PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA E.S.E. HOSPITAL SAGRADO CORAZON DE JESUS DE QUIMBAYA, QUINDIO

Tabla Contenido

La gerente de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío**, en uso de sus facultades Constitucionales (Art. 315-5) y legales (Ley 136 de 1994)

CONSIDERANDO

Que en el artículo 15 de la Constitución Política, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

Que la Ley 1273 de 2009 por medio del cual se modifica el Código Penal, 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 "TIC", entre otras disposiciones.

Que la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales reglamentado por el Decreto 1377 de 2013, incorporó los lineamientos necesarios para que los organismos públicos y privados identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base de datos.

Que la Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública en las instituciones del Estado, estableció los procedimientos para el ejercicio y garantías para el registro de activos de información.

Que por medio del Decreto 1078 de 2015, se expidió el Reglamento de Sector de Tecnologías de la Información y las Comunicaciones en el Artículo 2.2.9.1.2,1 de dicho decreto se instituye los componentes de la estrategia y es cuarto componente denominado Seguridad y privacidad de la Información "Comprende las acciones transversales en los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada"

Que por medio de CONPES 3854 de 2016 se fijó la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

Que conforme a la normatividad citada surge la necesidad de adoptar una política de seguridad y privacidad de la información considerando el papel estratégico de las

tecnologías de información y comunicaciones -TIC; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en la institucion, incentivando la cultura de seguridad de la información a los

Usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

Que el fundamento de una política de seguridad y privacidad de la información es buscar la gestión del conocimiento como base para la mejora continua de la misma, adaptándola a la normatividad vigente en el sector, las tendencia tecnológicas y los cambios en la gestión de procesos y procedimientos tecnológicos en la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío.**
En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°: ADOPTAR la Política de Seguridad y Privacidad de la Información en la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío**, Como Lineamiento General Para la implementación de la Estrategia de Gobierno en Línea.

ARTÍCULO 2°: REGULAR las políticas, alcances, objetivos y procedimientos relacionados con la seguridad y privacidad de la información, conforme a lo señalado en el presente Decreto.

ARTÍCULO 3°: PROPÓSITO:
Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los activos informáticos (computadores, redes de datos, software, procesos y funcionarios) de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** conectados o no a la red interna y a la información que porcese o intercambie. La protección de los activos de una amplia gama de amenazas, asegura la continuidad de la operación de los servicios y funciones, minimiza los daños de la organización, maximiza la eficiencia de la administración pública y el mejoramiento continuo, propicia aumentar la confianza de la administración local ante terceros proveedores, contratistas y ciudadanos, conoce los posibles riesgos en la seguridad de la información, reduce el tiempo de respuesta a los incidentes, y provee mejores prácticas en el aseguramiento de la información. Finalmente, apoyar y controlar el cumplimiento de los requisitos legales, reglamentarios, contractuales y técnicos que haya lugar en su aplicación.

En la actualidad la información de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. En nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.
Con la promulgación de la presente Política de Seguridad de la Información la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

ARTÍCULO 4°: DESCRIPCIÓN DE LA POLÍTICA:
La política está compuesta de un documento llamado Política General de Seguridad de La información y documentos de políticas específicas técnicas. La **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** en cumplimiento de la normatividad vigente y en consideración con la necesidad de ofrecer mejores servicios a la ciudadanía ha implementado La política de Seguridad de La información, la cual, se aplica a los actores que intervienen o utilizan activos informáticos de la intitución, entre ellos contratistas, proveedores, funcionarios de planta, agentes de entidades de control, visitantes y ciudadanos. Está política se aplica a los procesos de prestación de servicios en trámites y otros procedimientos administrativos de la institucion, y es consistente con las políticas de Actualización y publicación de contenidos, la política de protección de datos personales y demás reglamentaciones responsabilidad de la administración.

ARTÍCULO 5°: RESPONSABILIDADES
La Gerente de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la articulacion con el ya creado ***COMITE DE GERENCIA DE SISTEMAS DE INFORMACION Y GESTION TECNOLOGICA*** cuya composición y funciones se encuentran relacionadas en este documento en el artículo 21 y serán reglamentadas por una mesa de trabajo compuesta por:

- **Presidente, Gerente**
- **Secretario, Coordinador del área de sistemas**
- **Coordinacion de calidad**

- **Coordinacion Financiera**
- **Coordinacion Medica**
- **Coordinacion Estadistica**
- **Contril Interno, Invitado**

En todo caso, dicha comisión o La Mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la institución para su aprobación mediante resolución o acto jurídico correspondiente. Los jefes de area, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto ***deben*** seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por El Comite de gerencia de sistemas de informacion y gestion tecnologica y aprobados por las directivas de la E.S.E.

- El área de sistemas de información de la **E.S.E.** es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institucion. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

- El área de sistemas de información debe presentar al ***COMITE DE GERENCIA DE SISTEMAS DE INFORMACION Y GESTION TECNOLOGICA*** informes sobres los incidentes de seguridad y estado de aplicación de la Política de Seguridad de La información en la E.S.E.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de gestionar la implementación de la política de gestión y análisis de riesgos.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de gestionar la implementación de la política y/o plan de continuidad del Negocio en armonía con las disposiciones legales y avance en otras áreas de la administración local.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de la mejora continua de la política de Seguridad de la Información.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de definir y reportar cuando haya lugar la aplicación las sanciones o medidas disciplinarias en el cumplimiento de la política por parte de los actores de la institucion previa investigación y soporte de la oficina de control interno.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de disponer y vigilar la comunicación y aplicación de la política de seguridad de la información a todos los funcionarios y contratistas de la **E.S.E.**, y ciudadanos.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de brindar al área de sistemas de informacion los recursos necesarios para la implementación de la política de seguridad de la información.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de revisar y actualizar la política de seguridad de la información al menos una vez al año y dejar documentada la acción.

