E.S.E Hospital
San Juan de Dios
El Carmen de Viboral
¡Protegemos y proyectamos la salud y la vida!

# D-GIN-005

# E.S.E SAN JUAN DE DIOS EL CARMEN DE VIBORAL

# PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA PETIC

## Actualización a Enero 2023

# TABLA DE CONTENIDO

## 1. PROPÓSITO DEL PETI

**El Plan Estratégico de Sistemas de Información – PETI**, tiene como propósito el de establecer una guía de acción clara y precisa para la administración de las Tecnologías de Información y Comunicaciones (TIC) del **HOSPITAL SAN JUAN DE DIOS DEL CARMEN DE VIBORAL**, mediante la formulación de estrategias y proyectos que garanticen el apoyo al cumplimiento de sus objetivos y funciones, en línea con el Plan de Desarrollo Institucional del Hospital actual.

Los proyectos y estrategias definidos en este documento son el resultado de análisis definidos previamente que tienen como objetivo el crecimiento tecnológico del Hospital San Juan de Dios de El Carmen de Viboral, sustentados en procesos continuos, ordenados, dinámicos y flexibles, con enfoque en el servicio a la comunidad y optimicen la toma de decisiones.

## 2. ALCANCE DEL PETI

Este documento describe las estrategias y proyectos que ejecutará el E.S.E HOSPITAL SAN JUAN DE DIOS, durante cada año, en cumplimiento de sus funciones y para el logro de sus objetivos; establece las estrategias que se aplicarán para lograrlo y establece las **POLÍTICAS DE LA PLANEACIÓN INFORMÁTICA.**

La línea de base sobre la que nace este documento son los objetivos, planes, políticas y estrategias del Plan de Desarrollo Institucional del Hospital San Juan de Dios

E.S.E y la guía de Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI del Mintic, 2016.

En este documento pretendemos definir acciones para realizar a corto y mediano plazo que permitan el crecimiento y la evolución del Hospital en el desarrollo de las TICs, articulando cada uno con las estrategias definidas en el Plan Estratégico del Hospital.

## 3. BENEFICIOS DE LA PLANEACIÓN Y JUSTIFICACIÓN DEL PETI

El Plan Estratégico de Sistemas de Información - PETI permite al **E.S.E HOSPITAL SAN JUAN DE DIOS DEL CARMEN DE VIBORAL**, evaluar la forma de como beneficiarse de la tecnología, logrando un esquema de operación integrada, unificada y reconociendo oportunidades de ahorro y consolidación de esfuerzos.

El E.S.E, HOSPITAL SAN JUAN DE DIOS formula el Plan Estratégico de Sistemas de información PETI involucrando los componentes del Plan de Desarrollo, por lo cual no es independiente a las estrategias trazadas en el mismo y contribuye a su cumplimiento de los objetivos de la institución.

La definición de políticas, estándares, metodologías, directrices y recomendaciones permiten beneficiar a los usuarios de los recursos informáticos, uso efectivo de tecnologías emergentes, aprovechamiento de herramientas y de redes de comunicaciones.

En conclusión los beneficios del PETI son:

- Garantizar la alineación del PETI con el Plan Estratégico de la Entidad
- Garantizar la contribución de las TICs al cumplimiento de los objetivos institucionales.
- Utilización de las TICs de la manera más conveniente para la entidad
- Orientar a los encargados de Tecnología en la forma de apoyar los objetivos institucionales

