRIVILEGIOS**

Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al área de Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax: 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[hospitalsanrafaelzarzal@telecom.com.co](mailto:hospitalsanrafaelzarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

sistemas (Administrador de la Red), para el cambio de privilegios.

**RESPONSABLE:** Ingeniero de sistemas

**Responsable del mantenimiento de la base de datos:** El ingeniero de sistemas coge la carpeta cron ubicada en el servidor central donde está instalado el sistema sihos, que no se encuentre llena y que mensualmente se esté borrando las copias repetidas y solo se deje una por mensual hasta tener por año 12 que luego son almacenadas en un disco duro.

### SEGURIDAD DE SISTEMAS DE INFORMACION

- ✓ Política: El área de sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como los backup de datos de información automatizados.
- ✓ Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el área de sistemas, También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Hospital Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por la Oficina Nuevas Tecnologías al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información

**RESPONSABLE:** Ingeniero de Sistemas

### VIOLACIONES DE SEGURIDAD INFORMÁTICA

- ✓ Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de sistemas.
- ✓ Ningún usuario del Hospital debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de sistemas.
- ✓ No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, Políticas y Estándares de Seguridad Informática, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Hospital.

**RESPONSABLE:** Ingeniero de Sistemas

### CONTROL DE ACCESOS REMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

información y del área de sistemas y la Gerencia del Hospital.

**RESPONSABLE:** Ingeniero de Sistemas, auxiliares de sistemas y personal autorizado por la gerencia

#### CONTROLES DE ACCESO LÓGICO

- ✓ Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.
- ✓ Todos los usuarios deberán informar los mecanismos de control de acceso provistos por el área de sistemas antes de poder usar la infraestructura tecnológica del hospital
- ✓ Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de del hospital, a menos que se tenga el visto bueno Políticas y Estándares de Seguridad Informática.

**RESPONSABLE:** Ingeniero de Sistemas

#### SEGURIDAD HARWARE, SOFTWARE Y REDES

##### PROCEDIMIENTO SEGURIDAD DE LA RED INALAMBRICA:

- ✓ Para la red inalámbrica se tiene la seguridad por registro de ip, registro de mac, y se tiene clave de acceso no podrá entrar a l red inalámbrica e internet ningún equipo de cómputo o móvil que llegue al hospital y quiera acceder a menos que llegue a sistema para su registro en donde se llenan los datos de la persona nueva o temporal. **RESONSABLE:** Ingeniero de Sistemas

##### ADMINISTRACIÓN DE LA RED

- ✓ Los usuarios de las áreas del hospital no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del hospital, sin la autorización del área de sistemas.
- ✓ EL hospital en cada computador tiene activo el firewalls la red esta unificada por grupos de trabajo según el área y se encuentra segmentada en varias áreas con el fin de mantener una integridad de la información.

**RESONSABLE:** Ingeniero de Sistemas

##### SEGURIDAD PARA LA RED

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

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

#### **REDES DE DATOS CABLEADA E INALAMBRICA:**

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

#### **EL ROUTER Y LA SEGURIDAD**

El área tesorería se encuentra aislado por seguridad de los datos en donde se trabaja con el portal del banco y tiene asignado una ip fija en donde nadie puede acceder a ella.

#### **SWITCHES:**

Uno se encuentra en sistemas y los otros dos en la oficina de estadística, dentro de un gabinete para evitar el polvo y la humedad y están protegidos con ups para evitar los bajones de energía, el de sistemas tiene malla a tierra y está pegado toda el área de sistemas a la subestación de energía con una línea independiente.

**RESPONDABLE:** Ingeniero de sistemas

#### **SEGURIDAD SISTEMA OPERATIVO**

**ANTIVIRUS:** Todos los equipos antes de trabajar con ellos el usuario se les instala un antivirus gratuito.

#### **ENTRADA AL SISTEMA WINDOWS:**

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

**RESPONSABLES:** Usuarios del sistema

#### **SEGURIDAD DEL SISTEMA DE INFORMACION**

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

**RESPONSABLE:** Ingeniero de Sistemas

#### **SEGURIDAD FISICA AL CENTRO DE CÓMPUTO**

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

✓ **PROCEDIMIENTO PARA LA ENTRADA Y SALIDA DEL PERSONAL DE SISTEMAS:**

Para la entrada en la puerta se tiene un candado en los que solo el personal encargado tiene llave de esa puerta, cada vez que la oficina va a quedar sola se debe cerrar y por ningún motivo se debe dejar abierta a si sea que el personal no se demora en la actividad fuera que realice.

**RESPONSABLES:** Ingeniero de Sistemas y auxiliar 1 y 2

**ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO**

- ✓ Política: Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de Hospital. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.
- ✓ Los usuarios y funcionarios de Hospital que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.
- ✓ El Área de sistemas en cabeza del Jefe de Sistemas, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las áreas funcionales del hospital restringidas.
- ✓ Todo equipo informático ingresado al área de sistemas restringidos deberá ser registrado en el libro de visitas.
- ✓ Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
- ✓ El Jefe del área de sistemas deberá solicitar a la gerencia los equipos de protección para las instalaciones contra incendios

**RESPONSABLE DE LA ENTRADA:** Auxiliar de sistemas 1, Auxiliar de Sistemas 2, ingeniero de Sistemas.

**EQUIPOS DE CÓMPUTO**

**Procedimiento seguridad equipos de cómputo**

A los equipos de cómputo se les hace mantenimiento preventivo trimestralmente

**RESPONSABLE DEL MANTENIMIENTO DE EQUIPOS:** Auxiliar de sistemas 1

**RED ELECTRICA**

**LA RED ELECTRICA DE LOS COMPUTADORES:**

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

El área de Mantenimiento en el caso de que se tenga algún inconveniente con algún toma de los router computadores o demás instalaciones eléctricas el área encargada es el área de mantenimiento.

**RESPONSABLE DEL MANTENIMIENTO DE LA RED ELECTRICA:**

Es el área de Mantenimiento y el responsable es el jefe inmediato del área.

**USO DEL INTERNET**

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

- ✓ Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Hospital, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de sistemas.
- ✓ Los usuarios de Internet del Hospital tienen que reportar todos los incidentes de seguridad informática al área de sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- ✓ Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados. Saben que existe la prohibición de descarga de software sin la autorización del área de sistemas. La utilización de Internet es para el desempeño de sus funciones y cargo en el Hospital y no para propósitos personales.