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es responsable de un plan de acción anual de revisión y mejora donde se incluyan al menos los responsables, recursos necesarios, mecanismos de evaluación y tiempos aplicables.

ARTÍCULO 6°: SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO
Todo el personal de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío**, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La el area de sistemas de informacion deben mantener un directorio completo y actualizado de tales perfiles.
El Comite de gerencia de sistemas de informacion y gestion tecnologica determina cuales son los atributos que deben definirse para los diferentes perfiles.
El Comite de gerencia de sistemas de informacion y gestion tecnologica debe elaborar, mantener, actualizar, mejorar y difundir el manual de “Responsabilidades Personales para la Seguridad de la Información en la **E.S.E**.
La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de area o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

6.1 Responsabilidades del personal de la ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío.

Todo el personal de la institucion, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno dellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por el area de sistemas de información, en cuanto a la información y la Red de Datos, en cuanto a los dispositivos hardware y los elementos software.

La Gerencia de la ESE Hospital Sagrado Corazon de Jesus mediante acto administrativo deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI inadecuado.

El Comité de Gerencia de Sistemas de información junto con el area de sistemas de la **E.S.E**. se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

El area de sistemas de información se encargará de tener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

6.2 Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la **ESE Hospital Sagrado Corazon de Jesus** quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI de la institución. El procedimiento para el registro de tales usuarios debe ser creado y mantenido por el area de sistemas de información. Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI de la institución.

6.3 Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información la institución http://ese-hscj.gov.co/ El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

ARTÍCULO 7°: ALCANCE DE LA POLÍTICA: La política será aplicable a todos los empleados, contratistas, proveedores, visitantes y ciudadanos de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso. Esta política se implementa a través de los siguientes anexos o políticas Específicas:

- ✓ **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
- ✓ **POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS**
- ✓ **POLÍTICA DE SEGURIDAD DE ACTIVOS INFORMÁTICOS**

- ✓ **POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO**
- ✓ **POLÍTICA DE SEGURIDAD DE CIFRADO**
- ✓ **POLÍTICA DE SEGURIDAD FISICA Y AMBIENTAL**
- ✓ **POLÍTICA DE SEGURIDAD OPERACIONAL**
- ✓ **POLÍTICA DE SEGURIDAD EN TELECOMUNICACIONES**
- ✓ **POLÍTICA DE SEGURIDAD EN ADQUICISÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**
- ✓ **POLÍTICA DE SEGURIDAD EN RELACIONES CON PROVEEDORES**
- ✓ **POLÍTICA DE SEGURIDAD EN GESTIÓN DE INCIDENTES**
- ✓ **POLÍTICA DE SEGURIDAD EN GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
- ✓ **POLÍTICA DE SEGURIDAD EN CUMPLIMIENTO**

ARTÍCULO 8°: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. ***Propósito:*** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad de los recursos informáticos en relación con la organización interna para la implementación de la política de seguridad de la información en la institución.

8.2. ***Descripción de la Política***: La política sobre organización de la seguridad de la información cubre aspectos de roles y responsabilidades, segregación de deberes, contactos y procedimiento en caso de incidentes de seguridad de la información, así como aspectos básicos para iniciar la operación y aplicación de la política.

8.3. Responsabilidades

- Las funciones del Comite de gerencia de sistemas de informacion y gestion tecnologica están contempladas en el presente manual
- Las funciones de inspección y vigilancia están a cargo de la oficina de Control Interno a través de la persona que se delegue.
- El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

8.4. Organización Interna.

8.4.1. ***Seguridad de La información Roles y Responsabilidades:*** Se deben definir y asignar las responsabilidades en relación con la seguridad de la información.

8.4.2. ***Separación de deberes:*** Durante la asignación de tareas se debe evaluar la posibilidad de conflicto de tareas o autorizaciones para que se asegure el uso autorizado y control de acceso en las tareas.

8.4.3. ***Contacto con las autoridades***: Se debe mantener contacto con las autoridades locales, regionales y nacionales para la atención de incidentes de seguridad de la información. Se puede evidenciar mediante la actualización del directorio de autoridades pertinentes.

8.4.4. ***Contacto con grupos de interés especial***: Gestionar la participación con grupos, asociaciones, o grupos especializados en la seguridad de la información.

8.5. ***Dispositivos Móviles*****.**

8.5.1. ***Política Para Dispositivos Móviles***: Se debe implementar una política y procedimientos para el tratamiento de dispositivos móviles en **la ESE Hospital Sagrado Corazon de Jesus**

8.6. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

8.7. ***Propiedad de la política*****:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

8.8 ***Sanciones***: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la institucion, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 9°: POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS

9.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad en la gestión de la protección de los recursos humanos para reducir el riesgo de fraude, robo, y mal uso de los activos informáticos de la institución.

9.2. ***Descripción y Alcance de la Política*****:**

La política de seguridad para gestión de los recursos humanos es aplicable a todo el personal vinculado directa o indirectamente a la entidad. Es decir, se extiende a funcionarios con nombramiento, contratistas, y entidades públicas o privadas con las cuales **la ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío**, tiene o presente interacción, uso o gestión de información.

Esta política debe asegurar las siguientes situaciones:

- El conocimiento de los roles y responsabilidades por parte del personal de la entidad, coherentes con las especificaciones administrativas en la gestión de manuales de funciones de la división de personal de la institución.
- La aplicación de actividades capacitación y entrenamiento para el fortalecimiento del sentido de conciencia de la seguridad de la información frente a la atención y mitigación de los riesgos y amenazas.
- Equipamiento de las mejores prácticas de los servidores públicos en la aplicación de las políticas de seguridad, privacidad y gestión de datos en el

desarrollo de las funciones y actividades cotidianas.

