



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 1 de 81	

Manual para la Administración del Riesgo



ELABORADO POR:	REVISADO POR:	APROBADO POR:
 Luz Andrea Álvarez Botero Profesional Especializada Calidad	 Diana Carolina Herrera Castaño Subgerente de Planeación	 Fernando José Da Pena Montenegro Gerente
Fecha: 8-Sep/2023	Fecha: 13-09-2023	Fecha: 15-09-2023



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 2 de 81	

TABLA DE CONTENIDO

1. INTRODUCCIÓN	5
2. OBJETIVOS	7
2.1. OBJETIVO GENERAL	7
2.2. OBJETIVOS ESPECÍFICOS.....	7
3. MARCO LEGAL	8
4. DEFINICIÓN DE TÉRMINOS.....	12
5. CONTEXTO ESTRATÉGICO.....	18
5.1. VISIÓN.....	18
5.2. MISIÓN.....	18
5.3. OBJETIVOS ESTRATÉGICOS.....	18
5.4. MAPA DE PROCESOS	20
6. METODOLOGÍA.....	21
6.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	21
6.2. IDENTIFICACIÓN DE RIESGOS.....	22
6.2.1. Descripción de riesgos	23
6.2.2. Clasificación de riesgos.....	25



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 3 de 81	

6.3. VALORACIÓN DE RIESGOS	26
6.3.1. Análisis de los riesgos.....	26
6.3.2. Evaluación de los riesgos.....	28
6.4. VALORACIÓN DE CONTROLES	29
6.4.1. Descripción de controles	30
6.4.2. Atributos de los controles	30
6.4.3. Efectividad de los controles.....	32
6.5. PLAN DE ACCIÓN	36
6.6. SEGUIMIENTO.....	37
7. LINEAMIENTOS RIESGOS FISCALES	39
7.1. DEFINICIÓN DE RIESGO FISCAL	39
7.2. IDENTIFICACIÓN DEL RIESGO FISCAL.....	40
7.3. VALORACION DE RIESGO FISCAL Y CONTROLES	47
8. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	48
8.1 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	49
8.2 CLASIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	50
8.3 VALORACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	53
8.4 IDENTIFICACIÓN RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	55
9. TRATAMIENTO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.....	57



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 4 de 81	

10.	LINEAMIENTOS RIESGOS DE CORRUPCIÓN.....	58
10.1	IDENTIFICACIÓN RIESGOS DE CORRUPCIÓN	58
10.3	VALORACIÓN RIESGOS DE CORRUPCIÓN	59
	Análisis de la probabilidad.....	59
	Análisis del impacto.....	60
10.4	TRATAMIENTO RIESGOS DE CORRUPCIÓN	63
	Gestión riesgos de corrupción.....	63
	Gestión riesgos de corrupción.....	64
11.	DIRECTRICES GENERALES.....	65
12.	ROLES Y RESPONSABILIDADES	67
13.	REFERENCIAS BIBLIOGRAFICAS.....	72
14.	ANEXOS.....	73
14.1.	ANEXO 01. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.....	73
14.2.	ANEXO 02. MATRIZ DE RIESGOS DE GESTIÓN.....	74
15.	CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS.....	75
15.1.	ANEXO 03. MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	80
15.2.	ANEXO 04. MATRIZ DE RIESGOS DE CORRUPCIÓN	81



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 5 de 81	

1. INTRODUCCIÓN

Teniendo en cuenta que con la expedición del 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”, se crea un solo Sistema de Gestión a través del Modelo Integrado de Planeación y Gestión MIPG, el cual se alinea con el Sistema de Control Interno y el Modelo Estándar de Control Interno MECI.

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos, el MIPG opera a través de 7 dimensiones que agrupan las políticas de gestión y desempeño institucional, por lo que permite identificar claramente las metas y necesidades que deben atender o satisfacer y definiendo los posibles riesgos asociados al cumplimiento de las mismas. En este sentido, la identificación y valoración de riesgos se integra en el desarrollo de los objetivos y la formulación de la estrategia de la entidad.

La administración del riesgo para las entidades públicas en todos sus órdenes cobra hoy mayor importancia, dado el dinamismo y los constantes cambios que el mundo globalizado exige. Estos cambios hacen que dichas entidades deban enfrentarse a



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 6 de 81	

factores internos y externos que pueden generar incertidumbre sobre el logro de sus objetivos.

En el proceso de fortalecimiento del Sistema del Control interno y de acuerdo con MIPG y teniendo en cuenta que el proceso de administración del riesgo es un esfuerzo conjunto entre la Alta Dirección y los servidores en todos sus niveles, SERVICIUDAD E.S.P., ha desarrollado la Administración del Riesgo, y para ello se actualizó el presente Manual donde se explica la metodología empleada en la elaboración de este instrumento de prevención en el desarrollo de una cultura de autocontrol y gestión institucional.

Ejercicio que inicia con la formulación de la política de Administración del Riesgo, la cual incluye los niveles de responsabilidad frente al seguimiento y evaluación de los riesgos y el impacto que estos puedan generar.

Por lo tanto, esta metodología, pretende establecer mecanismos para identificar, valorar y minimizar los riesgos a que constantemente están expuesta la empresa, fortaleciendo así el Sistema de Control, MIPG promueve el mejoramiento continuo de las entidades, razón por la cual éstas deben establecer acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación de éste.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 7 de 81	

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Identificar y establecer los elementos y el marco general de actuación para la gestión integral de los riesgos de toda naturaleza a los que se enfrenta la empresa, así como definir y evaluar los controles que permitan mitigar los riesgos que afecten el cumplimiento de los objetivos institucionales.

2.2. OBJETIVOS ESPECÍFICOS

1. Establecer un modelo de gestión de riesgo que sea conforme con la normatividad y los estándares nacionales e internacionales, teniendo en cuenta los recursos y las necesidades de cada proceso.
2. Diseñar una herramienta para el despliegue del modelo de gestión de riesgos propuesto que incluya los riesgos de gestión, de corrupción y seguridad de la información.
3. Articular del modelo de la gestión del riesgo con el Modelo Integrado de Planeación y Gestión (MIPG).



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 8 de 81	

3. MARCO LEGAL

Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan.

Artículo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 489 de 1998: Estatuto básico de Organización y funcionamiento de la administración pública.

Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Decreto 2145 de 1999: Por el cual se dictan normas sobre el Sistema Nacional de Control interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y territorial y se dictan otras disposiciones. Modificado parcialmente por el Decreto 2593 del 2000



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 9 de 81	

Directiva Presidencial 09 de 1999: lineamientos para la implementación de la política de lucha contra la corrupción.

