E.S.E. HOSPITAL
San Rafael
DE ITAGÜÍ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

CONTENIDO

1 JUSTIFICACIÓN

La E.S.E. Hospital San Rafael de Itagüí, en cumplimiento de sus funciones misionales, administrativas y de apoyo, gestiona diariamente un volumen significativo de información, incluyendo datos personales, datos sensibles de salud, información financiera, contractual y administrativa, cuya protección resulta crítica para garantizar la continuidad del servicio, la confianza de los usuarios y el cumplimiento de las obligaciones legales.

En un contexto institucional cada vez más dependiente de plataformas tecnológicas, sistemas de información clínicos y administrativos, servicios en red y canales digitales, la seguridad y privacidad de la información se constituye en un pilar estratégico para la sostenibilidad organizacional y la adecuada prestación del servicio público de salud. El incremento de amenazas cibernéticas, accesos no autorizados, errores humanos y fallas tecnológicas hace necesario adoptar medidas preventivas, correctivas y de mejora continua que reduzcan la exposición al riesgo.

El presente Plan de Seguridad y Privacidad de la Información para la vigencia 2026 establece el marco estratégico, operativo y normativo para la implementación y fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), como componente fundamental de la Política de Gobierno Digital y del Modelo Integrado de Planeación y Gestión – MIPG.

Este plan se formula conforme a los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, integrándose al Plan de Acción Institucional de acuerdo con lo dispuesto en el Decreto 612 de 2018, y adoptando un enfoque de gestión del riesgo alineado con el ciclo de mejora continua Planear – Hacer – Verificar – Actuar (PHVA).
La implementación del Plan de Seguridad y Privacidad de la Información permitirá:

- Proteger los activos de información institucionales.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Fortalecer la cultura organizacional en seguridad digital.
- Prevenir, detectar y responder oportunamente a incidentes de seguridad de la información.
- Asegurar el cumplimiento de la normatividad vigente en materia de protección de datos personales, transparencia y seguridad digital.
- Proporcionar evidencia verificable ante auditorías internas, externas y entes de control.

La Alta Dirección manifiesta su compromiso con la implementación, seguimiento y mejora del MSPI, disponiendo los responsables institucionales y promoviendo el cumplimiento de las políticas, procedimientos y controles definidos en el presente plan.

2 ENFOQUE DIFERENCIAL

La E.S.E. Hospital San Rafael de Itagüí reconoce la diversidad de la población a la que presta sus servicios y adopta el enfoque diferencial como principio transversal en la gestión institucional de la información. Este enfoque reconoce la existencia de poblaciones con características particulares asociadas a edad, género, etnia, condición de discapacidad, orientación sexual, víctimas del conflicto armado u otras condiciones de vulnerabilidad.

En este sentido, la gestión de la seguridad y privacidad de la información incorpora medidas específicas que garantizan la protección reforzada de los datos personales y sensibles de estas poblaciones, evitando cualquier forma de discriminación, uso indebido o acceso no autorizado.

El tratamiento de la información se realiza en coherencia con el manual institucional “Atención en salud con enfoque diferencial” MN-04-AT, asegurando que los controles de acceso, los procesos de custodia documental y las medidas de seguridad tecnológica respeten los derechos fundamentales de los titulares de la información.

3 OBJETIVO GENERAL

Establecer e implementar el Plan de Seguridad y Privacidad de la Información para la vigencia 2026 en la E.S.E. Hospital San Rafael de Itagüí, como instrumento estratégico orientado a la protección integral de los activos de información institucionales, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, en cumplimiento de la normatividad vigente y en coherencia con los objetivos institucionales.

3.1 OBJETIVOS ESPECÍFICOS

- Proteger los activos de información institucionales mediante la implementación de controles administrativos, técnicos y físicos acordes con el MSPI.
- Identificar, analizar, evaluar y tratar los riesgos de seguridad y privacidad de la información, manteniéndolos en niveles aceptables.
- Fortalecer la cultura organizacional de seguridad digital mediante programas permanentes de capacitación, sensibilización y divulgación.
- Garantizar el cumplimiento de las disposiciones legales, reglamentarias y normativas relacionadas con seguridad digital, protección de datos personales y transparencia.
- Establecer políticas, procedimientos y lineamientos claros para el uso, manejo, acceso, custodia, respaldo y transferencia de la información.
- Implementar mecanismos de prevención, detección, gestión y respuesta ante incidentes de seguridad de la información.
- Generar información confiable y segura como soporte para la toma de decisiones institucionales.

4 RESPONSABLE(S) DEL PLAN

La responsabilidad de la formulación, implementación, seguimiento y actualización del Plan de Seguridad y Privacidad de la Información estará a cargo del Área de Tecnologías y Sistemas de Información, en articulación con:

- Oficina Asesora de Planeación y Calidad
- Oficina Asesora Jurídica
- Gestión del Talento Humano
- Oficina de Control Interno
- Líderes de procesos estratégicos, misionales y de apoyo

La Alta Dirección ejercerá supervisión y direccionamiento estratégico a través del Comité Institucional de Gestión y Desempeño.

5 DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión 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 ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **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. (Ley 594 de 2000, art 3)
- **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).
- **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)

- **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).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **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 ciudadano, 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 Mixtos**: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **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 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 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)
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **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)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección** de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **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).
- **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).
- **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **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 en cualquier medio: impreso o digital. (ISO/IEC 27000).

- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (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).
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6 META

Alcanzar la implementación efectiva de al menos el 90 % de las acciones y medidas definidas en el Plan de Seguridad y Privacidad de la Información al finalizar el año fiscal en curso, garantizando el cumplimiento de los lineamientos establecidos en el Decreto 612 de 2018 y demás disposiciones normativas aplicables.

Al finalizar la vigencia 2026, alcanzar:

- **≥ 90%** de ejecución de actividades del Plan MSPI 2026.
- **100%** de seguimiento trimestral del avance (4 cortes).
- **≥ 90%** de cobertura del personal objetivo en sensibilización/capacitación anual.

7 MARCO NORMATIVO

- Constitución Política de Colombia (Art. 15, 209, 269).
- Ley 1581 de 2012 (Protección de datos personales) y Decretos reglamentarios (1377 de 2013, 886 de 2014 y demás compilatorios aplicables).
- Ley 1712 de 2014 y Decreto 103 de 2015 (Transparencia y acceso a la información).
- Decreto 1078 de 2015 (Decreto Único Sector TIC).
- Decreto 1499 de 2017 (MIPG).
- Decreto 612 de 2018 (Planes institucionales integrados al Plan de Acción).
- Decreto 2106 de 2019 (Seguridad digital en trámites/procesos por medios digitales).
- CONPES 3854 de 2016 (Seguridad digital) y CONPES 3995 de 2020 (Confianza y Seguridad Digital).
- Resolución MinTIC 500 de 2021 (Lineamientos estrategia de seguridad digital y adopción MSPI).
- Resolución MinTIC 746 de 2022 (Fortalece el MSPI y lineamientos adicionales).
- Resolución MinTIC 02277 de 2025 (Actualiza el Anexo 1 de la Res. 500/2021 y ajusta estándares).
- Decreto 338 de 2022 (Gobernanza de seguridad digital, infraestructuras críticas cibernéticas y servicios esenciales).

- ISO/IEC 27001:2022 e ISO/IEC 27005:2022 como estándares de referencia (no certificación obligatoria).

8 DIAGNOSTICO

El presente diagnóstico tiene como finalidad establecer el estado actual de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital San Rafael de Itagüí, a través del uso de la herramienta oficial de autodiagnóstico, con el fin de identificar las brechas existentes, determinar el nivel de madurez de la entidad en materia de seguridad de la información y establecer los insumos clave para la planificación estratégica y la mejora continua del modelo.
Incluye:

- Análisis GAP
- Resultados del autodiagnóstico
- Análisis interno
- Recomendaciones iniciales

8.1 Análisis GAP – Herramienta de Autodiagnóstico

La evaluación se realizó utilizando la herramienta de autodiagnóstico del MSPI dispuesta por el Ministerio TIC, la cual permite valorar la existencia, pertinencia y efectividad de los controles relacionados con las dimensiones clave del modelo, tales como: gobierno de la seguridad, gestión de riesgos digitales, gestión de incidentes, formación y concientización, infraestructura tecnológica, y continuidad del negocio.

8.2 Resultados del Autodiagnóstico

A partir del análisis, se evidenció lo siguiente:

- **Nivel de implementación general del MSPI:** Bajo. La entidad presenta un avance inicial en la adopción formal del modelo.
- **Controles implementados**: Se cuenta con mecanismos básicos de protección de la información, especialmente en lo relacionado con el respaldo de bases de datos, control de accesos físicos y lógicos, y algunas prácticas de uso responsable de las TIC.
- **Controles faltantes o en estado parcial:**
  - No se cuenta con un SGSI formalizado ni certificado.
  - Falta consolidar políticas institucionales en seguridad digital aprobadas por la alta dirección.
  - No se ha implementado un procedimiento integral para la gestión de incidentes de seguridad de la información.
  - Falta seguimiento de indicadores de monitoreo y seguimiento periódicos para evaluar la efectividad de los controles implementados.
  - Limitada cobertura en programas de sensibilización y capacitación en seguridad de la información.

8.3 Análisis Interno

Durante el diagnóstico se revisaron componentes clave de la organización:

- **Talento humano:** Existe personal técnico con funciones asignadas en tecnología, sin embargo, no hay un rol específico de Oficial de protección de datos y seguridad de la Información.
- **Procesos y procedimientos:** Algunos procedimientos existen, pero no están alineados con las directrices del MSPI.
- **Cultura organizacional:** Se identifica baja apropiación de prácticas seguras en el uso de herramientas tecnológicas por parte del personal.
- **Infraestructura tecnológica:** Se cuenta con conectividad, servidores y sistemas operativos institucionales, pero se requiere robustecer los esquemas de protección frente a accesos no autorizados y ciber amenazas.
- **Recursos disponibles:** Limitaciones presupuestales restringen la adquisición de soluciones especializadas en ciberseguridad.

El Hospital San Rafael de Itagüí presenta un estado de madurez inicial en la implementación del MSPI. Se han desarrollado acciones puntuales en materia de seguridad tecnológica, pero aún se requiere estructurar formalmente el modelo, establecer roles y responsabilidades, y generar capacidades organizacionales para su sostenibilidad. Recomendaciones Iniciales:

- Establecer un Comité de Seguridad de la Información con representación de áreas clave.
- Formular y adoptar la Política Institucional de Seguridad y Privacidad de la Información.
- Definir un plan de formación y sensibilización continuo.
- Priorizar recursos técnicos y humanos para la implementación progresiva de controles del MSPI.