- Brindar las prácticas y controles que permitan especificar las responsabilidades de las personas y organizaciones cuando dejan o terminan la vinculación con la entidad.

9.3. Responsabilidades

9.3.1. El Comite de gerencia de sistemas de informacion y gestion tecnologica está encargado de laborar y actualizar la política y los procedimientos relativos a seguridad de la información.

9.3.2. El Personal de la institución es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

9.4. *Lineamientos para Antes de Asumir el Empleo*:

9.4.1. Se debe verificar los antecedentes y autenticidad de los soportes documentales entregados por los aspirantes al empleo.

9.4.2. Construir el esquema de clasificación de la información a la que se va a tener acceso por parte del empleado en el marco del perfil a suplir el cual es informado por el presonal responsable de su contrato o del supervisor del mismo.

9.4.3. Definir acuerdos de responsabilidad y compromisos de acuerdo a los requerimientos de seguridad de la información, objetivos y funciones del empleo.

9.5. *Lineamientos Durante la Ejecución Del Empleo*:

9.5.1. Responsabilidad de la Alta Gerencia: Exigir a los empleados, contratistas y terceros el cumplimiento de sus responsabilidades en la seguridad de la información.

9.5.2. Toma de Conciencia, educación, y formación en seguridad de la información: Todos los empleados, contratistas y donde sea pertinente debe desarrollarse procesos de educación, toma de conciencia y actualización de las políticas y procedimientos aplicables.

9.5.3. Proceso Disciplinario: Se debe contar con un proceso formal y comunicado para emprender acciones contra los funcionarios que hayan cometido una violación a la seguridad de la Información.

9.6. *Lineamientos de Terminación o Cambio de Empleo*:

9.6.1. Procedimiento de terminación o cambio de responsabilidades de empleo: Se debe contar con un proceso formal y comunicado para realizar la terminación o cambio de empleo de los funcionarios.

9.6.2. Terminación o cambio de responsabilidades de empleo: Se aplica la normatividad vigente para la terminación o cambio de empleo, en cuanto a la presentación de informes y procedimientos de empalme.

9.7. *Alcance de la política*: La política será aplicable a todos los empleados de la

institución.

9.8. ***Propiedad de la política*****:** La política es propiedad de la institución y del area de sistemas de información el encargado de implementar las medidas para su seguimiento e informes de cumplimiento.

9.9. ***Sanciones*****:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley, y la Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 10°: POLÍTICA DE SEGURIDAD DE ACTIVOS INFORMÁTICOS

10.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos (computadores, redes de datos, software, procesos y funcionarios) en particular la gestión de los activos por parte de los funcionarios de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío.** conectados o no a la red interna y a la información que ellos poseen y manipulan.

10.2. ***Descripción de la Política*****:** Este documento de política atiende aspectos de la seguridad de la información como Responsabilidad sobre los activos, Clasificación de la información, Manejo de los soportes de almacenamiento. Estos lineamientos permiten implementar acciones de control sobre el manejo de información, manejo de activos físicos y responsabilidades en el uso y propiedad.

10.3. ***Responsabilidades*** El Comite de gerencia de sistemas de informacion y gestion tecnologica es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.

El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, Normas, pautas, y procedimientos de seguridad a lo largo de toda la institución. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

10.4. ***Lineamientos Responsabilidad sobre los activos*****:**

- El funcionario que recibe formalmente el activo es responsable de operación, manejo y traslado.
- El funcionario es responsable de notificar o hacer que notifique oportunamente a las dependencias encargadas de atender los fallos o incidentes de seguridad sobre los activos a cargo.
- El funcionario es responsable de acuerdo a la normatividad vigente del inventario de activos e información que reposan en los activos o se deleguen

en su uso y aprovechamiento.

- La propiedad del activo informático es del funcionario a quién mediante documento de entrega del activo se registre como usuario responsable.
- Se entiende como uso aceptable de los equipos, aquellas prácticas que no ocasionen daños o mal funcionamiento de los activos. Entre ellas se puede mencionar:
    - Desconectar los equipos cuando se vayan a usar.
    - No Ingerir alimentos cerca de los activos informáticos.
    - Proteger los activos informáticos de riesgos de lluvia, golpes o sustancias peligrosas.
- Evitar Exponer los activos a posibles hurtos. Entregar, prestar o ceder los activos sin ningún registro o documento de autorización.
- Permitir a terceros la utilización de los equipos o activos informáticos sin la debida autorización.
- Utilizar los activos para actividades diferentes a las funciones o actividades contratadas.
- Solicitar los mantenimientos preventivos con oportunidad y periodicidad.
- Facilitar el acceso a activos de información sin la debida autorización.
- Los activos informáticos deben devolverse a almacén de manera formal y evitar reasignar de manera arbitraria y sin previa autorización del jefe inmediato, responsable del activo o directiva de almacén o el area de sistemas de información.

10.5. ***Lineamientos Clasificación de La información*****:**

- El funcionario es responsable de administrar los datos e información del activo informático de acuerdo al soporte del area de sistemas de información, de manera, que se especifique expresamente los datos institucionales y los datos personales.
- Realizar copias de seguridad de los datos e información personales e institucionales periódicamente o adelantar estos con el personal autorizado del area de sistemas de información.
- Cuando se haya adelantado el proceso de inducción y entrenamiento a los funcionarios de la institución en términos de las políticas de seguridad y gestión de tecnología por parte del area de sistemas de información, cada funcionario debe firmar el acuerdo de confidencialidad y responsabilidad.

