


| | | |
|--|--|--|
| ESE HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA | |  HOSPITAL UNIVERSITARIO San Rafael <small>de Tunja</small> |
| CÓDIGO: S-M-02 | MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION | |
| VERSIÓN: 004 | | FECHA: 2022-12-23 |

TABLA DE CONTENIDO

[1. INTRODUCCIÓN Y/O JUSTIFICACIÓN](#)

[2. OBJETIVO GENERAL](#)

[3. OBJETIVOS ESPECÍFICOS](#)

[4. ALCANCE](#)

[5. MARCO LEGAL APLICABLE](#)

[6. RESPONSABLE](#)

[7. RECURSOS, MATERIALES, INSUMOS Y EQUIPOS](#)

[8. DESCRIPCIÓN/ IMPLEMENTACIÓN](#)

[9. EVALUACIÓN](#)

[10. DEFINICIONES Y/O GLOSARIO](#)

[11. DOCUMENTO SOPORTE /ANEXOS](#)

[12. SOPORTE /ANEXOS](#)

[13. BIBLIOGRAFÍA](#)

[14. CONTROL DE CAMBIOS](#)

1. INTRODUCCIÓN Y/O JUSTIFICACIÓN

La E.S.E Hospital Universitario San Rafael Tunja, es una Empresa Social del Estado líder en la prestación de servicios de salud de mediana y alta complejidad, con vocación docente, investigativa y amigable con el medio ambiente, para brindar atención integral con calidad y calidez humana, garantizando la seguridad al paciente y su familia.

La E.S.E Hospital Universitario San Rafael Tunja, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Modelo de Seguridad y Privacidad de la Información -MSPI, de acuerdo con la Política de Gobierno Digital y en concordancia con la misión y visión de la entidad.

La Seguridad de la Información, como principio de la Política de Gobierno Digital, busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

La información tiene la característica de ser uno de los activos más importantes para cualquier organización, debido a que de su tratamiento confidencial depende la rentabilidad y continuidad de su modelo de negocio, por esta razón la seguridad de la información resulta ser un factor crítico para la estabilidad de la entidad.

El manual de Seguridad de la Información de la E.S.E Hospital Universitario San Rafael Tunja, es un documento que contiene los objetivos, alcance, definiciones, la política general de seguridad y las políticas específicas, que soportan el Modelo de Seguridad y Privacidad de la Información, que orientan y apoyan la gestión y administración en materia de seguridad de la información.

2. OBJETIVO GENERAL

Establecer acorde a los lineamientos del MSPI la política general de seguridad de la información, sus dominios y el alcance, que protejan los activos de información y los datos personales a través de acciones de aseguramiento de la Información, teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad de la entidad, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo, con el fin de prevenir, proteger, administrar y resguardar los activos, teniendo en cuenta los principios de seguridad de integridad, disponibilidad,

3. OBJETIVOS ESPECÍFICOS

- Identificar los lineamientos del MSPI especificados en la Guía de la política general de seguridad y privacidad de la información y dominios de las políticas de seguridad de la información junto con los activos de información que se desean asegurar, acorde a los riesgos identificados.
- Establecer el alcance, marco normativo y lineamientos en materia de seguridad y privacidad de la información, en protección y resguardo de los activos de información en la entidad.
- Definir la política general de seguridad de la información bajo los lineamientos del MSPI, acorde a los activos, el alcance y planeación estratégica que garantice la continuidad del negocio.
- Especificar los dominios de la política general de seguridad de la información detalladamente en donde se identifique que es lo que regula la política, a quien va dirigida, las excepciones, su procedimiento y las consecuencias que acarrea el incumplimiento de estas.

4. ALCANCE

La Política General de Seguridad y Privacidad de la Información y Seguridad Digital aplica para todos los usuarios que generan, procesan, almacenan, consultan, acceden, adquieren, administran, gestionan, modifican, eliminan los activos de información que se encuentran en software, hardware, infraestructura tecnológica, infraestructura de red, infraestructura física, personal, servicios, procesos, bases de datos, Sistemas de Información o WEB y documentos físicos de la E.S.E Hospital Universitario San Rafael De Tunja, sin importar la modalidad de vinculación con la entidad, se hace extensiva a funcionarios, proveedores, personal en formación y en desarrollo de prácticas académicas, contratistas y demás terceros.

5. MARCO LEGAL APLICABLE

- **Ley 23 de 1982:** Ley de propiedad intelectual y derechos de autor.
- **Constitución Política de Colombia de 1991:** Artículo 15 consagra que “Todas las personas tienen el derecho a su intimidad personal y familiar y a su buen nombre. De igual modo, tienen el derecho a conocer, actualizar y a rectificar las informaciones que hayan recogido sobre ellas en los bancos de datos y en los archivos de las entidades públicas y privadas”.
- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000:** Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- **LEY 603 DE 2000:** Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- **Ley 962 de 2005:** Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
- **Ley 1266 de 2008,** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Resolución 1995 de 1999:** Normas para el Manejo de la Historia Clínica.
- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2578 de 2012:** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- **Decreto 2609 de 2012:** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- **Norma técnica colombiana NTC/ISO 27001:2013:** Sistema de seguridad de la Información
- **Norma ISO 27001:** Sistemas de Gestión de la Seguridad de la Información.
- **Ley 1712 DE 2014:** Ley de Transparencia y del derecho de acceso a la información pública nacional.
- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **CONPES 3854 de 2016:** Política Nacional de Seguridad Digital.
- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015. Tiene como principio la seguridad de la información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

6. RESPONSABLE

Líder de seguridad de la información o quien designe el Comité de Seguridad de la Información de la E.S.E Hospital Universitario San Rafael Tunja.

7. RECURSOS, MATERIALES, INSUMOS Y EQUIPOS

NO APLICA.

8. DESCRIPCIÓN/ IMPLEMENTACIÓN

8.1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La dirección de la E.S.E. Hospital Universitario San Rafael de Tunja, entendiendo la importancia de una adecuada gestión de La información y analizando que es un recurso que, como el resto de los activos tiene un gran valor para la entidad se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para E.S.E. Hospital Universitario San Rafael de Tunja, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Implementar el sistema de gestión de seguridad de la información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de E.S.E. Hospital Universitario San Rafael de Tunja.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de E.S.E. Hospital Universitario San Rafael de Tunja:

1. La E.S.E. Hospital Universitario San Rafael de Tunja ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
3. La E.S.E. Hospital Universitario San Rafael de Tunja protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
4. La E.S.E. Hospital Universitario San Rafael de Tunja protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La E.S.E. Hospital Universitario San Rafael de Tunja protegerá su información de las amenazas originadas por parte del personal.
6. La E.S.E. Hospital Universitario San Rafael de Tunja protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La E.S.E. Hospital Universitario San Rafael de Tunja controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La E.S.E. Hospital Universitario San Rafael de Tunja implementará control de acceso a la información, sistemas y recursos de red.
9. La E.S.E. Hospital Universitario San Rafael de Tunja garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. La E.S.E. Hospital Universitario San Rafael de Tunja garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. La E.S.E. Hospital Universitario San Rafael de Tunja garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. La E.S.E. Hospital Universitario San Rafael de Tunja garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9. ESTABLECIMIENTO DE POLITICAS ESPECIFICAS

9.1 Gestión De Activos

La E.S.E Hospital Universitario San Rafael Tunja, considera los activos de información como un valor financiero y estratégico, por lo cual esta política va enfocada en que los activos tengan una adecuada confidencialidad, integridad, disponibilidad y no repudio.

9.1.1 Identificación de los Activos

Para realizar el levantamiento o identificación de activos, lo realizará el Líder de Seguridad de la información o quien designe la Coordinación Tecnológica de Información y Comunicaciones , este proceso se actualizará al año después de haber registrado los activos en la Matriz de Activos de la Información S-F-46; pero cada área o líder de proceso es el responsable de tener identificados los activos nuevos y los de baja, los activos pueden ser identificados en los procesos, áreas, que se encuentran asignados a los usuarios, clientes, proveedores, personal en formación y en desarrollo de prácticas académicas, contratistas y demás terceros. Los activos deben estar asignados a un propietario y un custodio quienes son los responsables de ellos y velaran por salvaguardarlos.

Las actividades que se realicen sobre archivos físicos, equipos de la infraestructura informática, redes, Internet, correo electrónico, servidores, base de datos, aplicaciones, sistemas de información institucional, entre otros activos de información, propiedad de la E.S.E. Hospital Universitario San Rafael Tunja, se debe usar para el cumplimiento de las funciones o actividades asignadas dentro de la labor contratada, enmarcada dentro la misión, visión de la entidad y dentro de las normas que reglamenten.

Se debe reportar al Equipo de Seguridad y Privacidad de la Información de las fallas o incidentes que afecten la integridad, disponibilidad y confidencialidad e incidentes de seguridad sobre los activos de información.

Los activos creados o generados en cualquier proceso o área de la entidad por funcionarios, contratista, proveedores, clientes, o terceros sin importar la modalidad de vinculación con la entidad son de propiedad de la E.S.E. . Hospital Universitario San Rafael Tunja y esto queda especificado en todos los contratos. Con acuerdo de confidencialidad C-F-43.

El internet es un activo que se debe utilizar para propósitos que vayan acorde con la planeación estratégica de la entidad, el utilizarlo para actividades que impliquen el mal uso como juegos, navegación en sitios de alto riesgo, contenido pornográfico, chistes, terroristas, hackers, abrir correos que son identificados como spam o que a simple vista sean de dudosa reputación o cualquier actividad que implique que se vulneren los activos o la entidad, acarrea sanciones acorde a procedimientos establecidos de acuerdo a la sanción.

Los usuarios no podrán descargar, instalar, modificar o descompilar software ya sea de propiedad de la entidad o no, estos procesos los deben realizar el área de Coordinación Tecnológica de Información y Comunicaciones.

El respaldo y backup de los activos de información debe ser responsabilidad del jefe de área o de los procesos, así como de su gestión y administración con apoyo de las áreas de Seguridad y Privacidad de La Información o Procesos Gestión de Sistemas de Información y Comunicaciones.

Las áreas deben proponer políticas que ayuden a proteger, gestionar y administrar sus activos y estas deben ser valoradas, aprobadas y publicadas por el Comité de Seguridad de la Información.

Los usuarios y contraseñas de los equipos, sistemas de información, redes, etc de la entidad son estrictamente confidenciales, personales e intransferibles y acarrea sanciones la mala gestión de estos.

Las redes sociales de la E.S.E Hospital Universitario San Rafael Tunja, son de uso exclusivo para el uso y beneficio de la entidad, el comité de seguridad de la información designara quienes serán los responsables de la gestión de estas y cuáles serán los correos institucionales que estarán vinculados, por lo tanto, ningún usuario sin importar su tipo de vinculación podrá utilizar los correos institucionales para crear redes sociales.

La mala gestión de las redes sociales y correos electrónicos institucionales genera sanciones y el contenido publicado debe cumplir con la normatividad de derechos de autor, propiedad intelectual, habeas data, tratamiento de datos personales, así como tampoco debe ser difamatorio, ofensivo u obsceno.

El mantenimiento y reparación de activos tecnológicos se realiza mediante el procedimiento mantenimiento y reparación de Activos y lo realiza los técnicos del área de Tecnológica de Información y Comunicaciones, se registra en un formato los problemas que presenta el activo, un posible diagnóstico, lo que se realizó, fecha de ingreso y de salida, el estado en que se recibe y entrega.

Si no se identifican los activos, no se pueden reconocer cuales son las vulnerabilidades y riesgos que tiene la entidad y mucho menos cuales son los controles que se deben implementar, lo que hace que la entidad se encuentre en un estado de vulnerabilidad muy alto y puede llegar a tener pérdidas considerables, así mismo, si los propietarios no tienen una buena gestión y administración de los activos que tienen a cargo. Para asegurar la confidencialidad, integridad y disponibilidad de todos los activos, se debe generar controles que queden documentados a los cuales se les debe realizar pruebas, monitoreo para que haya una mejorar continua.

9.1.2 Clasificación de Activos

La clasificación de los activos se realiza de acuerdo con el derecho de acceso a la información (Información pública, Información Pública Clasificada, Información Pública Reservada), que generan la criticidad del activo (Alta, Media, Baja) acorde a la confidencialidad, integridad y disponibilidad. Esta clasificación se realiza para que se dé cumplimiento a la Ley 1712 de 2014 en donde se especifican los lineamientos de Transparencia y del Derecho de Acceso a la Información. El responsable o propietario del activo es quien define o asigna la clasificación y criticidad asumiendo la responsabilidad y así mismo también puede actualizarla.

9.1.3 Etiquetado de la Información

Para el etiquetado de los activos de información se define que el área de Almacén y Tecnología de Información y Comunicaciones son los responsables de este procedimiento el cual va acorde a los siguientes tipos de información y quedo establecido bajo resolución:

Hardware: El etiquetado es definido y gestionado por el área de Almacén y se encuentra aprobado por medio de resolución

Software: El etiquetado es gestionado por el área de Procesos Gestión de Sistemas de Información y Comunicaciones y se genera por medio de las licencias que se contratan con los proveedores.

Información: Esta se encuentra en documentos físicos o virtuales y su etiquetado es definido y gestionado por el área de Gestión Documental y Control de Calidad a través de las Tablas de Retención Documental (TRD).

Personas: Se identifican por medio del número de contrato ya sea funcionario, contratista, proveedor o demás modalidad de vinculación con la entidad y es definido por el área de Recursos Humanos.

Otros: Al identificar otros tipos de activos que no son muy usuales el etiquetado es definido por el área de Seguridad y Privacidad de la Información o Procesos Gestión de Sistemas de Información y Comunicaciones y debe ser aprobado por medio de resolución.

Las etiquetas de los activos no deben ser removidas, dañadas, cambiadas, modificadas porque el responsable del activo recibirá sanciones de acuerdo con la falta; pero si sufren alguna de las anteriores acciones por el uso, fenómenos naturales deberán informar a sus jefes inmediatos y posteriormente a las áreas que les asigno el activo para posteriormente realizar las respectivas modificaciones.

Los activos no deben tener etiquetas, gráficos, publicidad, información o distintivos decorativos que no pertenezca a la entidad, deben estar tal cual como se los entregaron las áreas de Almacén o Tecnología de Información y Comunicaciones.

9.1.4 Devolución de los Activos

La entidad al generar un empleo, contrato o acuerdo debe estipular en las cláusulas cuales son las normas, procedimientos, estatutos, procesos a los que se deben alinear las personas o entidades involucradas cuando inicien y finalicen el desarrollo de sus actividades en la entidad. Documentos deben incluir un formato S-F-03 Entrega de Equipos; donde se verifique las características y el estado de los activos que recibe y entrega un funcionario, contratista, proveedor, cliente o tercero sin importar su tipo de vinculación o relación con la entidad cuando finalicen un empleo, contrato o acuerdo, después de que se ejecuten los pasos de estos procedimientos la entidad procederá a realizar el último pago del saldo que deba.

Las personas o entidades que entreguen un activo en un estado malo o ya para eliminar y sin justificación coherente en donde especifique que no tuvo nada que ver con su deterioro, daño o pérdida deberá responder por el mantenimiento, reparación o adquisición de otro activo con las mismas características. Se debe realizar un procedimiento que contenga un formato en donde se registre la información necesaria si algún activo presenta un daño, modificación o pérdida total, esta situación se debe informar al jefe inmediato para que se proceda a enviarlo al área encargada de realizarle mantenimiento, diagnóstico y reparación y por ningún motivo la persona o entidad debe tratar de solucionar el inconveniente al menos que se encuentre estipulado en el contrato que tiene con la entidad.

La devolución de los activos se debe realizar porque el funcionario, cliente, contratista o tercero, finaliza, se le presenta una situación extrema, cambia de cargo, acuerdo o contrato que tenga con la entidad, esta devolución debe realizarse mediante procedimientos definidos por la entidad

en donde deben quedar incluidos en el inicio y finalización del contrato sin importar la modalidad de vinculación con la entidad.

9.1.5 Gestión de Medios Removibles

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden generar riesgos para la Entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.

La E.S.E. Hospital Universitario San Rafael de Tunja se reserva el derecho de restringir el uso de medios removibles. Mientras esté permitido es responsabilidad de los usuarios que el medio removible conectado esté libre de virus y/o código malicioso, que pueda poner en riesgo la Integridad, confidencialidad y disponibilidad de la información y de los recursos tecnológicos de la E.S.E. Hospital Universitario San Rafael de Tunja.

Los funcionarios, Proveedores, personal en formación y en formación de prácticas académicas, contratistas y demás terceros son responsables de la custodia de los dispositivos móviles y deberán cumplir con la política de seguridad y privacidad resolución 238 de 2022 en la cual se adopta las políticas de seguridad y privacidad de la información.

9.1.6 Disposición de los Activos

Para la eliminación, retiro, traslado o reúso de activos se debe generar normas y seguir los lineamientos del procedimiento Disposición de Activos acorde al área que los asigna (Almacén, Gestión Documental, Tecnología de Información y Comunicaciones) en donde a través de un formato se registra el responsable actual del activo, el estado en que este se encuentra, quien lo retira o traslada, el motivo del retiro o traslado, la fecha en que se realiza el procedimiento, etc. Se les debe realizar backups a estos activos antes de ser retirados y el área Tecnología de Información y Comunicaciones es responsable de realizar estas acciones, bajo solicitudes expedidas por la Alta Dirección, jefes de Área, Comité de Seguridad de la Información, Almacén, Tecnología de Información y Comunicaciones, etc.

En la solicitud debe estar especificado y autorizado que el área de Tecnología de Información y Comunicaciones realice también la reposición o asignación de otro activo si fue especificado, este activo mínimo debe permitir que cumpla con las mismas funciones que realizaba con el anterior activo. La instalación, configuración del activo repuesto debe realizarse en un plazo máximo de 48 horas después de haberse retirado el anterior.

10. POLÍTICAS DE CONTROL DE ACCESO

10 .1 ACCESO AL CENTRO DE CÓMPUTO, SERVIDORES Y EQUIPOS DE COMUNICACIÓN

La E.S.E Hospital Universitario San Rafael Tunja, a través del Proceso de Tecnologías de la Información y las Comunicaciones - TICS, controla el acceso al centro principal de cómputo, de servidores y comunicaciones, restringiendo esta área al personal autorizado por el Coordinador de Tecnologías de la Información y las Comunicaciones. El acceso se hará mediante equipos con tecnología biométrica.

El acceso de personal externo o distinto al área de Tecnología, que requiera ingresar deberá estar autorizado por el Coordinador de Tecnologías de la Información y en todo momento debe estar acompañado por un funcionario del mismo proceso.

El Proceso de Tecnologías de la Información y las Comunicaciones, en adelante TICS, bajo el personal encargado deberá realizar monitoreo del funcionamiento de los sistemas de control de acceso, extinción de incendios, aire acondicionado, control de temperatura y en general todos los equipos y servidores que se encuentran en del centro de cómputo principal.

El acceso del personal de Tecnologías de la Información al área de Tecnología de la información se hará mediante control de tarjeta de proximidad; el cual deberá ser concedido por el coordinador del área y retirado en caso de pérdida o por retiro del personal. En caso de extraviarse se debe reportar al coordinador inmediatamente para su desactivación y reposición.

