PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Empresa Social del Estado
Hospital San Rafael Nivel II
San Juan del Cesar, La Guajira

Dra. María Isabel Cristina González Suárez
Gerente Vigencia 2024 - 2028

Tabla de Contenido

1. INTRODUCCION

La Política de Seguridad, Confidencialidad, Privacidad de la Información y la Protección de los Datos es la declaración general que representa la posición de la ESE HOSPITAL SAN RAFAEL NIVEL II con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

2. OBJETIVOS:

La ESE Hospital San Rafael Nivel II, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información

Objetivo General

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

Objetivos Específicos

A. Mitigar los riesgos de la entidad.
B. Cumplir con los principios de seguridad de la información.
C. Cumplir con los principios de la función administrativa.
D. Mantener la confianza de los funcionarios, contratistas y terceros.
E. Apoyar la innovación tecnológica.
F. Implementar el sistema de gestión de seguridad de la información.
G. Proteger los activos de información.

H. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
I. Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos del ESE Hospital San Rafael Nivel II.
J. Garantizar la continuidad del servicio frente a incidentes.

3. ALCANCE:

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la ESE Hospital San Rafael Nivel II y la ciudadanía en general.

4. RESPONSABLE:

Ing. Talma Leonor Quintero Morales.

5. TERMINOS Y DEFINICIONES

6. NORMATIVIDAD APLICABLE:

N°	DESCRIPCION	INTERNA	EXTERNA
1	Ley 1712 de 2014, art 4	Acceso a la Información Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.	
2	ISO/IEC 27000 - ISO/IEC 27001	Activo en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.	
3	Ley 594 de 2000, art 3	Archivo Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.	
4	Ley 1581 de 2012, art 3	Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el	

		Tratamiento de datos personales	
5	Ley 1581 de 2012, art 3	Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables	
6	Decreto 1377 de 2013, art 3	Datos Personales Públicos Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.	
7	Norma ISO 20000	Su objetivo es proporcionar un control continuo, una mayor eficiencia y oportunidades para seguir mejorando. Eso significa trabajar dentro de su organización para alinear el personal y los procedimientos de su servicio al cliente, servicios de apoyo, prestación de servicios y equipo de operaciones.	
8	Norma ISO 20000-1	permite la gestión de servicios de TI de forma metódica a través de la implementación del PHVA (Planear – Hacer – Verificar – Actuar) que ha sido la estructura base y más exitosa de las normas ISO	

7. METODOLOGIA

7.1. PLATAFORMA ESTRATEGICA:

7.1.1. MISION

Somos una Empresa Social del Estado que presta servicios de salud integrales de baja y mediana complejidad en el departamento de La Guajira, con oportunidad, continuidad, seguridad y humanización; teniendo como pilar la gestión del conocimiento para fortalecer el talento humano, mediante la educación e investigación en salud, con base en los principios fundacionales de un hospital para todos, orientado por la ética, la inclusión social y la excelencia en la práctica clínica encaminados a la sostenibilidad financiera con responsabilidad social a través de recursos físicos y tecnológicos que garantizan la satisfacción de nuestros usuarios y sus familias.

7.1.2. VISION

Durante los próximos cuatro años la ESE Hospital San Rafael Nivel II de San Juan del Cesar, mantendrá el posicionamiento como la principal institución de salud en el departamento de La Guajira, prestando servicios con altos estándares de acreditación, atención diferencial, fortalecimiento financiero, desarrollo sostenible, líder referente en atención humanizada, conocimiento, investigación e innovación.