Decreto 4485 de 2009: Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4,1 Requisitos generales literal g) "establece controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder".

NTC ISO 90011:2015: Numeral A.4 Enfoque basado en Riesgos

Decreto 2593 del 2000: Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.

Decreto 1537 de 2001: Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (...) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (...) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (...) que se enmarca en cinco tópicos (...) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 10 de 81	

entidades públicas (...).

Decreto 1599 de 2005: Por el cual se adopta el Modelo Estándar de Control Interno para el Estado colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.

Decreto 943 de 2014: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI). Decreto 4485 de 2009 Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos generales literal g) “establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad; cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder”. Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.

Decreto 4637 de 2011: Crea la Secretaría de Transparencia en el Departamento Administrativo de la Presidencia de la República, quien establece lineamientos para la prevención de la corrupción.

Decreto 1649 de 2014: Funciones de la Secretaría de Transparencia: 13) Señalar la metodología para diseñar y hacer seguimiento a las estrategias de lucha contra la corrupción y de atención al ciudadano que deberán elaborar anualmente las entidades



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 11 de 81	

del orden nacional y territorial.

Decreto 1081 de 2015: Señala como metodología para elaborar la estrategia de lucha contra la corrupción la contenida en el documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.”

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.

Norma Técnica Colombia NTC-ISO 31000: gestión del riesgo, principios y directrices.

Guía para la administración del riesgo y el diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital, Versión 4: la cual tiene como objetivo unificar los lineamientos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5: en la que se actualizan y precisan algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo. Es



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 12 de 81	

importante resaltar que se mantiene la estructura general bajo tres pasos principales, los cuales fundamentan la estructura metodológica que desde las primeras versiones de la guía se ha venido desarrollado.

Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6: En el que se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal, que se complementa con el Anexo denominado catalogo indicativo de puntos de riesgo fiscal para facilitar el análisis en el marco del modelo de operación por procesos.

4. DEFINICIÓN DE TÉRMINOS

Administración de riesgos: Rama de la administración que aborda las consecuencias del riesgo. Consta de dos etapas: El diagnóstico o valoración, mediante identificación, análisis y determinación del Nivel, y El manejo o la administración propiamente dicha, en que se elabora, ejecuta y hace seguimiento al Plan de manejo que contiene las Técnicas de Administración del Riesgo propuestas por el grupo de trabajo, evaluadas y aceptadas por la alta dirección.

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

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 13 de 81	

por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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).

Riesgo de Corrupción: Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 14 de 81	

probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

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. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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 se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 15 de 81	

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Control: Medida que permite reducir o mitigar un riesgo.

Mapas de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.

Riesgo fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 16 de 81	

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales”. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)”. A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 17 de 81	

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 18 de 81	

5. CONTEXTO ESTRATÉGICO

5.1. VISIÓN

En el año 2026 Serviciudad será reconocida a nivel nacional por la prestación eficiente y sostenible de los servicios públicos, garantizando la autonomía hídrica y el fortalecimiento de la gestión del servicio de aseo.

5.2. MISIÓN

Prestamos servicios públicos domiciliarios de acueducto, alcantarillado y aseo con eficiencia, calidad y continuidad, mejorando la calidad de vida de nuestros usuarios.

5.3. OBJETIVOS ESTRATÉGICOS

1. Garantizar la sostenibilidad financiera.
2. Fomentar la innovación y creación de nuevas unidades de negocio.
3. Definir un plan de fortalecimiento del servicio de aseo.
4. Definir un plan de financiamiento para garantizar la liquidez financiera en el tiempo.
5. Planear y desarrollar innovaciones e iniciativas de acueducto, alcantarillado y aseo con viabilidad técnica y financiera.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 19 de 81	

6. Optimizar la operación y mantenimiento de la infraestructura existente.
6. Lograr un nivel económicamente eficiente de pérdida de agua.
8. Optimizar la gestión comercial.
9. Ampliar la cobertura, brindando soluciones a los acueductos comunitarios.
10. Prestar servicios continuos y de calidad.
11. Mejorar la satisfacción de los usuarios.
12. Fortalecer la seguridad hídrica.
13. Garantizar la disposición segura de los vertimientos.
14. Fomentar el desarrollo e innovación tecnológica.
15. Garantizar la implementación de tecnologías de información de la organización y la prestación adecuada de los servicios en cuanto a disponibilidad y seguridad.
16. Implementar la gestión estratégica del talento humano.
17. Fortalecer las competencias y el sentido de pertenencia al interior de la empresa.
18. Fortalecer el Gobierno corporativo.

