E.S.E. HOSPITAL
San Rafael
DE ITAGÜÍ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1 JUSTIFICACIÓN

El presente plan tiene como finalidad establecer, de manera estructurada y coherente, las acciones necesarias para el tratamiento de los riesgos identificados en materia de seguridad y privacidad de la información en la E.S.E. Hospital San Rafael de Itagüí. Su formulación se encuentra alineada con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y con la normatividad vigente en Colombia, en particular la Ley 1581 de 2012, la Ley 1712 de 2014, y el Decreto 1078 de 2015, entre otras disposiciones aplicables a entidades públicas.

En este sentido, se diseñará e implementará un Plan de Tratamiento de Riesgos que permita adoptar medidas preventivas, correctivas y de mitigación sobre los riesgos priorizados, producto del análisis institucional. Este plan incluirá la definición de responsables, cronogramas, recursos y controles específicos, orientados a garantizar la protección efectiva de los activos de información, así como el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y legalidad.

La gestión del tratamiento de riesgos constituye una fase crítica dentro del ciclo del MSPI y responde al compromiso institucional de salvaguardar la información personal, clínica, financiera, administrativa y misional, frente a amenazas y vulnerabilidades que puedan comprometer la operación institucional, los derechos de los titulares de la información y la confianza ciudadana. Adicionalmente, este instrumento da cumplimiento a los mandatos normativos relacionados con la protección de datos personales, el acceso a la información pública y la ciberseguridad en el sector público.

Su implementación permitirá reducir la exposición al riesgo, fortalecer la cultura organizacional en torno a la seguridad de la información y asegurar que los controles implementados respondan de manera eficaz a los riesgos identificados. Asimismo, el plan facilitará la toma de decisiones estratégicas, contribuirá al cumplimiento de los estándares del Gobierno Digital, promoverá la mejora continua del Sistema de Gestión de Seguridad de la Información y garantizará una prestación de servicios en salud confiable, segura y orientada a las necesidades de los ciudadanos.

2 ENFOQUE DIFERENCIAL

El principio de enfoque diferencial reconoce que hay poblaciones con características particulares debido a su edad, género, raza, etnia, condición de discapacidad y víctimas de la violencia para las cuales el SGSSS ofrecerá especiales garantías y esfuerzos encaminados a la eliminación de situaciones de discriminación y marginación. Para lo que la E.S.E Hospital San Rafael de Itagüí implementa el manual "Atención en salud con enfoque diferencial" MN-04-AT

3 OBJETIVO GENERAL

Establecer e implementar un conjunto de acciones orientadas al tratamiento efectivo de los riesgos identificados en materia de seguridad y privacidad de la información, con el fin de

preservar la confidencialidad, integridad, disponibilidad y legalidad de los activos de información de la E.S.E. Hospital San Rafael de Itagüí, en cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente aplicable.

3.1 OBJETIVOS ESPECÍFICOS

- Definir las medidas de tratamiento (prevención, mitigación, corrección o aceptación) para cada uno de los riesgos priorizados en el análisis institucional de seguridad de la información.

- Establecer los controles técnicos, administrativos y físicos necesarios para reducir la probabilidad de ocurrencia y el impacto de los riesgos sobre los activos de información.

- Asignar responsables, recursos y plazos de ejecución para cada acción contemplada en el plan, asegurando su implementación y seguimiento oportuno.

- Contribuir al fortalecimiento de la cultura institucional en materia de seguridad y privacidad de la información, a través de la adopción de prácticas de gestión del riesgo alineadas con el MSPI y el Gobierno Digital.

- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información mediante el monitoreo, evaluación y retroalimentación periódica del plan de tratamiento.

4 RESPONSABLE(S) DEL PLAN

El liderazgo, coordinación y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información estarán a cargo del Área de Tecnologías y Sistemas de Información de la E.S.E. Hospital San Rafael de Itagüí, la cual será responsable de su implementación, actualización y evaluación continua, en articulación con las demás áreas institucionales y bajo la supervisión de la alta dirección.

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, anonimizarían 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 ejecución efectiva de al menos el 90 % de las acciones y medidas definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al finalizar la vigencia 2026, garantizando la mitigación de los riesgos priorizados y el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), el Decreto 1078 de 2015, la Ley 1581 de 2012, la Ley 1712 de 2014 y demás disposiciones normativas aplicables.

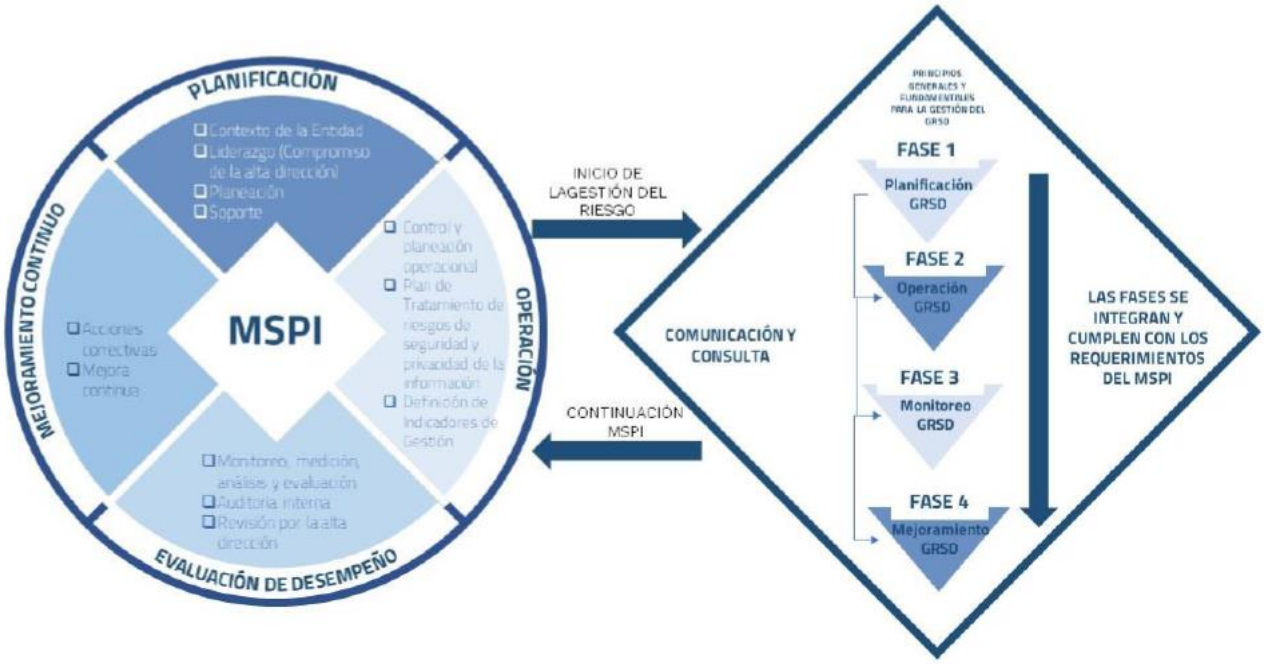
7 INTEGRACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La integración del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a lo dispuesto en el Decreto 1078 de 2015 y en el marco de la estrategia de Gobierno Digital, constituye un componente esencial para que las entidades públicas consoliden un entorno institucional seguro, confiable y resiliente frente a los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

En este contexto, el MSPI exige la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que no solo permita establecer controles efectivos, sino que también incorpore de forma sistemática la gestión del riesgo como su base fundamental. La articulación entre el MSPI y la guía de gestión del riesgo expedida por Función Pública se materializa en la alineación de las actividades de cada modelo: en la fase de Planificación del MSPI se desarrollan tareas como la identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos; en la fase de Implementación se ejecutan los planes de tratamiento definidos para reducir o eliminar las amenazas identificadas; en la fase de Evaluación del Desempeño se realiza el monitoreo y revisión de los controles, la medición de la efectividad de los tratamientos aplicados y la evaluación de los riesgos residuales; y, finalmente, en la fase de Mejoramiento Continuo, ambas metodologías convergen para identificar oportunidades de optimización, corrección y fortalecimiento del sistema con base en los hallazgos obtenidos en las etapas anteriores.

Esta integración permite a las entidades adoptar un enfoque preventivo, basado en evidencia y alineado con los principios de gestión institucional, garantizando así una mayor madurez en la protección de los activos de información y en el cumplimiento de la normatividad vigente.
En este sentido, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información no se concibe como un instrumento aislado, sino como un componente operativo directamente articulado al Modelo de Seguridad y Privacidad de la Información (MSPI). Las actividades, controles, seguimientos e informes generados en el marco del MSPI servirán como evidencia para la ejecución, monitoreo y evaluación del presente plan, optimizando recursos institucionales, evitando duplicidad de esfuerzos y fortaleciendo la coherencia del sistema de gestión de seguridad de la información.