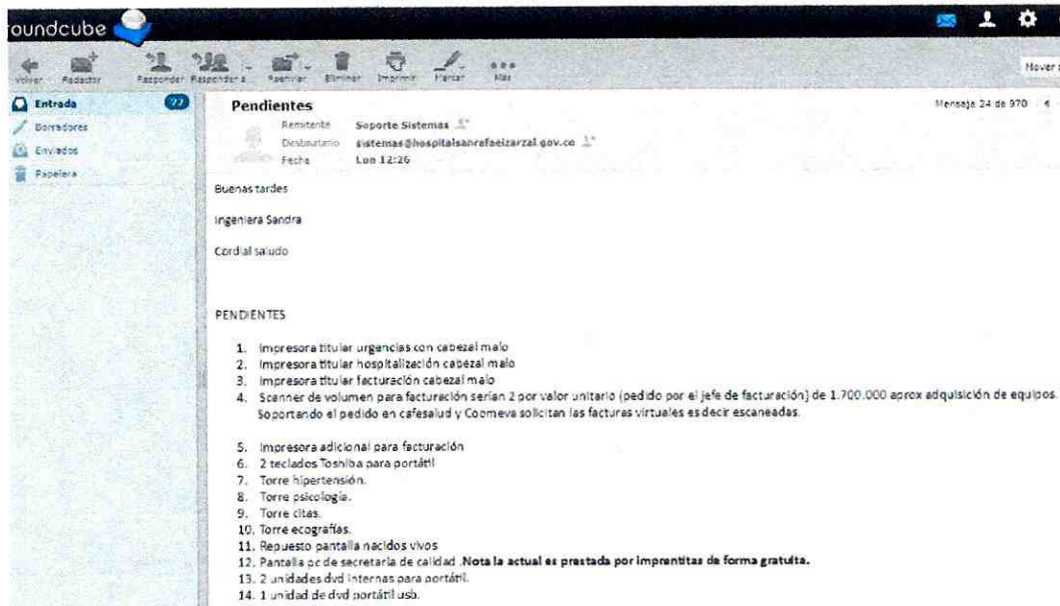
**RESTRICCIONES PARA EL ACCESO A INTERNET**

- ✓ El área de sistemas instala en los equipos de cómputo el archivo host con las paginas prohibidas para que el usuario no acceda sin autorización, se crea una cuenta invitado y administrador para que no lo modifiquen y no puedan ver ni instalar los DNS para internet.
- ✓ Para la acceder a la red inalámbrica el router está con filtrado de mac y con una ip estática que tiene que ser consultada al área de sistemas para poder instalarla.
- ✓ Se coloca nombres raros para que no se encuentre fácil la red.
- ✓ El acceso a internet está restringido para personas de fuera del hospital a menos que la gerencia autorice.
- ✓ Se cambia constantemente la puerta de enlace para evitar intrusos.

**SOLICITUD DE PEDIDOS**

Los pedidos de sistemas se hacen por correo electrónico al área administrativa Adjunto: 2016-2019

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	PÁGINA: 24 de 42	



Se envían adjunto listado de pendientes y se va solicitando en correo la viabilidad de la compra sea un insumo o una solicitud de un servicio.

## CONTROLES EN LA COMPRA DE COMPUTADORES

### USO DE DISPOSITIVOS EXTRAÍBLES

- ✓ El área de sistemas, velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- ✓ Cada Jefe de Área o dependencia debe reportar al área de sistemas el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.
- ✓ El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- ✓ El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.
- ✓ Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el área de sistemas con el respectivo visto bueno de la gerencia o



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

en su defecto de su Jefe inmediato o un superior

### **PÉRDIDA DE EQUIPO**

- ✓ El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- ✓ El préstamo de portátiles tendrá que solicitarse al área de sistemas, con el visto bueno del encargado de sistemas.
- ✓ El servidor o funcionario deberán dar aviso inmediato al área de sistemas, y a la Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

### **MANTENIMIENTO DE EQUIPOS**

- ✓ Únicamente el personal autorizado por el área de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.
- ✓ Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación

### **PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS**

- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de sistemas en caso de requerir este.
- ✓ El Área de Inventarios de activos o almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el area de sistemas
- ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores del hospital.
- ✓ Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.
- ✓ Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- ✓ Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**

**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**



CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 26 de 42

- ✓ Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- ✓ El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal del área de sistemas.
- ✓ Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación a el área de sistemas a través de un plan detallado.
- ✓ Queda terminantemente prohibido que el usuario o funcionario distinto al personal del área de sistemas abra o destape los equipos de cómputo.

#### **CONTROLES DE ACCESO FÍSICO**

- ✓ Cualquier persona que tenga acceso a las instalaciones del hospital, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.
- ✓ Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones del hospital únicamente con la autorización de salida del área de sistemas.
- ✓ El acceso al centro de cómputo está restringido por un letrero y solo entra el personal que está autorizado.

#### **PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMÁTICOS**

- ✓ El usuario o funcionario deberán reportar de forma inmediata al área de sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
- ✓ El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- ✓ Es responsabilidad del usuario o funcionario evitar en todo momento o la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

#### **PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMÁTICOS**

El usuario o funcionario deberán reportar de forma inmediata al área de sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- ✓ El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

confidencial o importante.

#### **SANCIONES**

- ✓ Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático

#### **CAPACITACIÓN EN SEGURIDAD INFORMÁTICA**

- ✓ Todo servidor o funcionario nuevo en el hospital deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

#### **OBLIGACIONES DE LOS USUARIOS**

- ✓ Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

#### **USUARIOS NUEVOS**

- ✓ Todo el personal nuevo de del hospital, deberá ser notificado al área de sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

#### **EQUIPO DESATENDIDO**

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados y autorizados por el área de sistemas cuando no se encuentren en su lugar de trabajo.

#### **SEGURIDAD INSTITUCIONAL**

- ✓ Política: Toda persona que ingresa como usuario nuevo al hospital para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

#### **EVALUACIÓN DE LAS POLÍTICAS**

- ✓ Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## PLANES DE CONTINGENCIA ANTE DESASTRE

### INFORMATICO

Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos, Ver Manual de Contingencias.

Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total.

### CONTROLES PARA LA GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO (BACKUPS)

Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

- ✓ Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores. Se pasaran a un disco duro externo diariamente y también se hace automáticamente 4 copias. El área de sistemas es la responsable de realizar las copias del sistema sihos.
- ✓ Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.
- ✓ Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas. Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.
- ✓ Se utilizará el programa Nero Express en la opción Copia de Seguridad o Back Up: Aplicación PC, Copiar Disco } Opción Datos: se escoge CD o DVD }
- ✓ Se añaden los archivos o carpetas Clic en cerrar } Clic en siguiente } Se introduce un CD o DVD en blanco en la unidad quemador de CD o DVD } Colocar nombre al disco (16 caracteres) } Si la información no abarca 700 megas en CD o 4.3 gigas en DVD se habilita } la pestaña: Permitir añadir archivos posteriormente. Clic en grabar } Marcar el CD o DVD colocándole la fecha de la copia y entregar a su Jefe } inmediato para su almacenamiento y custodia.
- ✓ Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el último día hábil del mes. Un funcionario del área de sistemas revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

### ALMACENAMIENTO PARA EL RESGUARDO DE PROGRAMAS Y ARCHIVOS DE DATOS

En el servidor se realizan copias de seguridad diarias de las cuales se van a un disco duro diferente donde se encuentra la información general del sistema y se sacan a un disco duro externo por si hay algún daño total del equipo luego se entregan archivo central para la salvaguarda.

**RESPONSABLE:** Ingeniero de sistemas

### CONTROLES CONTRA VIRUS O SOFTWARE MALICIOSO

- ✓ Para revisar si el antivirus se actualiza correctamente, seleccione el icono de su programa antivirus Nod32, toda memoria que se coloque en el puerto usb del computador debe ser vacunada.

Se vacuna con software gratuito para evitar compra de licencias.

### USO DEL CORREO ELECTRÓNICO

- ✓ Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al hospital, a menos que cuente con la autorización del área de sistemas.
- ✓ Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del hospital. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
- ✓ Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- ✓ Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

### IDENTIFICACIÓN DEL INCIDENTE

- ✓ El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- ✓ Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar a la área de sistemas.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

- ✓ Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del hospital debe ser reportado a área de sistemas.

### USO DE MEDIOS DE ALMACENAMIENTO

Los usuarios y servidores del hospital deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC's) del hospital serán registradas y podrán ser objeto de auditoría.

### Sistemas de información

Describe la situación actual de los sistemas de información de acuerdo con las siguientes categorías (definidas en el dominio de sistemas de información del Marco de Referencia – Documento de generalidades):

#### Sistemas misionales:

**Aplicativo sihos: Versión 2016:** Es un sistema de información totalmente integrado el área asistencial y financiera para el manejo de la facturación y evolución de la historia clínica sistematizada.

**Tecnologías Sinergia S.A.S** gerencia@sinergiaonline.com - www.sinergiaonline.com Teléfonos: +57 (8)2712383 / 2713588 Celular: + 57 (316) 529 9660 / (316) 281 0910  
 Todos los Derechos Reservados 2015.

**Líder TI:** Ing. Sandra Milena Rincón Isaza

#### Módulos que lo componen el aplicativo sihos:

Facturación, Admisiones, Citas médicas, Contabilidad, Cartera, Glosas, Nomina, Consulta Externa, consulta especializada, inventarios, liquidación de servicios, Observación e internación, Odontología, presupuesto, procedimientos, promoción y prevención, terapia, tesorería, triage, urgencias.

### Servicios Tecnológicos

Situación actual de los servicios tecnológicos de acuerdo con las siguientes categorías:

La gestión de los servicios tecnológicos se realiza de manera centralizada desde la sede principal Hospital Departamental San Rafael y las sedes rurales y urbanas entran por ip pública al aplicativo sihos, usando el medio de comunicación internet, todas estas son administradas por sistema de información central del hospital.



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**



**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 31 de 42

## 11. MANUAL DE FUNCIONES

<b>I. IDENTIFICACION</b>	<b>66679932</b>
<b>Nivel:</b>	<b>Ingeniero</b>
<b>Denominación del Empleado:</b>	<b>Ingeniera de sistemas</b>
<b>No de cargos:</b>	<b>Uno (1)</b>
<b>Dependencia</b>	<b>Sistemas</b>
<b>Cargo del Jefe Inmediato</b>	<b>Subgerencia Administrativa</b>

### PROPOSITO PRINCIPAL

Administración de los recursos informáticos del hospital en hardware y software y las redes de datos, sitio web del hospital, soporte técnico a usuarios, soporte en el envío de informes a los entes de control y capacitación a los usuarios.

### DESCRIPCION DE FUNCIONES ESENCIALES

1. Administración de la base de datos sihos
2. Administración de la red de datos
3. Soporte técnico a los usuarios
4. Soporte en el envío de archivos a los entes de control
5. Capacitaciones a los usuarios, y Asesorar el personal del hospital sobre el uso y el manejo de los equipos informáticos (hardware y software).
6. Recarga de cartuchos de impresoras de tinta, programación del video proyector para las reuniones.
7. Programar préstamo de video proyector
8. Actualización de hoja de vida de los equipos y de inventarios
9. Realizar copias de seguridad de la información sihos diariamente.
10. Instalación de programas.
11. Configuración de impresoras locales y de red.
12. Entrada y salida de equipos para reparación
13. Adecuación de equipos nuevos
14. Actualización del sitio web del hospital

### FUNCIONES BASICAS DEL CARGO EN RELACION CON LOS PROCESOS:

1. Proceso para la administración de la base de datos Proceso para la creación de usuarios.
2. Administración de la red datos, auditoría y control de la red de datos supervisándola con software de monitoreo de red y revisión de direcciones IP
3. Soporte técnico en sistemas a los usuarios del hospital y los centros de salud
4. Soporte en el envío de archivos a los entes de control
5. Capacitación a usuarios
6. Recarga de cartuchos de tinta, se trae del área funcional el cartucho, se recarga con la tinta solicitada en almacén y luego se llena el formato y se hace firmar a la persona la carpeta.


