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

CAMBIOS EFECTUADOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
02	Diseño del plan institucional según lineamientos del Decreto 612 de 2018, orientado al cumplimiento de los objetivos y metas institucionales, priorizadas para la vigencia 2025	31-01-2025

	ELABORÓ	REVISÓ	APROBÓ
FECHA	**31-01-25**	**31-01-25**	**31-01-25**
CARGO	**Asesor Administrativo**	**Comité Institucional de Gestión y Desempeño**	**Gerente**

1. INTRODUCCIÓN

La evolución tecnológica y las continuas revoluciones digitales en donde se enmarca la información como el componente más importante en los procesos productivos de cada entidad, ha permitido que la gestión de activos de información cobre una importante relevancia para identificar las debilidades o fallas, que afecten sus pilares de seguridad (disponibilidad, confidencialidad e integridad) todo bajo una misma y correcta administración donde salvaguarde estos importantes elementos.

Con lo anterior uno de los principales objetivos de la seguridad y privacidad de la información es protegernos de un conjunto de amenazas que atenten contra los activos de información y a sus pilares de seguridad como, también identificar los actores y roles de cada uno de los que intervienen en el manejo, soporte y control de estos activos, por lo tanto, para que todo lo enmarcado en la política de seguridad y privacidad de la información se cumpla, la entidad debe dar un tratamiento, administración y adecuada clasificación a la información bajo unos procedimientos que estén alineados con la Política de Seguridad y Privacidad de la Información de la E.S.E Hospital San Vicente de Ramiriquí.

2. DEFINICIONES

- **Riesgo**: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- **Activo**: Todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc.
- **Información**: La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Análisis de riesgos**: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización
- **Causa**: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados
- **Consecuencia**: Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo**: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control**: Medida que modifica el riesgo. 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.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos**: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento**: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Estimación del riesgo.** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evitación del riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **Identificación del riesgo.** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Integridad**: Propiedad de la información relativa a su exactitud y completitud.
- **Impacto.** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Nivel de riesgo**: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **Monitoreo**: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.
- **Propietario del riesgo**: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Proceso**: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.
- **Riesgo en la seguridad de la información**: 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.
- **Riesgo Inherente**: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Residual**: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguimiento**: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- **Tratamiento del Riesgo**: Proceso para modificar el riesgo.
- **Valoración del Riesgo**: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

3. OBJETIVO

Establecer una guía que proporcione una metodología adecuada para tratamiento de los riesgos y que permita identificar los roles de cada una de las partes y los responsables de cada activo de información que gestionarán dichos riesgos orientados a seguridad y privacidad de la información con el fin de para minimizar la probabilidad que se materialice una amenaza y un posible alto impacto en la Entidad.

