E.S.E. HOSPITAL UNIVERSITARIO SAN RAFAEL DE TUNJA		
CÓDIGO: S-M-02	MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION	
VERSIÓN: 008		FECHA: 2024-11-26

TABLA DE CONTENIDO

1. INTRODUCCIÓN Y/O JUSTIFICACIÓN

La E.S.E Hospital Universitario San Rafael de 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 de 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 de 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 Modelo de Seguridad y Privacidad de la Información- 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, confidencialidad.

3. OBJETIVOS ESPECÍFICOS

- Identificar los lineamientos del Modelo de Seguridad y Privacidad de la Información- 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 Modelo de Seguridad y Privacidad de la Información- MSPI, acorde a los activos, el alcance y planeación estratégica que garantice la continuidad del negocio.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.
- 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 incumpliendo de estas.
- Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la entidad.

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 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

El líder de seguridad de la información o quien designe por la Coordinación del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, de la E.S.E. Hospital Universitario San Rafael de Tunja.

7. RECURSOS, MATERIALES, INSUMOS Y EQUIPOS

- **Humanos:** Funcionarios, profesionales y tecnicos de TIC.
- **Financieros:** De acuerdo a la disponibilidad asignada para determinada vigencia.
- **Técnicos o recursos tecnologicos**: Computadoras, servidores, teléfonos, sistemas de seguridad, como intangibles sistemas operativos, programas de ciberseguridad, bases de datos, redes internas, entre otros.

8. DESCRIPCIÓN/ IMPLEMENTACIÓN

ESTABLECIMIENTO DE POLITICAS ESPECÍFICAS

8.1 Política de organización Interna de la seguridad de la información

8.1.1 Objetivo

La E.S.E. Hospital Universitario San Rafael de Tunja, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité de Gestión y Desempeño Institucional a través del cual se lleva seguimiento de tareas de seguridad de la información.

Las políticas de seguridad de la información se deben verificar, definir, implementar, revisar y actualizar para mantener salvaguardados los activos de la entidad.

Toda solicitud, requerimiento, adquisición de bienes y/o servicios donde se incluyan equipos informáticos, desarrollo, adquisición de software serán revisados, validados y liderados por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, en cuanto a lo que se refiere a software deben cumplir con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

8.1.2 Lineamientos generales

Los activos de información deben estar bajo la responsabilidad del responsable del activo, para evitar conflicto y reducir oportunidades de modificación (intencional o no), no autorizada o mal uso de los activos de información de la E.S.E. Hospital Universitario San Rafael de Tunja.

- El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe mantener y documentar los contactos con autoridades (Policía, bomberos,Fiscalia etc.) u otros especializados, con el fin de contactar en caso de que se presente un incidente de seguridad de la información y requiera de asesoría externa.
- Los proyectos que se desarrollen en la E.S.E. Hospital Universitario San Rafael de Tunja deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- En cualquier caso, los proyectos desarrollados por la E.S.E. Hospital Universitario San Rafael de Tunja deben estar alineados a las políticas de seguridad contenidas en el presente manual.

8.1.3 Anexos

- S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
- S-F-46 MATRIZ DE ACTIVOS DE INFORMACIÓN.
- S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
- S-F-03 ENTREGA DE EQUIPOS

8.1.4 Asignación de responsabilidades para la seguridad de la información.

Todo el personal que tenga acceso a la información de la E.S.E. Hospital Universitario San Rafael de Tunja, es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este manual; entre ellos están: funcionarios, proveedores, personal en formación y en desarrollo de prácticas académicas, contratistas, terceros y visitantes.

La Gerencia de la E.S.E. Hospital Universitario San Rafael de Tunja, es el ente máximo y se encuentra representado por los integrantes del Comité Institucional de Gestión y Desempeño de la E.S.E. Hospital Universitario San Rafael de Tunja, es responsable de revisar y aprobar la política de Seguridad de la Información y Ciberseguridad; revisar la eficacia de la implementación de la política de Seguridad; proporcionar y avalar los recursos necesarios para el desarrollo e implementación de iniciativas de Seguridad; comunicar la importancia de una gestión eficaz de la Seguridad de la Información y seguridad digital; promover el cumplimiento de las políticas y normas definidas en el *Sistema de Gestión* de la *Seguridad de la Información* -SGSI.

El Comité Institucional de Gestión y Desempeño, es un grupo interdisciplinario conformado al interior de la E.S.E. Hospital Universitario San Rafael de Tunja, es responsable de revisar y aprobar las políticas de Seguridad de la Información y seguridad digital, revisar los lineamientos definidos por Seguridad de la Información; revisar la implementación del *Sistema de Gestión* de la *Seguridad de la Información* -SGSI en Entidad; realizar el seguimiento a la gestión de Seguridad de la Información y seguridad digital; apoyar la implementación de los lineamientos en la entidad en temas de Seguridad de la Información y Ciberseguridad;

promover la sensibilización y comunicación al interior de la entidad del Sistema de Gestión de Seguridad de Información

El Comité Institucional de Gestión y Desempeño, este comité asumiera el rol encomendado por la norma ISO 27001:2013, denominado Comité de Seguridad de la información.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, es el líder de la implementación y gestión de los controles de seguridad y ciberseguridad que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad que se encuentre bajo la coordinación del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, es responsable definir políticas, procedimientos de gestión de accesos lógicos y esquema, metodología de construcción de roles y perfiles para los accesos a plataformas e infraestructura de la entidad; definir procedimientos de gestión de logs; definir líneas base, guías de aseguramiento, etc. para aseguramiento de los sistemas; definir la metodología y procedimientos del ciclo de vida de desarrollo de software incluyendo requerimientos de seguridad en cada etapa; definir la estrategia de respaldo de información; definir políticas y procedimientos de gestión de cambios; definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la entidad Implementación de planes de remediación de vulnerabilidades; adquirir e implementar herramientas de gestión de logs y correlación; adquirir e implementar tecnologías de seguridad; adquirir, implementar y configurar la red y las plataformas tecnológicas de acuerdo con el diseño propuesto; realizar los ajustes/mejoras necesarias en el proceso de desarrollo de software; ajustes o mejoras a la estrategia de respaldo de información.

Los propietarios de los Activos de Información, son los líderes de proceso los que tienen la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el procedimiento S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN e instructivo S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad; realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida; mantener actualizada la matriz de activos de información S-F-46 MATRIZ DE ACTIVOS DE INFORMACIÓN, definida por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, validando los controles de acceso asignado a los activos; identificar riesgos asociados con la Seguridad de la Información en los procesos de los cuales son responsables o tienen participación; reportar oportunamente eventos o incidentes de Seguridad de la Información.

8.1.5 Segregación de tareas.

Todo el personal que tenga acceso a la información de la E.S.E. Hospital Universitario San Rafael de Tunja, debe tener claramente definidos sus deberes frente a la gestión de la Seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.

En todos los sistemas de información de la Entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

De acuerdo a los lineamientos dados en el manual S-M-15 ESQUEMA GOBIERNO, que determina el esquema de gobernabilidad de las tecnologias de información y comunicación y define los roles y procesos necesarios para soportar la ejecución de las actividades en el marco de dominio de TI y defini los paframetros para restringir y controlar la asignacion y usu de derechos de acceso privilegiado de acurdo a lo establecido en el procedimiento S-PR-12 GESTION Y ADMINISTRACION DE DIRECTORIO ACTIVO.

8.1.6 Contacto con las autoridades.

La E.S.E. Hospital Universitario San Rafael de Tunja, en cabeza del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control (Procuraduría General de la Nación, Contraloría General de Boyaca fiscalía general de la Nación, Policía Nacional, Comando Conjunto Cibernético, MINTIC.

Dado el caso de presentarse ataques cibernéticos es el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, el encargado de denunciar anomalías debera establecer contacto con las autoridades, acorde al procedimiento de la institución S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Autoridades de Seguridad de la Información	Organización	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	https://caivirtual.policia.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing		
Ingeniería Social		
Respuesta a Emergencias Cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
		https://cc-csirt.policia.gov.co
	Ministerio de las Tecnologías de la Información y las Comunicaciones	01-800-0914014
	– MINTIC.	https://www.mintic.gov.co
	Alta Consejería para las TIC – Gobierno Digital.	http://ticbogota.gov.co/ http://estrategia.gobiernoenlinea.gov.co

8.1.7 Contacto con grupos de interés especial.

La E.S.E. Hospital Universitario San Rafael de Tunja, a través del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y amenazas nuevas.

Grupo de interés Especial	Contacto	Correo
Ministerio de Tecnologías de la Información y las comunicaciones	01-800-0914014	
Infraestructura crítica - Comando Conjunto Cibernético (CCOC)	57 (1) 315 0111 Ext. 21131	info@ccoc.mil.co
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	57 (1) 315 0111 Ext. 21131	ponal.csirt@policia.gov.co
COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	(+ 571) 295 98 97	contacto@colcert.gov.co

8.1.8 Seguridad de la información en la gestión de proyectos.

La seguridad de la información se debe articular al procedimiento de gestión de proyectos de la E.S.E. Hospital Universitario San Rafael de Tunja, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.

Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, asegurar que se sigan las siguientes directrices:

a. Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar y estimar los controles necesarios.

b. Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

Dispositivos para la movilidad y teletrabajo

La E.S.E. Hospital Universitario San Rafael de Tunja, a traves del area de Tecnologias de la Información -TIC, define los dispositivos moviles que se pueden utilizar dentro de las instalaciones, previa solicitud a traves de la mesa de ayuda por lider del proceso o area.
Las directrices para el uso de dispositivos móviles personales, como teléfonos inteligentes, tabletas y computadoras portátiles, permiten asegurar la protección de la información y la optimización de la productividad de los empleados.
Los equipos portatiles que no son propiedad de la Entidad, no deben estar incluidos en el dominio de la E.S.E. Hospital Universitario San Rafael de Tunja, para conectarse a los servicios de la red de datos.
La asignación de cualquier dispositivo movil de propiedad de la Entidad, se realizara a traves del formato S-F-03 ENTREGA DE EQUIPOS, y su custodia, almacenanamiento y salida de las instalaciones de la entidad es responsabilidad del lider del proceso.

Aplica a todos los colaboradores de la entidad que utilicen dispositivos móviles personales, incluyendo teléfonos inteligentes, tabletas y computadoras portátiles, en el desempeño de sus funciones.

Esto incluye el acceso a correos electrónicos, sistemas de información y datos sensibles de la organización. La política abarca el uso de dichos dispositivos en cualquier entorno relacionado con el trabajo, ya sea en las instalaciones de la entidad, en ubicaciones remotas o durante actividades fuera de la entidad.

Se busca garantizar la seguridad de la información y el cumplimiento de las políticas de la entidad y fomentar un ambiente de trabajo productivo y responsable.

Normas de Uso:

- Los dispositivos móviles deben ser utilizados principalmente para actividades relacionadas con el trabajo.
- El uso personal de los dispositivos debe ser limitado y no debe interferir con las responsabilidades laborales.
- Está prohibido el uso de aplicaciones y servicios no autorizados que puedan comprometer la seguridad de la información.