	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

7. Programar préstamo de video proyector, Se llena un formato para el préstamo de video proyector y lo deben de firmar a la hora de entregarlo
8. Actualización de hoja de vida de los equipos, actualización de inventarios
9. Realizar copias de seguridad de la información sihos
10. Instalación de programas
11. Formateo de los equipos. Se verifica el equipo en hardware y el software necesario para la utilización,
12. Configuración de impresoras locales y de red.
13. Entrada y salida de equipos para reparación
14. Instalación de programas cuando se requiera, programa de laboratorio( anexo 1)

### 12. ESTRATEGIA DE SERVICIOS TECNOLOGICOS

La estrategia para la prestación de los servicios tecnológicos en cuanto a disponibilidad, operación continúa, soporte a los usuarios, administración y mantenimiento.

#### Soporte técnico

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL E.S.E.</b>																			
												Solicitud No. <input type="text"/>								
	<b>AREA DE SISTEMAS DE INFORMACION</b> <b>SOLICITUD DE SOPORTE TECNICO Y NECESIDADES POR USUARIO</b>																			
<b>casos:</b>																				
web	Fac	Red	imp	pc	Por	Cap	Soft	Rec	Proye	inf	Sist	Reun	Mto							
<b>Fecha de la Solicitud:</b>		DD	MM	AÑO	Soporte técnico															
					Ingeniera:															
<b>Area:</b>					pasante:															
<b>Solicitado por:</b>																				
<b>Descripción del problema:</b>																				
<table border="1" style="width: 100%;"> <tr> <td style="width: 30%;"><b>Quie Recibe</b></td> <td style="width: 30%;"><b>Quien Resuelve</b></td> <td style="width: 20%;"><b>Fecha Resuelto</b></td> <td style="width: 20%;"><b>Firma</b></td> </tr> <tr> <td><input type="text"/></td> <td></td> <td></td> <td></td> </tr> </table>													<b>Quie Recibe</b>	<b>Quien Resuelve</b>	<b>Fecha Resuelto</b>	<b>Firma</b>	<input type="text"/>			
<b>Quie Recibe</b>	<b>Quien Resuelve</b>	<b>Fecha Resuelto</b>	<b>Firma</b>																	
<input type="text"/>																				
			<input type="text"/>			<table border="1" style="width: 100%;"> <tr> <td>dd</td> <td>mm</td> <td>Año</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table>			dd	mm	Año	<input type="text"/>	<input type="text"/>	<input type="text"/>						
dd	mm	Año																		
<input type="text"/>	<input type="text"/>	<input type="text"/>																		

#### Soporte en correo institucional

En el correo institucional del área de sistemas se subdivide en 3 correos:

[sistemas@hospitalsanrafaelzarzal.gov.co](mailto:sistemas@hospitalsanrafaelzarzal.gov.co)

Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)

[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)



	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

[mantenimiento@hospitalsanrafaelzarzal.gov.co](mailto:mantenimiento@hospitalsanrafaelzarzal.gov.co)

[soporte@hospitalsanrafaelzarzal.gov.co](mailto:soporte@hospitalsanrafaelzarzal.gov.co)

En los cuales los usuarios pueden realizar sus solicitudes de manera virtual, para así lograr evitar el gasto de papel.

## MANTENIMIENTO DE EQUIPOS

### PLAN MANTENIMIENTO PREVENTIVO 2020

#### OBJETIVO

Efectuar el servicio de mantenimiento preventivo, para garantizar que los equipos de cómputo se conserven en condiciones óptimas de funcionamiento, previniendo las posibles averías y fallas, y consiguiendo así que el trabajo se realice con los mayores niveles de calidad y seguridad, distribuidos en las diferentes áreas de la institución.

#### ALCANCE

Este procedimiento es aplicable a los usuarios que cuenten con un equipo de cómputo.

#### NORMAS DE OPERACIÓN

Se notificará vía email o telefónico y hasta con un día de anticipación, al jefe del servicio, la fecha en que se llevará a cabo el mantenimiento. En caso de que el servicio tenga cargas de trabajo que impidan la aplicación del mantenimiento, se deberá notificar con el fin de ser reprogramado.

El mantenimiento preventivo que se aplicará consistirá en la limpieza de las cubiertas exteriores del equipo (chasis) y el interior del mismo, el cual consta de monitor, CPU, teclado, mouse, impresora y demás periféricos. También se realizará un diagnóstico a fin de verificar el buen funcionamiento del equipo eliminando virus informáticos en caso de que existan y la reinstalación de software cuando sea necesario (en caso de existir reinstalación de sistema operativo con el pc se alargara 5 horas de trabajo por cuestión de copias de seguridad y reinstalación).

Una vez realizado el mantenimiento, el usuario deberá verificar el funcionamiento de su equipo a fin de detectar cualquier desperfecto. Una vez revisado el equipo y recibido de conformidad, cualquier avería posterior tendrá que ser reportada de forma inmediata.

Cada reporte de mantenimiento preventivo deberá estar firmado por el responsable del servicio o usuario del equipo cuando el mantenimiento esté concluido.

Nota: el cronograma está sujeto a modificaciones. Por parte de la administración en los casos que los operarios sean perfilados a otras actividades no dispuestas en el cronograma.

#### CRONOGRAMA DE MANTENIMIENTO PREVENTIVO

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

En las siguientes dos hojas, se indican las fechas programadas por servicio para el Mantenimiento Preventivo, así como también el número de equipos desktop e impresoras.

DEPENDENCIA	FECHA	EQUIPOS		Total	
		DE MESA	PORTATIL	EQUIPOS	IMPRESORAS

#### **Estrategia de mejoras de sistemas**

Cuál es la estrategia para la prestación de los servicios tecnológicos en cuanto a implementación de mejores prácticas.

Se realiza un diagnostico en las áreas del hospital y las sedes y se realiza planes de mejoramiento para finiquitar los problemas.

#### **Estrategia de tercerización**

Cuál es la estrategia de la institución pública en cuánto a tercerización de los servicios tecnológicos.

