

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	1 de 35

POLITICA DE SEGURIDAD DE LA INFORMACION



SEPTIEMBRE 2020

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	2 de 35

Elaborado por:

Diego Fernando Martinez

Revisò:

Gerencia de la E.S.E Hospital Sagrado Corazón de Jesus

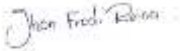
Derechos reservados a favor de E.S.E Hospital Sagrado Corazón de Jesús, La Hormiga, Valle del Guamuez, Putumayo.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	3 de 35

CONTROL DE DOCUMENTO

	NOMBRE	CARGO	DEPENDENCIA	FECHA	FIRMA
AUTORES	Diego Fernando Martinez	Coordinador sistema de gestión documental	Sistemas de información	Septiembre de 2020	
REVISÓ	Jhon Fredy Reina Taimal	Profesional Universitario	Planeación	Octubre de 2020	
APROBACIÓN					

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	4 de 35

HOJA DE ACTUALIZACION

Versión	Elaborado por	Revisado por	Motivo	Hojas a reemplazar	Fecha	Firma
1.0	Diego Fernando Martinez	Gerencia E.S.E Hospital Sagrado Corazón de Jesús	Elaboración Programa de conservación documental	N/A	OCTUBRE 2020	

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	5 de 35

INTRODUCCIÓN

Los niveles de seguridad que exigen hoy en día las tecnologías de la información son cada vez más altos y complejos, esto debido al crecimiento exponencial que ha tenido la Internet en los últimos años. La protección de información y bloqueo de intrusos, son tan solo ejemplos de los objetivos a lograr para que la infraestructura informática de una organización sea segura.

La posibilidad de expandir la cobertura de servicios, de interconectar bases de datos y de acercar a los usuarios separados por grandes distancias, ha llevado a la aparición de nuevas amenazas en los sistemas computarizados, si crece la cobertura, crece la vulnerabilidad.

Hoy por hoy, muchas organizaciones gubernamentales y no gubernamentales, nacionales e internacionales desarrollan políticas de seguridad que rigen el uso adecuado de la tecnología y hacen recomendaciones para aprovechar sus ventajas y evitar su uso indebido; previendo así problemas en el uso de los bienes y servicios informáticos de las entidades.

Las políticas de seguridad informática surgen como una herramienta organizacional necesaria para concientizar a cada uno de los integrantes de una empresa sobre la importancia, la sensibilidad de la información y la necesidad de su conservación con el mínimo de riesgo y un alto grado de seguridad que Favorezca el desarrollo de la organización, garantice su óptimo funcionamiento y el buen uso de los equipos y recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	6 de 35

JUSTIFICACIÓN

Ante el gran crecimiento de las redes de información y del uso de internet para la conexión de las mismas, la transmisión de datos y la optimización de las telecomunicaciones que se ha dado en los últimos años, es evidente que la vulnerabilidad de los sistemas crece al mismo ritmo y es necesario que las medidas de seguridad y protección sean cada vez más eficientes y menos fáciles de burlar por personas dedicadas al hacking, virus informáticos, software espía y demás ataques que traten de afectar la información de las empresas.

Cada día las empresas de nuestro país y de nuestra región tienen un riesgo mayor de sufrir ataques por hackers, incluso algunas ya se han visto afectadas por problemas de virus, caída de servidores y pérdida de valiosa información. Las amenazas están en todo tipo de entidades, y pueden ser externas o internas, entre ellas tenemos: Uso indiscriminado de la Internet, mala práctica de los usuarios, descuido en la manipulación de los equipos y el desconocimiento de conceptos básicos de manejo de dispositivos informáticos. Es por eso, que la política de seguridad informática cumple un papel determinante en la protección de las redes, los datos y los equipos de una Institución.

Ante la alta tasa de equipos infectados y la consiguiente pérdida de información por virus y mala manipulación de la información, la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús, en su función de ofrecer recursos informáticos, seguros, estables y confiables, decide elaborar un Manual de Políticas de Seguridad que compile las medidas tomadas en los últimos meses, y con el fin de poder garantizar, el cumplimiento de las políticas que le asegurarán a la entidad una protección continua tanto para los activos tangibles como para los intangibles.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	7 de 35

ALCANCE

La aplicación del Manual de Políticas de Seguridad Informática, de la ESE Hospital Sagrado Corazón de Jesús acogería a todos los funcionarios, de planta y contratistas, asistenciales y administrativos que hagan uso de herramientas informáticas y/o estén conectados a la red de la institución.

