PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

emserfusa E.S.P.	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información. El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

En busca de mejorar la seguridad de EMSERFUSA E.S.P, es necesario que se ejecute el plan para el tratamiento de los riesgos de seguridad y privacidad de la información. El propósito de este plan es adoptar una cultura preventiva que funcione una vez se materialice una amenaza de la seguridad en la empresa, sin embargo, se deben planear acciones que reduzcan el riesgo, cuyo objetivo debe estar orientado a desarrollar estrategias para identificar, analizar, tratar, evaluar y monitorear los riesgos.

Teniendo en cuenta lo establecido por el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad - MSPI de MinTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. OBJETIVO GENERAL

Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica alineada al instructivo para la Gestión del Riesgo (E-IN-005), que permita a los responsables de los procesos de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P gestionar los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información que hacen parte del Registro de Activos de Información de EMSERFUSA E.S.P y que sean identificados con una criticidad alta por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad.

2.1 OBJETIVOS ESPECÍFICOS

- Definir y aplicar lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información.
- Desarrollar el plan en alineación con los requisitos legales establecidos por la legislación colombiana.
- Incluir el plan en la cultura organizacional de la empresa para que sea base del conocimiento de la gestión de los riesgos de seguridad y privacidad de la información, de los servicios digitales y de la continuidad del negocio.
- Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos
- Establecer e implementar controles específicos a través de planes.
- Reducir la probabilidad de materialización de los riesgos sobre los activos de información.
- Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos

3. ALCANCE

Mitigar o controlar los riesgos de acuerdo con su nivel de impacto sobre los activos de información, sistemas de información, aplicaciones y redes de datos, realizando una gestión adecuada de los riesgos de seguridad y privacidad de la información, con el fin de que haya una integración de los procesos, las buenas prácticas que incluyan la toma decisiones para prevenir incidentes que pueda afectar el desarrollo de las operaciones normales de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P.

4. DEFINICIONES

- **Activo:** Cualquier elemento que tenga valor para la organización.
- **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.
- **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.
- **Amenaza:** Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **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. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)
- **Causa:** Elemento específico que origina el evento.
- **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.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **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.
- **Criterios de riesgos:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **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.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **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.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **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.
- **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.
- **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.
- **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.
- **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.
- **Probabilidad:** Posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.
- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Riesgo:** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los

intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **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
- **Vulnerabilidad:** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

5. MARCO NORMATIVO

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 1078 del 26 de mayo del 2015 Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones
- Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de 11. Gobierno Digital, antes Gobierno en Línea y 12. Seguridad Digital.
- Decreto 612 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.
- Resolución 500 del 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

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Departamento Administrativo de la Función Pública 2020.
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, territoriales y sector público, Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013
- Norma Técnica Colombiana NTC-ISO 31000:2011
- CONPES 3854 de 2016. Política Nacional de Seguridad digital

6. VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

La Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P asume la gestión de los riesgos de información (incluyendo los riesgos tecnológicos) con base en la Política Institucional de Administración del Riesgo y recomendaciones de las ISO 31000 y 27005.

Se tomará como base para la gestión de los riesgos de información, el ejercicio documentado de identificación del contexto organizacional, aplicado a cada uno de los procesos estratégico, misional y de apoyo de la entidad; de igual forma se parte de la metodología de tratamiento de riesgo de la entidad razón por la cual este documento solamente abordará las etapas de identificación y clasificación del riesgo cuando se trata de un Riesgo de Seguridad Digital.

