POLÍTICAS DE GOBIERNO DIGITAL

ELABORADO POR: XIOMARA HOYOS BELTRAN	**REVISADO POR:** LAURA JIMENEZ HERRERA	**APROBADO POR:** ARMANDO SEGURA EVAN
CARGO: Jefe Subsistemas de Información	**CARGO:** Asesor Calidad	**CARGO:** Gerente

Tabla de contenido

1. INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado una gran relevancia, más aún con la intervención de herramientas de carácter globalizador como Internet y en particular el acceso a diversos contenidos de información en un sin número de sitios web en los que se puede navegar, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados, llevando a que muchas organizaciones gubernamentales y no gubernamentales desarrollen políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades. De esta manera, la política de seguridad en informática de la ESE Hospital Regional del Magdalena Medio emerge como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades. El proponer esta política de seguridad requiere un alto compromiso de la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

En el presente documento se establecerán las políticas de seguridad de la información que se deben cumplir para darle un manejo adecuado a la seguridad, permitiendo así su correcto tratamiento y respaldo.

2. GLOSARIO

Política: Describe la posición de la entidad sobre la seguridad informática; es decir toda persona que ingresa a la institución para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente manual.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el

dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Antivirus: Programa cuya finalidad es prevenir los virus informáticos, así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

Dominio: Sistema de denominación de hosts (estaciones de trabajo) en red, está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario.

Encriptar: Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Firewall: Un cortafuego es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Es un punto de red que actúa como entrada a otra red.

Hardware: Componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

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

Servidor: Computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Software: Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

Activos de información: Es todo activo que almacena, procesa o muestra información. Los activos pueden ser tanto software como hardware, digitales o físicos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Establecer los lineamientos y directrices generales de seguridad informática, relacionados con el uso de la plataforma tecnológica y la utilización de los servicios informáticos de la Entidad, que debe seguir todo el personal y usuarios de la ESE Hospital Regional del Magdalena Medio

3.2. OBJETIVOS ESPECÍFICOS

- Definir un marco de referencia para direccionar el actuar del personal en el desarrollo de sus actividades, con miras a unificar la forma de realizar las tareas, propendiendo por el aumento de la productividad y la aplicación de las mejores prácticas de T.I.

- Mantener la confidencialidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Hospital, para alcanzar la misión institucional.

- Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este documento y otras de carácter institucional, legal o emitido por otros órganos del Estado, que guarden relación con normativas aplicables a la materia.

- Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.

- Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.

4. ALCANCE

Los lineamientos contenidos en el presente documento son de observancia obligatoria para todo el personal que labore en, o para el Hospital, que por sus funciones tenga acceso a equipos de cómputo, sistemas y aplicaciones, bases de datos, instalaciones del centro de cómputo y en general, a todos los recursos informáticos de la organización.

Establecer un marco de gobierno para que el uso de las TIC de la institución logre satisfacer las necesidades actuales y futuras derivadas de la estrategia de la Entidad, siguiendo los criterios de innovación, calidad, eficiencia, escalabilidad, y de arquitectura empresarial. Estas políticas son aplicables a todos los colaboradores, consultores, contratistas, terceras partes, que usen las tecnologías de información y la comunicación de la organización.

4.1. Supervisión de las políticas

La supervisión del cumplimiento de las "Políticas Generales sobre Tecnologías de Información", queda a cargo del Jefe de Subsistema de Información y el Ingeniero de Apoyo al área de Sistemas; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

4.2. Violación a las políticas

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado al Área de Sistemas a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con Talento Humano. Este documento será revisado y/o actualizado por parte del Área de Subsistemas de Información, con la finalidad de estarlo mejorando. Estas modificaciones serán aprobadas y comunicadas a través del área de Calidad.