7.1.3. VALORES CORPORATIVOS

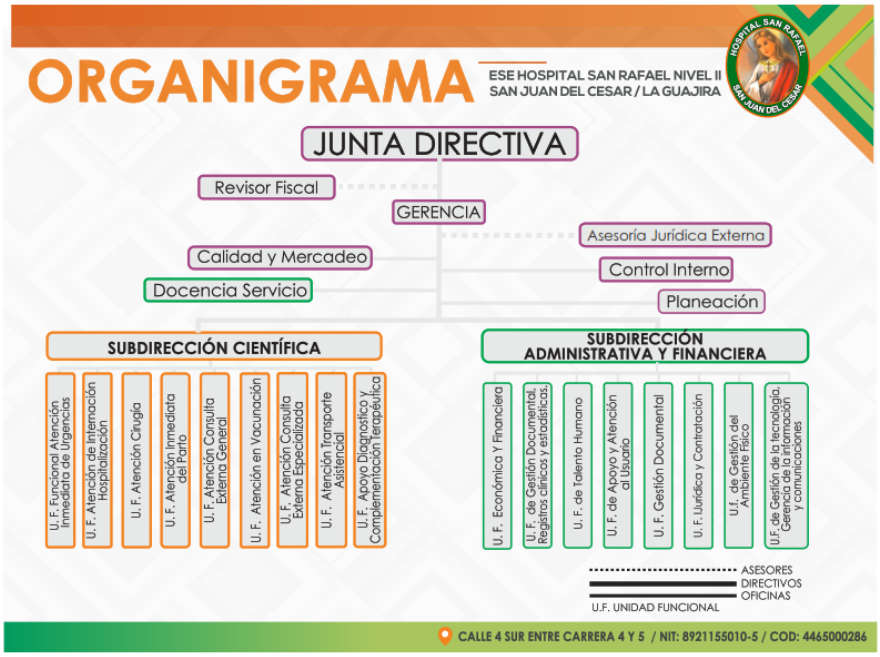
- **Respeto:** Valoramos el trabajo de nuestros colaboradores; cumplimos con la normatividad vigente y los protocolos de atención; comprendemos y valoramos los intereses y necesidades de nuestros usuarios sin discriminarlos ni ofenderlos.
- **Justicia:** Reconocemos y protegemos los derechos de cada persona, de acuerdo con sus necesidades y condiciones, defendemos la ética y moral que deben estar siempre presente en la atención a nuestros usuarios. Somos fieles y sentimos gratitud por nuestra Institución.
- **Compromiso:** Actuamos en forma correcta en el desarrollo de los roles asignados y las tareas encomendadas. Buscamos alcanzar altos niveles de rendimiento en aras de la máxima satisfacción de nuestros usuarios; asumimos el rol de servidor público que nos corresponde, entendiendo el valor de los compromisos y responsabilidades con los usuarios de los servicios que la institución presta.
- **Honestidad:** Buscamos siempre ser decentes, pudorosos, dignos, veraces y sinceros. Caminando hacia la rectitud y la honradez en la forma de ser y de actuar.
- **Diligencia:** Nos sentimos obligados a usar responsablemente los recursos públicos para cumplir las obligaciones que nos corresponden; se cumple con el tiempo estipulado para cada obligación, asegurando la calidad del servicio y los productos que se entregan.

