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

OFICINA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ALCALDÍA MUNICIPAL DE SAN JOSÉ DE CÚCUTA.

2024

Contenido

1. Introducción.

En la era digital actual, la seguridad de la información se ha convertido en un pilar fundamental para el éxito y la sostenibilidad de cualquier entidad pública o privada que debido al crecimiento exponencial de las tecnologías de la información, la gestión efectiva de los riesgos de seguridad se ha vuelto más crítica que nunca, la capacidad de salvaguardar la confidencialidad, integridad y disponibilidad de la información que se genera dentro de la administración es esencial para preservar el conocimiento y la gestión la reputación, la confianza del cliente y el cumplimiento de regulaciones.

En el presente documento se desccriben las bases para el desarrollo e implementación del Plan de Tratamiento de Riesgos de Seguridad de la Información. Este plan es una iniciativa estratégica destinada a identificar, evaluar y gestionar proactivamente los riesgos que podrían comprometer la seguridad de la información en la Alcaldía de San José de Cúcuta.

2. Objetivo.

Establecer los lineamientos para proporcionar un marco estructurado y eficaz que trate de manera integral los riesgos de Seguridad y Privacidad de la Información y seguridad digital que se presenten en la Alcaldía de San José de Cúcuta con el objetivo de proteger, preservar la información de la entidad.

3. Objetivos Generales.

- Sensibilizar a los funcionarios de la Alcaldía de San José de Cúcuta en Seguridad y Privacidad de la Información.
- Identificar los riesgos de Seguridad y Privacidad de la información y seguridad digital que se puedan presentar en la Alcaldía de San José de Cúcuta.
- Elaborar y actualizar el mapa de riegos de seguridad digital de la entidad.
- Implementar medidas de seguridad digital efectivas.
- Dar cumplimiento a la normativa vigente.

4. Definiciones

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de 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. (ISO/IEC 27000).

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).

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

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Está asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

Control o Medida: Medida que permite reducir o mitigar un riesgo.

5. Metodología.

La administración de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

La metodología estará enfocada en la identificación, análisis y tratamiento de los riesgos que se puedan generar en la administración y afecten el cumplimiento de los objetivos de los procesos, y la toma de decisiones previniendo la materialización de estos riesgos. Esta metodología está basada en los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública y en la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTIC y la norma ISO 27001.

La oficina TIC como líder del Sistema de Gestión de Seguridad y Privacidad de la Información estableció un proceso para darle tratamiento a estos riesgos el cual se describe a continuación:

Identificación del riesgo (Activos y Amenazas)

- ✓ Se identifica y analiza las actividades que puedan ocasionar riesgos de información críticos, incluyendo datos, sistemas, redes y aplicaciones.
- ✓ Identifica las amenazas potenciales que podrían afectar la seguridad de activos.

Análisis de Riesgos:

- ✓ Se evalúa la probabilidad de ocurrencia y el impacto que pueda generar en la entidad la amenaza identificada.
- ✓ Se realiza un análisis de vulnerabilidades para identificar posibles debilidades en los controles de seguridad existentes.

Clasificación del riesgo:

- ✓ Se clasifican los riesgos en función de su gravedad y urgencia.
- ✓ Así mismo se deberá priorizar los riesgos para centrarse en los más críticos.

Valoración del Riesgo:

- ✓ Se establecen criterios para determinar qué tan crítico es el riesgo en el entorno de seguridad de la información.

Controles del Riesgo.

- ✓ Se deberán establecer ye ejecutar las actividades de tratamiento específicas para cada riesgo, como controles preventivos, medidas de mitigación, transferencia de riesgos o aceptación con el objetivo que el riesgo sea tratado y se disminuyan sus potenciales efectos sobre la entidad.

Monitoreo Continuo:

- ✓ Se realiza monitoreo continuo para evaluar la efectividad de los controles de seguridad.

Revisión y Mejora Continua:

- ✓ Se realizan revisiones regulares del plan de tratamiento de riesgos de seguridad de la información.

6. Fundamentos.

- ✓ Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
- ✓ 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
- ✓ Herramienta para la gestión de riesgos (Matriz para la identificación y valoración de riesgos SGSI).
- ✓ Norma ISO 27001 Sistema de Gestión de Seguridad de la Información.

7. Plan De Tratamiento De Riesgos

A continuación, se detalla el plan para el tratamiento de riesgos con sus respectivas actividades y entregables.

ID	ACTIVIDAD	Descripción	Periodo	Entregable
01	Sensibilización a los funcionarios.	Gestionar la capacitación con el MinTIC en Seguridad y Privacidad de la Información.	1 de febrero – 30 de abril de 2024	Informe de capacitación de los funcionarios .
02	Identificación de Riesgos.	Identificar analizar y evaluar los riesgos de seguridad y privacidad de la información	1 de mayo – 30 de junio de 2024	Informe de riesgos identificados .
03	Valoración del riesgo.	Se debe valorar que tanto impacto puede tener el riesgo identificado sobre la entidad	1 de julio – 30 de agosto de 2024	Matriz de riesgos de seguridad digital.
04	Aceptación del riesgo.	Una vez identificado se deberá aceptar y aprobar el riesgo.	1 de julio – 30 de agosto de 2024	Matriz de riesgos de seguridad digital.
05	Actualización de matriz de riesgos.	En esta actividad el riesgo debe ser incorporado y publicado en la matriz de riesgos de seguridad digital de la entidad.	1 de septiembre – 30 de octubre de 2024.	Matriz de riesgos de seguridad digital.

06	Actividades de control.	Se establecen las actividades que conlleven a la mitigación de los riesgos identificados en la entidad	1 de septiembre – 30 de octubre de 2024.	Matriz de riesgos de seguridad digital.
07	Seguimiento y monitoreo.	Se realiza una revisión de los riesgos identificados y se analiza su mitigación y se implementan acciones de mejora.	1 de noviembre – 30 de diciembre.	Informe de seguimiento y monitoreo de la matriz de riesgos.

8. Hoja de ruta

Audiencia	Medio socialización	Instrumento	Fecha
Miembros del comité.	Presentación ante el comité de gestión y desempeño institucional.	Documento en powert point. Documento pdf.	Fecha del comité de gestión y desempeño.
Usuarios interno y externos.	Publicación sede electrónica.	Página web.	31 de enero del 2024.