PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

2023

1040.26.12

PEDRO ANTONIO ORDÓÑEZ
Contralor

Equipo Oficina de Informática

CONTRALORÍA GENERAL DE SANTIAGO DE CALI
Cali, enero de 2023

Tabla de contenido

Contenido

1. INTRODUCCIÓN

La administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades a través de una política de administración de riesgos minimizar pérdidas y maximizar oportunidades.

Con el Plan de Tratamiento de Riesgos se busca mitigar los riesgos identificados en el análisis de riesgos (Perdida de la Confidencialidad, Integridad y Disponibilidad de los activos de información) evitando aquellas situaciones que impidan el logro de los objetivos de la entidad.

Este plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, de tal forma que se definen y aplican los controles con los cuales se busca mitigar la materialización de los riesgos de seguridad y privacidad de la información y seguridad digital en la entidad.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones de control que se deben tomar para mitigar los riesgos identificados, estas acciones son organizadas en forma de controles o medidas de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad, la CGSC define medidas que serán aplicadas en el año 2023.

De esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la seguridad y privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad de los activos, Pérdida de Integridad de los activos y Pérdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la Contraloría General de Santiago de Cali.

2. DEFINICIONES

- 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).

- Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- Impacto: son las consecuencias que genera la materialización de un riesgo.

- Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el 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.

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

3. OBJETIVOS

Objetivo general:

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación a los que la Contraloría General de Santiago de Cali pueda estar expuesta y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Objetivos específicos:

- 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 conocimiento referente a la gestión de riesgos seguridad y privacidad de la información, seguridad digital y continuidad de la operación.
- Tomar decisiones y adoptar medidas para la mejora continua sobre seguridad digital, mediante la definición de indicadores que permitan medir el grado de implementación de los controles.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

4. ALCANCE

Realizar una eficiente gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos institucionales. Teniendo en cuenta la Metodología para administración del riesgo de gestión, corrupción, seguridad digital y de la información Versión 6 adoptada por la entidad y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 5 de la función pública, se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la CGSC. El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por la función pública, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. MARCO NORMATIVO

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril 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.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- La guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5 emitida por el DAFP.

6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del riesgo, a su vez transmite la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad. Estas se fundamentan en las medidas de respuesta que se derivan de las diferentes zonas de riesgo identificadas en la matriz de riesgo.

Las Políticas de Administración de Riesgos de la entidad se encuentran inmersas en la Metodología para la Administración del Riesgo de Gestión, Corrupción, Seguridad Digital y de la información Código MET-P2-156 Versión 6, de acuerdo con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 5 de la función Pública.

Con la entrada en vigencia del decreto 1499 de 2017 del Modelo Integrado de Planeación y Gestión (MIPG), que integra los Sistemas de Gestión de la Calidad y de Desarrollo Administrativo, crea un único Sistema de Gestión y, lo articula con el Sistema de Control Interno, el cual se actualiza y alinea con los mejores estándares internacionales como son el Modelo COSO 2013, COSO ERM 2017 y el Modelo de las Tres Líneas de Defensa, con el fin de entregar a los ciudadanos, lo mejor de la gestión para producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción.

La política de administración de riesgo establece las guías de acción necesarias a los funcionarios de la Contraloría General de Santiago de Cali, para coordinar y administrar los eventos que pueden inhibir el logro de los objetivos de la entidad, capacitándolos y habilitándolos para ello.

Identifica las opciones para tratar y manejar los riesgos que basadas en la valoración, permiten tomar decisiones adecuadas acerca de si se acepta, se elimina, se evita, se reduce, se comparte un riesgo o se transfiere legalmente el impacto. Trasmiten la posición de la dirección respecto al manejo de los riesgos y fijan lineamientos sobre los conceptos de calificación de riesgos, las prioridades en la respuesta, la forma de administrarlos y la protección de los recursos.

Apetito del riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Aceptar un riesgo, significa asumirlo, porque su frecuencia es muy baja y no representa ningún peligro para la entidad.

Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la frecuencia (medidas de prevención), como el impacto (medidas de protección).

Compartir el riesgo, reduce su efecto a través de la transferencia de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

Evitar o Eliminar el riesgo, cuando su frecuencia y gravedad son altas.

Cabe señalar que, para los riesgos de corrupción, las acciones que debe tener en cuenta la alta dirección para su administración son:

Evitar o Eliminar el riesgo: “Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas”.

Reducir el riesgo: Implica tomar las medidas encaminadas a disminuir la probabilidad (medidas de prevención). “La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles”.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: La implementación de las políticas de administración de riesgos que se presentan en este documento.

