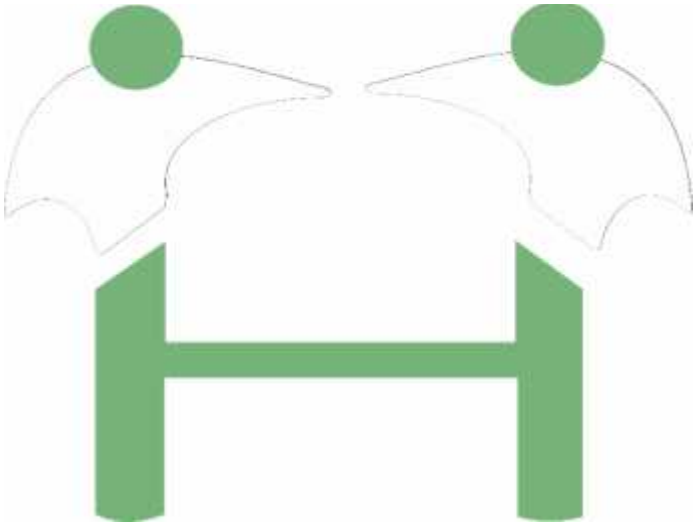
HOSPITAL SAN ANTONIO DE CHIA



DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

"TIC"

Plan de Seguridad y privacidad de la información.

Chía - 2018

TABLA DE CONTENIDO

1. OBJETIVO

La **E.S.E. Hospital San Antonio de Chía**, consiente de la importancia en el manejo, trato y conservación de la información como activo y herramienta fundamental para los procesos internos y externos de la institución bajo los principios de integridad, confidencialidad, seguridad y disponibilidad de los datos, adopta el siguiente plan de seguridad y privacidad de la información.

2. ALCANCE

Este Plan de Seguridad y Privacidad de la Información y su política, es una herramienta que abarca todas las áreas del hospital y el centro de salud de cota, que cuentan con sistemas y canales comunicación, información y recursos informáticos.
Comienza desde el análisis de los posibles riesgos a que están sujetos los equipos y la red de datos, se pretende reducir la posibilidad de ocurrencia de estos y establecer los procedimientos para dar solución en caso que se presente algún evento.

3. RESPONSABLES

Jefe del Área de las TIC

4. TERMINOLOGÍA

- **Acceso a la Información Pública**
  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control De sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo**
  En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, Personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**
  En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo**
  Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e Información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

- **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**
  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**
  Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización**
  Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales**
  Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad**
  Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio**
  Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control**
  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos**
  Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales**
  Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos**
  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. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**
  Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos**
  Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales 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. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad**
  Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad**
  Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos**
  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. (Ley 1581 de 2012, art 3)
- Gestión de incidentes de seguridad de la información
  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de continuidad del negocio**
  Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**
  Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad**
  En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada**
  Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos**
  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. (Ley 1581 de 2012, art 3).

- **Riesgo**
  Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**
  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**
  Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y
  recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información**
  Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad**
  Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

5. MARCO LEGAL

- Acceder los datos personales que hayan sido objeto de Tratamiento conforme a lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la Constitución, a la Ley 1581 de 2012 y a las demás normas que la reglamenten, modifiquen o subroguen.

6. CONTENIDO DEL PLAN

La **E.S.E. Hospital San Antonio de Chía** consiente de la importancia en el manejo, trato y conservación de la información, como herramienta fundamental para los procesos internos y externos 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, seguridad y confidencialidad de la información.

De acuerdo a este plan 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. 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. Hospital San Antonio de Chía.**

6.1. Gestión de Activos

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

La **E.S.E. Hospital San Antonio de Chía,** por medio del departamento de informática y la gerencia administrativa velara por garantizar la integridad física y magnética de la plataforma tecnológica de la institución ante los posibles riesgos que puedan generarse por acontecimientos de índole natural, factores externos o internos y que afecten el pleno funcionamiento de los elementos informáticos con los que cuenta la institución,

garantizando la continuidad de los procesos, la salvaguarda de la información y los activos informáticos con lo que cuenta el hospital.