## 4. NORMATIVIDAD

| NORMA | DESCRIPCION |
|---|---|
| Directiva Presidencial 02 de 2002 | Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software). |
| Ley 872 de 2003 | Con esta Ley se ordena la creación del Sistema de Gestión de Calidad (SGC) en las instituciones del Estado, como una herramienta para la gestión sistemática y transparente, que permita dirigir y evaluar el desempeño institucional en términos de calidad y satisfacción social con la prestación de los servicios, enmarcada en los planes estratégicos y de desarrollo que el sector Estatal debe cumplir para ejercer su función social. |
| DECRETO 1011 DE 2006 | Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud. |
| RESOLUCIÓN 1445 DE 2006 | El cumplimiento del Sistema Único de Acreditación es voluntario para las IPS de naturaleza privada. Para las IPS de naturaleza pública, entre estos las Empresas Sociales del Estado (E.S.E.) |
| Decreto Nacional 1151 del 14 de abril de 2008 y Manual para la implementación de la Estrategia de Gobierno en Línea de la República de Colombia | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones. |
| Ley 1273 de 2009 | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las |

| | |
|---|---|
| | tecnologías de la información y las comunicaciones, entre otras disposiciones |
| Decreto 0019 de 2012 | Por la cual se dictan normas para suprimir o reformar regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública. |
| Resolución 123 de 2012 | Por la cual se modifica el artículo 2 de la Resolución 1445 de 2006. |
| Constitución Política 1991 Articulo 61 | El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley |

## 5. MAPA DE PROCESOS


## 6. FILOSOFIA ESTRATEGICA DEL DEPARTAMENTO DE SISTEMAS

### 6.1. MISION

La misión del Departamento de Sistemas del ESE San Juan de Dios de El Carmen de Viboral, es la de apoyar la buena prestación de los servicios, en los niveles operativo, administrativo y estratégico, implementando un sistema de información dentro de los criterios de adecuación tecnológica que sirvan de apoyo al crecimiento, organización y proyección de la institución.

## 6.2. VISION

En el año 2024 la plataforma, los procesos y procedimientos tecnológicos de la E.S.E Hospital San Juan de Dios de El Carmen de Viboral, serán reconocidos por su alto desempeño y permanente estabilidad y confiabilidad; posicionándose como una de las mejores de la región y destacándose por su permanente innovación.

## 6.3. POLÍTICAS INFORMÁTICAS

En el departamento de sistemas del E.S.E HOSPITAL SAN JUAN DE DIOS, se establecen las siguientes políticas en cuanto a relación de cada usuario.

Cada que ingresa un usuario a la institución, se entrega el formato F-GIN-003, el cual se diligencia con todos los accesos a las aplicaciones de la institución y se anexa detrás las siguientes políticas. Como evidencia de recibido el usuario firma en un listado de recibido de claves de usuarios

1. Políticas de Seguridad
2. Políticas de Contraseñas y el control de acceso
3. Políticas para uso de Cuentas usuarios

Políticas de equipos

Estas políticas aplican a equipos cuando se instalan o formatean, y lo hace el área de sistemas antes de la entrega al usuario final y se maneja con forma de dicho usuario verificando la entrega de los mismos

En resumen, contamos con 42 políticas así:

| | |
|---|---|
| Políticas de Seguridad: | 26 |
| políticas de contraseñas y control de acceso | 3 |
| políticas para uso de cuentas de usuarios | 5 |
| Políticas de equipos | 8 |
| TOTAL | 42 |

Las políticas generales, son las siguientes:

**Políticas de Seguridad:**

- Conocer y aplicar las políticas y procedimientos apropiados con relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax, servidores) para otras actividades que no estén directamente relacionadas con el trabajo ..
- Proteger meticulosamente su contraseña, por ningún motivo revelársela a nadie y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta (mínimo 8 dígitos) y que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente al área de Sistemas cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales y que considere aun en los mínimos aspectos como inesperada o impredecible.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse en las horas no laborables.
- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.
- Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas.
- No se permite fumar, comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua, etc).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- No pueden moverse los equipos o reubicarlos sin permiso. Para cambiar de lugar y/o llevar un equipo fuera de alguna sede del Hospital, Se requiere del Área de sistemas.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Área de sistemas o a los Directivos de la Compañía
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar. Ejemplo: un mensaje de correo electrónico cuyo objetivo es transmitir o comunicar información confidencial.
- No se debe llevar al sitio de trabajo computadores portátiles (Laptops, NoteBooks) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (como un disquete, CD, USB, etc.), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa.
- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Área de Sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.
- Para prevenir demandas legales o la introducción de virus informáticos, no debe instalarse software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución freeware o shareware, a menos que haya sido previamente aprobado por el Área de Sistemas.
- No deben usarse disquetes u otros medios de almacenamiento en cualquier computadora a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.
- No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañia.
- El personal que utiliza un computador portátil que contenga información confidencial, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información en la medida de lo posible, debe estar cifrada.

