uesvalle
Unidad Ejecutora de Saneamiento del Valle del Cauca

Valle Invencible

GOBERNACIÓN VALLE DEL CAUCA
Secretaría de Salud

Política de Administración de Riesgos

Año 2021

TABLA DE CONTENIDO

INTRODUCCIÓN

La Política de Administración de Riesgos de la Unidad Ejecutora de Saneamiento del Valle del Cauca UESVALLE, establece a los servidores públicos, colaboradores, contratistas y público en general, nuestro compromiso e interés de identificar y controlar los riesgos institucionales que puedan atentar en el cumplimiento de nuestras funciones enmarcadas en el Decreto departamental número 1798 de 2017 y el Plan Estratégico Institucional 2020-2023 “Un compromiso social y responsable por la Salud Ambiental”, dentro del marco normativo.

Dentro del Modelo Integrado de Planeación y Gestión MIPG, elaboramos esta nueva versión con el fin de atender la nueva Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas Versión 5 de diciembre 2020, elaborado por el Departamento Administrativo de la Función Pública, adaptándola de acuerdo con el tamaño y complejidad de las entidades públicas recomendada por la mencionada guía.

1. OBJETIVO

Establecer la Política para la Administración de Riesgos en la Unidad Ejecutora de Saneamiento del Valle del Cauca – UESVALLE.

2. ALCANCE

Esta política incluye los riesgos de gestión, los riesgos de corrupción y los riesgos de seguridad de la información.

Esta política es aplicable a todos los funcionaros públicos y contratistas, que desarrollan sus funciones y actividades respectivamente, a través de los procesos institucionales.

Esta política se alinea con la séptima dimensión del Modelo Integrado de Planeación y Gestión MIPG denominada Control Interno.

Esta política contribuye al control interno de la entidad, y fomenta la cultura del autocontrol hacia el interior de los procesos.

3. NORMAS DE REFERENCIA

El riesgo y su administración están fundamentados principalmente en el siguiente marco normativo:

Norma/ Guía	Descripción
Ley 87 de 1993	Se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
Ley 1474 de 2011	Estatuto Anticorrupción Artículo 73. Plan Anticorrupción y de atención al ciudadano.
Decreto 1083 de 2015	Decreto Único Reglamentario del Sector de Función Pública.
Decreto 1499 de 2017 y Manual Operativo.	Modelo Integrado de Planeación y Gestión para entidades públicas
Guía	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 – Función Publica. Diciembre de 2020

4. GLOSARIO

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.

Administración de Riesgos. Metodología adoptada por la Alta dirección y todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de riesgos se convierta en una parte natural de planeación, de gestión y operación en el día a día.

Alta Dirección. Integrada por las máximas autoridades administrativas de una entidad y quien posee el máximo nivel de responsabilidad. Para las entidades de la rama Ejecutiva, la alta dirección se define en los términos de los Decretos 770 y 785 de 2005.

Amenazas. Causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

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.

Autocontrol. Capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.

Autogestión. Capacidad de toda organización pública para interpretar, coordinar, aplicar y evaluar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada por la Constitución, la ley y sus reglamentos.

Autorregulación. Capacidad de cada una de las organizaciones para desarrollar y aplicar en su interior métodos, normas y procedimientos que permitan el desarrollo, implementación y fortalecimiento continúo del Sistema de Control Interno, en concordancia con la normatividad vigente.

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.

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

Causa Inmediata. Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz. Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

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

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.

Control. Medida que permite reducir o mitigar un riesgo.

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

Factores de Riesgo. Son las fuentes generadoras de riesgos.

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

Integridad. Propiedad de exactitud y completitud.

Mapa de Riesgos. Documento con la información resultante de la gestión del riesgo.

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.

Plan Anticorrupción y de Atención al Ciudadano. Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Política Organizacional o de empresa. Es la orientación o directriz dictada desde más alto nivel de la organización que se compromete a cumplir y que establece una conducta y unidad de criterio a observar, en la toma de decisiones e implementación de las estrategias para el logro de los objetivos propuestos. Debe ser divulgada, entendida y acatada por todos los miembros de la organización y es la base para desarrollar los demás documentos institucionales, como los planes, manuales, procedimientos, entre otros.

Probabilidad. Se entiende la posibilidad de ocurrencia del riesgo. Estará asociad 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.

Riesgo. Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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.

Riesgo de Gestión. Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

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 Inherente. Nivel de riesgo propio de la actividad en ausencia controles. El resultado de combinar la 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.

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. Para el riesgo de corrupción la tolerancia es inaceptable.

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

5. DECLARACION DE LA POLITICA DE ADMINISTRACION DE RIESGOS

Se parte de la idea de reconocer, que existe la posibilidad que en la UESVALLE se presenten riesgos de gestión, de corrupción y en seguridad de la información; los cuales, puedan materializarse y afectar las personas, el patrimonio y la capacidad institucional, generando dificultades para cumplir con las funciones institucionales.

