CONCEJO
SANTIAGO DE CALI

OFICINA INFORMÁTICA Y TELEMÁTICA

PLAN DE TRATAMIENTO DE RIESGOS

SANTIAGO DE CALI, ENERO DEL 2022

CONTENIDO

INTRODUCCION

El Concejo Distrital de Santiago de Cali se encuentra adelantando esfuerzos respecto a la definición de un Modelo de Seguridad y Privacidad de la Información (MSPI), dentro de las cuales se encuentran la identificación y clasificación de los activos de información pasos los cuales son insumo para el tratamiento de los riesgos que se ciernen sobre los activos de información.

La identificación y clasificación de los activos de información es una actividad estratégica para el Concejo al igual que lo es el tratamiento de riesgos, puesto que la primera determina la caracterización de los activos, se definen los roles y responsabilidades que tiene el personal sobre los mismos y reconoce sus niveles de confidencialidad, integridad y disponibilidad y la segunda determina el grado de exposición al riesgo y los controles que deban ser apropiados para llevar el riesgo a un nivel tolerable con el cual se pueda seguir desempeñando las labores institucionales de la mejor manera.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad 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.

TERMINOS Y DEFINICIONES

A continuación, se presenta el significado a términos que serán de manejo del presente documento y en el desarrollo de Modelo de Seguridad y Privacidad de la Información (MSPI)

Activo: Es cualquier cosa que tiene valor para la organización. Existen varios tipos de activos como:

- Información.
- Software.
- Físicos o hardware.
- Servicios.
- Talento humano.
- Intangibles como la reputación y la imagen.

Amenaza: Causa potencial de un incidente no deseado, que pueda ocasionar daño a un sistema u organización.

Análisis de Impacto al Negocio: Donde se determinan los recursos críticos y el tiempo de recuperación con las respectivas ventanas de criticidad mediante las cuales se debe restaurar los activos evaluados.

Análisis del Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.

Custodio: Encargado de guardar el activo con cuidado y vigilancia. Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información (sea el caso que depende de componentes tecnológicos); además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario de la información haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.

Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.

Propietario: El término “Dueño” o “Propietario” identifica a un individuo o a una entidad que tiene responsabilidad aprobada por la Dirección por el control de la producción, el desarrollo, el

mantenimiento, el uso y la seguridad de los activos. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

Evento de Seguridad de la Información: Se refiere a cualquier situación que pueda afectar los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información. Por ejemplo, una persona sospechosa que se encuentra cerca de un área protegida representa un incremento en el riesgo, pero no afecta los resultados comerciales ni compromete la información que se encuentre en el espacio restringido.

Incidente de Seguridad de la Información: Es un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones e información del negocio o ya se ha materializado y afectado a la organización.

Integridad: Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.

Principio del Mínimo Privilegio: Todos los usuarios en cualquier momento deben contar con tan pocos privilegios como sea posible para el ingreso a un activo de información.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la Información: Preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio, trazabilidad y confiabilidad podrían estar involucradas.

OBJETIVOS

- Conocer cuales son los riesgos inherentes de mayor impacto a los cuales se encuentra expuesto el Concejo Distrital de Cali en el desarrollo de su función pública.
- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los que pueda estar expuesto el Concejo Distrital de Cali, preservando la integridad, confidencialidad y disponibilidad de la información en el cumplimiento de los objetivos, la misión y la visión institucional.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana mediante la adopción de buenas prácticas recomendadas por el Gobierno Nacional respecto a la seguridad y privacidad de la información y la gestión del riesgo.
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.
- Fortalecer y apropiar el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información en los servidores públicos, contratistas y demás personas que hagan parte del desarrollo de la función pública del Concejo Distrital de Cali.

ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos de la entidad de acuerdo a lo establecido en el sistema de gestión de calidad y en la adopción de buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información haciendo uso del conocimiento y lineamientos impartidos por el Gobierno Nacional en los distintos materiales y guías de Gestión de Riesgos de Seguridad y Privacidad de la información. El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad

POLITICA DE GESTION DEL RIESGO

El Concejo Distrital de Cali en su compromiso con el aseguramiento de los activos de información y la gestión del riesgo, ha constituido una política de Gestión del Riesgo la cual ha sido consensuada entre un grupo interdisciplinar de profesionales especialistas en las áreas de tecnología, jurídico y calidad de procesos, con la finalidad de poder involucrar en esta una visión holística desde el ámbito legal, de procesos y tecnología, siendo tecnología un área de soporte para el desarrollo de los procesos en el Concejo.

La política de Gestión de Riesgos se encuentra en proceso de aprobación.

METODOLOGIA

El Plan de Tratamiento de Riesgos contempla la definición acciones a desarrollarse en pro de mitigar los riesgos que se ciernen sobre los activos de información del Concejo Distrital de Cali, siguiendo las actividades y mejores prácticas recomendadas por el Gobierno Nacional y normatividades del mercado en gestión del riesgo (Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información, ISO 31000).

GESTION	ACTIVIDAD	TAREA
Gestión del riesgo	Actualización de lineamientos de riesgo	Actualizar política y metodología de gestión del riesgo
	Sensibilización	Socialización de las guías y herramientas para la gestión del riesgo
	Identificación de seguridad y privacidad de la información	Identificación, análisis y evaluación de riesgos
		Realimentación, revisión y verificación de los riesgos identificados
	Aceptación de riesgos identificados	Aceptación, aprobación de riesgos identificados y planes de tratamiento
	Publicación	Publicación de la matriz de riesgos
	Seguimiento fase de tratamiento	Seguimiento estado de planes de tratamiento de riesgos identificados y verificación de evidencias (los controles que se definan en este apartado como medida para el tratamiento de los riesgos serán confrontados respecto a los controles establecidos en la Norma ISO 27001 Anexo A)
	Evaluación de riesgo residual	evaluación y aceptación del riesgo residual
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales
		actualización de la guía de gestión de riesgos de seguridad de la información, conforme a cambios solicitados
	Monitoreo y Revisión	Generación, Informe, presentación y reporte de indicadores

DESARROLLO DE LA METODOLOGIA.

Fase 1: Análisis de la Información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso del Concejo, desarrollándose las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

Fase 2: Desarrollo de los proyectos

- Determinar la medida.
- Definir los responsables de las medidas.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de cada medida.
- Definir las actividades a realizar para el desarrollo de la medida.

Fase 3: Análisis de los proyectos

En esta etapa se realizarán las actividades que permitan la estructuración de las medidas.

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

Fase 4: Definición del organigrama de responsabilidades

En esta fase se realizará un organigrama teniendo en cuenta la estructura organizacional del Concejo y se definirán responsabilidades respecto a la administración y gestión del riesgo.

- Identificación de las funciones en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo.

- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

Fase 5: Ciclo de vida del tratamiento de riesgos

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.
Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.
Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.
Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

OPORTUNIDADES DE MEJORA

El Concejo Distrital de Cali no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

RECURSOS

El Concejo Distrital de Cali, en el esfuerzo por salvaguardar y gestionar el riesgo que se cierne sobre sus activos de información, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	Hace referencia al personal adscrito a las diferentes dependencias del Concejo, servidores públicos y contratistas.
Técnicos	Guías y herramientas técnicas para la administración del riesgo y el diseño de controles en entidades públicas.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza de acuerdo a un indicador de gestión que está orientado principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, el indicador que se alimenta con los indicadores internos del modelo de seguridad y privacidad de la información MSPI y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones para la mejora del modelo de seguridad.

La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el número de controles a implementarse como propuesta para la mejora del perfil de riesgo y el porcentaje de implementación década uno de ellos. (en la definición del indicador o indicadores se recomienda observar la guía Numero 9 “Guía de indicadores de gestión para la seguridad de la información” dada por MINTIC).