**Políticas de Contraseñas y el control de acceso:**

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

**Políticas para uso de Cuentas usuarios:**

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

## 7. PLANEACIÓN DE INFORMÁTICA

Es importante para el Hospital, definir procesos de Planeación de Sistemas con el fin de direccionar el camino para establecer esquemas de coordinación tecnológica mediante las siguientes metas:

- El Plan Estratégico de Sistemas, responde al Plan de Desarrollo del Hospital.
- El Plan Estratégico de Sistemas, está direccionado hacia el Plan de Gestión el cual contiene los objetivos de la entidad.
- El Plan Estratégico de Sistemas, está orientado a apoyar los procesos que actualmente se implementan en el Hospital como parte del Sistema Integral de Gestión de la calidad.
- El Plan Estratégico de Sistemas permitirá establecer lineamientos de apoyo para el cumplimiento de la implementación de las políticas de Gobierno Electrónico y Racionalización de Trámites liderado por la Alcaldía Municipal.
- Los proyectos de inversiones que contemple el Plan Estratégico de Sistemas deben estar definidos con base en el levantamiento de autodiagnóstico sobre la Infraestructura Física, Procedimientos y Gestión para los diferentes subsistemas de tecnología y sus respectivos componentes que son Cableado estructurado, equipos de Cómputo, Sistema Telefónico, Internet, Sistemas Operativos, Servicios de red, etc.
- Anualmente, se desarrolla un plan operativo de Sistemas de información, el cual detalla las actividades a desarrollar en el periodo, con base en los documentos del area de sistemas que se actualizan periódicamente y los diagnósticos realizados durante el año anterior.
- El Plan operativo se debe mantener actualizado a cada vigencia en lo referente a diagnósticos, línea de base, dimensionamiento de infraestructuras tecnológicas y avances en ejecución.

## 8. ESTANDARIZACIÓN

El Hospital mediante la adopción de estándares, planea facilitar el mejoramiento de la integración informática y la comunicación, propiciando alto grado de compatibilidad y previniendo la duplicación de esfuerzos para la apropiación de soluciones tecnológicas.

Adicionalmente, los estándares serán complementarios a las políticas de

Seguridad Informática aprobadas por el Hospital.

## 8.1. ESTRATEGIA

La Estrategia Informática del Hospital, está orientada hacia los siguientes parámetros

- Implementar estándares relacionados con
  - ✓ Estándares para Equipo
  - ✓ Estándares para el licenciamiento de software
  - ✓ Estándares para la definición de Proyectos Inversión de Sistemas de Información
  - ✓ Estándares para la Adquisición de Recursos Tecnológicos
  - ✓ Estándares para la página WEB, Correo Interno y Correos Externos Institucionales
- Coordinación entre las diversas áreas de servicios del Hospital.
- Contar en el programa de Inducción orientada al trabajo a realizar, inclusión de las Políticas Institucionales de seguridad y uso de recursos informáticos, al momento de iniciar labores con el Hospital.
- Aprovechamiento de los recursos tecnológicos en forma eficiente y eficaz.
- Promover la cultura informática en el Hospital.
- Incentivar el uso de los recursos informáticos de comunicaciones.
- Identificar los Activos de Información con el fin de fortalecer la integración de sistemas y bases de datos del Hospital, para tener como meta final, un Sistema Integral de Información.