Ilustración 1. Integración del plan de tratamiento de riesgos de seguridad y privacidad de la información con el modelo de seguridad y privacidad de la información (MSPI)



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

8 PLANIFICACIÓN DE LA GRSD

La fase de planificación constituye el punto de partida del ciclo de gestión de riesgos de seguridad de la información. En esta etapa, la E.S.E. Hospital San Rafael de Itagüí ha adoptado un enfoque integral que permite identificar de forma estructurada los riesgos que pueden afectar sus activos de información, establecer su contexto institucional, asignar responsables, y definir las estrategias para su tratamiento.

8.1 Contexto interno y externo de la entidad pública

Se realizó un análisis del contexto interno, considerando factores como la estructura organizacional, la disponibilidad de recursos humanos, tecnológicos y financieros, los sistemas de información institucionales, el mapa de procesos, y los objetivos estratégicos definidos en el Plan de Desarrollo Institucional. Así mismo, se identificaron las dependencias clave, las líneas de mando, los responsables del tratamiento de la información y los canales de comunicación internos. Análisis PESTEL

En cuanto al contexto externo, se analizaron aspectos normativos, tecnológicos y sociales, incluyendo el marco jurídico que regula el tratamiento de datos personales y la seguridad de la información (Leyes 1581 de 2012, 1712 de 2014, Decreto 1078 de 2015), así como los lineamientos del MSPI, del Gobierno Digital y las recomendaciones del MinTIC. Se consideraron también las relaciones con entes de control, proveedores, contratistas, y ciudadanía, como usuarios de servicios digitales. Análisis modelo CANVAS

8.2 Alcance para aplicar la gestión de riesgos de seguridad de la información

El alcance de la gestión de riesgos de seguridad de la información debe abarcar de manera integral todos los procesos de la entidad pública que involucren activos de información, servicios digitales, tecnologías de la información o tratamiento de datos personales. Este alcance debe estar alineado con los criterios establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), como habilitador de la Estrategia de Gobierno Digital definida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
En consecuencia, la administración del riesgo deberá aplicarse de forma transversal en los procesos misionales, de apoyo y estratégicos, asegurando una cobertura efectiva frente a amenazas que puedan comprometer la confidencialidad, integridad, disponibilidad o legalidad de la información bajo custodia de la entidad.

8.3 Alineación o creación de la política de gestión de riesgo de seguridad de la información.

El Hospital cuenta con una política integral de gestión del riesgo, que establece de manera explícita el compromiso institucional con la identificación, valoración, tratamiento y monitoreo de los riesgos de seguridad de la información en todos los niveles organizacionales.
Dicha política fue formulada conforme a los lineamientos establecidos en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información del Departamento Administrativo de la Función Pública (DAFP), y se encuentra articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI). Su adopción y actualización están a cargo de la línea estratégica de la entidad, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG), y se reflejan en los instrumentos de planeación institucional, asegurando alineación con los objetivos estratégicos y el marco normativo vigente.

8.4 Definición de roles y responsabilidades

8.4.1 Responsable de seguridad de la información

El responsable de Seguridad Digital y de la Información es el encargado de liderar la implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI) en la E.S.E. Hospital San Rafael de Itagüí. Este rol debe estar adscrito a la línea estratégica de la entidad, en concordancia con lo dispuesto en el Manual Operativo del MIPG, y se articula con las responsabilidades definidas en el marco de las tres líneas de defensa establecidas en la Política de Administración del Riesgo.
Sus principales funciones comprenden:

- Liderar la implementación del MSPI en la entidad, asegurando su alineación con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y con la normativa vigente en materia de protección de datos y seguridad de la información.
- Fomentar la adopción de la Política de Gobierno Digital y su integración con los procesos institucionales.

- Asesorar a la entidad en el diseño, adecuación y sostenibilidad del MSPI, incluyendo la identificación de brechas frente al modelo y la situación actual institucional.
- Planificar y coordinar la implementación del MSPI, incluyendo la elaboración de cronogramas, la definición de tareas y el seguimiento a su ejecución.
- Definir, elaborar, adoptar e implementar políticas, procedimientos, estándares y documentos necesarios para la operación del sistema de gestión de seguridad y privacidad de la información.
- Actualizar el procedimiento para la identificación y valoración de activos de información, asegurando su clasificación conforme a los principios de confidencialidad, integridad y disponibilidad.
- Adoptar y mantener el procedimiento formal para la gestión de riesgos, abarcando su identificación, análisis, evaluación y tratamiento.
- Brindar acompañamiento a los líderes de proceso (primera línea de defensa) en la identificación de riesgos, selección de controles y formulación de planes de tratamiento.
- Realizar seguimiento a la ejecución de los planes de tratamiento de riesgos, asegurando su cumplimiento dentro de los plazos, recursos y niveles de responsabilidad establecidos.
- Proponer la formulación de políticas y lineamientos institucionales en materia de seguridad y privacidad de la información.
- Diseñar e implementar estrategias de sensibilización y formación, dirigidas a servidores públicos y contratistas, en coordinación con las diferentes dependencias.
- Apoyar los planes de mejoramiento institucional, contribuyendo al cierre de brechas identificadas en auditorías o evaluaciones en materia de seguridad y privacidad de la información.
- Definir, socializar e implementar el procedimiento de gestión de incidentes de seguridad de la información, con criterios de reporte, análisis y respuesta efectiva.
- Reportar oportunamente a la alta dirección y al Comité de Coordinación de Control Interno cualquier variación significativa en los niveles de riesgo o incidentes que puedan comprometer la seguridad institucional.
- Poner en conocimiento de las dependencias competentes cualquier irregularidad o práctica que represente un riesgo para la seguridad o privacidad de la información, de acuerdo con la normatividad vigente.
- Promover la cultura de seguridad de la información en todos los niveles organizacionales, fortaleciendo la capacidad institucional para prevenir, detectar y responder a amenazas digitales.

El cumplimiento de estas funciones es clave para fortalecer el sistema de gestión del riesgo de seguridad de la información, proteger los activos críticos institucionales y asegurar la confianza de los ciudadanos en el uso de los servicios digitales de la entidad.

8.4.2 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.

8.4.3 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.

8.4.4 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.

8.4.5 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.

8.5 Definición de recursos para la Gestión de riesgos de seguridad de la información

Para garantizar una implementación efectiva del Modelo de Seguridad y Privacidad de la Información (MSPI), la E.S.E. Hospital San Rafael de Itagüí ha definido la asignación de recursos técnicos, humanos, financieros y tecnológicos necesarios para el desarrollo y sostenibilidad del proceso de gestión de riesgos de seguridad de la información.

La disponibilidad y planificación de estos recursos es responsabilidad de la línea estratégica o alta dirección, la cual debe asegurar que se incorporen dentro de los instrumentos de planificación institucional y en el presupuesto anual, conforme a los principios de eficiencia del gasto público y al marco normativo vigente.

Entre los principales recursos considerados se encuentran:

- Personal capacitado e idóneo, con formación técnica y experiencia en seguridad de la información, gestión de riesgos, protección de datos personales y normatividad aplicable. Este recurso humano es clave para la identificación, análisis, evaluación y

tratamiento de los riesgos, así como para el diseño y operación de los controles requeridos.

- Recursos económicos suficientes, destinados a la implementación de los controles de mitigación definidos en el plan de tratamiento de riesgos, incluyendo adquisición de software especializado, fortalecimiento de infraestructura tecnológica, servicios de consultoría o auditoría especializada, y programas de sensibilización y formación para funcionarios.

- Tiempo institucional asignado, que permita el desarrollo de actividades específicas de gestión del riesgo, como reuniones de trabajo con líderes de procesos, ejercicios de valoración, implementación de controles, análisis de incidentes y ciclos de mejora continua.

- Sistemas, procesos y tecnologías, que respalden la operación segura y confiable de los activos de información, incluyendo plataformas de respaldo, gestión documental, autenticación digital, monitoreo de seguridad, y mecanismos de respuesta ante incidentes.

- Recursos para actividades de mejora continua, monitoreo y auditorías, necesarios para evaluar la efectividad de los controles implementados, analizar los riesgos residuales y retroalimentar el sistema de gestión del riesgo de seguridad de la información.

La adecuada definición y disponibilidad de estos recursos permite fortalecer la capacidad institucional para prevenir, detectar y mitigar riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y legalidad de la información bajo custodia del hospital.