7.1.4. PRINCIPIOS CORPORATIVOS

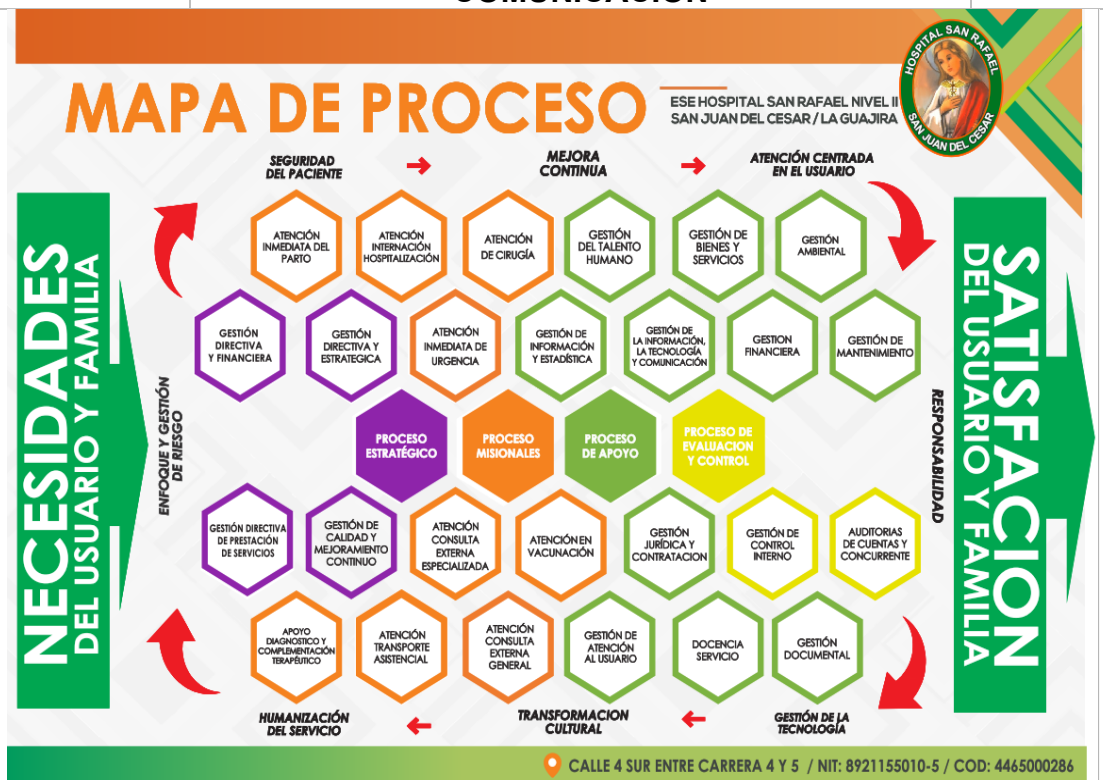
- **Trabajo en equipo**: Cada uno de los colaboradores aporta acciones valiosas y pertinentes en la consecución de objetivos comunes, Se establecen objetivos precisos y se establecen los aportes de cada miembro del equipo para llegar con éxito al resultado deseado.
- **Humanización:** Sentimos solidaridad, consideración y empatía por nuestros usuarios, respetamos sus derechos y le hacemos conocer sus deberes.
- **Orden:** Somos disciplinados, acatamos la legislación vigente y los lineamientos de la Institución; mantenemos en nuestras acciones equilibrio, paz y armonía.
- **Igualdad:** Todos y cada uno de nuestros usuarios gozan de los mismos derechos y tienen acceso a las mismas oportunidades sin ningún distingo. Damos un trato equitativo.

- **Transparencia**: Desempeñamos de la mejor manera el trabajo asignado, procuramos que nuestros usuarios entiendan claramente nuestras intenciones, acciones y procederes.
- **Excelencia**: Trabajamos incansablemente hacia el éxito, con disciplina y responsabilidad. Buscamos siempre ser mejores cada día para llegar a la meta.
- **Enfoque diferencial**: reconocemos las condiciones y posiciones de los distintos actores sociales, desde una mirada diferencial de estado socioeconómico, género, etnia, discapacidad e identidad cultural.
- **Mejoramiento Continuo**: trabajamos continuamente en las acciones que permiten que los procesos y la empresa sean más competitivos en la satisfacción del cliente interno y externo.

7.1.5. ORGANIGRAMA



7.1.6. MAPA DE PROCESOS



7.1.7. POLITICAS INSTITUCIONALES

7.1.7.1. IAMII

La E.S.E Hospital San Rafael Nivel II, utiliza la estrategia IAMII (INSTITUCION AMIGA DE LA MUJER Y LA INFANCIA INTEGRAL) con enfoque integral, haciendo énfasis en aspectos tales como: lactancia materna, parto natural, nutrición infantil, seguimiento al crecimiento y desarrollo y procura siempre de la buena relación niño-madre-entorno.