Seguridad y Privacidad:

- Todos los dispositivos deben estar protegidos con contraseñas fuertes y autenticación de dos factores.
- Los datos sensibles deben ser y almacenados de manera segura.
- Los colaboradores deben informar inmediatamente cualquier pérdida o robo de dispositivos.

Para el uso de los dispositivos móviles, de uso personal y que se utilicen para trabajar en la E.S.E. hospital universitario san Rafael de Tunja, dentro o fuera de sus instalaciones o sedes se debe tener en cuenta:

- El dispositivo debe estar protegido a través de usuario y contraseña de ingreso.
- El ingreso de dispositivos móviles (tabletas y computadoras portátiles) a las instalaciones de la entidad, debe ser registrado en la bitácora de ingreso de equipos de cómputo en la recepción.
- El uso de Dispositivos móviles debe ser autorizado por el Subgerente respectivo, jefe inmediato y/o supervisor del contrato, en el formato **[S-F-60] VERIFICACION DE REQUISITOS PARA EQUIPOS DE COMPUTO EXTERNO**
- La información de carácter institucional contenida en cualquier Dispositivo móvil debe estar almacenada en un cuenta de OneDrive asignada por el área de TI.
- Con el fin de prevenir riesgos asociados a la pérdida o fuga de información aplicados a los dispositivos móviles autorizados, no se podrá almacenar información institucional de manera local en los dispositivos móviles.
- No es permitido almacenar en dispositivos personales información confidencial de la entidad.
- Una vez se termine el contrato, obra o labor, el colaborar debe informar al área de TI, la entidad podrá realizar el borrado completo de todos los datos e información institucional que se encuentren en el dispositivo móvil, si considera que es necesario, **sin contar con el consentimiento del propietario del dispositivo.**

- En el caso de teléfonos inteligentes que usen correo electrónico, el área de TI también deberá deshabilitar la cuenta.
- Para la conexión del Dispositivo a la red institucional, debe ser verificado y cumplir con lo establecido en el formato **S-F-60 VERIFICACION DE REQUISITOS PARA EQUIPOS DE COMPUTO EXTERNOS**
- Es responsabilidad de colaborador, la protección de la información de la entidad que tenga bajo su manejo en estos dispositivos, la cual no debe ser compartida por ningún medio fuera de la red institucional.
- El propietario del dispositivo, es responsable de las actualizar el antivirus periódicamente.
- Si se utiliza el dispositivo móvil en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas, así como evitar la conexión a redes públicas, las cuales no cuentan con ningún tipo de monitoreo o seguridad y representan un riesgo para la seguridad de la información.
- En caso de pérdida, robo del dispositivo, el incidente o evento de seguridad deberá ser reportado a la entidad a través de la mesa de servicio GLPI.
- La entidad no pagará y/o reconocerá a los colaboradores, ningún valor o subsidio por el uso con fines laborales o pérdida o daño de los dispositivos.
- En el caso de uso del correo electrónico a través de teléfono inteligente, es responsabilidad del colaborador su buen uso y seguridad de la información allí contenida.
- El propietario del dispositivo móvil, al conectarse a la red institucional, acepta los controles establecidos en el **S-M-02 MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD.**
- Una vez se autorice la conexión de un dispositivo móvil a la red de dominio de la entidad, la entidad tendrá acceso para visualizar y monitorear los datos, que hayan sido almacenados, transferidos o procesados en el mismo.
- El colaborador se compromete a hacer uso productivo y seguro de la red de dominio de la entidad.
- Todos los incidentes o y/o eventos de seguridad relacionados con dispositivos móviles, deben ser reportados inmediatamente a través de la mesa de servicios GLPI de acuerdo al procedimiento **S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.**

Teletrabajo

El área de Tecnología de la Información establece y divulga el uso de la información y los servicios tecnológicos necesarios para garantizar el adecuado funcionamiento de la modalidad de Teletrabajo y deberá verificar que los equipos personales cumplan con los lineamientos referentes a seguridad de la información, teniendo en cuenta lo enmarcado en la normatividad, así mismo se deben tener en cuenta la revocación de servicios cuando el Trabajador no continué realizando actividades de Teletrabajo, previa solicitud a traves de la mesa de servicios, autorizada por el lider del proceso o área.

Para los casos de teletrabajo, el acceso a la red y/o sistemas de información de la entidad se debe realizar por medio de conexión a una VPN (Red Privada Virtual) como herramienta esencial para proteger la información y garantizar un acceso seguro a la red de la entidad, especialmente en entornos de teletrabajo.

La VPN (Red Privada Virtual) asegura la seguridad de la información mediante diversas funciones, como:

1. Cifra la conexión a internet, lo que protege los datos que se envían y reciben, evitando que terceros puedan interceptarlos.
2. Oculta la dirección IP del usuario, lo que dificulta el seguimiento de su actividad en línea.
3. Permite a los empleados acceder a la red de la empresa de manera segura desde ubicaciones remotas, facilitando el teletrabajo.
4. Establece un túnel seguro entre el dispositivo del usuario y el servidor de la empresa, asegurando que la comunicación sea confidencial.
5. Permite el acceso a contenido restringido en ciertas regiones, ya que se puede simular que el usuario está en otra ubicación.

Los Trabajadores en modo Teletrabajo o cualquier persona que requiera conexión vía VPN se les deberán aplicar los permisos de navegación y control de acceso limitado a su perfil o privilegios y se llevará registro de su conexión.

Esta conexión debe ser solicitada a través de la mesa de servicios GLPI de acuerdo a lo definido en el procedimiento S-PR-29 SOLICITUD PARA LA CREACIÓN DE LAS VPN en el FORMATO S-F-59 SOLICITUD DE ASIGNACIÓN DE CREDENCIALES Y RECURSOS DE ACCESO REMOTO Y/O INTERNET, en donde el proceso de tecnologías de la información realiza la verificación de los requisitos mínimos requeridos para la conexión por medio el formato S-F-60 VERIFICACION DE REQUISITOS PARA EQUIPOS DE COMPUTO EXTERNOS.

8.2 Política de seguridad relativa a los recursos humanos

8.2.1 Objetivo

Asegurar, reducir el riesgo de robo, fraude y mal uso de los equipos de cómputo, sistemas de información e información, que los funcionarios de planta, contratistas y terceros de la E.S.E. Hospital Universitario San Rafael de Tunja, que son asignados para el cumplimiento de sus funciones.

8.2.2 Lineamientos generales

- Todos los funcionarios de planta, contratistas y terceros que presten sus servicios a la E.S.E. Hospital Universitario San Rafael de Tunja, a los que se brinde información reservada o clasificada, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de confidencialidad y no divulgación.
- Este acuerdo debe incluir la aceptación del Manual de políticas y lineamientos en seguridad y privacidad de la información y ciberseguridad, el tratamiento de la información de la Entidad, en los términos de la Ley 1581 de 2012, 1712 de 2014 y las demás normas que la adicionen, modifiquen, reglamenten o complementen.
- Se debe contar con un programa de capacitación y sensibilización en Seguridad de la Información, el cual debe contemplar en su contenido: políticas y procedimientos, roles y responsabilidades, metodología de activos, metodología de riesgos, marco legal y regulatorio de Seguridad de la Información.
- Todo colaborador debe recibir una inducción sobre las políticas y procedimientos de Seguridad de la Información al iniciar su relación contractual con la E.S.E. Hospital Universitario San Rafael de Tunja.
- El proceso de contratación de personal debe incluir la verificación de antecedentes disciplinarios y estudio de seguridad del candidato.
- Establecer control de las novedades de los colaboradores de su área tales como: retiros, vacaciones, cambio de área entre otros, asociadas con su relación contractual con la E.S.E. Hospital Universitario San Rafael de Tunja.
- Todos los colaboradores de la E.S.E. Hospital Universitario San Rafael de Tunja, deben cumplir con un proceso de selección acorde con la criticidad de la información que van a manejar.

8.2.3 Anexos

- TH-PR-08 SELECCIÓN , INGRESO Y PROMOCION DE PERSONAL
- TH-PR-17 VINCULACION LABORAL
- TH-F-45 FORMATO DE VERIFICACIÓN DE REQUISITOS
- TH-PR-47 VALIDACIÓN HOJA DE VIDA CONTRATISTAS
- TH-F-72 FORMATO DE SEGUIMIENTO CONDUCTOR DE AMBULANCIA Y MENSAJERO.
- TH-F-71 ACTA DE COMPROMISO DE INDUCCIÓN Y REINDUCCIÓN.
- TH-F-51 ACUERDO DE CONFIDENCIALIDAD EN EL MANEJO Y TRATAMIENTO DE LA INFORMACIÓN- PERSONAL DE PLANTA.
- C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN PROCEDIMIENTO COPIAS

8.2.4 Antes de la contratación.

No obstante que la vinculación al sector público se rige por la Comisión Nacional del Servicio Civil (CNSC) por méritos y validación de algunos soportes académicos y laborales. Es importante que el proceso de Gestión de Talento Humano proporcional a las responsabilidades o al manejo de información sensible de la entidad, establece el proceso de verificación de los antecedentes de los candidatos que aspiran a un cargo, el cual se debe llevar a cabo de acuerdo con las leyes y reglamentos, siendo

proporcionales a los requisitos dentro de la E.S.E. Hospital Universitario San Rafael de Tunja, a la clasificación de la información que va a tener acceso y, a los riesgos percibidos.

Para el personal de Planta, desde el proceso de Gestión Talento Humano, se cuenta con los procedimientos TH-PR-08 SELECCIÓN, INGRESO Y PROMOCION DE PERSONAL y procedimiento TH-PR-17 VINCULACION LABORAL, para la verificación del personal de carrera y provisional desde la postulación del cargo, teniendo en cuenta los dictámenes legales y lo mandado por el Departamento Administrativo de la Función Pública, así mismo se cuenta con formato TH-F-45 FORMATO DE VERIFICACIÓN DE REQUISITOS, en el cual se dan los lineamientos para la revisión de los antecedentes del personal y demás requisitos acordes al cargo a contratar de acuerdo con la legislación vigente.

Para el personal en misión, desde el proceso de Gestión Talento Humano, se cuenta con procedimiento TH-PR-42 SELECCIÓN DEL PERSONAL EN MISIÓN mediante el cual se realiza verificación de requisitos y formato TH-F-45 FORMATO DE VERIFICACIÓN DE REQUISITOS y TH-F-72 FORMATO DE SEGUIMIENTO CONDUCTOR DE AMBULANCIA Y MENSAJERO, en el cual se dan los lineamientos para la revisión de los antecedentes del personal y demás requisitos acordes al cargo a contratar de acuerdo con la legislación vigente.

Para el personal contratista, se cuenta con el procedimiento TH-PR-47 VALIDACIÓN HOJA DE VIDA CONTRATISTAS y formato TH-F-71 ACTA DE COMPROMISO DE INDUCCIÓN Y REINDUCCIÓN, así mismo se cuenta con formato TH-F-45 FORMATO DE VERIFICACIÓN DE REQUISITOS, en el cual se dan los lineamientos para la revisión de los antecedentes del personal y demás requisitos acordes al cargo a contratar de acuerdo con la legislación vigente.

