PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E HOSPITAL SANTA MARGARITA

La Cumbre - Valle

VIGENCIA 2025

40-42.15

TABLA DE CONTENIDO

40-42.15

1. INTRODUCCIÓN

En el marco de las responsabilidades de una Empresa Social del Estado (ESE) en Colombia, garantizar la seguridad y privacidad de la información se ha convertido en una prioridad estratégica. Los hospitales públicos administran y procesan datos sensibles, como historias clínicas, datos personales de los pacientes y registros administrativos, los cuales son esenciales para la prestación de servicios de salud de calidad y deben estar protegidos frente a amenazas de seguridad y posibles vulneraciones.

Este plan de seguridad y privacidad de la información tiene como propósito establecer un marco integral que permita la gestión segura de los datos, alineado con las normativas nacionales como la Ley 1581 de 2012 (Protección de Datos Personales) y el Decreto 1377 de 2013, así como con estándares internacionales en ciberseguridad.

A través de este plan, la ESE busca mitigar riesgos, proteger la confidencialidad e integridad de la información, y garantizar su disponibilidad para los usuarios autorizados, fortaleciendo la confianza de la comunidad y promoviendo un entorno seguro para la prestación de servicios de salud de alta calidad. Este compromiso con la seguridad de la información es un paso esencial para consolidar la eficiencia operativa y el cumplimiento de las responsabilidades legales y éticas de la institución.

2. CONTEXTO INSTITUCIONAL

2.1. ARTICULACIÓN CON EL PLAN DE DESARROLLO

Se articula el plan de seguridad y privacidad de la información con el objetivo estratégico número 2. "*Mejorar la eficiencia operativa y la calidad en los procesos hospitalarios, impulsando la actualización de infraestructura, la adopción de tecnologías innovadoras, el fortalecimiento del posicionamiento institucional y la optimización de las finanzas, alcanzando estándares de excelencia."* del plan de desarrollo para la vigencia 2024-2028

VISIÓN

Consolidarnos como un Hospital con énfasis en los servicios de prestador primario, referente en la prestación Integral de servicios de salud de baja complejidad, centrados en las personas de acuerdo con sus necesidades, integrado con los demás actores del sistema, implementando el Modelo de Acción Integral Territorial humanizado y seguro, con enfoque de gestión sostenible por su eficiencia, responsabilidad social y amigable con el medio ambiente. Generado bienestar en el municipio de La Cumbre Valle.

40-42.15

MISIÓN

Satisfacer las necesidades de salud de la baja complejidad de nuestros pacientes, integrando la atención primaria en salud (APS), práctica clínica y la educación, en una permanente búsqueda de la excelencia para beneficio de la comunidad.

VALORES INSTITUCIONALES

Honestidad: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud, y siempre favoreciendo el interés general.

Respeto: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

Compromiso: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.

Justicia: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

3. GLOSARIO DE TÉRMINOS

Sistema de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). Dichos elementos formarán parte de alguna de estas categorías. Sus elementos son personas, datos, actividades o técnicas de trabajo, recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente). Todos estos elementos interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

Confidencialidad: La propiedad que esa información esté disponible y no se divulgada a personas, entidades o procesos no autorizados.

40-42.15

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Sistema de Gestión de Seguridad de la Información: Esa parte del sistema gerencial general basada en un enfoque de riesgo comercia; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Gerencia de la Información: Es la gestión de la institución sobre los requerimientos de información de la organización relacionados con los procesos de atención y necesidades de los clientes, la planeación, direccionamiento y mejoramiento de la organización, la gestión de recursos y la productividad.

Usuarios del Sistema: Es aquella persona que usa algo para una función en específico

Información: Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Copia de Seguridad. (BACKUP): Se define como Backup o copia de seguridad, la actividad de resguardar de forma segura la información contenida en un medio de almacenamiento de origen (disco duro) a un medio de almacenamiento de destino de diferente tipo (otro disco duro, servidor de Backup, USB, CD, DVD, ZIP, entre otros)

Información Sensible: Son todos aquellos archivos digitales generados desde los sistemas de información con los cuales la Institución cuenta.

Incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y gestionar los fallos de seguridad de la información. (ISO/IEC 27000).

