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

	NOMBRE	CARGO	FECHA
ELABORÓ	Jaime Andrés Sánchez Díaz	Líder de Sistemas	01/2026
VALIDÓ	Diego Fernando Rivera Castro	Jefe de la Oficina Asesora de Planeación	01/2026
APROBÓ	Comité Institucional de Gestión y Desempeño		01/2026

CONTENIDO

1.

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, tiene como finalidad ser un instrumento de mejora continua, implementa un método lógico y sistemático que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

Este se elabora con base al Modelo de Seguridad y Privacidad de la Información emitida por MinTIC con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en Seguridad y Privacidad de la Información, el Comprende las acciones transversales, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada, salvaguardando los datos y asistenciales y administrativos en nuestro hospital, garantizando la Confidencialidad, Integridad y Disponibilidad de la información, con instrumentos que permitan la autenticación y no repudio en sus procesos informáticos.

El Hospital Regional de Moniquirá, se enfocará en el Modelo de Seguridad y Privacidad de la Información –MSPI-, en cuanto a la Gestión de Riesgos será utilizada la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica teniendo en cuanta como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

La metodología planteada, permitirá analizar lo que se tiene (Diagnostico), identificando las necesidades de la organización en cuanto al Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

De igual manera este documento se debe actualizar de forma periódica (anual) y garantizando que se encuentre acorde a los objetivos estratégicos organizacionales https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html .

2. OBJETIVOS

2.1. Objetivo General

Identificar, Controlar y mitigar los riesgos asociados a la seguridad y privacidad de la información, con el fin de proteger los activos de información, el manejo de medios, control de acceso y gestión de usuarios y así proteger la Confidencialidad, Integridad y Disponibilidad de la información, así como su privacidad tomando en cuenta tanto los procesos como de las personas vinculadas con la información de la institución

2.2. Objetivos Específicos

- Identificar y Gestionar los activos de información.
- Identificar los riesgos sobre los activos de información.
- Gestionar los controles para la mitigación de Riesgos.

3. TÉRMINOS Y DEFINICIONES

Las únicas fuentes validas, son las de referentes académicos o páginas estatales y/o gubernamentales.

ID	Termino	Definición	Fuente
1	Ámbito	Área o temática que aborda un dominio y que agrupa temas comunes dentro del dominio. Es la segunda capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial.	TI
2	Ambiente (de desarrollo, pruebas o producción)	Es la infraestructura tecnológica (hardware y software) que permite desarrollar, probar o ejecutar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información.	TI
3	Activo	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma	TI

ID	Termino	Definición	Fuente
		(sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).	
4	Activo de Información	En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.	TI
5	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 auditoria. (ISO/IEC 27000).	TI
6	Amenazas	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).	TI
7	Dato	Es una representación simbólica de una característica particular de un elemento o situación, que pertenece a un modelo de una realidad. Tiene un tipo (por ejemplo numérico, cadena de caracteres o lógico) que determina el conjunto de valores que el dato puede tomar. En el contexto informático, los datos se almacenan, procesan y comunican usando medios electrónicos. Constituyen los elementos primarios de los sistemas de información.	TI
8	Información	Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.	TI
9	Servicio Tecnológico	Es un caso particular de un servicio de TI que consiste en una facilidad	TI

ID	Termino	Definición	Fuente
		directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.	
10	Servicio de TI	Es una facilidad elaborada o construida usando tecnologías de la información para permitir una eficiente implementación de las capacidades institucionales. A través de la prestación de estos servicios es que TI produce valor a la organización. Los servicios de información son casos particulares de servicios de TI. Los servicios de TI deben tener asociados unos acuerdos de nivel de servicio. Servicio institucional	TI
11	Datos Personales	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).	TI
12	Privacidad	En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.	TI

ID	Termino	Definición	Fuente
13	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).	TI
14	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).	TI
14	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).´	TI
16	Riesgo de seguridad de la información	Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.	TI
17	Seguridad de la información	Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).	TI
18	Sistema de Gestión de Seguridad de la Información SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades,	TI