El centro de cómputo principal y cuartos secundarios de cableado estructurado y telecomunicaciones, estarán a cargo y del proceso de Tecnologías de información y comunicaciones, los cuales tendrán medidas necesarias de seguridad, restricción de acceso y protección para estos sitios, como cuartos cerrados, medidas ambientales de temperatura, humedad, entre otras que se consideren.

El acceso de los usuarios y equipos a la red de datos de la institución se hace a través del ingreso de usuario y clave en un servidor de dominio de Windows de la Institución (Directorio Activo) que lo autentica y le permite el ingreso de la cuenta a las aplicaciones y demás recursos de la red con los privilegios otorgados.

La creación de cuentas de usuarios de dominio está a cargo del proceso de TICs. El administrador del servidor de dominio al momento de crear las cuentas debe conceder privilegios de "usuario normal del dominio" para las cuentas de las áreas que se requieren y solo los usuarios autorizados por Coordinador del área de Tecnología tendrán el privilegio de rol de supe-usuarios según el rol desempeñado.

El acceso a internet desde dispositivos móviles a personal de funcionarios, visitantes, contratistas o terceros, se podrá otorgar mediante red inalámbrica (Wi-Fi), cuando existan las condiciones técnicas y siempre que la comunicación se dé por red física o lógica diferente a la red interna de datos (Red de transmisión de información entre usuarios, equipos, servidores y aplicaciones institucionales); de manera que no se conecten a

esta red, controlando el riesgo de acceso no autorizado a través de la red.

10.2 Control De Acceso Con Usuario Y Contraseña

Los servicios e infraestructura tecnológica de la entidad, roles, perfiles y usuarios que necesitan acceso por medio de usuario y contraseñas se relacionan a continuación, así como también se encuentran relacionados detalladamente en el instructivo de roles, perfiles, usuarios y permisos en donde se especifican los accesos de cada uno.

Acceso a infraestructura tecnológica (Router, Swicht, AccesPoint): Perfil administrador redes.

Acceso a firewall: Perfil administrador seguridad.

Acceso a servidores: Perfil administrador servidores.

Acceso a Servidores virtuales: Perfil administrador servidores.

Acceso a administrador de discos: Perfil administrador servidores.

Acceso a aplicaciones: Perfil administrador aplicaciones, usuario final.

Acceso a internet: Perfil administrador servidores, usuario final.

Acceso a wifi: Perfil administrador Red, usuario final.

Acceso a Intranet: Perfil administrador Red, usuario final.

Acceso a la nube: Perfil administrador Nube, usuario final.

Acceso a office 365: Administrar de servidores y usuario final.

Acceso a Correo electrónico: Perfil administrador servidores, usuario final.

Acceso a equipos de cómputo: Perfil administrador servidores, perfil técnico, usuario final.

Acceso a dispositivos móviles: Perfil administrador servidores, perfil técnico, usuario final.

El coordinador Gestión de Sistemas de Información y Comunicaciones es quien asigna los roles a los usuarios que tienen acceso como administradores en las plataformas tecnológicas y también es el que actualiza esos usuarios y contraseñas.

Para el control de acceso a redes, aplicaciones, y/o sistemas de información, se cuenta con un formato en donde se realiza la respectiva petición donde está registrado los datos personales de quien solicita el acceso, así como cuando se le suspende o elimina de acuerdo alguna causa (finalización de contrato, cambio de equipo, penalización, mantenimiento, etc), este procedimiento especifica cómo se realizara la creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas, el responsable de ejecutar estas acciones es el área de Procesos Gestión de Sistemas de Información y Comunicaciones, así mismo este formato debe llevar la firma del jefe inmediato, firma del coordinador de Gestión de Sistemas de Información y Comunicaciones, firma de la persona que se le va a crear el usuario y contraseña, la fecha de activación, los permisos, perfiles, roles y servicios asignados, etc. Las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, es que los usuarios y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. Cada funcionario, contratista o tercero debe tener un usuario y una contraseña para el acceso y es responsable de ellos, por lo tanto, si se comete alguna acción mal intencionada contra la entidad serán sometidos a investigación y recibir las posibles sanciones si se encuentran culpables.

Los perfiles administradores de las plataformas son los responsables de crear, actualizar, suspender, eliminar los usuarios y contraseñas para los usuarios finales y técnicos. Los usuarios que tengan acceso a la nube u office 365 deben tener acceso solo desde la red de la entidad, son excepciones los usuarios que soliciten y sean aprobados para tener acceso externo de la red. Los usuarios podrán acceder a los servicios desde solo un equipo de la entidad y tendrán excepciones los usuarios que se les aprobaron el acceso desde cualquier sitio de la red.

Se debe configurar cuales son los horarios en los que no va han acceder los diferentes tipos de usuarios para que no se permita el ingreso o el inicio de sesión en los equipos y si el usuario necesita acceder porque va a trabajar horas extras debe solicitar el permiso al área de Gestión de Sistemas de Información y Comunicaciones. Acorde a lo anterior se debe realizar monitoreo y configuración de alertas de intento de inicio de sesión de los usuarios en horarios que no son permitidos, para realizar las respectivas investigaciones, sanciones y posibles vulnerabilidades que quieren aprovechar en la red o infraestructura tecnológica.

10.3 Suministro del control de acceso Y Seguridad Física En La Institución

E.S.E. Hospital Universitario San Rafael Tunja, mantiene su seguridad física a través del contrato de servicio de vigilancia y seguridad privada, dispuesta en zonas estratégicas y de acceso a la institución, tendientes a minimizar los riesgos de hurtos, robo de menores o de agresiones por parte de terceros hacia los usuarios y funcionarios, para ello debe establecer las medidas mínimas necesarias evidenciándose acciones positivas para los usuarios que se encuentren dentro de la Institución.

E.S.E. Hospital Universitario San Rafael Tunja, mantiene su seguridad a través de una Unidad de Policía en la institución las 24 horas del día.

El acceso a la E.S.E. Hospital Universitario San Rafael Tunja de funcionarios, contratistas, personal asistencial y demás colaboradores vinculados a la institución, debe realizarse únicamente por la puerta principal, vigilado por el personal de seguridad privada autorizado, los cuales deben controlar el acceso mediante la presentación del carnet institucional y el cual se debe mantener de manera visible durante el tiempo que permanezca dentro de la Institución. Ver Circular para ingreso de colaboradores por entrada principal 2016100000125-GER, INT-PR-01 ingreso de personal a la E.S.E. Hospital San Rafael Tunja.

Los requisitos para el ingreso de estudiantes o personal en formación a la institución, se debe realizar cumpliendo los protocolos de bioseguridad y las normas de reglamento estudiantil dispuestos en la circular de requisitos para el ingreso de estudiantes a la institución 2017000000365-GER.

El personal de seguridad privada debe controlar el ingreso de visitantes asignando la ficha correspondiente al área a la que se dirige, previa entrega de un documento de identificación por parte del visitante.

En el ingreso de visitantes a las oficinas administrativas, debe ser controlado, confirmando el ingreso y autorización al área respectiva. El área que recibe la visita es responsable de las actividades realizadas mientras dure la visita.

El acceso de pacientes que ingresan por el servicio de urgencias se hace de acuerdo con el procedimiento interno U-PR-02 Atención De Paciente En El Servicio De Urgencias; en todos casos debe estar controlado y vigilado por el personal de seguridad.

El personal de vigilancia debe contar con todos los elementos de dotación, identificación, protección, y comunicación que facilitan el cumplimiento de sus funciones de seguridad.

La carga y descarga de mercancías y suministros médicos de la E.S.E Hospital Universitario San Rafael Tunja, se debe realizar únicamente por las puertas asignadas de suministros médicos, almacén y sótano los cuales deben ser vigiladas por el personal de seguridad privada, para evitar el acceso no autorizado, hurto o pérdida de elementos.

El personal de guardia de seguridad debe controlar el ingreso y salida de paquetes, ingreso y salida de equipos de cómputo y demás elementos que salen de la institución con la debida autorización, realizando el registro del elemento en el libro respectivo.

El Circuito Cerrado de Televisión (CCTV) es un mecanismo de apoyo al procedimiento de seguridad de la institución y debe ser monitoreado por el personal de seguridad privada de manera permanente, en las áreas de accesos, pasillos, áreas de concurrencia de la institución y demás lugares dónde se encuentre las cámaras de seguridad del Circuito.

Los Circuitos Cerrados de Televisión dispuestos dentro de las Unidades de Cuidados Intensivo y dentro de otros servicios como el Archivo, serán monitoreados por el personal respectivo asistencial o administrativo autorizado por el Coordinador de la unidad o del área. Cada coordinador definirá la frecuencia, forma, responsable (s) de acuerdo con las condiciones propias de cada servicio.

La Gerencia de la E.S.E. Hospital Universitario San Rafael Tunja, es la única autorizada de realizar entrega de material de grabaciones y certificaciones de imágenes grabadas dentro de la institución, en aquellos casos en que se requiera como prueba dentro de un proceso adelantado por autoridad civil, penal, fiscal o disciplinaria.

El ingreso de visitantes y acompañantes de pacientes a la institución es permitido en los horarios establecidos por la oficina de Atención al Usuario en la guía informativa de horarios de visitas. El personal de seguridad debe orientar a los usuarios visitantes, sobre la ubicación del área a visitar.

El ingreso de vehículos a parqueaderos se debe controlar por el personal de guardia de seguridad de acuerdo con las condiciones, horarios y autorización propias para cada vehículo, establecidas por la gerencia de la Entidad. El personal de vigilancia debe realizar rondas preventivas brindándole seguridad a las instalaciones y a los usuarios.

Todo paciente al retirarse de la institución debe presentar en la portería la boleta de paz y salvo para verificar los datos personales y retirar la manilla que lo identifica como paciente.

El personal de vigilancia y seguridad privada debe tener en cuenta lo descrito en el procedimiento INT-PR-01 Control De Ingreso De Visitantes. Para controlar el ingreso y egreso de visitantes, el ingreso de funcionarios de fuerzas Públicas y Militares (POLICIA, EJERCITO, INPEC) en servicio a La E.S.E. Hospital Universitario San Rafael Tunja.

El personal de vigilancia y seguridad privada debe mantener registro de los incidentes de seguridad o novedad presentada en la institución.

Ante cualquier incidente de seguridad física llamar al personal de vigilancia a la extensión 2101 o cualquier unidad de apoyo de seguridad privada dispuesto en la portería principal, urgencias, consulta externa, parqueaderos, neonatos y ginecología, psiquiatría y demás lugares de rondas o dispuestos por la entidad.

10.4 Creación De Cuenta Y Acceso A Sistemas De Información

La creación de cuentas de usuario en los sistemas de información o plataformas informáticas de la Entidad debe ser notificado y autorizado por el área de Talento Humano y el Coordinador de Proceso al que pertenece dicho usuario, al proceso o área de Tecnologías de la Información y Comunicación -TICs encargada de crear la cuenta, mediante correo electrónico; especificando las aplicaciones, permisos y roles (perfil de usuario requerido). Los administradores de creación de cuenta previo a la creación de la cuenta deben validar si es requerida o no capacitación del usuario en el sistema o módulo del sistema solicitado, antes de conceder datos de acceso.

Las credenciales asignadas (usuario y clave) de acceso a los sistemas de información, servidores, equipos o plataformas informáticas, deben ser asignadas de manera individual y cada usuario deberá mantenerla de manera confidencial y queda prohibido divulgarla o prestarla; el usuario es responsable por el acceso, modificación o registro que se haga en las plataformas asignadas con dichas credenciales. En caso de otorgar claves de manera genéricas en la mejora del proceso de asignación, estas deberán ser notificadas para ser cambiadas por el usuario de manera inmediata.

Para conceder acceso al sistema de Información de Historia Clínica y su componente administrativo de Servinte, Sistema de Gestión documental, Sistema Daruma Salud, Nómina, Imágenes diagnósticas, Sistema de laboratorio, el personal debe contar con la capacitación requerida antes de conceder datos de acceso.

Para conceder la consulta de documentos, permisos de acceso y roles a los diferentes sistemas de información se hará de acuerdo las funciones a realizar en el mismo. Estos privilegios vienen establecidos en algunos sistemas de información y en otros se crea el perfil o rol antes de asignarlos. El proceso de TICS y/o líderes de sistemas de información serán los que otorguen o dicten los privilegios.

Solo usuarios autorizados deberán autenticarse mediante los mecanismos de control de acceso provistos en los sistemas de información institucionales, servidores o mecanismos de tecnologías de la Información y las Comunicaciones - TICS, antes de usar la infraestructura tecnológica del hospital o consultar información en dichas plataformas. Queda prohibido el ingreso a la infraestructura tecnológica y sistemas de información del hospital sin ser autorizado.

Cualquier cambio en los privilegios, permisos, roles o perfiles de los usuarios en los sistemas de información, deberán ser solicitados al coordinador del proceso al que pertenece y éste a su vez solicitarlos a través de correo electrónico al personal encargado del proceso de TICS de otorgar o modificar dichos privilegios; de tal forma que tenga conocimiento de los cambios solicitados.

Cuando un usuario olvide su contraseña o bloquee su usuario, deberá notificarlo al personal encargado del proceso de TICS, quienes se encargarán de desbloquear o renovar dichas credenciales.

Cuando el usuario se retire de la institución o no utilice más el sistema en el cual se encuentra registrado, el usuario debe ser deshabilitado de manera inmediata por los administradores del sistema, previa comunicación del mismo usuario, del líder del proceso al que pertenece el usuario, legalización de la paz y salvo o del área de Talento Humano.

Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio y/o dejarlos en un lugar donde personas no autorizadas puedan encontrarlos.

En los sistemas de información donde se pueda controlar la vigencia de la contraseña, esta tendrá una vigencia de sesenta (60) días, finalizando este periodo deberá cambiarla de acuerdo con las características de seguridad mencionadas anteriormente, para los sistemas que no tiene control de vigencia de la clave, el mismo usuario deberá cambiarlas en el mismo periodo.

Los usuarios deberán observar los siguientes lineamientos para la construcción de sus Contraseñas:

1. Deben contener caracteres especiales, números y letras mayúsculas y minúsculas.
2. Deben ser difíciles de adivinar, esto quiere decir que las contraseñas no deben relacionarse con datos de la vida personal del usuario.
3. No deben utilizarse contraseñas que usa en otras cuentas, o que ya hayan sido usadas anteriormente.

Queda prohibido el acceso y conexión de equipos de cómputo o de comunicaciones que NO son de la entidad a la red de datos interna del Hospital, sin autorización del Coordinador Tecnologías de la Información y con previa solicitud escrita y justificada del solicitante.

10.5 Dispositivos Móviles

Los dispositivos móviles que son de la entidad deben estar registrados y a cargo del área de Almacén o en el área Procesos Gestión de Sistemas de Información y Comunicaciones, donde se debe llevar un historial de cada uno.

Para la asignación o préstamo de dispositivos móviles de la entidad a funcionarios, contratistas o terceros se genera en el formato S-F-03 Entrega de Equipos, en el cual queda registrado mediante un formato las características del activo, los datos de la persona a la cual se le realiza el préstamo, el tiempo máximo del préstamo, la multa o sanción por daño, pérdida o no devolución del activo, firmas de los involucrados y si deja algún objeto (Cedula, carnet) como garantía. Cuando se realice la devolución en este mismo formato de debe especificar la fecha de entrega, el estado del dispositivo y si dejó algún objeto realizar su respectiva devolución. Todas las áreas también tienen asignados activos que utilizan normalmente en sus procesos, para el préstamo de estos también se debe utilizar el mismo procedimiento y cada área es responsable de estos.

Para el ingreso y salida de dispositivos móviles externos de la entidad se genera un documento donde quede estipulado que la entidad no se hace responsable por pérdida o daños de este.

La entidad determina a los funcionarios, contratistas o terceros que tienen acceso a las redes inalámbricas, chats corporativos y/o correos electrónicos de la entidad mediante el uso de dispositivos móviles, adicionalmente se describe las responsabilidades que tienen los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información, los

responsables de instalar y configurar estos servicios son el área de Gestión de Sistemas de Información y Comunicaciones.

El área de Gestión Documental y Talento Humano, diseñaron lineamientos para la administración de los archivos de acuerdo con lo establecido en la normatividad de Tablas de Retención. Para los documentos físicos o virtuales se generan las Tablas de Retención Documental (TRD) donde se indica el tipo de clasificación de las series, subseries y documentos.

10.6 Políticas De Seguridad En Comunicaciones

El área de comunicaciones de la entidad es el área autorizada para entregar información oficial a los medios de comunicación a través de los medios informativos dispuestos por la entidad, con el aval de la Gerencia o su delegado. Otras comunicaciones del hospital que se trasmitan a los medios a través de entrevistas o comunicados de prensa, radio y televisión, por otros funcionarios de la institución, también deben estar autorizados y delegados por la Gerencia de la entidad apoyados en la oficina de Comunicaciones.

En el proceso de comunicación tener en cuenta lo descrito en los procedimientos y manuales internos:

CO-PO-01 Políticas de operaciones de comunicaciones.

CO-PR-01 Comunicación interna.

CO-PR-03 Comunicación Externa Para Programa de Radio y Televisión

CO-PR-06 Divulgación de información de comunicado de prensa.

CO-PR-07 Divulgación de información a través de boletín de prensa.

CO-PR-05 Producción piezas comunicativas y Publicitarias.

CO-M-01 Manual de uso medios de comunicación.

- El único proceso autorizado para la toma de fotos, grabaciones y videos en la institución es la oficina de comunicaciones de la entidad, en el caso de requerir toma de fotografías o videos de pacientes o usuarios, esta área debe diligenciar autorización a través de consentimiento informado por el titular de derechos y/o por cada una de las personas que aparezcan en la toma y avalado previamente por la Gerencia o Asesor de Desarrollo de Servicios y/o por alguien con autoridad designado por la Gerencia.

La sentencia de Tutela T-233 de 2007 indica la obligación de solicitar autorización al titular de derechos respecto del cual se pretenda obtener una grabación, registro fotográfico o cualquier otro medio fílmico, bajo la esfera del derecho a la intimidad previsto en el artículo 15 de la Constitución Política de Colombia.

- Se prohíbe a todos los funcionarios, personal médico y asistencial en formación, contratistas, pacientes, terceros o acompañantes que ingresen o presten sus servicios a la E.S.E. Hospital Universitario San Rafael Tunja la toma de fotos y registros en video al interior de la entidad, sin la autorización del proceso de comunicaciones y/o área TIC, avalado previamente por la Gerencia o Asesor de Desarrollo de Servicios y/o por alguien con autoridad designado por la Gerencia.

La transgresión de derechos por el incorrecto manejo de información, así como de los medios que se utilizan para la obtención de esta están contemplados en los artículos 189 a 191 de la ley 599 de 2000 (Código Penal).