## 8.2. ESTÁNDARES PARA EQUIPO

Las características mínimas de requerimiento, serán determinadas acorde con la tecnología de punta accesible a nuestras condiciones financieras, tanto en velocidad, capacidad, transferencia de datos, en voz e imágenes y compatibilidad con la infraestructura del parque computacional del Hospital. (Tanto para equipos de cómputo como para impresoras).

Los equipos que se adquieran deberán tener su licenciamiento completo a nivel de sistema operativo.

## 8.3. ESTÁNDARES PARA EL LICENCIAMIENTO DE SOFTWARE

Con el fin de asegurar la compatibilidad y el transporte de documentos serán bajo licencias de Microsoft Windows.

Todo equipo que se requiera conectar a la red de cableado estructurado del Hospital deberá contar con el respectivo licenciamiento del software en cuanto al sistema operativo y tener los aplicativos instalados. Para el control de estas instalaciones, se diligencia el formato F-GIN-005, el cual contiene la lista de verificación de cada una de los requerimientos de cada equipo, según el area a laborar. Este registro debe ser firmado por el area que recibe el equipo. Por ninguna razón, se permite el ingreso de equipos personales o de otras Instituciones a la red del Hospital.

La instalación de cualquier licencia de software se realizará a través del personal del área de Sistemas, lo que mitigará los riesgos o contingencias legales derivadas del uso de plataformas o soluciones que involucren innovaciones protegidas por derechos de propiedad intelectual.

## 8.4. ESTÁNDARES PARA LA DEFINICIÓN DE PROYECTOS INVERSIÓN DE SISTEMAS DE INFORMACIÓN

La definición de los proyectos de hardware, software o especiales de Sistemas de Información estarán orientados en disminuir la brecha marcada por el Autodiagnóstico, quién permite identificar qué aspectos requieren de una atención más inmediata.

Los proyectos de sistemas se desarrollan con base en las necesidades del Hospital a nivel de

- Actualización Tecnológica,
- Sistemas de Información eficientes,
- Seguridad de la información (Firewall físico y Antivirus) y
- Accesibilidad a los recursos informáticos de red (Intranet e Internet).

- Integración del manejo de información a través de un sistema de información
- Desarrollos adicionales según identificación de necesidades específicas.

## 8.5. ESTÁNDARES PARA LA ADQUISICIÓN DE RECURSOS TECNOLÓGICOS

Estos estandares, están definidos en el documento D-GIN-001, administración del sistema de información.

## 8.6. ESTÁNDARES PARA LA PÁGINA WEB, CORREO INTERNO Y CORREOS EXTERNOS INSTITUCIONALES

El Hospital desarrolla su página web en la plataforma gratuita de Une Tigo, y se utilizan las herramientas de diseño y seguridad establecidas en esta plataforma.

Desde el PETI se apoyará al área de Comunicaciones de la Alcaldía Municipal en la implementación del Gobierno en Línea y Antitrámites según la normatividad.

El área de Comunicaciones del Hospital en conjunto con el area de Sistemas del Hospital, direcciona las actualizaciones de la Página WEB del Hospital.

El correo electrónico Institucional se maneja con dominio del Hospital y ya sea en servidor interno o externo administrado por terceros y con administración propia, de manera que los funcionarios del Hospital cuenten con su correo propio institucional, el cual tiene como estandarización, el cargo del usuario, para que sea heredable a las personas que realicen la misma función, en caso de cambio de funcionarios.

La información a Entidades Externas se enviara a través de los correos electrónicos institucionales asignados por el área de Sistemas y solo se permite acceso a correos personales, a áreas con restricciones administradas por el area de sistemas.