4. ALCANCE

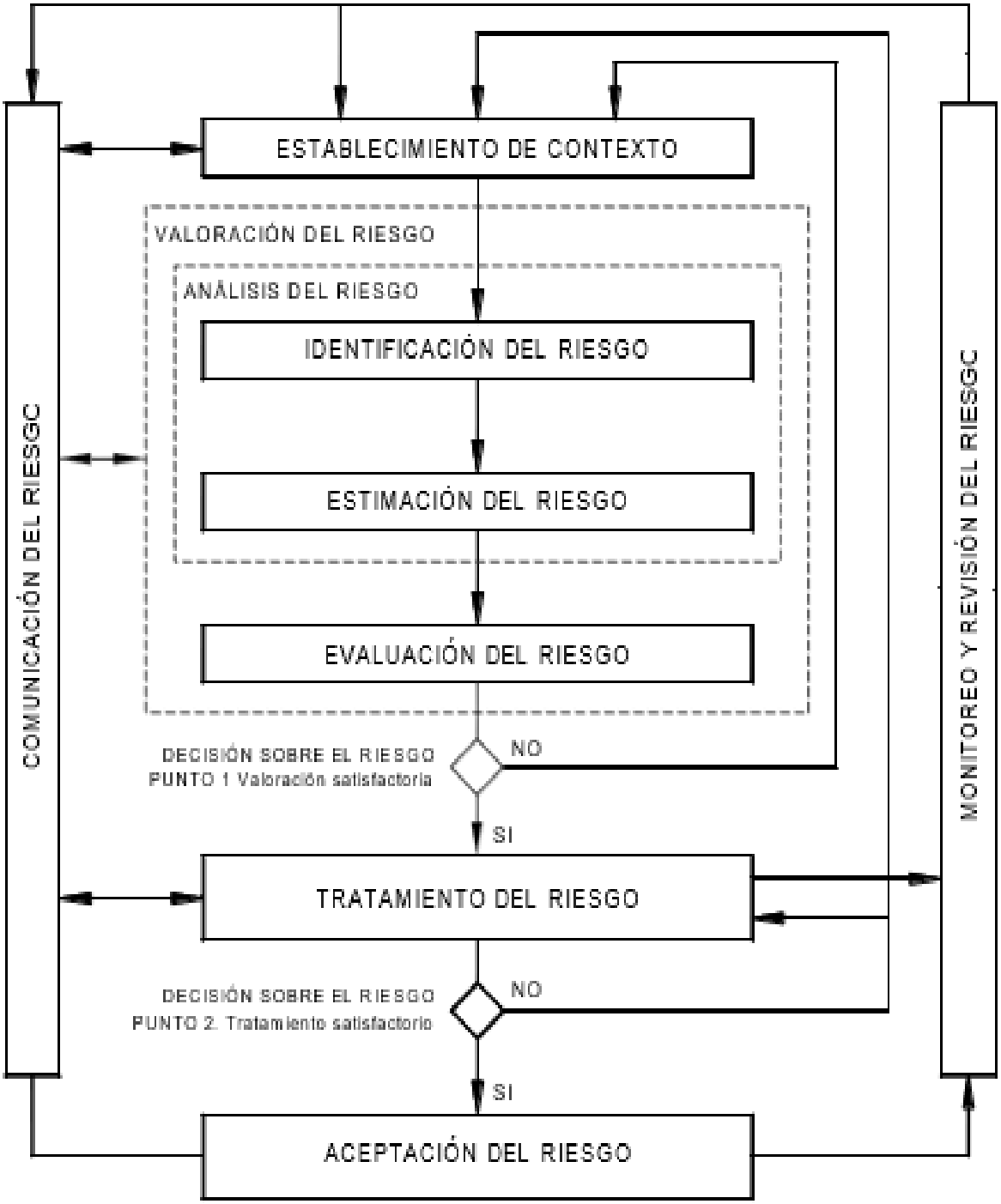
El plan de tratamiento de riesgo está orientado para la ser aplicado a toda la entidad, sus servidores públicos, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios de tecnología de la información de la E.S.E Hospital San Vicente de Ramiriquí, con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas por el MINTIC, para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

5. MARCO REFERENCIAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Resolución 500 de marzo 10 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- NTC / ISO 27001:2013, Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.
- NTC/ISO 31000:2009, Gestión del Riesgo. Principios y directrices.
- Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 527 de 1999 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
- Ley 1712 de 2014, Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- Ley Estatutaria 1581 de 2012, Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- Decreto 103 de 2015, Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
- Decreto 1494 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Ley 1474 de 2011, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

6. MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN



7. IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD DIGITAL

Este documento apoya al dueño de la información o delegado para la etapa de identificación y clasificación del riesgo cuando se trata de un "Riesgo Seguridad Digital", alineado con el Instructivo para la Gestión del Riesgo del MINTIC, en donde es necesario tener en cuenta que estos riesgos serán tratados en sus etapas iniciales y finales de acuerdo al mencionado instructivo y para los activos de información que en el Registro de Activos de Información de la entidad, hayan sido clasificados como de criticidad "Alta" por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad, razón por la cual se consideraría que existe un riesgo de la información en alguno de éstos tres pilares.