10.6. *Lineamientos Manejo de los soportes de almacenamiento***:**

- El funcionario es responsable del manejo, protección de los soportes de información. Se entiende por soportes los medios físicos o electrónicos para el almacenamiento de datos e información que le hayan delegado o asignado.
- Evitar sacar de las instalaciones de la administración los medios o soportes de información sin previa autorización o registro en los documentos correspondientes.
- La eliminación de soportes físicos o electrónicos debe realizarse de acuerdo a lo establecido en las tablas de retención documental de cada área o de acuerdo a los lineamientos del Comité de Archivo de la E.S.E.

10.7. *Alcance de la política***:** La política será aplicable a todos los funcionarios de

la institución sin distinción de la forma de vinculación. Se entiende como funcionario a la persona vinculada a la institución mediante cualquier tipo o forma, en este sentido, se aplica a funcionarios de carrera administrativa, libre nombramiento, contratistas, pasantes, practicantes entre otros.

10.8. *Propiedad de la política***:** La política es propiedad de la institución y es el area de sistemas de información la encargada de implementar las medidas para su cumplimiento.

10.9. ***Sanciones*:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la institucion, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 11°: POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO

11.1. ***Propósito*:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad en relación con las directivas de control de acceso a los recursos informáticos (computadores, redes de datos, software, procesos y funcionarios) de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío.** conectados o no a la red interna y a la información que ellos poseen y manipulan.

11.2. ***Descripción de la Política*:**

La información y los equipos de cómputo como recursos necesarios y fundamentales para el desarrollo normal de las actividades institucionales y misionales de la **E.S.E.** y se requieren un marco que permita preservar y restringir de acuerdo a su importancia, por ello, es necesario establecer un conjunto de acciones para proteger los sistemas informáticos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

El presente documento emplea medidas para salvaguardar la información física y lógica, las reglas de uso de la red, uso de las estaciones de trabajo y restricciones de acceso.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias, legales e incluso el despido o terminación del contrato.

11.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica está encargado de elaborar y actualizar la política y los procedimientos relativos a

seguridad en informática y telecomunicaciones.

- El area de sistemas de información, y gerencia , son responsables de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución.
- El area de sistemas de información debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

11.4. *Lineamientos de Control de Acceso*.

11.4.1. *Política de Control de Acceso*: Se debe establecer, documentar y revisar una política de control de acceso con base en la normatividad vigente, aspectos administrativos y operacionales, y requerimientos de seguridad de la información.

11.4.2. *Acceso a redes y servicios de red*: Sólo está permitido el acceso a los recursos de red a los usuarios que efectivamente se les haya autorizado.

11.5. *Lineamientos de Gestión de Usuarios*.

11.5.1. *Registro y Cancelación de Usuarios*: Debe existir un procedimiento formal de registro y cancelación de derechos de acceso a los usuarios.

11.5.2. *Suministro de acceso de usuarios*: Debe existir un procedimiento formal para el suministro de derechos de acceso a todos los sistemas y servicios a los usuarios.

11.5.3. *Gestión de Derechos de Acceso Privilegiado*: Debe existir controles para restringir, conceder y controlarla asignación y uso con acceso privilegiado.

11.5.4. *Revisión de los Derechos de Acceso de los usuarios*: Se delega a los propietarios de los activos la revisión de los derechos de acceso de los usuarios de manera periódica.

11.5.5. *Cancelación o Ajuste de los derechos de acceso*: Los derechos de acceso de empleados, contratistas, y terceros deben cancelarse a la información, instalaciones, y servicios al momento de terminar el empleo, finalización del contrato o acuerdo, y se deben ajustar los cambios.

11.6. *Lineamientos de Responsabilidades de Usuarios*.

11.6.1. *Uso de información secreta o sensible*: Se debe exigir a los usuarios que cumplan con las prácticas reglamentadas por la ley en el uso y gestión de información de autenticación secreta.

11.7. *Lineamientos de Control de Acceso a Sistemas y aplicaciones*.

11.7.1. *Restricción de Acceso a la Información*: Se debe aplicar la política de control de acceso a las funciones e información de los sistemas de aplicaciones.

11.7.2. *Procedimiento de Conexión Segura*: De acuerdo a la política de control de Acceso se requiere la aplicación de procesos de conexión segura.

11.7.3. *Sistema de Gestión de Contraseñas*: Los sistemas de Gestión de Contraseñas deben ser interactivos y asegurar contraseñas de calidad.

11.7.4. *Uso de Programas utilitarios privilegiados*: Se debe restringir y controlar el uso de programas utilitarios que puedan tener la capacidad de anular los controles de los sistemas y aplicaciones.

11.7.5. *Control de Acceso a Códigos Fuente de Programas*: Se debe restringir el acceso a códigos fuente de programas.

11.8. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

11.9. ***Propiedad de la política*****:** La política es propiedad de la institución.

11.10. ***Sanciones*****:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 12°: POLÍTICA DE SEGURIDAD DE CIFRADO

12.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos de criptografía de la **ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío.** conectados o no a la red interna y a la información que ellos poseen y manipulan los funcionarios.

12.2. ***Descripción de la Política*****:**

Los activos que permiten implementar medidas basadas en tecnologías criptográficas son objeto de protección, uso apropiado por parte de los sistemas, aplicaciones y personas. Se entienden por recursos criptográficos a las claves de gestión de certificados, los certificados, archivos cifrados y mecanismos basados en controles de cifrados.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias, legales e incluso el despido o terminación del contrato.

12.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica está encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- El area de sistemas de información y propietarios de activos criptográficos son responsables de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de estos recursos.

12.4. ***Lineamientos sobre Controles Criptográficos*****.**

12.4.1. ***Política de Uso de Controles Criptográficos***: Se debe implementar una política de protección de los controles criptográficos de la entidad.

12.4.2. ***Gestión de Claves***: Cuando haya lugar se debe implementar una política o procedimiento que permita controlar y proteger las claves criptográficas durante su ciclo de vida.