Por lo tanto, nuestro compromiso es administrar los riesgos con enfoque preventivo y proactivo, mediante una herramienta metodológica y estratégica, que permita identificarlos, evaluarlos y tratarlos con acciones mediante la implementación de controles efectivos, para prevenirlos o que se minimice su impacto.

Para avanzar en este proceso, la Dirección General propiciará los mecanismos que garanticen los recursos necesarios, de acuerdo con la disponibilidad presupuestal y la priorización institucional, que permitan la implementación, el seguimiento y evaluación de esta política.

6. LINEAMIENTOS GENERALES

a) **Adopción de la guía.** Para la administración del Riesgo en la entidad se tendrá en cuenta la Guía para la Administración del Riesgo y el Diseño de controles en Entidades Públicas. Versión 5 de diciembre de 2020 elaborado por el departamento administrativo de la Función Pública, adoptándose conforme al tamaño y complejidad institucional, así mismo, se adoptarán los instrumentos que sean necesarios para fortalecer el control de los riesgos.

b) **Alineación.** La Administración de los riesgos de la entidad, se alineara conforme a las funciones establecidas (Estatutos), el Plan Estratégico vigente y la normatividad que le aplique.

c) **Modelo de operación por procesos.** Se alcanzan resultados coherentes y previsibles de manera más eficaz y eficiente, cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente.

d) **Pensamiento basado en riesgos para el desarrollo de la planeación, el control, la evaluación y la mejora.** Toda actividad tiene riesgo de que su resultado previsto no se cumpla, por tanto, se debe prevenir o reducir efectos no deseados de manera proactiva y preventiva.

e) **El compromiso con la gestión de riesgos es de todos.** Las personas competentes, empoderadas y comprometidas en toda la organización, son esenciales para aumentar la capacidad de la Entidad de generar y proporcionar valor.

f) **Gestión con Gradualidad.** La gestión institucional se realiza conforme a la capacidad institucional, con la priorización razonable del uso de los recursos disponibles.

g) **Principios del Modelo Estándar de Control Interno.** Para la Administración de riesgos, se atenderá los principios de Autocontrol, Autorregulación y Autogestión.

h) **Coherencia estratégica y operativa.** Los objetivos de cada proceso deben estar alineados con los diferentes planes de la entidad, como el Plan Estratégico, Plan Operativo Anual y demás planes normativos. Se debe asegurar que el objetivo del proceso contribuya a los objetivos estratégicos.

7. CONTEXTO

En la identificación de los riesgos se debe analizar el contexto que pueda afectar el cumplimiento de las funciones institucionales realizado en actividades a través de los procesos establecidos. Se debe tener en cuenta el contexto tanto interno como externo así:

a) **Contexto Externo de la Entidad:**

1. Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.
2. Económicos: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
3. Sociales: Demografía, responsabilidad social, orden público.
4. Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
5. Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
6. Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

b) **Contexto Interno de la Entidad:**

1. Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
2. Personal: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
3. Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
4. Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
5. Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
6. Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

c) Contexto del proceso institucional:

1. Diseño del Proceso: Claridad en la descripción del alcance y objetivo del proceso.
2. Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

3. Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
4. Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.
5. Responsables del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
6. Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

La entidad debe tener en cuenta la matriz DOFA general (Debilidades, Oportunidades, Fortalezas y Amenazas), contenida en el plan estratégico institucional.

8. LÍNEAS DE DEFENSA, RESPONSABLES Y RESPONSABILIDADES

Las líneas de Defensa y responsabilidades de la Administración del Riesgo de la Entidad, tendrá como referencia a lo establecido en la séptima dimensión Control Interno del Modelo Integrado de Planeación y Gestión MIPG, así:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD
Estratégica	Representante Legal y Comité Institucional de Coordinación de Control Interno	1. Definir la Política de Administración de Riesgos y hacerlo aprobar por el Representante Legal, y supervisar su cumplimiento. 2. Analizar los riesgos y eventos críticos y emitir directrices y mejora de los controles.
Primera Línea	Responsables de Procesos	1. Atender la Política de Administración de Riesgos. 2. Identificar, valorar los riesgos y diseñar las acciones (controles) para evitarlos o reducir su impacto, que puedan afectar el logro de los planes y actividades a su cargo y participar en la construcción de los mapas de riesgos. 3. Supervisar la ejecución de los controles por el equipo de trabajo en la gestión del día a día y evaluar su efectividad. 4. Informar sobre la materialización de los riesgos y realizar el ajuste del Mapa de Riesgos. 5. Divulgar y sensibilizar sobre los riesgos y controles en su proceso a cargo. 6. Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno.