8.6 Identificación de activos de información

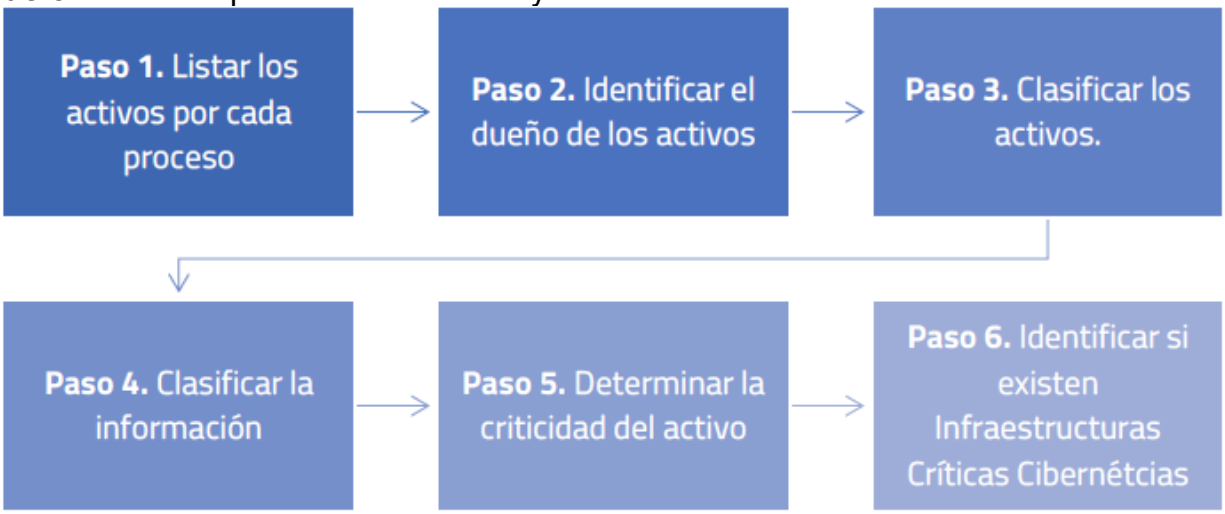
En el marco de la gestión de riesgos de seguridad de la información, un activo se entiende como cualquier elemento —tangible o intangible— que participa en el tratamiento, almacenamiento, transmisión o acceso a la información y que posee un valor para la entidad. En este contexto, los activos pueden incluir desde hardware, software, redes, servicios web, sistemas de información, datos digitales, documentos físicos, infraestructura, instalaciones, personal clave y conocimiento organizacional, hasta servicios externos y procesos críticos de operación.

La E.S.E. Hospital San Rafael de Itagüí reconoce que identificar, clasificar y valorar sus activos de información es una condición esencial para garantizar la protección adecuada de los mismos, tanto en su funcionamiento interno (BackOffice) como en los servicios prestados a la ciudadanía (FrontOffice). Este ejercicio permite priorizar los esfuerzos de seguridad, establecer controles adecuados y cumplir con los principios de confidencialidad, integridad, disponibilidad y legalidad.

La responsabilidad de identificar y valorar los activos de información recae sobre la Primera Línea de Defensa, conformada por los líderes de proceso, quienes deberán realizar esta

actividad en su respectivo ámbito funcional, bajo la orientación técnica del responsable de Seguridad Digital o de la Información de la entidad. Para la construcción del inventario institucional de activos de información, se deben seguir los siguientes pasos metodológicos.

Ilustración 2. Pasos para la identificación y valoración de activos



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

8.6.1 Pasos para la identificación y valoración de activos

1) **Listar los activos por proceso:** Identificar los activos utilizados en cada proceso, asignándoles un nombre, código o consecutivo, y una descripción clara de su función o utilidad.

Paso 1. Listar los activos por cada proceso:

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

Ejemplo:

PROCESO	ACTIVO	DESCRIPCION
Gestión Financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad
Gestión Financiera	Aplicativo de Nómina	Sistema que permite gestionar la nómina y los pagos
Gestión Financiera	Cuentas de Cobro	Formatos de cobro diligenciados

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

2) **Identificar el dueño del activo:** Asignar formalmente un responsable para cada activo, usualmente el líder de proceso, quien será el encargado de velar por su protección y mantenimiento.

Paso 2. Identificar el dueño de los activos:

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá

Ejemplo:

ACTIVO	DESCRIPCION	DUEÑO DEL ACTIVO
Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe Oficina de Nómina

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

3) **Clasificar los activos:** Categorizar cada activo según su tipo: información, hardware, software, servicios, componentes de red, instalaciones, personal o intangibles (como reputación o know-how institucional).

Ejemplo:

ACTIVO	TIPO DE ACTIVO
Base de datos de nómina	Información
Aplicativo de Nómina	Software
Cuentas de Cobro	Información

Tabla 1. Tipología de activos

TIPOLOGÍA DE ACTIVOS	
TIPO DE ACTIVO	**DESCRIPCIÓN**
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el 'good will', entre otros

TIPOLOGÍA DE ACTIVOS	
TIPO DE ACTIVO	**DESCRIPCIÓN**
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

4) **Clasificar la información contenida:** Determinar la naturaleza de la información asociada al activo, de acuerdo con la Ley 1581 de 2012 (protección de datos personales) y la Ley 1712 de 2014 (acceso a la información pública), clasificándola como pública, reservada o confidencial, y evaluando si contiene datos personales.

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5

Ejemplo:

ACTIVO	TIPO DE ACTIVO	Ley 1712 de 2014	Ley 1581 de 2012
Base de datos de nómina	Información	Información Reservada	No Contiene datos personales
Aplicativo de Nómina	Software	N/A	N/A
Factura de venta	Información	Información Pública	No contiene datos personales

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

5) **Determinar la criticidad del activo:** Valorar el impacto que tendría la pérdida de confidencialidad, integridad o disponibilidad del activo, asignando un nivel de criticidad (alta, media o baja) que refleje su importancia para el proceso o para la operación institucional.

ACTIVO	TIPO DE ACTIVO	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de Criticidad
Base de datos de nómina	Información	ALTA	ALTA	ALTA	ALTA
Aplicativo de Nómina	software	BAJA	MEDIA	BAJA	MEDIA
Listas de asistencia	Información	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Una vez se ejecute la identificación de los activos, la entidad definirá si se gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección.

6) **Identificar si el activo es parte de una Infraestructura Crítica Cibernética (ICC):** Analizar si el activo es esencial para la continuidad del servicio y si su afectación pudiese generar impactos significativos a nivel social, económico o ambiental, según criterios establecidos por el Comando Conjunto Cibernético de Colombia.

Este inventario servirá como base para la gestión del riesgo, el diseño de controles, la respuesta a incidentes y la priorización de inversiones en seguridad. La información obtenida debe documentarse formalmente, mantenerse actualizada y estar disponible para los ejercicios de valoración de riesgos, auditorías, y seguimiento al cumplimiento del MSPI.

8.7 Identificar los riesgos inherentes de seguridad de la información

La E.S.E. Hospital San Rafael de Itagüí desarrolla el proceso de identificación de riesgos de seguridad de la información en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), considerando el contexto estratégico institucional, así como los factores internos, externos y específicos de cada proceso. Esta etapa es esencial para prevenir afectaciones a la confidencialidad, integridad, disponibilidad o legalidad de los activos de información, en cumplimiento de la normatividad vigente y los principios de gobierno digital.

8.7.1 Etapas del proceso de identificación:

8.7.1.1 Identificación y documentación de procesos y activos

La identificación de riesgos parte del inventario actualizado de los procesos institucionales (estratégicos, misionales y de apoyo) y los activos de información asociados. Esta actividad es liderada por los responsables de cada proceso, en articulación con la Oficina de Planeación y el responsable de Seguridad Digital.

8.7.1.2 Identificación de amenazas y vulnerabilidades

Se identifican las amenazas potenciales (naturales, deliberadas o accidentales) que podrían afectar la seguridad de los activos de información, así como las vulnerabilidades que puedan ser explotadas. Para ello, se recurre a fuentes como registros de incidentes, auditorías internas, análisis técnicos y juicios de expertos.

A continuación, se presentan diferentes categorías de amenazas que constituyen situaciones o fuentes potenciales de daño para los activos de información y que pueden dar lugar a la materialización de riesgos. Estas amenazas se clasifican, a modo de ejemplo, en tres tipos según su origen:

- Deliberadas (D): producto de acciones intencionales como ataques, accesos no autorizados o sabotajes.
- Fortuitas (F): derivadas de fallos involuntarios, errores humanos o accidentes.
- Ambientales (A): relacionadas con fenómenos naturales o condiciones del entorno físico y tecnológico.

