# PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

## PLANES INTEGRADOS 2025

ESE HOSPITAL SAN CAMILO LELIS

VEGACHI | ANTIOQUIA

## INTRODUCCIÓN

Los sistemas de información son herramientas fundamentales en las empresas prestadoras de servicios de salud para la adecuada toma de decisiones a todo nivel, basados en la integración de la información clínica y administrativa originada en los diferentes procesos de la organización.

Este modelo pretende garantizar la estructura, coherencia y funcionamiento del sistema de información del Hospital para generar una respuesta oportuna y veraz a los requerimientos de los usuarios, sus familias, los funcionarios y demás clientes de la institución.

Además, define la metodología para la estandarización de la información, mecanismos para la seguridad y confidencialidad de la misma, identificación de necesidades y requerimientos de información, diseño y desarrollo, generación, validación y análisis, la tecnología con que se cuenta para apoyar todos los procesos institucionales, el almacenamiento y conservación de la información y el soporte tecnológico necesario para garantizar el adecuado funcionamiento.

## 1 OBJETIVO:

Desarrollar un sistema de información en la institución con criterios de seguridad, oportunidad, confiabilidad y confidencialidad, que permita hacer seguimiento y evaluación de la gestión de la calidad de la atención en salud brindada a los usuarios, tomar decisiones adecuadas basadas en hechos y datos y cumplir con los requerimientos legales y de los clientes internos y externos.

## 2 ALCANCE:

El proceso de gerencia de la información inicia con la identificación de las necesidades de información y termina con los mecanismos para garantizar la seguridad de la información

## 3 RESPONSABLES:

Es responsable de la adecuada implementación del Modelo la Gerencia de la información para la calidad, el Tecnico operativa del area de sistemas, los coordinadores de los servicios y programas son responsables de la generación de los datos, la Gerencia y la Subdireccion administrativa son responsables del análisis de la Información.

## 4 DEFINICIONES:

**Bases de Datos:** Listado en medio magnético o físico de las personas afiliadas al SGSSS suministrado por las entidades aseguradoras o entidades estatales responsables de la población afiliada que tienen contrato con el Hospital.

**Sistema de información:** Conjunto de tecnologías informáticas construidas, procedimientos diseñados, mecanismos de control implementados y asignación de personas responsables de la captura, procesamiento, administración y distribución de datos e información.

**Información Externa:** Conjunto de datos de fuentes externas provenientes de las instancias con las cuales la organización está en permanente contacto, así como de las variables que no están en relación directa con la entidad, pero que afectan su desempeño. Ejemplo: ciudadanía, proveedores, contratistas, entidades reguladoras.

**Información Interna:** Conjunto de datos que se originan y/o procesan al interior de una entidad, provenientes del ejercicio de su función. Información de los diferentes procesos, informes, actas de reuniones, registros contables y de operación, entre otros.

**Minería de Datos** El objetivo general del proceso de minería de datos consiste en extraer información de un conjunto de datos y transformarla en una estructura comprensible para su uso posterior.

**Dato:** Materia prima de la información, registro individual y puntual de un hecho.

**Seguridad:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

**Confidencialidad**: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

**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 semi-privado 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 esta ley. "

**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 esta ley.

**Validez:** Verificación de la corrección de los datos, refleja una situación verdadera

**Hacker**: Persona que, gracias a sus grandes conocimientos informáticos, puede introducirse sin permiso en la información que tengan otros ordenadores o redes informáticas de particulares, empresas o instituciones si están conectados a Internet

**Cracker**: Persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y pueden disponer de muchos medios para introducirse en un sistema

**Correo Electrónico**: Sistema para enviar mensajes en Internet. El emisor de un correo electrónico manda los mensajes a un servidor y éste, a su vez, se encarga de enviárselos al servidor del receptor. Para acceder al correo electrónico es necesario que el receptor se conecte con su servidor

**Internet:** Internet es una Red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).

**Hardware:** Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

**Software:** Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red.

**Malware:** Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios.

**Spyware**: Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal (datos de acceso a Internet, acciones realizadas mientras navega, páginas visitadas, programas instalados en el ordenador, etc.).

**Troyano:** Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

**Backdoor**: Vulnerabilidad de un sistema operativo, página Web o aplicación que puede ser motivo de entrada para hackers, crackers, o gusanos. Uno de los más usados es la aplicación Back Orífice creado específicamente para entrar en sistemas operativos Windows usando troyanos. Puerta trasera.

**Gusano**: Programa informático que se auto duplica y auto propaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes.

**Spam**: Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir loncha de mortadela

**Backups:** Copia de ficheros o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

**Phishing:** Duplicación de una página Web con el objeto o con el efecto de hacer creer al visitante que se encuentra en la en la página original.

**HOAX:** Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real

**RUAF** Registro único de afiliaciones

**SIHO** Sistema de Información Hospitalaria

**SIVIGILA** Sistema de Vigilancia epidemiológica

## 5 GERENCIA DE LA INFORMACIÓN

### 5.1 Principios del sistema de información

- **Gradualidad:** La información que debe entregarse será desarrollada e implementada de manera progresiva en lo relacionado con el tipo de información que se recolectará y se ofrecerá a los usuarios.
- **Sencillez:** La información se presentará de manera que su capacidad sea comprendida y asimilada por la población.
- **Focalización:** La información estará concentrada en transmitir los conceptos fundamentales relacionados con los procesos de toma de decisiones de los usuarios para la selección de las EAPB y las IPS.
- **Validez y confiabilidad:** La información será validada en la medida en que efectivamente presente aspectos centrales de calidad y confiable en cuanto mide calidad en todas las instancias en las cuales sea aplicada.

- **Participación:** En el desarrollo e implementación de la información, participaran de manera activa las entidades integrantes del Sistema General de Seguridad Social en Salud.
- **Eficiencia:** Debe recopilarse solamente la información que sea útil para la evaluación y mejoramiento de la calidad de la atención en salud y debe utilizarse la información que sea recopilada.

### 5.2 Identificación de necesidades de la Información

Los diferentes procesos definen sus necesidades de información para el desarrollo de las actividades y la toma de decisiones, para ello se identifican los requerimientos de entidades externas como los organismos del Gobierno local, departamental y Nacional, Entidades Estatales como organismos de control, Empresas Administradoras de Planes de Beneficio (EABP), Universidades, Organizaciones no Gubernamentales, entre otras y requerimientos internos de otros procesos representada en los datos generados en las actividades, los indicadores de gestión, perfil epidemiológico, indicadores estadísticos, bases de datos.