La Política de Seguridad que se implemente requiere un alto compromiso por parte de cada uno de los funcionarios de la institución, capacidad para detectar fallas y anomalías y el establecimiento de controles continuos para renovar y actualizar dicha política en función del ambiente dinámico, cambiante y evolutivo que nos rodea.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	8 de 35

OBJETIVO GENERAL

Elaborar un Manual de Políticas de Seguridad Informática para la ESE Hospital Sagrado Corazón de Jesús, que cree una cultura organizacional de buenas prácticas en el aspecto computacional y fortalecer la protección física y lógica de los activos informáticos de la entidad.

OBJETIVOS ESPECIFICOS

- Establecer normas de cuidado de equipos, periféricos y demás dispositivos fiascos.
- Sensibilizar a todos los usuarios de la ESE Hospital Sagrado Corazón de Jesús acerca de la necesidad de poner en práctica el Manual.
- Crear mecanismos de protección a partir de la toma de precauciones, básicas pero fundamentales a la hora de utilizar los recursos de red tales como internet o intranet.
- Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la ESE Hospital Sagrado Corazón de Jesús.
- Documentar las políticas de seguridad, creadas para la ESE Hospital Sagrado Corazón de Jesús y junto con el plan de contingencia, establecer los parámetros fundamentales de estabilidad y confiabilidad del área informática de la institución.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	9 de 35

GLOSARIO

Activo: Conjunto de bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar (manejar o controlar) equipos informáticos o servicios físicamente separados.

Amenaza: Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

Antivirus: Son una herramienta simple cuyo objetivo es detectar y eliminar virus Informáticos.

Área Crítica: Área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la ESE Hospital Sagrado Corazón de Jesús.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Bases de Datos: Conjunto de datos interrelacionados y de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

Cadena: Mensaje que intenta inducir al receptor a realizar algún número de copias de un mensaje de correo para luego pasarlas a uno o más receptores nuevos.

CD (Disco compacto): Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

Comando: Instrucción u orden que el usuario proporciona a un sistema informático, a través de una línea de texto basada en palabras clave.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	10 de 35

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.

Crack: Programa que realiza una modificación permanente o temporal sobre otro en su código, para obviar una limitación o candado impuesto a propósito por el programador original. Algunas legislaciones consideran este tipo de programas ilegales por facilitar la vulneración de los derechos de autor de códigos no libres o comerciales.

Dirección IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, una interface de conexión de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol).

Hacking: Acción de infiltrarse ilegalmente a sistemas informáticos y redes de telecomunicación con fines delictivos.

Hardware: Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

HOAX: (Engaño, mentira, patraña). Mensaje de e-mail con contenido falso o engañoso generalmente proveniente en forma de cadena.

Integridad: Proteger la información de alteraciones no autorizadas por la institución.

DVD (Disco Versátil Digital): Dispositivo de almacenamiento óptico en forma de disco, similar al CD, pero de mayor capacidad de almacenamiento (4.7 GB).

Internet: Red de redes de computadoras conectadas a nivel mundial, se emplea para el intercambio de información, el acceso a bases de datos, entre otros fines.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	11 de 35

Equipo de Cómputo: Dispositivo con la capacidad de aceptar y procesar información, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

Intranet: Red de computadoras privadas que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información, datos y sistemas operativos. **Equipo de Telecomunicaciones:** Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Keygen: Programa informático, generalmente ilegal, que al ejecutarse genera un código para que un determinado programa software de pago en su versión de prueba pueda ofrecer los contenidos completos del mismo.

Estabilizador: Dispositivo para la toma de la tensión de la red eléctrica que alimenta al computador y a la red.

Mantenimiento: Acciones que tienen como objetivo mantener un artículo o restaurarlo a un estado original.

Filtro de contenidos web: Herramienta informática que bloquea o permite el acceso a determinados sitios de internet.

Memoria USB: Dispositivo de almacenamiento masivo que utiliza memoria flash para guardar la información que se puede requerir.

FTP (File Transfer Protocol): Protocolo y software que permite la transferencia de archivos entre máquinas conectadas a una red.

Módulo: Parte de un programa de computador.

Periférico: Dispositivos externos que se conectan al computador.