9 PLANIFICACION

La fase de planificación tiene como propósito estructurar, con base en los resultados del diagnóstico inicial, las acciones necesarias para implementar de manera efectiva el Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital San Rafael de Itagüí. Esta etapa permite definir el alcance del modelo, establecer responsabilidades institucionales, dimensionar los recursos humanos, técnicos y financieros requeridos, y proyectar el cronograma de ejecución de las actividades programadas.

Este proceso es esencial para garantizar una implementación ordenada, efectiva y medible del modelo, conforme a las disposiciones del Decreto 767 de 2022, el Decreto 612 de 2018 y las guías técnicas emitidas por el Ministerio TIC. A continuación, se describen los productos clave generados en esta fase:

- **Alcance del MSPI**: Define las áreas, procesos, sistemas de información, activos críticos y usuarios involucrados en la implementación del modelo, en coherencia con la estructura organizacional y el portafolio de servicios del hospital.

- **Plan**: Documento expedido por la Gerencia, mediante el cual se asignan formalmente las funciones, competencias y responsabilidades institucionales en materia de seguridad y privacidad de la información, incluyendo la designación de los responsables del MSPI y del SGSI.
- **Política de Seguridad y Privacidad de la Información:** Documento institucional que expresa el compromiso de la Alta Dirección con la protección de los activos de información, estableciendo principios rectores, lineamientos generales y criterios de cumplimiento para todo el personal y terceros vinculados.
- **Roles y Responsabilidades**: Documento que detalla los actores institucionales comprometidos con el MSPI, sus funciones específicas y el nivel de responsabilidad asignado en el marco de la gestión de la seguridad de la información.
- **Procedimiento de Inventario y Clasificación de Información**: Define el proceso mediante el cual se identifican, registran y clasifican los activos de información e infraestructura tecnológica crítica, según su nivel de sensibilidad y valor institucional.
- **Metodología de Clasificación**: Instrumento técnico que establece las categorías, criterios y niveles de confidencialidad, integridad y disponibilidad para clasificar la información institucional, alineado con estándares internacionales como ISO/IEC 27001 y 27005.
- **Procedimiento de Gestión de Riesgos:** Metodología adoptada por la E.S.E. para identificar, analizar, evaluar y tratar los riesgos de seguridad de la información, articulando las etapas del ciclo PHVA y alineando los controles con los riesgos priorizados.
- **Plan de Tratamiento de Riesgos**: Documento que especifica las medidas correctivas, preventivas y de mitigación que serán implementadas frente a los riesgos identificados, incluyendo responsables, tiempos y recursos asignados.
- **Manual de Políticas de Seguridad:** Compilación de las políticas específicas en materia de acceso, uso, respaldo, dispositivos móviles, contraseñas, redes, gestión de incidentes, entre otras, que regulan el comportamiento institucional frente a la seguridad de la información.
- **Plan de Capacitación, Sensibilización y Comunicación**: Estrategia institucional dirigida a fortalecer la cultura de seguridad digital mediante actividades formativas periódicas, campañas internas de sensibilización y mecanismos de comunicación eficaces para mantener informados a todos los actores involucrados.

Este componente de planificación constituye el cimiento técnico y operativo del Plan de Seguridad y Privacidad de la Información, permitiendo orientar con claridad las acciones a ejecutar, sus responsables, cronogramas y mecanismos de seguimiento. La estructuración adecuada de estos instrumentos garantiza la sostenibilidad del modelo y su integración con la gestión institucional del riesgo y la mejora continua.

9.1 Contexto de la entidad

9.1.1 Comprensión de la organización y de su contexto

La E.S.E. Hospital San Rafael de Itagüí es una institución prestadora de servicios de salud de carácter público, que cumple una función estratégica en el sistema de salud del Valle de Aburrá, ofreciendo servicios de atención primaria, ambulatoria, hospitalaria y especializada. Su

operación está regida por los principios de calidad, accesibilidad, seguridad del paciente, sostenibilidad financiera y gestión con enfoque en resultados.

En el desarrollo de su misión institucional, el hospital se encuentra expuesto a factores internos y externos que pueden impactar la seguridad de la información:

Factores internos:

- Procesos asistenciales y administrativos soportados en plataformas digitales.
- Personal técnico y clínico con acceso a información sensible de pacientes y de la gestión hospitalaria.
- Recursos tecnológicos en constante uso y evolución.
- Cultura organizacional en proceso de fortalecimiento frente a la ciberseguridad.

Factores externos:

- Crecientes amenazas cibernéticas a nivel sectorial y nacional.
- Interacciones con entidades reguladoras, EPS, entes territoriales y proveedores.
- Cumplimiento de lineamientos del MIPG, la Política de Gobierno Digital y estándares internacionales como ISO 27001.
- Expectativas de la ciudadanía en materia de protección de datos personales y transparencia.

La comprensión de este contexto permite ajustar la implementación del MSPI a las condiciones reales de la entidad, alineándose con los objetivos estratégicos definidos en el Plan de Desarrollo Institucional y el Modelo Integrado de Planeación y Gestión (MIPG).

9.1.2 Necesidades y expectativas de los interesados

La E.S.E. ha identificado a sus partes interesadas clave, internas y externas, cuyas necesidades deben ser consideradas para garantizar la eficacia del MSPI:

- Partes interesadas internas:
  - Servidores públicos y contratistas de áreas administrativas, asistenciales, tecnológicas y financieras.
  - Directivos y líderes de procesos.
  - Comité de Seguridad de la Información.