La identificación de estas necesidades de información se consolida en la Matriz Para El Control Y Seguimiento De Informes Externos E Internos.

### 5.3 Identificación de las Fuentes de información

Toda la información que genera la Institución se obtiene del Software administrativo, financiero y asistencial, en el cual se han registrado todas las atenciones y actividades realizadas a la población y las transacciones de los diferentes procesos.

La información que se genere en puestos de salud y brigadas en las veredas que se encuentre en medio físico se migran a medios electrónicos, ya digitando o escaneando e incorporando al módulo.

Donde se encuentre instalado el software administrativo, financiero y asistencial se realiza directamente las actividades como la facturación, historia clínicas y bases de datos.

El tecnico en sistemas genera los reportes de las actividades de los diferentes servicios y procesos la entrega a los responsables de cada proceso para su análisis. El Comité tecnco cientifico trimestralmente evalúa la gestión de la información y elaboren el plan de mejoramiento de acuerdo a los resultados.

Cada responsable de la información exporta los datos al formato requerido según su necesidad o exigencia de los entes externos.

### 5.4 Validación de los Datos

Para la validación de los datos los líderes de los procesos comparan las diferentes fuentes para corroborar que sean datos verdaderos, en la Matriz para el control y seguimiento de informes internos y externos se define la fuente de validación de datos.

Realizar entrenamiento a los líderes en el manejo del módulo de auditoria a la historia clínica para validar los datos.

La opción de Auditoria en el módulo de Historias Clínicas permite la validación de las atenciones facturadas frente a las atenciones prestadas, lo identifica si hay subfacturación, reingresos en urgencias y hospitalización, volumen de remisiones, entre otros.

Cada módulo administrativo y financiero tiene el mecanismo para la validación de los datos.

### 5.5 Procesamiento de la Información

Extraer y organizar los datos necesarios para la generación de la información tanto asistencial como administrativa por los responsables de los procesos

Los Coordinadores de los servicios recopilan los datos generados en los procesos como eventos adversos, encuestas de satisfacción, tratamientos terminados de odontología, infecciones intrahospitalarias, pacientes controlados en el programa de hipertensión arterial, los datos de la Resolución 4505 de 2012, fichas de vigilancia epidemiológica, bases de datos de los programas de PYP, entre otros. Ver Matriz para el control y seguimiento de informes internos y externos.

La funcionaia de Salud Publica verifica el registro oportuno de los nacidos vivos y defunciones en la plataforma RUAF realizada por el personal médico

Los Coordinadores reportan las horas laboradas, cuadros de turnos, novedades de personal a la Jefe de Talento Humano para la elaboración de la nómina.

Medición de los indicadores de gestión por los líderes de los procesos.

El área de Gestión Financiera en sus diferentes procedimientos procesa la información de acuerdo a los requerimientos legales e internos del Hospital.

Los demás informes están identificados en cada uno de los procedimientos del SIGC con sus respectivos responsables.

### 5.6 Almacenamiento y Aprovechamiento (minería de datos)

### 5.7. Generación de la Información

Elaboración de los diferentes informes de acuerdo a los requerimientos externos e internos de las entidades y los procesos por parte de los Coordinadores y Responsables en cada uno de los procesos, cumpliendo con los plazos establecidos. Ver Matriz para el control y seguimiento de informes internos y externos.

### 5.7 Validación de la Información

Verificar que la información obtenida es correcta y confiable. Para ello utilizar los validadores de las diferentes entidades o la confrontación con otros informes generados en la Institución.

Si se encuentran inconsistencias se hace las correcciones y se valida nuevamente hasta que no se generen errores, garantizando que la información que se envié sea válida y confiable.

### 5.8 Seguridad de la Información

La institución ha definido las Políticas de Seguridad de la Información, las cuales pretenden prevenir y evitar que las amenazas latentes en el entorno puedan acceder, manipular, o deteriorar la información almacenada en el Sistema de Información, indicando a su vez el manejo adecuado de la información institucional generada en los diferentes procesos organizacionales.

El área de sistemas del hospital se encarga de brindar servicio directo al usuario, desde la adquisición, instalación, configuración, puesta en marcha, traslado y accesoria en el manejo de hardware, software y telecomunicaciones.

Capacitación y entrenamiento en el uso de las herramientas informáticas, custodia y resguardo de las bases de datos e información de las diferentes dependencias de la empresa. Así pues, este documento contiene una clasificación de estas políticas, las cuales son:

### 6.4.1 *HARDWARE*

**Adquisición de equipos**

La compra de equipos se realiza por compra directa o a través de invitación pública según los estatutos de contratación.

Los equipos de cómputo, que se adquieren tienen una garantía como mínimo de dos años en el puesto de trabajo

Los equipos que esten presentes en el mercado en línea de ensamblaje en los últimos seis meses.

Los monitores son tipo LCD, con tres años de garantía. Estos equipos permiten un mejor desempeño a los funcionarios pues disminuye los síntomas de fatiga, ojos rojos, y sequedad ocular.

Las impresoras tienen como mínimo una garantía de seis meses, y disponen del sistema de ahorro de energía Powersave y permite configurar los equipos con el modelo de ahorro de energía para que se active correctamente pasado un tiempo sin actividad.

Inmediatamente después de tener completamente instalada la plataforma de hardware en la institución, se inicia un periodo de inducción y capacitación por el personal del área de sistemas.

**Instalación de equipo de cómputo.**

- Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores y equipos periféricos), que esté o sean conectados en la institución o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe cumplir con los siguientes requisitos:
  - Visto bueno por el área de sistemas
  - Estar cubierto por el seguro contra corriente débil
  - Tener su placa de identificación y relacionado en el inventario del área a la cual se ha asignado.
  - Verificar que el área de trabajo sea segura y cuente con el mobiliario mínimo para su uso.
  - Los equipos informáticos no deben instalarse cerca de ventanales en los cuales entra directamente la luz del sol, ya que el calor puede dañar los circuitos electrónicos.
  - Todos los equipos deben estar conectados al sistema acondicionado de energía.

