# PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA PETIC

**E.S.E HOSPITAL SANTA ISABEL DE GOMEZ PLATA**

**2022**

# Plan Estratégico de Sistemas de Información y Tecnología PETIC - 2021

## E.S.E Hospital Santa Isabel

## Contenido

## OBJETIVOS

### Objetivo General

- Diseñar el plan estratégico de tecnologías de la información en la E.S.E Hospital Santa Isabel de Gómez Plata y unidades funcionales relacionadas a la misma.
- Adoptar las conductas de seguridad activa y pasiva que posibiliten la protección de los datos y del propio individuo en sus interacciones en Internet y en la gestión de recursos y aplicaciones locales.
- Utilizar con seguridad y eficacia sistemas operativos de uso común, tanto bajo licencia como de libre distribución.

### Objetivos Específicos

- Elaborar plan estratégico acorde con el plan de desarrollo de E.S.E Hospital Santa Isabel.
- Mejorar los recursos tecnológicos para el desarrollo de las actividades desempeñadas.
- Hacer seguimiento continuo a la tecnología y software adquirido por la E.S.E.
- Administrar bases de datos institucionales, redes de interconexión institucional y sistemas de soporte informático.
- Adquirir e implantar sistemas y aplicaciones informáticas, planteando la utilización de tecnologías avanzadas en el campo de la informática.
- Proporcionar capacitación y acompañamiento a los usuarios en el manejo de los sistemas de información.

## • JUSTIFICACION

- Con el fin de ayudar al mejoramiento de los procesos y lograr establecer una cultura en el cliente interno, respecto al cuidado de los equipos de cómputo e ingreso de datos; entre otros. El presente plan requiere de una serie de condiciones, tanto internas, como externas para edificar un entorno de trabajo adecuado. Debe partir de la modernización técnica, definición de roles para que el personal garantice la prestación del servicio de las TICs y reestructuración de funciones.

- Se espera contar con la participación decidida de todos y cada uno de los actores internos.

(personal administrativo, asistencial y directivo) para el logro de este plan, para que éstas permitan brindar al paciente y su familia una mejor y oportuna atención.

## PROPORSITO DEL PETIC

El Plan Estratégico de Sistemas de Información – PETIC, tiene como propósito el de establecer una guía de acción clara y precisa para la administración de las tecnologías de información y comunicaciones (TIC) de la E.S.E Hospital Santa Isabel de Gómez Plata, 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.

## ALCANCE DEL PETIC

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.

## Beneficiarios de la planeación y Justificación del PETIC

El E.S.E, Hospital Santa Isabel formula el Plan Estratégico de Sistemas de información PETIC 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 PETIC son:

- ✓ Garantizar la alineación del PETIC 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.

## Marco Normativo

| NORMA | DESCRIPCIÓN |
|---|---|
| **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. |
| **NTCGP 1000:2009** | Permite a las entidades del Estado de la Rama Ejecutiva del Poder Público evaluar y dirigir el desempeño institucional en términos de calidad y de satisfacción social, de manera sistemática y transparente, de acuerdo con lo establecido en el Artículo 2 de la Ley 872/2003. |
| **Constitución Política 1991 Articulo 61** | El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley |

## Retos Estratégicos

Teniendo en cuenta puntos estratégicos: los contenidos y aplicaciones, plataformas, conexión, financiación, los cuales dan las bases para el desarrollo del plan, se definen unos interrogantes que se convierten en los retos estratégicos que darán pie a los objetivos de este plan:

- ✓ ¿Cómo podemos promover la producción, difusión y recepción de contenidos a través del uso de las TIC?
- ✓ ¿Cómo podemos mejorar la capacitación y creación de ambientes favorables para el aprovechamiento de las TIC?
- ✓ ¿Cómo podemos lograr la conectividad y mejorar la infraestructura de TIC a bajo costo y mejor calidad para la institución?

- ✓ ¿Cómo obtener, aumentar o mejorar los conceptos de sostenibilidad para la inserción, instalación y uso de TIC para la institución?

## 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.

**SEGURIDAD Y CONTROL**

## 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 área de sistemas.

## 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.

## 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 área 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 área 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.

## 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.
- ✓ El hospital garantizara el almacenamiento externo de la copia de seguridad de la información del aplicativo Institucional.

**Política 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 entidad.
- 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 corporativas,

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.

**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.

## Glosario de Términos

**TIC: Tecnologías de la Información y la Comunicación**

**Internet**: Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí**.**

**Intranet**: Es una red informática que utiliza el protocolo de internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

**Miembros de esa organización tienen acceso a ella.**

**Software**: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

**Ofimático**: es el conjunto de métodos, aplicaciones y herramientas informáticas que se usan en labores de oficina con el fin de perfeccionar, optimizar, mejorar el trabajo y operaciones relacionados. La palabra ofimática es un acrónimo compuesto de la siguiente manera ofi (oficina) y matica (informática).

**Plataformas**: Una plataforma es, por ejemplo, un sistema operativo, un gran software que sirve como base para ejecutar determinadas aplicaciones compatibles con este. También son plataformas la arquitectura de hardware, los lenguajes de programación y sus librerías en tiempo de ejecución, las consolas de videojuegos,

etc.

**Aplicativos**: Es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas. Esto lo diferencia principalmente de otros tipos de programas, como los sistemas operativos (que hacen funcionar la computadora), las utilidades (que realizan tareas de mantenimiento o de uso general), y las herramientas de desarrollo de software (para crear programas informáticos).

**CONTROL DE CAMBIOS**

| ELABORO | REVISO | APROBÒ |
|---|---|---|
| **Bairon Andrés Rendón** | **Alex David Zapata Palacio** | |

| HISTORIAL DE CAMBIOS | | |
|---|---|---|
| VERSION | **ORIGEN DE CAMBIOS** | **FECHA** |
| **02** | Creación de documento | 21/01/2022 |

María Eugenia Correa Z.

Gerente