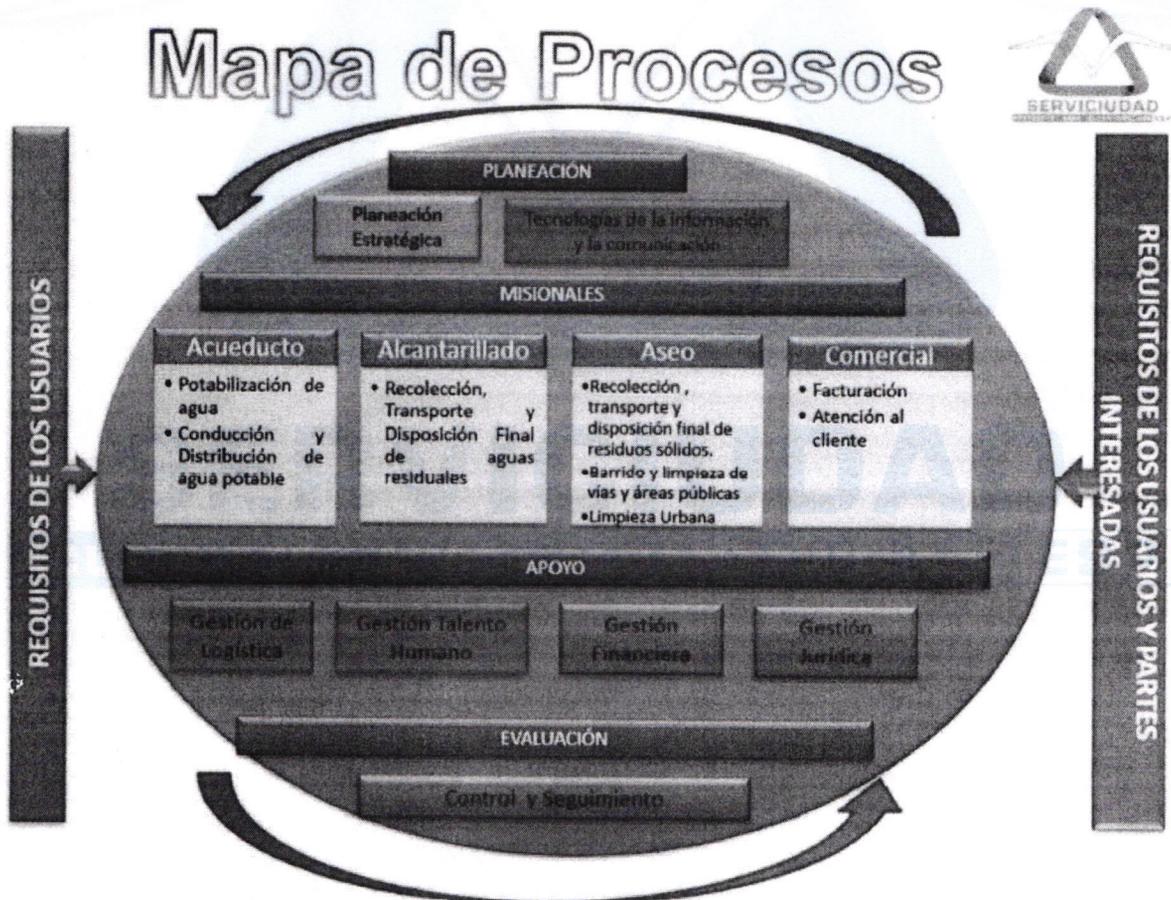


SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 20 de 81	

19. Promover la cultura ciudadana respecto a los servicios.

20. Incrementar la satisfacción de los grupos de interés.

5.4. MAPA DE PROCESOS





SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 21 de 81	

6. METODOLOGÍA

La metodología establecida para la gestión de riesgos de Serviciudad E.S.P está basada en la guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, emitida en noviembre de 2022 por el Departamento Administrativo de la Función Pública –DAFP.

Antes de iniciar con la metodología y una vez determinados los lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos, planeación institucional, entre otros aspectos, lo anterior para conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

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.

6.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Es la declaración de la dirección y las intenciones generales de una organización con



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 22 de 81	

respecto a la gestión del riesgo, esta establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

La política debe contener los objetivos estratégicos de la entidad, se deben identificar los niveles de responsabilidad frente al manejo de riesgos, y los mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad.

Los lineamientos para la política de administración del riesgo son establecidos por la alta dirección, liderado por el representante legal y con participación del Comité Institucional de Coordinación de Control Interno.

Estos lineamientos se deben tener en cuenta desde el ejercicio del direccionamiento estratégico y de planeación, ya que es allí donde se debe contemplar el tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales.

6.2. IDENTIFICACIÓN DE RIESGOS

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden afectar el cumplimiento de los objetivos.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 23 de 81	

- Analizar los objetivos estratégicos y de los procesos.
- Identificar los puntos de riesgo dentro del flujo de los procesos.
- Identificar las áreas de impacto, ya sea que traiga consecuencia económica o reputacional.
- Identificar las áreas de factores de riesgo.

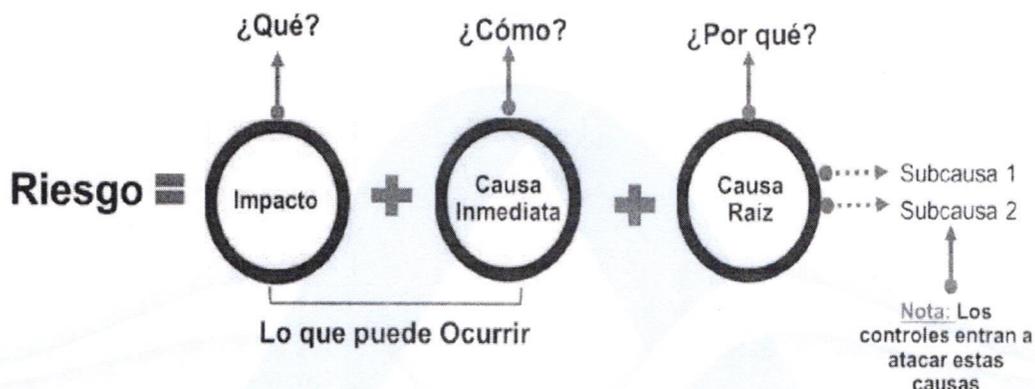
Identificación del riesgo					
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo

6.2.1. Descripción de riesgos

Es la redacción que permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz. Esta descripción debe ser detallada y que sea de fácil entendimiento tanto para el líder del proceso como para personas ajenas al proceso. La siguiente estructura propuesta por la guía facilita la redacción y claridad:



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 24 de 81	



Recordando los conceptos de la estructura tenemos:

Impacto: son las consecuencias que puede ocasionar a la organización la materialización del riesgo, estas pueden ser afectaciones económicas o reputacionales, o ambas.

Causa inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo, es la situación más evidente frente al riesgo, redacte de la forma más concreta posible. (Responde al "Cómo").

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas, se deben redactar de la



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 25 de 81	

forma más concreta posible. (Responde al "Por Qué").

6.2.2. Clasificación de riesgos

Esta clasificación permite agrupar los riesgos de acuerdo a una serie de factores generadores, por lo tanto se clasifica cada uno de los riesgos en las siguientes categorías:

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Fraude externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude interno: Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 26 de 81	

de discriminación.

Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos fijos/ eventos externos: Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

6.3. VALORACIÓN DE RIESGOS

Busca establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, que permita estimar la zona de riesgo inicial o inherente, así mismo, confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final o residual.