## Políticas de Hardware

Hacen parte de la infraestructura física el servidor, UPS, Acondicionador de energía estaciones de trabajo, antenas inalámbricas, modem, suiche, impresoras, periféricos y otros equipos soporte de los programas de computadores y de la operación de la institución.

Cada uno de los recursos tecnológicos son exclusivamente para asuntos relacionados con las actividades del Hospital; por lo tanto, todos los usuarios deben guiarse por las políticas de uso y seguridad de la información, así como por las normas y procedimientos que para tal fin sean creados por la Gerencia a través del área de Sistemas.

**Servidores y estaciones de trabajo**

a) A todos los equipos se les deberá garantizar que estén ubicados en un área que cumpla con los requerimientos de seguridad física, control de acceso, condiciones ambientales y alimentación eléctrica necesaria.

b) El nuevo hardware, o modificaciones en este, debe contemplar la revisión de las políticas de seguridad, de forma que se realicen los ajustes a las ya existentes y/o incorporación de nuevas políticas a que haya lugar.

c) Todos los equipos de cómputo y componentes deben estar completa y exhaustivamente probados y aceptados de manera formal por parte del área de Sistemas, antes de ser colocados en funcionamiento.

d) Todos los equipos a los cuales el encargado de sistemas no esté en capacidad o no pueda realizar el mantenimiento preventivo deben contar con contratos de mantenimiento vigente y apropiado con empresas y personal técnico calificado y debidamente autorizado.

e) Los proveedores que dispongan servicios externos a la Institución deben conocer y aplicar las políticas de seguridad y de confidencialidad de la información.

f) El área de Sistemas es la única autorizada para dar de baja los equipos de cómputo, periféricos y de comunicación de propiedad de la institución, garantizando la mitigación de los riesgos de confidencialidad y seguridad de la información.

g) Todas las fallas de hardware de los sistemas de información deben ser reportadas oportunamente y registradas en un Formato de Soporte y ser atendido por área de Sistemas.

h) El área de Sistemas deberá contar con un inventario de todos los equipos de cómputo del Hospital, estableciendo la condición de adquisición de cada uno de ellos.

i) El área de Sistemas revisará los recursos físicos: equipos de cómputo, servidor, impresoras, componente de comunicaciones (Switch, Router, módem, etc.), componente eléctrico (UPS).

j) El uso de los equipos de cómputo de la Institución será para facilitarles el desempeño de su trabajo. Se obliga al usuario el uso correcto de ellos, por tanto, puede ser restringido de él en cualquier momento, cuando se demuestre un mal uso de este.

k) Solo el área de Sistemas podrá acceder y manipular los equipos de la Institución entregados como herramienta de trabajo a los funcionarios, y queda prohibida cualquier manipulación, alteración, mantenimiento, instalación o desactivación de los mismos.

l) Todos los equipos de cómputo deberán tener como fondo de escritorio única y exclusivamente material institucional, no se permitirá otro tipo de imagen en reemplazo del mismo, por tanto, cada usuario deberá garantizar que este permanezca.

m) El Área de Sistemas deberá seleccionar, adquirir, instalar y mantener el software antivirus apropiados para la salvaguardar la información, en todas y cada una de las estaciones de trabajo y equipos portátiles de la Institución.

n) El Área de Sistemas deberá mantenerse un inventario formal, actualizado y licenciado del software de la entidad.

o) Está expresamente prohibido a los usuarios, prestar sus Usuarios y Contraseñas.

p) Está expresamente prohibido el uso de recursos de cómputo para fines personales.

q) Los usuarios de la tecnología y comunicaciones deberán tener el debido cuidado para evitar dañar equipo de cómputo, impresoras y demás equipos tecnológicos.

r) Los usuarios de la Institución no podrán modificar la configuración preestablecida (hardware o software) de los equipos de las oficinas, consultorios y demás áreas: (alteración de direcciones Ethernet o I.P, cambio del nombre, cambio de dominio,

alteración en el arranque del ordenador, etc.).

s) La protección física de los equipos corresponde a quienes en un principio se le asigna, y corresponde notificar los movimientos en caso de que existan, a la oficina de sistemas.
t) Todo equipo que se conecte a la red de datos de la empresa debe tener instalado programa de antivirus debidamente licenciado y actualizado.
u) La instalación de equipos de cómputo del hospital debe ser autorizado y realizado por personal de la oficina de sistemas.
v) La inducción sobre el manejo específico de los recursos informáticos que el hospital entregue al usuario final está a cargo de la oficina de sistemas.
w) Todas las personas que requieran del sistema de información para el desempeño de sus funciones deben previamente acreditar conocimientos básicos del sistema operativo WINDOWS, y del software de oficina OFFICE, y en lo posible certificados por instituciones reconocidas en el medio.

**Mantenimiento de equipo de cómputo.**

a) Al Contratista de sistemas le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin se desarrolla un plan de mantenimiento preventivo con dos visitas al año por equipo, y de una visita para el cableado estructurado.

b) El Área de Sistemas, exclusivamente coordinara el mantenimiento preventivo y correctivo de los equipos de cómputo pertenecientes a la ESE.

c) El contratista de mantenimiento del hardware y software registra cada mantenimiento preventivo y correctivo de los equipos de cómputo en la hoja de vida.

**Reubicación del equipo de cómputo.**

La reubicación del equipo de cómputo se realiza diligenciando la plantilla de traslado de inventario físico de la empresa.

No se permite la reubicación o retiro de elementos o del equipo de cómputo/Impresora sin la presencia del área de sistemas y sin la autorización del Jefe de área, administrador o de quien figure como responsable del mismo.

**Encendido del equipo de cómputo**

a. Todo equipo de cómputo se debe encender así:
   1. Estabilizador de Voltaje o Regulador
   2. Pantalla o Monitor
   3. CPU

**Apagado del equipo de cómputo**

a. Cada usuario una vez finalizado su jornada de trabajo o cuando se suspenden actividades por más de media hora, deberá dejar el equipo ordenado y apagado. Los computadores de urgencias y hospitalización en lo posible apagarlos por media hora dos veces en la noche y obligatoriamente a las 2 am para generar la copia de seguridad.

b. Cerrar todas las aplicaciones o programas ejecutados en el computador. Cada software trae su correspondiente forma de cierre y debe efectuarse en la forma que este lo indique.

c. Extraer todo medio externo, como CD, DVD, memorias USB u otros, de las unidades. Esto se realiza con el fin de evitar inconvenientes al momento de arrancar nuevamente los equipos de cómputo (La institución no responde por perdida de dispositivos por mal uso o descuido de los mismos).

d. No dejar claves personales expuestas al uso público. No entregar, revelar o exponer las claves al uso público.

e. Cada usuario debe garantizar que termina y cierra su sesión de trabajo en el computador en el que se encontraba desempeñándose.