## 9. SEGURIDAD Y CONTROL

### 9.1. PROPÓSITO

La **seguridad informática** consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para que un sistema se pueda definir como seguro debe tener estas cuatro características

- Integridad: La información sólo puede ser modificada por quien está autorizado.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

El Hospital, si es necesario, ajustará sus Políticas de Seguridad Informática a través de los documentos del area de sistemas.

### 9.2. ALCANCE

La Política de Seguridad Informática del Hospital aplica a todos los activos de información de la institución.

El Hospital define como los Activos de Información:

- Elementos de Hardware y de Software de procesamiento.
- Almacenamiento y comunicaciones.
- Bases de Datos y Procesos.

- Procedimientos y Recursos Humanos asociados con el manejo de los datos.
- La Información Misional, Operativa y Administrativa del Hospital
- Elementos de hardware y de software del Hospital

De la misma forma, estas políticas están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como el Internet y Correo Electrónico, brindando a los funcionarios pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida.

Estas Políticas aplican a todos los funcionarios, consultores, contratistas, o terceras personas que accedan a los activos de información del Hospital, con las respectivas autorizaciones los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que los trabajadores del Hospital.

## 9.3. CUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad es obligatorio y extensible a todos los funcionarios, consultores, contratistas, o terceras personas que accedan a los activos de Información del Hospital. El incumplimiento de las políticas por negligencia o intencionalidad, hará que el Hospital tome las medidas correspondientes, tales como acciones disciplinarias, cesación del contrato de prestación de servicios, acciones legales, reclamo de compensación por daños, etc.

## 9.4. ACCESO A LOS RECURSOS DE INFORMACIÓN

Todos los funcionarios, consultores, contratistas, o terceras personas que accedan a los activos de información del Hospital deben ser autorizados previamente sin discriminación alguna por parte del area de sistemas y tienen los siguientes deberes:

- Se debe custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción,

ocultamiento o utilización indebidas.

- Se debe vigilar y salvaguardar los útiles, equipos, que le han sido encomendados y su utilización de acuerdo al uso de las buenas prácticas, y racionalmente, de conformidad con los fines a que han sido destinados.
- El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización. Esta autorización es asignada por el area de Sistemas.
- El acceso a los recursos de información de la organización presupone la aceptación de este documento de políticas de seguridad, así como las respectivas sanciones por su incumplimiento, lo cual se confirma a través de la firma de un acuerdo de responsabilidad, F-GIN-006.
- Los funcionarios del Hospital, deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con las funciones propias de la organización y que esta sea utilizada de acuerdo a los criterios de confidencialidad definidos por el Hospital.

## 9.5. PROTECCIÓN DE LA INFORMACIÓN

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida de los activos de la información del Hospital. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

Todos los funcionarios, consultores, contratistas, o terceras personas que accedan a los activos de información del Hospital deben

- Definir y ejecutar procedimientos de seguridad para la entrega de información, apoyándose de algunos lineamientos muy claros donde se determine qué información se considera confidencial, restringida o pública.
- La copia de seguridad de información, es responsabilidad de todos los funcionarios, consultores, contratistas, o terceras personas que accedan a estos activos informáticos. Se diligencia el formato de control, para que del area de sistemas se revise constantemente la programación del cobian y de las rutas de las copias.

- El Hospital garantizara el almacenamiento externo de la copia de seguridad de la información del aplicativo Institucional.

## 9.6. PROTECCIÓN DE LOS RECURSOS TECNOLÓGICOS

El Hospital asegurará la contratación requerida para mantener actualizadas las licencias de Antivirus y Firewall, las cuales permitirán proteger los recursos informáticos contra ataques de virus, ingresos maliciosos y filtrados de contenido de correos, archivos, USB, CD, etc.

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida del negocio. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales y así mismo, su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

La infraestructura de Servidores y equipos de telecomunicaciones del Hospital, está ubicada en un área protegida o cerrada, en la cual sólo se permitirá el ingreso de personal autorizado, es decir, a quienes deban cumplir alguna función específica relacionada con dichos equipos.