- ✓ Se tiene un contrato de soporte y mantenimiento del aplicativo SIHOS de la empresa Sinergia S.A., el cual es actualizado cada año.
- ✓ Se tiene contrato de mantenimiento de las impresoras externo con la empresa grupo tecnológico impretintas, el cual realiza mantenimiento preventivo y correctivo a las impresoras del hospital y las sedes al igual que dentro del mismo contrato se tiene una cláusula de disponibilidad, que empieza a regir después de que los funcionarios dejan de laborar se activa la cláusula de lunes a lunes fuera del horario de oficina, sábados domingos festivos, y después de las 5: 0 de la tarde hasta las 7 de la mañana del siguiente día.
- ✓ Compra de equipos se hace con la empresa grupo tecnológico impretintas.

#### **Administración de sistemas de información:**

- ✓ La persona encargada de administrar los servicios tecnológicos es la ingeniera Sandra Milena Rincón Isaza, el cual realiza la administración del sistema basado en el punto

#### **Sistemas de información**

- ✓ Se encuentran alojados los sistemas de información en el área de sistema del hospital también hay un parte en el área de estadística que son switches, y router en lugares estratégicos para dar conectividad, y el gabinete central y el switche principal está alojado en el área de sistemas.
- ✓ Con la empresa sinergia S.A. se realizan las solicitudes de desarrollo y quedan estipuladas para que en cada actualización estas sean actualizadas en el sistema del Hospital el cual ya previamente le han hecho el control de calidad a la información y las bases de datos no van a sufrir ningún colapso.

#### **Infraestructura:**

Se describe los componentes de infraestructura del Hospital la institución, detallando para cada Calle 5 No. 6-32, Zarzal – Valle del Cauca, Tel: 2220046 – 2220043 – 2209914, Fax. 106, Urgencias 2209585

[www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co)  
[hospitalsanrafaeldezarzal@telecom.com.co](mailto:hospitalsanrafaeldezarzal@telecom.com.co) - [hospitaldepartamentalsanrafael@hotmail.com](mailto:hospitaldepartamentalsanrafael@hotmail.com)



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
 Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

CÓDIGO: P-GDG 01    VERSIÓN: 2    FECHA: 01/02/2014    TRD: 24-07    PÁGINA: 35 de 42

componente los sistemas de información, bases de datos, el hardware y equipos de cómputo y telecomunicaciones, y en general todos los servicios tecnológicos que soporta.

**Inventario de sistemas de información y equipos de cómputo ,2019**



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**INVENTARIO DE EQUIPOS DE COMPUTO AREA DE SISTEMAS DE INFORMACIÓN**  
**A DICIEMBRE 31 DE 2018**



N.º	AREA	COMPUTADORES-UPS- ESTABILIZADOR					IMPRESORAS					PERIFERICOS		
		DE MESA	ABILIZADOR	UPS	SERVIDOR	TOD O EN UNO	POR TATI L	TINTA	CARTA	ASEI	MULTIFUCI		KE	MAT RIZ DE QUIN
1	ALMACEN	2	1	1						1				
2	PROMOTORAS	1		1										
3	ARCHIVO CENTRAL	1		1										
4	SISTEMAS	4	1	2	3		1	2						
5	FACTURACION CUENTAS MEDICA	8	1	8		1		2			2			1
6	HOSPITALIZACION CAMAS			3			5					1		
7	HOSPITALIZACION PEDIATRIA						1							
8	FACTURACION CAJAS HOSPITALIZ	1		1				1			1			
9	LABORATORIO	2		3										
10	FACTURACION LABORATORIO	1	1					1				1		
11	QUIROFANO						3					1		
12	ACTIVOS FIJOS Y/O CALIDAD					1								
13	OBSTETRICIA (maternidad)		1					2				1		
14	PROGRAMACION DE CIRUGIAS	1		1										
15	VENTANILLA UNICA	1		1				1						
16	ANEXOS	1	1											
17	CITAS	1	1									1		
18	SIAU	1	1					1						
19	FACTURACION CAJAS PRINCIPAL	3		2				2				1		
20	CONSULTORIO MEDICOS NUEVOS	1		1										
21	CONSULTORIO MEDICOS NUEVOS 2	1	1									1		
22	TRABAJO SOCIAL	1		1										
23	TALENTO HUMANO	1	1					1						
24	CONSULTA EXTERNA	1		2			7	1				3		
25	ESTADISTICA	4	3	2				1		1				
26	TERAPIA FISICA Y RESPIRATORIA	1					1							
27	PSICOLOGO	1	1											
28	FACTURACION CAJA PYP PROMD	2		2				1				1		
29	VACUNACION			1		1	1	1						
30	ODONTOLOGIA	2		2			2					1		
31	CITOLOGIA	1		1										
32	ECOGRAFIAS	1		1										
33	CRECIMIENTO Y DESARROLLO	1	1											
34	MEDICO PYP (consultorio 3)						1							
35	URGENCIAS PLAN B	1	1									1		
36	CRONICOS (EMA)	1		1								1		
37	PLANIFICACION FAMILIAR						1							
38	URGENCIAS	3		5		5		2				1		
39	TRIAGE			1		1								



HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.  
VALLE DEL CAUCA  
Nit: 891900441-1



SISTEMAS DE INFORMACION  
PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION  
PETI

CÓDIGO: P-GDG 01    VERSIÓN: 2    FECHA: 01/02/2014    TRD: 24-07    PÁGINA: 36 de 42



HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.  
INVENTARIO DE EQUIPOS DE COMPUTO AREA DE SISTEMAS DE INFORMACIÓN  
A DICIEMBRE 31 DE 2018