4. MARCO LEGAL

Como referente normativo se tienen principalmente las siguientes disposiciones:

Ley 1581 de 2012 (Ley de Protección de Datos Personales): Establece el régimen general de protección de datos personales en Colombia y regula el tratamiento de estos, garantizando los derechos de los titulares, como la confidencialidad, acceso, rectificación y eliminación de información.

Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012 y establece disposiciones específicas para el manejo de datos personales, incluidos lineamientos sobre autorización de tratamiento, derechos de los titulares y medidas de seguridad.

40-42.15

Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública): Garantiza el acceso a la información pública, pero también resalta la importancia de proteger los datos sensibles y la información que pueda comprometer la privacidad o la seguridad.

Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo): Define principios relacionados con la protección de datos personales y el derecho a la reserva de información en los procesos administrativos.

Ley 1273 de 2009: Introduce el delito de "protección de la información y los datos" en el Código Penal, estableciendo sanciones para quienes accedan, usen, modifiquen o revelen información sin autorización.

Resolución 1995 de 1999: Regula el manejo de las historias clínicas en Colombia, destacando la confidencialidad como un principio fundamental en el tratamiento de la información médica.

ISO/IEC 27001: Estándar internacional para la gestión de la seguridad de la información, aplicable a la protección de datos en el ámbito hospitalario.

ISO/IEC 27799: Guía específica para implementar controles de seguridad en el manejo de información de salud.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Gestionar, establecer en forma estandarizada, los lineamientos de seguridad de la información, los requerimientos de información de los clientes, internos y externos, integrando la información administrativa y asistencial dentro de los diferentes niveles de gestión y toma de decisiones de la institución, contemplando siempre la seguridad y privacidad de la información.

5.2. OBJETIVOS ESPECÍFICOS

- Fortalecer la protección de la información sensible, garantizando la seguridad de los datos personales y clínicos de los pacientes, así como de la información administrativa, mediante la implementación de políticas, procedimientos y controles alineados con la normatividad vigente.

40-42.15

- Mitigar riesgos de ciberseguridad, identificando, evaluando y minimizando los riesgos asociados a posibles amenazas de seguridad, como accesos no autorizados, fugas de información, ciberataques y errores humanos.

- Implementar una cultura de seguridad de la información, promover la formación y sensibilización del personal de la ESE sobre la importancia de la seguridad y privacidad de la información, fomentando buenas prácticas en el manejo de los datos.

- Garantizar la continuidad operativa, Desarrollar e implementar mecanismos que permitan la recuperación rápida y eficiente de la información ante incidentes de seguridad, desastres o fallos tecnológicos, asegurando la continuidad de los servicios de salud.

- Incorporar herramientas tecnológicas y sistemas de información seguros, que cuenten con medidas de protección avanzadas y permitan un manejo eficiente de los datos.

- Diseñar indicadores y métricas que permitan evaluar el desempeño del plan, identificar brechas de seguridad y ejecutar acciones de mejora de manera constante.

6. ALCANCE

El presente Plan Estratégico aplica para todos los procesos que contribuyen al desarrollo de los recursos de tecnologías de información y comunicación en la E.S.E. Hospital Santa Margarita de La Cumbre.

Al desarrollar e implementar este documento se describirá los lineamientos en seguridad y privacidad de la información del Hospital Santa Margarita de la Cumbre, los cuales deben ser conocidos y apropiados por empleados, contratistas y todo tercero que tenga acceso, almacene, o procese información del Hospital Santa Margarita, o información de pacientes. (Historia clínica, tratamiento o trámite realizado) enfocados en los procesos institucionales, las políticas de gerencia de la información en el Plan de Gerencia de la información que articulado con el Plan de Desarrollo Institucional 2016-2020, guiará los mecanismos de identificación de las necesidades en seguridad y privacidad de la información de la ESE Hospital Santa Margarita de la Cumbre.

40-42.15

7. POLÍTICAS GENERALES DE AUTOCONTROL

7.1. POLÍTICA DE SEGURIDAD

7.1.1. EQUIPO:

De la instalación de equipo de cómputo.