8.2.5 Investigación de antecedentes.

La verificación de antecedentes está a cargo del proceso de Gestión Talento Humano, el cual debe tener en cuenta toda la privacidad pertinente, la protección de la información de datos personales y legislación laboral, y cuando se permita, debe incluir lo siguiente:

- La disponibilidad de referencias satisfactorias, por ejemplo, una laboral y una personal;
- Una verificación (completa y precisa) de la hoja de vida del solicitante;
- Confirmación de las certificaciones y títulos brindados.
- Una verificación de permisos especiales de permanencia (pasaporte o documento similar)
- Una verificación más detallada, como la información de antecedentes penales.
- Establecer acuerdos o compromisos contractuales con el personal contratista donde se indiquen las responsabilidades en cuanto a la seguridad de la información.
- Firma formato de autorización de tratamiento de datos personales por parte del contratista.

8.2.6 Términos y condiciones de contratación.

Todos los funcionarios, contratistas o terceros de la E.S.E. Hospital Universitario San Rafael de Tunja, a los que se brinde acceso a información confidencial deben firmar un acuerdo de confidencialidad, antes de tener acceso a las instalaciones de procesamiento de información. TH-F-51 ACUERDO DE CONFIDENCIALIDAD EN EL MANEJO Y TRATAMIENTO DE LA INFORMACIÓN-PERSONAL DE PLANTA, el cual tiene aplicabilidad para todos los funcionarios de planta y formato C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN, para contratistas y terceros.

8.2.7 Durante la contratación.

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedor o terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información de la E.S.E. Hospital Universitario San Rafael de Tunja, debe ser informado en el momento que inicie sus actividades contractuales, desde el proceso Gestión Talento Humano, con apoyo del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, además:

a. Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información ejemplo (Servinte, Daruma, Enterprise, Iplan, etc.) o a la plataforma o red institucional de la E.S.E. Hospital Universitario San Rafael de Tunja, a través de la mesa de servicios acorde al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES, previo diligenciamiento del formato S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS, éste debe estar autorizado por el líder, coordinador del área y/o proceso o supervisor del contrato.

b. La solicitud se debe realizar a través de la mesa de servicios de la entidad y debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información.

c. Desde el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, se debe gestionar el requerimiento descrito en el procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES y formato S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS, dando alcance a cada solicitud realizada, con el profesional del sistema de información o componente tecnológico que corresponda.

d. Desde el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, se debe notificar el alcance dado desde el procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES, con el fin de que el funcionario, contratista, proveedor o tercero, sea notificado y de inicio a sus labores o actividades contractuales.

8.2.8 Responsabilidades de gestión.

Es responsabilidad del proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC verificar el cumplimiento de los controles definidos y en apoyo del proceso de Gestión Talento Humano de la Entidad, incluir dentro de su plan de formación institucional y programa de inducción y reinducción lineas especificas de las políticas de seguridad de la información.

8.2.9 Concienciación, educación y capacitación en seguridad de la información

La política de seguridad Resolución 238 del 08 de junio de 2022, debe ser socializada de acuerdo con las actualizaciones que puedan llevarse a cabo, y socializada por correo electronico intitucional y publicada en pagina web de la E.S.E. Hospital Universitario San Rafael de Tunja, para conocimiento de todo el personal objetivo e incluirla en el proceso de inducción y reinducción de nuevos funcionarios y contratistas.

La Entidad realiza concienciación, educación y capacitación en seguridad de la información a traves del plan de formación institucional y campañas de información y educación en seguridad de la información.

8.2.10 Proceso disciplinario.

Dentro de las estrategias de seguridad de la información, E.S.E. Hospital Universitario San Rafael de Tunja, seguirá el proceso establecido en la Ley 734 de 2002 y la *Ley 1952 de 2019*, para investigar a los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información.

El proceso disciplinario también se debe utilizar como medida preventiva para evitar que los funcionarios, contratistas y terceros de la E.S.E. Hospital Universitario San Rafael de Tunja, violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad sin justificación alguna.

El adelantamiento de los procesos disciplinarios corresponde a la oficina de Control Interno Disciplinario, de acuerdo con las competencias señaladas en la ley. Actuaciones que conllevan a la violación de la seguridad de la información de la E.S.E. Hospital Universitario San Rafael de Tunja, son entre otras:

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, "documentos impresos que contengan Información pública (P), Información pública clasificada (C), Información pública reservada (R).
- No guardar la información digital, producto del procesamiento de la información perteneciente a la E.S.E. Hospital Universitario San Rafael de Tunja.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos a las Tablas de Retención Documental-TRD destinadas para tal fin, obviando las medidas de seguridad.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de las plataformas tecnológicas o sistemas de información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la E.S.E. Hospital Universitario San Rafael de Tunja.
- Enviar Información pública (P), Información pública clasificada (C), Información pública reservada (R), por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, que sirvan para transmitir, recibir y almacenar datos.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización del proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, de La E.S.E. Hospital Universitario San Rafael de Tunja.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la E.S.E. Hospital Universitario San Rafael de Tunja.
- No cumplir con las actividades designadas para la protección de los activos de información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la E.S.E. Hospital Universitario San Rafael de Tunja, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar Información pública (P), Información pública clasificada (C), Información pública reservada (R), en Pos-it, apuntes, agendas, libretas, etc., sin el debido cuidado.
- Almacenar Información pública (P), Información pública clasificada (C), Información pública reservada (R), en cualquier dispositivo de almacenamiento que no permanezca a la E.S.E. Hospital Universitario San Rafael de Tunja, o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la E.S.E. Hospital Universitario San Rafael de Tunja, sin la debida autorización.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la E.S.E. Hospital Universitario San Rafael de Tunja para beneficio personal.
- El que sin autorización acceda en todo o parte de los sistemas de información o se mantenga dentro del mismo en contra de la voluntad de la E.S.E. Hospital Universitario San Rafael de Tunja.
- El que impida u obstaculice el funcionamiento o el acceso normal a los sistemas de información, los datos informáticos o las redes de telecomunicaciones de la E.S.E. Hospital Universitario San Rafael de Tunja.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en los equipos de cómputo o Sistemas de Información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- El que viole datos personales de las bases de datos de la de la E.S.E. Hospital Universitario San Rafael de Tunja.

- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la E.S.E. Hospital Universitario San Rafael de Tunja.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la E.S.E. Hospital Universitario San Rafael de Tunja, o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la entidad.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la E.S.E. Hospital Universitario San Rafael de Tunja, o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la E.S.E. Hospital Universitario San Rafael de Tunja a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier equipo de cómputo de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones de la E.S.E. Hospital Universitario San Rafael de Tunja, documentos con información institucional calificada como Información pública (P), Información pública clasificada (C), Información pública reservada (R), o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, clasificada como Información pública (P), Información pública clasificada (C), Información pública reservada (R), a personas o Entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la E.S.E. Hospital Universitario San Rafael de Tunja, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la E.S.E. Hospital Universitario San Rafael de Tunja, o de alguno de sus funcionarios.
- Realizar cambios no autorizados en los sistemas de información de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizados por proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Copiar sin autorización los programas de la E.S.E. Hospital Universitario San Rafael de Tunja, o violar los derechos de autor o acuerdos de licenciamiento a personas no autorizadas.

8.2.11 Cese o cambio de puesto de trabajo.

Se debe informar acorde al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES , por parte del, jefe de area o proceso, supervisor de contrato al proceso de Gestión Talento Humano, a través de la mesa de servicios al proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, una vez finalice la terminación de contrato y/o traslado de área o cambio de funciones de manera inmediata.

La emisión de paz y salvo para funcionario o contratista debe considerar:

a. Tener formato de paz y salvo firmado por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, el cual asegura que se retiraron los accesos lógicos y físicos de acuerdo con el procedimiento de control de acceso.

b. Tener formato de paz y salvo igualmente firmado por jefe inmediato, coordinador o supervisor de contrato, donde se aseguró de la transferencia apropiada de información salvaguardando la información en las Tablas De Retención Documental - TRD al sucesor del cargo e informe de gestión que indica el estado de las actividades realizadas (en desarrollo, finalizadas o pendientes) y la aceptación del jefe inmediato, coordinador o supervisar de contrato.

En el momento de existir alguna novedad relacionada de retiro, inhabilidad, investigación, cambio de función u otras, el jefe de área o a quien este delegue, deberá salvaguardar la información propia de la Entidad, en el caso de los contratistas en terminación de contrato anticipada, temporal, cesión del contrato u otras, aplicara el mismo procedimiento de salvaguardar la información. Lo relacionado a información física con procedimiento de archivo de gestión y archivo histórico por parte de la

dependencia atendiendo lineamientos y Tablas De Retención Documental - TRD establecidas por el proceso de Gestión Documental; y lo relacionado a información digital mediante solicitud realizada al área de Sistemas de Información para realizar el respectivo Backup.

8.3 Política de Gestión de activos

8.3.1 Objetivo

Establecer los lineamientos, las reglas e instrucciones que permitan la gestión y clasificación de los Activos de Información de la E.S.E. Hospital Universitario San Rafael de Tunja, con el fin de identificarlos, protegerlos y asegurarlos, de acuerdo con estándares de seguridad internacionales y a las prácticas y recomendaciones dadas por la política de Gobierno Digital.

8.3.2 Lineamientos generales

- La E.S.E. Hospital Universitario San Rafael de Tunja tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de información, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.
- La Entidad debe identificar los activos asociados a cada Sistema de Información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.
- La Entidad debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: Confidencialidad, integridad y disponibilidad.
- Debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.
- La Entidad deberá definir procedimientos para el rotulado y manejo de información de acuerdo con el esquema de clasificación definido.

8.3.4 Anexos

- C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN.
- S-F-03 ENTREGA DE EQUIPOS
- S-F-05 FORMATO DE MANTENIMIENTO PREVENTIVO O CORRECTIVO DE SOFTWARE.
- S-F-46 MATRIZ DE ACTIVOS DE INFORMACIÓN
- S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
- S-PR-31 BORRADO SEGURO DE LA INFORMACIÓN ELECTRONICA
- S-F-62 BORRADO SEGURO DE LA INFORMACIÓN
- S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
- S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN
- S-F-40 FORMATO SOLICITUD DE COPIAS DE SEGURIDAD
- S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- AHC-PR-10 RECONSTRUCCION HISTORIA CLINICA EXTRAVIADA
- AHC-PR-03 ARCHIVO DE HISTORIA CLINICA
- AHC-PR-05 SOLICITUD DE COPIA DE HISTORIA CLINICA EN CONSULTA EXTERNA E INTERNACIÓN
- GD-PR-15 CONSULTA Y PRESTAMO DE DOCUMENTOS
- GD-F-01 FICHA REGISTRO PARA CONSULTA O PRESTAMO DOCUMENTOS.
- GD-PR-03 PRODUCCIÓN DE DOCUMENTOS
- GD-PR-04 TRANSFERENCIAS DOCUMENTALES PRIMARIAS

- GD-PR-06 ORGANIZACIÓN DE DOCUMENTOS
- GD-PR-07 RECEPCION DE DOCUMENTOS
- GD-PR-08 DISTRIBUCION DE DOCUMENTOS
- GD-PR-09 TRAMITE DE DOCUMENTOS
- GD-PR-10 CONSERVACION DE DOCUMENTOS
- GD-PR-11 DISPOSICIÓN FINAL DE DOCUMENTOS

8.3.5 Responsabilidad sobre los activos.

Cada área o líder de proceso es el responsable de tener identificados y reportar los activos nuevos y los de baja a quien corresponda, 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.