7. METODOLOGÍA

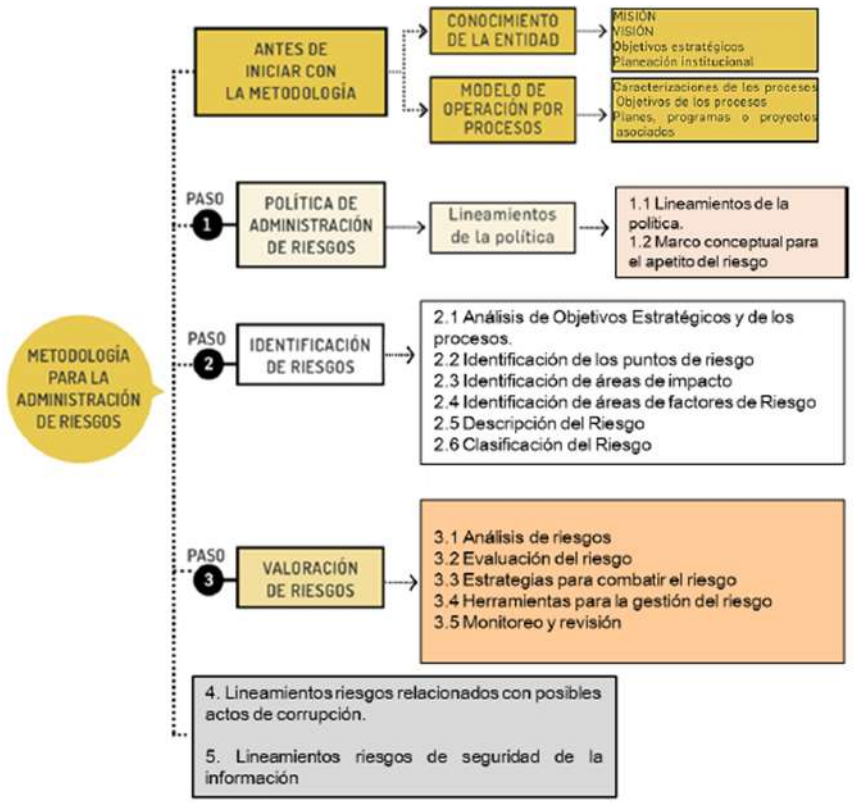
La Contraloría General de Santiago de Cali plantea y adopta la metodología para la Administración del Riesgo de Gestión, Corrupción, Seguridad Digital y de la información CÓDIGO MET-P2-156 Versión 6, tomando como referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 5, lo cual conduce no solo a una gestión pública más eficiente, sino también servirá para que se cumpla con los objetivos corporativos.

7.1 DESARROLLO METODÓLOGICO

La metodología para la Administración del Riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el conocimiento de esta desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada.

A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Metodología para la Administración del Riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

7.2 OPORTUNIDAD DE MEJORA

El análisis de los riesgos debe ser la base para la identificación de nuevas oportunidades de mejora en cada uno de los procesos de la Entidad, lo cual es una consecuencia positiva producto del resultado del tratamiento del riesgo.

8. RECURSOS

Este plan se lleva a cabo con recursos propios: humanos, físicos, tecnológicos y financieros; con énfasis en aplicación de controles y acciones para gestionar los riesgos, el seguimiento y control de la gestión, así como la implementación de las acciones de control definidas en este plan están bajo la responsabilidad del dueño del riesgo.

9. PRESUPUESTO

El dueño del riesgo es el responsable de la estimación del presupuesto para el plan de tratamiento de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, identificados en cada uno de los procesos de la entidad, corresponderá a la Contraloría General de Santiago de Cali la asignación del mismo.

10. MEDICIÓN

La medición se realizará mediante un indicador de gestión que está orientado principalmente a determinar el grado de implementación de los controles definidos en el plan de tratamiento de los riesgos de seguridad y privacidad de la información y seguridad digital que permitirá tomar decisiones y adoptar medidas para la mejora continua sobre la seguridad de la información.

11. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de Abril 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.

- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- La guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5 emitida por el DAFP.

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

- Plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el Ministerio de Tecnologías de la Información y la Comunicaciones.

- Decreto 338/2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

	Nombre	Cargo	Firma
Proyectó	Noralba Hoyos Ruiz	Profesional Universitario Secretaria	
Revisó	Equipo Informática	Oficina de Informática	
Aprobó	Comité Directivo	Comité Directivo	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			