12.5. ***Alcance de la política*****:** La política será aplicable a todos los empleados, contratistas y servicios de la institución.

12.6. ***Propiedad de la política*****:** La política es propiedad de la institución.

12.7. ***Sanciones*****:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 13°: POLÍTICA DE SEGURIDAD FISICA Y AMBIENTAL

13.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la seguridad física y ambiental de la institución.

13.2. ***Descripción de la Política*****:**

Esta política ofrece los aspectos para proteger los activos de las amenazas alrededor de los espacios físicos, condiciones de trabajo o actividad y la ejecución de las funciones de la organización. Cubre temas Como la gestión de áreas seguras, controles y seguridad física, gestión de equipos y maquinaria, y entorno de trabajo de los empleados, contratistas y terceros.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias, legales e incluso el despido o terminación de contrato.

13.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica esta encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La Dirección Administrativa (gerencia), el area de sistemas de información y control interno son los responsables de implementar y velar por el cumplimento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos y la gestión de la seguridad física y ambiental.

13.4. *Lineamientos sobre áreas seguras*.

13.4.1. *Perímetro de Seguridad Física*: Se debe especificar formalmente el perímetro de áreas seguras o que contengan información confidencial, crítica, e instalaciones de manejo de información.

13.4.2. *Controles físicos de Entrada*: la gerencia debe especificar controles de acceso físico de acuerdo a las condiciones del entorno y clasificación de la información, y asegurar que solo se permita el acceso a personal autorizado.

13.4.3. *Seguridad en oficinas, salones e instalaciones*: Se debe especificar el diseño de controles en el acceso a oficinas, salones e instalaciones.

13.4.4. *Protección contra amenazas externas y ambientales*: Se debe especificar controles que permitan la protección contra desastres naturales, ataques maliciosos o accidentes de acuerdo al diseño de control de acceso físico.

13.4.5. *Trabajo en áreas seguras*: Se debe implementar las medidas que especifiquen los mecanismos de protección de las áreas y personas de acuerdo a las actividades y análisis de riesgos técnicos, legales, ambientales y laborales.

13.4.6. *Áreas de despacho y carga*: Especificar, señalizar y controlar el acceso a áreas de despacho y carga, áreas donde se pueda dar acceso no autorizado de personas. Estos lugares deben ser bien definidos y permitir el aislamiento de las zonas de protección de la información.

13.5. *Lineamientos sobre equipos*.

13.5.1. *Ubicación y protección de los equipos*: Los equipos o activos informáticos deben ubicarse y protegerse de riesgos de amenazas ambientales, y posibilidades de acceso no autorizado.

13.5.2. *Servicios públicos de soporte*: Los equipos deben disponer de mecanismos de protección de fallas de potencia u otros tipos de interrupciones.

13.5.3. *Seguridad del cableado*: Se debe implementar mecanismos de protección de las redes de cableado de energía y telecomunicaciones, que portan datos o brindan el servicio a sistemas y servicios de la entidad. Estos deben protegerse de interceptaciones, interferencias o daños.

13.5.4. *Mantenimiento de Equipos*: Deben existir programas de mantenimiento regular para asegurar su disponibilidad e integridad.

13.5.5. *Retiro de Activos*: Los equipos, información o software no deben retirar de su sitio sin autorización previa.

13.5.6. *Seguridad de equipos y activos fuera del predio*: Se debe especificar procedimientos y controles a los activos fuera de los predios de la entidad, teniendo en cuenta los posibles riesgos.

13.5.7. *Disposición segura y reutilización*: Durante la disposición final se deben revisar si estos conservan dispositivos de almacenamiento para asegurar que datos, software o licencias sean retirados o sobre escritos de forma segura antes de su disposición o reusó.

13.5.8. *Equipos sin supervisión de los usuarios*: Los usuarios deben asegurarse que los equipos sin supervisión han sido asegurados de forma apropiada.

13.5.9. *Política de escritorio limpio y pantalla limpia*: Se debe adoptar una política de escritorio libre de papeles, dispositivos de almacenamiento removibles en los puestos de trabajo, y una política de pantalla limpia que no refleje

información en las instalaciones de procesamiento de información.

13.6. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

13.7. ***Propiedad de la política*****:** La política es propiedad de la institución.

13.8. ***Sanciones*****:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 14°: POLÍTICA DE SEGURIDAD OPERACIONAL

14.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la operación, documentación, copias de respaldo y registros de la institución.

14.2. ***Descripción de la Política*****:**

La gestión de procedimientos, responsabilidades, copias de respaldo, control de cambios, registros y documentación son temas que permiten la protección y continuidad de los servicios. Mediante esta política se fundamenta las prácticas para asegurar la operación y procesos de la E.S.E.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

14.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- El area de sistemas de información, la Dirección Administrativa (gerencia) y control interno son los responsables de implantar y velar por el cumplimento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos y activos señalados en esta política.

14.4. **Procedimientos Operacionales y Responsabilidades*.***

14.1.1. ***Procedimientos de Operación Documentadas***: Los procedimientos deben estar documentados y publicados para todos los usuarios. En particular,

para la entidad se deben documentar y disponer los procedimientos de acuerdo a los lineamientos del MECI y el SUIT. De igual manera, los procedimientos operativos de áreas de planeación y sistemas deben estar documentados y publicados.

14.1.2. ***Gestión de Cambios***: Se deben documentar y controlar los cambios en procesos y procedimientos, instalaciones, y sistemas de información.

14.1.3. ***Gestión de Capacidad***: Se debe implementar mecanismos que permitan realizar seguimiento a los recursos, cambios y ajustes, proyección de capacidad futura, desempeño y aseguramiento.