6.3.1. Análisis de los riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 27 de 81	

Análisis del riesgo inherente				
Frecuencia con la cual se realiza la actividad	Probabilidad Inherente %	Criterios de impacto	Impacto Inherente %	Zona de Riesgo Inherente

Paso 1. Determinar la probabilidad:

Es la posibilidad de ocurrencia del riesgo, la cual está asociada a la exposición al riesgo que tenga el proceso o actividad que se esté realizando, por lo que se basa en el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

A continuación se establecen los criterios que definen el nivel de probabilidad:

Tabla 4 Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 28 de 81	

Paso 2. Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

6.3.2. Evaluación de los riesgos

La evaluación del riesgo se realiza a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial o inherente.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 29 de 81	

Se realiza un análisis del riesgo inherente, mediante el cual se determina el nivel de severidad con base en la combinación entre la probabilidad y el impacto. Cruzando los datos se obtiene la zona de riesgo representada en la matriz de calor:

		Impacto				
		Leve	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Muy Alta	Alto	Alto	Alto	Alto	Extremo
	Alta	Moderado	Moderado	Alto	Alto	Extremo
	Media	Moderado	Moderado	Moderado	Alto	Extremo
	Baja	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja	Bajo	Bajo	Moderado	Alto	Extremo

6.4. VALORACIÓN DE CONTROLES

Se establecen las medidas que permiten reducir o mitigar el riesgo, para esto se detallan los controles establecidos en los procesos para cada riesgo identificado, al igual que los atributos que lo caracterizan.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 30 de 81	

No. Control	Descripción del Control		Afectación	Atributos					
	Responsable	Acción		Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia

6.4.1. Descripción de controles

Los controles deben ser claros para lo cual se tiene en cuenta la siguiente estructura que facilita la descripción del control:

Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

6.4.2. Atributos de los controles

Se analiza la efectividad de los controles a partir de las características relacionadas con la eficiencia y la formalización, teniendo en cuenta el análisis de los atributos para de cada control.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 31 de 81	

Atributo 1. Tipología:

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Atributo 2. Implementación:

Control manual: controles que son ejecutados por personas.

Control automático: son ejecutados por un sistema.

Atributo 3. Documentación

Atributo 4. Frecuencia:

Continua: El control se aplica siempre que se realiza la actividad que conlleva el riesgo.

Aleatoria: El control se aplica aleatoriamente a la actividad que conlleva el riesgo.



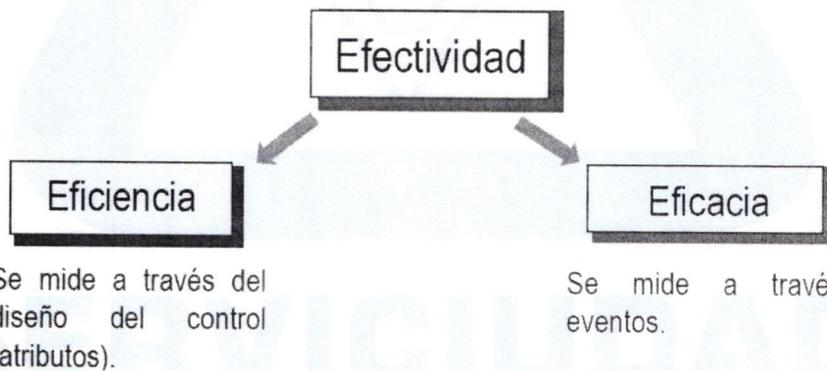
SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 32 de 81	

Atributo 5: Evidencia

Con registro: El control deja un registro permite evidencia la ejecución del control.

Sin registro: El control no deja registro de la ejecución del control.

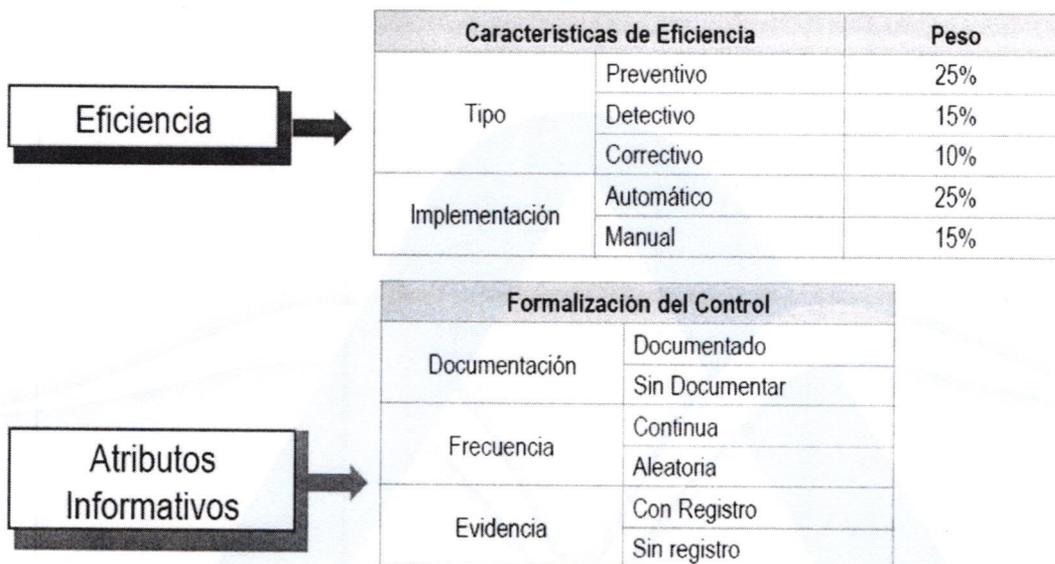
6.4.3. Efectividad de los controles



La eficiencia de los controles se mide con base en la tipificación y la implementación de los mismos, establecido por la suma del peso de cada atributo que corresponda



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 33 de 81	

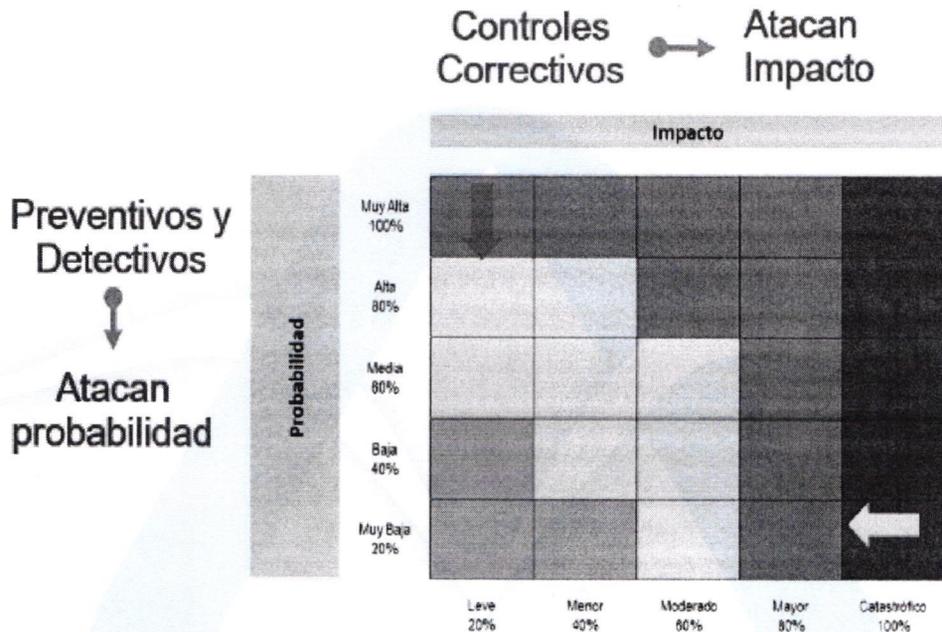


Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 34 de 81	



El resultado de aplicar la efectividad de los controles al riesgo inherente se llama riesgo residual. El cálculo matemático establecido para conocer el valor del riesgo residual es:

$$\text{Nivel Riesgo Residual} = \% \text{ Riesgo Inherente} - (\% \text{ Riesgo Inherente} * \% \text{ Control})$$

Se debe tener en cuenta que el riesgo inherente tiene dos valores por separado uno para la probabilidad y otro para el impacto, por lo tanto, se debe establecer el nivel el nivel de riesgo residual para cada uno.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 35 de 81	

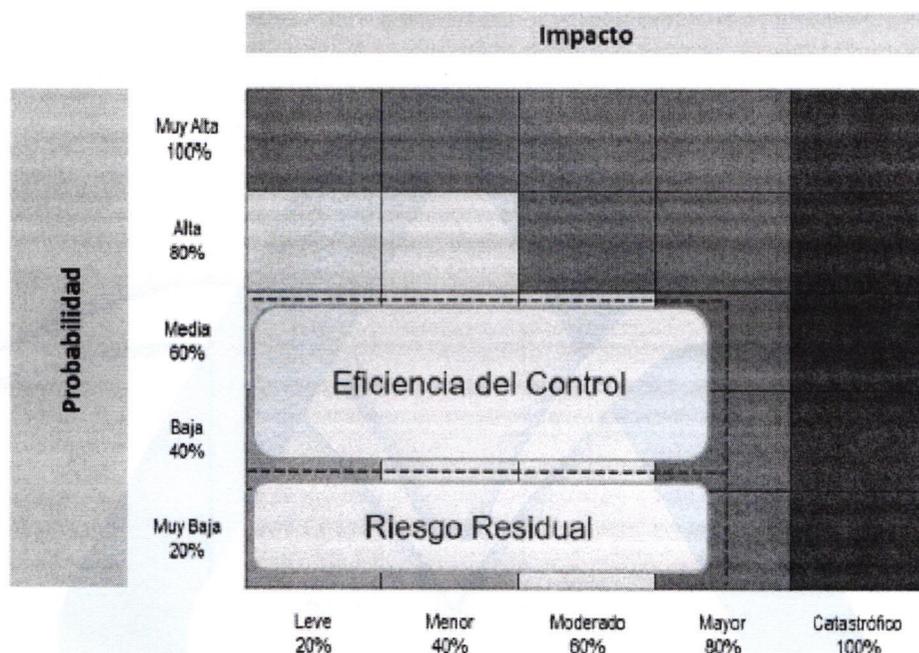
Evaluación del riesgo - Nivel del riesgo residual			
Probabilidad Residual Final	%	Impacto Residual Final	%
Zona de Riesgo Final			

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, afectando la probabilidad o el impacto según corresponda.

Dependiendo del nivel de severidad en que se ubique el riesgo residual, la empresa podrá priorizar la atención de los mismos, así como definir su tratamiento y las acciones a seguir.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 36 de 81	



6.5. PLAN DE ACCIÓN

Se establece la estrategia para combatir el riesgo, decisión que se toma frente a un determinado nivel de riesgo, la cual puede ser aceptarlo, reducirlo o evitarlo.

Aceptar: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Evitar: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina no asumir la actividad que genera este riesgo.

Reducir: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 37 de 81	

determina tratarlo mediante transferencia o mitigación del mismo.

Transferir: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas.

Mitigar: Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo.

Cuando la decisión es reducir, se requiere definir un Plan de Acción, el cual es una herramienta de planificación empleada para la gestión y control de tareas o proyectos, no necesariamente es un control adicional.

Se requiere establecer:

- Responsable
- Fecha de implementación
- Fecha de Seguimiento

6.6. SEGUIMIENTO

Una vez identificados los riesgos, establecidos los controles y el plan de acción que se requiera, se debe llevar un seguimiento a los eventos que se presenten, se pueden considerar incidentes que generan o podrían generar pérdidas (económica o



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 38 de 81	

reputacional) a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué falla pudieron tener los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Para identificar si los controles fueron efectivos, se debe evaluar su desempeño:

Desempeño del control = # eventos / frecuencia del riesgo

Recordando que la frecuencia es el # veces que se realiza la actividad.

Es necesario que el responsable del proceso monitoree continuamente los riesgos y las medidas de control, así como la eficacia de las acciones tomadas, lo anterior dado que estos necesitan ser revisados constantemente para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos o la aparición de nuevos riesgos.

En el seguimiento de cada riesgo deben quedar descritas de la forma más clara las evidencias de las acciones que se emplearon para dar tratamiento al riesgo con su respectiva fecha de aplicación.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 39 de 81	

7. LINEAMIENTOS RIESGOS FISCALES

El control fiscal además de posterior y selectivo a través de las auditorías (control micro), es preventivo y concomitante, buscando con ello el control permanente al recurso público, para lo cual, una de las herramientas previstas es la articulación con el sistema de control interno.

La metodología que se propone es de gran utilidad para gestionar de manera efectiva los recursos, bienes e intereses públicos, previniendo efectos dañosos, lo cual a la vez permite, mitigar la posibilidad de configuración de responsabilidades fiscales para los diferentes gestores públicos.