- El envío masivo de mensajes informativos institucionales, solo se deberá realizar a través de la cuenta de correo electrónico comunicaciones@hospital-sanrafael-tunja.gov.co, perteneciente al área de Comunicaciones de la institución y única autorizada para tal fin; con previa aprobación por parte de la gerencia de la institución y/o a solicitud del área interesada, diligenciado el formato respectivo con código CO-F-02 Solicitud de piezas comunicativas y Publicitarias. Como contingencia ante el no acceso a la cuenta de correo oficial y ante la eventual necesidad de comunicación importante por parte de la entidad, se autoriza la cuenta esehospital-sanrafael-tunja@gmail.com, operada también por la oficina de Comunicaciones.

10.7 Políticas De Tratamiento Y Protección De Datos Personales

La E.S.E. Hospital Universitario San Rafael Tunja, cuenta con la política de protección de datos personales, adoptada en la resolución interna 078 de 2017 de acuerdo con lo dispuesto en la ley 1581 de 2012, así:

En la E.S.E. Hospital Universitario San Rafael Tunja somos respetuosos de los datos personales de los titulares, y buscamos informar de manera suficiente a las personas sobre los derechos que tienen en su calidad de titulares de la información, como es el de conocer, actualizar y rectificar o suprimir sus datos personales frente a la entidad en su condición de responsable del tratamiento y en los términos de ley. Así mismo el hospital velará por el uso adecuado del tratamiento al cual serán sometidos los datos personales y finalidad de estos de todos sus usuarios, niños, niñas y/o adolescentes, enmarcados siempre dentro del cumplimiento de la misión institucional como prestador de servicios de salud, y demás funciones administrativas, constitucionales y legales de la Entidad.

La E.S.E Hospital Universitario San Rafael Tunja, como responsable del tratamiento de datos personales de sus titulares y en cumplimiento a lo señalado en la Ley Estatutaria 1581 de 2012, reglamentada por el decreto 1377 de 2013, informa que previamente a la expedición de la normatividad mencionada, ha recolectado datos personales de los titulares, imprescindibles para el cumplimiento de la misión institucional como Prestador de Servicios de Salud, y demás funciones administrativas, constitucionales y legales de la Entidad.

El personal que realice tratamiento de datos personales debe conocer y conducirse por las disposiciones previstas en la ley 1581 del 2012 y demás normas que la reglamentan y la política adoptada por la entidad; entendiéndose por tratamiento, cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

10.7.1 Responsables Del Tratamiento:

La E.S.E. Hospital Universitario San Rafael Tunja, actuará como responsable del tratamiento de datos personales; y las distintas dependencias tanto asistenciales como administrativas, actuarán como encargados del tratamiento y protección de datos personales, cuando por cualquier motivo posea o reciba, o realice tratamiento de información personal de cualquier ciudadano.

La Oficina de tecnologías de Información -TICs es el responsable de la administración de los datos personales que reposan en las diferentes bases de datos que tenga a cargo; y también estará atenta para resolver peticiones, consultas, reclamos por parte de los titulares, actualización, rectificación y supresión de datos personales, de las solicitudes que se reciban a través de los distintos canales dispuestos por la entidad para tal fin.

De acuerdo con la ley de tratamiento y protección de datos personales; el personal administrativo y clínico que labora en el hospital y que haga uso o tratamiento de datos personales deberá conducirse de acuerdo con las normas o leyes establecidas para este fin.

10.7.2 Autorización para el Tratamiento de Datos Personales

La autorización del titular de la información debe ser suministrada de forma expresa y de manera previa al tratamiento; toda vez que el titular debe estar plenamente informado de los efectos de su autorización.

Para garantizar lo anterior, cuando a través de cualquier operación que incorporen información de personas naturales a las bases de datos de la E.S.E. Hospital Universitario San Rafael de Tunja, se pondrá a disposición del titular un documento de autorización para el tratamiento de datos personales (físico o electrónico), el cual deberá contener como mínimo el tratamiento al cual serán sometidos y la finalidad de este; de no contar con la autorización previa y expresa del titular de la información, HUSRT deberá abstenerse de realizar tratamiento a la misma, con excepción de los siguientes eventos en los cuales no será necesaria la autorización:

1. Llevar a cabo medidas necesarias para la ejecución de un contrato que se haya celebrado con el titular.
2. Enviar información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
3. Realizar tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
4. Realizar tratamiento de datos de naturaleza pública, o aquellos relacionados con el registro civil de las personas.

10.7.3 Tratamiento y Finalidades

Los datos personales en poder de la E.S.E. Hospital Universitario San Rafael de Tunja, serán requeridos para recolectar, recaudar, transferir, almacenar, usar, circular, suprimir, procesar, compartir, actualizar, intercambiar y disponer conforme a las siguientes finalidades de carácter general:

1. Para la prestación de los servicios asistenciales a sus pacientes y familias.
2. Para la gestión administrativa de la atención en salud.
3. Para comunicar información sobre servicios de salud, actividades, eventos académicos y empresariales, publicaciones, publicidad asociada a la salud, boletines de prensa, innovación empresarial, mensajes de protocolo, tarjetas de navidad e informes de gestión.
4. Para promocionar otros canales digitales como sitios web, blogs, redes sociales y videos de los canales de E.S.E. Hospital Universitario San Rafael de Tunja "En el San Rafa Se trabaja con el Alma".
5. Para el cumplimiento de las obligaciones legales y las exigencias de las entidades que regulan y vigilan el Sector Salud y demás autoridades competentes.
6. Para el cumplimiento de las obligaciones derivadas de las relaciones contractuales y comerciales existentes.
7. Para conocer de manera prospectiva las necesidades de sus grupos de interés con el fin de innovar en la prestación de sus servicios.
8. Para el diligenciamiento de encuestas, formularios y evaluación de indicadores de oportunidad y calidad de los servicios.
9. Para fines investigativos, científicos, formativos y educativos.
10. Para la seguridad de pacientes, colaboradores, visitantes, terceros y demás personas que ingresen a las instalaciones de la E.S.E. Hospital Universitario San Rafael de Tunja.
11. Para fines de eficiencia, seguridad y tecnología.
12. Realizar transacciones económicas en el portal web.
13. Para la actualización de datos entregados por el Titular.

Además de las finalidades generales, existen finalidades particulares, atendiendo a la relación que tienen los titulares de los datos personales con la , como a continuación se describen:

a. Finalidades especiales para el tratamiento de los datos de pacientes y sus familias:

1. Obtener datos fundamentales para la investigación clínica y epidemiológica.
2. Enviar resultados de exámenes diagnósticos.
3. Lograr comunicación relacionada con nuestros servicios, a través de diferentes medios.
4. Brindar información sobre campañas y programas especiales, mercadeo, promoción de servicios y educación al usuario.
5. Realizar encuesta de satisfacción de servicios y atenciones prestadas.
6. Contestación, gestión y seguimiento a solicitudes de mejoramiento, peticiones, quejas, sugerencias y reclamos.
7. Caracterización y seguimiento a la población, para la gestión del riesgo en salud, utilizando la información derivada de los servicios

asistenciales.

b. Finalidades especiales para el tratamiento de los datos personales de empleados:

1. Realización de publicaciones internas y externa.
2. Apertura de acceso a plataformas tecnológicas propias de la organización.
3. Brindar información a empresas que solicitan verificar datos laborales de los empleados.
4. Comunicar jornadas de capacitación y mejoramiento continuo.
5. Informar procesos de selección y promoción interna.
6. Establecer una relación contractual.
7. Evaluaciones de desempeño, satisfacción laboral, nómina, crecimiento personal, bienestar, seguridad y salud en el trabajo.
8. Cumplir con el proceso de afiliación al Sistema General de Seguridad Social Integral.
9. Emitir certificaciones relativas a su condición de empleado, tales como certificados de ingresos y retenciones, constancias laborales, entre otros.

c. Finalidades especiales para el tratamiento de los datos personales de proveedores, clientes, contratistas, convenios y alianzas:

1. Evaluación de bienes y servicios prestados por las partes.
2. Seguimiento y gestión de la relación contractual.
3. Reportes y reclamaciones a las compañías aseguradoras en los casos que aplique.
4. Las demás que sean propias de la celebración, ejecución, evolución, terminación y liquidación de la relación contractual.

10.7.4 Derechos y Deberes

10.7.1 Derechos del Titular de Datos Personales

De conformidad con lo dispuesto en el artículo 8 de la Ley 1581 de 2012, el titular de los datos personales tiene los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales.
2. Solicitar prueba de la autorización otorgada al responsable del tratamiento de la información.
3. Ser informado por la E.S.E. Hospital Universitario San Rafael de Tunja, previa solicitud, respecto del uso que se les ha dado a sus datos personales.
4. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012, una vez haya agotado el trámite de consulta o reclamo ante la E.S.E. Hospital Universitario San Rafael de Tunja, como responsable del tratamiento.
5. 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.
6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

10.7.2 Derechos de los Niños, Niñas y Adolescentes

En el tratamiento de datos personales a cargo de la E.S.E. Hospital Universitario San Rafael de Tunja se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes, por tanto, queda proscrito el tratamiento de datos personales de estos, salvo aquellos datos que sean de naturaleza pública y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos.

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente, otorgará la autorización a la E.S.E. Hospital Universitario San Rafael de Tunja, previo ejercicio del menor de su derecho a ser escuchado, a la información y a la libertad de expresión; opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

10.7.3 Legitimados para el ejercicio de los derechos del titular

Los Derechos antes mencionados y consagrados en las diferentes disposiciones normativas sobre la protección de datos personales, podrán ser ejercidos por las siguientes personas:

1. El titular, acreditando su identidad.
2. Los causahabientes del titular, quienes deberán acreditar tal calidad.
3. El representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro o para otro.

Los Derechos de los niños, niñas y adolescentes serán ejercidos por quienes estén facultados para representarlos.

10.7.4 Deberes del responsable y/o Encargado del Tratamiento

En los procesos organizacionales de la E.S.E. Hospital Universitario San Rafael de Tunja, somos conscientes que los datos personales son propiedad de las personas naturales a las que se refieren y que sólo ellas pueden decidir sobre los mismos. En este sentido, se hará uso de ellos sólo en aquellas finalidades para las que se encuentra debidamente facultado en la autorización obtenida al momento de adquirir el dato, y respetando en todo momento los mandatos Constitucionales, la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Así las cosas, la E.S.E. Hospital Universitario San Rafael de Tunja, se compromete a cumplir en forma permanente con los deberes consagrados en el artículo 17 de la Ley 1581 de 2012, respecto a la protección de datos personales.

1. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de Hábeas Data.
2. Solicitar y conservar, copia de la respectiva autorización otorgada por el titular.
3. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información que se suministre sea veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar la información, comunicando todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
7. Rectificar la información cuando sea incorrecta y comunicarla.
8. Suministrar al encargado, únicamente datos cuyo tratamiento esté previamente autorizado.
9. Exigir al encargado del tratamiento en todo momento respeto a las condiciones de seguridad y privacidad de la información del titular.
10. Tramitar las consultas y reclamos formulados.
11. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
12. Informar a solicitud del titular sobre el uso dado a sus datos.
13. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

10.7.5 El Ejercicio de los Derechos del Titular

Los titulares de la información podrán, en cualquier momento, ejercer los derechos consagrados en la Ley 1581 de 2012 de conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada para el tratamiento, informarse sobre el uso que se ha dado a los datos, revocar la autorización y solicitar la supresión de sus datos cuando sea procedente.

Para el ejercicio de estos derechos, el titular de la información podrá acudir a los siguientes canales de comunicación de la E.S.E. Hospital Universitario San Rafael de Tunja:

Documento escrito: Dirigido a la Oficina Jurídica, en la carrera 11 No 27 - 27 Tunja.

El titular del dato y/o interesado en ejercer uno de estos derechos, acreditará esta condición mediante comunicación escrita (Física o digital), anexando copia de su documento de identidad. En caso de que el titular este representado por un tercero deberá allegarse el respectivo poder, el apoderado deberá igualmente acreditar su identidad en los términos indicados.

En la solicitud para ejercer su derecho de Habeas Data, se deberá suministrar con precisión y veracidad los datos de contacto (dirección física, teléfono, correo electrónico, etc.) para efectos de dar respuesta y atender su solicitud; indicando el nombre e identificación del titular y de sus representantes, de ser el caso y la petición concreta y precisa de información, acceso, actualización, rectificación, cancelación, oposición al tratamiento y/o revocatoria del consentimiento.

La E.S.E. Hospital Universitario San Rafael de Tunja documentará y almacenará las solicitudes realizadas por los titulares de los datos o por los interesados en ejercicio de cualquiera de los derechos, así como las respuestas a tales solicitudes.

10.7.6 Consultas de Base de Datos

Los titulares de los datos personales o sus legitimados podrán consultar la información personal que repose en cualquier base de datos de la E.S.E. Hospital Universitario San Rafael de Tunja, en consecuencia, el responsable del tratamiento suministrará a estos toda la información contenida en los registros o que esté vinculada con la identificación del titular.

La consulta será atendida a través de los diferentes medios físicos o electrónicos habilitados para ello. En cualquier caso, la E.S.E. Hospital Universitario San Rafael de Tunja dará respuesta en un término máximo de diez (10) días hábiles, contados a partir de la fecha de su recibo.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

La E.S.E. Hospital Universitario San Rafael de Tunja, en cumplimiento de su deber de información en relación con el tratamiento de datos personales comunica de forma debida a las personas que tengan interés en registrarse en nuestras bases de datos y en el portal Web que el suministro de los datos personales solicitados es de entera responsabilidad de sus titulares, razón por la cual estos deben ser veraces y fidedignos.

Este acto propio y voluntario de cada persona exime de cualquier responsabilidad a La E.S.E. Hospital Universitario San Rafael de Tunja, por la calidad de estos; por lo cual, se asume de buena fe que la información personal suministrada que es provista por el titular del dato está actualizada, es exacta, veraz y fidedigna.

La persona que use datos personales que no sean propios será responsable de las sanciones que la ley colombiana establece en relación con la violación de datos personales.

10.7.7 Medidas de Seguridad

En el tratamiento de los datos personales, la E.S.E. Hospital Universitario San Rafael de Tunja, adoptará medidas de seguridad físicas, lógicas y administrativas, conforme el riesgo que pueda derivar el acceso a los datos personales tratados, adoptando un procedimiento interno sobre estas medidas, que serán de obligatorio acatamiento.

10.7.8 Uso de Imágenes y Video

En la E.S.E. Hospital Universitario San Rafael de Tunja, informa sobre la existencia de mecanismos de seguridad adoptados mediante la difusión en sitios visibles de anuncios de video vigilancia. De acuerdo con lo anterior, se cuenta con un sistema de video vigilancia instalado en diferentes sitios al interior de sus instalaciones y oficinas, la cual es utilizada para fines de seguridad como derechos de cada uno de los pacientes, acompañantes, empleados y cualquier otra persona natural.

La E.S.E. Hospital Universitario San Rafael de Tunja, manifiesta que la información recolectada se utilizará para fines de seguridad de los pacientes, acompañantes empleados, y cualquier persona natural, así como de los bienes e instalaciones. Esta información podrá ser empleada como prueba ante cualquier autoridad u organización. Solo si se tiene conocimiento de una novedad se realiza backups a este registro para tenerlo como prueba ante una instancia judicial.

10.7.9 Entrega De Datos Personales A Autoridades

Cuando las autoridades o administrativas en ejercicio de sus funciones legales o judiciales soliciten a la E.S.E. Hospital Universitario San Rafael de Tunja, el acceso y/o entrega de datos de carácter personal contenidos en cualquiera de sus bases de datos, se hará la entrega de la información, previa verificación de la legalidad de la petición y la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad.

10.7.9.1 Datos del responsable

El responsable del tratamiento de la información personal registrada en nuestras bases de datos es la E.S.E. Hospital Universitario San Rafael de Tunja, quienes se identifican con los siguientes datos:

- Nombre o Razón Social: E.S.E. Hospital Universitario San Rafael de Tunja
- Nit: 891.800.231-0
- Domicilio: Tunja- Boyaca
- Dirección: Cra. 11 No. 25 - 25
- Correo electrónico: info@hospitalsanrafaeltunja.gov.co
- juridicanotificaciones@hospitalsanrafaeltunja.gov.co
- Teléfono: (608) 7405050

10.7.10 Propiedad Intelectual

Los contenidos del sitio web son propiedad de la E.S.E. Hospital Universitario San Rafael de Tunja ó están autorizados por los autores intelectuales de dichos contenidos o tendrán que estar referenciados ya sea el contenido o de donde se haya sacado la información publicada.

- Los contenidos del sitio web que sean de autoría ajena la E.S.E. Hospital Universitario San Rafael de Tunja estarán protegidos por las leyes colombianas en materia de derechos de autor, también por las normas internacionales de Copyright.
- El no cumplimiento en las políticas de privacidad, en las condiciones de uso y propiedad intelectual puede acarrear acciones desde la restricción al sitio web, hasta acciones disciplinarias o legales dado el caso.

10.7.11 Derechos Que Le Asisten Al Titular De La Información:

El titular de los datos personales tiene derecho a conocer, actualizar y rectificar sus datos personales frente a La E.S.E. Hospital Universitario San Rafael Tunja, en su condición de responsable del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido, o no haya sido autorizado.

10.7.11.1 Canales Para Atención Para Datos De Historia Clínica

- Envío de correo electrónico a: estadistica@hospitalsanrafaeltunja.gov.co,
- Oficio impreso radicado en ventanilla de la entidad,
- Presencial en las ventanillas disponibles de Atención al usuario.
- Actualización y rectificación de nombres e identificación de Historia Clínica las áreas de Archivo de Historia clínicas serán las encargadas de realizar las modificaciones, según los horarios de cada área.
- Horario: de 8am a 12m y 2pm a 5pm

10.7.11.2 Canales De Atención Para Otras Bases De Datos

- Envío de correo electrónico a: estadistica@hospitalsanrafaeltunja.gov.co,

- Oficio impreso radicado en ventanilla de la entidad,
- Presencial en las ventanillas disponibles de Atención al usuario.
- Presencial en las ventanillas disponibles de Atención al usuario.
- La actualización o rectificación de datos estará a cargo del área de Tecnologías de la Información y comunicaciones.
- Horario: de 8:00 am a 12:00m y 2:00pm a 5:00pm

10.7.12 El Tratamiento Al Cual Serán Sometidos Los Datos Y La Finalidad Del Mismo

Tratamiento: Los datos personales proporcionados a La E.S.E. Hospital Universitario San Rafael Tunja por los diferentes canales de atención dispuestos por la entidad y a través de los sistemas de información institucionales, de pacientes, estudiantes, trabajadores, contratistas, y demás usuarios, serán objeto de tratamiento de recolección, almacenamiento, uso, actualización, rectificación, circulación o supresión, según lo amerite cada caso, bajo el cumplimiento de las demás funciones administrativas, constitucionales y legales de la Entidad.

Finalidad: Los datos personales, dispuestos en las bases de datos de La E.S.E. Hospital San Rafael Tunja, serán usados para la finalidad específica para la que fueron suministrados, enmarcados dentro del cumplimiento de la misión institucional como prestador de servicios de salud y en el cumplimiento de las demás funciones administrativas, constitucionales y legales de la Entidad.

10.7.13 Acceder o Consultar La Política De Tratamiento De Información

Los titulares pueden acceder o consultar en cualquier momento la política de tratamiento y protección de datos personales a través del enlace ubicado en el pie de la página web de la institución.