- Todo equipo de cómputo (computadores, estaciones de trabajo, servidores, y equipos accesorios), que esté o sea conectado a la red de datos Hospital SANTA MARGARITA DE LA CUMBRE, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite el Área de sistemas. (ver Manual del buen uso del computador)

- El Área de sistemas en coordinación con el área de inventarios deberá tener un registro de todos los equipos propiedad del Hospital SANTA MARGARITA DE LA CUMBRE.

- El equipo de la institución que sea de propósito específico como computadores, portátiles, impresoras, fotocopiadoras y video bean u otros y tenga una misión crítica asigna-da, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica.

- Los responsables de las áreas de activos fijos, mantenimiento, deberán en conjunto con el Área de sistemas dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

- La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las responsables correspondientes (área de mantenimiento, área de inventarios, área de sistemas y otros de competencia).

Del mantenimiento de equipo de cómputo.

- Al Área de sistemas, corresponde la realización del mantenimiento preventivo y correctivo de los equipos de propiedad de la institución, el mantenimiento preventivo y correctivo de equipos adquiridos en modo canon arrendamiento será realizados bajo la responsabilidad del proveedor, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar.

40-42.15

- En el caso de los equipos atendidos por terceros, el Área de sistemas deberá informar al respecto al responsable de cada área cuando se diera lugar.

- Corresponde al Área de sistemas dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

De la actualización del equipo.

- Prohibido hacer cualquier tipo de reparación en los equipos del Hospital Santa Margarita de la Cumbre por parte de los usuarios, se deberá reportar al área de informática cualquier problema con los mismos, para evitar daños y pérdidas de información.

- Prohibido hacer cualquier cambio en las configuraciones de los equipos (por ejemplo: nombres de usuarios de red, direcciones IP, impresoras, etc.), por parte de los usuarios ya que pueden presentarse fallas en la red.

- Prohibida la instalación de cualquier hardware adicional a los equipos (por ejemplo: cámaras, módems, USB, celulares, etc.), por parte de los usuarios.

De la reubicación del equipo de cómputo.

- La reubicación del equipo de cómputo se realizará por el área de sistemas, emitirá un informe que será entregado al área de activos fijos, para que sea actualizada su ubicación en el sistema de control de los activos del Hospital Santa Margarita.

- El equipo de cómputo a reubicar sea del Hospital Santa Margarita, o bien externo, se hará únicamente bajo la autorización del responsable, contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo. Igualmente es necesario garantizar la cadena de custodia de la información contenida en los equipos a reubicar

7.1.2. CONTROL DE ACCESOS

Del acceso a áreas críticas.

- En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un control estricto del tráfico de personal que ingresa al área de servidores, SIN EXCEPCION.

40-42.15

- Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifique el Coordinador del área de sistemas, gerente o su delegado.

Del control de acceso al equipo de cómputo.

- Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de estos.

- Las áreas donde se encuentren equipos cuyo propósito reúna características de imprescindible y de misión crítica, ejemplo (equipos clínicos, facturación, financiera, sistemas, entre otros), deberán sujetarse también a las normas que establezca el área de sistemas.

- Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el área de sistemas tiene la facultad de acceder a cualquier equipo de cómputo esté o no bajo su supervisión.

Del control de acceso local a la red.

- El área de sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

- El área de sistemas es el responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

- Dado el carácter unipersonal del acceso a la red de Hospital Santa Margarita, el área de sistemas verificará el uso responsable de este recurso.

- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos) conectado a la red es administrado únicamente por el área de sistemas.

- Todo el equipo de cómputo que esté o sea conectado a la red Hospital Santa Margarita, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite El Área de Sistemas.

De control de acceso remoto.

- El área de sistemas es responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

40-42.15

- El usuario de estos servicios deberá sujetarse a las instrucciones emitidas por el área de sistemas y en concordancia con los lineamientos generales de uso de Internet.

- El acceso remoto que realicen personas ajenas a la institución deberá ser autorizado por la gerencia en forma escrita y dirigida al área de sistemas.

De acceso a los sistemas administrativos.

- Tendrá acceso a los sistemas administrativos solo el personal del Hospital Santa Margarita, que esté autorizado por escrito o por medio del soporte de personal de apoyo administrativo o técnico.

- Los servidores de bases de datos administrativos son de uso específico, por lo que se prohíbe el acceso de cualquier persona, excepto para el personal del área de sistemas.