- Partes interesadas externas:
  - Pacientes y usuarios de los servicios de salud.
  - Entidades de control (Supersalud, MINSALUD, Contraloría, Procuraduría).
  - Proveedores tecnológicos y operadores logísticos.
  - Ministerio TIC y organismos del orden nacional.

- Principales necesidades y expectativas identificadas:
  - Confidencialidad y protección de los datos personales y clínicos.

- Accesibilidad segura a los sistemas de información.
- Trazabilidad y validación de la información institucional.
- Cumplimiento normativo (Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1437 de 2011, entre otras).
- Disponibilidad de canales de denuncia oportuna ante incidentes.

9.1.3 Definición del alcance del MSPI

El Modelo de Seguridad y Privacidad de la Información será implementado de forma transversal en todos los procesos estratégicos, misionales, de apoyo y de evaluación del Hospital San Rafael de Itagüí, haciendo énfasis en los siguientes elementos:

- Procesos cubiertos:
  - Gestión clínica (consulta externa, hospitalización, urgencias, farmacia, entre otros).
  - Gestión administrativa y financiera (talento humano, jurídica, cartera, archivo, entre otros).
  - Sistemas de información institucional (HIS, ERP, correos institucionales, aplicaciones en la nube).
  - Infraestructura tecnológica crítica: servidores, redes, sistemas de respaldo, datacenter local.

- Cobertura física:
  - Sede principal y puntos de atención descentralizados del hospital.

- Alcance funcional:
- Incluye activos de información físicos y digitales, personal interno y externo con acceso a sistemas institucionales, procedimientos asociados al tratamiento de datos, infraestructura TIC y procesos relacionados con la gestión de riesgos digitales.

Este alcance será documentado formalmente y podrá integrarse al Sistema Integrado de Gestión o al Modelo de Planeación y Gestión Institucional.

9.2 Política de seguridad y privacidad de la información

La E.S.E. Hospital San Rafael de Itagüí adopta el compromiso institucional de proteger sus activos de información como fundamento para garantizar la continuidad, calidad y confiabilidad de los servicios de salud que presta a la comunidad. En coherencia con su misión asistencial y su responsabilidad frente a los usuarios, la entidad promueve un entorno seguro para la gestión de la información, aplicando principios de confidencialidad, integridad y disponibilidad, y asegurando el cumplimiento de la normatividad vigente.

Esta política establece los lineamientos necesarios para prevenir, detectar y responder eficazmente ante amenazas que puedan comprometer los sistemas de información y la privacidad de los datos personales y clínicos, fomentando una cultura organizacional basada en el uso responsable, ético y seguro de la información.

Compromisos de acción institucionales

- La E.S.E. Hospital San Rafael de Itagüí se compromete a dar cumplimiento a los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad y privacidad de la información, incluyendo lo dispuesto en el Decreto 767 de 2022, la Ley 1581 de 2012, la Ley 1712 de 2014 y demás normas concordantes.
- La entidad promoverá la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la evaluación periódica de riesgos, el seguimiento a los controles implementados y la ejecución de planes de acción para fortalecer el sistema.
- Se adoptarán mecanismos para asegurar la confidencialidad, integridad y disponibilidad de la información institucional, protegiendo los sistemas, redes y documentos físicos ante amenazas internas y externas.
- La E.S.E. garantiza la difusión efectiva de esta política y sus compromisos entre todos los servidores públicos, contratistas y demás partes interesadas internas, promoviendo una cultura de seguridad y el cumplimiento de las directrices establecidas.
- Esta política estará disponible para las partes interesadas pertinentes, a través de medios físicos y digitales institucionales, asegurando su conocimiento y consulta oportuna.
- La entidad adoptará procedimientos para la identificación, reporte, análisis y atención de incidentes de seguridad de la información, mitigando su impacto y evitando su recurrencia.
- Se garantizará la asignación de roles claros, responsabilidades institucionales y recursos técnicos, humanos y financieros necesarios para implementar, mantener y mejorar el MSPI.
- Se integrarán criterios de seguridad de la información en los procesos estratégicos, misionales y de apoyo de la institución, desde su planeación hasta su ejecución y evaluación.

9.2.1 Principios rectores

- **Confidencialidad**: La información sólo estará disponible para quienes estén debidamente autorizados.
- **Integridad**: Se garantizará que la información se mantenga exacta, completa y libre de manipulaciones no autorizadas.
- **Disponibilidad**: La información estará accesible cuando sea requerida, bajo condiciones seguras.
- **Legalidad y Transparencia**: Todas las acciones en el tratamiento de la información se realizarán conforme a la ley y de forma verificable.
- **Responsabilidad Individual:** Cada usuario es responsable del uso seguro de los sistemas y datos que se le asignan.

9.3 Roles y responsabilidades

9.3.1 Responsable de Seguridad de la Información para la entidad

La responsabilidad de Seguridad de la información será el liderar la implementación del Modelo de seguridad y privacidad de la información en la entidad y tendrá las siguientes responsabilidades:

- Fomentar la implementación de la Política de Gobierno Digital
- Asesorar a la entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
- Realizar la estimación, planificación y cronograma de la implementación del MSPI.
- Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
- De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.
- Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
- Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.
- Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

9.3.2 Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

- Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
- Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.
- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.
- Aprobar acciones y mejores prácticas que en la implementación del MSPI.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

9.3.3 Oficina asesora Jurídica

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

9.3.4 Gestión del Talento Humano

- Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente.
- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