Para más información acerca de la política de tratamiento y protección de datos personales, consultar en resolución interna 078 de 2017 de acuerdo con lo dispuesto en la ley 1581 de 2012.

10.8 Políticas De Privacidad Y Confidencialidad De La Información

La E.S.E. Hospital Universitario San Rafael Tunja a través de funcionarios, personal médico y asistencial, en formación, contratista, y demás vinculados a la Entidad, mantendrán la debida reserva y protegerán en todo momento los documentos e información que esté a su cargo o cuidado; y en especial aquellos que incluyan información personal, confidencial, sensible y de reserva legal.

La Historia Clínica (Min-Salud Resolución 1995 DE 1999), es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

Se prohíbe a los funcionarios, personal médico, personal en formación contratista o vinculado a la entidad, suministrar información registrada de los sistemas de información, ya sea verbal, escrita, impresa o por medios electrónicos, sin previa autorización del Coordinador del proceso y en respuesta expedida por la Gerencia de la Entidad a solicitudes formales de información de acuerdo con los procedimientos o trámites administrativos, constitucionales o de ley.

La información de la E.S.E. Hospital Universitario San Rafael Tunja NO se debe tratar en lugares públicos ni en presencia de terceros. Sin embargo, se reconoce que en casos excepcionales se tengan que discutir en dichos lugares o con personas ajenas a la entidad.

En atención a lineamiento del grupo de trabajo de Gobierno en digital, estrategia de cero papel, se establece que la papelería de re uso que contiene información de datos personales de los pacientes como, nombres y apellidos, números de celular, identificación o diagnósticos o cualquier otra que identifique o relacione a los pacientes y demás personas, se debe ocultar o rayar para poder reusar el papel sin ningún inconveniente. En el caso que estos documentos contengan este tipo de información y no se puedan reutilizar el papel, se deben rasgar y depositar en la caneca destinada a reciclaje de papel.

10.9 Acuerdos De Confidencialidad De La Información

De conformidad con lo establecido en la Ley 1581 de 2012, ley de Protección y uso de datos personales y en la resolución interna 078 de 2017, políticas de protección de datos personales y la presente política de seguridad de la información, el personal como: funcionarios, personal en formación, contratistas y/o terceros, y demás personal que presten sus servicios en la E.S.E. Hospital Universitario San Rafael Tunja, deberán aceptar y firmar los acuerdos de confidencialidad, con ocasión a sus funciones o labores asignadas y al realizar operaciones de tratamiento sobre datos personales y otras informaciones, tales como recolección, almacenamiento, uso, registro, modificación, consulta, circulación o supresión, de los datos almacenados en los archivos físicos, archivos digitales, sistemas de información o bases de datos institucionales; y se compromete a mantener la confidencialidad o no divulgación de la información por ningún medio electrónico, verbal, impresa, ni total, ni parcialmente, sin contar con previa autorización.

La coordinación de Talento Humano debe velar por que los funcionarios y demás colaboradores vinculados a la entidad por las diferentes modalidades de contratación o vinculación, formalicen el acuerdo de confidencialidad de la información antes del inicio de su labor.

Para el personal de planta en la institución el formato a diligenciar para el acuerdo es el [\(TH-F-51\) Carta De Confidencialidad Manejo De La Información](#).

La Coordinación de Contratación de la Entidad, debe incluir en las minutas de los contratistas, cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes a la confidencialidad y privacidad de la información, [\(C-F-43\) Acuerdo De Confidencialidad De La Información](#); con el fin de reducir el riesgo de robo, fraude, mal uso, fuga de información en el tratamiento que se haga sobre la misma y trasmisión por cualquier medio.

Todo funcionario o contratista que termine su relación contractual con el hospital debe hacer entrega formal de la información que haya recibido o generado a raíz del objeto contratado o de su gestión con E.S.E. Hospital Universitario San Rafael Tunja.

10.10 Clasificación De La Información Confidencial Y De Reserva Legal

La E.S.E. Hospital Universitario San Rafael Tunja con el fin de resguardar la información privilegiada y de reserva legal ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Los líderes de las áreas de la E.S.E. Hospital Universitario San Rafael Tunja, son los responsables de identificar y asociar el nivel de clasificación de la información que maneja a su cargo, teniendo en cuenta los criterios, niveles de clasificación y reserva legal, para ser actualizados por el Área de Gestión documental. Para más información que se encuentran detallados en el manual CÓDIGO: GD-M-02 Manual De Administración De Información Privilegiada Y De Reserva Legal.

Los niveles de clasificación de la información de la E.S.E Hospital Universitario San Rafael Tunja, definidos en el manual son:

| Nombre del inventario de información | Área | Información confidencial | Reserva Legal | Soporte Jurídico |
|--------------------------------------|-----------------------------|--------------------------|---------------|---|
| Informes de jurídica | Jurídica | X | | Información confidencial |
| Derechos de petición | Jurídica | X | | Información confidencial |
| Tutelas | Jurídica | x | | Información confidencial |
| Procesos Jurídicos | Jurídica | X | | Información confidencial |
| Procesos Disciplinarios | Jurídica | X | | Información confidencial |
| Información de Historia Clínica | Archivo de Historia Clínica | X | X | La Ley 23 de 1981 y la resolución del MINSALUD de 1995 del 1999, establecen como carácter de reservado a la historia clínica. |
| Información Contable | Contabilidad | X | X | Ley 43 de 1990 art 63 y 64, 65, 67 Por la cual se reglamenta el ejercicio del contador público y contempla el carácter de reserva de la información que maneja. |
| Historia laboral del personal | Recursos Humano | X | x | Ley 1437 de 2011, artículo 24 |
| Hojas de vida | Recursos Humano | X | X | Ley 1437 de 2011, artículo 24 |
| expedientes pensionales | Recursos Humano | X | X | Ley 1437 de 2011, artículo 24 |
| Quejas | SIAU | X | | Información confidencial |
| | | | | |

| | | | | |
|---|-------------------|---|--|--|
| Notificaciones a entes de control de la infancia y adolescencia | Trabajo Social | X | | Ley 1712 de 2014, artículo 19 |
| Informes de aptitud ocupacional | Salud Ocupacional | X | | Decreto 1443 de 2014, Resolución 1918 de 2009 - MiniSalud, Sentencia T-161 de 1993 |

11. POLÍTICAS DE DERECHOS DE AUTOR DE LA E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL TUNJA

La E.S.E. Hospital Universitario San Rafael Tunja, protege los derechos de autor de la entidad en los desarrollos especializados, profesionales, tecnológicos y técnicos en las áreas administrativas y asistenciales de la institución, que se desarrollen durante y como fruto de las funciones del contrato y serán de propiedad de la institución, dado que hay remuneración o retribución convenida en el desarrollo intelectual, manual, operativo, creativo entre otros; Teniendo en cuenta la Política de derechos de autor de la Entidad adoptada bajo la resolución Interna 245 de 2017, la ley de derechos de autor y la circular 07 de 2012 del Ministerio del Interior y de Justicia que se pronunció en los siguientes términos: *“Los derechos de autor sobre las obras creadas por empleados o funcionarios públicos, en cumplimiento de las obligaciones constitucionales y legales de su cargo, serán de propiedad de la entidad pública correspondiente. Se exceptúan de esta disposición las lecciones o conferencias de los profesores. Los derechos morales serán ejercidos por los autores, en cuanto su ejercicio no sea incompatible con los derechos y obligaciones de las entidades públicas afectadas”*.

Se exceptúan del acceso a la información los secretos comerciales, industriales, profesionales, según el artículo 18, literal c de la ley 1712 de 2014.

12. POLÍTICAS DE RECURSOS TECNOLÓGICOS

12.1 Políticas De Uso De Internet

Los funcionarios, personal en formación y contratistas de La E.S.E. Hospital Universitario San Rafael Tunja, que tengan acceso a internet deberá hacer uso eficiente de este recurso y NO utilizarlo para realizar prácticas ilícitas, ver páginas con contenidos pornográficos, malintencionados, de manera ociosa, o sitios que se detecten como peligrosos, tampoco para descargar y/o almacenar en los computadores de la institución, archivos o programas, imágenes, videos, juegos, películas y música, entre otros; ya que pueden violar las normas de derechos de autor y descargar contenidos o programas malintencionados que pueden dañar la información del equipo.

El acceso a internet de la entidad deberá estar controlado a través de mecanismos o equipos de seguridad informática por el área de TICS y adicional al canal principal, contar con un canal secundario redundante, como contingencia ante caídas de internet.

El área de TICS, podrá monitorear el uso de internet, implementar políticas para conceder permisos a sitios web requeridos según necesidad de grupos de usuarios; restringir el acceso a otros sitios que puedan saturar la red de datos, páginas con contenidos dañinos, entre otros que puedan afectar la seguridad de los sistemas de información.

No está permitido el intercambio de información institucional de la E.S.E. Hospital Universitario San Rafael Tunja, de sus clientes, usuarios, contratistas, o funcionarios, con sitios web externos; a menos que se trate de reportes de información obligados de ley, intercambio entre servidores externos que hacen parte de la plataforma tecnología del Hospital, reporte de casos referentes a los sistemas de información o intercambio con otros centros de salud o diagnóstico por telemedicina.

El personal de funcionarios, contratistas y/o terceros, personal en formación y demás vinculados a la institución, no pueden asumir en nombre de la E.S.E. Hospital Universitario San Rafael Tunja posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

12.2 Políticas De Uso De Correo Electrónico

El correo electrónico institucional es una herramienta de intercambio de información oficial y apoyo a labor realizada en la institución, deberá ser consultada, usada y gestionada de manera periódica, eficiente y responsable por los usuarios a cargo, dentro de las labores asignadas.

La apertura de cuentas institucionales de correo electrónico estará a cargo del proceso de Tecnologías de la Información y comunicaciones -TICS, de acuerdo con solicitud previa del coordinador del área que la requiera. El nombre de la cuenta debe relacionarse con la actividad o labor que se indique y bajo el dominio de la entidad, determinando el tamaño del buzón de acuerdo con las necesidades de la cuenta.

El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo bajo el dominio@hospitalsanrafaeltunja.gov.co y cumpliendo con las normas para el uso del correo electrónico institucional de la E.S.E. Hospital Universitario San Rafael Tunja, establecidas mediante Circular No. 201610000635-GER, de la Institución. De igual manera, las cuentas de correo personal o bajo otros dominios, no se deben emplear para el envío de mensajes o labores institucionales.

La información oficial de la institución que requiera ser enviada por correo electrónico en archivos adjuntos, debe enviarse con membrete y en formatos institucionales y preferiblemente en formatos no editables. La información puede ser enviada en el formato original bajo la responsabilidad del remitente y únicamente cuando el receptor justifique hacer modificaciones autorizadas a dicha información.

El envío masivo de mensajes informativos institucionales, solo se deberá realizar a través de la cuenta de correo electrónico comunicaciones@hospitalsanrafaeltunja.gov.co, perteneciente al área de Comunicaciones de la institución y única autorizada para tal fin.

Cuando se requiera el envío de documentos entre las áreas del Hospital, se debe preferir el uso de envío de correo electrónico al envío de documentos físicos, para dar cumplimiento a la estrategia de cero papel y eficiencia administrativa, siempre que el trámite o procedimiento administrativo o ley lo permita.

Tener precaución al enviar archivos adjuntos que excedan 5MB y a su vez enviado a varios contactos, ya que pueden saturar los correos institucionales e intentar reducir peso y/o enviarlos con compresión.

Todos los mensajes enviados deben respetar el estándar de formato e imagen Institucional definido por la E.S.E. Hospital Universitario San Rafael Tunja y conservar en todos los casos el mensaje corporativo de confidencialidad y cumplir con la siguiente estructura, de acuerdo Circular No. 201610000635-GER, así:

Nombre del funcionario

Cargo

ESE Hospital San Rafael Tunja
PBX. (57) Teléfono y Extensión Correspondiente
Carrera 11 No 27-27 Tunja- Boyacá Colombia
Correo electrónico institucional
www.hospitalsanrafaeltunja.gov.co
www.hospitalsanrafaeltunja.gov.co



"Ahorre agua, recicle los desechos en bolsas independientes, y antes de imprimir un documento, reflexione si es necesario hacerlo, de ello depende el futuro de nuestros hijos. Preservar el medio ambiente es responsabilidad de todos"

La información contenida en este correo electrónico y en todos sus archivos anexos, es confidencial y/o privilegiada y sólo puede ser utilizada por la(s) persona(s) a la(s) cual(es) está dirigida. Si usted no es el destinatario autorizado, cualquier modificación, retención, difusión, distribución o copia total o parcial de este mensaje y/o de la información contenida en el mismo y/o en sus archivos anexos está prohibida. Si por error recibe este mensaje, le ofrezco disculpas, sírvase borrarlo de inmediato, notificarle de su error a la persona que lo envió y abstenerse de divulgar su contenido y anexos.

Con el fin de mejorar la organización del correo electrónico, los usuarios de correos deberán organizar sus mensajes por años y carpetas, de acuerdo al tema. Si se reciben correos no deseados o Spam, se deberán marcar como tal en el correo y luego proceder a eliminarlos.

Si se llega a recibir algún correo de las características de spam o de manera masiva que resulte desconocido, dudoso, no esperado, y/o con archivos adjuntos desconocidos; no reenviarlo, ni descargar o ejecutar dichos archivos y reportarlo inmediatamente al área de Soporte de Tecnologías de la Información, para que puedan proceder a su revisión, análisis y posible eliminación, ya que podrían poner en riesgo la información del equipo o daño en el computador.

Está prohibido enviar o reenviar correos con mensajes con contenido religioso, político, racista, sexista, solidaridad, ventas, bromas, publicitarios, difamatorios, no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad, la moral y vida de las personas, que atenten contra el normal desempeño del servicio de correo electrónico, mensajes mal intencionados que puedan afectar otros sistemas de terceros, mensajes que vayan en contra de las leyes o mensajes que promuevan actividades ilegales.

Cuando se requiera el uso de correo electrónico institucional en dispositivos móviles personales, este acceso debe ser autorizado por el Coordinador de Tecnología de la Información y Comunicaciones, llenando el formato de control respectivo, por el personal encargado de otorgar el acceso y retirarlo en caso de retiro formal de la personal de la institución a solicitud del usuario.

El usuario que tiene asignada una cuenta de correo electrónico es responsable de todas las acciones y mensajes que se lleven a cabo en su nombre y en nombre de la institución. La ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales; reglamenta la validez jurídica e implicaciones en el uso del correo electrónico como mensaje de datos.

Queda prohibido enviar información institucional a destinatarios externos o fuera de la entidad, en mensajes de correo electrónico, sin previa validación del Coordinador o líder del proceso o de superior inmediato, salvo aquellos mensajes autorizados y que se hacen de manera periódica y como parte de labor o gestión diaria con otras entidades, siempre y cuando no ponga en riesgo jurídico a la entidad.

Se prohíbe utilizar las cuentas de correo electrónico institucional, como punto de contacto con comunidades interactivas de contacto o redes sociales, tales como Facebook, Twitter, Instagram, entre otras. Solo la cuenta institucional autorizada del área de comunicaciones podrá hacerlo.

12.3 Políticas De Recursos Tecnológicos Informáticos

La E.S.E. Hospital Universitario San Rafael Tunja, busca hacer uso eficiente de los recursos de Tecnologías de la Información y Comunicaciones, manteniéndolos operativos, en buen estado y como apoyo a la gestión en el cumplimiento de las funciones laborales, contratadas y/o autorizadas al personal clínico y administrativo de la entidad, para el normal desempeño y funcionamiento de las áreas y continuidad a las operaciones de la Entidad.

12.4 Uso Y Mantenimiento Y Protección De Equipos.

Los equipos de la infraestructura tecnológica se deben incluir dentro del programa de renovación tecnológica, modernización de infraestructura, dotación y mantenimiento Hospitalario, según resolución interna 304 de 2016. Tener en cuenta la resolución, el procedimiento MAN-PR-06 Plan De Mantenimiento Hospitalario y el manual S-M-00 Manual De Priorización De La Información Y Las Comunicaciones, los equipos de cómputo de la

entidad deben contar con software de protección como antivirus actualizado, para prevenir propagación de aplicaciones mal intencionado, como virus, robo o pérdida de información, entre otros.

En cuanto a la operación de los computadores, en esta sección se describen algunas buenas prácticas, más, sin embargo, tener en cuenta lo descrito en el manual S-M-05 “Manual De Normas Y Buen Uso De Computadores”.

Cuando los equipos de la infraestructura informática de la entidad requieran de revisión y/o mantenimiento o se evidencien fallas que afecten el funcionamiento de estos o posibles amenazas de aplicaciones mal intencionadas, como virus, entre otros; se debe informar o reportar al área de Tecnologías de la Información y Comunicaciones -TICs, para que realicen el diagnóstico y mantenimiento respectivo. El correo para reportar es sistemas@hospitalsanrafeltunja.gov.co, o a la extensión 2226. El personal técnico tendrá en cuenta el S-F-04 Mantenimiento Preventivo De Software Hardware, y S-F-05 Mantenimiento Preventivo De Software, y la utilización de la plataforma de GLPI (<http://192.168.10.111/glpi/front/ticket.php>); Permite la creación y/o actualización de tickets vía correo electrónico para realizar las solicitudes de necesidades tecnológicas que se requiera en la institución con el cual se realiza seguimiento a cada uno de los casos que se ingresen a la plataforma.

Todos los equipos que hacen parte de la infraestructura tecnológica de la E.S.E. Hospital Universitario San Rafael Tunja tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información, deben ser ubicados, protegidos y usados adecuadamente para prevenir la pérdida, daño, robo, fuego, agua, polvo, vandalismo, humo, evitando el consumo o bebida de alimentos cerca de los mismos, previniendo acceso no autorizado de los mismos, entre otros que atenten contra la integridad de los mismos.

Está prohibido que los usuarios, instalen o desinstalen software, que desatapen y realicen conexiones internas en los computadores, que realicen conexiones de red con equipos ajenos a la institución o no autorizadas, o realicen modificaciones que afecten el funcionamiento del sistema en el equipo de cómputo. El personal técnico de Tecnologías de la Información y las Comunicaciones - TICs es el área la encargada de realizar dichas acciones y de velar por que las conexiones de red y software instalado cuente con la autorización y el licenciamiento respectivo.

La instalación, actualización, modificación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E. Hospital Universitario San Rafael Tunja es responsabilidad del personal avalado por el proceso Tecnologías de Información y Comunicaciones -TICs, y por tanto son los únicos autorizados para realizar esta labor.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros.

Independientemente de la asignación individual de los equipos realizada por el Hospital, todos los funcionarios deben velar por la seguridad y protección de los equipos dentro y fuera de las instalaciones, y no dejar los equipos desatendidos con el personal en visita. Los equipos portátiles deben ser transportados con cuidado y llevado como equipaje de mano.

Queda prohibido en los computadores de la entidad, el almacenamiento, circulación y visualización de archivos en cualquier formato cuyo contenido sea de obsceno, racista, difamatorio, entre otros, que resulten ofensivos y/o que pudieran perjudicar la imagen institucional o de sus funcionarios. Tampoco está permitido guardar en los computadores archivos de música, videos, películas, fotos, a menos que sean archivos institucionales y que no sean violatorios de los derechos de autor.