14.1.4. ***Separación de ambientes de desarrollo, ensayo y operación***: Se debe especificar y separar los entornos de desarrollo y ensayo, y operación. Se debe asegurar para evitar accesos no autorizados.

14.1.5.*Protección contra códigos maliciosos*: Se deben implementar controles de detección, prevención y recuperación. Se debe promover la conciencia apropiada entre los usuarios.

14.5. *Copias de Respaldo*.

14.5.1. ***Copias de Respaldo de La información***: Se deben hacer copias de la información, software e imágenes de sistemas periódicamente y de acuerdo al procedimiento o política de copias de seguridad.

14.6. *Registro y seguimiento*.

14.6.1. *Registros de Eventos*: Se deben elaborar, conservar y revisar los registros de eventos acerca de actividades de usuarios, fallas del sistema, excepciones, y eventos de seguridad.

14.6.2. *Protección de la Información de registro*: Se deben incorporar mecanismos de protección de los registros de eventos.

14.6.3. *Registros del administrador y operador*: Se debe aplicar los procedimientos de registro, conservación y revisión en las bitácoras de roles administrador y operador.

14.6.4. *Sincronización de relojes*: Se deben implementar mecanismos de sincronización de reloj entre los diferentes activos que prestan servicios, con referencia a una fuente de tiempo.

14.7. *Control de Software Operacional*.

14.7.1. ***Instalación de software en sistemas operativos***: Se debe disponer de procedimientos sobre la instalación de software en sistemas operativos.

14.8. Gestión de Vulnerabilidades técnicas

14.8.1. *Gestión de vulnerabilidades*: Se debe recolectar con oportunidad información sobre las vulnerabilidades de los sistemas en producción, evaluar el nivel de exposición y plantear acciones o medidas apropiadas.

14.8.2. *Restricciones sobre la instalación de software*: Se debe formalizar la instalación de software por parte de los usuarios mediante la documentación y registro de procedimientos.

14.9. *Consideraciones sobre auditorías de sistemas de información*:

14.9.1. *Controles sobre auditorías de sistemas de información*: Se debe plantear los requisitos y actividades a ejecutar en las auditorías a los sistemas en operación, de manera que armonicen con los procesos de los servicios.

14.10. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución.

14.11. ***Propiedad de la política*****:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

14.12. ***Sanciones*****:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 15°: POLÍTICA DE SEGURIDAD EN TELECOMUNICACIONES

15.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos basados en comunicaciones por redes de datos o telemáticas de la institución.

15.2. ***Descripción de la Política*****:**

En esta política se abordan las consideraciones sobre gestión de la seguridad en las redes y sistemas de telecomunicación, de igual manera, en los escenarios que permitan el intercambio o transferencia de datos con otras entidades.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

15.3. ***Responsabilidades***

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

15.4. ***Gestión de seguridad de redes*****.**

15.4.1. ***Controles de redes***: Se debe implementar mecanismos para gestionar y controlar las redes de datos para proteger los sistemas de información y aplicaciones.

15.4.2. ***Seguridad de los servicios de red***: se deben identificar mecanismos de

seguridad, niveles de servicio, y requisitos de los servicios de red. Incluir estas características en los acuerdos de nivel de servicio, ya sea que se provean internamente o por terceros.

15.4.3. ***Separación de las Redes***: Se deben implementar mecanismos que permitan la separación en grupos de usuarios, servicios de información y sistemas de información.

15.5. ***Transferencia de información*****.**

15.5.1. ***Políticas y procedimientos de transferencia de información***: Se debe especificar políticas y/o procedimientos formales para el intercambio de información que protejan el uso de todo tipo de comunicaciones.

15.5.2. ***Acuerdo sobre transferencia de información***: Los acuerdos para transferencia de información debe tratar sobre la transmisión segura de datos dentro de la organización y con otras entidades.

15.5.3. ***Mensajes electrónicos***: Se deben especificar mecanismos para la protección de los servicios de mensajería.

15.5.4. ***Acuerdos de confidencialidad o no divulgación***: Se deben especificar, documentar, revisar y actualizarlos acuerdos de confidencialidad que disponga la institucion.

15.6. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución.

15.7. ***Propiedad de la política*****:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

15.8. ***Sanciones*****: En** caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 16°: POLÍTICA DE SEGURIDAD EN ADQUICISÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

16.1. ***Propósito*****:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la adquisición y desarrollo de sistemas de información de la institución.

16.2. ***Descripción de la Política*****:**

Para la protección de los sistemas de información se incorporan actividades en los escenarios de adquisición, desarrollo y mantenimiento de los sistemas de información.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.
Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

16.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

16.4. *Adquisición, desarrollo y mantenimiento de sistemas de información*.

16.4.1. ***Análisis y especificación de Requisitos de seguridad de los sistemas de información***: en todos los proyectos de sistemas nuevos o mejoras se deben incluir requerimientos de seguridad de la información.
16.4.2. ***Seguridad de servicios de las aplicaciones en redes públicas***: Se deben incluir requerimientos que cubran la atención a posibles fraudes, divulgación, modificación o disputas contractuales en aplicaciones sobre redes públicas.
16.4.3. ***Protección de Transacciones de servicios de aplicaciones***: Se deben proteger los servicios transaccionales sobre situaciones de transmisión incompleta, enrutamiento errado, alteración no autorizada de mensajes, divulgación, duplicación o reproducción no autorizados.
16.5. ***Seguridad en los procesos de desarrollo*.**
16.5.1. ***Política de Desarrollo Seguro***: Se debe especificar los aspectos, reglas y lineamientos en los proyectos de desarrollo de software dentro de la organización.
16.5.2. ***Procedimiento de Control de Cambios***: Se debe formalizar, documentar y publicar el procedimiento de gestión de cambios de acuerdo al ciclo de vida de desarrollo de software.
16.5.3. ***Revisión técnica de aplicaciones después de cambios en la plataforma de operación***: Cuando se debe cambios en la plataforma tecnológica de operación se debe revisar la operación de las aplicaciones y servicios.
16.5.4. ***Principios de construcción de software seguro***: Se deben especificar, documentar, mantener los requerimientos de software que hagan la producción de software seguro en la organización y se deben aplicar en todos los trabajos de implementación.
16.5.5. ***Ambiente de desarrollo seguro***: Se debe implementar mecanismos de

aseguramiento de los entornos de desarrollo en todo el ciclo de vida del software.