7.1. DEFINICIÓN DE RIESO FISCAL

Riesgo Fiscal es el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 40 de 81	

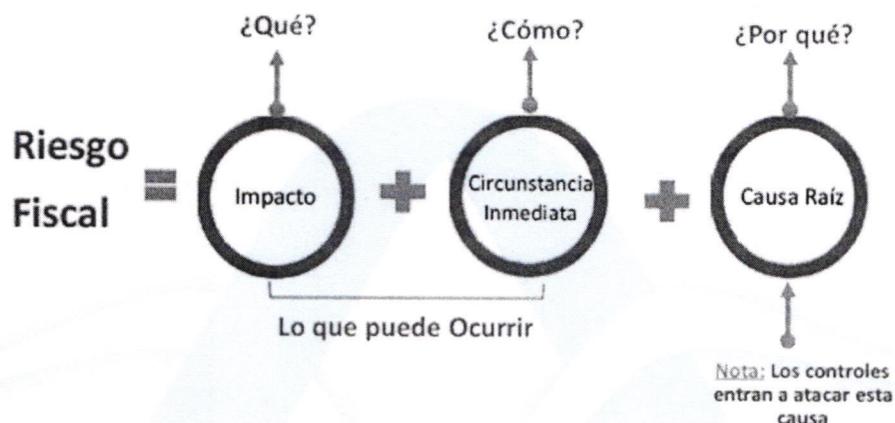
públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

7.2. IDENTIFICACIÓN DEL RIESGO FISCAL

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Es decir, las situaciones en las que potencialmente se genera riesgo fiscal, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas. Se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

La estructura propuesta para la redacción de riesgos fiscales es la siguiente:

SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 41 de 81	



Para redactar un riesgo fiscal se debe tener en cuenta:

- **Iniciar con la oración:** Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
- **Impacto:** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- **Circunstancia inmediata:** Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica - causa raíz- para que se presente el riesgo.
- **Causa Raíz:** Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 42 de 81	

- **IMPACTO:**

El área de impacto para los riesgos fiscales siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública.

- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.

Ejemplos: Las calles, plazas, puentes, vías, parques etc.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 43 de 81	

públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

- **Recurso público:** Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 44 de 81	

pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

- CIRCUNSTANCIAS INMEDIATAS

Se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica -causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Ahora bien, para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 45 de 81	

la causa principal del riesgo fiscal).

Para este taller, puede usar las siguientes preguntas orientadoras:

1. ¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
2. Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.

Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.

Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.

Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 46 de 81	

conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado.

Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.

3. En un ejercicio autocrítico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?

Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.

4. ¿Qué puntos de riesgo fiscal y circunstancias inmediatas del “¿Catálogo Indicativo



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 47 de 81	

y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” son aplicables a la entidad? Ver Anexo.

- CAUSA RAIZ

Es cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro. La determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. Debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto-.

7.3. VALORACION DE RIESGO FISCAL Y CONTROLES

Para realizar la evolución de los riesgos fiscales, la determinación del riesgo inherente y la valoración de los controles correspondientes se debe seguir la metodología anteriormente definida en el Capítulo 6.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 48 de 81	

8. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

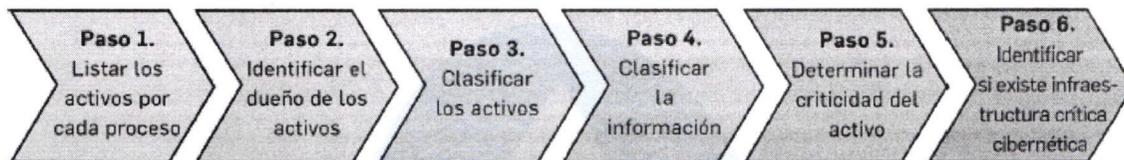
La política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI). El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 49 de 81	

¿CÓMO IDENTIFICAR LOS ACTIVOS?:



8.1 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso, de esta forma se determina qué es lo más importante que posee la entidad y sus procesos. Algunos de los activos pueden ser:

-Aplicaciones de la organización

-Servicios web

-Redes

-Información física o digital

-Tecnologías de información TI

-Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 50 de 81	

En cada proceso, deberán listarse los activos, indicando para cada uno un consecutivo, nombre y descripción breve, deberá tener un dueño designado y demás características que permitan su identificación.

Identificación del activo											
Referencia	Proceso	Activo	Descripción	Idioma	Ubicación	Medio de Conservación/ Soporte	Fecha Generación de la Información	Formato	Propietario	Custodio	Usuario

8.2 CLASIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza:

Información: Corresponden a este tipo datos e información almacenada o procesada electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

Hardware: Se consideran los medios materiales físicos destinados a soportar directa o



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 51 de 81	

indirectamente los servicios que presta la Entidad.

Software: Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la Entidad y la prestación de los servicios.

Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

Recurso Humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información

Instalaciones: Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones.

Infraestructura crítica cibernética nacional: se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 52 de 81	

Clasificación del activo		
Tipo de Activo	Ley 1712 de 2014	Ley 1581 de 2012

De igual manera se debe clasificar la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 5.

LEY 1712 DE 2014: Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.

LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014	INFORMACIÓN PÚBLICA RESERVADA	INFORMACIÓN PÚBLICA CLASIFICADA	INFORMACIÓN PÚBLICA	NO CLASIFICADA
---------------------	-------------------------------------	---------------------------------------	------------------------	-------------------



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 53 de 81	

Ley 1581 de 2012	CONTIENE DATOS PERSONALES	NO CONTIENE DATOS PERSONALES	NA
---------------------	------------------------------	------------------------------------	----

8.3 VALORACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso.

	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
TIPO	DESCRIPCIÓN	DESCRIPCIÓN	DESCRIPCIÓN
ALTA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 54 de 81	

MEDIA	<p>Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.</p>	<p>Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.</p>	<p>La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.</p>
BAJA	<p>Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.</p>	<p>Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.</p>	<p>La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.</p>
NO CLASIFICADA	<p>Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.</p>	<p>Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.</p>	<p>Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.</p>



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 55 de 81	

8.4 IDENTIFICACIÓN RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben identificar los activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres riesgos mencionados:

AMENAZAS	
TIPO	DESCRIPCIÓN
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministros de agua
	Fallas en el sistema de suministros de energía
	Fallas en el sistema de suministros de aire acondicionado
	Fallas en el sistema de suministros de internet



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 56 de 81	

Perturbación debida a la radiación	Radiación Electromagnética
	Radiación térmica
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
	Hurto de información
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

VULNERABILIDADES	
TIPO	DESCRIPCIÓN
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura, polvo o suciedad
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 57 de 81	

	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
	Programación obsoleta
	Seguridad desactualizada
	Software sin soporte
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general

9. TRATAMIENTO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Una vez se han identificados los riesgos de los activos de información, se procede a su valoración del riesgo, analizando la probabilidad y el impacto que pueda generar la materialización de dicho riesgo. De igual manera se deben establecer los controles y su



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 58 de 81	

respectiva valoración para detectar el riesgo residual y dar el tratamiento que corresponda.