Red: Conjunto de computadoras y elementos interconectados que permiten una comunicación entre sí y forman parte de un mismo ambiente.

Servicio: Conjunto de aplicativos, programas informáticos o sitios web que apoyan la labor administrativa de la institución, sobre los procesos diarios que demanden información o comunicación en la misma.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	12 de 35

Software: Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software espía: Controla el uso de la computadora sin el conocimiento o consentimiento del usuario. Los software espía pueden grabar la secuencia de pulsación de teclas, el historial de navegación, contraseñas y cualquier otra información confidencial y privada, y enviar estos datos a un tercero vía Internet.

Soporte Técnico: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de la institución.

SPAM: Mensajes no solicitados, no deseados o de remitente no conocido.

UPS (Uninterrupted Power System): Sistema de Potencia Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

Usuario: Cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga algún tipo de vinculación con la ESE Hospital Sagrado Corazón de Jesús.

Virus Informático: Programa software que altera el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	13 de 35

RIESGOS INFORMÁTICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo Informático como: **“La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños.”**

En una entidad, los riesgos informáticos, son latentes día a día y pueden afectar gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas como lo ilustra la siguiente tabla.

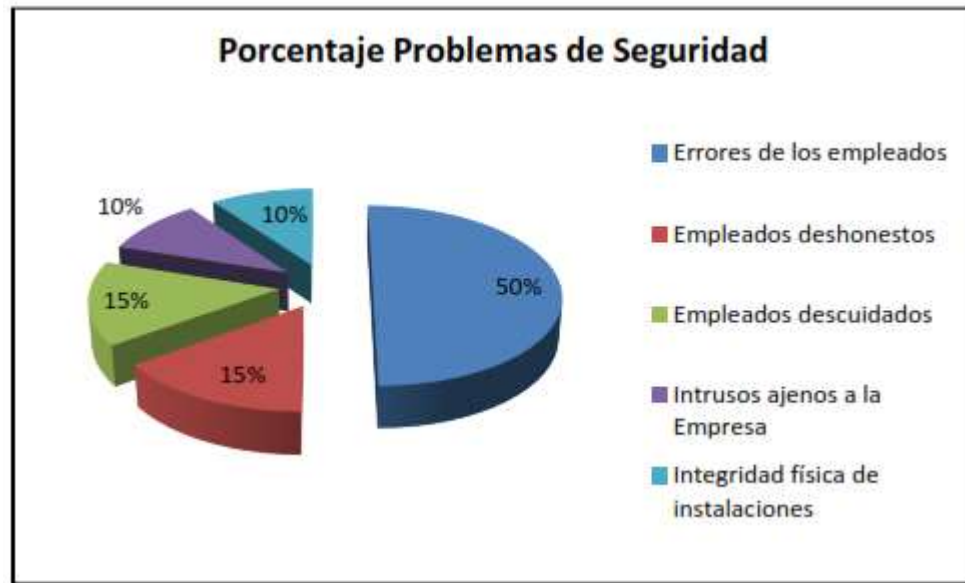
RIESGOS EXTERNOS	RIESGOS INTERNOS
<p>Origen Tecnológico: Cuando parte de la infraestructura tecnológica de la institución depende de terceros y esta falla inesperadamente. Ej. Caída de la conexión a internet.</p>	<p>Origen Tecnológico: Cuando la infraestructura informática o los mecanismos de protección de la institución fallan. Ej. Caída inesperada de alguno de los servidores, cambios bruscos en el fluido eléctrico de la institución</p>
<p>Origen Humano: Producidos por errores en el suministro de información a la entidad, o errores en soportes técnicos realizados a equipos de la institución por terceros. O también producidos por posibles ataques de hackers desde el exterior.</p>	<p>Origen Humano: Cuando los usuarios cometen errores (voluntarios o no) al utilizar los recursos informáticos de la institución. Errores en el diligenciamiento de información por parte de los usuarios de la red de la institución, mal manejo de los equipos, pueden causar serias inconsistencias en el sistema.</p>
<p>Origen Natural Cuando eventos extraordinarios de origen natural, afectan físicamente la infraestructura de la institución, tocando también a las redes y equipos informáticos. Ej. Terremotos, incendios, etc.</p>	

Estudios muestran que los problemas de seguridad en sistemas basados en redes se distribuyen de la siguiente manera:

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	14 de 35



Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos:

- Problemas por ignorancia
- Problemas por ociosidad
- Problemas por malicia

Entre estas razones, la ignorancia es la más fácil de manejar. Desarrollando tácticas de entrenamiento, capacitación y procedimientos formales e informales son fácilmente neutralizadas. Los usuarios, además, necesitan controles, que les recuerde cosas que ellos deberían conocer.