7.1.7.2. HUMANIZACION Y BUEN TRATO AL USUARIO, SU FAMILIA Y CLIENTE INTERNO

La ESE Hospital San Rafael Nivel II de San Juan del Cesar, como elemento fundamental durante la atención y prestación de sus servicios, mantiene el respeto, privacidad, dignidad, comunicación y diálogo con el usuario y su familia; ofreciendo una asistencia integral y cálida, garantizando el buen trato, con normas definidas de comportamiento tanto para el cliente interno y externo de la entidad, bajo el respeto de sus derechos como ser humano.

7.1.7.3. CALIDAD Y MEJORAMIENTO CONTINUO

En la ESE Hospital San Rafael Nivel II de San Juan del Cesar, estamos comprometidos a prestar servicios de atención en salud a los usuarios y su familia, bajo el cumplimiento estricto de los requisitos obligatorios, velando por el mejoramiento continuo, monitoreando indicadores de calidad y avanzando en la obtención de estándares superiores, con personal humanizado y competente que permita la transformación cultural con responsabilidad social.

7.1.7.4. PRESTACIÓN DE SERVICIOS DE SALUD

La ESE Hospital San Rafael Nivel II en reconocimiento de los lineamientos de la Política Nacional de Prestación de Servicios de Salud, se compromete a brindar a los usuarios y sus familias una atención integral, de calidad y segura, centrada en el paciente como ser humano digno, sin discriminación; en un ambiente favorable para la docencia y la investigación, enmarcada en los componentes del Sistema Obligatorio de Garantía de la Calidad en Salud (SOGCS), en concordancia con nuestro nivel de complejidad y responsabilidad social.

7.1.7.5. GESTION ESTRATEGICA DEL TALENTO HUMANO

La ESE Hospital San Rafael Nivel II se compromete a la gestión del talento humano, cumpliendo con el ciclo de planeación, vinculación, desarrollo y retiro, buscando la satisfacción de sus necesidades, expectativas y al fortalecimiento de capacidades y competencias, promoviendo la transformación cultural institucional en un ambiente de dignidad y respeto.

7.1.7.6. ADMINISTRACION DEL RIESGO

La ESE Hospital San Rafael Nivel II se compromete a gestionar las estrategias necesarias para una adecuada administración del riesgo de la entidad, que permita que desde cada proceso se realice la identificación, valoración, análisis y tratamiento de los riesgos, contribuyendo así al cumplimiento de la plataforma estratégica, planes y proyectos institucionales.

7.1.7.7. POLITICA DE INTEGRIDAD

La ESE Hospital San Rafael Nivel II se compromete a trabajar en la promoción de una cultura de integridad, que sirva como guía de comportamiento para sus colaboradores que con lleve hacia el logro de una gestión, caracterizada por el actuar honesto, ético, profesional enmarcado en la transparencia, la eficiencia, la eficacia, y la clara orientación hacia el cumplimiento de los fines esenciales del Estado y consolidar la confianza de la ciudadanía.

7.1.7.8. SEGURIDAD Y SALUD EN EL TRABAJO

La ESE Hospital San Rafael Nivel II se compromete desde la alta gerencia a gestionar los recursos necesarios para el diseño, implementación, evaluación y mejoramiento continuo del Sistema de Gestión en Seguridad y Salud en el Trabajo, la protección integral de todos sus colaboradores y el ambiente, promoviendo acciones encaminadas a prevenir incidentes, accidentes, enfermedades laborales, fomentando hábitos de vida saludables y el desarrollo de la protección a la vida y la salud de sus colaboradores.

7.1.7.9. AMBIENTE FISICO

La E.S.E Hospital San Rafael Nivel II promueve acciones de prevención de consumo de alcohol y otras sustancias psicoactivas y cultura de no fumador, para contribuir a mejorar el bienestar de los usuarios y colaboradores, que permitan un adecuado desempeño del personal, fundamentados en principios de igualdad, confidencialidad y equidad.