6.1 MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

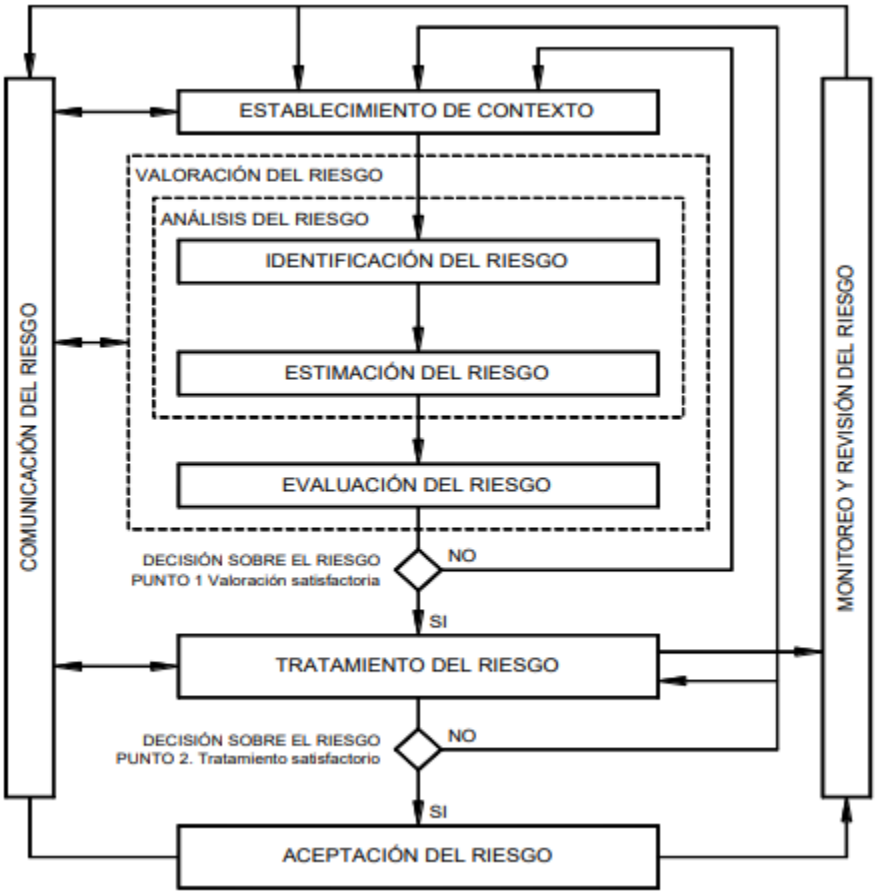

Ilustración 1: Proceso para la administración de riesgos de seguridad y privacidad de la información

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

Ilustración 2: Criterios 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.

Ilustración 3: Niveles de clasificación

7. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P . Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de

falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo.

Ilustración 4: Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013)

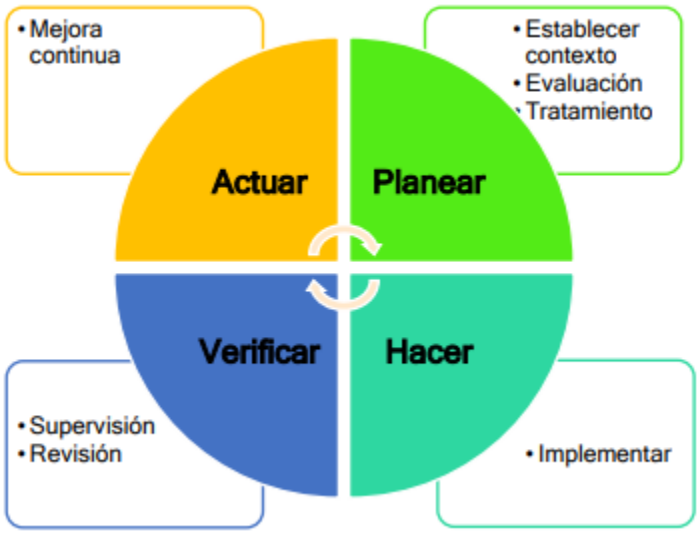

Ilustración 5: Ciclo PHVA y la gestión de riesgos

8. PLAN DE TRATAMIENTO

De acuerdo con los resultados del análisis de riesgos se identifican vulnerabilidades que deben ser corregidas para los procesos de la empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, lo que conlleva a un plan de tratamiento base que debe ser aplicado y que se describe en este documento. A continuación, se aborda el plan de tratamiento con base en los dominios de la Norma ISO 27001 base fundamental del Modelo de Seguridad y Privacidad de la Información - MSPI.