16.5.6. ***Desarrollos contratados externamente***: Se debe supervisar y monitorizar los desarrollos contratados externamente.

16.5.7. ***Pruebas de seguridad de sistemas***: Durante el desarrollo se deben ejecutar pruebas de la seguridad de los sistemas.

16.5.8. ***Pruebas de aceptación de los sistemas***: para los sistemas nuevos, actualización o nuevas versiones se deben adelantar pruebas de aceptación en relación con el modelo de negocio y los criterios especificados.

16.6. ***Datos de Ensayo*****.**

16.6.1. ***Protección de datos de ensayo***: para la prueba de sistemas los datos deben ser seleccionados, protegidos y controlados.

16.7. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

16.8. ***Propiedad de la política*****:** La política es propiedad de la institución.

16.9. ***Sanciones*****: En** caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 17°: POLÍTICA DE SEGURIDAD EN RELACIONES CON PROVEEDORES

17.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos en relación con los temas de relación con los proveedores de la institución.

17.2. ***Descripción de la Política*****:**

Esta política plantea aspectos a considerar frente a la protección de los activos de información que pueden ser accedidos por terceros o proveedores. Cubre temas como los acuerdos, composición y prestación de los servicios y gestión de las relaciones con proveedores.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe a la gerencia que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

17.3. Responsabilidades

17.3.1. El Comite de gerencia de sistemas de informacion y gestion tecnologica es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.

17.3.2. El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos.

17.4.*Seguridad de la Información en las relaciones con los proveedores*.

17.4.1. ***Política de seguridad de la información en relaciones con los proveedores***: se debe especificar y documentar los lineamientos, riesgos y aspectos a definir en los acuerdos de acceso a la información con los proveedores.

17.4.2. ***Tratamiento de la seguridad de la información dentro de los acuerdos con proveedores***: Dentro de los acuerdos se deben especificar los requisitos de seguridad de la información con el proveedor teniendo en cuenta elementos como el acceso, proceso, almacenar, comunicar o suministrar componentes de infraestructura de TI.

17.5. *Gestión de la prestación de servicios de proveedores*.

17.5.1. ***Seguimiento y revisión de los servicios de proveedores***: Se deben programar con periodicidad el seguimiento, revisión y auditoría de los servicios prestados.

17.5.2. ***Gestión de Cambios a los servicios de los proveedores***: Se deben establecer mecanismos que apoyen la gestión de cambios de los servicios, que incluyan aspectos como mantenimiento, mejora de políticas, procedimientos, y controles de seguridad.

Teniendo en cuenta variables como los procesos de servicios, criticidad y reevaluación de riesgos.

17.6. *Alcance de la política*: La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

17.7. *Propiedad de la política*: La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

17.8. *Sanciones*: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 18°: POLÍTICA DE SEGURIDAD EN GESTIÓN DE INCIDENTES

18.1. *Propósito*: Proporcionar una serie de reglas, lineamientos y

mecanismos para garantizar disponibilidad, confidencialidad e integridad en la gestión de incidentes de seguridad de la institución.

18.2. *Descripción de la Política*:

La política de gestión de incidentes formaliza los aspectos a organizar y tener en cuenta en el tratamiento, comunicación y resolución de incidentes de seguridad que puedan originarse en **la ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío**.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

18.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- El area de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos.

18.4. Gestión de incidentes y mejora de la seguridad de la información.

18.4.1. *Responsabilidades y procedimientos*: Se debe especificar el esquema de atención de los incidentes de seguridad donde se documenten las responsabilidades y procedimientos a aplicar.

18.4.2. *Informe de eventos de seguridad de la información*: Los incidentes de seguridad deben comunicarse oportunamente mediante los canales apropiados establecidos.

18.4.3. *Informe de Debilidades de Seguridad de la información*: Se debe promover entre los recursos humanos la buena práctica de reportar las debilidades, sospechas o fallas de seguridad de la información.

18.4.4. *Evaluación de eventos de seguridad de información y decisión sobre ellos*: Los eventos deben analizarse y clasificarse si encajan como incidentes de seguridad de la información.

18.4.5. *Respuesta a incidentes de seguridad de la información*: De acuerdo a los procedimientos documentados se debe dar respuesta, y esto debe quedar registrado.

18.4.6. *Aprendizaje obtenido de los incidentes de seguridad de la*

información: Se debe documentar lo ocurrido para analizar y resolver los incidentes de seguridad, y preservar esta información para mitigar la ocurrencia futura.

18.4.7. ***Recolección de evidencia***: La entidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición, preservación de información que pueda servir como evidencia.

18.5. ***Alcance de la política*:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

18.6. ***Propiedad de la política*:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

18.7. ***Sanciones*:** En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 19°: POLÍTICA DE SEGURIDAD EN GESTIÓN DE LA CONTINUIDAD DEL SERVICIO

Propósito: **Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos en relación con los temas de gestión de la continuidad de las operaciones de la institución.**

19.1. Descripción de la Política:

La gestión de la continuidad de las operaciones de los procesos de la administración local puede cubrir desde la definición de la continuidad de la seguridad de la información y de los procesos misionales o de Servicios de la entidad hasta los aspectos de verificación y revisión de las políticas y procedimientos aplicados.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

19.2. Responsabilidades

19.2.1. El Comite de gerencia de sistemas de informacion y gestion tecnologica encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.