**Periféricos**

a. La información clasificada como altamente confidencial nunca puede enviarse a una impresora en red sin que haya una persona autorizada para salvaguardar su confidencialidad durante y después de la impresión.

b. Todas las fallas de hardware de los sistemas de información deben ser reportadas oportunamente, ser registradas y atendidas por el Área de Sistemas.

**Red de Datos**

1. Red Física

a. El Área de Sistemas debe instalar y/o mantener, con personal calificado y debidamente autorizado, la red de datos y voz, con el fin de garantizar la operación, seguridad e integridad.

b. Cualquier equipo y/o elemento activo y/o pasivo de la red que no se utilice debe ser desactivado y controlado.

c. No está permitido hacer seguimiento o monitoreo de puertos o tráfico de red, por parte de personas diferentes a las autorizadas por el Área de Sistemas.

d. La red de datos y voz debe estar diseñada y configurada para contar con un alto rendimiento, confiabilidad y seguridad, ajustándose a las necesidades de la Institución.

e. La instalación, desinstalación y manejo de programas y equipos de transmisión de datos es competencia exclusiva del Área de Sistemas.

f. La administración de la red debe ser realizada por personal debidamente calificado de la Institución

g. El adecuado suministro de fluido eléctrico continuo para equipos de misión crítica, requiere de UPS que permitan mantener y garantizar la continuidad de los servicios de fluido eléctrico durante las caídas de voltaje.

**2. Red Inalámbrica**

a. El Área de Sistemas es la encargada de la seguridad y uso de la red inalámbrica.

b. Los Jefes de área, funcionarios, contratistas y visitantes no podrán instalar Access Point (AP) de propiedad de los mismos.

**3. Red de Voz**

Teléfonos Fijos

a. Todas las pruebas, instalación e implementación de elementos de telefonía deben cumplir con los estándares técnicos y compatibilidad definidos por el funcionario o área encargada de la administración de la telefonía en conjunto.

b. No se podrá grabarse información confidencial o sensible en máquinas de audio respuesta y/o sistemas de correos de voz.

Teléfonos Celular

a. No está permitido transmitir información confidencial.

b. El teléfono celular solo es de uso institucional y no para uso personal de los funcionarios de la ESE.

**Acceso físico a instalaciones**

a. Los datos de la entidad deben ser administrados y guardados apropiadamente, para salvaguardarlos de ataques físicos, de accesos no autorizados por la red y/o delincuentes digitales.

b. El acceso debe ser registrado, controlado y monitoreado por el propietario del activo, para identificar el mal uso de los sistemas de información y así reducir el riesgo de pérdida de información.

### 6.4.2 CONTROL DE ACCESOS

**Acceso a áreas críticas.**

El acceso a las áreas de los archivos clínicos y administrativos son de carácter restringido, al igual que para el área de Informática.

a) Sólo ingresa al área el personal que trabaja en la misma.
b) El ingreso de personas extrañas solo podrá ser bajo una autorización del responsable del área
c) Siempre ésta área debe permanecer cerrada, limpia y organizada.
d) Las visitas a estas áreas por personas ajenas a la entidad, podrán hacerlo con previa identificación personal y sólo para realizar labores propias del área.
e) Esta área debe recibir aseo y mantenimiento por lo menos una vez al día y sus adecuaciones físicas se realizan de acuerdo con las normas de seguridad industrial establecidas para tal fin.
f) El área de servidores debe estar demarcado, con restricción total de acceso a personal diferente de sistemas. Con control de temperatura menos de 20 ºC. No se puede tener habilitado un puesto de trabajo en el área de servidores.

**Control de acceso al equipo de cómputo.**

Cualquier Terminal que pueda ser utilizada como acceso a los datos de un Sistema controlado, es encerrada en un área segura o guardada, de tal manera que no sean usadas, excepto por aquellos que tengan autorización para ello.

Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la oficina de sistemas tiene la facultad de acceder a cualquier equipo de cómputo del Hospital.

En los lugares donde se tienen instalados los equipos informáticos esta prohibido consumir alimentos.

**Control de acceso local a la red.**

Todo el equipo de cómputo que esté o sea conectado a la Red o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso que emite la oficina de sistemas.

El área de sistemas realiza control del tráfico del uso de red, en caso de detectarse mal uso de los recursos de Internet será susceptible de proceso disciplinario y sanción.

**Acceso a los sistemas administrativos.**

La instalación y uso de los sistemas de información se rigen por las políticas de la oficina de sistemas:

Al servidor de bases de datos, se prohíbe el acceso de cualquier usuario, excepto para el personal del área de Sistemas.

El control de acceso a cada sistema de información de la entidad es determinado por la oficina de sistemas quien es responsable de asignar los perfiles de los usuarios y definir los grupos de trabajo.

### 6.4.2 MECANISMOS DE VERIFICACIÓN DE USO ADECUADO

Las cuentas del Sistema de Información son responsabilidad de cada usuario y en el caso de presentarse alguna irregularidad el encargado del área de sistemas está en la capacidad de realizar una auditoría a cada una de las cuentas de los usuarios.

**Acceso a Internet.**

El hospital define a que usuarios les autoriza el acceso a Internet.

El acceso a Internet es autorizado por la oficina de sistemas, acorde a políticas institucionales.

### 6.4.3 UTILIZACIÓN DE LOS RECURSOS DE LA RED:

Los recursos disponibles a través de la red del hospital serán de uso exclusivo para asuntos relacionados con las actividades del hospital.

Le corresponde a sistemas administrar, mantener y actualizar la infraestructura de la red del hospital.

Los equipos de la tecnología de la información no se utilizan para realizar trabajos personales.