Pautas para tener en cuenta

a) Los usuarios deben acatar los lineamientos contenidos en las diferentes políticas y planes en cuanto el acceso, divulgación, almacenamiento, copia, transmisión y Eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital de La **E.S.E. Hospital San Antonio de Chía,** debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad, para tal caso la responsabilidad será del comité de archivo.

c) Los usuarios deben tener en cuenta las siguientes consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

d) 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.

e) 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.

f) La responsabilidad en cuanto al cumplimento de lo anteriormente descrito, recae sobre cada funcionario responsable de su oficina y deberá en la medida de sus posibilidades garantizar el cumplimiento de las normas e informar las irregularidades al respecto.

6.2. Control de Acceso

6.2.1. Política de acceso a redes y recursos de red

El área de las TIC de La **E.S.E. Hospital San Antonio de Chía,** como 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.

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas de La **E.S.E. Hospital San Antonio de Chía,** cuenten con métodos de autenticación que evite accesos no autorizados.

b) El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de La **E.S.E. Hospital San Antonio de Chía,** así como velar por la aceptación de las responsabilidades de dichos terceros.

Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

c) 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. Hospital San Antonio de Chía**, deben contar con el formato de autorización del certificador del contrato para la creación de las cuentas de usuario y el acuerdo de Confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la **E.S.E. Hospital San Antonio de Chía** deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

e) Los equipos de terceras personas que ingresen al hospital y que utilicen de alguna manera las redes de la institución, deberán garantizar el licenciamiento de ley de los sistemas operativos y el software instalado en los mismos y velar por el uso adecuado, así mismo serán los responsables ante los entes de control por el incumplimiento de las normas de derechos de autor y demás normas y leyes de protección a la propiedad intelectual, eximiendo a la institución de toda responsabilidad al respecto.

6.2.2. *6.2.2 Política de administración de acceso de usuarios*

La **E.S.E. Hospital San Antonio de Chía** 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 que la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la **E.S.E. Hospital San Antonio de Chía**; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) 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, para los casos de funcionarios que se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo, las jefaturas de las áreas serán las responsables de informar de manera escrita la novedad y será responsabilidad de ellos la no actualización de los perfiles de usuario.

c) El proceso Gestión de TIC, debe asegurarse que una vez le sea informado por los jefes de área los usuarios o perfiles de usuario que deben ser actualizados, se asigne o inhabilite el acceso a los diferentes recursos de la plataforma tecnológica.

d) 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.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

6.2.3. *6.2.3 Política de control de acceso a sistemas de información y aplicativos*

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

El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. 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.

Pautas para tener en cuenta

a) 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.

b) 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.

c) El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de **E.S.E. Hospital San Antonio de Chía**.

d) 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.

e) El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

g) 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.

h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura.

6.2.4. *6.2.4 Políticas de seguridad física*

La **E.S.E. Hospital San Antonio de Chía** provee 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 y de uso exclusivo del área de informática.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario, estas deberán quedar registradas en un formato de registro de acceso.

b) El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

c) La ESE Hospital San Antonio de Chía debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la **E.S.E. Hospital San Antonio de Chía.**

d) El proceso Gestión de TIC debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones de la **E.S.E. Hospital San Antonio de Chía** 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 y su seguimiento será responsabilidad de los jefes de cada área.

f) 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. **Hospital San Antonio de Chía** en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible a la secretaria general o jefe inmediato.

g) 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.

6.2.5. *6.2.5 Política de seguridad para los equipos*

La **E.S.E. Hospital San Antonio de Chía** 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. Hospital San Antonio de Chía.**
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 generados.

e) El proceso Gestión de TIC debe 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.

f) El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la **E.S.E. Hospital San Antonio de Chía** cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso Gestión de Recursos Físicos y activos fijos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad posean las pólizas de seguro correspondientes.

i) El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la **E.S.E. Hospital San Antonio de Chía.**

j) 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.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la **E.S.E. Hospital San Antonio de Chía**, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al proceso Gestión de TIC.

m) Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

p) 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 por parte del responsable del activo en el momento del hecho.

6.2.6. *6.2.6 Política de uso adecuado de internet*

La **E.S.E. Hospital San Antonio de Chía** consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b) El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c) El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.

d) El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

e) El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

f) Los usuarios del servicio de Internet de la **E.S.E. Hospital San Antonio de Chía**, deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

g) 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.

h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, web-proxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

i) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

k) No está permitido el intercambio no autorizado de información de propiedad de la **E.S.E. Hospital San Antonio de Chía**, de los funcionarios, con terceros.