N o.	AREA	COMPUTADORES-UPS- ESTABILIZADOR					IMPRESORAS					RIFERIC		
		DE MESA	ABILIZAD	UPS	SERVI DOR	TOD O EN UNO	POR TATI L	FINTA	CART	ASEI	MULTIFUC		ICKE	MAT RIZ DE PUNT
40	RAYOS X						1							
41	SUB CIENTIFICA	1		1							1			
42	GERENCIA			1		1	1	1						
43	SECRETARIA DE GERENCIA	1		1				1						
44	SUBDIRECCION ADMINISTRATIVA	1		1							1			
45	AUXILIAR DE PRESUPUESTO			1		1								
46	PRESUPUESTO	1		1					1	1				
47	CONTROL INTERNO	1		1										
48	GLOSAS			1		1								
49	CARTERA	1		1										
50	CONTABILIDAD	1		1				1						
51	JURIDICA	1		1				1						
52	CONTRATACION	1	1											
53	TESORERIA	1	1	1				1						
54	CONSULTORIO TBC						1							
55	CONSULTORIO CONTROL MEDICO PRENATAL						1							
56	Barrio Bolivar	3		2			1	1				1		
57	La Paila	3		2			2	1					1	
58	IAMI	1		1										
59	ASKI	1												
60	REPUESTO	2					1							
61	SANEAMIENTO						1							
62	REFERENCIA Y CONTRAREFERENCIA (BODEGA)						1							
63	REMANENTES										3			
64	PENDIENTE INSTALAR SUBGEREN	1												
65	FARMACIA	2		2				1				1		
66	PENDIENTE INSTALAR ANGELA	1												
67	AUXILIAR DE CARTERA						1							
<b>TOTAL</b>		<b>75</b>	<b>18</b>	<b>63</b>	<b>3</b>	<b>12</b>	<b>36</b>	<b>25</b>	<b>1</b>	<b>8</b>	<b>3</b>	<b>18</b>	<b>1</b>	<b>1</b>
<b>TOTAL FINAL</b>							<b>189</b>						<b>56</b>	<b>1</b>
<b>TOTAL COMPUTADORES</b>							<b>126</b>							

**Conectividad:**

**Arquitectura de las redes de datos del Hospital:**

- ✓ **Redes cableadas:** las áreas cableadas son algunas cajas, presupuesto, contabilidad, sistemas, almacén, estadística, odontología un equipo, laboratorio, programación de cirugías, ventanilla única.
- ✓ **Redes inalámbrica:** las áreas conectadas son facturación, área financiera, área e consulta externa, urgencias, cajas de pyp, archivo, hospitalización, cirugía, pediatría, ginecología, medico pyp, citología.
- ✓ **Canales de internet:** Fibra óptica con ert 4 megas dedicado, movistar para el área financiera 10 megas, tesorería 7 megas movistar, urgencias 7 megas movistar 5.
- ✓ **Hosting:** La página web del Hospital tiene dominio [www.hospitalsanrafaelzarzal.gov.co](http://www.hospitalsanrafaelzarzal.gov.co) y está alojada en Colombia hosting
- ✓ **Backup:** Las copias de seguridad se suben a dropbox la nube

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

#### Sedes del Hospital:

- ✓ Sede Barrio Bolívar: 12 megas movistar
- ✓ Sede la Paila movistar 2 megas.
- ✓ **Ip pública:** los centros de salud entran al aplicativo del Hospital por una ip pública.

Servicios de operación: Se catalogan como servicios de operación aquellos que garantizan la operación, mantenimiento y soporte de la plataforma tecnológica; de las aplicaciones, de los sistemas de información y de los servicios informáticos.

- ✓ Las personas encargadas de la infraestructura tecnológica del Hospital son:

**Soporte técnico:** Victor Hugo Bernal Libreros

**Mantenimiento de equipos de cómputo:** Jhonathán Agudelo Cardona

Existen contratos de soporte técnico fuera del horario laboral con la empresa Grupo tecnológico y el mantenimiento de impresoras es externo.

- ✓ Quién realiza la administración y operación de las aplicaciones, es la ingeniera Sandra Milena Rincón contratada por medio tiempo y existen contratos de soporte de las aplicaciones con la empresa sinergia S. A. y contrato de mantenimiento y actualización.
- ✓ La ingeniera Sandra Milena Rincón Isaza realiza la administración y operación de los servicios informáticos (correo electrónico institucional y la instalación todos los integrantes de sistemas, telefonía (contrato externo), comunicaciones unificadas (2 proveedores Movistar y ERT como plan B) , DNS (Google, Movistar y ERT), , antivirus (NOd 32), , mesa de servicios (área de sistemas extensión (122), existen contratos de soporte para los servicios informáticos con el grupo tecnológico impretintas.

#### Gestión de Información

Se identifica en el punto 2.5.3 Sistemas de información, Los cuellos de botella del hospital, se basan en el manejo de las impresoras, y la red inalámbrica del hospital que es deficiente su conectividad hacia el aplicativo sihos (lentitud).

- ✓ Red eléctrica con muchos bajones de energía
- ✓ Planta eléctrica no cuenta con automático.

A partir de esta información se realiza un análisis general del estado de la gestión de la información del hospital: principales esfuerzos y logros, problemáticas y recomendaciones generales.

#### PLAN DE ACCION:



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
 Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 38 de 42

<b>Gestión de la Infraestructura Tecnológica, Software Hardware, Redes y Comunicaciones</b>	Solicitud de proyecto para el automático de la planta eléctrica	Favorecer los equipos de cómputo para que no se quemen por altibajos de energía	2016-2019	Se estima que en el año 2019.
	Adquisición de software de ventanilla única y archivo.	Dar cumplimiento a la ley, por organización del área	2016-2019	Se estima que en el año 2019.
	Compra de ticket y cajón para consultorio nuevo	Mejorar el servicio de entrega de la formula medica	2016-2019	Se estima que en el año 2019.
	Instalación del internet en las veredas	Conectividad en las veredas para acceder al servidor del hospital	2016-2019	Se estima que en el año 2019.
	Renovación de equipos	Aumentar el rendimiento y la velocidad	2016-2019	Se estima que en el año 2019.
	Cambio de la red inalámbrica a red cableada	Prestar un mejor servicio sin caídas del sistema y conectividad eficiente y rápida.	2016-2019	Se estima que en el año 2019.
	Capacitaciones al personal	Capacitar al personal en el manejo de la historia clínica y realizar convenio con el sena cartago para cursos cortos presenciales	2016-2019	Se estima que en el año 2019.
	Reforma a la red eléctrica del Hospital	Evitar los bajones de energía que dañen fuentes de poder	2016-2019	Se estima que en el año 2019.

	<b>HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.</b> <b>VALLE DEL CAUCA</b> <b>Nit: 891900441-1</b>				
	<b>SISTEMAS DE INFORMACION</b> <b>PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION</b> <b>PETI</b>				
	CÓDIGO: P-GDG 01	VERSIÓN: 2	FECHA: 01/02/2014	TRD: 24-07	

## SOFTWARE

	Creación de nuevos correos institucionales	Fomentar la cultura del cero papel.	2016-2019.	Se estima que en el año 2016-2019.
	Mejoras en el Sitio Web	Mejorar, actualizar y crear nuevas estrategias de gobierno en línea para el sitio web del Hospital	2016-2019.	Se estima que en el año 2016-2019.