ID	Termino	Definición	Fuente
		responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).	
19	Partes interesadas (Stakeholders)	Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, pág. 11)	TI
20	Hardware	Se refiere a la parte física del equipo, la parte tangible, la que se puede ver y tocar.	TI
21	Software	Estos son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador. Por ejemplo Word, Excel, los sistemas operativos, los navegadores de internet, etc.	TI
22	Control de Riesgos	El Control de Riesgos se refiere al proceso de identificar, evaluar y mitigar los riesgos que pueden afectar negativamente a una organización, proyecto o individuo. Esto implica el uso de estrategias y medidas para minimizar o eliminar los efectos adversos de estos riesgos. Es fundamental en la gestión empresarial y se aplica en diversos sectores para asegurar la continuidad y el éxito de las operaciones.	TI
23	Medidas de Mitigación	Las medidas de mitigación son acciones que se implementan para reducir los efectos adversos de un fenómeno o situación perjudicial. Estas medidas pueden aplicarse en	TI

ID	Termino	Definición	Fuente
		diversos contextos como el medio ambiente, la salud, la seguridad, y la economía, entre otros. En general, el objetivo es disminuir la vulnerabilidad y el impacto negativo sobre las personas, las propiedades y los recursos	
24	Tipos de Activos de Seguridad de la información	Los activos de seguridad de la información se refieren a los recursos valiosos que se deben proteger para asegurar la confidencialidad, integridad y disponibilidad de la información en una organización	TI

4. MARCO LEGAL

Las Normas para considerar en lo referente al Hospital Regional de Moniquirá ESE y el Ministerio de las TIC son las siguientes: ´

ID	Norma	Número	Año	Emisor	Define
1	Ley Estatutaria de Protección de Datos Personales	1581	2012	Congreso de la República	Establece el régimen general de protección de datos personales en Colombia.
2	Decreto Reglamentario de la Ley de Protección de Datos Personales	1377	2013	Gobierno Nacional	Reglamenta parcialmente la Ley 1581 de 2012 sobre protección de datos personales.
3	Ley de Transparencia y del Derecho de Acceso a la Información Pública	1712	2014	Congreso de la República	Regula el acceso a la información pública y su protección bajo criterios de reserva y clasificación.

ID	Norma	Número	Año	Emisor	Define
4	Decreto Único Reglamentario del Sector Presidencia	1081	2015	Gobierno Nacional	Reglamenta la gestión de la información pública y la transparencia.
5	Ley de Delitos Informáticos	1273	2009	Congreso de la República	Protege la información y los datos frente a accesos, alteraciones y usos no autorizados.
6	Política Nacional de Seguridad Digital	CONPES 3854	2016	Consejo Nacional de Política Económica y Social – CONPES	Establece lineamientos para la gestión del riesgo digital y la ciberseguridad en el Estado.
7	Decreto Único Reglamentario del Sector TIC	1078	2015	Gobierno Nacional	Compila las normas del sector TIC, incluyendo Gobierno Digital y Seguridad Digital.
8	Decreto de Lineamientos para el fortalecimiento institucional de las áreas TIC	415	2016	Ministerio TIC	Define responsabilidades y liderazgo de las áreas TIC en las entidades públicas.
9	Decreto de Política de Gobierno Digital	767	2022	Gobierno Nacional	Establece la Política de Gobierno Digital e integra el Modelo de Seguridad y Privacidad de la Información (MSPI).