Tabla 2. Amenazas comunes

AMENAZAS COMUNES		
TIPO	**AMENAZA**	**ORIGEN**
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
	Perdida de los servicios esenciales	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	D, F
	Falla en equipo de telecomunicaciones	D, F

AMENAZAS COMUNES		
TIPO	**AMENAZA**	**ORIGEN**
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: ISO/IEC 27005:2009

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 3. Amenazas dirigidas por el hombre

AMENAZAS DIRIGIDAS POR EL HOMBRE		
FUENTE DE AMENAZA	**MOTIVACIÓN**	**ACCIONES AMENAZANTES**
Pirata informático, intruso ilegal	✓ Reto ✓ Ego ✓ Rebelión ✓ Estatus ✓ Dinero	✓ Piratería ✓ Ingeniería Social ✓ Intrusión, accesos forzados al sistema ✓ Acceso no autorizado
Criminal de la computación	✓ Destrucción de la información ✓ Divulgación ilegal de la información ✓ Ganancia monetaria ✓ Alteración no autorizada de los datos	✓ Crimen por computador ✓ Acto fraudulento ✓ Soborno de la información ✓ Suplantación de identidad ✓ Acceso no autorizado
Terrorismo	✓ Chantaje ✓ Destrucción ✓ Explotación ✓ Venganza ✓ Ganancia política ✓ Cubrimiento de los medios de comunicación	✓ Bomba/Terrorismo ✓ Guerra de la información ✓ Ataques contra el sistema (DDoS) ✓ Penetración en el sistema ✓ Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	✓ Ventaja competitiva ✓ Espionaje económico	✓ Ventaja de defensa ✓ Ventaja política ✓ Explotación económica ✓ Hurto de información ✓ Intrusión en privacidad personal ✓ Ingeniería social ✓ Penetración en el sistema ✓ Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	✓ Curiosidad ✓ Ego ✓ Inteligencia ✓ Ganancia monetaria ✓ Venganza ✓ Errores y omisiones no intencionales (ej. error en el ingreso de datos, error de programación) ✓ Error en el ingreso de datos, error de programación	✓ Asalto a un empleado ✓ Chantaje ✓ Observar información reservada ✓ Uso inadecuado del computador ✓ Fraude y hurto ✓ Soborno de información ✓ Ingreso de datos falsos o corruptos ✓ Interceptación ✓ Código malicioso ✓ Venta de información personal ✓ Errores en el sistema ✓ Intrusión al sistema ✓ Sabotaje del sistema ✓ Acceso no autorizado al sistema

Tabla 4. Vulnerabilidades comunes

VULNERABILIDADES COMUNES	
TIPO	**VULNERABILIDADES**
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

FUENTE: ISO/IEC 27005

NOTA: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Tabla 5. Amenazas y vulnerabilidades

AMENAZAS Y VULNERABILIDADES		
TIPO DE ACTIVO	**EJEMPLO VULNERABILIDADES**	**EJEMPLO DE AMENAZAS**
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección física	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos
	Copia no controlada	Hurtos medios o documentos
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
SOFTWARE	Software ampliamente distribuido en términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos

	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta Fallas del equipo de telecomunicaciones
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
RED	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
PERSONAL	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Hurto de medios o documentos
LUGAR	Ubicación en área susceptible de inundación	Destrucción de equipos o medios
	Red energética inestable	Falla en equipo de telecomunicaciones
	Ausencia de protección física de la edificación (Puertas y ventanas)	Hurto de medios o documentos
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos

ORGANIZACIÓN	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de estos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

8.7.1.3 Análisis del contexto

Se revisa el entorno interno (estructura organizacional, tecnologías implementadas, cultura institucional) y el externo (normativa, actores externos, amenazas emergentes) para establecer los factores de riesgo que pueden incidir sobre la seguridad de la información. Como complemento, se emplean herramientas de diagnóstico como el análisis PESTEL y la matriz DOFA para identificar variables críticas.

8.7.1.4 Caracterización de riesgos

Cada riesgo identificado se describe especificando sus posibles causas, eventos de materialización y consecuencias. Se hace énfasis en aquellos riesgos que puedan impactar la operación institucional, el cumplimiento de los objetivos estratégicos y la confianza de los usuarios y partes interesadas.

8.7.1.5 Participación de los líderes de proceso

La identificación se realiza de forma participativa a través de sesiones de trabajo, entrevistas y talleres con los líderes de proceso, quienes aportan desde la experiencia operativa. Se promueve el enfoque de autocontrol y la apropiación del riesgo desde cada dependencia
.

8.7.1.6 Categorización y documentación

Los riesgos se documentan en la matriz institucional de riesgos de seguridad de la información, incluyendo su vinculación con activos críticos, procesos afectados, amenazas, vulnerabilidades y posibles impactos. Esta matriz es actualizada al menos una vez por vigencia y sirve como insumo para las etapas de valoración y tratamiento.

8.7.1.7 Consideraciones clave:

- Se consideran como riesgos principales: pérdida de confidencialidad, integridad, disponibilidad o legalidad de la información institucional.
- La E.S.E. no acepta riesgos críticos sin acciones de mitigación. Todo riesgo identificado debe tener definida una acción preventiva, correctiva o de tratamiento.
- La Oficina de Seguridad de la Información apoya técnicamente la identificación y garantiza que se aplique una metodología homogénea en toda la entidad.

8.8 Identificación del nivel de confianza para la autenticación digital

En el marco del fortalecimiento de la seguridad digital y la prestación confiable de servicios electrónicos, la E.S.E. Hospital San Rafael de Itagüí realiza la identificación de trámites y servicios ciudadanos digitales que requieren mecanismos de autenticación digital, con el fin de asegurar que el acceso a estos sea realizado exclusivamente por los usuarios autorizados.
Para ello, se define el nivel de confianza requerido para cada trámite o servicio, de acuerdo con los riesgos asociados a una autenticación errónea, conforme a la clasificación establecida en la Guía de Lineamientos para los Servicios Ciudadanos Digitales del MinTIC:

- **Nivel bajo**: Aplica a trámites cuyo riesgo de suplantación o uso indebido es mínimo. Se requiere una autenticación básica.
- **Nivel medio:** Corresponde a servicios donde el impacto de una autenticación fallida puede generar afectaciones moderadas. Se exige un nivel de autenticación más robusto.
- **Nivel alto:** Se requiere cuando la autenticación errónea puede derivar en daños importantes a la integridad de la información o a los derechos del titular. Implica autenticación con factores múltiples.
- **Nivel muy alto:** Reservado para trámites críticos donde la suplantación puede generar consecuencias legales, económicas o reputacionales extremas. Requiere autenticación con los más altos estándares de seguridad digital.

8.8.1 Proceso de análisis:

Para determinar el nivel adecuado de confianza, se deben seguir los siguientes pasos:

1) Identificación de activos de software asociados a trámites o servicios digitales, a partir del inventario de activos de información institucional.
2) Determinación de si el servicio requiere autenticación exclusiva por parte del titular de la información, en cuyo caso se hace necesario establecer mecanismos formales de autenticación digital.
3) Análisis de riesgos aplicando la metodología institucional:

a. Evaluación de la pérdida de confidencialidad, integridad o disponibilidad del activo en caso de suplantación o acceso no autorizado.
b. Consideración de vulnerabilidades específicas, como la ausencia de mecanismos de autenticación robusta.
c. Identificación de amenazas, como la falsificación de derechos o accesos indebidos.

4) Valoración de probabilidad e impacto, con base en los criterios definidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP), determinando si el nivel de riesgo es bajo, moderado, alto o extremo.
5) Asignación del nivel de confianza correspondiente (bajo, medio, alto, muy alto), de acuerdo con el nivel de riesgo residual identificado.

Una vez definido el nivel de confianza requerido para cada trámite o servicio, la entidad debe proceder con la vinculación técnica al servicio de Autenticación Digital del ecosistema de Servicios Ciudadanos Digitales, conforme a lo establecido en la normativa vigente y las directrices del MinTIC.

Este componente permite asegurar que los servicios digitales de la E.S.E. se brinden bajo condiciones adecuadas de seguridad, protegiendo la identidad de los usuarios, los datos personales y la integridad del sistema de información institucional.

8.9 Identificación y evaluación de los controles existentes

Una vez identificados y valorados los riesgos inherentes en materia de seguridad de la información, la E.S.E. Hospital San Rafael de Itagüí procede a realizar la identificación y evaluación de los controles existentes, con el fin de evitar esfuerzos o inversiones innecesarias y garantizar la eficiencia en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
Este análisis permite verificar si actualmente existen controles que mitigan total o parcialmente los riesgos identificados, así como evaluar su diseño, implementación, eficacia operativa y aplicabilidad al contexto institucional. La revisión de estos controles se realiza considerando tanto medidas técnicas como administrativas, humanas y físicas.