5. POLÍTICAS DE SEGURIDAD

5.1. Uso de computadores y portátiles

- Los computadores de la ESE Hospital Regional del Magdalena Medio, no podrán ser utilizados para visualizar almacenar material no permitido y/o obsceno.
- La ESE Hospital Regional del Magdalena Medio, permitirá, en cierto límite, el almacenamiento de información personal en los discos duros de los computadores asignados a cada empleado o contratista, sin embargo, no será responsable de dicha información ni se ejecutarán esfuerzos tendientes a su recuperación.

5.2. Uso de Software

- Todo software que utilice la ESE Hospital Regional del Magdalena Medio será adquirido de acuerdo con las normas vigentes, estos recursos informáticos están disponibles para fortalecer el flujo de información interna y externa para lograr eficiencia operativa, por lo tanto, estos deberán ser utilizados en las actividades propias del cargo.
- Cualquier instalación de software deberá ser realizado o, autorizado y aprobado por el área de subsistemas de información.

- La ESE Hospital Regional del Magdalena Medio, se reserva el derecho de retirar las licencias de software, en cualquier momento, a aquellos usuarios que hagan uso indebido del software, o que incumplan total o parcialmente estos términos de uso.

- Cualquier información o inquietud de los usuarios con relación a la copia o utilización de un software determinado, deberá solicitarse como soporte técnico al Area de Subsistemas de Información o a través de correo electrónico (sopsistemas@esehospitalrmm.gov.co), enviado copia del soporte al Jefe de Subsistema de Información (sistemas@esehospitalrmm.gov.co)

- El uso de cualquier tipo de software, es exclusivo para el tiempo en el cual el servidor o servidora forme parte de la ESE Hospital Regional

del Magdalena Medio, cuando se desvincule de la institución, se deberá desinstalar cualquier licencia de software que se encuentre en la computadora que él tenga asignada.

- El usuario se obligará a respetar todos los derechos de la propiedad intelectual y a usar el software de forma diligente, correcta, lícita, y en particular, se comprometerá a abstenerse de:
  - Utilizar el software con fines contrarios a la ley y a lo establecido por el Hospital.
  - Copiar, modificar, reproducir o utilizar el software propiedad de la ESE Hospital Regional del Magdalena Medio con fines de lucro.

.

- Todos los desarrollos propios como: programas, archivos, entre otros y que sean creados en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentren almacenados en los equipos de cómputo, pertenecen a la ESE Hospital Regional del Magdalena Medio, deberán reportarse y entregarse al área de Subsistemas de Información para ser incluidos en el inventario de software de la institución.
- Ningún empleado o contratista del Hospital, o a quien le ha sido asignado un computador, podrá instalar software o hardware que no haya sido aprobado o adquirido por la entidad. Solamente el personal de sistemas o quién sea autorizado por el Área de Subsistemas de Información, podrá realizar esta labor.

5.3. Restricciones

- Intentar o realizar accesos a cuentas de usuario que no sean las propias (uso de cualquier protocolo o programa para hallar vulnerabilidades o explotación de recursos).

- Invadir la privacidad de los demás a través del computador asignado, así como intentar modificar o tener acceso a archivos, contraseñas o datos que pertenecen a otros.

- Utilizar los computadores de la Entidad para Introducir virus computacionales, malware, programas espías o cualquier otro

programa diseñado para dañar el equipo o el software utilizado en el hospital o de cualquier manera, arriesgar la seguridad de las computadoras o el sistema de red de la Entidad.

- Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de los usuarios. Excepto cuando el Área de Subsistemas de Información para asegurar el correcto funcionamiento así lo requiera.

- Afectar o paralizar algún servicio por la ejecución intento de ejecución de programas indebidos.

- Modificar archivos que no sean propiedad del usuario, aunque se tengan permisos de escritura.

- Acceder, analizar o exportar archivos que sean accesibles a todo el mundo pero que no sean del usuario, salvo que se encuentre en una ubicación que admita su uso público.

- Uso de los recursos tecnológicos de la empresa por familiares o amigos de los funcionarios, o por personal no autorizado.

5.4. Recomendaciones

- No se debe comer o colocar líquidos cerca del computador (CPU, teclado), se pueden producir choques eléctricos y por ende el daño irreparable del mismo.