ID	Norma	Número	Año	Emisor	Define
10	Modelo de Seguridad y Privacidad de la Información – MSPI	N/A	Vigente	Ministerio TIC	Define el marco metodológico para la gestión de la seguridad y privacidad de la información en entidades públicas.
11	Norma Técnica Colombiana – Sistema de Gestión de Seguridad de la Información	NTC ISO/IEC 27001	Vigente	ICONTEC	Establece requisitos para implementar, mantener y mejorar un SGSI.
12	Código de Buenas Prácticas de Seguridad de la Información	NTC ISO/IEC 27002	Vigente	ICONTEC	Proporciona controles y buenas prácticas para la seguridad de la información.
13	Acuerdo sobre Gestión de Documentos Electrónicos	003	2015	Archivo General de la Nación	Define lineamientos para la gestión y preservación de documentos electrónicos.
14	Acuerdo sobre Gestión Documental en Entidades Públicas	008	2019	Archivo General de la Nación	Establece criterios para la gestión documental en entidades públicas.
15	Acuerdo sobre Conservación de Documentos	002	2018	Archivo General de la Nación	Regula la conservación documental en el marco de la gestión documental.
16	Convenio sobre la Ciberdelincuencia (Convenio de Budapest)	Ley 1928	2018	Congreso de la República	Aprueba el convenio internacional para prevenir y combatir la

ID	Norma	Número	Año	Emisor	Define
					ciberdelincuencia.
17	Código Penal – Protección de la Información y los Datos	Ley 1273	2009	Congreso de la República	Tipifica delitos relacionados con la violación de datos y sistemas informáticos.
18	NTC ISO 3100:2018 . Gestión del Riesgo. Principios y Directrices	NTC ISO 3100:2018	2018	ICONTEC	Marco de referencia para la gestión de riesgos
18	Lineamientos de Gestión del Riesgo en Seguridad Digital Decreto 1083 de 2015	N/A	Vigente	Ministerio TIC / DAFP	Orienta la identificación, análisis y tratamiento de riesgos de seguridad digital.

5. RECURSOS

5.1. Talento Humano

ID	Recurso	Cantidad
1	INGENIEROS DE SISTEMAS	2
2	TEGNOLOGOS EN SISTEMAS	2
3	TECNICO EN SISTEMAS	1

5.2. Recursos económicos

ID	Recurso	Cantidad
1	20% de los honorarios anuales de un profesional de apoyo del área de sistemas para la implementación y seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	5.368.080

6. ENFOQUE DIFERENCIAL

Bajo este contexto el Hospital Regional de Moniquirá estableció el *Protocolo Enfoque Diferencial en todos los Servicios GIU-PT -01. Cargado en la pltaforma.*

7. DIAGNOSTICO PARA EL PLANTEAMIENTO DE ACCIONES

Durante la vigencia 2025, el Hospital Regional de Moniquirá E.S.E. adelantó actividades fundamentales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), orientadas a la identificación de los activos de información institucionales y la evaluación de los riesgos asociados a estos, en concordancia con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Política Institucional de Administración del Riesgo y la Guía para la Gestión del Riesgo del Departamento Administrativo de la Función Pública (DAFP), con referencia a la norma ISO 31000.

Como resultado de dicho ejercicio, la entidad construyó y documentó el inventario de activos de información, clasificándolos de acuerdo con su naturaleza, criticidad y relación con los procesos misionales, estratégicos y de apoyo. De manera complementaria, se realizó el análisis de riesgos de seguridad y privacidad de la información, identificando amenazas, vulnerabilidades, impactos y niveles de riesgo, considerando los principios de confidencialidad, integridad y disponibilidad de la información.

La matriz de riesgos elaborada en 2025 permitió identificar riesgos relevantes asociados, entre otros aspectos, a:

- Accesos no autorizados a la información.
- Pérdida, alteración o indisponibilidad de la información institucional.
- Fallas en la continuidad de los servicios tecnológicos.
- Debilidades en controles técnicos, administrativos y operativos.
- Dependencia de servicios tecnológicos críticos para la prestación de los servicios de salud.

Este ejercicio constituyó una línea base institucional para la gestión de riesgos de seguridad y privacidad de la información, permitiendo evidenciar que, si bien la entidad cuenta con avances importantes en la identificación y documentación de activos y riesgos, persisten brechas en

la implementación, seguimiento, monitoreo y efectividad de los controles, así como en la gestión de incidentes y la continuidad operativa.