Al respecto, se debe tener en cuenta que la criticidad de los activos de información será valorada de acuerdo a la Guía para la Gestión y Clasificación de Activos de Información de MINTIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital, midiéndose por los tres pilares de la seguridad de la información "CONFIDENCIALIDAD", "INTEGRIDAD", "DISPONIBILIDAD" según la clasificación que determina el numeral 7 de dicha Guía, de la siguiente manera:

Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tras la valoración del activo de información por cada uno de los tres pilares en el Formato Registro de Activos de Información, se debe clasificar el Activo en el nivel de criticidad "ALTA", "MEDIA" o "BAJA"), de acuerdo a las condiciones de la Guía para la Gestión y Clasificación de Activos de Información de MINTIC de la siguiente manera:

Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

El resultado de esta valoración se refleja finalmente en el instrumento de información pública, Registro de Activos de Información, a partir del cual se seleccionan para tratamiento de riesgos, todos los activos de información clasificados con nivel de criticidad "ALTA"

De acuerdo con lo especificado en la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas y con ayuda del Módulo de Gestión del Riesgo del sistema SIPG se deberá especificar la amenaza de acuerdo a la siguiente tabla de referencia:

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

Tras el registro de una amenaza, se deberán especificar las vulnerabilidades, de acuerdo con la metodología del Anexo 4 – Lineamientos para la Gestión del Riesgo de seguridad digital en las Entidades Públicas y con ayuda del Módulo de Gestión del Riesgo del aplicativo SIIP, se deberá especificar la vulnerabilidad de acuerdo a la siguiente tabla de referencia:

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

8. CRONOGRAMA DE ACTIVIDADES

Para la elaboración del cronograma se debe contar con el recurso humano que tenga los conocimientos en el tratamiento de riesgos de seguridad y privacidad de la información y así poder realizar la programación de las actividades establecidas por el MINTIC, descritas en la siguiente tabla. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

Gestión	Actividades	Tareas	Responsable de	Fechas Programación Tareas

			la Tarea	Fecha Inicio	Fecha Final
Gestión de Riesgos	Levantamiento de activos de información	Actualizar activos de información	Equipo de Gestión de Riesgos	01/25	12/25
	Actualización lineamientos de Riesgos	Actualizar Política y Metodología de Gestión de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Sensibilización	Socializar Guía y Herramienta de Gestión de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Socialización con la Jefatura	Socializar con jefe(a) de la OIP	Equipo de Gestión de Riesgos	01/25	12/25
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Diseño del Plan de Tratamiento de Riesgos	Diseñar del Plan de Tratamiento de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Publicación Plan de Tratamiento de Riesgos	Publicación Matriz de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Desarrollo Plan de Tratamiento de Riesgos	Ejecutar Plan de Tratamiento de Riesgos	Equipo de Gestión de Riesgos	01/25	12/25
	Evaluación de Riesgos Residuales	Evaluación de Riesgos Residuales	Equipo de Gestión de Riesgos	01/25	12/25
	Mejoramiento Continuo	Identificar oportunidad de mejora con resultados obtenidos	Equipo de Gestión de Riesgos	01/25	12/25
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	01/25	12/25

9. FASES METODOLOGÍA TRATAMIENTO DE RIESGOS

Se establecen varias etapas para la mitigación de los riesgos sobre los activos, estas actividades se definen mediante las siguientes fases:

FASE 1: Activos de Información

1. Levantamiento de Información
2. Clasificación de los activos de información
3. Socialización documento final con Coordinador

FASE 2: Plan Seguridad y Privacidad de la Información

1. Identificación de Riesgos
2. Borrador Plan de Tratamiento de Riesgos
3. Socialización Coordinador y jefe de la OIP
4. Publicación tratamiento de Riesgos

FASE 3: Evaluación de Riesgos de Seguridad y Privacidad de la Información

1. Controles según en análisis y evaluación de riesgos
2. Validar riesgos mitigados en la evaluación de riesgos
3. Analizar aplicabilidad de las medidas
4. Priorización de las medidas
5. Definir los responsables de cada uno de los riesgos
6. Establecer objetivos sobre cada uno de los riesgos
7. Definir las Actividades a realizar

FASE 4: Monitoreo de Controles de Riesgos de Seguridad y Privacidad de la Información

1. Identificación de las funciones de la entidad en materia de seguridad de la información.
2. Definición del grupo de trabajo de gestión de riesgo por parte de la entidad.
3. Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.