La ociosidad será siempre un riesgo latente pero, se encuentra que éste es un problema menor cuando los usuarios “chocan” con los límites que ponen los sistemas de seguridad.

La malicia, se debe combatir creando una cultura en la organización que aliente la lealtad de los empleados.

Calidad y Oportunidad en los Servicios

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	15 de 35

RESPONSABILIDADES DE LA OFICINA DE SISTEMAS DE INFORMACION

Administrar y coordinar diariamente el proceso de Seguridad Informática de la ESE Hospital Sagrado Corazón de Jesús. El Código único Disciplinario (Ley 734 de 2002) Art.34 Num.28. Establece: **“Son deberes de todo servidor público: Controlar el cumplimiento de las finalidades, objetivos, políticas y programas que deban ser observados por los particulares cuando se les atribuyan funciones públicas.”**

Ser el eje para todos los procesos de seguridad y ser capaz de guiar y aconsejar a los usuarios de la institución sobre cómo desarrollar procedimientos para la protección de los recursos.

Desarrollar procedimientos de seguridad detallados que fortalezcan la política de seguridad informática institucional.

Promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.

Elaborar un Plan de Contingencia, con la finalidad de dar una respuesta rápida, que sirva para la investigación de la eventualidad ocurrida y para la corrección del proceso mismo.

Establecer vínculos con otras oficinas de sistemas de otras empresas, capacitarse y actualizarse en temas de seguridad con el objetivo de ampliar sus conocimientos y aplicar soluciones a problemas de seguridad del entorno institucional.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	16 de 35

QUE SON POLÍTICAS DE SEGURIDAD?

Son las reglas y procedimientos que regulan la forma en que una organización mitiga los riesgos y busca establecer los estándares de seguridad a ser seguidos por todos los involucrados en el uso y mantenimiento de las herramientas tecnológicas.

Se consideran como el primer paso para aumentar la conciencia de seguridad de la información, están orientadas hacia la formación de buenos hábitos.

CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para efectos de comprensión y estructuración de este documento, la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús ha clasificado las políticas de seguridad en los siguientes grupos:

Equipos: Todo lo relacionado con el hardware, su uso y cuidado.

Usuarios: Concerniente a las personas que utilizan los recursos informáticos de la institución.

Software: los recursos lógicos tales como programas, aplicativos y demás.

Redes e Internet: las medidas que se deben tomar a la hora de utilizar los recursos de telecomunicación.

Datos e Información: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la institución.

Administración de seguridad Informática: Establece la forma en que la Oficina de Sistemas gestiona la seguridad de la infraestructura informática de la ESE Hospital Sagrado Corazón de Jesús.

POLITICAS DE SEGURIDAD DE EQUIPOS

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	17 de 35

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: **“Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.”**

Los equipos son la parte fundamental para el almacenamiento y gestión de la información. La función de la Oficina de Sistemas es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas en caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura informática. Comprende las siguientes políticas:

1. Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la ESE Hospital Sagrado Corazón de Jesús, sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas, de lo contrario no le será permitido conectar su equipo o dispositivo.

Para los equipos que no sean propios de la ESE Hospital Sagrado Corazón de Jesús, se debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrir los equipos o periféricos de terceros.

2. La oficina de Sistemas tendrá registro de todos los equipos que son propiedad de la ESE Hospital Sagrado Corazón de Jesús, Si se requiere hacer un traslado de computador, periférico o accesorio, debe contar con el consentimiento de la oficina de propiedad planta y equipo. Si el equipo necesita trasladarse en calidad de préstamo (periodos de horas o días), debe notificarse a la oficina de Sistemas y diligenciar el formato correspondiente.

3. Cualquier equipo, periférico o accesorio de propiedad de la ESE Hospital Sagrado Corazón de Jesús que necesite ser retirado de la Institución tendrá que autorizarlo la Oficina de Sistemas.