En este contexto, el diagnóstico realizado en 2025 no se considera un ejercicio aislado, sino un insumo estratégico que alimenta directamente el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026. El plan parte de los resultados obtenidos, evita la duplicidad de esfuerzos, prioriza los riesgos identificados y orienta las acciones hacia el fortalecimiento de los controles existentes, la implementación de medidas adicionales de mitigación y el seguimiento sistemático de los riesgos residuales.

De esta manera, el presente Plan de Tratamiento de Riesgos consolida y da continuidad al proceso iniciado en 2025, enfocándose en:

- La actualización y validación de los activos de información y sus riesgos asociados.
- La definición e implementación de controles técnicos, administrativos y operativos.
- El fortalecimiento del proceso de gestión de incidentes de seguridad de la información.
- La mejora de las capacidades de continuidad y recuperación ante eventos adversos.
- El seguimiento periódico y la evaluación de la efectividad de los controles implementados.

Este enfoque garantiza la coherencia del plan con el MSPI, fortalece la madurez institucional en la gestión de la seguridad y privacidad de la información y responde a los requerimientos de auditoría, asegurando trazabilidad entre el diagnóstico, el análisis de riesgos y las acciones definidas para su tratamiento.

8. PLAN DE ACCIÓN

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
1	Actualización de Activos de Información	Líder de Sistemas	Inventario de Activos actualizado y alineado con tablas de Retención de gestión Documental	09/2026
2	Actualización Riesgos de seguridad y privacidad de la Información	Área TIC	Riesgos aprobados por el CIGYD	03/2026
3	Identificación de controles (100%)	Área TIC	Número de controles documentados / Total de riesgos identificados	03/2026
3	Seguimiento a los diferentes tipos de controles implementados (Tabla Anexo) (100%)	Área TIC	Número de seguimientos con registro / Total de seguimiento planificados	04/2026 a 12/2026 (Mensual)
4	Implementación y actualización del Procedimiento de Gestión de Incidentes de Seguridad de la Información	Área TIC	Procedimiento aprobado y registros de incidentes gestionados	03/2026
5	Ejecución de pruebas de vulnerabilidad sobre	Área TIC	Informe de pruebas de vulnerabilidad y plan de	06/2026

	infraestructura y sistemas críticos		tratamiento	
6	Implementación y prueba del Plan de Recuperación de Desastres (DRP)	Área TIC	DRP documentado y evidencia de prueba de recuperación	07/2026
7	Capacitación y sensibilización del personal en seguridad y privacidad informática	Área TIC / Talento Humano	Cronograma	Febrero/ 2026
			Ejecución de Capacitaciones	Abril-junio/ 2026
			Evaluación de conocimiento	Julio/2026

Tipos de Controles

Control	Tipo	Enfoque	Aplicación
Procedimiento DRP	Administrativo	Preventivo / Correctivo	Activación ante caída de servicios
Backups y restauración	Técnico	Preventivo / Correctivo	Recuperación de información
Monitoreo de servicios	Técnico	Detectivo	Detección temprana
Acciones correctivas	Correctivo	Correctivo	Restablecer y mejorar
Continuidad operativa	Administrativo / Técnico	Continuidad	Atención mínima garantizada
Comunicación	Administrativo	Preventivo	Información oportuna

9. BIBLIOGRAFÍA

https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

ISO 31000, citado en http://www.uptc.edu.co/export/sites/default/gel/documentos/plan_trata_rie_seg_inf2020.pdf

10. CONTROL DE CAMBIOS

Espacio de diligenciamiento en caso de requerir alguna actualización o cambio del documento.

CONTROL DE CAMBIOS			
Versión	**Descripción del Cambio**	**Aprobó**	**Fecha**
1	Actualización anual del plan	CIGYD	01/2026