9.3.5 Auditoría interna y/o oficina de control interno

La Oficina de Control Interno, o quien ejerza funciones de auditoría interna en la E.S.E. Hospital San Rafael de Itagüí, cumple un papel fundamental en la verificación del cumplimiento y la

mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI). Sus responsabilidades específicas incluyen:

- Ejecutar auditorías periódicas al cumplimiento de la política, los procedimientos, controles y compromisos asociados al MSPI y al Sistema de Gestión de Seguridad de la Información (SGSI).
- Evaluar la eficacia de los controles implementados para proteger los activos de información frente a riesgos de confidencialidad, integridad y disponibilidad.
- Emitir informes de auditoría con hallazgos, recomendaciones y oportunidades de mejora, dirigidos a la Alta Dirección y a las áreas responsables del MSPI.
- Verificar el cumplimiento normativo relacionado con la seguridad de la información, la protección de datos personales y los principios de transparencia, en concordancia con las leyes y decretos aplicables.
- Hacer seguimiento a los planes de mejoramiento derivados de auditorías internas o externas, incidentes reportados o no conformidades relacionadas con la seguridad de la información.
- Promover la cultura del autocontrol y el mejoramiento continuo, mediante la difusión de buenas prácticas y la evaluación sistemática de la gestión de riesgos informáticos.

La independencia técnica y administrativa de la Oficina de Control Interno garantiza la objetividad de sus observaciones, permitiendo fortalecer la gestión institucional y asegurar la protección efectiva de la información en todos los niveles de la organización.

9.4 Identificación de activos de información e infraestructura critica

Establecer una metodología que permita identificar, inventariar, clasificar y proteger los activos de información e infraestructura crítica de la E.S.E. Hospital San Rafael de Itagüí, con base en los principios de confidencialidad, integridad y disponibilidad, garantizando su gestión adecuada frente a amenazas y riesgos.

9.4.1 Lineamientos Generales

La E.S.E. Hospital San Rafael de Itagüí adoptará un proceso sistemático de identificación y clasificación de activos de información que:

- Determine cuáles activos deben formar parte del inventario institucional, por su valor estratégico, operativo o normativo.
- Establezca criterios claros de clasificación basados en la evaluación del impacto que tendría la pérdida de confidencialidad, integridad o disponibilidad del activo.
- Permita una actualización periódica del inventario, ajustándose a cambios en procesos, estructura, tecnología o funciones.
- Esté alineado con las recomendaciones de la Guía No. 5 del MinTIC, la Norma ISO/IEC 27001:2013 y el Dominio 8 de Gestión de Activos.

9.4.2 Definición de Activos

Cada área de proceso, bajo coordinación del equipo de tecnología y seguridad de la información, debe identificar sus activos, los cuales pueden clasificarse como:

- Información: bases de datos, documentos clínicos, contratos, manuales, archivos físicos o digitales.
- Software: aplicaciones clínicas y administrativas, ERP, HIS, herramientas ofimáticas.
- Hardware: servidores, estaciones de trabajo, routers, impresoras, dispositivos biomédicos conectados.
- Servicios: internet, intranet, correo electrónico, VPN, servicios en la nube.
- Recurso humano: personal clave con conocimiento crítico.
- Otros: elementos específicos que soportan procesos estratégicos.

9.4.2.1 Inventario

Se elaborará y mantendrá una matriz de activos que incluya:

- Identificador único.
- Nombre del activo y proceso asociado.
- Tipo de activo.
- Ubicación física o lógica.
- Propietario y custodio.
- Usuarios y niveles de acceso.
- Clasificación según Confidencialidad-Integridad-Disponibilidad.
- Justificación de la clasificación.
- Nivel de criticidad: Extremo, Alta, Media o Baja.

9.4.2.2 Clasificación de los Activos

La clasificación se realizará evaluando tres propiedades:

Confidencialidad

NIVEL	DESCRIPCIÓN CRITERIO DE CONFIDENCIALIDAD	DENOMINACIÓN	
1	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado o no	Publica	Bajo
2	Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la institución, el Sector Público Nacional o terceros.	Reservada de uso interno	Moderado
3	Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves	Reservada confidencial	Alto

NIVEL	DESCRIPCIÓN CRITERIO DE CONFIDENCIALIDAD	DENOMINACIÓN	
	para la institución, el Sector Público Nacional o terceros.		
4	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la institución o a terceros.	Reservada secreta	Extremo

Integridad

NIVEL	DESCRIPCIÓN CRITERIO DE INTEGRIDAD	DENOMINACIÓN
1	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación.	Bajo
2	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación.	Moderado
3	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves.	Alto
4	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves.	Extremo

Disponibilidad

NIVEL	DESCRIPCIÓN CRITERIO DE DISPONIBILIDAD	DENOMINACIÓN
1	Información cuya inaccesibilidad no afecta la operación	Bajo
2	Información cuya inaccesibilidad no afecta la operación, aunque puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.	Moderado
3	Información cuya inaccesibilidad permanente durante una semana podría ocasionar impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen de la entidad.	Alto
4	Información cuya inaccesibilidad permanente durante un día podría ocasionar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.	Extremo

9.4.2.3 Revisión y Actualización

El inventario será revisado al menos una vez al año o cuando:

- Se modifique el proceso asociado.
- Se incorporen o eliminen activos.
- Se reasigne el responsable o custodio.
- Cambien los sistemas que alojan la información.

9.4.2.4 Publicación y Protección

El inventario de activos será clasificado como información confidencial, de uso restringido, y solo podrá ser modificado por personal autorizado previa validación del Oficial de Seguridad de la Información.

