E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

(DECRETO 612 ABRIL 04 DE 2018 - DAFP)

MILENA DEL CARMEN CHAVES CHARRIS
GERENTE

GUAMAL MAGDALENA
2018

RESOLUCION No. 0123
(29 de Junio de 2018)

"Por medio de la cual se adopta el Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena"

La Gerente de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal, Magdalena, en ejercicio de sus facultades legales y estatutarias, en especial en la Ley 1581 de 2012,

CONSIDERANDO:

Que la Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la E.S.E. con respecto a la protección de los activos de información, que soportan los procesos de la Entidad.

Que con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando el cumplimiento de las normas legales, esta ESE establecerá la realización de un Plan de Seguridad y Privacidad de la información.

Que el artículo 2.2.22.3.14 del Decreto Nacional No. 1083 de 2015, modificado por el artículo 1º del Decreto Nacional No. 612 de 2018, ha determinado que las Instituciones del Estado deben integrar planes institucionales y estratégicos que se mencionan en dicho artículo, entre los cuales se destaca el Plan de Seguridad y Privacidad de la Información, acorde con la aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata la Ley 1474 de 2011.

Que conforme a lo anterior,

RESUELVE:

ARTICULO PRIMERO: Adoptar para la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena, el Plan de Seguridad y Privacidad de la Información, el cual se encuentra anexo a la presente Resolución y hace parte integral de la misma.

ARTICULO SEGUNDO: La presente Resolución rige a partir de su expedición y deroga las normas internas de esta Empresa Social del Estado que le sean contrarias.

COMUNIQUESE Y PUBLIQUESE:

Dada en Guamal, Magdalena a los 29 días del mes de Junio de 2018.

MILENA DEL CARMEN CHAVES CHARRIS
Gerente E.S.E.

INTRODUCCION

La Gerencia y gestión de la Información es un activo intangible que constituye la antesala de la gestión del Conocimiento, centrada en facilitar y gestionar la información relacionada con el tema de interés, para ser consultada en cualquier medio, momento y lugar, por lo tanto, es acertado afirmar que la Información es un elemento vital en la pirámide de actividades, factores y elementos que hacen que una organización sea exitosa.

Actualmente disponer de información no es un problema, la principal dificultad radica esencialmente en la calidad de la información, entendiendo por calidad, la veracidad, fiabilidad, precisión y pertinencia de la información final que necesita una empresa para la toma de decisiones.

Desarrollar una adecuada planeación de la seguridad y privacidad de información no solo ahorra tiempo, costo y esfuerzo, sino que apalanca todos y cada uno de los procesos definidos en el direccionamiento estratégico de la empresa.

1. ALCANCE.

Este documento identifica los mecanismos de registro, captura y consolidación de los datos, definiendo sus fuentes a las que se accede mediante procesos informáticos para responder de manera oportuna a las necesidades de información del cliente interno y externo.

2. RESPONSABILIDADES.

En general, los responsables del velar por el manejo adecuado de la Información son todas las personas que hacen parte del Talento Humano de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal – Magdalena.

3. MARCO LEGAL.

- **Ley 23 de 1982.** Derechos de autor.
- **Ley 527 de 1999.** Por medio de la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Resolución 1995 de 1999.** Por la cual se establecen normas para el manejo de la Historia Clínica.
- **Ley 594 de 2000.** Por medio de la cual se dicta la ley general de archivos y se dictan otras disposiciones.
- **Ley 603 de 2000.** Disposición del informe anual de Gestión presentado por los administradores de las sociedades comerciales, deberán incluir entre otros el estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor.
- **ISO 27001 del mes de octubre del 2005.** Sistema de Gestión de la seguridad de la información.
- **Decreto 1011 de 2006.** Por el cual se establece el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud del Sistema General de Seguridad Social en Salud.
- **Resolución No. 1043 de 2006.** Por la cual se establece las condiciones que deben cumplir los Prestadores de Servicios de Salud para habilitar sus servicios e implementar el componente de auditoría para el mejoramiento de la calidad de la atención y se dictan otras disposiciones.
- **Resolución No 1446 de 2006.** Por la cual se define el Sistema de Información para la Calidad y se adoptan los indicadores de monitoria del Sistema Obligatorio de Garantía de Calidad de la Atención en Salud.
- **Resolución No. 1445 de 2008.** Por la cual se definen las funciones de la Entidad Acreditadora y se adoptan otras disposiciones, modificada por la resolución 123 de 2012.
- **Ley No. 1273 de 2009.** Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

4. OBJETIVOS.

- Adoptar políticas que definan los objetivos y principios de la seguridad de la información en la E.S.E. Hospital Nuestra Señora del Carmen de Guamal - Madalena, las cuales sean de obligatorio conocimiento y cumplimiento por el personal de la entidad.

- Garantizar respaldo y seguridad a la información que generan los procesos de la E.S.E. Hospital Nuestra Señora del Carmen de Guamal - Magdalena.

