Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

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

El presente plan se realiza con el objeto de dar a conocer cómo se desarrollará la implementación y socialización del componente de la Estrategia en **seguridad y privacidad de la información**, el cual busca guardar los datos de los usuarios como un tesoro, garantizando la seguridad de la información.

2. OBJETIVOS:

2.1. Objetivo General

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la ESE HOSPITAL SAN RAFAEL NIVEL II con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

2.2. Objetivos Específicos

- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la ESE HOSPITAL SAN RAFAEL NIVEL II para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Aplicar las metodologías del DAFP e ISO respectivamente en seguridad y riesgo de la información para la ESE HOSPITAL SAN RAFEL NIVEL II.

3. ALCANCE:

Poner en funcionamiento una administración de riesgos de seguridad y privacidad de la información, en cualquiera de las formas que se manejen (física-digital), que den continuidad segura y confiable en todos los procesos de la institución.

4. RESPONSABLE:

Líder de Sistemas.

5. TERMINOS Y DEFINICIONES:

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas,

soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000-ISO/IEC 27001).

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

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los usuarios, 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. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000- ISO/IEC 27001).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000- ISO/IEC 27001).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000- ISO/IEC 27001).

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

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

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

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

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

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

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

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado

civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

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

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

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

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

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

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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

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

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000- ISO/IEC 27001).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000- ISO/IEC 27001).

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

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000- ISO/IEC 27001).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000- ISO/IEC 27001).

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

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000- ISO/IEC 27001).

6. NORMATIVIDAD APLICABLE: (Interna y/o Externa)

N°	DESCRIPCION	INTERNA	EXTERNA
1	ISO/IEC 27001		X

2	LEY 1581 DE 2012, ART 3		**X**
3	LEY 1712 DE 2014, ART 4		**X**
4	LEY 1581 DE 2012, ART 3 LITERAL H		**X**

7. METODOLOGIA

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la ESE HOSPITAL SAN RAFAEL NIVEL II, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

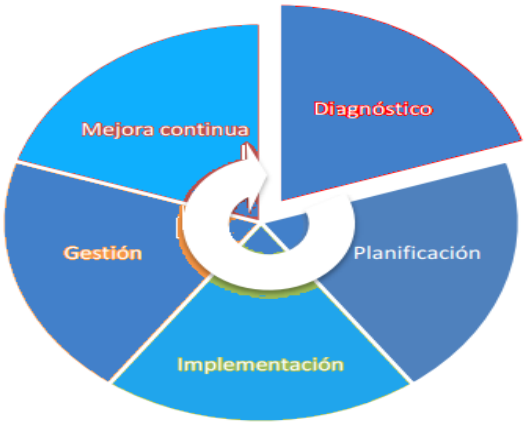


Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

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.