## 9.7. AUTORIZACIÓN DE USUARIOS

Todos los usuarios deben ser identificados independientemente con permisos de acceso específicamente e individualmente autorizados. Los métodos de acceso de usuarios deben exigir un proceso de autenticación.

Para cumplir con esta política, desde el area de Sistemas del Hospital, se cuenta con los documentos D-GIN-001, D-GIN-002 y D-GIN-003, en los cuales se describen los aplicativos y los permisos por grupos de usuarios. En el momento de ingreso de un nuevo usuario, se asignan los permisos según el area donde laborara y se diligencia el formato F-GIN-003 con los usuarios y claves a los aplicativos a ingresar.

## 9.8. RESPONSABILIDAD

Los usuarios y custodios de los activos de información del Hospital, son responsables por el uso apropiado, protección y privacidad de estos activos.

Los sistemas generarán y mantendrán unas apropiadas reglas de auditoría para identificar usuarios, y documentar los eventos relacionados con eventos de seguridad.

Los activos de información deben estar disponibles para soportar los objetivos del Hospital. Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y acceso por individuos autorizados.

El área de sistemas del Hospital tiene el plan de contingencias y recuperación en el documento D-GIN-003, para garantizar la continuidad del negocio.

## 9.9. INTEGRIDAD

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

## 9.10. PLANES DE CONTINGENCIA

El Plan de Contingencia adoptado por el Hospital en el documento D-GIN-003, contiene las siguientes directrices:

- Contemplar todos los tipos de riesgos posibles para la entidad y los planes de acción en cada caso.
- Ser revisado periódicamente de acuerdo con el Plan Estratégico de Sistemas (PETI) y con cambios en las condiciones operativas de la entidad.

## 9.11. DEMOCRATIZACIÓN DE LA INFORMACIÓN

El Hospital San Juan de Dios de El Carmen de Viboral, cuenta con un portal www.hospitalcarmenv.gov.co, el cual está disponible para el ciudadano 24x7.

El Hospital a través del area de sistemas y con el apoyo de comunicaciones deberá garantizar el cumplimiento de la normatividad nacional en cuanto a "Estrategia de Gobierno en Línea y Antitrámites", según las directrices del Comité de Gobierno en línea de la Alcaldía Municipal.

En cuanto a la definición de los alcances del acceso a Internet por parte de los funcionarios del Hospital, se tienen definidos PERFILES de acuerdo al área, el manejo de información requerido y al nivel de consulta que se requieran realizar para el desarrollo de las actividades de cada uno de los funcionarios autorizados; con el fin de determinar un uso adecuado de los recursos con que cuenta el Hospital (Ancho de Banda).

A nivel de la Intranet cada usuario autorizado cuenta con un buzón de correo a través del cual se facilita la comunicación entre las diferentes áreas y la socialización de información.

Se debe promover el uso de la intranet (red de comunicación interna), el uso institucional de Internet y el chat interno, entre los funcionarios de la entidad para abrir espacios de socialización de la información.
El hospital cuenta con canal en Youtube y redes sociales, los cuales son administrados desde el area de comunicaciones.

## 9.12. CALIDAD

El Plan Estratégico de Sistemas de Información del Hospital, estará ajustándose dinámicamente de acuerdo a los cambios y necesidades para el cumplimiento de los objetivos generales, al Sistema de Gestión de la Calidad (Ley 872 de 2003), a los estándares de Acreditación (Resolución 123 de 2012) y a la implementación del Modelo Estándar de Control Interno MECI (Decreto 1599 de 2005), Iso y demás sistemas con los que cuenta el Hospital; en lo referente a los componentes de Sistemas de Información.

## 9.13. RACIONALIZACIÓN DEL GASTO

La definición de los proyectos de hardware, software o especiales de Sistemas de Información estarán orientados en disminuir la brecha marcada en el Autodiagnóstico, quién permite identificar qué aspectos requieren de una atención más inmediata.