9.5 Valoración de los riesgos de seguridad de la información

La valoración del riesgo se realizará con base en los siguientes elementos:

9.5.1 Identificación de riesgos

A partir del inventario de activos de información y el directorio de servicios, se identificarán amenazas que puedan afectar negativamente la información institucional, considerando escenarios de pérdida de:

- Confidencialidad: acceso no autorizado a la información.
- Integridad: modificación o destrucción no autorizada de la información.
- Disponibilidad: indisponibilidad o inaccesibilidad de la información o del servicio.
- Privacidad: uso indebido de datos personales o sensibles.
- Continuidad operativa: interrupciones que afecten procesos misionales y críticos del hospital.

9.5.2 Valoración del impacto y la probabilidad

Se utilizarán criterios institucionales definidos en el procedimiento de gestión de riesgos aprobado, clasificando:

- Impacto: en niveles bajo, medio y alto, según sus efectos operativos, legales, financieros o reputacionales.
- Probabilidad de ocurrencia: en niveles improbable, posible o probable, según evidencia histórica, controles existentes y exposición.

9.5.3 Criterios de aceptación del riesgo

Un riesgo podrá ser aceptado cuando:

- Su nivel sea bajo y los controles existentes sean eficaces.
- El costo de mitigación sea desproporcionado frente al impacto esperado.
- Sea temporal y esté bajo monitoreo activo.
- Toda aceptación de riesgo deberá ser documentada y aprobada por la Alta Dirección.

9.5.4 Determinación de niveles de riesgo

El nivel de riesgo será calculado mediante una matriz de riesgo que cruce impacto y probabilidad, permitiendo su clasificación como:

- Alto: requiere tratamiento inmediato.
- Medio: requiere plan de acción y seguimiento.
- Bajo: puede ser gestionado con controles existentes.

9.5.5 Priorización y tratamiento

Los riesgos se priorizarán según su nivel de exposición, valor del activo afectado y criticidad del proceso. Esta priorización será insumo para el Plan de Tratamiento de Riesgos de Seguridad de la Información.

9.6 Plan de tratamiento de los riesgos de seguridad de la información

El Plan de Tratamiento de los Riesgos de Seguridad de la Información será desarrollado como una herramienta estratégica para establecer medidas orientadas a mitigar los riesgos identificados durante el análisis, tales como la pérdida de confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucionales. Su propósito es reducir la incertidumbre frente al cumplimiento de los objetivos institucionales de la E.S.E. Hospital San Rafael de Itagüí, en concordancia con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

Este plan contempla la evaluación y selección de acciones específicas para el control de riesgos, organizadas en actividades detalladas que incluyen tareas, responsables asignados y cronogramas de ejecución dentro de la vigencia del plan. Las actividades han sido definidas con base en el análisis de riesgos, las características de los procesos y las necesidades institucionales en materia de seguridad y privacidad, permitiendo establecer un marco operativo claro para su implementación (PL_12_DI).

9.7 Capacitación, Comunicación y Divulgación de Información

9.7.1 Capacitación

La E.S.E. Hospital San Rafael de Itagüí diseñará, implementará y evaluará un plan permanente de formación en seguridad y privacidad de la información, con el propósito de fortalecer la cultura organizacional frente a los riesgos asociados al tratamiento de la información y asegurar el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI). Este plan contemplará:

- **Capacitación en inducción**: Todo el personal de nuevo ingreso recibirá formación introductoria sobre los lineamientos de seguridad y privacidad de la información.
- **Capacitación anual general**: Dirigida a todo el personal de planta, contratistas y directivos, para reforzar conocimientos sobre los principios de seguridad de la información, políticas institucionales, procedimientos y normatividad vigente.
- **Capacitación por cambios relevantes**: Se realizarán sesiones extraordinarias ante actualizaciones normativas, ajustes estructurales o riesgos emergentes, cuando lo determine el Oficial de Seguridad de la Información.

9.7.1.1 Requisitos de los programas de capacitación:

- Los contenidos serán revisados y actualizados periódicamente, de acuerdo con cambios regulatorios o institucionales.

- Se adaptarán según las funciones de cada colaborador, asegurando pertinencia y aplicabilidad.
- Cada sesión contará con una evaluación de conocimientos para medir la comprensión y el logro de los objetivos.
- Se dejará constancia escrita de cada actividad de capacitación, incluyendo lista de asistencia, evaluaciones aplicadas y resultados obtenidos.
- Todos los programas estarán documentados con su alcance, metodología, medios utilizados y procesos de evaluación.

9.7.2 Comunicación y divulgación de información

La E.S.E. garantizará la adecuada comunicación interna y externa de los lineamientos del MSPI, a través de un plan articulado de comunicación institucional.

- **Reportes internos:** Generados por el Oficial de Seguridad de la Información con el fin de alertar sobre posibles debilidades o incidentes relacionados con seguridad, privacidad, corrupción, fraude o soborno.
- **Reportes externos**: Aquellos exigidos por entidades de control o normativas vigentes, que serán remitidos por el Oficial de protección de daos y seguridad de la información a las autoridades competentes en los plazos y formatos establecidos.
- **Respuestas institucionales**: Se atenderán oportunamente las solicitudes de información de organismos administrativos, judiciales o de control en relación con el MSPI.