## Gobierno de TI

Estructura Organizacional y Talento Humano., detallando la cantidad de personas que conforman el área, sus funciones, el tipo de contratación (Agremiada sindical), es ingeniera de sistemas, coordinadora del área de sistemas, Tecnólogo electrónico soporte técnico (planta), Mantenimiento de equipos de cómputo tecnólogo sistemas (Agremiado sindical) La cantidad de personas que soportan el área son 3 presenciales y la empresa del grupo tecnológico como tercero.



## ENTENDIMIENTO ESTRATÉGICO

### Modelo operativo



**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
**Nit: 891900441-1**



**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

CÓDIGO: P-GDG 01

VERSIÓN: 2

FECHA: 01/02/2014

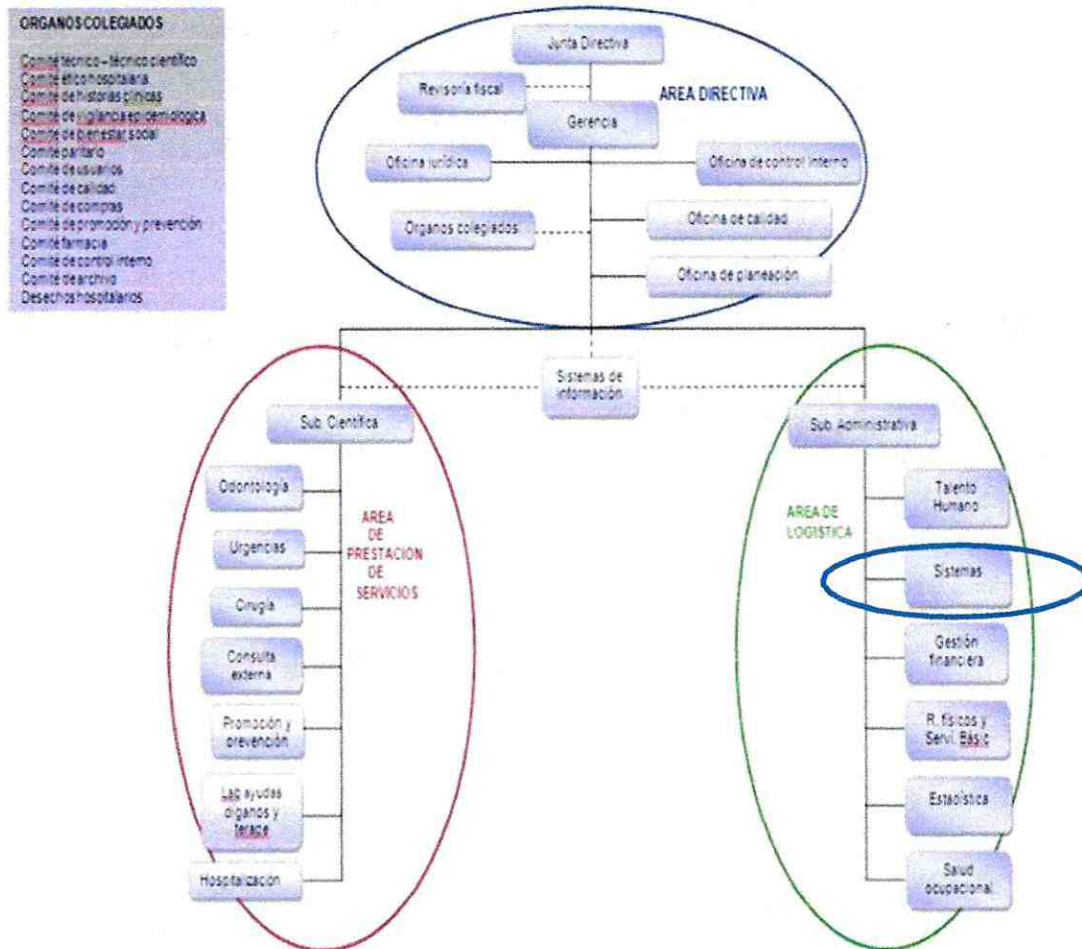
TRD: 24-07

PÁGINA: 40 de 42

## Organigrama



### ORGANIGRAMA HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL



**Área de sistemas de información 2019**

**Soporte técnico indicadores por funcionario**





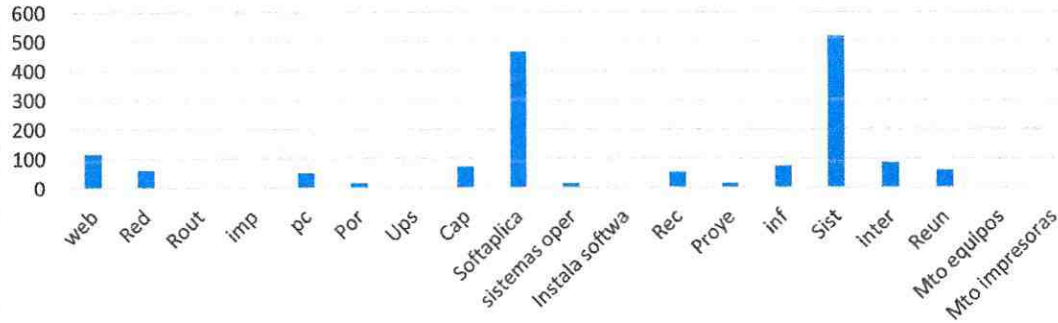
**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
 Nit: 891900441-1