PRIVACIDAD Y CONFIDENCIALIDAD

6.2.7. 6.2.7 Política de *tratamiento* y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales y el

manual de políticas internas de la **E.S.E. Hospital San Antonio de Chía** 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, de manera confidencial y con los mecanismos de seguridad necesarios para impedir que terceros no autorizados tengan acceso a la misma.

Así mismo establece los términos, condiciones y finalidades para las cuales en caso de delegar a un tercero el tratamiento de datos personales, la **E.S.E. Hospital San Antonio de Chía** exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Con esto la **E.S.E Hospital San Antonio de Chía** busca proteger la privacidad de la información personal de sus usuarios y funcionarios, estableciendo los controles necesarios para preservar aquella información que 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 por ello que la **E.S.E Hospital San Antonio de Chía** adopta e implementa para el cumplimento de la presente política, el **"A*cta de confidencialidad de la información" y* *el* *"Formato de autorización de tratamiento de datos personales".***

Así mismo y con el fin de proteger la integridad y resguardo de la información tratada por medios o canales electrónicos, se establece las condiciones en las que se deberá advertir al receptor la política de confidencialidad de esa información. Para lo cual será de obligatorio cumplimento introducir en el cuerpo del mensaje electrónico "Institucional", y/o cual cualquiera que sea el medio de difusión la siguiente información al pie del mensaje.

"CONFIDENCIALIDAD: Este correo electrónico contiene información legal confidencial y privilegiada de la ESE Hospital San Antonio de Chía. Si Usted no es el destinatario a quien se desea enviar este mensaje, tendrá prohibido darlo a conocer a persona alguna, así como a reproducirlo o copiarlo. Si recibe este mensaje por error, favor de notificarlo al remitente y desecharlo de su sistema, puede notificar sus inquietudes por medio de nuestro PBX 5951230 o al correo electrónico hchia@esehospitalchia.gov.co.La ESE Hospital San Antonio de Chía no se hace responsable por la adulteración, falsificación y modificación de la información contenida por este medio."

Pautas para tener en cuenta

a) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

f) Las Unidades de Gestión de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros.

g) El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

i) 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, será responsabilidad de ellos y sujetos a las sanciones que determine la ley por la entrega de información sin las precauciones correspondientes.

6.2.8. 6.2.8- Disponibilidad del servicio e información

La **E.S.E. Hospital San Antonio de Chía** 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, ha decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

6.2.9. *6.2.9 Política de* continuidad*, contingencia y recuperación de la información*

La **E.S.E. Hospital San Antonio de Chía** 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.

6.2.10. 6.2.10 Copias de Seguridad

Toda información que pertenezca a la base de datos principal de información HIS 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 en los planes y manuales correspondientes. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

El área de las TIC de la **E.S.E. Hospital San Antonio de Chía** debe realizar pruebas controladas para asegurar que las copias de seguridad puedan ser correctamente leídas y restauradas.

El proceso y Unidades de Gestión debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. El profesional especializado con funciones de Control Interno 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 en sus equipos es responsabilidad exclusiva de dichos usuarios,

Pautas para tener en cuenta

a) El proceso Gestión de TIC, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b) El proceso Gestión de TIC , debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres

c) El proceso Gestión de TIC debe realizar los análisis de impacto al entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) El proceso Gestión de TIC debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información

e) El proceso Gestión de TIC, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

Item	Estrategia (Que se quiere lograr)	Actividades (Acciones para la ejecución del Plan)	Responsable (Quien lo debe hacer)
1			
2			

7. ANEXOS

1- Acta de Confidencialidad.
2- Autorización de tratamiento de datos
3- Política de tratamiento y protección de datos personales y confidencialidad de la información.

8. APROBACIÓN DEL DOCUMENTO		
Elaboró	**Revisó**	**Aprobó**
Firma: Nombre: Andrés Cubillos Cargo: Ing de Sistemas	Firma: Nombre: Ana Isabel Parra Cargo: Sub-Gerente Administrativo	Firma: Nombre: Rosemberg Rincón Cargo: Gerente

9. CONTROL DE CAMBIOS			
Fecha	**Versión**	**Cambio**	**Motivo**