9.7.3 Estrategia de divulgación

Para garantizar la comprensión y apropiación del MSPI, el Hospital desarrollará acciones de divulgación periódica, dirigidas a todos los grupos de interés:

- Frecuencia: Mínimo una (1) vez por año.
- Formatos: Publicaciones impresas, boletines digitales, infografías, cápsulas educativas y contenidos multiformato adaptados a cada tipo de público.
- Contenido clave: Políticas de seguridad, canales de denuncia, obligaciones de los colaboradores, sanciones por incumplimiento y casos prácticos.
- La divulgación se ejecutará a través de los canales establecidos en el plan de comunicaciones institucional, tales como:
- Página web institucional: https://hsanrafael.gov.co/
- Plataforma interna Intranet
- Correo institucional y pantallas informativas

10 OPERACIÓN

Tras concluir la fase de planificación del MSPI, la E.S.E. Hospital San Rafael de Itagüí iniciará la implementación de controles definidos en el Plan de Tratamiento de Riesgos. Esta etapa busca que cada medida —técnica, administrativa o física— se ejecute de manera

documentada y por proceso, cumpliendo los requisitos del MSPI y obteniendo aval explícito del Comité Institucional de Gestión y Desempeño, tal como lo establece la guía del Ministerio TIC. Para ello, se detallan las estrategias y actividades que detallará actividades, responsables, cronograma y presupuesto, y se generará la correspondiente evidencia de implementación, que servirá de respaldo para auditorías y la evaluación de efectividad del plan. Además, durante la operación se integrarán componentes clave de protección de datos, transparencia y acceso a la información pública. En sintonía con la Ley 1581 de 2012 y sus decretos reglamentarios, se aplicarán los principios de privacidad en el tratamiento de datos personales

Asimismo, se garantizará el cumplimiento de la Ley 1712 de 2014 (Estatutaria de Transparencia), publicando de forma proactiva la información institucional relevante y atendiendo oportunamente las solicitudes de acceso a información pública, según su modalidad y plazos legales

Así, la implementación del MSPI no solo protegerá los activos internos, sino que reforzará el compromiso de la entidad con la transparencia y el control ciudadano, integrando las buenas prácticas del gobierno digital.

11 EVALUACIÓN DE DESEMPEÑO

La evaluación del desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital San Rafael de Itagüí permitirá conocer el grado de cumplimiento de las acciones planificadas, la eficacia de los controles implementados y el nivel de madurez en la gestión del riesgo digital. Esta evaluación se realizará mediante el seguimiento y análisis periódico de los indicadores definidos en la fase de implementación, los cuales estarán incluidos en el tablero de control del Plan de Acción institucional, conforme al Decreto 612 de 2018. Dichos indicadores permitirán medir avances relacionados con la protección de datos personales (Ley 1581 de 2012), la transparencia y el acceso a la información pública (Ley 1712 de 2014), y el cumplimiento normativo general (Decreto 2106 de 2019 y normas complementarias). Los resultados se documentarán en informes que serán analizados y validados por el Comité Institucional de Gestión y Desempeño, integrando así el enfoque de mejora continúa previsto por el MIPG.

Adicionalmente, se realizará un proceso de auditoría interna para verificar el cumplimiento del MSPI, identificar posibles no conformidades y proponer acciones correctivas. Las auditorías deberán estar programadas y aprobadas por el Comité de Coordinación de Control Interno e incluirán temas clave como incidentes de seguridad, cambios regulatorios (PESTEL), eficacia de los controles, y evolución del contexto organizacional. Los hallazgos de las auditorías, junto con los informes de seguimiento y evaluación de indicadores, serán insumo para la Revisión por la Dirección, que se llevará a cabo en intervalos definidos por la alta dirección. Esta revisión permitirá determinar la conveniencia, adecuación y eficacia del MSPI, así como establecer compromisos institucionales para su fortalecimiento, dejando constancia en actas oficiales del comité de gestión institucional.

12 MEJORAMIENTO CONTINUO

Una vez finalizada la fase de evaluación de desempeño del MSPI, la E.S.E. Hospital San Rafael de Itagüí procederá a consolidar los resultados obtenidos a través del análisis de indicadores, auditorías internas y revisiones por parte de la alta dirección. Esta información servirá como insumo para la identificación de brechas, oportunidades de mejora y debilidades estructurales u operativas en la gestión de seguridad y privacidad de la información. Con base en esta evaluación integral, se diseñará un Plan de Mejoramiento Continuo, que establecerá acciones correctivas y preventivas específicas, dirigidas a optimizar los controles implementados, fortalecer la cultura institucional en ciberseguridad y elevar el nivel de madurez del modelo.

Este plan incluirá acciones concretas con responsables, plazos definidos y medios de verificación, garantizando su trazabilidad y seguimiento desde el Comité Institucional de Gestión y Desempeño. Las acciones podrán estar orientadas a revisar políticas, actualizar procedimientos, reforzar programas de formación, ajustar configuraciones técnicas o rediseñar controles ineficaces. Asimismo, se fomentará un enfoque proactivo de mejora continua en todos los niveles de la organización, permitiendo no solo la corrección de fallas detectadas, sino también la anticipación a nuevos riesgos emergentes del entorno digital. La implementación sistemática de este componente reafirma el compromiso del hospital con la protección de la información, la transparencia y el cumplimiento normativo permanente.