4. Todo equipo de la Institución, debe estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	18 de 35

en conjunto con el área de mantenimiento de la ESE Hospital Sagrado Corazón de Jesús. En general, todos los equipos, periféricos y accesorios computacionales de la red de la ESE Hospital Sagrado Corazón de Jesús deben estar lejos de dos factores principales: La luz directa del Sol y de humedades, filtraciones y demás medios que puedan hacer que el equipo tenga contacto con el agua.

5. Todo equipo o periférico perteneciente a la red de la ESE Hospital Sagrado Corazón de Jesús, deberá contar con un dispositivo de protección eléctrica, ya sea estabilizador de corriente o UPS, que resguarde al equipo ante un cambio brusco en la corriente eléctrica de la entidad o del sector donde se ubica. Por lo anterior:

Todo equipo propiedad de la institución, y que no cuente con alguno de estos dispositivos de protección, no puede ponerse en funcionamiento. Si el funcionario conectara el equipo, será el directo responsable de los daños que puedan ocurrirle a este, y se le aplicará ley 734. Régimen Único Disciplinario.

En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas.

6. Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Sistemas, que evaluará la viabilidad de dicho cambio.

.7. La protección física y la limpieza externa de los equipos corresponde al funcionario de sistema al que se le asigne la tarea, y la custodia y cuidado en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús. Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás.

En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	19 de 35

desconectarse de inmediato e informar oportunamente a la oficina de Sistemas quien hará el mantenimiento necesario he informara a quien corresponda para que se tomen las medidas correctivas necesarias.

8. No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, CD o DVD, nuevas tecnologías en los equipos de la ESE Hospital Sagrado Corazón de Jesús, salvo en aquellos casos en donde por fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas.

Para garantizar lo anterior, la oficina de Sistemas bloquea los puertos USB (solamente para el uso de memorias), y las unidades de CD/DVD, si algún usuario necesita que ese bloqueo sea levantado, deberá solicitarlo a la oficina de Sistemas, que a su vez hará llegar la solicitud a la Gerencia para su evaluación y decisión. Esta medida aplica para funcionarios y contratista que laboren en la Institución y que de una u otra manera tengan acceso a los equipos del Hospital.

9. Toda instalación de equipo, mantenimiento o proceso de soporte técnico a nivel de hardware, sin importar su nivel de complejidad, debe ser única y exclusivamente realizado por personal de la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús. Bajo ningún concepto se autoriza que personal ajeno a la oficina de Sistemas manipule los equipos de la ESE Hospital Sagrado Corazón de Jesús.

10. Para solicitar servicio de mantenimiento a un equipo, periférico o accesorio, se debe diligenciar un formato anexo.

11. Los equipos de cómputo de la ESE Hospital Sagrado Corazón de Jesús no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. (Ley 734). Está totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión. El único personal autorizado para esta labor, es el de la oficina de Sistemas. De detectarse que se está presentando esta conducta se informara y se tomaran las medidas correctivas necesarias.

12. No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de la ESE Hospital Sagrado Corazón de Jesús.

13. Los funcionarios de La oficina de Sistemas de la ESE Sagrado Corazón de Jesús son los únicos autorizados para manejar, mantener y velar por la

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	20 de 35

integridad y seguridad de los servidores centrales de la institución, a su vez de mantener las claves de estos.

14. El servidor central de la red de la ESE Hospital Sagrado Corazón de Jesús debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.

15. Los equipos propiedad del Hospital deben usarse solamente para las actividades propias de la ESE Hospital Sagrado Corazón de Jesús, por lo tanto los usuarios no deben usarlos para asuntos personales. (Delito contra los bienes de la administración pública).


16. La adquisición de nueva infraestructura de procesamiento de la información (Hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser autorizada por la Oficina de Sistemas y el jefe de la oficina afectada.

17. Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo.

18. Todo equipo de cómputo que este asignado a áreas asistenciales y requiera ser retirado del servicio para mantenimiento, reparación, reubicación o reemplazo, debe previamente pasar por un proceso de desinfección en sitio, con el fin de prevenir posible contaminación.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	21 de 35

POLITICAS DE SEGURIDAD DE USUARIOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.

Todos los funcionarios y contratistas de la ESE Hospital Sagrado Corazón de Jesús, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este Documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por el Hospital.

La información almacenada en los equipos de cómputo del Hospital es propiedad de la ESE Hospital Sagrado Corazón de Jesús y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso del Hospital debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.


Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

1. Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del jefe de la Oficina quien debe velar por su adecuado manejo.

2. Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo a la oficina de Sistemas quienes le facilitarán el acceso y lo acompañarán en el proceso. Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos;

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	22 de 35

El uso no autorizado o impropio de la conexión al Sistema; el uso indebido de las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.

3. El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas a la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús.

4. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código, tienen que solicitar una auditoría a la oficina de Sistemas que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

5. Informar inmediatamente a la oficina de Sistemas cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.

A cualquier infracción a la política de seguridad informática cometida por un funcionario y/o contratista de la ESE Hospital Sagrado Corazón de Jesús, se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: **“Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”**


6. En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de la ESE Hospital Sagrado Corazón de Jesús, la oficina de Sistemas dispone de un funcionario para atender y solucionar estos inconvenientes que está debidamente reportado en la oficina de Regionalización medica quien es el encargado de localizarlo.

7. Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: **“Son deberes de todo servidor público: denunciar los delitos contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”**

8. Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo


	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	23 de 35

de la información que maneje, especialmente si dicha información es crítica. Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 22: **“Son deberes de todo servidor público: Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.”**

9. La oficina de Sistemas es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la institución.

10. Los usuarios de la red de la ESE Hospital Sagrado Corazón de Jesús recibirán capacitación para el manejo de las herramientas desarrolladas en la institución. La asistencia a la capacitación es obligatoria y requisito indispensable para acceder al sistema de información de lo contrario no se le asigna claves y contraseñas. Esta totalmente prohibido el uso de contraseñas o claves de otro usuario.

11. No se permitirá el almacenamiento y/o procesamiento de información propiedad del Hospital, en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita al Hospital proteger la información.


	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	24 de 35

POLITICA DE SEGURIDAD DE SOFTWARE

1. La oficina de Sistemas es la única responsable de la instalación de software informático y de telecomunicaciones.
2. En los equipos de cómputo de la ESE Hospital Sagrado Corazón de Jesús, no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de “Cracks”, “Keygens” y demás aplicativos.
3. Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la ESE Hospital Sagrado Corazón de Jesús.
4. Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.
5. Las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas.
6. La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas y a la disponibilidad presupuestal con el que se cuente.
7. Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.
8. La oficina de Sistemas administrará los diferentes tipos de licencias de software con la que cuenta la ESE Hospital Sagrado Corazón de Jesús y vigilará su vigencia de acuerdo a sus fechas de caducidad.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	25 de 35

POLITICAS DE SEGURIDAD DE LA RED E INTERNET

1. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de la ESE Hospital Sagrado Corazón de Jesús previa solicitud por escrito.

2. Se prohíbe utilizar la red y los equipos de la ESE Hospital Sagrado Corazón de Jesús para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 24: **“Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”**

3. En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la ESE Hospital Sagrado Corazón de Jesús.

4. Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.

Utilizar los recursos de la ESE Hospital Sagrado Corazón de Jesús para el acceso no autorizado a redes y sistemas remotos.


Acceder remotamente a los equipos de la ESE Sagrado Corazón de Jesús, los únicos funcionarios autorizados para realizar estas prácticas son los de la oficina de Sistemas, al momento de dar soporte a los usuarios en horario extra laboral.

Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.

Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	26 de 35

Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.

Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.

El intercambio no autorizado de información de propiedad del Hospital, de sus usuarios y/o sus funcionarios, con terceros.

El acceso a cuentas de correos personales de ningún tipo desde la red del Hospital y solo se podrán utilizar las cuentas de correo electrónico suministradas por la Institución Algunos ejemplos de los sistemas de correos electrónicos personales no autorizados son yahoo, Hotmail, gmail.

Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario. **Código Único Disciplinario (Ley 734 de 2002) Art. 35 Num. 9: “A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres.”**


5. La oficina de Sistemas tiene habilitado un equipo con acceso total a internet, en el cual, los usuarios puedan realizar consultas o actividades personales, de corta duración. La oficina de Sistemas no se responsabiliza por pérdidas de información en ese equipo, ya que es de uso público y periódicamente se está eliminando información ajena a la institución. La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas

6. Los servicios bancarios vía web a nombre de la ESE Hospital Sagrado Corazón de Jesús, solamente podrán ser utilizados por el jefe de tesorería y únicamente en el equipo que este tenga asignado. La oficina de Sistemas, tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.

7. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por la oficina de Sistemas.

Calidad y Oportunidad en los Servicios


Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	27 de 35

8. El uso de carpetas compartidas está prohibido para todos los funcionarios y/o contratistas, ya que en caso de infiltrarse un virus o programa malicioso, usa este medio para propagarse. Las únicas carpetas compartidas que pueden existir en la red de la ESE Hospital Sagrado Corazón de Jesús, son las copias de seguridad programadas, tanto de base de datos como de información de los usuarios. Está prohibido el uso abusivo de estos recursos por parte de los usuarios en forma tal que afecte negativamente el rendimiento de la red.

9. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina de Control Interno y Control Interno disciplinario para que se tomen las medidas pertinentes.

10. Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital. Los buzones no deberán contener mensajes con más de un año de antigüedad. Pero se debe dejar un histórico del registro de los mensajes. Todos los mensajes enviados deben respetar los formatos de imagen corporativa definidos por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	28 de 35

POLITICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

1. Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva. Aplicación de la Ley 594 de 2000 Ley de Archivos. Tablas de Retención Documental.

2. La copia de seguridad de la base de datos central de la ESE Hospital Sagrado Corazón de Jesús se genera así:

Dos copias diarias del aplicativo SIHOS, una diaria del aplicativo Infosalud y una diario del aplicativo Compuconta almacenadas en un equipo diferentes a los servidores; Una copia semanal en disco, que será almacenada de acuerdo a los requerimientos necesarios para dicho fin ubicado en un sitio distante del área de trabajo. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de las mismas. La ubicación de los medios de almacenamiento, deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

3. El propietario de la información, con la participación de un funcionario de la oficina de Sistemas son los encargados de la creación y seguimiento de las copias de seguridad realizadas a la información previamente seleccionada por el usuario.


4. Cualquier aplicación, archivo desconocido o sospechoso que aparezca en la información del usuario (ya sea en el equipo local, correo electrónico), no debe ser abierto o ejecutado sin antes contar con la asesoría de la oficina de Sistemas, que se encargará de examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.

5. No está permitido extraer información por ningún medio y bajo ningún motivo de la institución.

6. Atender todas las disposiciones de la Ley 527 de 1999. Que define y reglamenta el acceso y uso de los mensajes de datos, del comercio

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	29 de 35

electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

7. La Ley 594/00 Ley General de Archivos, en sus Artículos 19 y 21 establece: Art. 19 “. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos: a) Organización archivística de los documentos; b) Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

PARAGRAFO 1o. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información.


PARAGRAFO 2o. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.

ARTICULO 21. PROGRAMAS DE GESTION DOCUMENTAL. Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos.

PARAGRAFO. Los documentos emitidos por los citados medios gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, su integridad y el cumplimiento de los requisitos exigidos por las leyes procesales Acuerdo 060/2001 del Archivo General de la Nación. **POR EL CUAL SE ESTABLECEN PAUTAS PARA LA ADMINISTRACION DE LAS COMUNICACIONES OFICIALES EN LAS ENTIDADES PUBLICAS Y LAS PRIVADAS QUE CUMPLEN FUNCIONES PÚBLICAS.** “Comunicaciones por E-mail **ARTICULO DÉCIMO TERCERO: Comunicaciones oficiales por correo electrónico:** Las entidades que dispongan de Internet y servicios de correo electrónico, reglamentarán su utilización y asignarán responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de los mismos, garantizando el seguimiento de las comunicaciones oficiales recibidas y enviadas. Para los efectos de acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales se deben atender las disposiciones de la Ley 527 de 1999 y demás normas relacionadas.

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	30 de 35

CODIGO PENAL Artículo 257. *Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones.* El que acceda o use el servicio de telefonía móvil celular u otro servicio de comunicaciones mediante la copia o reproducción no autorizada por la autoridad competente de señales de identificación de equipos terminales de éstos servicios, derivaciones, **o uso de líneas de telefonía pública básica conmutada local, local extendida o de larga distancia no autorizadas**, o preste servicios o actividades de telecomunicaciones con ánimo de lucro no autorizados, incurrirá en prisión de dos (2) a ocho (8) años y multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes. **Texto resaltado declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia de la Corte Constitucional 311 de 2002** La pena anterior se aumentará de una tercera parte a la mitad, para quien hubiese explotado comercialmente por sí o por interpuesta persona, dicho acceso, uso o prestación de servicios de telecomunicaciones no autorizados. Igual aumento de pena sufrirá quien facilite a terceras personas el acceso, uso ilegítimo o prestación no autorizada del servicio de que trata este artículo.