- Siempre, al final de la jornada, se debe apagar el computador y/o el monitor.

- El usuario debe cambiar la contraseña regularmente o cuando considere que la misma pudo haber sido copiada.

- Reportar inmediatamente las anomalías detectadas

- Mantener depurado el correo institucional para evitar el riesgo de no recibir comunicación efectiva.

- La institución se enfocará en la implementación gradual, según la directiva presidencial 04 de abril 3 de 2012 de la política cero papel, a través de crear conciencia en los usuarios.

5.5. Consideraciones

- La ESE Hospital Regional del Magdalena Medio, no será responsable por las transacciones financieras electrónicas que realicen los empleados desde el computador asignado o desde cualquier computador que esté disponible para uso público y se encuentre en las instalaciones del Hospital.

- Reparación y mantenimiento de equipos: Los usuarios deben saber que el personal técnico tiene la autoridad para acceder a archivos individuales o datos cada vez que deba realizar un mantenimiento, sin embargo, el personal técnico del Área de Subsistemas de Información, no puede exceder su autoridad en ninguna de estas eventualidades, para usar esta información con propósitos diferentes a los de mantenimiento o reparación.

- Respuesta al uso indebido de computadores y sistemas de información: Cuando por alguna causa razonable determinada, se presuma el uso indebido de un computador o portátil, soportado en lo dispuesto en la ley 1341 de 2009, con autorización de la Gerencia, el Área de Subsistemas de Información puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a el(los) involucrado(s) en el incidente, para investigar y aplicar las sanciones a que hubiere lugar. Los empleados del Área Subsistemas de Información y a quienes se designe, están en la obligación de monitorear constantemente los computadores y portátiles de la institución a través de los medios correspondientes, para responder oportunamente frente a cualquier acción que atente contra la disponibilidad, seguridad o desempeño correcto de los mismos.

5.6. Asignación cuentas de usuario en los Software del Hospital

- Todos los funcionarios y contratistas que laboran para la ESE Hospital Regional del Magdalena Medio deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.

- La asignación de usuario y contraseña en los diferentes Software de la institución, es única e intransferible, todo lo que se haga con su usuario será responsabilidad del funcionario

- Una vez asignada la cuenta y la contraseña, la asignación de los permisos a este usuario deberá ser solicitada al área de Subsistema de Información y a los Jefes de Area se encargaran de informar las autorizaciones de ingreso a los diferentes módulos de acuerdo con su perfil.

- Cada usuario que haga uso de los diferentes Software de la institución, deberá tener definido un rol específico según su cargo y perfil profesional y/o funcional

- Antes de asignar usuario y contraseña a los diferentes funcionarios del hospital, estos deben estar en la base de datos con la información personal requerida por la oficina de Talento Humano.

- Las claves para el acceso a los aplicativos de reportes a entes de control, deberán ser entregados y custodiados por el área de Subsistemas de Información.

- Las claves de acceso compartidas asignadas a los funcionarios de los sistemas información de la Entidad tienen únicamente carácter de consulta, estas no permiten modificación de la información, no deben divulgarse hacia el exterior de la entidad, se cambiarán anualmente o cuando se requiera y exclusivamente se utilizarán para la gestión de la Entidad.

- Todos los accesos y claves de usuarios para el uso de los sistemas de información de la entidad, deberán ser desactivados o cambiados después de que un funcionario, deje de prestar sus servicios al hospital.

5.7. Seguridad del Hardware

- Los computadores del hospital son instalados por el Área de Subsistemas de Información de acuerdo a los requerimientos de las normas para cableado ANSI/TIA-1179ª y en la parte eléctrica se siguen las recomendaciones del código eléctrico colombiano RETIE, garantizando un ambiente seguro

- Los equipos de cómputo son para el desarrollo de las actividades institucionales no para otros fines y es responsabilidad del jefe de área o coordinador de servicio velar por su correcto uso.