Primera Línea	Profesionales Responsables de ARO.	1. Cumplir y hacer cumplir al equipo de trabajo a su cargo en la gestión del día a día, con los controles establecidos frente a los riesgos para evitar su materialización o para la minimización del impacto. 2. Generar reportes cuando se requiera al Comité Institucional de Coordinación de Control Interno. 3. Ayudar con la divulgación y sensibilización sobre los riesgos y controles en el Área Operativa.
Segunda Línea	Oficina de Planeación o quien haga sus veces) (Gerencia Riesgos) Supervisores e interventores de contratos Comités Institucionales	1. Monitorear y asegurar que los controles y la gestión de riesgos implementados en la Primera Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende. 2. La Oficina de Planeación en coordinación con los responsables de procesos debe consolidar el Mapa de Riesgos, generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno y ayudar con la divulgación y sensibilización sobre los riesgos y controles a todos los servidores de la entidad. 3. Los supervisores e interventores deben realizar seguimiento a los riesgos de sus respectivos contratos e informar las alertas respectivas que atenten con el cumplimiento de los objetivos. 4. Los Comité institucionales deben realizar sus actuaciones con enfoque basado en riesgos.
Tercera Línea	Oficina de Control Interno.	1. Proporcionar información sobre la efectividad de la gestión del riesgo y controles establecidos en la Línea Estratégica y la operación de la Primera y Segunda línea de Defensa con un enfoque basado en riesgos. 2. Comunicar al Comité Institucional de Coordinación de Control Interno sobre la evaluación del riesgo detectada en las auditorías internas. 3. Alertar sobre la probabilidad de riesgo no identificados. 4. Actuar como secretario del Comité Institucional de Coordinación de Control Interno

9. NIVELES DE ACEPTACIÓN AL RIESGO.

En la evaluación del riesgo, la interceptación de la calificación del Impacto (Fila) con la calificación de la probabilidad de Ocurrencia (Columna), nos indica el cuadrante de la Zona de Riesgo respectiva, que puede ser Extremo, Alto, Moderado y Bajo.

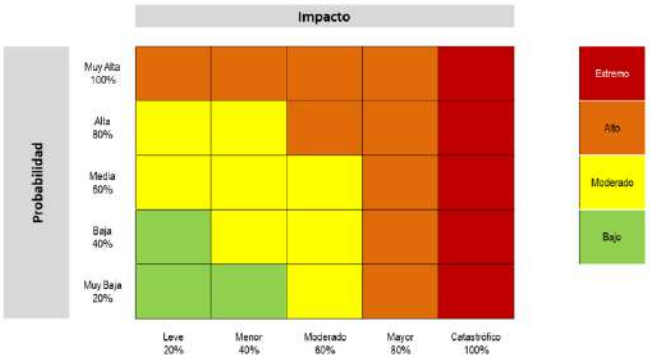
9.1. Riesgos de Gestión y Riesgos de Seguridad de la información

Para los Riesgos de Gestión y Riesgos de Seguridad de la información, los niveles de Impacto serán Leve (20%), Menor (40%), Moderado (60%), Mayor (80%) y Catastrófico (100%) y los niveles de Probabilidad serán Muy baja (20%), Baja (40%), Media (60%), Alta (80%) y Muy Alta (100%).

La interceptación de la calificación del Impacto (Fila) con la calificación de la probabilidad de Ocurrencia (Columna), nos indica el cuadrante de la zona de Riesgo respectiva, que puede ser Extremo, Alto, Moderado y Bajo.

Las zonas de Riesgo Extremo y Alto no son aceptables (Color Rojo y Anaranjado).
Las zonas de Riesgo Moderado y Bajo son aceptables (Color Amarillo y Verde)

La Matriz de calor (niveles de severidad) para estos tipos de riesgos es el siguiente:



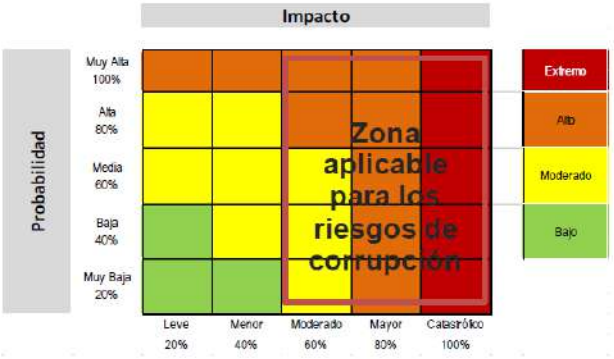
9.2. Riesgos de Corrupción

Para los Riesgos de Corrupción, los niveles de Impacto serán Moderado (60%), Mayor (80%) y Catastrófico (100%) y los niveles de Probabilidad serán Muy baja (20%), Baja (40%), Media (60%), Alta (80%) y Muy Alta (100%).