- El control de acceso a cada sistema de información de Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados.

Del Servicio de correo electrónico e Internet.

- En concordancia con la legislación y de común acuerdo con las políticas generales de informática el área de sistemas es el responsable de instalar y administrar el o los servidores WWW. Es decir, sólo se permiten servidores de páginas autorizados por el área.

- El área de sistemas será el encargado de la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

- Los accesos a las páginas Web a través de los navegadores deben sujetarse a los lineamientos y restricciones del área de sistemas.

- A los responsables de los servidores Web corresponde la verificación de respaldo y protección adecuada.

- El material que aparezca en la página de Internet del Hospital Santa Margarita deberá ser aprobado por el área de sistemas y área de comunicaciones, respetando la ley

40-42.15

de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

- Con referencia a la seguridad y protección de las páginas, así como al diseño de estas será por el área de sistemas.

- Queda prohibido instalar y bajar música MP3 o videos de Internet, ya que esto hace más lento el servicio de correo e Internet, además de que el uso de música MP3 sin licencias es un delito.

- Prohibido hacer el uso de Internet y correo electrónico para fines ajenos a la labor que cada uno realiza en el Hospital santa margarita de La Cumbre.

- Prohibido el envío masivo de cadenas de correo electrónico, ya que esto satura los servidores y promueve la propagación de virus.

- Prohibido escuchar música a través de Internet, el hacerlo incrementa el tráfico y hace más lento el servicio.

- Constantemente están llegando virus por medio del correo electrónico, por lo cual se les solicita tener precaución con los correos electrónicos de personas extrañas y con anexos desconocidos, en caso de duda, comunicarse con el área de sistemas.

De utilización de los recursos de la red.

- Los recursos disponibles a través del Hospital Santa Margarita serán de uso exclusivo para asuntos relacionados con las actividades del trabajo del Hospital.

- De acuerdo con las disposiciones de la gerencia, corresponde al área de sistemas ad-ministrar, mantener y actualizar la infraestructura de la red Hospital santa margarita de la cumbre.

- El área de sistemas debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas de la institución.

- Queda prohibida la reproducción de música vía red local, ya que esto incrementa el tráfico en la red, haciendo muchos más lentos los servicios de Internet y correo y además esta reproducción es ilegal.

40-42.15

7.1.3. SOFTWARE

De la adquisición de software.

- Se les recuerda que el uso de software y sistemas sin licencia es un delito, por lo cual queda prohibido instalar software ajeno y sin licencia, de lo contrario la responsabilidad legal recaerá en la persona que incurra en esta práctica.

- En concordancia con la política de la institución, la unidad de Gestión Informática y el área de sistemas, son los organismos oficiales del Hospital para establecer los mecanismos de procuración de sistemas informáticos.

- De acuerdo con el Programa Nacional de Informática, El Hospital en conjunto con la Unidad de Gestión Informática, propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala y de acorde al plan de austeridad del Gobierno de la República.

- Corresponderá al área de sistemas emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

- De acuerdo con los objetivos globales del área de sistemas se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

- En cuanto al software libre o sin costo deberá respetarse la propiedad intelectual intrínseca del autor.

- El área de sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

De la instalación de software.

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

- En caso de requerir la instalación de algún software adicional, comunicarse con el área de sistemas, para asegurar que se cuenta con su correspondiente licencia y en caso afirmativo asegurar su adecuada instalación evitando dañar los sistemas e información contenidos en los equipos.

40-42.15

- El área de sistemas es el responsable de brindar asesoría y supervisión para la instalación de software informático.

- 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 física de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al área de sistemas.

De la actualización del software.

- La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo con el plan de acción que anualmente sea propuesta por el área de sistemas y áreas que requieran.

- Corresponde al área de sistemas autorizar cualquier adquisición y actualización del software.

- Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo con el plan de actualización desarrollado por el área de sistemas.

De la auditoria de software instalado.

La oficina de Control Interno del Hospital santa margarita de la cumbre en conjunto con el área de sistemas son los responsables de realizar revisiones periódicas para asegurar que sólo programas con licencia que estén instalados en los computadores de la institución.

Software propiedad de la institución.