8.3.6 Inventario de activos.

Líder de Seguridad de la información o quien designe la Coordinación del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, realizara el consolidado del inventario de activos reportado por el lider de cada proceso, el cual debe verificar y actualizar con una periodicidad anual, este proceso se actualizará después de haber sido registrados en el formato S-F-46 MATRIZ DE ACTIVOS DE LA INFORMACIÓN acorde a los lineamientos dados en el procedimiento S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN.

8.3.7 Propiedad de los activos.

Para la información que se genera en la E.S.E. Hospital Universitario San Rafael de Tunja, el propietario es la misma E.S.E. Hospital Universitario San Rafael de Tunja; para el caso que la información sea generada para otra Entidad, el propietario es el nombre de dicha Entidad.

8.3.7.1 Custodio

Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información; además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario del activo haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.

8.3.7.2 Uso aceptable de los activos.

La información, archivos físicos, sistemas de información, servicios, y los equipos (ej: estaciones de trabajo, portátiles, tablets, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la E.S.E. Hospital Universitario San Rafael de Tunja, son activos de la entidad y se proporcionan a los funcionarios, contratistas y proveedores o terceros autorizados, para cumplir con los propósitos del negocio.

Todos los funcionarios y contratistas deben etiquetar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices de Etiquetado de la Información que están dentro del procedimiento S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN e instructivo S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

Los funcionarios, contratistas, proveedores o terceros y, todo aquel que cuente con acceso a la información de la E.S.E. Hospital Universitario San Rafael de Tunja, debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes en formato S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

8.3.7.3 Devolución de 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, o acta de liquidación de contrato.

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 perdida 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.

8.3.8 Clasificación de la información.

8.3.8.1 Disponibilidad: Efecto que se genera para la Entidad cuando el activo de información no puede estar disponible cuando se requiere.

VALOR DEL ACTIVO	Nivel	DISPONIBILIDAD
3 (Alto)	ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (Medio)	MEDIA	la no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen moderado de la entidad.
1 (Bajo)	BAJA	la no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de perdida de imagen.

8.3.8.2 Confidencialidad: Nivel de Acceso a la información. El activo sólo sea accedido por el personal, procesos o Entidades que se encuentran autorizadas.

VALOR DEL ACTIVO	Nivel	DISPONIBILIDAD
3 (Alto)	ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (Medio)	MEDIA	la no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen moderado de la entidad.
1 (Bajo)	BAJA	la no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de perdida de imagen.

8.3.8.3 Integridad: Establecer cuál es el efecto de la modificación no autorizada de los datos del activo de información, que impacto tendría en los procesos donde se encuentra involucrado y a su vez que consecuencias tendría para la Entidad.

VALOR DEL ACTIVO	Nivel	INTEGRIDAD
3	ALTA	La información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
2	MEDIA	información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones o generar perdida de imagen moderada a funcionarios de la entidad.
1	BAJA	información cuya perdida de exactitud y completitud conlleva un impacto no significativo para la entidad i entes externos.

8.3.8.4 Nivel de Criticidad o importancia del Activo de Información: Teniendo en cuenta los niveles seleccionados tanto en la Disponibilidad, Confidencialidad e Integridad, se genera automáticamente el Nivel de Criticidad del activo de Información para la Entidad.

- **Alta.** Activos de información en los cuales la clasificación de la información en tres o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta; Son aquellos que apoyan en muchas actividades del negocio, se les debe realizar identificación de riesgos y aplicar controles de seguridad específicos o especializados, políticas, estrategias, procedimientos etc., que coadyuven con el control del riesgo.
- **Media.** Activos de información en los cuales la clasificación de la información es alta en dos de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio; Son aquellos que tienen información apoyan en pocos procedimientos del negocio.
- **Baja.** Activos de información en los cuales la clasificación de la información en todos sus niveles es baja; Son aquellos que no contienen información crítica, y por lo tanto no les debe realizar identificación de riesgos ni aplicar controles de seguridad específicos, políticas, estrategias, procedimientos etc., que coadyuven con la mitigación y control del riesgo.

8.3.5 Directrices de clasificación.

Para realizar el levantamiento o identificación de activos, lo realizará el Líder de Seguridad de la información o quien designe la Coordinación del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, este proceso se actualizará al año después de haber registrados en el formato S-F-46 MATRIZ DE ACTIVOS DE LA INFORMACIÓN acordes con el procedimiento S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN.

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 de 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 de Tunja y esto queda especificado en todos los contratos, diligenciando el formato C-F-43. ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN.

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, accesos remotos, 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 proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC.

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 Gestión y desempeño Institucional.

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 de 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 el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, 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.

8.3.6 Etiquetado y manipulado de la información.

El etiquetado de los activos se realiza de acuerdo con el derecho de acceso a la información:

- **Información pública (P):** Es toda información que ha sido declarada de acceso público, de acuerdo con las normas existentes por la persona o grupo de personas de la Entidad responsables del activo de información y que por lo tanto no tienen requerimientos seguridad frente a la Confidencialidad.

- **Información pública clasificada (C):** Como lo prescribe la Ley 1712 de 2014, información pública clasificada es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014. Esta corresponde a toda aquella información que pudiere causar un daño a los siguientes derechos:

A. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.

B. El derecho de toda persona a la vida, la salud o la seguridad.

C. Los secretos comerciales, industriales y profesionales.

D. También corresponden a esta categoría los datos que son catalogados como "dato semiprivado o privado" de acuerdo con el decreto 1377 de 2013; además de los datos de uso interno de la Entidad y que no deben ser conocidos por el público en general.

- **Información pública reservada (R):** En los términos de la Ley 1712 de 2014, la información pública reservada es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses. públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014. Se trata de una información que solo puede ser conocida y utilizada por un grupo muy reducido de empleados debidamente autorizados por el responsable de la información, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar pérdidas. Información relacionada con:

a. La defensa y seguridad nacional;
b. La seguridad pública;
c. Las relaciones internacionales;
d. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
e. El debido proceso y la igualdad de las partes en los procesos judiciales;
f. La administración efectiva de la justicia;
g. Los derechos de la infancia y la adolescencia;
h. La estabilidad macroeconómica y financiera del país;
i. La salud pública.

También corresponde a información de carácter reservado los datos catalogados como sensibles por el decreto 1377 de 2013.

8.3.7 Manipulación de activos.

Conforme a 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 de acuerdo con los directrices definidas en el instructivo S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

8.3.8 Manejo de los soportes de almacenamiento.

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 proceso de Gestión de Sistemas de Información y Comunicaciones -TIC.

La E.S.E. Hospital Universitario San Rafael de Tunja, a través del proceso de Gestión de Sistemas de Información y Comunicaciones -TIC articulado con el proceso de Gestión documental, 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 Gestión de Sistemas de Información y Comunicaciones -TIC, realiza el respecto de 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 Gestión de Sistemas de Información y Comunicaciones -TIC, 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 procedimiento S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN.

El proceso de Gestión de Sistemas de Información y Comunicaciones -TIC, 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 con el formato S-F-40 FORMATO SOLICITUD DE COPIAS DE SEGURIDAD y procedimiento S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN.

El proceso de Gestión de Sistemas de Información y Comunicaciones -TIC, debe proveer y disponer de los recursos necesarios de los medios de almacenamiento que permitan los planes de copias, restauración y resguardo de los activos críticos de la Entidad; 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 la información de acuerdo con Tablas de Retención Documental -TRD del área. La copia será de manera anual mínimo o cuando el coordinador lo considere pertinente siempre que no supere el año. La copia generada por las Unidad Productora de Documentos-UPD se respaldará en cinta o el medio previsto por el encargado del proceso de Gestión de Sistemas de Información y Comunicaciones -TIC, siempre y cuando se encuentre debidamente organizada conforme a las Tablas de Retención Documental -TRD respectiva. La ruta y carpeta a guardar la copia en equipo diferente será: c:\copiatrd_nombre_area\fecha (aaaa/mm/dd).

El proceso de Gestión de Sistemas de Información y Comunicaciones -TIC, 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 líder, jefe, supervisor del área a la que pertenece, de acuerdo al procedimiento S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN y se entregará la copia respectiva al mismo para su custodia, gestión y control.

8.3.9 Gestión de soportes extraíbles.

El uso de medios removibles (dispositivos USB, discos duros portables, CD, DVD, Blu-ray, etc.) en la E.S.E. Hospital Universitario San Rafael de Tunja, está restringido, los medios removibles no están autorizados como opción de respaldo de información.

El uso de medios removibles es un requerimiento que debe ser solicitado a través de la mesa de servicios GLPI, que debe ser evaluado y autorizado por el Líder de proceso Gestión de Sistemas de Información y Comunicaciones -TIC, toda vez que la justificación de uso tenga un sentido coherente y netamente institucional.

Cuando se autorice el uso de medios removibles en las instalaciones de la entidad, cada vez que se conecte o lean estos medios en las estaciones de trabajo de la E.S.E. Hospital Universitario San Rafael de Tunja, deberán ser escaneados obligatoriamente por el software Antimalware Endopoint suministrado por la Entidad, con el fin de evitar infección por malware o programas con contenido malicioso o prohibido.

Cualquier dato o información que se gestione en medios removibles debe mantener el tratamiento de acuerdo con la clasificación de la información definida en el procedimiento S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN, instructivo S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

Para asegurar los principios de confidencialidad en el manejo de un activo de información tipo información digital, se deben tener en cuenta los controles descritos a continuación:

• Es responsabilidad de cada funcionario o Contratista que utilice medios removibles, tomar las medidas de resguardo necesarias sobre estos activos, con el fin de evitar accesos no autorizados, daños, perdida de información o del activo mismo.

• Ante la pérdida, extravío o robo de un medio removible, el funcionario o contratista debe informar oportunamente (Tiempo no superior a 8 horas) al personal de Mesa de Servicios previo diligenciamiento del formato S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, informando con el mayor grado de detalle, indicando la información que se perdió, si fue extraviado o robado, a su vez estos eventos se deberán manejar como incidentes de seguridad de la información.

8.3.9.1 Eliminación de soportes.

Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o borrado seguro de datos antes de ser reutilizados o dados de baja, de acuerdo a los lineamientos definifos en los procedimentos GD-PR-10 CONSERVACION DE DOCUMENTOS GD-PR-11 DISPOSICION FINAL DE DOCUMENTOS para el caso de informacion contenida en soportes fisicos, para el caso de borrado de informacion electronica segun lo defenido en el procedimiento S-PR-31 BORRADO SEGURO DE LA INFORMACIÓN ELECTRONICA, previa solicitud a traves de mesa de servicicios por el responsable del activo.