Texto subrayado declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia de la Corte Constitucional 311 de 2002

Artículo 258. *Utilización indebida de información privilegiada.* El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, incurrirá en multa.

Artículo 294. *Documento.* Para los efectos de la ley penal es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria.


Artículo 398. *Peculado por uso.* El servidor público que indebidamente use o permita que otro use bienes del Estado o de empresas o instituciones en que éste tenga parte, o bienes de particulares cuya administración, tenencia o custodia se le haya confiado por razón o con ocasión de sus funciones, incurrirá en prisión de uno (1) a cuatro (4) años e inhabilitación para el ejercicio de derechos y funciones públicas por el mismo término.

POLITICAS EN ADMINISTRACION DE SEGURIDAD INFORMATICA

1. El nivel de prioridad de cada servicio en cuanto a seguridad y estabilidad informática, deberán estar bajo monitoreo permanente y se define en el siguiente orden:

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal
 Conmutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029
 www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com
 La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	31 de 35

ASISTENCIALES	
1	SERVICIO DE URGENCIAS
2	SERVICIO DE QUIROFANOS
3	SERVICIO DE HOSPITALIZACION
4	SERVICIO DE CONSULTA EXTERNA
5	SERVICIO DE APOYO DIAGNOSTICO Y TERAPEUTICO


ADMINISTRACION	
1	SISTEMAS DE INFORMACION
2	ARCHIVO CLINICO
3	FINANCIERA
4	RECAUDO
5	ARCHIVO Y CORRESPONDENCIA
6	OTROS

2. Las auditorías de uso de los recursos informáticos a cada dependencia de la

ESE Hospital Sagrado Corazón de Jesús deberá realizarse periódicamente de acuerdo al calendario que establezca la Oficina de Sistemas. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios.

3. Toda la información almacenada en los equipos de la ESE Hospital Sagrado Corazón de Jesús, puede ser auditada por funcionarios de la oficina de Sistemas en la verificación del cumplimiento de las políticas de seguridad establecidas. Los hallazgos encontrados serán reportados a la oficina de Control Interno, Control Interno Disciplinario y Gerencia para que se establezcan los correctivos necesarios.

4. Los jefes de oficina son los responsables en la implementación y garantía inicial del cumplimiento de políticas que hayan sido publicadas, modificadas o adicionadas recientemente. Cualquier violación a las políticas y normas de seguridad establecidas en este documento y aprobadas mediante acto administrativo será sancionada disciplinaria o penalmente. Para las infracciones más graves, se acatará lo estipulado en la ley 1273 de 2009 de delitos informáticos, y Ley 734 de 2002 Código Único Disciplinario.

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	32 de 35

LISTA DE ANEXOS

ANEXO 1 – LEY 1273 DE 2009

LEY 1273 DE 2009

(Enero 5)

Diario Oficial No. 47.223 de 5 de enero de 2009

CONGRESO DE LA REPÚBLICA

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.

EL CONGRESO DE COLOMBIA DECRETA:

ARTÍCULO 1o. Adicionase el Código Penal con un Título VII BIS denominado “De la Protección de la información y de los datos”, del siguiente tenor:

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático.* El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en

Calidad y Oportunidad en los Servicios

Dirección: Barrio la Parke vía el Rosal

Comutador 4287089 Ext. 101 Fax: 4282488 Celular: 3108020679 - 3123506029

www.hospitalhormiga.gov.co - Email: esehormiga2008@hotmail.com

La Hormiga - Valle del Guamuez – Putumayo

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	33 de 35

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.


Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO	
		1244-46.09	
		VERSION	1.0
		PÁGINAS	34 de 35

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.


CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

	POLITICA DE SEGURIDAD DE LA INFORMACION	CODIGO 1244-46.09	
		VERSION	1.0
		PÁGINAS	35 de 35

ARTÍCULO 2o. Adiciónese al artículo 58 del Código Penal con un numeral 17, así: Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:
17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

ARTÍCULO 3o. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así: Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:

6. De los delitos contenidos en el título VII Bis.