4.1. Objetivo Estratégico.

Mejorar continuamente los procesos de Direccionamiento y Gerencia, atención al cliente asistencial y de apoyo administrativo, mediante la adopción e implementación de procesos de mejoramiento de la calidad y asumiendo resultados de autoevaluaciones periódicas.

5. GERENCIA DE LA INFORMACION.

5.1. Enfoque desde la calidad para la gestión de la información.

Los procedimientos que conforman el proceso de gerencia y gestión de la información en la entidad, según normatividad vigente, son:

5.1.1. Recolección y Consolidación de la Información:

- Identificar las fuentes de la información y los instrumentos de recolección
- Identificar los métodos de captura y validación de los datos
- Capturar la información
- Procesar la información
- Realizar la consolidación
- Clasificar la información
- Automatizar o sistematizar la información
- Validar la información
- Generar bases de datos
- Educar al usuario

5.1.2. Entrega de la información:

- Recepcionar los requerimientos de solicitudes de información
- Clasificar los requerimientos de información
- Priorizar la información para su generación y entrega
- Generar la información solicitada
- Validar la consistencia de la información
- Remitir la información según los requerimientos
- Verificar si existen variaciones inesperadas de la información detectadas en el comparativo de los datos.
- Entregar la información en el medio solicitado y en los tiempos establecidos.

- Archivar la documentación generada

5.1.3. Implementación e Implantación del Sistema de Información:

- Identificar necesidades de información
- Consolidar y priorizar las necesidades de información
- Determinar o identificar las fuentes de información
- Determinar si la información puede ser sistematizada o física
- Parametrizar la información: información sistematizada e información física
- Indagar diferentes tecnologías para la sistematización de la información
- Establecer si la sistematización de la información es factible

5.1.4. Seguridad de la información:

- Inventariar la Información que se genera y recibe en la entidad
- Priorizar el grado de seguridad de la información
- Definir plan de seguridad de la información
- Desplegar el plan de seguridad de la información
- Ejecutar el plan de seguridad de la información
- Hacer seguimiento al plan de seguridad de la información
- Implementar Acciones de mejoramiento

6. MECANISMOS PARA LA IDENTIFICACION DE NECESIDADES DE INFORMACION.

La Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal – Magdalena, cuenta con diversos mecanismos para identificar las necesidades de información tanto de clientes internos como clientes externos.

7. IMPLEMENTACION DE POLITICAS DE SEGURIDAD DE LA INFORMACION.

La E.S.E., con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

1. **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
2. **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
3. **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

7.1. Objetivo.

Definir los mecanismos y todas las medidas necesarias por parte de la E.S.E., tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

8. DESCRIPCION DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION.

8.1. Generalidades.

La E.S.E. en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en la E.S.E.

8.2. Gestión de Activos.

- **Política para la identificación, clasificación y control de activos de información**.

La E.S.E. realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

Para el cumplimiento de estos procesos los funcionarios públicos y contratistas deben considerar lo siguiente:

1. Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

2. La información física y digital de la E.S.E. debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.
3. Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen correos electrónicos, asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionado.

4. Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

5. La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

8.3. Control de Acceso.

- **Política de acceso a redes y recursos de red.**

El responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Para el cumplimiento de estos procesos los funcionarios públicos y contratistas deben considerar lo siguiente:

1. Formalizar el proceso Gestión de TIC (Tecnologías de la Información y las Comunicaciones), que asegure que las redes inalámbricas de la E.S.E. cuenten con métodos de autenticación que evite accesos no autorizados.

2. Formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

3. Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la E.S.E., deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de confidencialidad firmado previamente.

- **Política de administración de acceso de usuarios.**

La E.S.E. establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Para el cumplimiento de estos procesos los funcionarios públicos y contratistas deben considerar lo siguiente:

1. El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre los sistemas de información de la E.S.E.

2. El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

3. El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

4. Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

- **Política de control de acceso a sistemas de información y aplicativos.**

La E.S.E. como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Para el cumplimiento de estos procesos los funcionarios públicos y contratistas deben considerar lo siguiente:

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

- Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

- El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de la E.S.E.

- El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso.

- **Políticas de seguridad física.**

La E.S.E. provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas.

Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido. Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

Los ingresos y egresos de personal a las instalaciones de la E.S.E. en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la E.S.E.; en caso de pérdida del carné, deben reportarlo a la E.S.E.

Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

- **Política de seguridad para los equipos.**

La E.S.E. para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta:

a) El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la E.S.E.
b) El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.
c) El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generado establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
d) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.
e) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

f) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
g) No está permitido el intercambio no autorizado de información de propiedad de la E.S.E.

8.4. Privacidad y confidencialidad.

Política de tratamiento y protección de datos personales en cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la E.S.E., a través del Comité de Seguridad de la Información, o quien haga sus veces, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales la E.S.E., como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la E.S.E. exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros. Los usuarios de los portales de la Contraloría Municipal de Villavicencio deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

8.5. Disponibilidad del servicio e información.

La E.S.E. con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

- **Política de continuidad, contingencia y recuperación de la información.**

La E.S.E. proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

8.6. Copias de Seguridad.

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados.