La información en las cintas de backups que contienen Información pública (P), Información pública clasificada (C), Información pública reservada (R), se debe cifrar, además deben estar protegidas en un lugar seguro.

La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

Se debe guardar varias copias de datos valiosos para la E.S.E. Hospital Universitario San Rafael de Tunja, en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.

8.3.9.2 Soportes físicos en tránsito

La E.S.E. Hospital Universitario San Rafael de 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 con lineamientos de Archivo General de la Nación.

8.3.9.3 Seguridad Entorno Físico Del Archivo Central

La E.S.E Hospital Universitario San Rafael de Tunja custodia su información institucional en un área de 1000 mts^2, donde se almacenan 7.189 metros lineales de información que corresponden a:

ARCHIVO HISTÓRICO: Documentación de los años 1915 a 1992 con 155 unidades de conservación.

ARCHIVO CENTRAL: Documentación de los años de 1993 a 2023 con 8.582 unidades de conservación.

ARCHIVO DE HISTORIAS CLÍNICAS: Expedientes desde 2008 a 2023, aproximadamente 420.000 expedientes.

Espacio dotado de un sistema de seguridad de cámara en línea, elementos de control de roedores e insectos con dispositivos electrónicos, sistema y red contra incendios, 4 termohigrómetros para control de factores ambientales como humedad relativa, limpieza y aspirado diario.

Para la consulta de documentos institucionales se debe seguir el procedimiento GD-PR-15 CONSULTA Y PRESTAMAMO DE DOCUMENTOS, 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 o jefe de área, Oficina Asesora Desarrollo de Servicios o Gerencia.

Se prohíbe a los usuarios externos consultar documentos de la E.S.E. Hospital Universitario San Rafael de Tunja, o hacer visitas de referenciación a la Entidad sin previa autorización de la Gerencia.

La documentación en las oficinas, se puede consultar previa autorización del coordinador o jefe de área, según procedimiento GD-PR-15 PRESTAMO DE DOCUMENTOS EN ARCHIVO DE GESTION.

8.3.9.4 Archivo De Historias Clínicas Físicas

La E.S.E. Hospital Universitario San Rafael de 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-PR-10 RECONSTRUCCION HISTORIA CLINICA EXTRAVIADA.

8.3.9.5 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 esta. 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 DE HISTORIA CLINICA.

8.3.9.6 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 RECONSTRUCCION HISTORIA CLINICA EXTRAVIADA.

8.3.9.7 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 con lo reglamentado en la resolución 839 de 2017.

8.3.9.8 Condiciones Físicas De Conservación De La Historia Clínica

Atendiendo a lo reglamentado en la resolución 839 de 2017 del Ministerio de Salud y Protección Social y Ministerio de Cultura, en su artículo 3°, las historias clínicas en custodia de la E.S.E Hospital Universitario San Rafael de Tunja, se retienen y conservan por un periodo mínimo de quince (15) años, contados a partir de la fecha de la última atención.

8.3.9.9 Impresión De Historias Clínicas.

En la E.S.E. Hospital Universitario San Rafael de 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 CLINICA 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.

8.10. Política de Control de acceso

8.10.1 Objetivo

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de las plataformas tecnológicas y los sistemas de información de la E.S.E. Hospital Universitario San Rafael de Tunja se encuentren debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

8.10.2 Lineamientos generales

- Establecer los mecanismos propios de control de acceso de la E.S.E. Hospital Universitario San Rafael de Tunja necesarios para garantizar la seguridad de la información.
- Definir, implementar y monitorear los controles de acceso adecuados para proteger la información y las instalaciones en donde se procesa, almacena, trata y se transmite.
- Analizar y realizar seguimiento permanente de las medidas de control de acceso utilizadas, verificando su eficiencia y efectividad.
- Permitir el acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la E.S.E. Hospital Universitario San Rafael de Tunja, únicamente a los usuarios que hayan sido permitidos específicamente y de acuerdo con el propósito de sus funciones y responsabilidades.
- Realizar el registro de las actividades relacionadas con el acceso a los activos de información de la Entidad, realizando auditorías continuas sobre los mismos y verificando el cumplimiento de los lineamientos y ejecución efectiva de los procedimientos asociados.
- Verificar el cumplimiento de los lineamientos establecidos, relacionados con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos.

8.10.3 Anexos

- S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES
- S-F-39 SOLICITUD CREACIÓN DE USUARIOS
- S-F-45 FORMATO SOLICITUD DE USUARIOS INGRESO A PLATAFORMA GLPI MESA DE SERVICIOS
- S-PR-29 SOLICITUD PARA LA CREACION DE VPN
- S-F-59 SOLICITUD DE ASIGNACION DE CREDENCIALES DE UNA VPN
- S-F-60 VERIFICACON DE REQUISITOS PARA EQUIPOS DE COMPUTO EXTERNOS

8.10.4 Requisitos de negocio para el control de accesos.

Por ningún motivo el usuario deberá acceder a la red o a los servicios TIC de la E.S.E. Hospital Universitario San Rafael de Tunja, utilizando una cuenta de usuario o clave de otro usuario.

Es responsabilidad del usuario cualquier acción que realice en el uso de las cuentas y claves asignadas.

La E.S.E. Hospital Universitario San Rafael de Tunja, suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, en donde se llevará a cabo la validación de los datos personales.

Las claves o contraseñas deben:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- nbsp; Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: i,$, %,&)

8.11 Política de control de accesos.

8.11.1 Control de acceso a las redes y servicios asociados.

El acceso a redes Wi-Fi se controla con autenticación por contraseña previa autorización del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC.

El proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado de acuerdo con las restricciones definidas.

Para los usuarios que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, líder del proceso o área, mediante solicitud por mesa de servicios al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, justificando la necesidad del acceso.

La conexión remota a la red de área local de la E.S.E. Hospital Universitario San Rafael de Tunja, debe ser realizada a través de una conexión VPN previa solicitud mediante la mesa de servicios, diligenciando formato S-F-59 SOLICITUD DE ASIGNACIÓN DE CREDENCIALES Y RECURSOS DE UNA VPN con autorización del coordinador del área o servicio y la respectiva subgerencia; el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC valida la solicitud recibida y realiza la verificacion del equipo a traves del formato S-F-60 VERIFICACION DE REQUISITOS PARA EQUIPOS DE COMPUTO EXTERNOS, para su posterior configuración y aprobación de la conexión.

La conexión a redes públicas abiertas está prohibida, así como la conexión a redes Wi-Fi públicas.

El acceso a la red Wi-Fi de la E.S.E. Hospital Universitario San Rafael de Tunja, para los visitantes, médicos concurrentes de las EAPB, debe realizarse por la red destinada para estos accesos a visitantes, de no conocer este acceso se debe solicitar a la mesa de servicios para su debida activación.

Es responsabilidad del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC definir los lineamientos a seguir para garantizar accesos seguros y confiables a los sistemas de información y plataformas tecnológicas de la E.S.E. Hospital Universitario San Rafael de Tunja.

8.11.2 Gestión de acceso de usuario.

Los procedimientos definidos por la E.S.E. Hospital Universitario San Rafael de Tunja, para administrar los privilegios de acceso de los usuarios a la información de la Entidad, deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta por lo menos, que:

Los líderes, jefes de área o proceso, supervisores de contrato de la E.S.E. Hospital Universitario San Rafael de Tunja, son los únicos funcionarios autorizados para realizar las solicitudes de acceso a los sistemas de información o delegados formalmente por el líder para ejecutar esta actividad, que se realiza acorde al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES - V6, mediante el formato S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS.

Para el acceso del personal asistencial al sistema de información Servinte Clinical Suite, el proceso de Gestión Talento Humano debe enviar solicitud a través de la mesa de servicios acorde al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES - V6, con el formato S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS. Para los estudiantes internos o de práctica la solicitud la debe realizar el coordinador o responsable del proceso Gestión Académica de la Entidad.

Ningún colaborador puede realizar solicitudes de acceso para sí mismo, excepto para el gerente, Subgerente Administrativo Y Financiero, Subgerente De Servicios De Salud.

Los jefes o delegados deben realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo en las herramientas establecidas para tal fin (mesa de servicios) acorde a al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES - V6, previo diligenciamiento de formato S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS y asignado al profesional encargado de realizarlo.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada área o proceso.

La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro (correo electrónico institucional). Esta entrega debe estar controlada por un proceso de administración formal que permita, informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios / contraseña) otorgados.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe aplicar el procedimiento definido para la creación de cuentas de usuario y correo electrónico.

Asignar identificaciones únicas a todos los funcionarios y colaboradores, es decir, que no debe existir cuentas genéricas para el acceso o gestión sobre los sistemas de información de la Entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). Cuando por razones del negocio u operación deben ser creadas únicamente como cuentas de servicio y no deben ser utilizadas por ningún funcionario o contratista. En el Directorio Activo se debe detallar el responsable de cada cuenta.

La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir el uso de las claves de usuarios administradoras, tales como: "root", "adm" y "system", entre otros, debe ser controlado por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, quienes son los responsables de dichos accesos, de esta gestión existirá un registro que permita identificar la trazabilidad es decir conocer el funcionario o colaborador que está haciendo uso de estos accesos.

Todo usuario del sistema debe tener un mecanismo de autenticación privado.

En caso de ser necesario se debe utilizar métodos de autenticación fuerte como sensores biométricos, huellas dactilares o "tokens" de hardware.

El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.

Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.

La utilización de información compartida por ejemplo unidades de red debe estar restringida mediante controles ejecutados por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, el responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.

8.11.3 Gestión de los derechos de acceso asignados a usuarios.

Cada contraseña es de uso personal e intransferible. Los servidores públicos, contratistas y terceros que trabajan para la E.S.E. Hospital Universitario San Rafael de Tunja, no han de revelar la contraseña de su cuenta a otros servidores públicos y/o terceros.

Se solicitará cambio de contraseña en el equipo del usuario periódicamente, adicional no se deberán utilizar contraseñas que hayan sido usadas con anterioridad.

Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones por medio de la cuenta de otro funcionario.

Los servidores públicos, contratistas y terceros que trabajan para la E.S.E. Hospital Universitario San Rafael de Tunja, deben notificar inmediatamente al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, si sospechan que alguien ha obtenido acceso sin autorización a su cuenta y debe modificarla inmediatamente.

El usuario es responsable por la custodia de su contraseña. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

No se deben almacenar contraseñas en formato legible, en archivos tipo "batch", scripts de login automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso o en otros sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

Cuando se presente un evento donde se deba realizar trabajo en casa, el usuario debe crear un servicio al administrador del directorio activo a través de la mesa de servicio, para realizar el cambio de clave cuando ésta expire. Ya que un usuario no puede hacer cambios de contraseñas a través del escritorio remoto.

8.11.4 Gestión de los derechos de acceso con privilegios especiales.

Cuando se requiera realizar labores de trabajo en casa el líder del área, proceso o supervisor de contrato debe solicitar por mesa de servicios al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, la creación de una Red Privada Virtual- VPN de acceso en los recursos tecnológicos que se hayan definido para trabajo fuera de oficina, indicando el tiempo de acceso por el cual se requiere la conexión.