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

- El área de sistemas deberá tener un registro de todos los paquetes de programación propiedad del Hospital santa margarita de la Cumbre.

- Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del Hospital santa margarita

40-42.15

de la cumbre ese mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

- Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo (backup) correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse, de acuerdo con lineamientos impartidos por el área de sistemas previamente.

- Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados según proceso implementado por el área de sistemas.

- Corresponderá al área de sistemas promover y difundir los mecanismos de respaldo y salvaguardar los datos y de los sistemas programáticos.

- El área de sistemas propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.

- El área de sistemas administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

Sobre el uso de software académico.

- Cualquier software que requiera ser instalado para trabajar sobre la red Hospital santa margarita de la cumbre deberá ser evaluado por el área de sistemas.

- Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades del Hospital santa margarita de la cumbre.

De la propiedad intelectual.

Corresponde al área de sistemas procurar que todo el software instalado en Hospital santa margarita de la cumbre esté de acuerdo con la ley de propiedad intelectual a que dé lugar.

7.1.4. SUPERVISIÓN Y EVALUACIÓN

- Cada una de las Áreas donde esté en riesgo la seguridad en la operación, servicio y funcionalidad de la información, deberá emitir las normas y los procedimientos que correspondan.

40-42.15

- Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca el área de sistemas.

- Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

- Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

7.1.5. USO DE DISPOSITIVOS EXTERNOS (MEMORIAS USB, CD ROM)

- En caso de recibir información por medio de Memorias USB, CD ROM debe ser con previa autorización y revisión por el área de sistemas.

- El ingreso Hospital santa margarita de la cumbre de computadores portátiles o equipos ajenos a la institución se hará con la supervisión y la autorización por escrito del área de sistemas.

7.1.6. INTERÉS GENERAL PARA TODAS ÁREAS DEL HOSPITAL

- Cada una de las áreas deberá emitir los planes de contingencia que correspondan a las actividades críticas que realicen.

- Procurar modular el volumen de los radios en un nivel adecuado, de manera que no interfiera con la labor de los demás compañeros.

- Apagar el equipo completamente al final de la jornada laboral y desconectar de la toma eléctrica.

- Prohibido pegar o marcar con adhesivos las pantallas de los equipos.

- Queda prohibido el uso del equipo de cómputo a personal ajeno al Hospital Santa Margarita, sin autorización y supervisión del responsable de este.

- Prohibida la duplicación de CDS de música, software, películas, en los equipos del Hospital Santa Margarita ya que al hacerlo estamos incurriendo en un delito.

40-42.15

- Prohibido ingerir cualquier alimento frente a los equipos.
- Prohibido fumar frente a los equipos.
- Procurar operar los equipos con las manos limpias, para evitar ensuciar los teclados y el Mouse.
- No tocar las pantallas de los monitores, ya que quedan residuos de grasa corporal y su limpieza no siempre es factible.
- No golpear los equipos.
- Cualquier extravío en los componentes del equipo, será responsabilidad del encargado de este y deberán ser repuestos por este.
- Los daños o pérdidas de los equipos, provocados por uso inadecuado, serán reparados con cargo al responsable del equipo.
- Prohibida la extracción de equipos de escritorio e impresoras de las instalaciones del Hospital Santa Margarita sin previa autorización del área de inventarios.
- Prohibido el uso de equipos para cualquier fin ajeno a las actividades inherentes a su puesto.
- Para llevar un control especial de las solicitudes realizadas por los usuarios al área de sistemas, todo requerimiento debe ser registrado en el módulo de soportes, creado para tal fin.

40-42.15

8. CONTROL DE CAMBIOS

LABORADO POR	REVISADO POR	APROBADO POR
Líder de Sistemas	Jefe de Oficina Administrativa y Financiera - Líder de Calidad	Gerente

REGISTRO DE CAMBIOS Y REVISIONES				
VERSIÓN	**FECHA**	**PÁGINAS**	**SOLICITANTE**	**OBSERVACIONES**
1	02/01/2025	18	Gerencia	Creación del documento por Nixon Bravo – Líder de Sistemas Revisado por Duvan Felipe Ochoa Toro – Líder de Calidad, Juan Manual Chávez – Jefe de Oficina Administrativa y Financiera Aprobado por Aicardo Solís - Gerente