- No puede modificarse la ubicación, ni la configuración del hardware y software instalado en los equipos de cómputo por parte de los usuarios sin el acompañamiento del área de Subsistemas de Información; se ha configurado en el dominio de la red políticas que restringen a los usuarios la modificación de la configuración de los equipos.

- Se realiza mantenimiento preventivo del 100% de los equipos, de acuerdo al Cronograma de mantenimiento y limpieza de equipos de cómputo, garantizando un mantenimiento anual.

- Cualquier falla en los computadores, impresoras o la red de datos debe reportarse inmediatamente al área de Subsistemas de Información y no tratar de manipular los equipos, ya que podría causar problemas como pérdida de la información o daño del equipo. El área de Subsistemas de Información registra la solicitud en el RTI-FR-001 Formato Identificación de Necesidades Clientes Internos V2 y clasifica la prioridad del evento.

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la Entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación técnica del área de Subsistemas de Información.

- Todos los equipos de cómputo y equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir el robo. Para ello el hospital protege contra robo los equipos portátiles y algunos de escritorio que se encuentran en zonas expuestas mediante un

sistema de cerrado de cámaras, Los demás equipos están ubicados en áreas con restricción de acceso físico a personal no autorizado y es responsabilidad del jefe de área velar por su seguridad.

- La reparación técnica de los equipos por la parte externa, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado, previamente informado Área de Subsistemas de Información

- Los equipos de cómputo y de red de se encuentran marcados y relacionados en un inventario detallando sus componentes principales como: marca, serial, garantía, ubicación, dirección IP. Los registros de inventario se mantienen actualizados, registrando las novedades de ingresos de equipos nuevos o bajos de inventario cuando se presentan. (Archivo Inventario de equipos).

- La pérdida o robo de cualquier componente de hardware debe ser reportada inmediatamente al Area de Subsistema de Información, quien informa a la administración para iniciar la investigación respectiva y la afectación de pólizas para la reposición de equipos. El área de Subsistema de Información evaluara la alternativa para dar continuidad a los requerimientos del área afectada.

5.8. Acceso físico y lógico

- Antes de conectar equipos de cómputo o algún dispositivo a la red de datos del hospital, el personal del área de Subsistemas de Información debe cumplir con el procedimiento de instalación de equipos.

- El hospital tiene implementado el sistema de acceso remoto para funcionarios autorizados y terceros a través de una VPN (Red privada virtual), la cual es validada por las políticas de acceso implementadas en el firewall de Windows, lo que garantiza un nivel de seguridad contra acceso no autorizado desde el exterior.

- Todo el intercambio de información desde la institución hacia redes externas o internet y viceversa son validadas por el firewall de Windows.

- Los aplicativos del sistema Medisoft de la E.S.E. Hospital Regional del Magdalena Medio y los módulos administrativos cuentan con un módulo de administración de privilegios los cuales delimitan la acción de los usuarios en los módulos del sistema. El perfil de los usuarios debe ser definido por los jefes de cada área y ser solicitados al Area de Subsistemas de Información para la creación y configuración de los usuario

- Cuando los usuarios dejen sus puestos de trabajo deben cerrar la aplicación y la sesión de trabajo, para evitar accesos no autorizados a datos o recursos compartidos del sistema.

- Los equipos de terceros que ingresan a la institución y deseen tener acceso a recursos como internet, deben solicitar al área de Subsistema de Información la configuración para acceso a la red, este acceso se direcciona de acuerdo a las políticas definidas por el área de Sistemas para separar su tráfico de los datos de nuestros equipos y servidores.

- Todos los equipos propiedad del hospital como computadores de escritorio, equipos portátiles, impresoras y equipos relacionados con sistemas de información no deben retirarse de las instalaciones físicas por ninguna persona a menos que esté previamente autorizado por escrito bajo la responsabilidad del área de Recursos Físicos.

- Los usuarios del sistema de información no pueden extraer información institucional para usos diferentes a los laborales.

