

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

**EMPRESA PUBLICA DE SOACHA
EPUXUA AVANZA E.I.C.E.**

Enero 2024

INTRODUCCIÓN Y GENERALIDADES

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC y el gobierno digital.

Por la cual es importante establecer 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 adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es importante que dentro de las organizaciones el plan de tratamiento de riesgos de Seguridad y Privacidad de la información este orientado estratégicamente al desarrollo de una cultura de carácter preventivo, donde cada usuario entienda los riesgos y las afectaciones que se puede presentar permitiendo tomar medidas que disminuyan la materialización de estos.

Para el tratamiento de riesgos de debe contar con un plan de gestión de riesgos para garantizar la continuidad del negocio, planeando acciones que disminuyan la afectación de los procesos, Por este motivo, se ha visto la necesidad de desarrollar la identificación, análisis, tratamiento, evolución y monitoreo de riesgo de seguridad de la información.

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Empresa Pública de Soacha EPUXUA AVANZA E.I.C.E.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos identificados en los procesos de la entidad, estas acciones son organizadas en actividades, definiendo para cada una de ellas las tareas, el responsable y sus fechas de ejecución que serán aplicadas durante la vigencia del plan.

Las actividades se definieron teniendo en cuenta la información del análisis de riesgos, de las necesidades y el contexto de los procesos de la entidad en cuanto a la seguridad y privacidad de la información proporcionando las herramientas necesarias para identificar sus características y definir los pasos a seguir para su ejecución.

La formulación y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información, se encuentra a cargo de la alta dirección, líderes de proceso y los funcionarios. Quienes deberán realizar estas gestiones teniendo en cuenta la importancia de la aplicación de las metodologías de gestión y administración del riesgo.

CONTEXTO ESTRATÉGICO DE LA ENTIDAD

La Empresa Pública del Municipio de Soacha, EPUXUA AVANZA E.I.C.E., fue creada mediante el Acuerdo No. 19 de 2021 por el Concejo Municipal de Soacha; es una empresa Industrial y Comercial del sector descentralizado del orden municipal altamente especializado, con personería jurídica, autonomía administrativa y financiera y patrimonio independiente.

Misión: La entidad tiene como misión contribuir al mejoramiento de la calidad de vida de los habitantes del Municipio de Soacha, por lo que desarrollará su objeto como una empresa autónoma especializada en la estructuración, gerencia, administración y desarrollo de proyectos de inversión, administración de los bienes inmuebles del municipio, y el inventario general del patrimonio del municipio, orientada al cumplimiento de políticas y metas organizacionales, a través de procesos integrales, eficientes, eficaces y transparentes que garanticen para sus clientes la satisfacción de sus requerimientos, contribuyendo de esta manera al desarrollo socioeconómico del municipio y de la región.

Visión: En el 2030 la EMPRESA PÚBLICA INDUSTRIAL Y COMERCIAL DEL ORDEN MUNICIPAL DE SOACHA, EPUXUA AVANZA E.I.C.E., será reconocida a nivel regional como una empresa experta, especializada, con inventario consolidado del patrimonio inmobiliario del Municipio, consolidada y robustecida en la gerencia integral de proyectos de inversión y promotora del desarrollo municipal y regional, auto sostenible.

Mediante la resolución 037 de 2023 se aprobó la operación por procesos de la entidad y se adoptó el Modelo Integrado de Planeación y Gestión – MIPG, la entidad presenta una estructura organización definida mediante el decreto 122 de 2021. Así mismo, mediante resolución 073 de 2023 se establecieron los mecanismos de planeación y seguimiento a la plataforma estratégica de la entidad.

Con la información que se recolectará en los diagnósticos durante la vigencia 2024, se analizarán los aspectos críticos para la Entidad y que deben ser analizados para priorizarlos de acuerdo al nivel de afectación y de riesgo que pueda generar a la entidad.