19.2.2. El area de sistemas de información en acompañamiento de las dependencias es responsables de los procesos de continuidad, de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los

controles sobre la protección de los recursos humanos.

***19.3. Continuidad del servicio*.**

19.3.1 Planificación de la continuidad de la seguridad de la información: La entidad debe definir los requisitos, mecanismos, reglas y lineamientos para implementar la continuidad de la seguridad de la información.

19.4.1. ***Implementación de la continuidad del negocio***: la entidad de establecer, documentar, implementar y mantener los procedimientos y controles que aseguran la continuidad de la seguridad de la información durante cualquier situación adversa.

19.4.2. ***Verificación, revisión y evaluación de la continuidad de la seguridad de la información***: Se deben establecer procedimientos para verificar que los controles de continuidad de la seguridad de la información son funcionales y responden ante situaciones desastre o siniestros.

19.4. ***Redundancia*.**

19.4.1. ***Disponibilidad de las instalaciones de procesamiento de información***: Se deben implementar instalaciones de procesamiento con redundancia suficiente para responder ante requisitos de disponibilidad.

19.5. ***Alcance de la política*:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

19.6. ***Propiedad de la política*:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

19.7. ***Sanciones*: En** caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 20°:. POLÍTICA DE SEGURIDAD DE CUMPLIMIENTO

20.1. ***Propósito*:** Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos en cuanto cumplimiento de la normatividad y compromisos documentados de la política de seguridad de la información de la institución.

20.2. ***Descripción de la Política*:**

La política de cumplimiento permite establecer los lineamientos requeridos para evitar la violación de reglas legales, estatutarias o contractuales en la implementación de la seguridad de la información o de cualquier requisito de seguridad en la administración local.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así

reducir los riesgos.
Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de la institución. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

20.3. Responsabilidades

- El Comite de gerencia de sistemas de informacion y gestion tecnologica encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- Las dependencias de la institución son responsables de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos.

20.4. *Cumplimiento de requisitos legales y contractuales*.

20.4.1. *Identificación de los requisitos legales y contractuales aplicables:* Se deben identificar, documentar, y mantener actualizados los requisitos legislativos, estatutarios, reglamentación y contractuales pertinentes para cada sistema de información o activo informático.

20.4.2. *Derechos de propiedad intelectual*: Se debe implementar procedimientos para dar cumplimiento a los requisitos legales, estatutarios, reglamentarios o contractuales relacionados con los derechos de propiedad intelectual de los recursos o productos usados en la entidad.

20.4.3. *Protección de registros*: Se debe implementar procedimientos, mecanismos y recursos necesarios para asegurar los registros contra pérdida, destrucción, fraude, acceso no autorizado; de acuerdo a los requisitos legales, estatutarios, reglamentarios y contractuales que aplique.

20.4.4. *Privacidad y protección de información identificable personalmente*: Se debe asegurar la privacidad y la protección de la información identificable personalmente; de acuerdo a los requisitos legales, estatutarios, reglamentarios y contractuales que aplique.

20.4.5. *Reglamentación de controles criptográficos*: Se debe aplicar controles criptográficos sobre todos los acuerdos o contratos en los que apliquen uso o intercambio electrónico de información.

20.5. *Revisión de la seguridad de la información*.

20.5.1. *Revisión independiente de la seguridad de la información*: Se debe revisar de forma independiente, las políticas, procedimientos, controles, objetivos y demás componentes de la seguridad de la información de la entidad, periódicamente.

20.5.2. *Cumplimiento con las políticas y normas de seguridad*: Los responsables de áreas o dependencias deben revisar con regularidad el

cumplimiento de los procedimientos y aplicación de procesos en relación con el cumplimiento con las políticas y normas de seguridad de la información.

20.5.3. ***Revisión de Cumplimiento Técnico***: Los sistemas de información se deben revisar con regularidad para verificar el cumplimiento con las normas y políticas de seguridad de la información.

20.6. ***Alcance de la política*****:** La política será aplicable a todos los empleados de la institución y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

20.7. ***Propiedad de la política*****:** La política es propiedad de la institución y es el area de sistemas de información el encargado de implementar las medidas para su cumplimiento.

20.8. ***Sanciones*****: En** caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 734 de 2002 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

ARTÍCULO 21°: FUNCIONES DEL COMITE DE GERENCIA DE SISTEMAS DE INFORMACION Y GESTION TECNOLOGICA.

El Comite de gerencia de sistemas de informacion y gestion tecnologica de **la ESE Hospital Sagrado Corazon de Jesus de Quimabaya, Quindío** tendrá dentro de sus funciones las siguientes:

21.1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la ESE Hospital Sagrado Corazon de Jesus.

21.2. Revisar los diagnósticos del estado de la seguridad de la información en la ESE Hospital Sagrado Corazon de Jesus.

21.3. Acompañar e impulsar el desarrollo de proyectos de seguridad.

19.4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la ESE Hospital Sagrado Corazon de Jesus

21.5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

21.6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

21.7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar
riesgos.

21.8. Realizar revisiones periódicas del SGSI (sistema de gestión de la seguridad de la información) por lo menos una vez al año y según los resultados de esta revisión definir las acciones pertinentes.

21.9. Promover la difusión y sensibilización de la seguridad de la información

dentro de la ESE Hospital Sagrado Corazon de Jesus.

21.10. Poner en conocimiento de la ESE Hospital Sagrado Corazon de Jesus, los documentos generados al interior del Comite de gerencia de sistemas de informacion y gestion tecnologica que impacten de manera transversal a la misma.
21.11. Las demás funciones inherentes a la naturaleza del Comité