9. METODOLOGÍA

El procedimiento de seguridad y privacidad de la información contempla las actividades que permiten dar tratamiento y control para mitigar los riesgos sobre los activos de información, sistemas de información, aplicaciones y redes de datos de EMSERFUSA E.S.P.

emserfusa E.S.P.	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

ID	Actividades	Acciones	Documentos y/o Registros	Tiempo
1	Identificar factores internos y externos de seguridad de la información	Teniendo en cuenta: 1. Los factores internos son aquellos que están dentro de la empresa. 2. Los factores externos son los que están fuera de la empresa.	Diligenciando el formato Factor Internos y externos de riesgo SGC-F-11.	Semestral
2	Identificar los riesgos	1. Identificar con precisión los activos de información. 2. Identificar claramente los atributos de los activos de información. 3. Identificar las herramientas que comprometan la información y sus componentes. 5. Determinar las vulnerabilidades y amenazas de los activos de información correspondientes a las aplicaciones y herramientas. 6. Definir los riesgos de seguridad de la información detectados en los aplicativos y herramientas.	Diligenciar el formato de identificación de riesgos SGC-F-12. Diligenciar el formato Matriz de Riesgos Diligenciar el formato Mapa de Riesgos Proceso de SGC-F-14	
3	Analizar el riesgo de los activos de seguridad de la información	1. Establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos. 2. Definir el impacto de sus consecuencias, calificándolos y evaluándolos. 3. Determinar la capacidad de la empresa para aceptarlos y manejarlos.	Seguir las instrucciones del Instructivo Administración del Riesgo SGC-I-03 Procedimiento Administración del Riesgo SGC-P-05	
4	Valoración del riesgo de seguridad de la información	1. Realizar la ponderación de riesgos identificados por cada activo de información. 2. Establecer prioridades para su manejo a partir de la evaluación de la probabilidad de ocurrencia e impacto de los riesgos de seguridad de la información detectados.	Diligenciar los siguientes formatos: Mapa de Riesgos SGC-F-14. Controles óptimos para administrar el riesgo SCG-F-15. Análisis de controles existentes SGC-F-16.	

5	Administración del riesgo	1. Tomar acciones de mejora o de prevención de los riesgos cuyo resultado haya sido medio o alto. 2. Salvaguardar la seguridad de la información contenida en los activos de la información debe ser una actividad clave para la mejora continua.	Diligenciar el Formato de acciones correctivas y preventivas OCI-F-14.	
6	Monitoreo de los mapas de riesgo	Una vez elaborados los mapas de riesgos es necesario monitorearlos, teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización.	Hacer seguimiento de los formatos diligenciados previamente	
7	Oportunidad de mejora	Establecer elementos de mejora continúa teniendo en cuenta: 1. Acciones tendientes a la corrección y a la prevención de aquellas situaciones que lleven al incumplimiento en lo dispuesto a nivel de la organización en el marco del SGSI basado en la norma ISO 27001. 2. Registrar los incidentes de seguridad de la Información en la herramienta de gestión.	Los incidentes se registran siguiendo lo establecido en el Procedimiento de servicios tecnológicos OPEI-P-11	Cada vez que sea necesario

Gestión	Actividades	Tareas	Responsable de la tarea	Corresponsable	Fecha programación
Gestión de riesgos	Levantamiento de activos de información	Actualización activos de información	Todas las áreas		Semestralmente
	Actualización lineamientos de riesgo	Actualizar o crear política metodología de gestión de riesgos	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	1 vez al año
	Sensibilización	Socializar guía y herramienta de gestión de riesgos	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	1 vez al año

	Identificación de riesgos de seguridad y privacidad de la información	Identificación, análisis, y evaluación de los riesgos	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	Semestralmente
	Diseño del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Diseñar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	1 vez al año
	Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Publicación de Matriz de Riesgos	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	1 vez al año
	Desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Ejecutar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	Transcurso del año
	Mejoramiento continuo	Identificar oportunidad de mejora con resultados obtenidos	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	Semestralmente
	Monitoreo y revisión	Generación presentación y reporte de indicadores	Jefe Oficina de Planeación e Informática - OPEI	P.U Sistemas y Redes- Sistemas y Catastro	Semestralmente

CONTROL DE VERSIONES

CONTROL DE VERSIONES			
FECHA	**VERSIÓN**	**DESCRIPCIÓN DE ACTIVIDADES**	**APROBADO**
XX/XX/XXXX	1	Creación del documento con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para que sea revisado y aprobado por la alta gerencia de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P	Comité Institucional de Gestión y Desempeño