**Manejo de las contraseñas**

- Evite utilizar contraseñas que tengan palabras que se pueden encontrar en el diccionario, ya que son más fáciles de violar mediante el uso de software especializado.
- Evite el uso de información que lo defina y que sea fácil de encontrar, como los números de su teléfono o los nombres de personas allegadas etc.
- Evite utilizar la misma contraseña.
- Cambie sus contraseñas con frecuencia.
- Utilice claves que son mezclas aleatorias de números y letras. Si es posible, también mezcle caracteres en mayúsculas y minúsculas.
- No revele su contraseña. De nada sirve crear una palabra clave que no se pueda violar, si la deja apuntada en un papel pegado a su computador.

### 6.4.4 SOFTWARE:

**Adquisición de software.**

Los productos de software que se adquieren cumplen con los requisitos y requerimientos específicos de la institución, en cuanto a la plataforma de software y de hardware. Tienen una alta calidad en cuanto al grado que satisface los requerimientos de la institución: precisión requerida, cantidad de recursos utilizados, control del acceso, facilidad de uso, facilidad de mantenimiento y prueba, portabilidad del software y facilidad de ínter operación.

Todo el software de la empresa está licenciado respetando los derechos de autor y se mantiene actualizado permanentemente con los parches y mejoras que le realizan al software.

Las licencias que se adquieren son las últimas que existen en el mercado y están probadas, por ningún motivo se debe adquirir software en fase de desarrollo o beta.

Se vela por las actualizaciones periódicas de los programas antivirus, sistemas operativos, software de oficina, manejador de bases de datos, utilitario etc.

En cuanto a los programas informáticos sin costo se respeta la propiedad intelectual intrínseca del autor.

La oficina de sistemas promueve y propicia que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

**Instalación de software.**

La oficina de sistemas brinda la asesoría, y supervisa la instalación del software básico para cualquier tipo de equipo.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

La instalación de software que desde el punto de vista de la oficina de sistemas pudiera poner en riesgo los recursos de la institución no está permitida.

Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento a la oficina de sistemas.

Si se instala software en el servidor principal se saca una copia de seguridad completa de éste, y se guarda en el disco externo.

**Actualización del software.**

La oficina de sistemas autoriza cualquier adquisición y actualización del software.

**Auditoria de software instalado.**

La oficina de sistemas y de control interno son las responsables de realizar revisiones periódicas para asegurar que sólo programas con licencia estén instalados en las computadoras de la institución.

Se cuenta con un inventario detallado del software instalado en cada máquina.

**Software propiedad de la institución.**

Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución y mantiene los derechos que la ley de propiedad intelectual le confiere.

Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución están resguardados.

**Propiedad intelectual.**

La oficina de sistemas procura que todo el software instalado en el hospital esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

**Copias de seguridad**

La información que genera cada dependencia queda bajo la responsabilidad de cada usuario, por lo cual se les ha otorgado una memoria USB para que en ella realicen copias de seguridad permanentemente de la información que maneja en su puesto de trabajo, la copia debe actualizarse una vez a la semana todos los archivos. Al momento del retiro del funcionario se debe hacer la entrega de la USB y toda la información que se maneje al archivo administrativo.

Los backups del sistema operativo, software de base, software del aplicativo se realizan cuando hay actualizaciones del software o instalación de nuevos aplicativos. Esta copia se saca en el servidor.

Se realizan pruebas periodicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

### 6.4.5 CONDICIONES FÍSICAS:

La institución realiza adecuaciones físicas en todas las áreas críticas en las cuales se genera, transmite y almacena información como el área de sistemas para garantizar su seguridad.

El centro de cómputo tiene permanentemente un agente extintor adecuado según el tipo de fuego y riesgo, garantizando su vigencia, para lo cual el personal de sistemas y mantenimiento está entrenado en su uso.

**Caídas y Subidas de Tensión**

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen los computadores personales, los monitores, las impresoras y los demás periféricos. Si las oscilaciones se encuentran fuera de este margen, se recomienda pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

### 6.4.6 DISCOS DUROS

- En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.
- No está permitido mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
- Está prohibido colocar el equipo en una zona donde se acumule calor, ya que el calor puede dilatar algunas piezas más que otras, o secar los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.
- Evitar en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.
- No colocar dispositivos móviles cerca o sobre los equipos de cómputo.

### 6.4.7 BUENAS PRÁCTICAS EN EL USO DE LAS HERRAMIENTAS INFORMÁTICAS

El tiempo en que el ordenador no está siendo utilizado interactivamente por el usuario es del orden de 3 horas por usuario día. Por lo tanto, se debe apagar el equipo en los horarios prolongados de inactividad más de media hora y en el horario de almuerzo.

### 6.5 CONFIDENCIALIDAD DE LA INFORMACIÓN:

La institución genera dos tipos de información: información clínica que se obtiene como resultado de la ejecución de los procesos misionales e información administrativa que se origina en la realización de los procesos estratégicos y de apoyo.

La confidencialidad de la información de la institución se maneja, teniendo en cuenta la normatividad vigente que rige para las entidades del sector público que integran el Sistema de Salud, las políticas institucionales establecidas y de acuerdo con las características de la información.

El Hospital se compromete con sus usuarios a respetar el derecho de la confidencialidad de su información de salud. Entendemos que esta información médica es personal y delicada,

por lo tanto la institución no la revelará a otras personas, a menos que el usuario lo solicite o la ley obligue o autorice para hacerlo.

La utilización de la Historia Clínica comprende las siguientes cuestiones independiente de que sea en papel o electrónica.

- **Quien puede acceder la HC?**

  Los profesionales de la salud implicados en la atención del paciente, personal administrativo a las órdenes de los anteriores, los encargados de la gestión (Admisiones, facturación y sistemas), y los responsables de control (Auditoria médica, Auditor del PAMEC, subdirección Científica).

- **A qué información pueden acceder?**

  Cada profesional debe acceder únicamente a aquella información que le es necesaria para el ejercicio específico de su función.

**NIVELES DE OPERACIÓN DEL SISTEMA DE INFORMACIÓN PARA LA CALIDAD**

En el Hospital, se utilizan los dos niveles de operación del Sistema de información para la calidad, establecidos en la resolución 1446 de 2006, por medio de los cuales se le realiza monitoria al sistema y se permiten evidenciar el desempeño e implementación de los diferentes procesos del Hospital acorde a lo establecido en el Sistema Obligatorio de Garantía de Calidad de la Atención en Salud.