La Jefe de la Oficina de Control Interno de la E.S.E. debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			
Acciones	**Resultados Esperados**	**Indicadores**	**Medios de Verificación**
Concientizar y comunicar la Política de Seguridad y Privacidad de la Información	Efectividad en la socialización de la política	Impacto: número de personas que pasaron la evaluación aplicada /total de personas evaluadas	Pantallazos de envío a correos electrónicos, registros de asistencias a la socialización, informe de evaluación
Designar un responsable del Plan de Seguridad y Privacidad de la Información	Tener un personal designado idóneo y competente, en procura de que la información sea segura y protegida	Documento referente	Acto administrativo o contrato que designe la actividad
Instalar y mantener actualizado el estado de conexión de antivirus, debidamente licenciado, en los equipos activos de la entidad.	Minimizar el riesgo de pérdida de información en los equipos de cómputos	Números de equipos con protección antivirus / total de equipos activos *100	Informe semestral de estado de equipos de la entidad, con protección de antivirus.
Realizar una adecuada y correcta ejecución y almacenamiento de los Backus de las bases de datos e información institucional	Lograr un 70% de efectividad en el procedimiento de copias de seguridad informática, que se realicen durante el mes	Número de copias mensuales programadas /total de copias realizadas	Informe por el responsable asignado del plan, sobre los Backus realizados durante el mes

Esta Política aplica a la información que obtenga la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena en el desarrollo de actividades de prestación de servicios de salud, y en las actividades laborales, comerciales, académicas y de investigación relacionadas con su desarrollo institucional.

8.7. Historias Clínicas.

La información relacionada con las Historias Clínicas de los pacientes y/o usuarios de esta E.S.E., está regulada por la Ley 23 de 1981 y por la Resolución 1995 de 1999, en cuanto al diligenciamiento, administración, conservación, custodia y confidencialidad de las historias clínicas, conforme a los parámetros del Ministerio de Salud y del Archivo General de la Nación.

La Empresa Social del Estado, Hospital Nuestra Señora del Carmen de Guamal, Magdalena, está comprometida para actuar con responsabilidad y proteger la privacidad custodiando la información en bases de datos y archivos físicos.

9. DEFINICIONES.

Se entiende por:

- **Autorización:** consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

- **Base de datos:** conjunto organizado de datos personales que sea objeto de tratamiento.

- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Datos sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Encargado del tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

- **Responsable del tratamiento:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

- **Titular:** persona natural cuyos datos personales sean objeto de tratamiento) Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

10. TITULAR.

Para efectos de esta Política se entenderán como titulares de datos personales, personas naturales o jurídicas entre ellas los pacientes y usuarios del servicio de salud, los proveedores, clientes, benefactores, estudiantes, profesionales de la salud y empleados en general.

10.1. Derechos del titular.

El Titular tendrá derecho a conocer rectificar y actualizar sus datos personales, solicitar prueba de la autorización salvo casos excepcionales por ley, ser informado sobre el uso que se le da a sus datos personales, presentar consultas e interponer quejas, solicitar revocatoria a la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena, incumplimiento en la normatividad y a acceder de manera gratuita a los datos personales que hayan sido objeto de tratamiento.

10.2. Deberes del titular.

El Titular debe garantizar la veracidad de la información que proporciona a la E.S.E. y actualizar su información de manera oportuna. En caso de falsedad en la información suministrada la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena, se exime de cualquier responsabilidad.

11. AUTORIZACION.

La E.S.E. requiere la autorización previa informada y expresa del titular la cual será obtenida por medios escritos bien sea físicos o electrónicos, de tal manera que pueda ser objeto de consulta posterior.

Al solicitar la información al Titular se debe informar de manera clara la finalidad para la cual se recaudan los datos personales, el tratamiento al cual pueden ser sometidos los datos personales, sus derechos y los medios a través de los cuales puede ejercerlos y la facultad de autorizar o no el tratamiento en caso de datos sensibles.

- **No se requiere autorización del titular de los datos personales cuando se trate de:**

- Responder a una orden judicial o cuando los solicita una entidad pública o administrativa en ejercicio de sus funciones legales;
- Datos personales de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Información autorizada por la ley para fines históricos, estadísticos o científicos
- Datos relacionados con el registro civil de las personas

- **Datos de niños, niñas y adolescentes:**

La autorización para el tratamiento de los datos personales de menores de edad debe realizarse bajo la facultad de los padres de familia o representantes legales del menor.

12. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.

En esta Política se identifica como Responsable de los datos personales a la Gerencia y al funcionario o servidor público que tenga bajo su responsabilidad los documentos que se generen en la Empresa Social del Estado Hospital Nuestra Señora del Carmen de Guamal, Magdalena y que tenga estos bajo su custodia.

Adoptado mediante Resolución No. 0123 del 29 de Junio de 2018.

MILENA DEL CARMEN CHAVES CHARRIS
Gerente E.S.E.