Los usuarios deben bloquear la sesión del equipo en la que se encuentran, cuando vayan a retirarse temporalmente en su lugar de trabajo, con el fin de evitar que otro usuario acceda o modifique su información. Cuando se retire por más de una hora o al finalizar la jornada deberán apagarlo, excepto aquellos equipos que funcionan como acceso y soporte remoto de manera continua.

La E.S.E. Hospital Universitario San Rafael Tunja, a través del área de Mantenimiento, provee y mantiene fuentes de energía eléctrica alterna como son la planta eléctrica que da una autonomía hasta de 70 horas y sistemas de alimentación no interrumpida (UPS) en los pisos con autonomía de 10 minutos a plena carga, como medida de protección eléctrica para los equipos y de manera que se pueda continuar operando ante una caída del suministro eléctrico. En caso de que no se restablezca la energía de planta eléctrica en un término de 10 minutos el área de mantenimiento debe informar a las áreas para que realicen apagado adecuado de los equipos y servidores donde se alojan los sistemas de información; evitando así el daño en los equipos, la pérdida o corrupción de información. Estos equipos deben ser revisados periódicamente por Mantenimiento, para asegurar su funcionamiento y condiciones normales de operación.

Queda prohibido que los usuarios de la aplicación Servinte Clinical Suite guarden información en los servidores de aplicaciones a los que se conectan remotamente. Debe guardar la información en sus equipos locales, pues al realizar mantenimiento a los servidores, la información podrá ser borrada sin previo aviso.

Al realizar transacciones bancarias en la entidad, se debe ingresar o escribir la dirección web del portal bancario directamente en los navegadores y no hacerlo a través de los buscadores como google, mensajes de texto o correos electrónicos; es recomendable también que los equipos destinados a este propósito se instalen las aplicaciones de protección proporcionados por el portal bancario y se registren las direcciones IP fijas ante los bancos a los que se accede. Lo anterior para evitar la práctica de Phishing, método utilizado por delinquentes cibernéticos para realizar estafas. El área de Tecnología de la Información apoyará la revisión o actualización.

12.5 Criptografía

Las conexiones remotas como teletrabajo, telemedicina, conexiones con proveedores o funcionarios del Hospital para operaciones de diagnóstico, mantenimiento, operación de infraestructura, actualización o revisión de los casos reportados sobre los sistemas de información o plataformas tecnológicas del Hospital, deben ser realizadas con medidas de seguridad a través de conexión por redes privadas virtuales (VPN) o bajo conexiones con protocolos que brinden seguridad y encriptación en las transmisiones de datos. Las conexiones remotas con personal ajeno a la entidad deben estar supervisadas por personal del área de Tecnologías de la Información o quien se designe por el Coordinador de esta área.

Queda prohibido el acceso y conexión de equipos de cómputo o de comunicaciones que NO son de la entidad a la red de datos interna del Hospital, sin autorización del Coordinador Tecnologías de la Información y con previa solicitud escrita y justificada del solicitante

El área de Tecnologías de la información establece los lineamientos para los controles criptográficos teniendo en cuenta lo siguiente:

Se deberán utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la información digital o electrónica reservada y clasificada.
- Deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada o restringida cuente con mecanismos de cifrado de datos.
- Deberá desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos.
- Deberá utilizar controles criptográficos para la transmisión de información clasificada, fuera del ámbito de la E.S.E. Hospital Universitario San Rafael de Tunja.
- El área de Tecnologías de Información y Comunicaciones -TICs se asegurarán que los controles criptográficos de los sistemas utilizados cumplan con los estándares establecidos para garantizar cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

12.6 Uso De Software Legal.

El personal técnico de Tecnologías de la Información debe realizar instalaciones de software con los medios proporcionados, licenciados por el Hospital y autorizados por el Coordinador de Tecnologías de la Información y Comunicaciones -TICs; El personal técnico de Tecnologías de la Información debe realizar revisiones del software instalado en los equipos al momento de realizar mantenimiento a los equipos y reportar cualquier novedad o hallazgo encontrado de software no licenciado, archivos de música, entre otros que infrinjan la ley de derechos de autor. Para descripción de novedades, tener en cuenta el S-F-05 Mantenimiento Preventivo De Software y reportar el incidente.

Queda prohibido suministrar o copiar software proporcionado o licenciado por el Hospital a terceros o usarlo para fines personales y/o en equipos ajenos de la Entidad.

12.8 Traslado, Baja, Daño O Pérdida De Equipos.

El traslado o reposición por daño de equipo informático, deberá contar con el aval del líder del proceso con previa autorización de la oficina de TICS del hospital y posteriormente notificarlo al área del almacén para actualización de inventario.

La E.S.E. Hospital Universitario San Rafael Tunja, a través del área de Almacén y suministros, dispone equipos para la baja, se deberá realizar de acuerdo con el procedimiento de Baja de Activos Fijos A-PR-03 y el Formato A-F-03 Formato De Activos Fijos Para Dar De Bajas.

La E.S.E. Hospital Universitario San Rafael Tunja cuenta con un seguro de protección contra daño, pérdida o robo para los equipos de cómputo, entre otros. En caso de pérdida o robo de un equipo de la E.S.E. Hospital Universitario San Rafael Tunja, se deberá informar inmediatamente al área de Almacén, para que se inicie el trámite interno.

El personal de Técnico de la oficina de Tecnología, en el momento de entregar equipos de cómputo autorizados por baja al área de Almacén debe identificar los dispositivos de almacenamiento y con herramientas de software destruir la información del disco duro respectivo, para evitar fuga de información.

En caso de daño de equipos de la entidad o pérdida de información en los mismos; debe reportarse a la Coordinación de área encargada para su procedimiento respectivo y al área de Tecnologías de Información para la evaluación técnica del daño, llenando el formato F-54

Reporte De Daño De Dotación Hospitalaria

12.9 Uso De Computadores Personales

Dictar lineamientos y recomendaciones para el uso de equipos personales al servicio de HUSRT.

Lineamientos Generales:

- Todo equipo de cómputo y/o dispositivo móvil que sea personal, pero sea usado para las labores institucionales, deberá estar registrado con número de serial ante la oficina TIC del HUSRT, diligenciando los formatos correspondientes.
- Todo equipo de cómputo y/o dispositivo móvil que sea personal, pero sea usado para las labores institucionales, deberá registrar su ingreso y egreso a la salida de la institución.
- Al conectar el equipo de cómputo y/o dispositivo móvil a la red de la E.S.E. Hospital Universitario San Rafael Tunja, este se adhiere a las políticas de red y demás descritas en este documento, (Manual de Políticas).
- Los mantenimientos preventivos y correctivos de los equipos de cómputo y/o dispositivos móviles personales serán responsabilidad del dueño de estos, La E.S.E. Hospital Universitario San Rafael Tunja no se hará responsable por daños causados en el uso interno o externo a la institución.
- Toda información que se trate en los equipos de cómputo y/o dispositivos móviles personales deberá ser almacenada únicamente en los medios autorizados por La E.S.E. Hospital Universitario San Rafael Tunja, no se podrá almacenar información en los equipos o dispositivos móviles personales que no se encuentren registrados.
- Notificar a la oficina TIC, cualquier sospecha de malware o situación que pueda afectar a la seguridad de la información y/o de las herramientas digitales, equipos suministrados por el HUSRT.
- Cuando el colaborador se desvincule de La E.S.E. Hospital Universitario San Rafael Tunja deberá entregar toda información relevante e importante propia de la institución, se deberá verificar junto con el área TIC, que en el equipo de cómputo y/o dispositivo móvil no existe información relacionada con la entidad, en caso contrario se deberá realizar un backups y realizar un borrado seguro de la información.
- En caso de robo o pérdida del equipo de cómputo y/o dispositivo móvil, y éste contenga información de la institución, se deberá reportar inmediatamente a la oficina TIC la situación, aclarando la información contenida.
- En caso de requerir una conexión remota, se debe solicitar al área TIC la previa configuración autorización.

Recomendaciones

- Conectar el equipo de cómputo y/o dispositivo móvil a redes conocidas y privadas evitando el uso de redes Wi-Fi públicas bajo toda circunstancia. Cuando sea posible, utilizar una red móvil confiable dentro y fuera de las instalaciones de La E.S.E. Hospital Universitario San Rafael Tunja.
- Proteger mediante contraseña segura los equipos de cómputo y/o dispositivo móvil.
- Hacer uso de antivirus en los equipos de cómputo y/o móvil.
- Realizar mantenimiento preventivo y correctivo del equipo de cómputo y/o móvil personal, teniendo cuidado de proteger la información de la entidad.
- Atender a la política de escritorio limpio, así como bloquear o suspender el equipo y/o dispositivo móvil, mientras no se encuentre en su lugar de trabajo.

13. POLÍTICAS SEGURIDAD DEL RECURSO HUMANO

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Talento Humano, debe propender por la sensibilización y concientización sobre la responsabilidad en el cumplimiento de las políticas de seguridad de la información de la Institución, con el fin de reducir el riesgo de robo, fraude, mal uso de los medios y la información contenida en ellos, asegurando la confidencialidad, disponibilidad e integridad de la información.

La Coordinación de Talento Humano y la Coordinación de Tecnologías, definirán y desarrollarán un programa de sensibilización y concientización de las políticas de seguridad de la información al personal vinculado a la institución, para desarrollar una cultura en seguridad de la información dentro del Hospital.

La Subgerencia Administrativa y Financiera, Subgerencia de Servicios de Salud y la Oficina Asesora de Desarrollo de Servicios, serán las encargadas de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos del personal, contratista y/o tercero según los lineamientos establecidos en la E.S.E Hospital Universitario San Rafael Tunja.

El área de Talento Humano será la encargada de diseñar, documentar y actualizar el manual específico de funciones y requisitos por competencias laborales, para los empleos que conforman la planta global de personal de la E.S.E. Hospital Universitario San Rafael Tunja, donde se detallan los roles, las responsabilidades, funciones o actividades a ser ejecutadas en el S-M-15 Manual Estrategia TI.

Todo el personal contratado por la E.S.E. Hospital San Rafael Tunja debe ser seleccionado de forma que cumpla los requisitos descritos en el FORMATO CÓDIGO: TH-F-45 VERIFICACIÓN REQUISITOS HOJA DE VIDA Y HABILITACIÓN, FORMATO CÓDIGO: A-F-06 FORMATO INSCRIPCIÓN KARDEX DE PROVEEDORES, FORMATO CÓDIGO. TH-F-51 ACUERDO DE CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN, de acuerdo con los requerimientos de cada cargo y por las leyes de la República de Colombia y lo dispuesto en el código sustantivo del trabajo.

En caso de que el proceso de selección o la contratación se realice por intermedio de terceros, la E.S.E. Hospital Universitario San Rafael Tunja, debe asegurar la definición clara de las responsabilidades y los mecanismos para manejar el incumplimiento de los requisitos. Sin importar el método de contratación, todo funcionario recibe y acepta el acuerdo de confidencialidad de las políticas de seguridad de la Institución.

La Subgerencia Administrativa y Financiera, Subgerencia de Servicios de Salud y la Oficina Asesora de Desarrollo de Servicios, en conjunto con el jefe directo del funcionario y/o responsable del tercero, son los encargados del proceso de terminación de labores y asegurar que todos los activos propios de la Institución sean devueltos, los accesos físicos y lógicos sean desactivados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de terminación de contrato.

En caso de que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de estos de acuerdo con su rol.

En caso de retiro o desvinculación laboral del funcionario, contratistas y/o tercero, éste debe hacer devolución del respectivo Carnet asignado en desarrollo de sus funciones, previo diligenciamiento del FORMATO CÓDIGO: TH-F-39 Acta De Entrega Puesto De Trabajo, para el proceso de terminación y liquidación de prestaciones sociales y demás obligaciones.

El funcionario que se retira ya sea contratista o personal de la institución que tenga asignado equipo de cómputo debe realizar entrega de la información al Coordinador o Jefe Inmediato y solicitar copia de la información al proceso de Tecnologías de la Información, como requisito para la firma del paz y salvo.

El área de talento Humano y educación médica y Coordinadores de Área, deberán informar al proceso de Tecnologías de la Información y Comunicaciones sobre las personas que se retiran o terminan su labor contratada, para que se proceda a desactivar los usuarios en los sistemas de información asignados.

14. POLÍTICAS DE GESTION DE ACTIVOS

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Almacén, mantiene el suministro, almacenamiento y entrega de insumos, materiales necesarios para el desarrollo de las actividades de la institución permitiendo satisfacer las necesidades de las áreas de la institución, realizando la correcta gestión y control del inventario físico y a través de la adecuada gestión con los proveedores.

El área de Almacén y suministros es el área encargada de realizar el ingreso y despacho de suministros; de mantener el control del inventario físico y actualizado de los activos de la institución; realizar la asignación de responsables de activos; realizar la baja de activos; realizar el plan de dotación de bienes muebles y enseres de uso administrativo y asistencial; entre otras actividades con la gestión de activos. Los procedimientos asociados y a tener en cuenta son:

A-PR-10 Inventario físico activos fijos;

A-PR-05 Control y registro de los inventarios de activos fijos;

A-PR-03 Baja de activos fijos;

A-PR-01 Ingreso de mercancías,

A-PR-02 Recepción Y Despacho De Mercancías.

A-PR-07 Plan De Dotación De Bienes .

14.1 Asignación de Activos

El área de Almacén y suministros, es el área encargada de realizar la asignación de activos a los colaboradores de la institución, según procedimiento A-PR-04 ASIGNACIÓN DE RESPONSABLE DE ACTIVOS FIJOS. Es responsabilidad del usuario de cuidar el inventario asignado.

14.2 Devolución de Activos

Todo el personal, contratista y/o tercero de la E.S.E Hospital Universitario San Rafael de Tunja, al momento de su retiro o cambio de funciones en la Institución debe hacer entrega a su jefe inmediato del equipo que se le había asignado, con toda la información contenida en él y una relación de la misma, previo diligenciamiento de Formato CÓDIGO: TH-F-39 Acta De Entrega Puesto De Trabajo.

14.3 Traslado de activos

Cualquier traslado de equipos de cómputo se realizará con la coordinación con el proceso de TICs previo diligenciamiento de FORMATO de almacén A-F-02 Registro De Activos.

14.4 Uso aceptable de los activos

Las actividades que realicen sobre archivos físicos, equipos de la infraestructura informática, redes, Internet, correo electrónico, servidores, base de datos, aplicaciones, sistemas de información institucional, entre otros activos de información, propiedad de la E.S.E. Hospital Universitario San Rafael Tunja, se debe usar para el cumplimiento de las funciones o actividades asignadas dentro de la labor contratada, enmarcada dentro la misión, visión de la entidad y dentro de las normas que reglamenten.

Se debe reportar al proceso de Tecnologías de la Información y Comunicaciones -Tics, fallas o incidentes que afecten la integridad, disponibilidad y confidencialidad e incidentes de seguridad sobre los activos de información.

Los funcionarios encargados de la seguridad y con apoyo del líder de cada una de las áreas deben realizar, mantener y actualizar el inventario de los activos de la información.

15. POLITICAS DE SEGURIDAD, PRIVACIDAD, REGISTRO, CUSTODIA Y ADMINISTRACIÓN DE LA HISTORIA CLINICA

La E.S.E. Hospital Universitario San Rafael de Tunja, durante la atención de sus pacientes, realiza el debido registro clínico en las atenciones realizadas en la Historia Clínica.

La Historia clínica es por ley, un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

El Ministerio de la protección social estableció a través de la resolución 1995 de 1999 normas para el manejo de la Historia Clínica, por lo tanto, La E.S.E. Hospital Universitario San Rafael de Tunja, tiene como política estricta, mantener sus Historias Clínicas dentro de los más altos estándares tanto de forma como de contenido.

La Historia Clínica es el documento privado de tipo técnico, clínico y legal, tiene valor para el paciente, el médico y la Institución. Constituye un elemento indispensable para la asistencia, docencia, la investigación, la asistencia, la facturación y la auditoría médica.

La E.S.E. Hospital Universitario San Rafael de Tunja, implementó la Historia Clínica electrónica a través del software Servinte Clinical Suite, conservando las características de la Historia como son la integralidad, racionalidad científica, secuencialidad, disponibilidad, oportunidad, seguridad, obligatoriedad de registro y calidad.

15.1 Custodia De La Historia Clínica.

La custodia de la Historia Clínica se encuentra a cargo de la E.S.E. Hospital Universitario San Rafael de Tunja. La responsabilidad es compartida por los diferentes procesos del Hospital tanto estratégicos, como misionales y de apoyo, quienes se encargan de velar por el correcto diligenciamiento, registro, manejo, seguridad y confidencialidad de la Historia clínica de acuerdo con competencias de cada proceso, a las normas que la rigen, a las directrices y políticas institucionales al respecto.

La Corte Constitucional en Sentencia T443 de 1994 expresa: “las instituciones de salud tendrían el deber especial de mantener archivos de información relevante que asegure a la persona, en las condiciones descritas, conocer plenamente cuál era su situación y cómo se procedió en el caso específico, así como la obligación de suministrarle toda la información personal cuando ésta la solicite”.

- **Comité de historias clínicas.** Defínase el comité de Historias Clínicas como el conjunto de personas que, al interior de una Institución Prestadora de Servicios de Salud, se encarga de velar por el cumplimiento de las normas establecidas para el correcto diligenciamiento y adecuado manejo de la Historia Clínica.
- **Copia de la historia clínica.** La Institución podrá entregar copia de la Historia Clínica al usuario o a su representante legal cuando este lo solicite siempre y cuando cumpla con los requisitos para la entrega o en los casos previsto por la ley. Formato F-28 Solicitud Copia Historia Clínica y procedimiento AHC-PR-05 Solicitud De Copia De Historia Clínica En Consulta Externa E Internación

En el momento de la entrega de la historia clínica física, se deberá dejar registro de su entrega en el libro de custodia respectivo.

Cuando la historia clínica sale del área de archivo, la responsabilidad de la custodia recae en otras áreas como se relaciona a continuación:

Para la consulta y revisión de historia Clínicas de las áreas administrativas se cuenta con el procedimiento AHC-PR-04 y libros de custodia definidos en este procedimiento.

Para la consulta Clínicas son entregadas al servicio de internación se cuenta con los libros de custodia AHC-L-23 y AHC-L-10, donde se registra la entrega y recibido de aquellas historias clínicas de los servicios donde aún no se encuentra sistematizada la historia clínica.

Para el servicio de consulta externa igualmente se cuenta con libros de custodia por especialidad AHC-L-04 donde se registran la entrega y recibido de la misma.

Está prohibido retirar la Historia Clínica Física de los servicios donde fue entregada fuera de los casos en que se realiza traslado del paciente, durante su proceso de facturación, o en casos específicos de gestión de los comités institucionales.

Está prohibido retirar la Historia Clínica Física de los servicios de hospitalización fuera de los casos en que se realiza traslado del paciente o durante su proceso de facturación, o en casos específicos de gestión de los comités institucionales. En todo caso, se dejará registro de la entrega de la Historia Clínica para su traslado en las notas de enfermería en la historia clínica.