**5.1.2 Nivel de Monitoria Externo:** Entre los diversos actores del Sistema Obligatorio de Garantía de Calidad de la Atención en Salud, se pueden proponer y utilizar en el marco de sus competencias indicadores de calidad adicionales a los que hace referencia la resolución 1446 de 2006, con el objeto de evaluar la calidad y promover acciones de mejoramiento en áreas específicas de responsabilidad, atendiendo al principio de eficiencia del Sistema de Información para la calidad contemplado en el artículo 47 del Decreto 1011 del 2006.

**5.1.3 Nivel de Monitoria Interno:** Está constituido por los indicadores que se evalúan y los eventos adversos que se vigilan al interior del Hospital como actor en la implementación del Sistema Obligatorio de Garantía de Calidad de la Atención en Salud.

Es obligatorio hacer la monitoria de indicadores de calidad y vigilar el comportamiento de los eventos adversos los cuales serán definidos teniendo en cuenta la resolución 1446 de 2006, la política nacional de seguridad de pacientes y los demás que establezca la institución acorde a los procesos de atención que se prestan.

Se encuentran comprendidos en este nivel, como de obligatorio cumplimiento e implementación los indicadores de seguimiento a riesgo establecidos en el Sistema Único de Habilitación.

Entre los indicadores de nivel de monitoria interna que se manejan en el Hospital están todos los definidos en la resolución 1441 de 2013, 1446 de 2006, circular 056, resolución 710 de 2012 y otros requeridos por diferentes organismos de control.

Un indicador se define como la expresión cuantitativa del comportamiento o desempeño de una organización o institución, cuya magnitud, al ser comparada con algún nivel de referencia, podrá estar señalando una desviación sobre la cual se tomaran acciones correctivas o preventivas según el caso.

Los indicadores de Gestión permiten analizar cómo se está Administrado la IPS en áreas como uso de recursos (eficiencia) cumplimiento de las actividades programadas (eficacia) y la satisfacción del usuario (calidad) entre otros.

Los indicadores de Gestión contienen unas características que se describen en las fichas técnicas y facilitan su medición y análisis. En la Institución las fichas técnicas de los indicadores tienes los siguientes criterios:

- **Objetivo:**

El propósito u objetivo debe expresar el ¿para qué? Se quiere generar el indicador seleccionado. Expresa el lineamiento político, la mejora que se busca y el sentido de esa mejora (maximizar, minimizar, eliminar, etc.)

El propósito permitirá tener claridad sobre lo que significa mantener un estándar de excelencia y adecuarlo permanentemente ante los diversos cambios, así como proponerse nuevos retos.

- **Tipo de Indicador**

**Eficacia o Resultado**: Esta se define como el logro de los resultados propuestos, por lo tanto conformaran este grupo los indicadores que nos indiquen si se cumplió o no el resultado esperado.

**Eficiencia:** Se define como la utilización de los recursos de acuerdo con un programa establecido.

**Impacto.** Miden los cambios o modificaciones positivas o negativas que se han producido en el entorno o sobre la población objetivo como consecuencia de la ejecución del plan o el cumplimiento de las funciones asignadas. Estos están relacionados con las contribuciones de los resultados generados a la solución de las necesidades existentes en el área de intervención de la entidad. La evaluación del impacto es la valoración de lo que la acción institucional después de un tiempo de haber realizado los planes, programas o proyectos o de haber cumplido las funciones asignadas. Para realizar la evaluación del impacto, básicamente existen dos procedimientos: a. Determinar el valor de los indicadores relevantes antes de iniciar el proyecto, y el valor que asumen estos mismos indicadores después de un tiempo de finalizado el proyecto, determinando las variaciones positivas o negativas. b. Dividir la población objetivo en dos segmentos: el primero (grupo testigo) que no recibe los beneficios del proyecto o no es objeto del accionar institucional, y el segundo (grupo objeto), al cual se entregan los resultados del proyecto, y que será evaluado en el cambio de sus condiciones

- **Atributo:** Es la característica de calidad que vamos a medir con el indicador
- **Formula:** Es la relación de los datos (numerador y denominador) que nos dará el resultado final del indicador
- **Tendencia Esperada**
- **Meta**
- **Fuente del dato**

Se registra la fuente de los datos, ya sea el documento, libro, formato o registro, en el que se captura la información requerida, en algunos casos el área que suministra la información.

- **Responsable de la recolección de los datos**

Se registra la dependencia y el cargo del responsable de la generación y transmisión del indicador a los responsables de la toma de decisiones.

El responsable de generarlo debe ser el Coordinador o jefe del área, con participación de todos sus funcionarios debe evaluar el resultado en caso de valores superiores o inferiores

al estándar con el fin de determinar las causas, en caso de no existir un estándar el Coordinador del área debe verificar en otras entidades de igual complejidad el estándar que manejan y si es aplicable, de lo contrario se entrará a establecer con base en un histórico que se puede variar si se comprueba que debe ser otro de acuerdo a la Gestión que se debe cumplir.

- **Responsable análisis de Datos**

Determina a quien le corresponde actuar en cada momento frente a la información que suministra el indicador. Además, debe registrar a quien se le debe dar a conocer la información resultante del indicador.

Los indicadores que tienen que ver con políticas, expectativas del usuario y competencia, le corresponden a la Dirección y Junta Directiva.

El análisis de los indicadores de tipo estándar e histórico, le corresponde al nivel ejecutivo.

- **Periodicidad:**

Determina la frecuencia con que debe generarse el indicador: Diario, semanal, mensual, semestral ó anual. La periodicidad permite evaluar las tendencias, analizar periodos y efectuar seguimiento que se puede verificar mediante gráficas.

- **Categoría de discriminación**

Las acciones que desarrolle el SOGCS se orientarán a la mejora de los resultados de la atención en salud, centrados en el usuario, que van más allá de la verificación de la existencia de estructura o de la documentación de procesos los cuales solo constituyen prerrequisito para alcanzar los mencionados resultados.

Para efectos de evaluar y mejorar la Calidad de la Atención de Salud, el SOGCS deberá cumplir con las siguientes características:

1. **Accesibilidad**. Es la posibilidad que tiene el usuario de utilizar los servicios de salud que le garantiza el Sistema General de Seguridad Social en Salud.