El funcionario o contratista debe haber instalado el cliente de la Red Privada Virtual- VPN en el computador personal de su hogar, con el fin de conectarse vía remota a los servicios tecnológicos de la E.S.E. Hospital Universitario San Rafael de Tunja.

Una vez ejecute el cliente de la Red Privada Virtual- VPN en el equipo de su casa debe autenticarse con las credenciales otorgadas por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, de manera individual y personal.

Establecida la conectividad a través de la IP del computador de escritorio en las oficinas de la E.S.E. Hospital Universitario San Rafael de Tunja, el usuario debe autenticarse con las credenciales normales de acceso brindada por el Directorio Activo. Esto permite que el usuario ingrese a los sistemas de información y recursos compartidos como si estuviera dentro de las oficinas de la Entidad.

Es muy importante que el usuario no copie archivos desde su sistema de archivos del computador de la casa hacia el computador al cual está conectado por la Red Privada Virtual- VPN y que es propiedad de la E.S.E. Hospital Universitario San Rafael de Tunja.

De igual manera es importante que todos los archivos que gestione el usuario mientras estén conectados por Red Privada Virtual- VPN en la estación de trabajo propiedad de la E.S.E. Hospital Universitario San Rafael de Tunja, no sean descargados a las unidades locales o escritorio del computador de la casa.

Esta restringido que el usuario se conecte a internet a páginas como YouTube, Streeming, redes sociales, entre otras a través de la Red Privada Virtual- VPN y desde la estación de trabajo de la Entidad.

Es importante de igual manera adquirir la rutina de desconexión y conexión continua mientras se realizan labores que no requieren de conectividad

Es importante que el usuario identifique la forma adecuada de desconexión de su estación de trabajo de la E.S.E. Hospital Universitario San Rafael de Tunja, para no cometer el error de apagar esta estación de trabajo. De apagar esta estación de trabajo de la Entidad en forma remota no le permitirá establecer conexiones futuras y deberá acudir a la línea de soporte del proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

8.11.5 Revisión de los derechos de acceso de los usuarios.

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 Gestión de Sistemas de Información y las Comunicaciones -TIC y/o líderes de sistemas de información serán los que otorguen o dicten los privilegios.

8.11.6 Retirada o adaptación de los derechos de acceso

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, para respectiva legalización de la paz y salvo y/o del proceso de Gestión Talento Humano.

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 previo diligenciamiento de formato S-F-39 SOLICITUD CREACIÓN DE USUARIOS SISTEMAS DE INFORMACION y registro de caso en la mesa de servicios al personal encargado del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, de otorgar o modificar dichos privilegios; de tal forma que tenga conocimiento de los cambios solicitados.

8.11.7 Responsabilidades del usuario.

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.

8.11.8 Uso de información confidencial para la autenticación.

Los usuarios deben cumplir con las prácticas de la Entidad para el uso de información de autenticación secreta.

8.11.9 Control de acceso a sistemas y aplicaciones.

Se deben utilizar los bienes y recursos informáticos asignados única y exclusivamente para el desempeño de su empleo, cargo, rol y/o función. De la misma forma las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, debe ser utilizada en forma exclusiva para fines institucionales de la Entidad.

Los sistemas de cómputo entregados por la E.S.E. Hospital Universitario San Rafael de Tunja, deben ser utilizados únicamente para propósitos propios de la Entidad y son propiedad del estado, por esta razón se recuerda que el uso que se le dé a los mismos es de carácter oficial.

No se pueden almacenar, instalar o utilizar juegos en los equipos de cómputo de la E.S.E. Hospital Universitario San Rafael de Tunja.

Las únicas personas autorizadas por la E.S.E. Hospital Universitario San Rafael de Tunja, para instalar y realizar cambios al software y hardware de los equipos de la Entidad, son los funcionarios y técnicos de soporte con previa autorización del Coordinador del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, motivo por el cual se prohíbe la instalación de algún software sin previa autorización, con el fin de constatar la seguridad y legalidad de este.

Los cambios, ajustes o mejoras en la infraestructura física o lógica de aplicaciones de la E.S.E. Hospital Universitario San Rafael de Tunja, deberán ceñirse a las políticas de seguridad informática de la Entidad.

8.11.10 Restricción del acceso a la información.

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 Gestión de Sistemas de Información y las Comunicaciones -TIC y/o líderes de sistemas de información serán los que otorguen o dicten los privilegios.

8.11.11 Gestión de contraseñas de usuario.

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 Gestión de Talento Humano y el Coordinador o líder de proceso o área al que pertenece dicho usuario, el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, Se encargada de crear la cuenta, previo diligenciamiento de formato S-F-39 SOLICITUD CREACIÓN DE USUARIOS SISTEMAS DE INFORMACION y registro de caso en la mesa de servicios acorde al procedimiento S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES -V6; 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.

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.

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.

Cuando un usuario olvide su contraseña o bloquee su usuario, deberá notificarlo al personal encargado del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, quienes se encargarán de desbloquear o renovar dichas credenciales.

En los sistemas de información donde se pueda controlar la vigencia de la contraseña, esta tendrá una vigencia de noventa (90) 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 de la institución, sin autorización del Coordinador de Gestión de Sistemas de Información y las Comunicaciones -TIC, con previa solicitud y registrado de caso en la mesa de servicios GLPI.

8.12 Política de Criptografía

8.12.1 Objetivo

Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas. Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de la E.S.E Hospital Universitario San Rafael de Tunja, sea por cualquier medio tecnológico existente, siempre deberá estar autenticado y sus conexiones deberán estar cifradas.

8.12.2 Lineamientos generales

- Toda información que se extraiga de los aplicativos misionales deberá estar cifrada para evitar que la misma pierda su confidencialidad.
- Con el fin de garantizar la confidencialidad e integridad de los documentos designados como sensibles, la E.S.E. Hospital Universitario San Rafael de Tunja, debe utilizar sistemas y técnicas criptográficas para la protección de la información
- En los sistemas de información se deben implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares y guías aplicables.
- Proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves considerándolos críticos o de alto riesgo y proteger las claves evitando que sean copiadas o modificadas sin autorización.
- La E.S.E. Hospital Universitario San Rafael de Tunja, deberá velar porque la información de su custodia o propiedad que es catalogada como reservada, clasificada o sensible se cifre al momento de almacenarse o transmitirse por cualquier medio.
- Las claves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con la Entidad.

8.13 Política Seguridad física y del entorno

8.13.1 Objetivo

Implementar el procedimiento de control de acceso a los centros de datos para garantizar la seguridad física que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.

8.13.2 Lineamientos generales

- Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones de procesamiento de información de la organización.
- Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.
- Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.
- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.
- Todos los colaboradores de la E.S.E. Hospital Universitario San Rafael de Tunja deben bloquear los equipos de cómputo cuando estén desatendidos, cerrar las sesiones de las aplicaciones o servicios de red cuando ya no se necesiten, adoptar la política de escritorio limpio de papeles y medios de almacenamiento removibles y tener la pantalla del computador despejada, libre de archivos o accesos directos a los programas.

8.13.3 Anexos

- A-PR-01 INGRESO DE MERCANCIAS
- INT-PR-01 CONTROL DE INGRESO DE VISITANTES.
- U-PR-02 ATENCIÓN DE PACIENTE EN EL SERVICIO DE URGENCIAS.
- S-F-27 CONTROL DE INGRESO DE PERSONAL AL DATACENTER.
- S-F-43 SOLICITUD TRASLADO DE EQUIPOS DE COMPUTO
- S-PR-10 MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA EQUIPOS DE COMPUTO

8.13.4 Áreas seguras.

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

El acceso de personal externo o distinto al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, que requiera ingresar deberá estar autorizado por el Coordinador del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, y realizar el diligenciamiento del formato S-F-27 CONTROL DE INGRESO DE PERSONAL AL DATACENTER y en todo momento debe estar acompañado por un funcionario del mismo proceso.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 del proceso Gestión de Sistemas de Información y las Comunicaciones –TIC, 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 los cuartos secundarios de cableado estructurado y/o rack de distribución, estarán a cargo y del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, los cuales tendrán las medidas de acceso y control.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

• Fumar dentro del Data Center.

• Introducir alimentos o bebidas al Data Center

• El porte de armas de fuego, corto punzantes o similares.

• Mover, desconectar y/o conectar equipo de cómputo sin autorización.

• Modificar la configuración del equipo o intentarlo sin autorización.

• Alterar software instalado en los equipos sin autorización.

• Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

• Extraer información de los equipos en dispositivos externos.

• Abuso y/o mal uso de los sistemas de información.

• Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

8.13.5 Perímetro de seguridad física.

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las instalaciones de procesamiento de información. La E.S.E. Hospital Universitario San Rafael de Tunja, utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

8.13.6 Controles físicos de entrada.

La E.S.E. Hospital Universitario San Rafael de 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.

La E.S.E. Hospital Universitario San Rafael de 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 de 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 carné institucional y el cual se debe mantener de manera visible durante el tiempo que permanezca dentro de la Institución.

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.

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 ATENCION DE PACIENTE EN EL SERVICIO DE URGENCIAS - V2, 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.

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 se 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 de 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 de 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.

8.13.7 Seguridad de oficinas, despachos y recursos.

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la Entidad:

- Datacenter.
- Encerramiento de planta eléctrica y UPS.
- Racks de distribución.

8.13.8 El trabajo en áreas seguras.

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.

c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado

solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas, mediante registro en formato.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el coordinador del proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

8.13.9 Áreas de acceso público, carga y descarga.

La carga y descarga de mercancías y suministros médicos, dispositivos y medicamentos de la E.S.E Hospital Universitario San Rafael de Tunja, se debe realizar únicamente por las puertas asignadas de Gestión de Suministros y Activos Fijos de acuerdo a los procedimientos A-PR-01 INGRESO DE MERCANCIAS - V8 y A-PR-02 RECEPCION Y DESPACHO DE MERCANCIAS - V7 y descarga e ingreso de dispositivos y medicamentos a través de las puertas del Servicio Farmacéutico procedimiento SF-PR 28 RECEPCIÓN TÉCNICO ADMINISTRATIVA DE MEDICAMENTOS DISPOSITIVOS MÉDICOS, MATERIAS PRIMAS, MATERIAL DE ENVASE Y GASES MEDICINALES, las 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.

8.13.10 Seguridad de los equipos.

Está prohibido que personal ajeno al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, destape o retire partes de los equipos de cómputo propiedad de la E.S.E. Hospital Universitario San Rafael de Tunja.

La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del

proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, por tanto, se debe solicitar soporte si se requiere, para la realización de estas labores.

Los equipos de cómputo no deben ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado, sin previa solicitud a través de mesa de servicios al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC y haber diligenciado y adjuntado el formato S-F-43 SOLICITUD TRASLADO DE EQUIPOS DE COMPUTO.