7.1.7.10. GESTION AMBIENTAL

La E.S.E. Hospital San Rafael Nivel II, reconoce su responsabilidad social de preservar el medio ambiente, mitigando el impacto ambiental que pueda afectar el entorno local, regional y global, implementando programas que promuevan la educación, concientización y participación de sus colaboradores en el uso eficiente de los recursos y la conservación de un ambiente sano y seguro, velando por la bioseguridad del cliente interno, usuario, familia y la comunidad.

7.1.7.11. GESTIÓN DE TECNOLOGÍA

La ESE Hospital San Rafael Nivel II se compromete a implementar un sistema de gestión a través del ciclo de adquisición, buen uso, control y disposición final de la tecnología, de acuerdo a las necesidades de cada uno de los servicios prestados en la entidad; propendiendo por la adecuada manipulación tecnológica, calidad, seguridad en la atención, satisfacción de los usuarios y preservación del medio ambiente, contribuyendo al logro de la plataforma estratégica.

7.1.7.12. POLÍTICA DE SEGURIDAD, CONFIDENCIALIDAD, PRIVACIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LOS DATOS

El Hospital está comprometido en actuar con responsabilidad, ética y profesionalismo para proteger la privacidad, confidencialidad y respeto de la información que obtiene, registra, usa, transmite y actualiza, mediante autorización previa, expresa y voluntaria del titular de la información en bases de datos y archivos físicos, además se compromete a garantizar los recursos financieros necesarios para el mejoramiento tecnológico e infraestructura requerida para que a los servidores públicos se les facilite el cumplimiento de este compromiso.

7.1.7.13. POLITICA DE RELACIÓN DOCENCIA-SERVICIO, INVESTIGACIÓN Y EDUCACION CONTINUADA

La ESE Hospital San Rafael Nivel II se compromete a gestionar escenarios de práctica e investigación idóneos, desarrollando habilidades, competencias y transferencia de conocimiento al personal de prácticas, que garantice una formación integral y una atención segura, humanizada hacia los pacientes y su familia, al igual que educación continuada a los miembros de la junta directiva y colaboradores de la ESE con el fin de contar con un talento humano actualizado y competente.

7.1.7.14. SEGURIDAD DEL PACIENTE

Desde el direccionamiento estratégico, la seguridad del paciente se incorpora como un compromiso institucional a través de la EXCELENCIA, entendida como la calidad de nuestros procesos en atributos de seguridad, satisfacción, eficiencia, pertinencia y oportunidad. Es así como la ESE Hospital San Rafael Nivel II, se compromete con la seguridad del paciente, como la iniciativa para hacer más seguros los procesos institucionales, impactar en la mejora de la calidad y proteger a los pacientes de los riesgos evitables que se derivan de la atención en salud.

7.1.7.15. POLITICA DE TRASNFORMACION CULTURAL Y RESPONSABILIDAD SOCIAL

La E.S.E Hospital San Rafel Nivel II promueve acciones de prevención de consumo de alcohol y otras sustancias psicoactivas y cultura de no fumador, para contribuir a mejorar bienestar de los usuarios y colaboradores, que permitan un adecuado desempeño del personal, fundamentados en principios de igualdad, confidencialidad y equidad.

7.1.7.16. POLITICA DE COMUNICACIONES Y TRANSPARENCIA DE LA INFORMACION

La ESE Hospital San Rafael Nivel II, con el fin de propiciar la educación e información a los usuarios, fortalecer la comunicación y espacios de transparencia institucional con sus grupos de interés (stakeholders), se compromete a manejar y divulgar la información de manera clara, veraz y oportuna a través de los distintos canales de comunicación institucionales generando condiciones para la sana discusión y el desarrollo de una gestión transparente.