2. **Oportunidad.** Es la posibilidad que tiene el usuario de obtener los servicios que requiere, sin que se presenten retrasos que pongan en riesgo su vida o su salud. Esta característica se relaciona con la organización de la oferta de servicios en relación con la demanda y con el nivel de coordinación institucional para gestionar el acceso a los servicios.

3. **Seguridad.** Es el conjunto de elementos estructurales, procesos, instrumentos y metodologías basadas en evidencias científicamente probadas que propenden por minimizar el riesgo de sufrir un evento adverso en el proceso de atención de salud o de mitigar sus consecuencias.

4. **Pertinencia.** Es el grado en el cual los usuarios obtienen los servicios que requieren, con la mejor utilización de los recursos de acuerdo con la evidencia científica y sus efectos secundarios son menores que los beneficios potenciales.

5. **Continuidad**. Es el grado en el cual los usuarios reciben las intervenciones requeridas, mediante una secuencia lógica y racional de actividades, basada en el conocimiento científico.

A continuación se relaciona un ejemplo de ficha técnica definida por la institución

## 6.3 ESTANDARIZACIÓN DE LA INFORMACIÓN

La estandarización de los procesos permite definir los indicadores que permitan evaluar el cumplimiento de las características de calidad y los factores críticos de éxito de los procesos y definir para cada uno de ellos los estándares de cumplimiento.

La metodología para la estandarización de los procesos se tiene definida en el instructivo para la elaboración y control de documentos, en el cual además se relaciona la estandarización de la estructura documental de la institución apoyada en las tablas de retención documental

En el software de Sistemas de Información integra la información clínica y administrativa, se permite parametrizar criterios de validación de los datos, de tal forma que no se ingrese información no coherente que entorpezca luego el análisis y la toma de decisiones. Por ejemplo se parametrizan variables como diagnósticos permitidos por edad y género, topes económicos de los contratos con las administradoras de planes de Servicios, datos requeridos en las diferentes plantillas de historia clínica, entre otros.

## 6.4 SEGURIDAD DE LA INFORMACIÓN

La asignación de permisos se realiza teniendo en cuenta las funciones que realiza el personal, asignando los siguientes permisos.

| Personal | Crear | Grabar | Consultar | Imprimir |
|---|---|---|---|---|
| Médicos | X | X | X | X |
| Jefes de enfermería y Auxiliares | X | X | X | |
| Archivo Clínico | | | X | X |
| Facturadores | | | X | X |

El personal asistencial se le asigna permisos de crear y grabar Historia Clínicas dependiendo de las plantillas que tenga diseñadas para tal fin.

Con respecto a la información administrativa en el procedimiento de elaboración y control de documentos se genera el listado maestro de documentos y registros en el cual se define que personal de la institución tiene acceso a los diferentes documentos y quien tiene copia controlada.

POLITICAS CONFIDENCIALIDAD DE LA INFORMACION

a. Todo usuario debe guardar el máximo respeto al trabajo de los demás, no destruyendo o copiando archivos de otros usuarios, (salvo su autorización directa) o interrumpiendo sus sesiones por cualquier procedimiento.
b. Ante cualquier duda sobre el uso de los recursos de cómputo, consúltese en primera instancia las ayudas o los manuales respectivos. En último extremo, acuda al personal del área de sistemas a través de una solicitud de soporte.
c. Cada coordinador debe garantizar que las copias que se realicen de trabajos de la entidad sean realizadas en medio extraíble (Memoria USB) proporcionadas por la institución y las cuales son exclusivas para el manejo de información y trámites de la entidad, y bajo ningún aspecto se pueden difundir, manipular, editar o presentar para trámites ajenos a la entidad.

POLÍTICAS SOBRE EL USO Y ADMINISTRACIÓN DE LA INFORMACIÓN Y LA RESPONSABILIDAD SOBRE LA MISMA.

a. El Hospital se reserva el derecho de monitorear todos los aspectos relacionados con cada sistema de cómputo, incluyendo la revisión de material bajado de Internet, monitoreo de sitios visitados en Internet, así como el correo enviado y recibido por los usuarios.
b. El mal uso del material existente (equipos, impresoras, scanner, internet etc.) puede dar lugar al reporte para inicio de acciones legales.
c. Únicamente el área de sistemas por orden puede instalar y desinstalar programas.
e. Está expresamente prohibido el uso de equipos con programas de cualquier tipo que no esté licenciado para uso del Hospital.
f. Los Usuarios no podrán efectuar cualquiera de las siguientes labores sin previa autorización del área de Sistemas, quedando absolutamente prohibido:

1. Copiar software para ser utilizado en los computadores de casa.
2. Proveer copias de software a contratistas, empleados temporales, amigos, parientes o cualquier otra tercera persona.
3. Instalar software en cualquier computador o servidor de la entidad.
4. Bajar software de Internet u otro servicio en línea a cualquier Computador o servidor.
5. Modificar, radicar, transformar o adaptar cualquier software.
6. Utilizar medios para capturar información ajena.
7. Sacar de las oficinas, sin la debida autorización del encargado, manuales, archivos, discos o que formen parte del catálogo del Servicio de Informática y Comunicaciones.
8. Grabar juegos, videos, fotografías, programas y música que saturen el disco duro de las máquinas, así como copiar los mismos a través de la red, lo que genera disminución en el rendimiento de la misma.
9. Copiar, sin autorización expresa, programas fuentes propiedad del hospital.
10. Tener archivos que hagan peligrar la integridad del sistema y/o puedan interferir el trabajo de otros usuarios.
11. Efectuar cambio del papel tapiz, protectores de pantalla y punteros de Mouse. La única imagen que podrá estar de tapiz ha de ser la de la imagen o logo institucional.
12. Ensuciar el recinto de trabajo, afectando elementos de cómputo, como Mouse, teclado e impresoras.

## 6.5 IDENTIFICACIÓN DE NECESIDADES DE INFORMACIÓN:

La Institución identifica los requerimientos de información externa e interna provenientes de la ciudadanía, los organismos de control, los contratistas, los proveedores, procesos internos y demás grupos interesados, con base en los lineamientos legales, los procesos y los propósitos de la organización. Adicional se identifican los componentes físicos, (hardware, software y tecnologías), de recurso humano, capacitación y entrenamiento necesarios para la captura, procesamiento, administración y distribución de datos e información.