En el momento de la entrega de la historia clínica física o de los documentos relacionados con la atención, se deberá dejar registro de su entrega en el libro de custodia respectivo.

Cuando la historia clínica sale del área de archivo, la responsabilidad de la custodia recae en otras áreas

15.2 Seguridad Del Archivo De Historias Clínicas

La E.S.E Hospital Universitario San Rafael Tunja, a través del proceso de Archivo de Historia Clínica, cuenta con un área restringida para el archivo físico de Historias Clínicas, con acceso limitado al personal de salud autorizado, conservando las Historias Clínicas en condiciones que garanticen la integridad física y técnica, sin adulteración o alteración física y técnica, sin adulteración o alteración de la información.

La E.S.E. Hospital Universitario San Rafael Tunja, a través del Proceso de Tecnologías de la Información y las Comunicaciones – TICS, controla el acceso al centro principal de cómputo, de servidores y comunicaciones, donde se almacena el sistema de Información de Historia Clínica Electrónica, restringiendo el acceso solo al personal autorizado por el Coordinador de Tecnologías de la Información y las Comunicaciones. Adicional se debe tener en cuenta lo descrito en el capítulo de Acceso al centro de cómputo, servidores y equipos de comunicación, de este manual.

El acceso al sistema de información de Historia clínica debe contar con mecanismos de autenticación para el ingreso al software de Historia Clínica a través de firma electrónica y de la configuración previa de permisos según cada perfil de usuario, lo que permite proteger la información contra ingresos y consultas no autorizadas.

El sistema de Información de Historia Clínica Electrónica no permite realizar modificaciones a la Historia una vez firmada, en caso de alguna corrección se pueden realizar notas aclaratorias, esta opción solo se habilita a quien haya firmado el registro.

En los registros de Historia clínica debe quedar claro y explícito quién es el responsable incluyendo firma, número de registro profesional. El formato electrónico con que cuenta la E.S.E. Hospital Universitario San Rafael Tunja tiene la configuración predefinida de fecha automática, firma electrónica y número de registro profesional garantizando que cada registro realizado quede firmado por el usuario que ingreso al sistema.

Los programas automatizados que se diseñan y utilizan para el manejo de las Historias Clínicas Sistematizada en la E.S.E. Hospital Universitario San Rafael Tunja, así como sus equipos y soportes documentales, están provistos de mecanismos de seguridad, que imposibiliten la incorporación de modificaciones a la Historia Clínica Electrónica una vez se registren y guarden los datos.

Por ser información de historia clínica electrónica la disposición de esta se almacenará y se conservará en el sistema de información bajo las mismas normas y periodos de retención documental de historia clínica física.

15.3 Privacidad De La Historia Clínica

Teniendo en cuenta que la historia clínica es un documento un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, solamente puede conocerse con autorización del paciente o en los casos previstos por la ley.

Todo el personal que tiene acceso a los registros de la historia clínica debe garantizar la confidencialidad de la información.

La Epicrisis, que según la Resolución 3374 de 2000 debe ser un soporte de la facturación, contiene información sobre las condiciones de un paciente; el hecho de que circule para estos efectos fuera de la Institución de Salud, no viola el derecho a la intimidad de los pacientes, puesto que los datos allí registrados tiene protección suficiente sobre su divulgación y son necesarios para las acciones del Ministerio de Salud relacionadas con la información para decisiones en beneficio de la comunidad (Sentencia del Consejo de Estado 6203 del 4 de mayo de 2001).

Queda prohibido que el personal paramédico, auxiliar o administrativo ponga a disposición del paciente o de terceros, documentos o información

relacionada con la Historia Clínica. En ningún caso los pacientes, ni sus familiares o amigos se constituirán en mensajeros de ninguno de los componentes de su historia.

Queda prohibida la toma de fotos, pantallazos, grabaciones y divulgación de información de Historia Clínica de los pacientes por cualquier medio de comunicación, sin el debido proceso de solicitud formal de copia de historia clínica.

15.4 Criterios De Calidad En La Historia Clínica

La E.S.E. Hospital Universitario San Rafael de Tunja, tiene como política estricta, mantener sus Historias Clínicas dentro de los más altos estándares tanto de forma como de contenido. Todo profesional médico o paramédico deberá ajustarse a las normas relativas al registro, elaboración y manejo de la Historia Clínica, la cual debe ser completa, veras, con rigor técnico en el registro, ser coherente y clara, sustentada, integral, secuencial, legible, sin espacios en blancos, enmendaduras mínimas, debe estar fechada y firmada; mantenimiento la confidencialidad de la información.

La Historia Clínica es un instrumento jurídico y probatorio al momento de determinar responsabilidades civiles, penales o administrativas. No realizar la Historia Clínica implica una falta grave del profesional, impide la defensa del profesional y de la Institución en caso de demandas y se convierte en un arma contra el médico y el Hospital, además, que afecta la calidad de la Historia.

En cuanto al personal en formación se refiere, estas normas hacen parte integral de su respectivo reglamento y como tal, su no observancia puede acarrear las sanciones correspondientes.

La Historia Clínica es el único documento válido para demostrar el tipo de atención médica que un paciente ha recibido, es fiel reflejo de la calidad de atención brindada por el médico y personal paramédico.

En adherencia al sistema de información de Historia Clínica, procedimientos y el respectivo manual, se debe realizar seguimiento periódico al tablero clínico del sistema, a la gestión realizada por los usuarios, así como a los demás registros clínicos y administrativos ingresados. Procedimiento de Seguimiento a tablero Clínico TRA-PR-33.

15.5 Apertura E Identificación Del Usuario En La Historia Clínica

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Facturación, realiza la apertura de Historia Clínica teniendo en cuenta los lineamientos de la resolución 1995 de 1999.

Se debe realizar el proceso de apertura de Historia clínica para los pacientes que ingresan o atienden por primera vez; para los que están en el sistema de Información, se debe indagar al paciente o responsable y solicitar los datos e información que se requieren y proceder a realizar la apertura de la historia bajo un nuevo episodio de atención. El ingreso del paciente debe contener la información completa, acorde a los campos previamente establecidos en el sistema. Ver el Procedimiento de Apertura de Historia Clínica AHC-PR-02; procedimiento de duplicidad TRA-PR-18; instructivo de admisión de paciente al Sistema de Información S-INS-02.

Los datos mínimos solicitados en la admisión, según resolución 1995 de 1999, son: datos personales de identificación del usuario, apellidos y nombres completos, estado civil, documento de identidad, fecha de nacimiento, edad, sexo, ocupación, dirección y teléfono del domicilio y lugar de residencia, nombre y teléfono del acompañante; nombre, teléfono y parentesco de la persona responsable del usuario, según el caso; aseguradora; tipo de vinculación y los demás requeridos por en el sistema de información de Historia Clínica de Servinte al momento de la admisión, que complementan la información requerida por la institución.

En la admisión del paciente, se debe realizar una correcta verificación e identificación del paciente, si es posible con el documento físico en mano, validando si ya existe o no en el sistema, antes de crearlo o de actualizar los datos; corroborando los datos administrados, con las diferentes bases de datos de las Empresas Prestadoras de Salud (EPS) en los que se encuentra afiliado el paciente, y las demás comprobaciones de manera que se evite errores en la identificación y la duplicidad de historias de pacientes. Procedimiento TRA-PR-16 Ingreso Clínico - Administrativo De Pacientes y S-INS-02 Instructivo Admisión Del Paciente Al Sistema De Información.

La Historia Clínica Electrónica en la E.S.E. Hospital Universitario San Rafael Tunja se conforma desde su inicio en expedientes electrónicos bajo un número de consecutivo único generado de manera automática por el sistema para cada paciente que ingresa a la institución. Este número único debe identificar al paciente dentro del software de Historia Clínica y relacionarlo en todo momento con el documento de identificación del paciente, permitiendo llevar la secuencialidad de la información consignada pese a los cambios de documentos por edades evolutivas. El sistema debe permitir identificar cada episodio para cada ingreso que realice el paciente en la institución.

15.6 Registro Y Manejo De La Historia Clínica

Obligatoriedad del Registro. De acuerdo con lo reglamentado en el manejo de historia clínica, los profesionales, técnicos y auxiliares que intervienen directamente en la atención a un usuario, tienen la obligación de registrar sus observaciones, conceptos, decisiones y resultados de las acciones en salud desarrolladas, conforme a las características señaladas en la resolución 1995 de 1999. El no realizarse o conducirse por las normas establecidas en el manejo y registro de la Historia Clínica, conlleva a un riesgo jurídico para la entidad y para el equipo de salud involucrado en la atención.

Todo profesional médico o paramédico deberá ajustarse a las normas relativas al registro, elaboración y manejo de la Historia Clínica, la cual debe diligenciarse en forma clara, legible, sin tachones, enmendaduras, intercalaciones, sin dejar espacios en blanco, de manera oportuna, de manera cronológica y sin utilizar siglas. Cada anotación debe llevar la fecha y hora en la que se realiza, con el nombre completo y firma del autor de la misma. Todo el personal que tiene acceso a los registros de la historia clínica debe garantizar la confidencialidad de la información.

Se establece que solo el personal docente que se encuentra incluido en los convenios docente - asistenciales suscritos por la institución puede intervenir como parte del equipo de atención en salud del paciente. En caso de realizar intervención, dejará el debido registro firmando las anotaciones en la Historia Clínica.

Se establece que las actividades realizadas por los estudiantes de programas académicos de pregrado que requieran ser registradas en la

Historia Clínica del paciente u otros registros, deberán ser consignadas por el personal en formación, los cuales serán sujetos a verificación, validación por el profesional médico responsable y respaldados con su firma, nombre y registro profesional.

El sistema de Historia clínica electrónica cuenta con formatos o plantillas, como Triage Medico, Ingreso a servicio, Nota de evolución, Registros de procedimientos, Interconsultas/Juntas, Nota de egreso, entre otras, que deben ser diligenciadas por el personal médico o paramédico de acuerdo a la atención del paciente, servicio y rol asignado en el sistema.

El manual AHC-M-01 Manual de Historia Clínica de la E.S.E. Hospital Universitario San Rafael de Tunja, establecerá los demás lineamientos en cuanto a la obligatoriedad del registro en la Historia Clínica.

15.7 Acceso A La Historia Clínica

El acceso a la Información contenida en la Historia clínica, se debe hacer solo en los términos provisto por la ley:

1. El usuario.
2. El Equipo de Salud.
3. Las autoridades judiciales y de Salud en los casos previstos en la Ley.
4. Las demás personas determinadas en la ley.

El acceso a la historia clínica se entiende en todos los casos, única y exclusivamente para los fines que de acuerdo con la ley resulten procedentes, debiendo en todo caso, mantenerse la reserva legal.

15.8 Administración Del Sistema De Información De Historia Clínica

La administración del Sistema de Información de Historia Clínica Integrada, Servinte Clinical Suite, está a cargo del Coordinador del Proceso de Tecnologías de la Información y Comunicaciones -TICs, y los ingenieros a cargo.

15.8.1 Historia Clínica Integrada Y Su Componente Administrativo

Los Ingenieros a cargo de del proceso Tecnologías de la Información y Comunicación -TICs, son encargados para la creación, activación, desactivación y modificación de cuentas de usuarios; establecer o quitar permisos o privilegios a los grupos de usuarios administrativos de acuerdo a su perfil o labor a realizar dentro del sistema; apoyo en la implementación de Historia Clínica Integrada; implementar funcionalidades en los componentes o módulos administrativos; reportar fallas o inconvenientes; llevar registro, control y solución de casos a inconvenientes encontrados; proponer, orientar y dar apoyo técnico en las funcionalidades del sistema de Historia Clínica Integrada y su componente administrativo; realizar auditorías en componentes administrativos del sistema; realizar orientación de las funcionalidades del sistema al personal que lo requiera; generar documentación acerca de los componentes administrativos cuando se requiera; realizar las copias de seguridad y respaldos necesarios al sistema de información; realizar mantenimiento y despliegue de servidores; apoyar técnicamente a líderes del programa esencia en el manejo de casos que lo requieran; realizar actualizaciones al sistema de información de la Historia Clínica.

15.8.2 Historia Clínica Integrada

Los líderes clínicos del programa Esencia son delegados por el Coordinador del proceso Tecnologías de la Información en la administración del Componente de Historia Clínica Integrada, para establecer o quitar permisos o privilegios a los grupos de usuarios clínicos de acuerdo a su perfil o labor a realizar dentro del sistema; apoyo en la implementación de la Historia Clínica; implementar funcionalidades en los componentes o módulos clínicos con apoyo de Ingenieros de TICs; reportar fallas o inconvenientes; llevar registro, control y solución de casos a inconvenientes encontrados; proponer, orientar y dar apoyo técnico en las funcionalidades del sistema de Historia Clínica Integrada; realizar auditorías de los tableros y demás componentes clínicos del sistema; generar documentación acerca del componente de Historia Clínica Integrada; realizar capacitación al personal que ingresa o que lo requiera.

15.9 Mantenimiento Al Sistema De Información

Acuerdo de Nivel de Servicio (ANS). La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Tecnologías de la Información y Comunicación - TICs, debe mantener los acuerdos contractuales del nivel de servicio con el proveedor del software, y demás componentes del sistema, especificando el tipo de servicio ofrecido, tiempo de respuesta, disponibilidad horaria, personal asignado, coste del acuerdo, garantías y condiciones de finalización del acuerdo, entre otra.

Mantenimiento De Infraestructura. El proceso de Tecnologías de la Información y Comunicaciones incluye los servidores y demás componentes del sistema de información de Historia Clínica en el plan de mantenimiento y/o actualización de la infraestructura, minimizando el riesgo de interrupción del sistema de información, sistemas de información desactualizados o inestables o por desactualización de la infraestructura.

Reportes y Solución de Fallas o Inconsistencias:

Reporte. Los usuarios del sistema de información de Servinte, Historia Clínica y módulos administrativos deben reportar las inconsistencias o fallas detectadas en el sistema de información al programa Esencia y al proceso de TICs respectivamente.

Soporte nivel 1. El programa Esencia y el proceso de TICs, con los casos de reportados deben iniciar la revisión y análisis del caso a nivel interno, en busca de estrategias de solución, documentando las soluciones. S-PR-01 Soporte De Historia Clínica Sistematizada, S-PR-09 Soporte A Los Usuarios De Los Sistemas De Información.

Soporte nivel 2. El programa Esencia y el proceso de TICs, con los casos reportados y en los casos no resueltos de manera interna, se debe iniciar el reporte del caso con la mesa y plataforma de servicio dispuesta por el proveedor, en busca de las estrategias de solución.

Actualizaciones de Software. Se debe gestionar las actualizaciones al sistema de información de Historia Clínica Servinte clínica suite y su componente administrativo, de acuerdo las actualizaciones por cambio de versión enviadas por el proveedor del software o en los casos o tickets

reportados por el Hospital, siempre que resulten convenientes para la entidad.

Las actualizaciones identificadas con respecto a los cambios normativos deben ser gestionadas por lo líderes o coordinadores de proceso y notificadas al Coordinador del Proceso de Tecnologías, para que se proceda a realizar la evaluación y gestión del cambio sobre el sistema de información. Si resulta procedente notificar al Proveedor del software sobre dicho cambio.

Las actualizaciones a realizar sobre el sistema de información se deben instalar en ambientes de prueba y ejecutar las pruebas correspondientes por los líderes a cargo antes de subirlas o instalarlas en producción, minimizando el impacto en el sistema de información por los cambios realizados. Tener presente la sección de Gestión del Cambio de este manual.

Queda prohibido que los usuarios de la aplicación Servinte Clínica Suite guarden información en los servidores de aplicaciones a los que se conectan remotamente. Debe guardar la información en sus equipos locales, pues al realizar mantenimiento a los servidores, la información podrá ser borrada sin previo aviso.

15.10 Consulta De Los Archivos De Historia Clínica

Para la consulta de pacientes inactivos deberá realizarse solicitud al área de archivo de historias clínicas, donde se definirá el procedimiento para acceso a esta información según el AHC-M-01 MANUAL HISTORIA CLINICA y procedimientos establecidos para la consulta y/o revisión de historia clínica, igualmente se atenderá lo señalado en la circular de Gerencia correspondiente.

Para aquellas dependencias internas que requieran revisar la historia clínica se cuenta con procedimientos propios de la oficina donde se deben adherir a estos y así mismo hacer la solicitud informando el motivo de la consulta.

En la Historia clínica electrónica el permiso de consulta de historia Clínicas inactivas está asociado a los permisos y roles definidos en el sistema para ciertos usuarios.

15.11 Creación y Cuentas de Usuario De Historia Clínica.

La creación de cuentas en el sistema de información de Historia Clínica está enmarcado en las políticas de acceso a los sistemas de información descritas en este manual. Adicional se especifica que:

- El área de Talento Humano es la encargada de notificar al área de Esencia, TICs y el Coordinador de área, el ingreso de personal, para la inclusión de estos en las capacitaciones respectivas.
- La capacitación en Historia Clínica y su componente administrativo es obligatoria, para el personal que se vincula a la institución y que requiere el manejo en el sistema clínico y administrativo respectivamente. La capacitación se hará de acuerdo a su perfil y manejo en el sistema.
- La capacitación en Historia Clínica está a cargo del Programa Esencia, llevando control de la asistencia y la capacitación impartida.
- La capacitación en el componente administrativo de Servinte es obligatoria y estará a cargo de los líderes administrativos con conocimiento y experiencia en el manejo de la aplicación que designe el coordinador o líder de área, llevando control de la asistencia y de la capacitación impartida.

Previo a la creación de cuenta los administradores de creación de cuenta deben validar la asistencia a las capacitaciones respectivas para proceder a otorgar el acceso.

Las credenciales asignadas (usuario y clave) de acceso al sistema de Historia Clínica, se asignan de manera personal e intransferible. El usuario deberá mantenerla de manera confidencial y queda prohibido divulgarla o prestarla; La persona es responsable por el acceso, modificación o registro que se haga a su con su usuario.

Las contraseñas deberán ser cambiadas cada tres meses como mínimo, cada usuario deberá mantenerla confidencialmente.

Cuando un usuario olvide su contraseña o bloquee su usuario, deberá notificarlo a la auxiliar de apoyo de Esencia o directamente al proceso de Tecnologías de la Información quienes se encargarán de desbloquear o renovar dichas credenciales.

Los auditores externos solo tendrán acceso a las historias clínicas de los pacientes de su EPS correspondiente, quienes podrán consultar la historia clínica de los pacientes activos durante la hospitalización; Igualmente deben mantener la reserva y confidencialidad de la información.

Cuando el personal se retire de la institución o no utilice más el sistema de Historia Clínica, el usuario debe ser deshabilitado de manera inmediata por los administradores, previa comunicación oportuna del mismo usuario, el líder del proceso al que pertenece y/o Talento Humano o a la firma del paz y salvo por el proceso de Tecnologías de la Información.

15.12 Permisos, Privilegios, Roles En El Sistema De Historia Clínica Electrónica

Los permisos sobre los módulos, secciones o funciones de Historia Clínica se agrupan en roles o grupos de usuarios de acuerdo a las actividades clínicas o administrativas a realizar en el sistema. Se debe conceder solo los privilegios necesarios sobre la Historia Clínica, permitiendo la consulta e impresión de la historia clínica solo al personal que lo requiere y de acuerdo a la función o rol en sistema desempeñar. Se debe restringir en los demás casos.