8.9.1 Fuente de referencia para controles:

Como insumo principal para esta etapa, se recurre a la sección 4 del MSPI - Objetivos de Control y Controles de Referencia, los cuales están basados en el Anexo A de la Norma ISO/IEC 27001:2013. Este estándar proporciona una guía estructurada para identificar controles orientados a la preservación de la confidencialidad, integridad y disponibilidad de la información, organizados en dominios como:

- Política de seguridad de la información
- Seguridad organizacional
- Seguridad de los recursos humanos
- Gestión de activos
- Control de accesos
- Criptografía
- Seguridad física y del entorno
- Seguridad en operaciones
- Seguridad en comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relación con proveedores
- Gestión de incidentes de seguridad
- Continuidad del negocio
- Cumplimiento legal y normativo

8.9.2 Proceso de evaluación de controles:

Identificación de controles aplicados a cada riesgo inherente, revisando los procedimientos, lineamientos, sistemas y prácticas ya implementadas por la entidad.

8.9.2.1 Clasificación del tipo de control:

- Preventivo: evita que el evento ocurra.
- Detectivo: permite identificar el evento una vez ocurrido.
- Correctivo: actúa después de ocurrido el evento para restablecer la situación.

8.9.2.2 Evaluación de la formalidad y eficacia de los controles:

- Formalidad: verificación de si el control está documentado y aprobado formalmente.
- Frecuencia de ejecución: continua, periódica o eventual, según su naturaleza.
- Efectividad: análisis de si el control cumple su propósito, mediante observación directa, entrevistas y revisión documental.
- Responsables: identificación de quién ejecuta y quién monitorea el control.

8.9.2.3 Documentación en la matriz de riesgos

Registrando los controles existentes asociados a cada riesgo, su tipo, frecuencia, nivel de efectividad y responsables, lo cual será insumo para valorar el riesgo residual.

Este ejercicio contribuye a fortalecer el sistema de gestión de riesgos de seguridad de la información, permite identificar controles ineficaces o ausentes y orientar adecuadamente la definición de medidas adicionales en la etapa de tratamiento de riesgos.

8.10 Tratamiento de los riesgos de seguridad de la información

Una vez identificados, analizados y evaluados los riesgos inherentes en materia de seguridad de la información, la E.S.E. Hospital San Rafael de Itagüí define las estrategias de tratamiento de riesgos, con base en los criterios de aceptabilidad y el apetito de riesgo institucional establecidos en la Política Integral de Administración de Riesgos.

El tratamiento de riesgos constituye un proceso cíclico y estratégico, cuyo objetivo es modificar el nivel de riesgo identificado mediante la implementación de medidas que reduzcan su probabilidad de ocurrencia, su impacto, o ambos. Este proceso se realiza teniendo en cuenta las opciones definidas en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información del Departamento Administrativo de la Función Pública (DAFP), las cuales son:

- Evitar el riesgo: Modificar o eliminar las actividades que originan el riesgo.
- Mitigar el riesgo: Aplicar controles que reduzcan su impacto o probabilidad.

- Compartir el riesgo: Transferir parcial o totalmente el riesgo a un tercero (por ejemplo, a través de seguros o acuerdos con proveedores).
- Aceptar el riesgo: Asumir el riesgo cuando se encuentra dentro de los límites de tolerancia institucional, dejando evidencia de su justificación.

8.10.1.1 Controles de referencia

Cuando la entidad decide mitigar un riesgo, debe seleccionar e implementar controles que permitan reducir de forma efectiva su probabilidad de ocurrencia o su impacto. Para ello, se debe tener como base la Sección 4. Objetivos de Control y Controles de Referencia del MSPI, fundamentada en el Anexo A de la Norma ISO/IEC 27001:2013, el cual proporciona un conjunto estructurado de controles agrupados por dominios como:

- Seguridad organizacional
- Gestión de activos
- Control de accesos
- Seguridad física y ambiental
- Seguridad en las operaciones
- Seguridad en el desarrollo de sistemas
- Continuidad del negocio, entre otros

No obstante, la E.S.E. podrá diseñar e implementar nuevos controles no contemplados en dicho anexo, siempre que estos resulten efectivos y eficaces para reducir el riesgo, de acuerdo con las condiciones específicas del entorno institucional.

8.10.1.2 Registro y ejecución del tratamiento

Cada acción de tratamiento debe ser registrada en el Plan de Tratamiento de Riesgos de Seguridad de la Información, indicando para cada riesgo:

- Acción seleccionada (evitar, mitigar, compartir o aceptar)
- Descripción de los controles asociados
- Responsable de implementación
- Recursos requeridos
- Plazos de ejecución
- Indicadores de seguimiento

La ejecución del plan de tratamiento es liderada por los líderes de proceso y el responsable de seguridad digital, con acompañamiento de la Oficina de Planeación y en articulación con la alta dirección. Este plan debe actualizarse de forma periódica y ajustarse en función de los resultados de monitoreo, auditorías y cambios en el entorno de riesgo.

El tratamiento eficaz de los riesgos permite asegurar la protección de los activos de información, garantizar la continuidad operativa institucional y fortalecer la confianza de los usuarios y partes interesadas frente a la gestión de la seguridad digital en la E.S.E.

8.11 Planes de Tratamiento de Riesgos de Seguridad de la información e Indicadores para la Gestión del Riesgo

La E.S.E. Hospital San Rafael de Itagüí formula e implementa planes de tratamiento de riesgos de seguridad de la información como instrumento de gestión clave para reducir los niveles de exposición a amenazas que puedan comprometer la confidencialidad, integridad, disponibilidad y legalidad de la información institucional.

Estos planes se estructuran con base en el Esquema de la Guía del DAFP, el cual orienta la consolidación técnica y operativa del tratamiento de los riesgos identificados y valorados, permitiendo hacer seguimiento efectivo a las medidas implementadas y a la eficacia de los controles.

8.11.1 Estructura del Plan de Tratamiento

Cada plan de tratamiento documenta, al menos, los siguientes elementos:

- Identificación del riesgo: Código, descripción y clasificación.
- Nivel de riesgo residual esperado: Luego de aplicar los controles.
- Acción de tratamiento definida: Evitar, mitigar, compartir o aceptar.
- Controles asociados: Existentes y por implementar (técnicos, administrativos o físicos).
- Responsables: funcionario o área encargada de implementar y monitorear la acción.
- Recursos requeridos: Humanos, tecnológicos o financieros.
- Cronograma de ejecución: Fechas de inicio, fin y estado de avance.
- Indicadores de gestión: Para evaluar efectividad y cumplimiento del tratamiento.
- Evidencias de implementación: Registros, informes, actas o soportes técnicos.

8.11.2 Indicadores para la Gestión del Riesgo

La E.S.E. establece indicadores de gestión para monitorear la eficacia y efectividad de las acciones implementadas. Estos indicadores deben ser medibles, verificables y relevantes, alineados con los objetivos institucionales y el Modelo de Seguridad y Privacidad de la Información (MSPI). Algunos ejemplos incluyen:

- % de ejecución del plan de tratamiento de riesgos
- % de riesgos mitigados con respecto al total priorizado
- Nivel de reducción del riesgo residual por riesgo identificado
- % de cumplimiento del cronograma del plan de tratamiento

Estos indicadores deben ser revisados periódicamente por la Línea Estratégica de la entidad y reportados al Comité de riesgos, como parte del proceso de monitoreo y mejora continua.

9 EJECUCIÓN

La fase de ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se enfoca en implementar de manera efectiva las acciones definidas en la etapa de planificación, dando cumplimiento a la ruta crítica establecida en los planes de tratamiento formulados.

En esta fase, la E.S.E. Hospital San Rafael de Itagüí asume el compromiso institucional de convertir la planeación estratégica en acciones concretas, destinadas a disminuir los niveles de riesgo identificados sobre los activos de información y garantizar la seguridad digital en la operación de sus procesos.

9.1 Responsabilidades durante la ejecución

La Línea Estratégica de la entidad tiene la responsabilidad de asegurar la disponibilidad y asignación de los recursos necesarios —humanos, tecnológicos, financieros y de tiempo— para dar inicio y continuidad a la implementación de los planes de tratamiento.
El responsable de Seguridad Digital y de la Información ejerce funciones de acompañamiento, verificación y supervisión, asegurando que:

- Los controles definidos sean implementados según lo previsto.
- Los responsables asignados —especialmente la Primera Línea de Defensa (líderes de proceso) y la Oficina de Tecnologías de la Información— ejecuten las tareas conforme al cronograma y con los recursos apropiados.
- Se mantenga un registro sistemático del avance, las evidencias de implementación y las desviaciones que puedan requerir ajustes correctivos.