Esta identificación se realiza teniendo en cuenta los criterios políticos, gubernamentales, económicos, sociales y ambientales además se incluye la identificación de los informes que se deben rendir a los grupos interesados los cuales alimentan la Matriz de Informes.

Cada proceso tiene definido mediante una matriz de información los requerimientos de información necesarios para el desarrollo de sus actividades.

A partir de la matriz de información y utilizando la herramienta del Cristal Report, la institución realiza la configuración de los reportes que van a ser utilizados por el personal de las áreas, para garantizar que el acceso a la información solicitada de manera rutinaria se realice de manera oportuna y confiable.

Cuando se presente fallas en la generación o transmisión de la información son atendidas por el área de Sistemas las cuales se registran la Solicitud de Soporte Técnico, éste formato está ubicado en la Intranet para facilitar su diligenciamiento y envío. Este es otro mecanismo para identificar necesidades de los usuarios.

## 6.6 DISEÑO Y DESARROLLO:

Cuando los requerimientos de información necesiten diseño y desarrollo, los responsables de cada proceso envían el requerimiento al jefe del departamento de sistemas quien envía su requerimiento a CNT Sistemas de Información para evaluar la viabilidad y la factibilidad y determina si es necesario realizar un nuevo desarrollo o se puede realizar una adaptación de algún requerimiento existente

El prototipo se evalúa y valida, con el dueño del requerimiento, verificando en cada etapa que cumpla con las expectativas y realiza los ajustes pertinentes.

Después de terminado el diseño se inicia la puesta en marcha del desarrollo la cual incluye la capacitación y el entrenamiento al usuario final y al responsable de la captura de los datos. De cada desarrollo se debe elaborar el instructivo de usuario.

Los requerimientos que no requieran un diseño específico se les da respuesta con las consultas rápidas, capacitación y entrenamiento.

## 6.7 VALIDACIÓN, ANALISIS Y GENERACIÓN DE LA INFORMACIÓN:

Los responsables de los procesos recopilan los datos e información relacionada con el desempeño de los procesos y servicios, utilizando para ello las herramientas de calidad como:

- Análisis estadístico
- Medición de indicadores
- Gráficos
- Análisis de Pareto
- Lluvia de ideas
- Información de planes y programas
- Análisis de costos
- Técnicas de análisis financiero

La matriz de informes define los responsables de la validación de los datos y la información antes de ser utilizados, de tal forma que se tomen decisiones con base en datos y hechos reales al igual que en la matriz de indicadores también se define los responsables da la captura de los datos y su validación.

Los procedimientos definidos por la institución contemplan actividades de validación, en el momento que la información es entregada como subproducto a los clientes identificados en los diferentes procedimientos, en caso que se identifiquen inconsistencias en la misma, se revisa la información conjuntamente con quien la originó y se toman acciones correctivas y preventivas para evitar su recurrencia.

**6.8 ALMACENAMIENTO Y CONSERVACIÓN DE LA INFORMACIÓN:**

La institución maneja 2 grandes archivos para el almacenamiento y conservación de la información física:

- Archivo administrativo: Documentación generada de los procesos administrativos, incluyendo las historias laborales
- Archivo clínico: Historias clínicas

Cada uno de ellos obedece a la normatividad vigente y su estructura se define de acuerdo a las tablas de retención documental, en las cuales se encuentra definido el tratamiento, custodia y conservación de la documentación incluyendo el control de los factores ambientales.

La institución ha definido las Tablas de Retención Documental en las cuales se establece el tiempo que se debe almacenar los documentos que genera la institución teniendo en cuenta las características de la información.

Tanto la información electrónica clínica como administrativa se almacena en bases de datos relacionales, que se administran por medio de procesos estandarizados para garantizar un adecuado almacenamiento y conservación, bajo los lineamientos de la política de seguridad de la información.

### 6.9 CONVENIOS CON TERCEROS:

Los terceros que se conecten a la red de datos del hospital están obligados a seguir las políticas de seguridad existentes.

Los terceros que tengan o traigan equipos de cómputo al Hospital, deben reportarlos a la oficina de sistemas, indicando los componentes de hardware que posea y presentar las copias de las licencias de software instalados en cada equipo.

El hospital no asume ninguna responsabilidad por pérdida de equipos de cómputo propiedad de terceros, ni por la información almacenada en dichos equipos.

### 6.10 DISPOSICIÓN FINAL DE LO EQUIPOS INFORMÁTICOS

El hospital al dar de baja sus equipos evalúa si estos son aptos para el cobro del siniestro a la Aseguradora y si aplica se procede a realizar el proceso de cobro, en caso de no aplicar, se determina obsolescencia tecnológica y dan de baja.

Para realizar la baja de los equipos la oficina de sistema genera un listado de los equipos a dar de baja con el respectivo informe técnico, el cual es enviado a la Subdirección para su aprobación, teniendo en cuenta el procedimiento de baja de inventarios.

## 7. PAPEL O ROL QUE DESEMPEÑA CADA ÁREA DE LA INSTITUCIÓN EN LA ACTIVIDAD INFORMÁTICA

### Área de sistemas

Es un área de servicios encargada de proporcionar en forma óptima la tecnología de sistemas que requiere la institución. Es responsable de que los equipos, herramientas informáticas, telecomunicación y sistemas de información, funcionen oportuna y adecuadamente. Adicionalmente es responsable de la administración y control de las bases de datos de la institución.

### Áreas usuarias

Durante el desarrollo de los sistemas es responsable de la definición detallada de los requerimientos, del diseño detallado de los documentos, entradas y salidas de los sistemas, y de las pruebas y puesta en marcha de los sistemas desarrollados.

Con respecto a los sistemas de información implantados es responsable de usar el sistema eficientemente, velando por la oportunidad, consistencia y confiabilidad de los datos registrados e informes requeridos.

### Control Interno

Durante el desarrollo de los sistemas es responsable de establecer los requerimientos de control y seguridad del sistema y de establecer los procedimientos administrativos requeridos para que el sistema funcione en una forma segura y confiable.

Una vez implantados los sistemas es responsable de velar por el cumplimiento de las normas y controles establecidos y de verificar la validez y funcionalidad de los planes de contingencia de los equipos y de cada sistema de información.

| Control de Cambios | | |
|---|---|---|
| **Fecha** | **Versión** | **Descripción** |
| 15/01/2025 | 1.0 | Creación. |
| | | |