Este tratamiento de los riesgos de seguridad de la información y los respectivos controles se realiza de acuerdo a lo indicado en los capítulos anteriores del presente documento.

10. LINEAMIENTOS RIESGOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Es de resaltar que la Secretaría de Transparencia, en la actualidad está analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción.

10.1 IDENTIFICACIÓN RIESGOS DE CORRUPCIÓN

Los riesgos de corrupción se establecen sobre los procesos, se debe evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, por lo que se debe tener claridad que se encuentran asociados a la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

En la descripción de los riesgos de corrupción se deben concurrir todos los componentes de su definición:

Acción u omisión + uso el poder + desviación de la gestión de lo público + beneficio privado.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 59 de 81	

10.3 VALORACIÓN RIESGOS DE CORRUPCIÓN

Se orienta a determinar la probabilidad de materialización del riesgo y sus consecuencias o su impacto. Para este caso la probabilidad y el impacto están definidos de diferente manera a como se establece en los riesgos de gestión.

Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 60 de 81	

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. A continuación, se detalla la lista de preguntas a tener en cuenta para establecer el impacto:



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 61 de 81	

N.º	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.			10
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

**Nivel de
impacto
MAYOR**

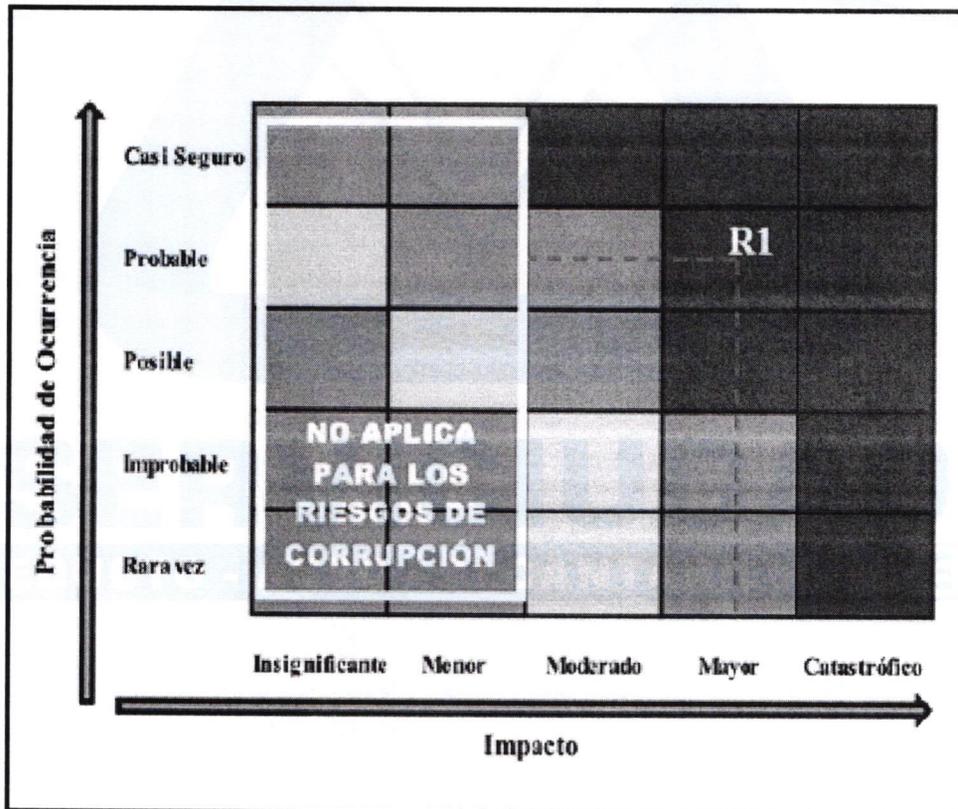
Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 62 de 81	

insignificante y menor.

Por último al ubicar en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto, se establece el nivel del riesgo inherente.





SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 63 de 81	

10.4 TRATAMIENTO RIESGOS DE CORRUPCIÓN

El tratamiento de los riesgos de corrupción solo recae sobre la probabilidad, es decir que no opera desplazamiento para el impacto. Se debe tener claro que en ningún caso, estos riesgos pueden ser aceptados, por tanto solo se pueden evitar o mitigar.

Gestión riesgos de corrupción

Seguimiento: El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver anexo 6. matriz de seguimiento a los riesgos de corrupción)



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 64 de 81	

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Gestión riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- 1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
- 2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- 3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- 4) Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 65 de 81	

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

11. DIRECTRICES GENERALES

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.
- Se requiere llevar una Base Histórica de Eventos.
- Incluir el indicador del desempeño de los controles en los indicadores de gestión de la empresa.
- Identificar los indicadores claves de riesgo, los cuales permiten capturar la ocurrencia



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 66 de 81	

de un incidente que se asocia a un riesgo identificado previamente considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

- Es esencial una revisión sobre la marcha para asegurar que el tratamiento mantiene su relevancia. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de monitoreo y revisión de los riesgos.
- Se debe actualizar periódicamente el inventario de activos de la información para de allí, actualizar los riesgos asociados a la seguridad de la información.
- Los mapas de riesgo deben ser publicados en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. La publicación debe ser parcial y fundamentada en la elaboración del índice de información clasificada y reservada.
- La política de riesgos de gestión, de corrupción y seguridad de la información y los



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 67 de 81	

mapas respectivos, deben ser socializados con los servidores públicos y contratistas de la entidad.

12. ROLES Y RESPONSABILIDADES

El modelo integrado de planeación y gestión (MIPG) desarrolla en la 7ª dimensión (control interno) las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en los diferentes servidores de la entidad:

- LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y supervisa el cumplimiento de los controles, está a cargo de la Alta Dirección y del Comité Institucional de Coordinación de Control Interno.

- 1º LÍNEA DE DEFENSA

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Responsables: Gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.

Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 68 de 81	

implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

Rol principal: diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

Actividades:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso.
- Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 69 de 81	

- Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

- 2° LÍNEA DE DEFENSA

Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

Responsables: servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 70 de 81	

entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

- 3° LÍNEA DE DEFENSA

Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Responsables: oficina de control interno, auditoría interna o quien haga sus veces.

Corresponde a las unidades de control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

Rol principal: proporcionar un aseguramiento basado en el más alto nivel de



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 71 de 81	

independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

Actividades:

- Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 72 de 81	

con los resultados de las auditorías realizadas.