Debe respetarse y no modificarse la configuración de hardware y software establecido por proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, debe conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar picos alto que puedan dañar el componente tecnológico. Estos puntos de corriente regulada se usan para regular la energía y que bien están soportados igualmente por las UPS en dado caso que se vaya la luz y no se apague abruptamente.

La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la E.S.E. Hospital Universitario San Rafael de Tunja, y que no son propiedad de la Entidad, es responsabilidad única y exclusiva de sus propietarios. La E.S.E. Hospital Universitario San Rafael de Tunja, no es la responsable por estos equipos en ningún caso.

8.13.11 Emplazamiento y protección de equipos.

El emplazamiento y la fortaleza de cada barrera estarán definidos por el coordinador del proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, de acuerdo con la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a. Definir y documentar claramente el perímetro de seguridad.

b. Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, alarmas, cerraduras, entre otros.

c. Verificar la existencia de un área de recepción atendida por personal. El acceso a dicha área estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

d. Extender las barreras físicas necesarias desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.

e. Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

8.13.12 Instalaciones de suministro.

La E.S.E. Hospital Universitario San Rafael de Tunja, cuenta con aire acondicionado de contingencia, UPS (sistema de alimentación ininterrumpida, en inglés (Uninterruptible Power Supply). que asegura el tiempo necesario de 15 minutos de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica. ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del Datacenter.

8.13.13 Seguridad del cableado.

El Datacenter de la E.S.E. Hospital Universitario San Rafael de Tunja, cumple con la normatividad de cableado estructurado y con las características de un Datacenter.

8.13.14 Mantenimiento de los equipos.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, coordina las labores de mantenimiento correctivo y preventivo, acorde con el procedimiento S-PR-10 MANTENIMIENTO PREVENTIVO Y CORRECTIVO PARA EQUIPOS DE COMPUTO, las cuales se realizan a través del grupo de técnicos de soporte y cuando sea necesario será subcontratado dicho servicio, adicional se realiza seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la Entidad.

El mantenimiento de servidores, switches, sistemas de almacenamiento se realizará mediante contratos a través de terceros y será supervisado por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

8.13.15 Salida de activos fuera de las dependencias de la empresa.

La salida de elementos de la E.S.E. Hospital Universitario San Rafael de Tunja, es controlada mediante el formato xxxxxxxx FORMATO ÚNICO DE RETIRO DE EQUPOS FUERA DE LAS INSTALACIONES, previa aprobación del líder o coordinador de área o servicio propietario del activo.

8.13.16 Seguridad de los equipos y activos fuera de las instalaciones.

Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones de la E.S.E. Hospital Universitario San Rafael de Tunja, deben seguir las siguientes directrices:

1. En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
2. Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
3. En caso de pérdida o robo de un equipo de la E.S.E. Hospital Universitario San Rafael de Tunja, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, para que se inicie el trámite interno correspondiente.

8.13.17 Reutilización o retirada segura de dispositivos de almacenamiento.

Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información salvaguardada en las Tablas de Retención Documental-TRD, definida para el área o proceso de la E.S.E. Hospital Universitario San Rafael de Tunja, que allí se encuentre almacenada (en caso de ser necesario).

Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. Ver indicaciones adicionales en el procedimiento de borrado seguro.

8.13.18 Equipo informático de usuario desatendido.

Todos los funcionarios y contratistas de la E.S.E. Hospital Universitario San Rafael de Tunja deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo simultáneamente las teclas Control +Alt +Supr), a su vez, el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe implementar mecanismos para cierres de sesión automáticos no superior a diez (10) minutos.

8.13.19 Política de puesto de trabajo despejado y bloqueo de pantalla.

Todos los funcionaros, contratistas de la E.S.E. Hospital Universitario San Rafael de Tunja, deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento.

Cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

a. Al imprimir documentos de carácter confidencial (Información pública (P), Información pública clasificada (C), Información pública reservada (R), estos deben ser retirados de la impresora inmediatamente.

b. Los computadores deben cargar por defecto el fondo de pantalla definidos por el proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, de la E.S.E. Hospital Universitario San Rafael de Tunja, éste no debe ser modificado y debe permanecer activo.

c. Los usuarios son responsables y asumen las consecuencias por la pérdida de información que este bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores de la E.S.E. Hospital Universitario San Rafael de Tunja. El escritorio lógico (del computador) debe estar libre de Información pública (P), Información pública clasificada (C), Información pública reservada (R).

d. La información de gestión del área que requiera ser almacenada por los usuarios en carpetas compartidas debe ser solicitado y previamente autorizado por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

8.14 Política de Seguridad de las operaciones

8.14.1 Objetivo

Contar con procedimientos documentados de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

8.14.2 Lineamientos generales

- Los procedimientos para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación se deben documentar y poner a disposición de los colaboradores.
- La coordinación de la oficina de Sistemas de Información debe gestionar la capacidad de los sistemas de procesamiento de información y comunicaciones, lo cual comprende:
- Todos los sistemas deben contar con sincronización de reloj a nivel de sistema operativo, teniendo como referencia la hora legal colombiana. No está permitida la desactivación del sistema de sincronización o la manipulación de la hora.
- La coordinación de la oficina de Sistemas de Información debe generar y mantener registros de auditoría sobre las actividades de los usuarios, excepciones y eventos de Seguridad de Información.
- Los registros de auditoría deben contar con controles para garantizar su integridad.
- La coordinación de la oficina de Sistemas de Información debe asegurar que las reglas de los firewalls y las firmas de los IPS/IDS, están configuradas de acuerdo con la lógica de negocio de los sistemas de información y aplicaciones de la E.S.E. Hospital Universitario San Rafael de Tunja, se debe garantizar que esta configuración permanece actualizada y se encuentra debidamente documentada.

8.14.3 Anexos

- S-PR-21 Procedimiento Copias De Seguridad De Sistemas De Información.
- S-F-40 Formato Solicitud De Copias De Seguridad
- S-F-05 Formato de Mantenimiento Preventivo o Correctivo de Software.

8.14.4 Gestión de cambios.

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se debe realizar de acuerdo con los lineamientos del Procedimiento de Gestión de Cambios.

8.14.5 Separación de entornos de desarrollo, prueba y producción.

La E.S.E. Hospital Universitario San Rafael de Tunja, cuenta en sus sistemas de información con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y máquinas virtuales.

La E.S.E. Hospital Universitario San Rafael de Tunja, cuenta con el acceso al ambiente de pruebas de la misma forma que controla el acceso al ambiente de producción.

8.14.6 Protección contra código malicioso.

Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la E.S.E. Hospital Universitario San Rafael de Tunja, contra códigos maliciosos.

Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado, previamente verificado y autorizado por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

El único servicio de antivirus autorizado en la E.S.E. Hospital Universitario San Rafael de Tunja, es el asignado directamente por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

El programa de antivirus debe ser instalado y desinstalado única y exclusivamente por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC. en los servidores y estaciones de trabajo.

8.14.7 Copias de seguridad.

La E.S.E. Hospital Universitario San Rafael de Tunja, debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC. define mediante el Procedimiento S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN, el cual define las actividades para la realización de backup requeridas; además:

El proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC, debe establecer las políticas de copias de seguridad desde la herramienta de backups, para los sistemas de información y bases de datos.

Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por el proceso de Gestión de Sistemas de Información y las Comunicaciones –TIC.

Todas las copias de respaldo deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.

Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.

Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.

Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de la E.S.E. Hospital Universitario San Rafael de Tunja.

8.14.7.1 Copias de seguridad de la información.

La E.S.E. Hospital Universitario San Rafael de Tunja, a través del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 con el 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 Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 con Tablas de Retención Documental -TRD del área. Esta información deberá estar organizada de acuerdo con su TRD. La copia será de manera anual mínimo, o cuando el coordinador de área o proceso lo considere pertinente siempre que no supere el año. La copia generada por las UPD se respaldará en cinta o el medio previsto por el encargado del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 Gestión de Sistemas de Información y Comunicaciones -TIC, 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 líder, jefe, supervisor del área a la que pertenece PR-21 PROCEDIMIENTO DE COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN y se entregará la copia respectiva al mismo para su custodia, gestión y control.

8.14.8 Sincronización de relojes.

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la E.S.E. Hospital Universitario San Rafael de Tunja, deben estar sincronizados utilizando como referencia la hora oficial de Colombia de INM (Instituto Nacional de Metrología) horalegal.inm.gov.co

8.15 política de Seguridad de las comunicaciones

8.15.1 Objetivo

Definir e implementar los mecanismos de control que considere apropiados para proteger la Confidencialidad, Integridad y Disponibilidad de la información en las redes definidas en la Entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información que viajan a través de estos canales de redes de comunicaciones.

8.15.2 Anexos

- 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
- CO-F-02 SOLICITUD DE PIEZAS COMUNICATIVAS Y PUBLICITARIAS

8.15.3 Gestión de la seguridad en las redes.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, debe definir e implementar mecanismos de separación de las redes de la E.S.E. Hospital Universitario San Rafael de Tunja, con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor) además:

El acceso remoto a las redes de la E.S.E. Hospital Universitario San Rafael de Tunja, se controla mediante conexiones VPN, las cuales deben estar monitoreadas para que se evidencie la desactivación de ésta en el tiempo que se ha definido.

8.15.4 Intercambio de información con partes externas.

El área de Comunicaciones Medios y Publicidad 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.

El único proceso autorizado para la toma de fotos, grabaciones y videos en la institución es el área de Comunicaciones Medios y Publicidad 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 de Tunja la toma de fotos y registros en video al

interior de la Entidad, sin la autorización del área de Comunicaciones Medios y Publicidad, 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 medíos que se utilizan para la obtención de esta están contemplados en los artículos 189 a 191 de la ley 599 de 2000 (Código Penal).

8.15.4.1 Mensajería electrónica.

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 Gestión de Sistemas de Información y las Comunicaciones -TIC, de acuerdo con solicitud previa del coordinador del área que la requiera y registro de caso en la mesa de servicios GLPI adjuntando formato diligenciado S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS. 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.

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 Comunicaciones Medios y Publicidad 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.

Cuando se requiera el envío de documentos entre las áreas de la Entidad, 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 de Tunja y conservar en todos los casos el mensaje corporativo de

confidencialidad y cumplir con la siguiente estructura:

Nombres y Apellidos de Funcionario
Cargo
Telefono fijo y extension
Carrera 11 No. 27-27 Tunja- Boyacá Colombia
Correo electronico institucional
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 con el 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 proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, 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 Gestión de Sistemas de Información y las Comunicaciones -TIC, llenando el formato de control respectivo.

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 Medios y Publicidad podrá hacerlo.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la E.S.E. Hospital Universitario San Rafael de Tunja, que sea creado a nombre personal a través de redes sociales como: Twitter®, Facebook®, Youtube® Likedink®, Blogs, Instagram, etc., se considera fuera del alcance de las políticas establecidas y

por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

La información publicada en las redes sociales que sea originada por la Entidad está a cargo el área de Comunicaciones Medios y Publicidad del debe ser autorizada por los directores o jefes de área para ser socializadas y con un vocabulario institucional. El nombre de la Entidad en las redes sociales no puede ser utilizado para difamar o afectar la imagen y reputación de las personas que no están de acuerdo o estén en contra de la E.S.E Hospital Universitario San Rafael de Tunja por información publicada.