9.1.1 Controles de referencia para la mitigación

En los casos donde el tratamiento del riesgo implique su mitigación, se debe considerar como base técnica la Sección 4 del MSPI – Objetivos de Control y Controles de Referencia, fundamentada en el Anexo A de la norma ISO/IEC 27001:2013. Esta referencia establece un conjunto de controles orientados a preservar la confidencialidad, integridad y disponibilidad de la información.

No obstante, la E.S.E. podrá diseñar e implementar controles propios, distintos a los contenidos en la norma, siempre y cuando estos resulten efectivos y eficaces para reducir la probabilidad o el impacto del riesgo identificado.

9.1.2 Seguimiento en la ejecución

Durante esta fase, se debe asegurar que:

- Las tareas se ejecuten dentro de los tiempos pactados.
- Los recursos asignados se utilicen de acuerdo con lo planeado.

- Cualquier ajuste necesario sea documentado y justificado.
- Se recopilen las evidencias que respalden la implementación efectiva de las acciones.

La ejecución disciplinada y documentada del plan de tratamiento es fundamental para lograr una gestión de riesgos madura, fortalecer la seguridad de la información institucional y garantizar el cumplimiento de las obligaciones normativas en materia de gobierno digital.

10 MONITOREO Y REVISIÓN

La fase de monitoreo y revisión del Plan de Tratamiento de Riesgos de Seguridad de la Información tiene como propósito verificar la efectividad de las acciones implementadas, evaluar el desempeño de los controles, y actualizar la gestión del riesgo de acuerdo con la evolución del entorno institucional, los resultados obtenidos y los hallazgos identificados.
Este proceso debe ser ejecutado bajo el enfoque de las Tres Líneas de Defensa definido en la Dimensión 7 – Control Interno del Modelo Integrado de Planeación y Gestión (MIPG), mediante actividades sistemáticas de seguimiento, revisión y evaluación técnica.

Actividades clave de monitoreo y revisión

10.1 Seguimiento al plan de tratamiento

- Monitorear en tiempo real el avance en la implementación de las acciones previstas.
- Verificar el cumplimiento de los cronogramas, responsables y uso adecuado de los recursos signados.

10.2 Evaluación de riesgos residuales

- Una vez ejecutadas las acciones, realizar una nueva valoración del riesgo para determinar si su nivel ha disminuido (ej. movimiento en el mapa de calor).
- Comparar el riesgo residual actual con la última medición para verificar el efecto del tratamiento aplicado.

10.3 Monitoreo y actualización de controles

- Revisar periódicamente las actividades de control existentes para determinar su vigencia, eficacia y pertinencia.
- Evaluar si los controles están diseñados e implementados adecuadamente y si están operando conforme a lo previsto.
- Recomendar ajustes, refuerzos o sustitución de controles, en caso de evidenciarse ineficiencia o ineficacia.

10.4 Análisis de incidentes de seguridad

- Considerar los incidentes de seguridad de la información reportados como insumo para reevaluar el riesgo y fortalecer el tratamiento.
- Analizar causas raíz y establecer medidas correctivas para prevenir su recurrencia.

10.5 Evaluación del desempeño del plan

- Aplicar los indicadores definidos para valorar el cumplimiento, la efectividad del tratamiento y el impacto de los controles en la gestión del riesgo.
- Documentar resultados, hallazgos y brechas persistentes.

10.6 Participación de la línea estratégica

La Alta Dirección y el Comité de riesgos deben recibir reportes periódicos del avance y resultados, para la toma de decisiones informadas y ajustes de alto nivel en la política de administración del riesgo.

10.7 Consideraciones adicionales

El proceso de monitoreo debe ser continuo, basado en evidencia y orientado a la mejora continua del sistema de gestión de riesgos de seguridad de la información. Las actividades de revisión deben quedar documentadas y formar parte del ciclo anual de gestión institucional, integrándose con auditorías internas, evaluaciones de control interno y planes de mejoramiento.

10.8 Registro y reporte de incidentes de seguridad de la información

La E.S.E. Hospital San Rafael de Itagüí reconoce la importancia de contar con un proceso estructurado y sistemático para el registro y análisis de los incidentes de seguridad de la información que se presenten en la entidad, con el objetivo de mejorar la capacidad institucional para anticiparse, responder y prevenir situaciones que afecten la confidencialidad, integridad, disponibilidad o legalidad de la información.

Propósito del registro de incidentes

10.8.1 El registro de incidentes permite:

- Identificar las causas que originaron el incidente, sean técnicas, humanas, organizacionales o externas.
- Detectar deficiencias o fallas en los controles existentes y valorar su efectividad real.
- Medir el impacto y las pérdidas generadas por el incidente, ya sean operativas, económicas, reputacionales o legales.
- Retroalimentar el proceso de gestión del riesgo, enriqueciendo el análisis de amenazas y vulnerabilidades para prevenir su recurrencia.
- Adoptar nuevos controles o ajustar los existentes con base en la evidencia obtenida.
- Construir estadísticas históricas que permitan identificar tendencias y patrones en la ocurrencia de incidentes.

10.8.2 Requisitos del proceso

La entidad implementara un procedimiento formal que contemple:

- Un formato estandarizado de reporte de incidentes, que incluya fecha, tipo de incidente, activo afectado, causa probable, controles comprometidos, impacto estimado, acciones tomadas y responsables.
- Una línea de reporte clara para que servidores públicos, contratistas o usuarios puedan informar oportunamente cualquier situación anómala o incidente detectado.
- Un registro consolidado de incidentes, bajo custodia del responsable de Seguridad Digital, que garantice integridad, trazabilidad y confidencialidad de la información reportada.
- La evaluación sistemática de cada incidente, con el fin de determinar si requiere revisión del plan de tratamiento de riesgos, rediseño de controles o reporte a instancias superiores.

10.8.3 Consideraciones sobre reporte externo

Si bien el reporte a terceros no constituye una obligación directa del presente componente, se recomienda que los incidentes relevantes, según su impacto y naturaleza, sean informados a los entes de control, autoridades regulatorias o instancias competentes, conforme a los marcos normativos aplicables y las buenas prácticas en materia de seguridad de la información.

Este proceso contribuye no solo a la mejora continua del MSPI, sino también al fortalecimiento de la cultura institucional de prevención y respuesta oportuna ante eventos que comprometan la seguridad digital del hospital.

10.9 Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública

La E.S.E. Hospital San Rafael de Itagüí, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), establece mecanismos formales para el reporte periódico y estructurado de la gestión del riesgo de seguridad de la información al interior de la organización. Estos reportes permiten a la alta dirección, al Comité de riesgos y a otras partes interesadas tomar decisiones informadas con base en la evolución de los riesgos, la eficacia de los controles y la efectividad de los planes de tratamiento implementados.

10.9.1 Responsable del reporte

El responsable de Seguridad Digital y de la Información debe consolidar y presentar estos reportes de forma periódica, asegurando su alineación con los lineamientos institucionales, los requerimientos del MIPG y las recomendaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

10.9.2 Contenido mínimo del reporte

Los informes deben incluir, como mínimo, los siguientes elementos:

- Matriz de riesgos identificados de seguridad de la información, con su respectiva clasificación y valoración.
- Listado de activos críticos de Tecnologías de la Información (TI) y Tecnologías de la Operación (TO), incluyendo aquellos considerados como Infraestructuras Críticas Cibernéticas (ICC).
- Reporte de niveles de criticidad o impacto de los activos y procesos evaluados.
- Estado de avance del Plan de Tratamiento de Riesgos, incluyendo acciones ejecutadas, pendientes, responsables y cronograma.
- Evolución del riesgo y su modificación, con base en nuevas amenazas, incidentes o controles implementados.
- Cantidad de riesgos fuera del nivel de tolerancia institucional, identificados según la evaluación periódica.
- Estimación del impacto económico potencial que se derivaría de la materialización de los riesgos más relevantes.

Frecuencia y momentos del reporte

Los reportes deberán generarse y presentarse:

- Periódicamente, al menos de forma semestral, como parte del ciclo de seguimiento institucional.
- Cuando se presenten cambios organizacionales o estructurales que impacten los procesos, activos o controles previamente definidos, lo cual requerirá una reevaluación de los riesgos.
- Cuando se incorporen nuevos procesos o servicios dentro del alcance del MSPI, requiriendo análisis de riesgos adicionales y su integración al sistema de gestión.

Estos reportes deben quedar formalmente documentados, socializarse con los tomadores de decisión, y servir como insumo para la mejora continua del modelo de seguridad de la información, la priorización de recursos, y el fortalecimiento de la cultura organizacional en torno a la gestión del riesgo.