- se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

13. REFERENCIAS BIBLIOGRAFICAS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 6, noviembre de 2022, elaborado por el Departamento Administrativo de la Función Pública.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas, Versión 5, noviembre de 2020, elaborado por el Departamento Administrativo de la Función Pública.
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Versión 1, agosto de 2018, elaborado por la Presidencia de la República.
- Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas. (Anexo 4 – DAFP)
- Guía para la gestión del riesgo de corrupción, 2015 elaborado por elaborado por la Presidencia de la República.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 73 de 81	

14. ANEXOS

14.1. ANEXO 01. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

POLITICA DE ADMINISTRACION DE RIESGOS

SERVICIUDAD E.S.P.

“Serviciudad E.S.P. en cabeza de la Alta Dirección y con el liderazgo del Representante Legal, se compromete a administrar adecuadamente los riesgos de gestión, de corrupción, Seguridad Digital y Fiscales, asociados a los objetivos estratégicos y a los procesos institucionales; a través de la correcta identificación y valoración de riesgos, lo cual permita establecer estrategias para mitigarlos y establecer controles con la participación activa de las diferentes líneas de defensa, con todos los servidores públicos y contratistas, que conlleven al mejoramiento continuo y al logro de la misión y visión de la organización.

La política de administración de riesgos es aplicable a todos los servicios, procesos, proyectos y planes de la entidad durante el desarrollo de su gestión y a todos los servidores públicos en el ejercicio de sus funciones”.



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 75 de 81	

15. CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación <u>por la que</u> se presenta el riesgo</i>
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 76 de 81	

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación <u>por la que</u> se presenta el riesgo</i>
		procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 77 de 81	

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación <u>por la que</u> se presenta el riesgo</i>
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 78 de 81	

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación <u>por la que</u> se presenta el riesgo</i>
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratistas



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 79 de 81	

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación <u>por la que</u> se presenta el riesgo</i>
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a	Pago de subsidios por encima del beneficio otorgado



SERVICIUDAD E.S.P.	Código CIMR-01	Versión 04
Manual Administración de Riesgos	Página 81 de 81	

15.2. ANEXO 04. MATRIZ DE RIESGOS DE CORRUPCIÓN

PROCESO / OBJETIVO	IDENTIFICACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO DE CORRUPCIÓN								Monitoreo y Revisión				
	CAUSA	RIESGO	Análisis del Riesgo			Zona de Riesgo	Valoración del Riesgo					Acciones	Fecha	Acciones Responsable	Indicador
			Riesgo inherente				Riesgo Residual								
			Probabilidad	Impacto	Calificación		Control	Probabilidad	Impacto	Calificación	Zona de Riesgo				
CONTRACTUAL	Concentración de la información en pocas personas/ manipulación y adulteración de la información.	Favorecimiento a terceros	3	4	EXTREMA	E: Zona de riesgo Extrema; Reducir el riesgo; Evitar; Compartir o Transferir	*Reintroducción al código de ética e integridad (Resolución 421 /2019), valores corporativos, manual de interventoría *Fortalecimiento de los procesos de selección y evaluación de proveedores	2	4	ALTA	A: Zona de riesgo Alta; Reducir el riesgo; Evitar; Compartir o Transferir	<ul style="list-style-type: none"> Seguimiento al cumplimiento de lo ordenado en el Manual de contratación. Socialización del código de ética e integridad en procesos de inducción y reintroducción año 2020. Publicación de la contratación año 2020 en página web de Serviciudad ESP y la página WEB de la Alcaldía de Dosquebradas. Reporte de la contratación al SIA Observa Comité evaluador de propuestas para efectos de la contratación. Socialización de manual de interventoría y manual de contratación a los supervisores e interventores de la empresa. Socialización del código de ética e integridad en procesos de inducción y reintroducción año 2020. Elaboración de auditorías al proceso de contratación por parte de la oficina de control interno de gestión. 			
	Falta de ética y transparencia en el manejo de la información por parte de funcionarios públicos	Sollicitud de dádivas o acceso a soborno (Tolerar incumplimientos en los requisitos contractuales establecidos a cambio de beneficios particulares)	3	5	EXTREMA	E: Zona de riesgo Extrema; Reducir el riesgo; Evitar; Compartir o Transferir	*Socialización permanente al código de ética e integridad, valores corporativos, manual de contratación. *Manual de interventoría	1	4	ALTA	A: Zona de riesgo Alta; Reducir el riesgo; Evitar; Compartir o Transferir	<ul style="list-style-type: none"> Socialización de manual de funciones para incorporar la formación del servicio al cliente en los perfiles de cargos. Socialización del código de ética e integridad en procesos de inducción y reintroducción año 2020. Implementación de la evaluación de desempeño. Selección de personal de conductores de vehículos atendiendo los lineamientos del plan de seguridad vial (PESV). Auditoría a los procesos de Talento Humano por parte de la oficina de Control Interno de Gestión. 			
TALENTO HUMANO	Beneficios personales, amiguismo	Tráfico de influencias (coacción sobre servidores públicos)	4	4	EXTREMA	E: Zona de riesgo Extrema; Reducir el riesgo; Evitar; Compartir o Transferir	*Aplicación de código de ética e integridad *Aplicación de procesos de selección de personal	2	4	ALTA	A: Zona de riesgo Alta; Reducir el riesgo; Evitar; Compartir o Transferir	<ul style="list-style-type: none"> Fortalecimiento del proceso de reintroducción al personal de la empresa. Control y monitoreo a los procesos en auditorías de calidad y control interno. Implementación de la evaluación de desempeño. Fortalecimiento de las competencias de personal a través de la ejecución del plan institucional de capacitación 2020 (PIC). 			
	Falta de procedimientos claros y manual de funciones socializado; ausencia de procesos de inducción y reintroducción	Incumplimiento de funciones	3	4	EXTREMA	E: Zona de riesgo Extrema; Reducir el riesgo; Evitar; Compartir o Transferir	*Programación y ejecución de los procesos de inducción y reintroducción al personal *Socialización de manual de funciones *Socialización manual de procedimientos	1	4	ALTA	A: Zona de riesgo Alta; Reducir el riesgo; Evitar; Compartir o Transferir	<ul style="list-style-type: none"> Fortalecimiento del proceso de reintroducción al personal de la empresa. Control y monitoreo a los procesos en auditorías de calidad y control interno. Implementación de la evaluación de desempeño. Fortalecimiento de las competencias de personal a través de la ejecución del plan institucional de capacitación 2020 (PIC). 			