- Todos los equipos cuentan con protección de antivirus la cual es actualizada en forma centralizada y automática. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de Subsistemas de Información. Los equipos de terceros que usan la red de datos de la E.S.E deben contar con un sistema de antivirus actualizado que será validado previamente por el área de Subsistemas de Información.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio

usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de Sistemas.

- Todo dispositivo de almacenamiento externo, memorias USB, CD, DVD, debe ser vacunado antes de abrir sus contenidos.

- Los usuarios son responsables de proteger sus contraseñas para poder ingresar a la red del Hospital. Ningún usuario puede acceder a la red con la contraseña o cuenta de otro usuario, en caso de infringir deberá someterse a lo dispuesto en la ley 1341 de 2009 (Se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC).

5.9. Seguridad del Software y datos

- Todo el software del hospital está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales. Todos los originales de instalación deben permanecer bajo seguridad de acceso físico, junto con las claves de instalación y actas de licencias en el área de subsistemas de Información y es responsabilidad del jefe del área velar por su correcto uso.

5.10. Prácticas de Uso de Internet

- Usar correctamente a cuentas de correo institucional

- No utilizar canales de chat o grupos sociales como Facebook, Messenger, etc., en horario laboral con fines personales.

- No descargar de Internet, ni alojar en los discos duros de los equipos de cómputo, música, videos, ni cualquier tipo de software sin licenciamiento.

- No abrir ningún mensaje, sitio web, ni archivo de fuente desconocida o muy poco conocidas. En caso de personas conocidas, se deben tomar precauciones, asegurándose de que esa persona es la responsable del envío y ante cualquier duda, borrar el mensaje, para evitar la contaminación de un virus.

- Todos los funcionarios del hospital, tienen la obligación a dar cumplimiento a la Ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. Por consiguiente se obligan a no utilizar los servicios, redes y sistemas del hospital que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.

- El spam o correo basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deben eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón así como la posibilidad de intrusión de virus en el sistema.

- Usar regularmente el antivirus y verificar periódicamente su actualización, el área de subsistema de información presta el soporte que se requiera para tal fin.

- No bajar nada de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. Si se bajan archivos, copiarlos a una carpeta y revisarlos con un antivirus actualizado antes de abrirlos.

- Se debe suministrar el correo electrónico asignado por el hospital con moderación, ya que podrían enviar publicidad no deseada.

- No utilizar la cuenta de correo electrónico suministrada por el hospital, para asuntos personales.

6. PROTECCIÓN CONTRA DESASTRES

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre (cortos circuitos, vandalismo, fuego y otras amenazas, etc.)

podrá afectar el nivel de servicio y la imagen del hospital, se debe prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

7. PLANES DE EMERGENCIA, CONTINGENCIA Y RECUPERACIÓN

El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento que se requiera permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos en un tiempo razonable para cada caso, y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

El mantenimiento del plan de Contingencias y Recuperación General incluye entre otros un proceso estándar que integra los planes de contingencia para computadoras y comunicaciones, así como también el inventario de hardware, software existente y los procesos que corren manualmente mientras dure la contingencia

8. INDICADORES Y MODALIDAD DE MONITOREO

El monitoreo y seguimiento se deberá realizar de manera coordinada con los responsables del área de subsistemas de información o quien haga sus veces, de conformidad con lo establecido en la ley 1341 de 2009 (Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC).

En cuanto a la periodicidad del seguimiento y funcionamiento de la política de seguridad de la información de acuerdo a los procedimientos

implementados en ESE Hospital Regional del Magdalena Medio, se realizarán auditorias con personal interno de la institución para la verificación y cumplimiento de objetivos, controles y procedimientos de seguridad de la Información. La Gerencia, Jefes de Oficina, Coordinadores de Área, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad. La ESE Hospital Regional del Magdalena Medio, asigna un funcionario para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la institución.

El seguimiento se realizará anualmente a la política de seguridad, con corte al 31 de diciembre.

9. BIBLIOGRAFÍA

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental".

CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
02-04-2019	001	Creación del Documento
31-05-2019	002	Actualización