1. Objetivo

Desarrollar las actividades necesarias para tratar preventiva e integralmente los riesgos de Seguridad y Privacidad de la Información, a los que la Alcaldía del municipio de San José de Cúcuta puede estar expuesto, por medio de la protección de la integridad, confidencialidad y disponibilidad de la información en la vigencia 2023.

2. Objetivos generales

- Identificar los riesgos de Seguridad y Privacidad de la información y seguridad digital que se puedan presentan en la Alcaldía de San José de Cúcuta.
- Sensibilizar a los funcionarios de la Alcaldía de San José de Cúcuta referente a la gestión de riesgos de seguridad y Privacidad de la información y Seguridad Digital en la entidad.
- Ejecutar las actividades de acuerdo con el plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Cumplir con los requisitos legales en cuanto a la normativa aplicable.

3. Alcance

El Plan de Tratamiento de Riesgos contempla los riesgos de seguridad de la información y seguridad digital a los que puede estar expuesto el municipio de San José de Cúcuta. Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, recursos de infraestructura tecnológica para el tratamiento de la información y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas.

4. Responsabilidad

La Oficina de las Tecnologías de la Información y la Comunicación de la Alcaldía Municipal de San José de Cúcuta.

5. Normatividad

Decreto 1078 de 2015: Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información).

CONPES 3854 de 2017: Política Nacional de Seguridad Digital

Decreto 767 de 2022: mediante el cual se actualizó la política de Gobierno Digital del país.

Guía N° 7 MINTIC: Guía de gestión de riesgos de seguridad y privacidad de la información

Guía N° 8 MINTIC: Controles de seguridad y privacidad de la información

Manual para la Implementación de la Política de Gobierno Digital: Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019.

Modelo de Seguridad y Privacidad de la Información: Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

NTC / ISO 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices.

6. Terminología

- Activo: cualquier elemento que tenga valor para la organización.
- Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- Causa: Elemento específico que origina el evento.
- 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.).
- Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

- Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del 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: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Identificación del riesgo: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- Riesgo aceptable: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- Riesgo residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento
- Riesgo: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de 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.

7. Contenido

7.1. Generalidades

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

En el presente plan se identificarán las opciones para tratar y manejar los riesgos basados en su valoración lo cual permite tomar decisiones adecuadas y fijar lineamientos para la

gestión de estos. Para la toma de decisiones se deben tener en cuenta algunos criterios para su correcto tratamiento como las que se nombran a continuación:

- Evitar: Es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo.
- Prevenir: corresponde al área de planeación, esto es, planear estrategias adecuadas a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.
- Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo.
- Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad.

En este sentido, el tratamiento de los riesgos es acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), en la Guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información.

En el presente plan se estipulan directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información.

7.2. Desarrollo

6.2.1 ACTIVIDADES PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.

Actividad	Fecha de inicio	Fecha Fin
Elaboración de los lineamientos de riesgos de seguridad de la información y seguridad digital	**1 de febrero**	**31 de marzo**
Sensibilización	**1 de abril**	**30 de mayo**
Identificación de la herramienta para la elaboración de la matriz de riesgos de seguridad de la información y seguridad digital.	**1 de mayo**	**30 de mayo**
Mesas de trabajo con los líderes de los procesos	**1 de mayo**	**30 de mayo**
Identificación de riesgos	**1 de junio**	**30 de septiembre**
Aceptación del riesgo	**1 de junio**	**30 de septiembre**
Publicación	**1 de junio**	**30 de septiembre**
Evaluación y análisis de riesgos	**1 de octubre**	**30 de diciembre**
Acciones de mejora	**1 de octubre**	**30 de diciembre**
Monitoreo y revisión	**1 de octubre**	**30 de diciembre**

Descripción de actividades:

1. Elaboración de los lineamientos de riesgos de seguridad de la información y seguridad digital.

Elaborar y/o actualizar la política y los procedimientos de la administración de riesgos de seguridad de la información y seguridad digital.

2. Sensibilización:

Capacitación acerca de la seguridad de la información y seguridad digital mediante el cual se da a conocer a funcionarios, contratistas y terceros de la entidad las políticas y procedimientos de tratamiento de riesgos de Seguridad y Privacidad de la Información y seguridad digital mediante charlas y el uso de las herramientas de comunicaciones disponibles en la Entidad

3. Identificación de la herramienta para la elaboración de la matriz de riesgos de seguridad de la información y seguridad digital.

Se deberá identificar la herramienta (matriz) para la identificación de los riesgos, esta herramienta será establecida bajo los lineamientos descritos por el MinTIC y la guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información.

4. Mesas de trabajo con los líderes del proceso.

Esta actividad conlleva a realizar diferentes reuniones con los líderes de los procesos para un trabajo articulado y colaborativo con todas las dependencias de la Alcaldía de San José de Cúcuta.

5. Identificación de riesgos.

En esta fase se identificarán los riesgos asociados a cada proceso, se tomará como insumo la matriz de activos de información de la entidad, una vez tomada se identificarán los riesgos de seguridad y privacidad de la información y seguridad digital.

6. Aceptación del riesgo.

Una vez identificado se procederá aceptar el riesgo

7. Publicación.

Publicar y aprobar la matriz de riesgos de seguridad de la información y seguridad digital una vez aprobada esta será publicada en la página web institucional.

8. Evaluación y análisis de riesgos.

Evaluar los riesgos residuales que fueron producto de la identificación de los riesgos de seguridad de la información y seguridad digital.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, clasificándolos y evaluándose con el fin de obtener información para establecer el nivel de riesgo.
Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

9. Acciones de mejora.

Identificar las acciones de mejora de acuerdo con el resultado de la evaluación y análisis de los riesgos.

10. Monitoreo y revisión.

En esta actividad se realizarán informes acerca del cumplimento de las actividades establecidas en el plan de tratamiento de riesgos así mismo se llevará un reporte de indicadores de acuerdo con los controles efectuados a cada riesgo.

8. Plan de comunicaciones

Audiencia	Medio socialización	Instrumento	Fecha
Miembros del comité.	Presentación ante el comité de gestión y desempeño institucional.	Documento en Power Point Documento Pdf	Fecha del comité de gestión y desempeño
Usuarios interno y externos.	Publicación sede electrónica.	Página web.	31 de enero del 2023