**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

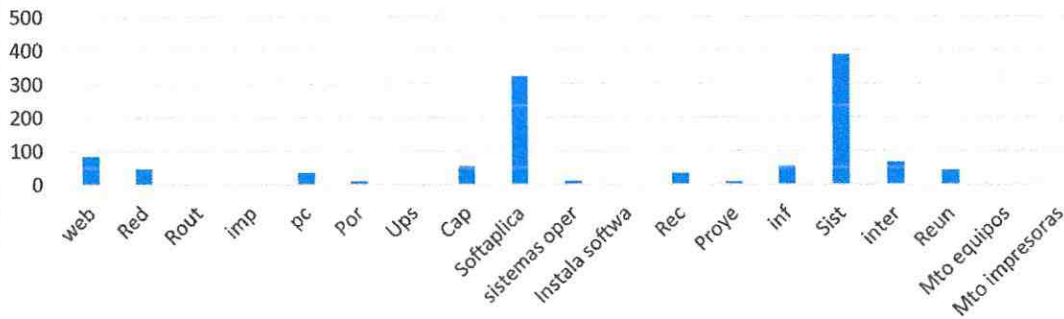
CÓDIGO: P-GDG 01    VERSIÓN: 2    FECHA: 01/02/2014    TRD: 24-07    PÁGINA: 41 de 42

Consolidado anual por Hospital y sus sedes, servicios areas de sistemas



Consolidado total de servicios atendidos por el area de sistemas

Hospital Departamental San Rafael



Consolidado total de solucion de casos por el area de sistemas



■ Presencial    ■ Telefonico    ■ Remoto    ■ Correo



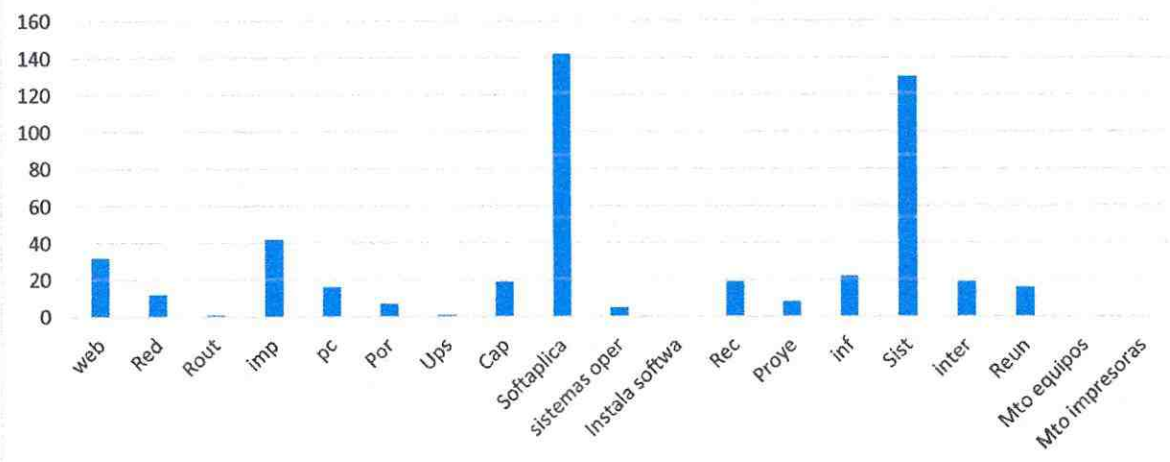
**HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**  
**VALLE DEL CAUCA**  
 Nit: 891900441-1



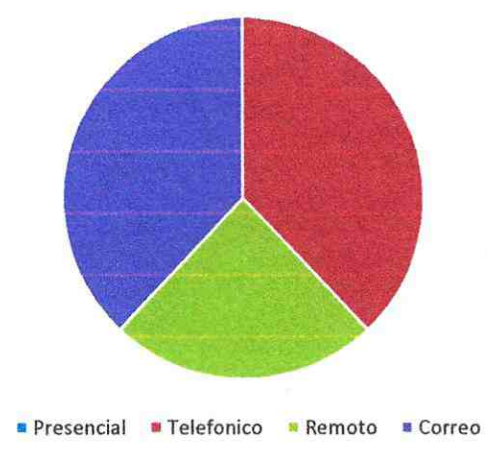
**SISTEMAS DE INFORMACION**  
**PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION**  
**PETI**

CÓDIGO: P-GDG 01    VERSIÓN: 2    FECHA: 01/02/2014    TRD: 24-07    PÁGINA: 42 de 42

**CONSOLIDADO DE SERVICIOS PRESTADOS LA PAILA**



**Solución de casos por la centro de salud de la Paila**





HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.  
VALLE DEL CAUCA  
Nít: 891900441-1



SISTEMAS DE INFORMACION  
PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION  
PETI

CÓDIGO: P-GDG 01

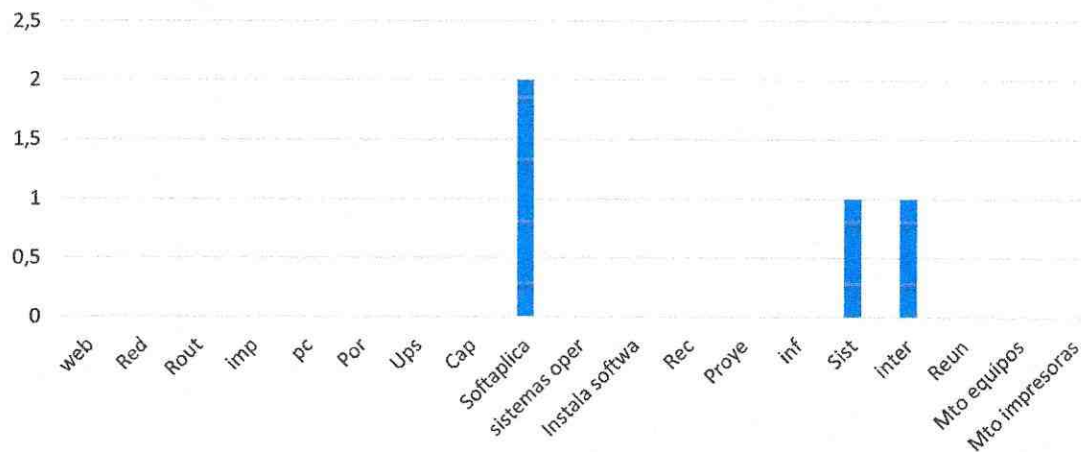
VERSIÓN: 2

FECHA: 01/02/2014

TRD: 24-07

PÁGINA: 43 de 42

### CONSOLIDADO DE SERVICIOS PRESTADOS BARRIO BOLIVAR



### Solución de casos centro de salud Barrio Bolívar