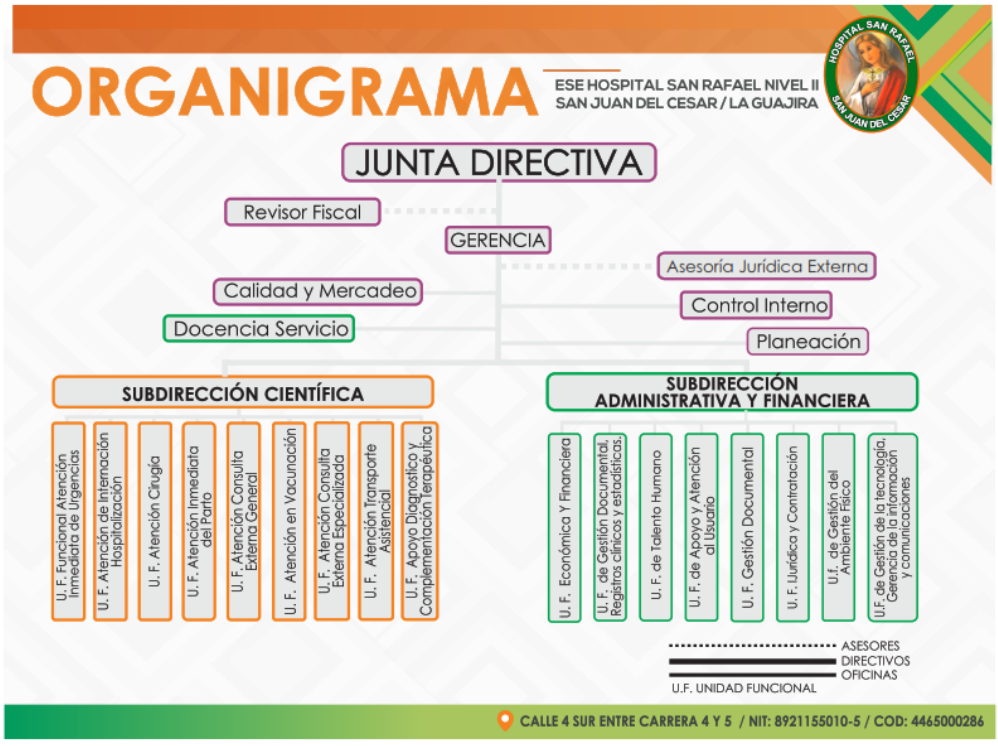
7.1.4. PRINCIPIOS CORPORATIVOS

- **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

7.2. POLITICAS INSTITUCIONALES

7.2.1. 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.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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.

7.2.5. 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.

7.2.6. 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.

7.2.7. 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.

7.2.8. 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.

7.2.9. 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.

7.2.10. 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.

7.2.11. 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.

7.2.12. 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.

7.2.13. 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.

7.2.14. 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.

7.2.15. 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.

7.2.16. 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.

7.2.17. 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.

7.2.18. 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:

- Realizar Diagnóstico
- Elaborar el Alcance del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- Realizar la Identificación de los Riesgos con los líderes del Proceso.
- Entrevistar con los líderes del Proceso
- Valorar del riesgo y del riesgo residual
- Realizar Mapas de calor donde se ubican los riesgos
- Plantear al plan de tratamiento del riesgo aprobado por los lideres

9. RECURSOS:

Humano: Gerente, Subgerentes, Líderes del Proceso, Profesionales de Sistema y Tecnología, Personal Externo

Físico: Firewall, PC y equipos de comunicación

10. TIEMPO DE EJECUCION – CRONOGRAMA DE ACTIVIDADES:

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDA Y PRIVACIDAD DE LA INFORMACION - VIGENCIA 2025

ACTIVIDAD	FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
SEMANAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar Diagnostico																																												
Elaborar el alcance del Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información																																												
Realizar la identificaci																																												

ón de los Riesgos con los Lideres del proceso																																												
Entrevista con los Lideres del Proceso																																												
Valoración del Riesgo residual																																												
Mapa de calor donde se ubican los Riesgos																																												
Seguimiento y control																																												

11. PRESUPUESTO

Se debe apoyar con la oficina de Subdirección administrativa y planeación para la realización de los estudios de mercados previos.

12. DIFUSION:

Capacitación, difusión por correo, publicación etc.

13. SEGUIMIENTO Y EVALUACION:

Al finalizar cada etapa se realizará una reunión con la Oficina de Planeación y Control Interno para presentar el informe del avance del plan y de esta manera evaluar todos los pasos que se han realizado.

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	Actualización de vigencia	31/01/2025
5.0	Actualización de vigencia	30/01/2026

16. CONTROL DEL DOCUMENTO:

Talma Quintero Morales **Líder de Sistemas y Tecnología**	Walter E. Coronel **Subdir. Administrativo** Viktor Petit **Asesor de Planeación**	María Isabel González Suarez **Gerente**	30/01/2026	Acta N° 02 del comité de Gestión y Desempeño
Elaboró/Actualizó	**Revisó**	**Aprobó**	**Fecha Ultima aprobación**	**Medio de aprobación**

*Original Firmado