Cualquier cambio en los privilegios, permisos, roles o perfiles de los usuarios en los sistemas de información, deberán ser solicitados al coordinador del proceso al que pertenece y éste a su vez solicitarlos a través de correo electrónico al personal del proceso a cargo de otorgar o modificar dichos privilegios; de tal forma que tenga conocimiento de los cambios solicitados.

La adición o modificación de permisos clínicos y administrativos deben ser validados previamente por el líder funcional clínico y administrativo respectivamente del sistema de Información de Historia clínica.

15.13 ESCANEADO DE DOCUMENTOS COMPLEMENTARIOS A LA HISTORIA CLINICA

La E.S.E. Hospital Universitario San Rafael Tunja, establece el escaneo de documentos de Historia Clínica, bajo un procedimiento a través del cual se escanea y relaciona a la Historia Clínica Electrónica documentos complementarios de la atención del paciente, así como los soportes de cuenta y los documentos físicos que se han producido dentro de la atención. Las actividades y responsables están determinados en el Procedimiento Escaneo Para Historia Clínica Electrónica TRA-PR-29.

No se deben escanear documentos que sean parte de la historia clínica electrónica o cuyo contenido se encuentre en algún registro de la historia clínica electrónica, excepto aquellos que requieran firma del paciente o acompañante.

Los documentos a escanear se definen y describen en el manual de historia clínica de la entidad. AHC-M-01 MANUAL HISTORIA CLINICA.

15.14 Archivo De Historias Clínicas Físicas

La E.S.E. Hospital Universitario San Rafael Tunja cuenta con un archivo físico de Historias Clínicas en las etapas del archivo de gestión, central e histórico, a través del proceso de Archivos de Historia Clínicas, el cual organiza y presta los servicios teniendo en cuenta los principios generales establecidos en el acuerdo 07 de 1994, expedido por el Archivo General de la Nación, la resolución 1995 de 1999, resolución 839 de marzo 2017, procedimiento de archivo AHC-L-03.

15.15 Foliación De La Historia Clínica Física

Todos los folios que componen la historia clínica deben numerarse en forma consecutiva, por tipos de registro, por el responsable del diligenciamiento de la misma. La foliación de documentos está a cargo del proceso de archivo de historias Clínicas y es imprescindible en la organización archivística de la Historia según procedimiento AHC-PR-03 Archivo Historia Clínica.

15.16 Perdida De Historias Clínicas Físicas Extraviada

Para los casos de Historia Clínica extraviada y/o documentación de Historias Clínicas, se procede a realizar el respectivo seguimiento y búsqueda según lo establecido en el procedimiento para Historia Clínica extraviada AHC-PR-10 Reconstrucción Historia Clínica Extraviada.

15.17 Retención Y Tiempo De Conservación Del Archivo De Historias Clínicas

La Historia Clínica debe conservarse por un periodo mínimo de quince (15) años contados a partir de la fecha de la última atención. Mínimo cinco (5) años en el archivo de gestión del prestador de servicios de salud, y mínimo diez (10) años en el archivo central, de acuerdo a lo reglamentado en la resolución 839 de 2017.

15.18 Condiciones Físicas De Conservación De La Historia Clínica

Los archivos de Historias Clínicas deben conservarse en condiciones locativas, procedimentales, medio ambientales y materiales, propias para tal fin de acuerdo con los parámetros establecidos por el Archivo General de la Nación en los Acuerdos 07 de 1994, 11 de 1996 y 05 de 1997, Ley 594 de 2000, Acuerdo 049 de 2000 del AGN o las normas que los deroguen, modifiquen o adicionen.

15.19 Impresión De Historias Clínicas.

En la E.S.E. Hospital Universitario San Rafael Tunja, se realiza la impresión de la epicrisis generada en la Historia Clínica Electrónica o de algunos de sus registros solo a criterio médico o por solicitud expresa del paciente. Si se solicitan antes de terminar la atención se generan epicrisis parciales, ya al final de la atención se puede generar la epicrisis final (Urgencias y/o hospitalización).

Se debe realizar impresión del consentimiento informado o de los requeridos durante la atención, o de la declaración de retiro voluntario.

La solicitud de copia de su Historia Clínica se debe hacer de acuerdo al trámite interno que se tiene establecido por el área de Archivo de Historias Clínicas de la Institución. Ver procedimiento AHC-PR-05. Solicitud de copia de historia clínica en consulta externa e internación.

Queda prohibida la impresión de Historia Clínica de los pacientes, con excepción de los casos de solicitud de copia impresa por el paciente, en los casos previsto por la ley, en los casos de impresión de la epicrisis, en procesos administrativos del hospital como soportes de cuentas médicas, revisión de casos epidemiológicos entre otros.

15.20 Plan De Contingencia Ante Fallo Del Sistema De Información Servinte

La E.S.E. Hospital Universitario San Rafael Tunja, establece un plan de contingencia descrito en el manual de Historia clínica, como un mecanismo que permite continuar con la prestación de la atención de forma integral, confidencial y segura en situaciones de contingencia por fallas del hardware, software o energía eléctrica donde se permita la continuidad de las operaciones, integralidad del registro de la Historia Clínica y se tengan herramientas que soporten los procesos de facturación. Ver Procedimiento de Contingencia Ante Fallo Del Sistema De Información Servinte- TRA-PR-38, el cual aplica para todos los procesos afectados en un fallo del sistema de información de Historia clínica. AHC-M-01 Manual Historia Clínica.

Una vez se solvente la situación de falla que dio origen a la contingencia y se encuentre en funcionamiento normal el sistema, se restringe y limita el uso de los formatos institucionales en físicos. Solo se permite en los casos de contingencia.

El manual de Historia clínica describe el plan de contingencia y define los formatos a tener en cuenta en el diligenciamiento durante la contingencia en cada área, los cuales se deben mantener en cada servicio.

15.21 Políticas De Prevención De Daño Antijurídico Derivados Del Manejo De Historia Clínica

La política de prevención del daño antijurídico derivado del manejo de historia clínica es aplicable a las áreas y dependencias de la E.S.E. Hospital Universitario San Rafael Tunja encargadas de la apertura, diligenciamiento y custodia de la historia clínica, así como a todos los colaboradores de los procesos que intervienen en la atención de un usuario que tienen relación directa con la información consignada en ella y en las cuales se identifique que el ejercicio propio de su actividad podría generar riesgos litigiosos para la Entidad.

Los términos y definiciones utilizados en la generación de la política de prevención del daño antijurídico se relacionan a continuación:

Daño Antijurídico: La responsabilidad patrimonial del Estado, según lo contemplado en el artículo 90 de la Constitución Política, tiene como fundamento el daño antijurídico, que ha sido definido doctrinalmente como aquel “que el titular del patrimonio considerado no tiene el deber jurídico de soportarlo, aunque el agente que lo ocasione obre él mismo con toda licitud” , evento en el cual el daño es un hecho jurídico que debe evitarse o repararse porque “no está contemplado por la Ley como carga pública que todo particular deba soportar”

Política de prevención del daño antijurídico: La política de prevención es la solución de los problemas administrativos que generan litigiosidad e implica el uso de recursos públicos para reducir los eventos generadores del daño antijurídico.

Historia Clínica: Es el documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente o usuario, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención.

Ahora bien, para la E.S.E. Hospital Universitario San Rafael Tunja es fundamental que la Historia clínica cumpla con los estándares enmarcados en la resolución 1995 de 1999 y demás normas concordantes, para lo cual se debe tener en cuenta las siguientes políticas:

1. La historia clínica deja de ser un registro de la información generada entre paciente y profesional, para formar parte de un sistema integrado en el que conviven la personalización y confidencialidad. La visión futurista, con bastante presente, conduce, electrón a electrón, a que la historia clínica deje de ser un registro de la información generada en la relación entre un paciente y un profesional o entre éste y una Institución para formar parte de un sistema integrado de información clínica y médica, en el que conviven la personalización y confidencialidad con el teórico acceso multimedia y universal, y en el que se archiva en soporte electrónico toda la información referente al paciente y a su atención.

2. Se debe realizar el diligenciamiento adecuado de la historia clínica por parte del personal de salud que interviene en la prestación del servicio para garantizar la calidad en la atención y el sostenimiento financiero. El no diligenciamiento o el diligenciamiento incompleto e inadecuado de la historia clínica representa riesgos importantes para la institución; a nivel administrativo, como objeciones por parte de los pagadores que afectan los ingresos económicos, a nivel jurídico por ser la historia clínica un documento legal y en la prestación misma de los servicios de salud, por falta de información certera y de calidad para la toma de las decisiones en el manejo del paciente.

3. La Historia Clínica tiene que garantizar unas funciones determinadas que van desde la asistencia, que siempre ha sido su aspecto más importante, la docente, la investigación, la gestión clínica y la planificación de recursos asistenciales, aspectos jurídico-legales y por qué no el control de la calidad asistencial. Debe ser única para cada persona acumulando toda su información clínica y además ser integrada de forma que contenga la información de todos los contactos y episodios del paciente.

4. Garantizar la calidad de los registros y la accesibilidad del personal autorizado, permiten en primer lugar, mejorar la calidad de atención a los pacientes, en segundo lugar, proteger la institución de riesgos legales institucionales y del personal de atención en salud, en tercer lugar, reducir las posibles fallas en el diligenciamiento desde el punto de vista de la actitud y aptitud por parte del personal de salud. Y por último disminuir los riesgos financieros generados por glosas o no pago de servicios por malos diligenciamientos de las historias clínicas.

5. Las historias clínicas y/o registros asistenciales, deben diligenciarse: clara, legible, sin tachones, enmendaduras, intercalaciones, sin dejar espacios en blanco y sin utilizar siglas. Cada anotación debe llevar la fecha y hora en la que se realiza, con el nombre completo y firma del autor de la misma.

6. Los registros en la Historia Clínica deben ser oportunamente diligenciados y conservados, garantizando la confidencialidad de los documentos protegidos legalmente por reserva.

7. Se debe tener en cuenta que la Historia Clínica como instrumento médico-legal, es el único documento con peso propio que permite valorar y/o evaluar a la responsabilidad profesional en los fueros civil, penal o administrativo, etc., como prueba elemental, básica y determinante del accionar profesional. Instrumento sobre el cual se realizará, durante la etapa probatoria el dictamen pericial médico, y que resulta ser un elemento clave en la elaboración del/de los informes Médico-Legal/es practicados por el/los expertos (Peritos) y que será apreciado judicialmente por el juez con el objeto de determinar una relación de causalidad o no en la responsabilidad médica profesional.

El objeto de estudio de todo informe pericial sobre responsabilidad médica profesional es la historia clínica, a través de la cual se valoran los documentos que la integran, con reconstrucción y análisis de los actos médicos realizados en el paciente. La historia clínica contiene eficacia probatoria toda vez que resulta ser una herramienta probatoria de singular importancia a la hora de determinar las responsabilidades de los profesionales intervinientes, pues constituye la relación de todos los datos y conocimientos tanto anteriores como actuales, relativos al paciente, y que nos ilustran sobre su estado al momento de los hechos.

8. En relación al contenido propio de la misma, deberá entonces ajustarse a guardar una información secuencial y cronológicamente bien ordenada.

9. Una correcta historia clínica que avale la buena práctica de la medicina es de vital importancia para eximir de responsabilidad al médico y a la Institución.

10. Una historia clínica llevada en forma o modo deficiente o incompleta demuestra la culpa profesional a través de la negligencia y/o imprudencia, cuando se encuentra corroborada por otros elementos probatorios producidos en la causa.

11. La historia clínica, debe caracterizarse por ser un documento veraz, constituyendo un derecho del usuario. El no cumplir tal requisito puede incurrirse en un delito tipificado en el actual Código Penal como un delito de falsedad.

12. Los datos en ella contenida deben ser realizados con criterios objetivos y científicos.

13. Los usuarios directos o indirectos de la Historia clínica deben garantizar que la misma sea un medio de comunicación de la información acerca de la atención prestada al paciente, que sirva de evidencia de la evolución de los pacientes, de sus enfermedades y tratamientos, para fines legales, financiación de la asistencia, docencia, gestión de la calidad y que proporcione datos clínicos reales para actividades administrativas, de investigación y docencia, controlando la calidad de la historia clínica en cada uno de los registros que se realicen.

Sanciones

El descuido en la elaboración y manejo de la historia clínica tiene consecuencias jurídicas importantes, no solo dentro de un proceso de responsabilidad profesional sino también en procesos penales relacionados con los llamados documentos privados. La historia clínica está vigilada por el código Penal.

La ley penal establece dos tipos de controles mediante los cuales se garantiza la legitimidad del documento:

Uno tiene que ver con la INTEGRIDAD FISICA del documento, de acuerdo en lo dispuesto en el artículo 224 del Código Penal que consagra el delito "Falsedad Material" (destruye, suprime u oculta total o parcialmente un documento privado que puede servir como prueba) y el otro que hace relación con su CONTENIDO y corresponde al tipo penal denominado "Falsedad Ideológica" (cuando en un documento genuino y verdadero se consignan hechos o declaraciones falsas). Las contempladas en la Ley 23 de 1981.

Igualmente se debe tener en cuenta es que el mal diligencia miento de la historia clínica, cometer omisiones al momento de diligenciar la misma, así como anotar información que no corresponde con la realidad puede generar sanción disciplinaria por parte del Tribunal de Ética Médica. Si quien incurre en estos hechos es empleado oficial comete el delito de prevaricato por omisión.

Así mismo, cuando se hacen anotaciones de las condiciones de salud de una persona, o actos médicos o procedimientos que nunca se realizaron, se comete el delito de falsedad ideológica en documentos privado.

En cuanto al derecho a la intimidad y la historia clínica, podemos decir que el derecho a la intimidad hace parte de la vida personalísima de cada ser humano y garantiza que nadie se inmiscuya en ella, incluye no pregonar afecciones, o deficiencias o enfermedades. Por tanto, una persona puede pedir que se hagan correcciones en su historia clínica, se actualicen o corrijan teniendo en cuenta el derecho del habeas data y siempre que la corrección o actualización corresponda a la realidad.

Cuando se presenten fallas en el sistema informático de la entidad, se recurrirá al diligenciamiento manual de la Historia; para ello cada servicio estará dotado de papelería marcada como contingencia la cual cumple con las especificaciones requeridas para la historia. Luego de reestablecido el sistema informático de la entidad, el profesional debe actualizar la información en la historia clínica del usuario, procedimiento que se debe llevar a cabo en el mismo mes que se presentó el evento.

16. Políticas De Seguridad En Gestión Documental

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Gestión Documental mantiene el archivo físico central de la entidad con condiciones, elementos de seguridad y organización adecuados para preservar la documentación recibida y archivada de la entidad, de acuerdo a lineamientos de Archivo General de la Nación.

16.1 Seguridad Entorno Físico Del Archivo Central

La E.S.E. Hospital Universitario San Rafael Tunja, en el archivo físico central cuenta con un repositorio de 720 metros cuadrados para albergar documentación que data de 1915 a 2017, dotado de un sistema de seguridad de cámaras en línea, elementos de control de roedores e insectos con dispositivos electrónicos, dos termohigrómetros, control de factores ambientales SF-F-17 para el control de la humedad relativa, temperatura, limpieza y aspirado diario.

Para la consulta de documentos institucionales se debe seguir el procedimiento GD-PR-13 CONSULTA DE DOCUMENTOS SEDE SANTA ANA, a través del correo institucional, llamada telefónica al archivo central del Hospital, allí se lleva un control con el formato Ficha de consulta y/o préstamo de archivos Institucionales GD-F-01 FICHA REGISTRO PARA CONSULTA O PRESTAMO DOCUMENTOS.

La información de archivos de la Entidad solo se entrega con previa autorización del coordinador de área, Oficina asesora Desarrollo de Servicios o Gerencia.

Se prohíbe a los usuarios externos consultar documentos del hospital o hacer visitas de referenciación a la entidad sin previa autorización de la Gerencia.

Tener en cuenta el GD-M-01 MANUAL DE COMUNICACIONES OFICIALES ACTUALIZADO v.3

Para consulta y/o préstamos de archivos entre oficinas o archivos de gestión se utiliza el control con el formato GD-F-20 FICHA REGISTRO PARA CONSULTA O PRESTAMO DOCUMENTOS ARCHIVOS DE GESTION

La documentación en las oficinas, se puede consultar previa autorización del coordinador de área, procedimiento préstamo de documentos de archivos de gestión.

Cada Unidad Productora de Documentos es responsable de organizar y de realizar una copia de seguridad por red en equipo diferente de donde se encuentra la información de acuerdo a Tablas de Retención Documental -TRD del área. Esta información deberá estar organizada de acuerdo a su TRD. La copia será de manera trimestral o cuando el coordinador lo considere. Esta a su vez será guardada en cinta o el medio previsto por el encargado del proceso de Tecnologías de la Información siempre y cuando se encuentre debidamente organizada conforme a la TRD respectiva. La ruta y carpeta a guardar la copia en equipo diferente será: c:\copiatrd_nombre_area\fecha (ddmmaaaa).

Los usuarios pueden consultar los procedimientos de Gestión Documental y los relacionados con el Sistema Orfeo, publicados en la plataforma para este fin por la Oficina de calidad. Seguir los procedimientos formales descritos a continuación de SGD Orfeo:

CA-F-74 CARACTERIZACION GESTION DOCUMENTAL

GD-PO-01 POLITICA OPERACIONAL GESTION DOCUMENTAL

GD-PR-02 ORGANIZACION DE FONDOS ACUMULADOS

GD-PR-03 PRODUCCIÓN DE DOCUMENTOS

GD-PR-04 TRANSFERENCIAS DOCUMENTALES PRIMARIAS

GD-PR-05 TRANSFERENCIA DOCUMENTALES SECUNDARIAS

GD-PR-06 ORGANIZACION DE DOCUMENTOS

GD-PR-07 RECEPCIÓN DE DOCUMENTOS

GD-PR-08 DISTRIBUCIÓN DE DOCUMENTOS

GD-PR-09 TRÁMITE DE DOCUMENTOS

GD-PR-10 CONSERVACIÓN DE DOCUMENTOS

GD-PR-11 DISPOSICIÓN FINAL DE DOCUMENTOS

GD-PR-12 TRASLADO ARCHIVOS SEDE SANTA ANA

GD-PR-13 CONSULTA DE DOCUMENTOS SEDE SANTA ANA

16.2 Sistema De Gestión Documental Orfeo

El sistema de información de gestión documental Orfeo es sistema oficial para el manejo de correspondencia de la entidad. Los usuarios deben tramitar las comunicaciones oficiales internas y externas a través de este sistema.

Prohibido recibir o generar comunicaciones por fuera del sistema de Gestión Documental ORFEO.

Los usuarios que requieran acceso para el manejo de correspondencia por este sistema, deben solicitar a través de su coordinador la inscripción al curso de capacitación dispuesto en la plataforma de la entidad al proceso de Tecnologías de la información, antes de solicitar datos de acceso a este sistema.