10.10 Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales

Una vez la E.S.E. Hospital San Rafael de Itagüí haya desarrollado e implementado el proceso de gestión del riesgo de seguridad de la información, deberá estar en capacidad de consolidar y reportar información crítica a las autoridades o instancias especializadas definidas por el Gobierno Nacional, con el propósito de contribuir a la construcción de un panorama nacional sobre amenazas, vulnerabilidades y riesgos emergentes en el sector público.

10.10.1 Finalidad del reporte externo

Este reporte busca aportar información estratégica para:

- Identificar necesidades comunes en las entidades públicas.
- Facilitar el diseño de políticas públicas orientadas al fortalecimiento de la ciberseguridad estatal.
- Promover la asignación eficiente de recursos para la implementación de controles en entidades con mayores niveles de exposición.
- Potenciar la generación de capacidades institucionales a nivel territorial y sectorial.

10.10.2 Contenido del reporte

Para este fin, la entidad deberá consolidar la siguiente información, como resultado del proceso aplicado con base en el Modelo de Seguridad y Privacidad de la Información (MSPI):

- Riesgos con nivel crítico identificados en el análisis institucional.
- Amenazas y vulnerabilidades críticas que ponen en riesgo los activos de información o servicios clave.
- Tipos de activos afectados por los riesgos críticos, especialmente aquellos que soportan servicios digitales expuestos a internet.
- Planes de tratamiento definidos para dichos riesgos, especificando si han sido ejecutados total o parcialmente.
- Servicios digitales críticos para la entidad, como sistemas de atención al usuario, portales de trámites, historiales clínicos electrónicos o plataformas de interoperabilidad.
- Infraestructuras Críticas Cibernéticas (ICC), cuando aplique, con información técnica suficiente que permita su inclusión en el panorama nacional de activos sensibles.

10.10.3 Consideraciones operativas

- Este reporte no implica el traslado de la responsabilidad sobre los riesgos o su tratamiento a la autoridad receptora.
- La información debe consolidarse de forma técnica, veraz y sustentada, siguiendo los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y otras instancias competentes.
- El responsable de Seguridad Digital y de la Información será el encargado de generar el informe, validarlo con la línea estratégica y remitirlo cuando se solicite o cuando se presenten situaciones que ameriten su reporte.

10.10.4 Reportes relacionados con ICC

En caso de que la E.S.E. haya identificado activos clasificados como Infraestructura Crítica Cibernética (ICC), deberá consolidar y reportar esta información de manera diferenciada, conforme a los lineamientos técnicos del Comando Conjunto Cibernético o de la autoridad

nacional definida para este fin, contribuyendo así a la protección coordinada de los activos vitales para la prestación de servicios esenciales del Estado.

10.11 Auditorías internas y externas

La gestión del riesgo de seguridad de la información en la E.S.E. Hospital San Rafael de Itagüí está sujeta a procesos de auditoría interna y externa con el propósito de garantizar su funcionamiento adecuado, identificar oportunidades de mejora y proporcionar aseguramiento independiente sobre la efectividad del Modelo de Seguridad y Privacidad de la Información (MSPI).

10.11.1 Auditoría interna

La Oficina de Control Interno, en su calidad de tercera línea de defensa según el Modelo Integrado de Planeación y Gestión (MIPG), es responsable de incluir la gestión del riesgo de seguridad de la información como parte del Universo de Auditoría Institucional, y realizar su evaluación conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno. Dicha evaluación debe:

- Verificar el cumplimiento de los lineamientos definidos en el MSPI y la normativa vigente en materia de protección de datos y seguridad digital.
- Evaluar la eficacia de los controles implementados para mitigar los riesgos identificados.
- Validar la correcta ejecución del Plan de Tratamiento de Riesgos.
- Analizar la gestión de incidentes de seguridad de la información, la trazabilidad de sus causas y la efectividad de las acciones correctivas.
- Emitir recomendaciones para el mejoramiento continuo del sistema de gestión de riesgos.

10.11.2 Auditoría externa

La entidad podrá estar sujeta a auditorías externas por parte de:

- Organismos de control, como la Contraloría General de la República, la Procuraduría General de la Nación o la Superintendencia Nacional de Salud.
- Revisoría Fiscal, en el marco de su función de vigilancia contable y operativa.
- Entidades certificadoras, en caso de adoptar esquemas de certificación voluntaria relacionados con seguridad de la información (ej. ISO/IEC 27001).
- Otras instancias externas, en función de convenios, requerimientos regulatorios o esquemas de evaluación sectorial.

Las auditorías externas complementan los mecanismos de control institucional, aportan una visión imparcial y fortalecen la rendición de cuentas sobre el desempeño en materia de seguridad y privacidad de la información.

10.11.3 Consideraciones operativas

- Los resultados de las auditorías deben ser documentados, socializados y gestionados mediante planes de mejoramiento.
- El responsable de Seguridad Digital y de la Información debe estar disponible para atender requerimientos técnicos, proporcionar evidencias y liderar el cumplimiento de hallazgos relacionados con el MSPI.
- Los hallazgos de auditoría deben alimentar los ciclos de monitoreo, revisión y actualización del sistema de gestión de riesgos.

Este componente garantiza la transparencia, mejora continua y eficacia del enfoque institucional frente a la protección de los activos de información.

10.12 Medición del desempeño

La E.S.E. Hospital San Rafael de Itagüí implementa mecanismos de medición del desempeño como parte fundamental del seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI). Estos mecanismos permiten evaluar de manera objetiva el cumplimiento de los objetivos propuestos en la gestión del riesgo de seguridad de la información, así como la efectividad de las acciones implementadas y de los controles establecidos. Propósito de la medición.

10.12.1 La medición del desempeño tiene como propósito:

- Verificar la efectividad de los planes de tratamiento de riesgos y la pertinencia de las estrategias aplicadas.
- Evaluar la eficiencia operativa de los controles de seguridad establecidos sobre los activos de información.
- Generar información objetiva y periódica para la toma de decisiones por parte de la alta dirección y el Comité Institucional de Coordinación de Control Interno.
- Identificar desviaciones, retrasos o brechas en la gestión del riesgo que deban ser corregidas o ajustadas.
- Fomentar la rendición de cuentas y la cultura de mejora continua en torno a la seguridad de la información.

10.12.2 Indicadores de desempeño

La entidad definió e implementara un conjunto de indicadores de gestión y resultado, medibles, verificables y alineados con los objetivos del MSPI. Algunos ejemplos de indicadores incluyen:

- % de implementación del plan de tratamiento de riesgos
- % de reducción del nivel de riesgo residual
- % de controles evaluados como eficaces
- % de incidentes de seguridad analizados con acciones correctivas implementadas

- % de cumplimiento del cronograma de evaluación y seguimiento de riesgos

Estos indicadores serán evaluados de forma periódica, según la frecuencia establecida por la entidad (trimestral, semestral o anual), y los resultados serán presentados a la línea estratégica como parte de los procesos de revisión y toma de decisiones en materia de seguridad de la información.

10.12.3 Consideraciones operativas

- La Oficina de Planeación y Calidad, en articulación con el responsable de Seguridad de la Información, será la encargada de consolidar los datos.
- Los resultados deben ser documentados en informes técnicos y utilizados como insumo para la revisión del MSPI, la actualización del mapa de riesgos y los ajustes a los controles implementados.
- Toda desviación significativa deberá dar lugar a la formulación de acciones de mejora o correctivas, y a su inclusión en los planes institucionales de seguimiento.
- Este componente fortalece el sistema de gestión del riesgo al proporcionar evidencia objetiva y continua sobre el nivel de desempeño institucional en materia de seguridad y privacidad de la información.

11 MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital San Rafael de Itagüí, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), establece como principio fundamental la mejora continua de la gestión de riesgos de seguridad de la información, con el fin de garantizar una respuesta efectiva ante amenazas emergentes, incidentes, no conformidades y hallazgos derivados de auditorías internas o externas.

Esta fase tiene como propósito fortalecer las capacidades institucionales para anticiparse, adaptarse y responder de manera oportuna a los desafíos que comprometan la confidencialidad, integridad, disponibilidad y legalidad de la información, así como para optimizar los controles y medidas existentes en el sistema.

Acciones clave para el mejoramiento continuo:

11.1 Revisión y análisis de hallazgos

- Analizar sistemáticamente los hallazgos derivados de auditorías internas, externas, revisiones de entes de control, autoevaluaciones y seguimiento de incidentes.
- Establecer la causa raíz y las consecuencias reales o potenciales de cada hallazgo.

11.2 Identificación de hallazgos recurrentes o similares

- Identificar patrones o eventos repetitivos que puedan reflejar debilidades estructurales o fallas sistemáticas en los controles implementados.
- Priorizar acciones correctivas que eviten su recurrencia.