13 PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

N°	ESTRATEGIA	ACTIVIDAD	RESPONSABLE	PERIODO	MEDIO DE VERIFICACIÓN
1	Gobierno del MSPI	Actualizar el Plan de Seguridad y Privacidad de la Información a la vigencia 2026	Líder de Sistemas	Enero	Plan MSPI 2026 aprobado
2		Socializar el Plan MSPI 2026 a líderes de proceso	Líder de Sistemas	Enero	Correo o acta de socialización
3		Sesiones ordinarias del Comité de Seguridad y Privacidad de la Información	Comité MSPI	Trimestral	Actas de comité
4	Políticas MSPI	Revisar y ratificar la Política de Seguridad y Privacidad de la Información	Líder de Sistemas	Febrero	Política ratificada/publicada
5		Revisar política de control de accesos y contraseñas	Líder de Sistemas	Febrero	Política publicada
6		Consolidar el Manual de Políticas de Seguridad de la Información	Líder de Sistemas	Julio	Manual publicado
7	Gestión de activos	Actualizar el inventario de activos de información	Líder de Sistemas	Marzo	Matriz de activos actualizada
8		Validar clasificación C-I-D de activos críticos	Líder de Sistemas	Abril	Matriz validada

N°	ESTRATEGIA	ACTIVIDAD	RESPONSABLE	PERIODO	MEDIO DE VERIFICACIÓN
9	Gestión de activos	Revisión del inventario de activos de información	Líder de Sistemas	Semestral	Registro de revisión
10		Actualizar la matriz de riesgos de seguridad y privacidad de la información	Líder de Sistemas / Planeación	Abril	Matriz de riesgos 2026
11		Seguimiento al plan de tratamiento de riesgos	Líder de Sistemas	Semestral	Registro de seguimiento
12	Controles operativos	Verificación de la ejecución de copias de respaldo	Líder de Sistemas	Mensual	Bitácora de respaldos
13		Realizar prueba de restauración de información	Líder de Sistemas	Semestral	Acta de prueba
14		Revisión de cuentas de usuario y accesos	Líder de Sistemas	Semestral	Reporte de revisión
15	Incidentes	Revisar y ratificar el procedimiento de gestión de incidentes	Líder de Sistemas	Junio	Procedimiento validado
16		Registro y gestión de incidentes de seguridad de la información	Líder de Sistemas	Trimestral	Registro de incidentes
17		Elaborar informe de incidentes de seguridad de la información	Líder de Sistemas	Semestral	Informe semestral
18	Proveedores y terceros	Verificar cláusulas de confidencialidad en contratos TIC	Jurídica / Sistemas	Mayo	Lista de verificación
19		Revisión de accesos de proveedores a sistemas institucionales	Líder de Sistemas	Semestral	Registro de accesos
20	Cultura de seguridad	Inducción en seguridad de la información a personal nuevo	Talento Humano / Sistemas	Permanente	Registro de inducción
21		Ejecutar campaña de sensibilización en seguridad de la información	Líder de Sistemas	Agosto	Pieza o correo
22		Ejecutar capacitación anual en seguridad de la información	Líder de Sistemas	Septiembre	Lista de asistencia

14 PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
TOTAL			

Nota: Presupuesto sujeto al programa de saneamiento fiscal y financiero de la E.S.E.

15 EVALUACIÓN

INDICADOR	FÓRMULA	META	FRECUENCIA
% de implementación de controles definidos en el plan de tratamiento de riesgos	(Controles implementados / Controles planificados) x 100	≥ 90%	Trimestral
% de cumplimiento del plan de capacitación en seguridad y privacidad	(Capacitaciones ejecutadas / Capacitaciones planificadas) x 100	100%	Anual
% de personal capacitado en seguridad de la información	(N° de personas capacitadas / Total de personal objetivo) x 100	≥ 90%	Anual
% de cumplimiento del plan MSPI	(Acciones ejecutadas / Acciones planificadas) x 100	≥ 90%	Trimestral

16 DOCUMENTOS DE REFERENCIA

CÓDIGO	NOMBRE
No aplica	Documento maestro del modelo de seguridad y privacidad de la información. Ministerio de tecnologías de la información y comunicación Octubre 2021
No aplica	Guía No. 5. Guía para la Gestión y Clasificación de Activos de Información. 2016
No aplica	Roles y responsabilidades. modelo de seguridad y privacidad de la información. Ministerio de tecnologías de la información y comunicación Octubre 2021

17 CONTROL DE DIVULGACIÓN

PROCESO- SERVICIO/ÁREA	CARGOS(S) A LOS QUE SE SOCIALIZA
Todas las áreas, procesos y/o servicios	Coordinadores, jefes y/o líderes de área

18 CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCIPCIÓN DEL CAMBIO	SOLICITANTE
2022 – 01 -15	1	Formulación del Plan para la vigencia 2022.	Líder de sistemas
2023 – 01 -14	2	Formulación del Plan para la vigencia 2023.	Líder de sistemas
2024 – 01 -26	3	Formulación del Plan para la vigencia 2024.	Líder de sistemas
2025 – 01 -29	4	Formulación del Plan para la vigencia 2025.	Líder de sistemas
2026 – 01 -30	5	Formulación del Plan para la vigencia 2026.	Líder de sistemas

19 ANEXOS

CÓDIGO	NOMBRE
No aplica	No aplica

Elaboró/actualizó:	Revisó:	Aprobó:
Francisco Javier Henao Hernández Líder Sistemas	Luisa Fernanda Rúa Vásquez Jefe Oficina Asesora Planeación y Calidad María Catalina Mejia Pineda Profesional de Planeación y Calidad	Luis Fernando Arroyave Soto Gerente
Firma:	Firma:	Firma:
Fecha: 2025-01-26	Fecha: 2025-01-26	Fecha: 2025-01-26