7.1.7.17. POLITICA RACIONAL DE ANTIBIOTICOS

La ESE Hospital San Rafael Nivel II se compromete a Generar lineamientos en la práctica asistencial que permitan el uso racional en la utilización de los antimicrobianos evitando que se dificulte o retrase la resolución de un proceso infeccioso y cause efectos secundarios innecesarios, que favorezca la aparición de microorganismos resistentes que puedan originar infecciones sistémicas o colonizaciones de difícil erradicación y evitar el aumento en el gasto farmacéutico sin obtener una mejora en la eficacia terapéutica; además contribuir con el bienestar de la sociedad por medio de estrategias educativas tanto a nuestros usuarios y colaboradores.

7.1.7.18. POLITICA GESTION DE LA TECNOLOGIA

La ESE Hospital San Rafael Nivel II se compromete a implementar un sistema de gestión a través del ciclo de adquisición, buen uso, control y disposición final de la tecnología, de acuerdo a las necesidades de cada uno de los servicios prestados en la entidad; propendiendo por la adecuada manipulación tecnológica, calidad, seguridad en la atención, satisfacción de los usuarios y preservación del medio ambiente, contribuyendo al logro de la plataforma estratégica.

8. CONTENIDO DEL PLAN:

8.1. Generalidades

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

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

8.2. Gestión de Activos Seguridad, confidencialidad, privacidad de la información y la protección de los datos

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

El facilitador del proceso de Gestión de Recursos Físicos con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

8.2.1. Pautas para tener en cuenta

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

- La información física y digital de la ESE Hospital San Rafael Nivel II debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

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

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

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

8.3. Control de Acceso

8.3.1. Procedimiento de acceso a redes y recursos de red

El Ingeniero de sistemas de la ESE Hospital San Rafael Nivel II, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

8.3.1.1. Pautas para tener en cuenta

- El proceso Gestión de TIC debe asegurar que las redes inalámbricas de la ESE Hospital San Rafael Nivel II cuenten con métodos de autenticación que evite accesos no autorizados.

- El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la ESE Hospital San Rafael Nivel II, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos

- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la ESE Hospital San Rafael Nivel II, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la ESE Hospital San Rafael Nivel II deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

8.3.2. Procedimiento de administración de acceso de usuarios

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

8.3.2.1. Pautas para tener en cuenta

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

- El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados

sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

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

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

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

8.3.3. Procedimiento de control de acceso a sistemas de información y aplicativos

La ESE Hospital San Rafael Nivel II como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.
El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

8.3.3.1. Pautas para tener en cuenta

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

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

- El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de la ESE Hospital San Rafael Nivel II.

- El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean

acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

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

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

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

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

8.3.4. Procedimiento de seguridad física

La ESE Hospital San Rafael Nivel II provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

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

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

Pautas para tener en cuenta

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

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

- La Sub Dirección Administrativa debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la ESE Hospital San Rafael Nivel II.

- La Sub Dirección Administrativa debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

- Los ingresos y egresos de personal a las instalaciones de la ESE Hospital San Rafael Nivel II en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la ESE Hospital San Rafael Nivel II; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

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

8.3.5. Procedimiento de seguridad para los equipos

La ESE Hospital San Rafael Nivel II para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta

- El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la ESE Hospital San Rafael Nivel II.

- El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

- El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

- El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

- El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

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

- El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la ESE Hospital San Rafael Nivel II cuente con la autorización documentada y aprobada previamente por el área.

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

- El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la ESE Hospital San Rafael Nivel II.

- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.

- Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la ESE Hospital San Rafael Nivel II, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

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

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

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

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

- En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

- Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

8.3.6. Procedimiento de uso adecuado de internet

La ESE Hospital San Rafael Nivel II consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

Pautas para tener en cuenta

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

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

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

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

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

- Los usuarios del servicio de Internet de la ESE Hospital San Rafael Nivel II deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

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

- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea, redes sociales otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la ESE Hospital San Rafael Nivel II.

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

- No está permitido el intercambio no autorizado de información de propiedad de la ESE Hospital San Rafael Nivel II, de los funcionarios, con terceros.