Notificaciones Fuera de Oficina

De acuerdo a la política de Desconexión Laboral al interior de la E.S.E Hospital Universitario San Rafael de Tunja, y con el fin de garantizar el goce efectivo del tiempo libre y los tiempos de descanso, licencias, permisos y vacaciones para conciliar la vida personal, familiar y laboral, es reponsabilidad de cada funcionario, contratista o tercero, realizar la activacion de notificacion fuera de oficina en los correos electronicos Outlook institucionales, de acuerdo a los modelos descritos segun aplique para cada caso:

Periodo de vacaciones

Buenos días:

Gracias por su mensaje. Actualmente me encuentro en periodo de vacaciones. Póngase en contacto al siguiente correo ejemplo@email.com. Quien estará disponible para atenderle.

Gracias por su comprensión.

Incapacidad

Buenos días:

Gracias por su mensaje. Estaré fuera de la oficina por incapacidad médica. Póngase en contacto al siguiente correo ejemplo@email.com . Quien estará disponible para atenderle.

Gracias por su comprensión.

Por otro motivo

Buenos días:

Gracias por su mensaje. Estaré fuera de la oficina sin acceso al correo electrónico. Póngase en contacto al siguiente correo ejemplo@email.com. Quien estará disponible para atenderle.

Gracias por su comprensión.

8.16 política de Gestión de incidentes de seguridad de la información

8.16.1 Objetivo

Establecer las actividades, condiciones y acciones para detectar, reportar, evaluar, clasificar, responder y aprender sobre los eventos e incidentes de seguridad de la información que se evidencien o presenten con cualquier activo de información de la E.S.E. Hospital Universitario San Rafael de Tunja, a fin de garantizar el tratamiento oportuno y eficaz para evitar daños o repercusiones que generen o aumenten el impacto.

8.16.2 Lineamientos generales

- Realizar la gestión de cada incidente contemplando todas las etapas de su ciclo de vida: reporte, asignación, tratamiento, respuesta y cierre.

- El proceso de gestión de incidentes debe explicitar de manera clara y sin ambigüedades los mecanismos y métodos para realizar los reportes de incidentes de seguridad, así como también la información mínima a proporcionar; manteniendo la confidencialidad de la información suministrada por quien reporte, así como su anonimato.
- Informar de forma completa e inmediata al responsable de seguridad de la información la existencia de un potencial incidente de seguridad informática.
- Adoptar medidas de seguridad eficientes para proteger los activos de información.
- Aprender de los incidentes de seguridad reportados y generar la conciencia necesaria a fin de prevenir nuevas ocurrencias cuando corresponda.

8.16.3 Gestión de incidentes de seguridad de la información y mejoras.

Asegurar que los eventos e incidentes de seguridad que se presenten en la Entidad, con los activos de información sean comunicados y atendidos oportunamente, de acuerdo al procedimioento S-PR-30 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, con el fin de ejecutar oportunamente las acciones correctivas.

Los funcionarios y contratistas de la E.S.E. Hospital Universitario San Rafael de Tunja, deberán informar a traves de la mesa de servicios adjuntando el formato S-F-54 REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN inmediatamente al proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC, cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados a traves del formato S-F-55 ACTA DE RECOLECCIÓN DE EVIDENCIAS DE INCIDENTES DE SEGURIDAD.

Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC y se dara respuesta al proceso mediante el formato S-F-56 NOTIFICACIÓN FINAL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Los resultados de las investigaciones serán informados en el Comité de Gestión y Desempeño Institucional, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

8.16.4 Responsabilidades y procedimientos.

Por parte del proceso de Gestión de Sistemas de Información y las Comunicaciones -TIC.

- Promoción y socialización de los riesgos asociados a incidentes de seguridad de la información de manera transversal a todas las áreas y procesos de la E.S.E Hospital Universitario San Rafael de Tunja.
- Clasificación y evaluación de un evento para determinar si corresponde o no a un incidente y su impacto.
- Seguimiento a eventos o incidentes de seguridad de la información.
- Reporte a la oficina asesora de Desarrollo de Servicios, los eventos o incidentes de seguridad de la información que una vez evaluados obtengan un impacto alto para la Entidad, en cualquier ámbito.
- Documentar los eventos e incidentes de seguridad de la información.

9. EVALUACIÓN

La evaluación y seguimeinto se realizara a traves del formato S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO

10. DEFINICIONES Y/O GLOSARIO

a. **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

b. **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema de información o la Entidad.

c. **CCTV:** Circuito Cerrado de Televisión.

d. **Ciberseguridad:** Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.

e. **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos Entidades o procesos no autorizados.

f. **Contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

g. **Control de acceso:** El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas.

h. **CSIRT:** (Computer Security Incident Response Team): Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.

i. **Disponibilidad:** Propiedad de ser accesible y utilizable sobre demanda por una Entidad autorizada.

j. **Incidente de seguridad de la información:** un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

k. **Integridad:** la propiedad de salvaguardar la exactitud e integridad de los activos.

l. **MSPI:** Modelo de Seguridad y Privacidad de la Información.

m. **VPN:** Red privada virtual.

11. DOCUMENTO SOPORTE /ANEXOS

Norma ISO 27001

12. SOPORTE /ANEXOS

S-F-29 DECLARACIÓN DE APLICABILIDAD CONTROLES ISO

S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN

S-F-46 MATRIZ DE ACTIVOS DE INFORMACIÓN
S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
S-F-03 ENTREGA DE EQUIPOS
S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
S-F-46 MATRIZ DE ACTIVOS DE INFORMACIÓN
S-M-15 ESQUEMA GOBIERNO
S-PR-12 GESTION Y ADMINISTRACION DE DIRECTORIO ACTIVO
S-PR-30 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
TH-PR-08 SELECCIÓN INGRESO Y PROMOCION DE PERSONAL
TH-PR-17 VINCULACION LABORAL
TH-F-45 FORMATO DE VERIFICACIÓN DE REQUISITOS
TH-PR-47 VALIDACIÓN HOJA DE VIDA CONTRATISTAS
TH-F-72 FORMATO DE SEGUIMIENTO CONDUCTOR DE AMBULANCIA Y MENSAJERO
TH-F-71 ACTA DE COMPROMISO DE INDUCCIÓN Y REINDUCCIÓN
TH-F-51 ACUERDO DE CONFIDENCIALIDAD EN EL MANEJO Y TRATAMIENTO DE LA INFORMACIÓN- PERSONAL DE PLANTA
C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN PROCEDIMIENTO COPIAS
TH-PR-42 SELECCIÓN DEL PERSONAL EN MISIÓN
TH-PR-47 VALIDACIÓN HOJA DE VIDA CONTRATISTAS
TH-F-51 ACUERDO DE CONFIDENCIALIDAD EN EL MANEJO Y TRATAMIENTO DE LA INFORMACIÓN-PERSONAL DE PLANTA
C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN
S-PR-13 GESTIÓN DE USUARIOS PARA EL ACCESO A SISTEMAS DE INFORMACION Y/O PLATAFORMAS INSTITUCIONALES
S-F-39 SOLICITUD DE CREACIÓN DE USUARIOS

C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN
S-F-05 FORMATO DE MANTENIMIENTO PREVENTIVO O CORRECTIVO DE SOFTWARE
S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
S-PR-21 COPIAS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN
S-F-40 FORMATO SOLICITUD DE COPIAS DE SEGURIDAD
AHC-PR-10 RECONSTRUCCION HISTORIA CLINICA EXTRAVIADA
AHC-PR-03 ARCHIVO DE HISTORIA CLINICA
AHC-PR-05 SOLICITUD DE COPIA DE HISTORIA CLINICA EN CONSULTA EXTERNA E INTERNACIÓN
GD-PR-15 PRESTAMO DE DOCUMENTOS EN ARCHIVO DE GESTION
GD-F-01 FICHA REGISTRO PARA CONSULTA O PRESTAMO DOCUMENTOS
GD-PR-03 PRODUCCIÓN DE DOCUMENTOS
GD-PR-04 TRANSFERENCIAS DOCUMENTALES PRIMARIAS
GD-PR-06 ORGANIZACIÓN DE DOCUMENTOS
GD-PR-07 RECEPCION DE DOCUMENTOS
GD-PR-08 DISTRIBUCION DE DOCUMENTOS
GD-PR-09 TRAMITE DE DOCUMENTOS
GD-PR-10 CONSERVACION DE DOCUMENTOS
GD-PR-11 DISPOSICIÓN FINAL DE DOCUMENTOS
S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN e instructivo S-INS-21
INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
S-PR-24 INVENTARIO CLASIFICACIÓN Y ETIQUETADO DE ACTIVOS DE INFORMACIÓN
C-F-43 ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN
S-INS-21 INSTRUCTIVO DILIGENCIAMIENTO MATRIZ INVENTARIO CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
S-F-39 SOLICITUD CREACIÓN DE USUARIOS
S-F-45 FORMATO SOLICITUD DE USUARIOS INGRESO A PLATAFORMA GLPI MESA DE SERVICIOS

13. 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

ISO/IEC 27002:2013. 14 DOMINIOS

https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

14. 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.
05	15/05/2023	Jorge Armando Figueredo Malagón	Se ajusta políticas acordes a los 114 controles definidos en la norma ISO 27001
06	16/07/2024	Jorge Armando Figueredo Malagón Karenth Paola Jimenez Santamaria	Se ajustan politicas de dispositivos para movilidad y teletrabajo, manejo de los soportes de almacenamiento, gestion de incidentes de seguridad de la información y mejoras y clasificación de la información.
07	19/09/2024	Jorge Armando Figueredo Malagón Karenth Paola Jimenez Santamaria	Se incluye apartado de notificaciones fuera de oficina, en el numeral de mensajeria instantanea Se incluye formatos S-F-59 Y S-F-60 y Procedimiento S-PR-23

08	13/11/2024	Jorge Armando Figueredo Malagón Karenth Paola Jimenez Santamaria	Se ajustan las politicas de Políticas de Uso de Dispositivos Móviles incluyendo normas de uso, seguridad y privacidad y Politica de teletrabajo, incluyendo solicitud de creacion de VPN Se ajusta la politica de eliminación de soportes en su numeral 8.3.9.1 Eliminación de soportes , en el cual se encluye los porcedimientos para la gestión.

Elaboró	Revisión Técnica	Socialización	Revisión General	Aprobó
Nombre: Jorge Armando Figueredo Malagón Cargo: Profesional Especializado Nombre: Karenth Paola Jiménez Santamaría Cargo: Profesional Especializado	Marbiz Said Ducuara Amado Profesional Universitario Blanca Nelly Castiblanco Sierra Apoyo a Gestión por Procesos	Jorge Armando Figueredo Malagon Profesional Especializado Blanca Nelly Castiblanco Sierra Apoyo a Gestión por Procesos	Monica Maria Londoño Forero Asesor Desarrollo de Servicios	German Francisco Pertuz Gonzalez Gerente

Jorge Armando Figueredo Malagon @ 2025-02-01, 13:07:02