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

	NOMBRE	CARGO	FECHA
ELABORÓ	Jaime Andrés Sánchez Díaz Cristian Sneider Aguirre Guerrero	Líder de Sistemas Apoyo de Sistemas	01/2025
VALIDÓ	Diego Fernando Rivera Castro	Jefe de la Oficina Asesora de Planeación	01/2025
APROBÓ	Comité Institucional de Gestión y Desempeño		01/2025

CONTENIDO

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

ID	Termino	Definición	Fuente
		adquiera, transforme o controle en su calidad de tal.	
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

ID	Termino	Definición	Fuente
9	Servicio Tecnológico	Es un caso particular de un servicio de TI que consiste en una facilidad 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.	TI
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	TI

ID	Termino	Definición	Fuente
		proteger dicha información en observancia del marco legal vigente.	
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	TI

ID	Termino	Definición	Fuente
		positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.	
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, 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).	TI
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,	TI

ID	Termino	Definición	Fuente
		los sistemas operativos, los navegadores de internet, etc.	
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 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	TI
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 a considerar en lo referente al Hospital Regional de Moniquirá ESE y el Ministerio de las TIC son las siguientes:´

ID	Norma	Numero	Año	Emisor	Define
1	Decreto 1377 de 2013	1377	2013	Secretaría Distrital de Seguridad, Convivencia y Justicia.	Protección de datos
2	Decreto 1747 de 2000	1747	2000	Gobierno Nacional.	Entidades de certificación, los certificados y las firmas digitales
3	Decreto 2364 de 2012	2364	2012	Gobierno Nacional.	Firma electrónica
4	Ley 1266 de 2008	1266	2008	Congreso de la República	Disposiciones generales de habeas data y se regula el manejo de la información
5	Ley 1450 de 2011	1450	2011	Función publica	Bases de datos y seguridad de la Información en PND
6	Ley 1712 de 2014	1712	2014	Función publico	Ley de Transparencia y acceso a la información pública
7	Ley Estatutaria 1581 de 2012	1581	2012	Gobierno nacional	Protección de datos personales
8	Ley 1928 de 2018	1928	2018	El congreso de Colombia	Convenio sobre la ciberdelincuencia

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.Equipos Físicos

ID	Recurso	Cantidad
1	EQUIPOS DE COMPUTO	4

5.3.Recursos Tecnológicos

ID	Recurso	Cantidad
1	NA	NA

5.4.Recursos económicos

ID	Recurso	Cantidad
1	Incluidos dentro del plan de seguridad de la información	NA

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

Para identificación de los activo se seguirá los lineamientos dados por el misterio de las TIC.

***Figura 1**. Metodología para la Gestión del riesgo de seguridad de la información según DAFP*

Imagen 2. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Los Riesgos se gestionarán de acuerdo con la política de institucional de Administración de Riesgos.

Es de resaltar que actualmente la entidad no cuenta riesgos identificados tratados y los controles actuales son el resultado del cumplimiento de la política de seguridad de la información y carece de enfoque sistemático.

8. PLAN DE ACCIÓN

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
1	Identificación de Activos de Información.	Área TIC	Inventarios de activos aprobado por el CIGYD	Julio
2	Identificar Riesgos de seguridad y privacidad de la Información	Área TIC	Riesgos aprobados por el CIGYD	Agosto
3	Seguimiento a controles	Área TIC	Seguimiento en Almera	Septiembre a Diciembre (Mensual)

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**