8.4. PRIVACIDAD Y CONFIDENCIALIDAD

Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la ESE Hospital San Rafael Nivel II a través del Comité de Seguridad de la Información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

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

Pautas para tener en cuenta

- Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
- Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
- El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de la ESE Hospital San Rafael Nivel II de los cuales reciba y administre información.
- El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
- Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
- Los usuarios de los portales de la ESE Hospital San Rafael Nivel II deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

8.4.1. Disponibilidad del servicio e información

La ESE Hospital San Rafael Nivel II con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidió crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

8.4.2. Procedimiento de continuidad, contingencia y recuperación de la información

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

8.4.3. Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de la ESE Hospital San Rafael Nivel II deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.
El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.
Pautas para tener en cuenta

- El Comité de Seguridad de la Información, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- El Comité de Seguridad de la Información, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres
- El Comité de Seguridad de la Información debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- El Comité de Seguridad de la Información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información
- El Comité de Seguridad de la Información, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de

entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

9. RECURSOS

- **Humano**: Aplica para todo el personal de la institución que maneja información.
- **Físico:** Firewall, PC y equipos de comunicación.

10. TIEMPO DE EJECUCION – CRONOGRAMA DE ACTIVIDADES:

NIT:892115010-5 COD: 4465000286	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION			Versión:1.0
	GESTION DIRECTIVA Y ESTRATEGICA			Página 1 de 1
ACTIVIDADES	**FECHA DE CUMPLIMIENTO**	**INDICADOR DE LOGRO**	**META**	**RESULTADO**
Administración de acceso de usuarios | Acceso a sistemas de información y aplicativos		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	
Seguridad física | Ubicación del servidor		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	
Seguridad para los equipos | Mantenimiento y Backups		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	
Uso adecuado de internet		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	
Disponibilidad del servicio e información		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	
Contingencia y recuperación de la información (R-FAST)		(N° DE ACTIVIDADES DESARROLLADAS EN EL PERIODOEN EL PLAN / NRO DE ACTIVIDADES PROPUESTAS EN EL PERIODO EN EL PLAN DE TRABAJO) X 100	100%	

11. PRESUPUESTO: N/A

12. DIFUSION:

Mediante socialización a todos los funcionarios de la ESE Hospital San Rafael Nivel II se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.hsrafaelsanjuan.gov.co.

Una vez aprobado el (manual, guía, protocolo, programa) por la Gerencia, revisados por Subdirección científica / Subdirección administrativa / Asesor de Calidad, el referente del proceso será el responsable cumplimiento de cada una de las actividades descritas, además se realizará el despliegue y la comprensión de la información a los responsables de las actividades dejando evidencia de la reunión de difusión respectiva. La oficina de Gestión de la Calidad tendrá bajo su custodia y control documental los documentos originales impresos.

13. SEGUIMIENTO Y EVALUACION:

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario

14. REFERENCIAS BIBLIOGRAFICAS

No aplica

15. CONTROL DE CAMBIO:

Versión	Descripción De Los Cambios	Fecha
1.0	Se crea el documento	28/01/2021
2.0	Actualización de acuerdo 07 de 2021 por medio del cual se modifica la estructura orgánica de la institución, se actualiza mapa de procesos, manual de procesos y procedimientos de la ESE. Actualización de plantillas institucionales	28/01/2022
3.0	Actualización de políticas institucionales	24/01/2023
4.0		31/01/2025

16. CONTROL DEL DOCUMENTO:

Talma Quintero Morales **Líder Sistemas y T.**	Walter E. Coronel **Subdir. Administrativo** Viktor Petit **Asesor de Planeación**	María Isabel González **Gerente**	30/01/2025	Acta N° 02 del comité de Gestión y Desempeño
Elaboró/Actualizó	**Revisó**	**Aprobó**	**Fecha Ultima aprobación**	**Medio de aprobación**