DEFINICIÓN DE ASPECTOS CRÍTICOS

- Daño físico en la infraestructura
- Eventos naturales
- Pérdidas de los servicios esenciales
- Compromiso de la información
- Fallas técnicas
- Acciones no autorizadas
- Compromiso de las funciones
- Amenazas humanas
- Mantenimiento insuficiente
- Descarga y uso no controlado de software
- Gestión inadecuada de la red
- Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
- Ausencia de procedimiento formal para el registro y retiro de usuario
- Ausencia de copias de respaldo
- Se requiere fortalecer y documentar la mejora continua del proceso.

Sin embargo, estas a situaciones identificadas y/o riesgos deben ser revisados de acuerdo a las metodologías de gestión del riesgo.

FORMULACIÓN DE LA VISIÓN ESTRATÉGICA DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El planteamiento de la Estrategia TI, está orientada a la protección y conservación del activo informático y toda la infraestructura tecnológica; deberá alinearse con el plan de desarrollo y con la finalidad de optimizar los recursos y visionar las necesidades actuales conforme a la demanda de protección y salvaguarda de la información, como estructura formal de políticas y lineamientos; adicionalmente, es necesario realizar un ejercicio de arquitectura empresarial de acuerdo con la estructura organizacional y funciones que definan la estrategia institucional y de tecnologías de la información dentro de los factores de definición y ejecución de procesos institucionales, Consolidación y presentación de indicadores, métricas e informes, Capacidad de respuesta operacional, Recurso humano capacitado, el sistema integrado de gestión de la entidad, el sistema de control interno y la gestión del riesgo.

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

OBJETIVO GENERAL

Definir las acciones necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, definiendo los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza, así como permitir la recuperación del sistema.

OBJETIVOS ESPECIFICOS

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, acorde a las necesidades de la entidad.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Dar a conocer la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Definir los principales elementos a proteger en la entidad.
- Identificar las principales amenazas en la entidad.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

FORMULACIÓN DE PLANES, PROGRAMAS Y PROYECTOS DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la identificación de riesgos se utilizará la metodología desarrollada por el Departamento Administrativo en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Así mismo, se tomaron referentes como la metodología de Gestión de Riesgos de Seguridad de la Información basada en la norma ISO 31000 y en la guía de Gestión del Riesgo Seguridad y Privacidad de la Información de MinTic, como se ilustra a continuación.



Proceso Gestión del Riesgo ISO 31000

Así mismo, los riesgos identificados, se deberán registrar en la matriz de riesgos institucional de la Empresa Pública Industrial y Comercial del Orden Municipal de Soacha, EPUXUA AVANZA E.I.C.E, donde se administrarán, a través de las instrucciones generadas y donde se aplicarán los controles para su prevención, mitigación, eliminación o asumir las consecuencias generadas.

CONTROL Y SEGUIMIENTO

Realizar monitoreo y evaluación a las actividades contenidas en el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información con el fin de prevenir, eliminar o mitigar de los riesgos identificados y generar las mejoras que se requieran. El monitoreo será realizado por el líder o responsable del proceso y se llevará a cabo de manera trimestral y se informará a la alta dirección sobre el resultado de su evaluación. Así mismo, El objetivo de la evaluación de la gestión del riesgo de los procesos de tecnología e información y de los procesos y/o dependencias tienen el fin de contribuir a la mejora continua del Sistema de Gestión de la entidad, de acuerdo a lo establecido en la resolución 073 de 2023.

Esto sin perjuicio de los seguimientos y evaluaciones independientes de la Oficina de Control Interno y los entes de Control.

AJUSTES AL PLAN

La alta dirección y/o los líderes d proceso podrán realizar los ajustes necesarios teniendo en cuenta los lineamientos establecidos en el presente documento, el Comité Institucional de Gestión y Desempeño, el Comité Institucional de Coordinación de Control Interno, las guías y procedimiento que la entidad disponga.

APROBACION

El presente plan fue presentado y aprobado en reunión conjunta del Comité Institucional de Coordinación de Control Interno, y el Comité Institucional de Gestión y Desempeño el día 30 de enero de 2024 como consta en acta 01 de 2024.