## 9.14. CULTURA INFORMÁTICA

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

## Políticas Generales sobre Cultura Informática

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

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

El Profesional de Sistemas del Hospital, deberán proveer la experiencia técnica para asegurar que la información del Hospital se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan.

Los usuarios son responsables de familiarizarse y cumplir con las políticas de seguridad de información, las dudas que puedan surgir alrededor de éstas deben ser consultadas con el Profesional de Sistemas del Hospital.

En forma periódica el area de Sistemas del Hospital, debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad, lo mismo que para verificar el cumplimiento de los estándares de configuración en las diferentes plataformas técnicas e instalaciones de tecnología de información.

Los sistemas de cómputo del Hospital deben ser utilizados únicamente para propósitos institucionales.

En los equipos de cómputo del Hospital no se pueden almacenar, instalar o utilizar juegos o música u otros programas no autorizados.

La utilización de la información del Hospital para cualquier propósito diferente para el cual ha sido específicamente creada, requiere permiso escrito del gerente del Hospital.

El área de Sistemas del Hospital realizará revisiones selectivas a la información almacenada en los equipos de cómputo con el fin de verificar la utilización del recurso.

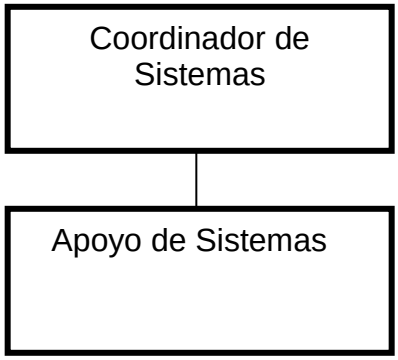
El área de Sistemas realizará la socialización de los procedimientos sobre el manejo de soportes técnicos a los usuarios.

El servicio de navegación en Internet que ofrece el Hospital solamente está permitido a páginas Institucionales, gubernamentales y educativas y aquellas que manejen información clínica de importancia para el Hospital. Solo los jefes de area, tienen acceso ilimitado a Internet.

Ningún usuario está autorizado para utilizar un acceso a Internet diferente al estándar configurado en los equipos del hospital, lo anterior aplica en forma general para todos los equipos pertenecientes al Hospital.

Ningún usuario del Hospital está autorizado para bajar software desde Internet (archivos, herramientas, parches, protectores de pantalla, etc.), ni para instalar ningún software en los equipos de cómputo que provenga de medios no autorizados (CD´s, diskettes, conexiones vía módem, etc.).

## 9.15. ESTRUCTURA ORGANIZACIONAL DE LA DEPENDENCIA DE SISTEMAS




## 9.16. DOCUMENTOS ADICIONALES DEL AREA DE SISTEMAS:

Para dar cumplimiento a todo el proceso de gerencia de la información, se cuenta con los siguientes documentos y formatos:

| | |
|---|---|
| P-GIN-001 | Procedimiento de administración del sistema de información |
| P-GIN-002 | Soporte técnico |
| F-GIN-001 | Formato de control de bases de datos |
| F-GIN-002 | Formato de Requerimientos internos de información |
| F-GIN-003 | Formato de asignación de claves |
| F-GIN-004 | Formato de Control de copias de seguridad |
| F-GIN-005 | Formato Control Formateo de Equipos |
| F-GIN-006 | Formato de acuerdo de responsabilidad de uso de elementos informáticos e información |
| F-GIB-011 | Inventario equipos de computo |
| T-GIN-001 | Tabla de requerimientos de información |
| D-GIN-001 | Documento de administración del Sistema |
| D-GIN-002 | Descripción del sistema de Información |
| D-GIN-003 | Manual de Contingencia de los recursos informáticos |
| D-GIN-004 | Política Protección De Datos |
| D-GIN-005 | PETI |