17. Políticas De Disponibilidad De Información, Gestión Y Continuidad Del Negocio

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Tecnologías de la Información y Comunicaciones - TICs, debe realizar un plan de continuidad del negocio, con el fin de mantener la disponibilidad de los sistemas de información relevantes, misionales y críticos de la entidad y generar procesos de recuperación o restablecimiento de manera oportuna, ante fallas, interrupciones e incidentes de seguridad.

17.1 Políticas De Copia Y Resguardo De Información

La E.S.E. Hospital Universitario San Rafael Tunja, a través del proceso de Tecnologías de la Información y Comunicaciones - TICs, identifica y clasifica los activos de información, de acuerdo a su valor, relevancia de los sistemas de información y que resulten críticos para la continuidad de las operaciones de la entidad, con el fin de generar planes periódicos de copias de seguridad, resguardo y restauración de los mismos, manteniendo su identificación, protección, integridad y disponibilidad de los medios con dicha información.

El proceso de Tecnologías de la Información identifica la información a respaldar respecto de bases de datos, sistemas de información, configuración de servidores, configuración de dispositivos de red, estaciones de trabajo con información crítica para la entidad, y demás informaciones que se consideren que se deben respaldar.

El proceso de Tecnologías de la Información y Comunicaciones, debe generar plan de copias de seguridad, programación y ejecución de las mismas, de los sistemas identificados, teniendo en cuenta periodicidad de las copias, tipo de información a respaldar, la frecuencia de la copia, ubicación física, retención de las mismas; así como los horarios en los que resulten más adecuados entorno al rendimiento de dichos sistemas de información S-PR-21 Procedimiento Copias De Seguridad De Sistemas De Información.

El proceso de Tecnologías de la Información debe realizar monitoreo de la generación de copias de seguridad y de los espacios disponibles en disco, y hacer los ajustes que resulten convenientes y de acuerdo al formato S-F-40 Formato Solicitud De Copias De Seguridad y S-PR-21 Procedimiento De Copias De Seguridad De Sistemas De Información.

El proceso de Tecnologías de la Información debe proveer y disponer de los recursos necesarios de los medios de almacenamiento que permitan los planes de copias, restauración y resguardo; cuando sea solicitada mediante formato S-F-05 Formato de Mantenimiento Preventivo o Correctivo de Software.

Cada Unidad Productora de Documentos -UPD es responsable de organizar y de realizar una copia de seguridad por red en equipo diferente de donde se encuentra la información de acuerdo a Tablas de Retención Documental -TRD del área. Esta información deberá estar organizada de acuerdo a su TRD. La copia será de manera trimestral mínimo o cuando el coordinador lo considere pertinente siempre que no supere los 3 meses. La copia generada por las UPD se respaldará en cinta o el medio previsto por el encargado del proceso de Tecnologías de la Información siempre y cuando se encuentre debidamente organizada conforme a la TRD respectiva. La ruta y carpeta a guardar la copia en equipo diferente será: c:\copiatrd_nombre_area\fecha (ddmmaaaa).

El proceso de Tecnologías de la Información, en caso de retiro de un funcionario, contratista o personal de la institución que tenga asignado equipo de cómputo, deberá realizar copia de la seguridad de la información contenido en el equipo, previa solicitud del área a la que pertenece.

17.2 Políticas De Restauración De Copias De Seguridad De Información

El proceso de Tecnologías de la Información establecerá un procedimiento y plan de restauración de copias para los sistemas de información respaldados, de manera periódica, con el fin de asegurar su confiabilidad de los medios y copias.

17.3 Gestión Del Cambio

Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos, que pueden afectar la operación del negocio de acuerdo con los lineamientos establecidos.

Previo a cualquier modificación sobre los sistemas de información en producción, que implique o pueda tener una afectación del servicio, debe ser comunicado al coordinador del área de Tecnología, para realizar evaluación y control de cambio a realizar. En caso de ser necesario, se deberá contar con autorización y notificación formal a través de correo o circular administrativa según lo indique el Coordinador.

La Gestión de Cambios debe contener como mínimo la identificación, justificación, el alcance, autorización y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica. Adicionalmente contar con un plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos pueden generar, y un plan alternativo para revertir los cambios no satisfactorios, eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio.

17.4 Ciclo De Vida De Los Sistemas De Información

La E.S.E. Hospital Universitario San Rafael Tunja, busca definir y gestionar las etapas que deben surtir los Sistemas de Información desde la definición de requerimientos hasta el despliegue, puesta en funcionamiento y uso, para tener un esquema claro y documentado de las etapas para la gestión de los sistemas de información durante el ciclo de vida, está identificado en el S-M-16 Ciclo de Vida de los Sistemas de Información HUSRT.

17.5 Separación De Los Ambientes De Desarrollo, Prueba Y Producción

La E.S.E Hospital Universitario San Rafael Tunja, ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

Dado lo anterior, los ambientes establecidos por la E.S.E Hospital Universitario San Rafael Tunja se definen así:

Ambiente de Desarrollo: Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.

Ambiente de Pruebas: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos para realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de la E.S.E Hospital Universitario San Rafael Tunja.

Ambiente de Producción: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la E.S.E. Hospital San Rafael Tunja. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, base de datos, programas ejecutables o compilados.

A través de las políticas de control de acceso físico y lógico definidas por la Institución, se controla el acceso a cada uno de los ambientes. Adicionalmente, los ambientes de desarrollo, pruebas y producción están separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

El proceso de TICS debe proveer gradualmente los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados, iniciando por los sistemas críticos en los cuales se realizan cambios con más frecuencia.

Igualmente debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así mismo que los menús muestren los mensajes de identificación apropiados en cada ambiente para reducir los riesgos de error.

17.6 Aceptación De Sistemas De Información

El proceso de TICS debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software que estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades de la E.S.E. Hospital San Rafael Tunja. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y pruebas funcionales establecidas.

Todo sistema que se implemente o instale en la E.S.E. Hospital San Rafael Tunja, sea comprado o en comodato, debe tener la capacidad de integrarse al sistema corporativo y será evaluado por el proceso de TICS para verificar su buen funcionamiento y los procedimientos de

mantenimiento y soporte.

17.7 Gestión De La Tecnología -TI

De acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información y Comunicaciones, en adelante PETI es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que una institución pública hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.

Para más información, consultar la guía técnica sobre la G.ES.06 Guía técnica de cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI. y el S-M-03 MANUAL PLAN ESTRATEGICO TECNOLOGIA DE LA INFORMACION PETI.

Tecnologías de la Información y Comunicaciones, debe incorporar e implementar los procedimientos en seguridad de la información que apliquen según el Modelo de Seguridad y Privacidad –MSPI de Gobierno Digital. Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.

Para la formulación de los planes de acción institucional, el proceso de Tecnologías de la Información y Comunicaciones debe tener en cuenta la formulación de planes y actualización anual, según decreto 612 de 2018 y el Manual Operativo del Modelo de Planeación y Gestión -MIPG:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información

17.8 Gestión De Incidentes De Seguridad Y Privacidad De La Información

Los incidentes de seguridad de la información que se identifique por el personal o usuarios del sistema de información, se deben reportar de inmediato al Líder de Seguridad del proceso de Tecnología de la información y comunicaciones –TICs, dónde se detalle la información acerca del incidente de manera completa y precisa, indicando el lugar, la fecha y detalle de los hechos ocurridos. Para lo cual se debe diligenciar el formato de S-F-24 Gestión de incidentes en seguridad y privacidad de la información.

El área de Tecnología de la Información debe definir un proceso que permita realizar la identificación, el reporte, análisis, clasificación, contención y recuperación de los incidentes ocurridos en seguridad de la información; llevando un registro y documentación de las soluciones encontradas; de manera que permita facilitar una recuperación rápida y eficientes frente a los incidentes reportados minimizando la pérdida de información y la interrupción de los servicios.

18. EVALUACIÓN

La E.S.E. Hospital Universitario San Rafael Tunja debe realizar la evaluación de las políticas de seguridad anualmente o cuando se considere necesario y realizar las actualizaciones que resulten después de evaluar los incidentes de seguridad ocurridos, los hallazgos de auditorías de seguridad de la información, frente a cambios que afecten la seguridad de la Entidad.

La E.S.E. Hospital Universitario San Rafael Tunja debe evaluar los riesgos identificados y la tolerancia al riesgo, para determinar su tratamiento y documentación en un Plan de Tratamiento de Riesgos.

La E.S.E. Hospital Universitario San Rafael Tunja, evalúa los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura tecnológica para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

19. DEFINICIONES Y/O GLOSARIO

Activo. Según ISO/IEC 13335, Todo lo que tiene valor para la Organización. Hay varios tipos de activos entre los que se incluyen: Información, Software, como un programa de cómputo; Físico, como un computador; Servicios, Personas, sus calificaciones, habilidades y experiencia; Intangibles, tales como la reputación y la imagen.

Activo de Información. Recurso tangible e intangible del o de los sistemas de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Entendiendo por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la entidad.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad.

Amenaza. Son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de información, puede ser de dos tipos: Amenazas internas y Amenazas externas.

Análisis del riesgo. Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Aplicaciones. Son programas de computador que están diseñados con capacidades lógicas y matemáticas para procesar información. El término Aplicación se utiliza para agrupar un conjunto de programas que responden a requerimientos particulares del negocio o área de negocio.

Backup. Copia idéntica de algo, copia de seguridad o copia respaldo de algo.

Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Custodio: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

Directorio activo: Se refiere a la función de un servidor principal que controla y administrar el acceso de las cuentas de usuario y recursos en red, bajo un esquema de organización de equipos en red conocido como dominio Windows o Directorio Activo. Una vez creado el usuario y este se autentica con las credenciales otorgadas, le permite el acceso al equipo y aplicaciones dispuesta de manera local y en red.

Dato. Representación de una información de manera adecuada para su tratamiento por un ordenador o Computadora. Es la unidad básica de la información.

Diagnóstico. es el análisis que se realiza para determinar cualquier situación y cuáles son las tendencias. Esta determinación se realiza sobre la base de datos y hechos recogidos y ordenados sistemáticamente, que permiten juzgar mejor qué es lo que está pasando.

Dominio de seguridad. Son agrupaciones de los objetivos y controles de seguridad de activos de información. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005, que contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios de seguridad.

Equipo de Salud. Para efectos de la historia clínica, son los Profesionales, Técnicos y Auxiliares del área de la salud que realizan la atención clínico asistencial directa del Usuario y los Auditores Médicos de Aseguradoras y Prestadores responsables de la evaluación de la calidad del servicio brindado.

Evaluación del riesgo. Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evaluación de la Amenaza. es el proceso mediante el cual se determina la probabilidad de ocurrencia y la severidad de un evento en un tiempo específico y en un área determinada. Representa la ocurrencia estimada y la ubicación geográfica de eventos probables.

Evento de seguridad de la información. Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida.

Firma Electrónica. Corresponde a métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permitan identificar a una persona en relación con un mensaje, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, teniendo en cuenta todas las circunstancias del caso, así como cualquier acuerdo pertinente. (Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7 de la ley 527 de 1999 sobre la firma electrónica y otras disposiciones).

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Habeas Data. Es el derecho constitucional fundamental que le permite a los ciudadanos conocer, actualizar y rectificar la información que se haya recogido sobre ellos en archivos y bancos de datos.

Hardware. Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Historia Clínica. Es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

Historia Clínica para efectos archivísticos. Se entiende como el expediente conformado por el conjunto de documentos en los que se efectúa el registro obligatorio del estado de salud, los actos médicos y demás procedimientos ejecutados por el equipo de salud que interviene en la atención de un paciente, el cual también tiene el carácter de reservado.

Incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y gestionar los fallos de seguridad de la información. (ISO/IEC 27000).

Información. Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Informática. Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores o computadoras.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Internet. Conjunto de redes de ordenadores compuesta de miles de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza el

protocolo TCP/IP para proporcionar comunicaciones de ámbito mundial. Se trata de un sistema de redes informáticas interconectadas mediante distintos medios de conexión, que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a plataformas digitales, páginas web, comercio electrónico, entre muchos otros más.

Impacto. Es la consecuencia negativa sobre un activo de la materialización de una amenaza.

Incidente de seguridad de la información. Evento que atenta contra la confidencialidad, integridad o disponibilidad de la información y los recursos tecnológicos. Evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento. Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Medios extraíbles. Son aquellos medios de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla como unidades externas de CD-DVD. El término medio extraíble también puede hacer referencia a algunos dispositivos de almacenamiento extraíbles, como memorias USB, discos duros externos o tarjeta de memoria.

MSPI. Modelo de Seguridad y privacidad de la Información por sus siglas MSPI, dispuesto a aplicar por las entidades del estado en el marco De la Política de Gobierno Digital.

Normas ISO 27000. El estándar ISO 27000 apunta a exigir niveles concretos y adecuados de seguridad informática, niveles necesarios para las empresas que compiten a través del comercio electrónico y que por lo tanto tienen que exponer sus infraestructuras de información.

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

PGR. Plan de Gestión de Riesgo.

Phishing. Es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales, software mal intencionado o incluso utilizando también llamadas telefónicas.

Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Política. Intención y dirección general expresada formalmente por la gerencia.

Principios de seguridad:

- **Confidencialidad.** Es la propiedad de la información, por la que se gestiona que es accesible únicamente a personal autorizado a conocer la información.
- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

PRD. Plan de Recuperación de Desastres.

Privacidad de la información: 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 Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietario de la información (titular): Es la unidad organizacional o proceso donde se crean los activos de información.

Puertos. Los puertos son conexiones eléctricas para conectar los periféricos (ratón, teclado, impresora) al ordenador. De esta forma el procesador puede comunicarse y controlar dichos periféricos.

Riesgo. Posibilidad o probabilidad de que se produzca un impacto sobre algún activo de la información que pueda incurrir en pérdidas del patrimonio. El riesgo es igual al producto entre la probabilidad y el impacto: Riesgo = Probabilidad X Impacto.

Red de Área Local. También conocida con el nombre de red LAN (por las siglas en inglés de Local Area Network). Hace referencia a la red de datos de manera local en la misma ubicación, casa o edificio, que permite conectarse a los sistemas de información y a otras redes como Internet.

Seguridad de la información. Hace referencia a todos los procedimientos y controles que son implementados por las personas y organizaciones para prevenir, proteger y resguardar la información del acceso y utilización no autorizado. Se refiere también al funcionamiento del conjunto de componentes (equipos informáticos, software especializado, recurso humano y redes de datos) que tienen por objeto el manejo, procesamiento, organización, almacenamiento y recuperación de la información para apoyar la toma de decisiones y el mejoramiento de los procesos organizacionales.

SGSI: Sistema de Gestión de la Seguridad de la Información, es utilizada para referirse a la gestión de los procesos y mecanismos de control que son utilizados para custodiar y proteger de amenazas la información sensible de las organizaciones. Los SGSI permiten a la gerencia de las organizaciones determinar con objetividad que información requiere ser protegida, por qué debe ser protegida, de qué debe ser protegida y como protegerla mediante la planificación e implantación de políticas, procedimientos y controles que mantengan siempre el riesgo por debajo del nivel asumible por la propia organización.

Sistema de Información: Un sistema de información (SI) es un conjunto de elementos como procesos, computadores, servidores, redes, datos, equipos con software de sistema operativo, con software de aplicaciones y sistemas de bases de datos; orientados al tratamiento y administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

Sistema Operativo. Es un conjunto de programas que administran los recursos del sistema (Recursos: Programas, archivos, memoria RAM, periféricos, disco duro, etc.). Ejemplo de Sistemas operativos son: DOS, Windows, Linux, Unix, Max Os, Android.

Software. Componente del ordenador que hace funcionar el conjunto de dispositivos físicos del hardware. El software está formado por los datos y programas que dotan de funcionalidad al hardware del ordenador.

Software de Aplicación: Es un conjunto de programas diferente al software del sistema operativo, éstos se encargan de manipular la información que el usuario necesita procesar, son programas que desarrollan una tarea específica y cuya finalidad es permitirle al usuario realizar su trabajo con facilidad, rapidez, agilidad y precisión.

Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

TICS: Tecnologías de la Información y las Comunicaciones.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

UPS. Es una fuente de suministro eléctrico que posee una batería con el fin de seguir generando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida) y en inglés UPS (Uninterruptible Power Supply).

Usuario: Es aquella persona que usa algo para una función en específico.

VPN: Red virtual privada por sus siglas en inglés Virtual Private Network.

Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.

Virus Informáticos. Son programas maliciosos (malware) que “infectan” a otros archivos del sistema con la intención de modificarlo o dañarlo.

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

Base De Datos: conjunto organizado de datos personales que sea objeto de tratamiento.

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

Dato Público: es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la Ley 1581 de 2012. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato Semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la Ley 1581 de 2012.

Dato Privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

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

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

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

Titular: persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión

Aviso De Privacidad: comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales

Habeas Data: es el recurso legal a disposición de todo individuo que permite acceder a un banco de información o registro de datos, que incluye referencias informativas sobre sí mismo. El sujeto tiene derecho a exigir que se corrijan parte o la totalidad de los datos en caso de que éstos le generen algún tipo de perjuicio o que sean erróneos.

Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un documento por el encargado por cuenta del responsable

20. DOCUMENTO SOPORTE /ANEXOS

Este documento no requiere documentos de soporte

21. BIBLIOGRAFÍA

- Procedimientos De Seguridad de La Información

https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

- Guía para la Gestión y Clasificación de Activos de Información

http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

- Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información

http://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- Modelo de Seguridad y Privacidad de la Información

http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

22. CONTROL DE CAMBIOS

| CONTROL DE CAMBIOS | | | |
|--------------------|------------|---------------------------------|---|
| VERSIÓN | FECHA | ELABORÓ | DESCRIPCIÓN DEL CAMBIO |
| 00 | 07/07/2017 | Jorge Armando Figueredo Malagón | Versión Original |
| 01 | 20/12/2018 | Alfredo Orjuela Peña | Se estructuró el documento, actualizando y adicionando las políticas de seguridad de la información, incluyendo las políticas de Historia Clínica |
| 02 | 01/11/2019 | Marbiz Said Ducuara Amado | Se ajustaron las definiciones pagina 12 y numeral 9.3 descrito en la página 19 y página 20 |
| 03 | 06/12/2021 | Guillermo Otálora Luna | Se incluye Políticas del uso de computadores personales en la institución |
| 04 | 21/12/2022 | Olga Lucia Ospina Cely | Se ajusta Política en los siguientes numerales: 10.5 Dispositivos Móviles, 17.1 Políticas De Copia y Resguardo De Información en estos puntos se retiro el formato S-F-22 el cual esta en estado Obsoleto y se remplazo por el S-F-40 Formato Copias de seguridad en estado Vigente. se adiciono el numeral 10.7 Políticas De Tratamiento Y Protección De Datos Personales. |

| REVISÓ | APROBÓ |
|--|--|
| Monica Maria Londoño Forero Asesor Desarrollo de Servicios | German Francisco Pertuz Gonzalez Gerente |

ESTE DOCUMENTO ES PROPIEDAD DE LA ESE HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA Y LA INFORMACION QUE POSEE ES CONFIDENCIAL. SU REPRODUCCIÓN ESTARÁ DADA A TRAVÉS DE COPIAS AUTORIZADAS