11.3 Adopción de acciones correctivas, preventivas y de mejora

- Formular e implementar medidas de mejora que permitan reducir la probabilidad o el impacto de riesgos similares en el futuro.
- Integrar estas acciones en los planes de tratamiento, el plan de mejora institucional o los sistemas de calidad de la entidad.

11.4 Revisión continua de controles y riesgos

- Evaluar periódicamente la pertinencia y eficacia de los controles existentes.
- Realizar ajustes ante cambios normativos, tecnológicos, de procesos o de contexto institucional.

11.5 Documentación y trazabilidad

- Llevar un registro sistemático y documentado del tratamiento realizado a cada hallazgo.
- Incluir información sobre las acciones adoptadas, responsables, cronograma de ejecución y resultados obtenidos.
- Usar esta información como insumo para la toma de decisiones y para retroalimentar los procesos de análisis de riesgos y planificación de controles.

11.6 Gestión del conocimiento y cultura de mejora

Promover en todos los niveles de la organización una cultura de autocontrol, aprendizaje institucional y proactividad, orientada a la mejora continua de la seguridad de la información.

11.7 Consideraciones finales

- La mejora continua no solo permite reducir vulnerabilidades existentes, sino también fortalecer la capacidad institucional para anticipar riesgos futuros, responder de manera eficiente a eventos adversos y asegurar la sostenibilidad del MSPI en el tiempo.
- Este enfoque permite a la E.S.E. evolucionar hacia un modelo de gestión más resiliente, estratégico y alineado con los estándares de gobernanza digital exigidos por la normativa nacional y las mejores prácticas internacionales.

12 CONTROLES DE REFERENCIA PARA LA MITIGACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital San Rafael de Itagüí, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), establece que la mitigación de riesgos identificados se debe realizar a través de la aplicación de controles de seguridad adecuados, basados en estándares internacionales y buenas prácticas, que garanticen la reducción efectiva de la probabilidad de ocurrencia o del impacto de los eventos adversos.

Para este fin, se adoptan como referencia los controles y objetivos de control definidos en el numeral 12.1 del documento maestro del MSPI, los cuales están alineados con el Anexo A de la Norma ISO/IEC 27001:2013, y ofrecen una base estructurada y validada para asegurar los activos de información frente a amenazas internas y externas.

12.1 Objetivos y dominios de control

Los controles están organizados en varios dominios estratégicos que cubren diferentes aspectos de la seguridad de la información, entre ellos:

12.1.1 Políticas de seguridad de la información

Establecimiento de directrices y normativas internas que orienten la gestión de la seguridad en la entidad.

12.1.2 Organización de la seguridad de la información

Asignación de roles, responsabilidades y estructuras de gobernanza.

12.1.3 Seguridad de los recursos humanos

Controles previos, durante y después del vínculo laboral, para garantizar la confiabilidad del personal.

12.1.4 Gestión de activos

Inventario, clasificación, protección y uso adecuado de los activos de información.

12.1.5 Control de accesos

Implementación de mecanismos de autenticación, autorización y segregación de funciones.

12.1.6 Criptografía

Uso de técnicas de cifrado y protección de la información confidencial.

12.1.7 Seguridad física y del entorno

Protección de instalaciones, equipos y medios físicos.

12.1.8 Seguridad en la operación

Procedimientos operativos, gestión de cambios, copias de respaldo, protección contra software malicioso, entre otros.

12.1.9 Seguridad en las comunicaciones

Control del acceso a redes, protección de la información en tránsito, gestión de servicios de comunicación electrónica.

12.1.10 Adquisición, desarrollo y mantenimiento de sistemas

Requisitos de seguridad en el ciclo de vida de los sistemas de información.

12.1.11 Relaciones con proveedores

Gestión de riesgos asociados a terceros con acceso a información o infraestructura crítica.

12.1.12 Gestión de incidentes de seguridad de la información

Reporte, respuesta y aprendizaje institucional derivado de incidentes.

12.1.13 Gestión de la continuidad del negocio

Medidas para garantizar la operación continua frente a interrupciones o desastres.

12.1.14 Cumplimiento

Aseguramiento del cumplimiento legal, contractual y normativo aplicable.

12.1.15 Aplicación práctica en la entidad

La selección e implementación de estos controles debe estar directamente relacionada con los riesgos priorizados en el proceso de análisis y valoración, y deberá justificarse en términos de su efectividad y viabilidad técnica, operativa y presupuestal. Además, se podrán diseñar controles complementarios o personalizados, siempre que cumplan con el propósito de mitigar eficazmente los riesgos y que sean evaluados periódicamente en cuanto a su eficiencia.

La documentación, asignación de responsables, frecuencia de aplicación y seguimiento de cada control será registrada en la Matriz de Controles del MSPI, lo cual facilitará su auditoría, monitoreo y mejora continua.

13 PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

La programación de estrategias y actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 se estructura de manera articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI), priorizando acciones viables, sostenibles y alineadas con la capacidad operativa institucional.

Las actividades definidas permiten gestionar, monitorear y mejorar de forma progresiva el tratamiento de los riesgos identificados, garantizando el cumplimiento normativo, la protección de los activos de información y la optimización de los recursos disponibles. La ejecución se realizará mediante actividades periódicas (mensuales, trimestrales o semestrales), evitando la duplicidad de esfuerzos y aprovechando los productos y evidencias generados en otros instrumentos de gestión institucional.

N°	ESTRATEGIA	ACTIVIDAD	RESPONSABLE	PERIODO	MEDIO DE VERIFICACIÓN
1	Gobierno del riesgo	Articular el Plan de Tratamiento de Riesgos con el Plan MSPI 2026	Líder de Sistemas	Enero	Plan de tratamiento articulado
2	Identificación del riesgo	Validar los activos de información críticos que soportan los riesgos priorizados	Líder de Sistemas	Marzo	Listado de activos críticos
3	Análisis del riesgo	Actualizar la matriz de riesgos de seguridad y privacidad de la información	Líder de Sistemas / Planeación	Abril	Matriz de riesgos actualizada
4	Evaluación del riesgo	Priorizar riesgos y definir nivel de tratamiento	Líder de Sistemas	Abril	Matriz priorizada
5	Tratamiento del riesgo	Definir y actualizar acciones de tratamiento de riesgos priorizados	Líder de Sistemas	Mayo	Plan de tratamiento de riesgos
6	Implementación de controles	Ejecutar y verificar los controles definidos para el tratamiento de riesgos	Líder de Sistemas	Trimestral	Registro de seguimiento
7	Gestión de incidentes	Analizar incidentes de seguridad como insumo para la reevaluación de riesgos	Líder de Sistemas	Semestral	Informe de análisis
8	Seguimiento y control	Realizar seguimiento al avance del Plan de Tratamiento de Riesgos	Líder de Sistemas	Trimestral	Registro de seguimiento
9	Evaluación y mejora	Evaluar la efectividad del tratamiento de riesgos y definir acciones de mejora	Líder de Sistemas	Diciembre	Informe de evaluación

14 PRESUPUESTO

La ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 se realizará, en su mayoría, con los recursos humanos, técnicos y tecnológicos existentes en la entidad, en articulación con el Modelo de Seguridad y Privacidad de la Información (MSPI).

En caso de requerirse recursos adicionales para la implementación de controles específicos, estos serán gestionados a través de los mecanismos institucionales de planeación y presupuesto, conforme a la disponibilidad financiera y a la priorización establecida por la línea estratégica de la entidad.

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 ejecución del plan de tratamiento de riesgos	(Número de acciones implementadas / Total de acciones previstas) x 100	≥ 90%	Trimestral
% de riesgos mitigados con respecto al total priorizado	(Riesgos mitigados con controles eficaces / Total de riesgos priorizados) x 100	≥ 90%	Trimestral
Nivel de reducción del riesgo residual por riesgo identificado	Comparación del nivel de riesgo antes y después del tratamiento	≥ 90%	Trimestral
% de cumplimiento del cronograma del plan de tratamiento	(Acciones ejecutadas en tiempo / Total de acciones programadas) 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
No aplica	Modelo nacional de gestión de riesgo de la seguridad de la información en entidades públicas. Anexo técnico: Anexo 4 – DAFP. 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
2022-01-17	1	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022	Samuel Guevara Mejía Líder Sistemas
2023-01-30	2	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023	Samuel Guevara Mejía Líder Sistemas
2024-01-20	3	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024	Henry González s. Líder Sistemas
2025-01-28	4	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025	Francisco Henao Hernández Líder Sistemas
2025-01-30	5	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026	Francisco Henao Hernández Líder 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