La interceptación de la calificación del Impacto (Fila) con la calificación de la probabilidad de Ocurrencia (Columna), nos indica el cuadrante de la zona de Riesgo respectiva, que puede ser Extremo, Alto, Moderado y Bajo.

No se admite tolerancia a los riesgos relacionados con prácticas corruptas, es decir TODAS las Zonas de Riesgo no son aceptables.

La Matriz de calor (niveles de severidad) para este tipo de riesgo es el siguiente:



10. NIVELES PARA CALIFICAR EL IMPACTO Y PROBABILIDAD.

10.1 Criterios para calificar el Impacto.

Para los **Riesgos de Gestión** y los **Riesgos de Seguridad de la información** se usará la tabla 5 de la guía, así:

Calificación	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, desconocimiento 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.

Para los **Riesgos de Corrupción** se usarála tabla 16 de la Guía de la Función Pública, así:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA 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.		

Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia de la Presidencia de la República.

10.2 Criterios para calificar la probabilidad

Para los riesgos de Gestión, Riegos de Corrupción y los Riegos de Seguridad se atenderá la tabla 4 de la guía, así:

Calificación	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%

11. VALORACION DE RIESGO INHERENTE, EVALUACION DE LOS CONTROLES EXISTENTES Y NIVEL DE RIESGO RESIDUAL

Con base al resultado de los factores internos y externos se deben determinar las causas y consecuencias para cada riesgo y su respectivo Nivel del Riesgo (Inherente) sin considerar los controles existentes conforme a la Matriz de calor según el tipo de riesgo que le aplica.

Para cada riesgo se debe realizar la Evaluación de los riesgos considerando los controles respectivos para determinar el Nivel de Riesgo (Residual) conforme a la Matriz de calor según el tipo de riesgo que le aplica. Con base al Nivel del Riesgo residual, se establecerá el plan de acción para atender el tratamiento de riesgo escogido.

Se seguirá la metodología descrita en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 – Función Pública. Diciembre de 2020.

La consolidación de la información se realizará en los formatos establecidos para ello así:

F-DE-01 Mapa de Riesgos de Corrupción.
F-DE-12 Mapa de Riesgos de Gestión.
F-DE-13 Mapa de Riesgos de Seguridad de la Información.

12. TRATAMIENTO DE RIESGOS

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo, y debe implicar un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo;
- Planificar e implementar el tratamiento del riesgo;
- Evaluar la eficacia de ese tratamiento;
- Decidir si el riesgo residual es aceptable;
- Si no es aceptable, efectuar el tratamiento adicional.

La selección de las opciones más apropiadas para el tratamiento del riesgo debe implicar hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, disponibilidad presupuestal, esfuerzo o desventajas de la implementación.

Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;
- Aceptar o aumentar el riesgo en busca de una oportunidad;
- Eliminar la fuente de riesgo;
- Modificar la probabilidad;
- Modificar las consecuencias;
- Compartir el riesgo (por ejemplo, a través de contratos, compras de seguros);
- Retener el riesgo con base en una decisión informada.

La política de Administración de Riesgo establece las opciones para tratar los riesgos residuales ya sea fortaleciendo los actuales controles o implementado nuevos controles, para lo cual deberá tener en cuenta las siguientes opciones de manejo:

Evitar el riesgo. Corresponde tomar medidas encaminadas a prevenir o eliminar las causas para su materialización u ocurrencia. Es siempre la primera alternativa a considerar y se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño, eliminación de la actividad que causa el riesgo, y como resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros.

Aceptar el riesgo. Corresponde a asumir las consecuencias del riesgo por considerar de muy baja probabilidad su ocurrencia y de leves consecuencias, o en su defecto, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se acepta la pérdida en caso de materialización. Se elaboran planes de contingencia para su manejo.

Reducir el riesgo. Corresponde tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), sus impactos (medidas de protección), o ambas. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

Compartir el riesgo. Se reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, mediante un contrato determinado, como en el caso de los contratos de seguros, tercerización o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

13. PERIODICIDAD PARA EL MONITOREO Y SEGUIMIENTO

El monitoreo y seguimiento se realizará con base a las responsabilidades de las Líneas de Defensa contenidas en esta política.

13.1 Riesgos de Gestión y Riesgos de Seguridad de la Información

13.1.1 Monitoreo.

El monitoreo de las acciones para controlar los riesgos de gestión y de seguridad de la información, se deben realizar dentro de la operación del día a día de la institución según lo programado; y la revisión y/o actualización del F-DE-12 Mapa de Riesgos de Gestión y del F-DE-13 Mapa de Riesgos de Seguridad de la Información, se realizarán como mínimo cada tres años o cuando las circunstancias lo ameriten, por motivo a cambios sustanciales en el contexto estratégico, modificaciones o cambios relevantes en los procesos y/o procedimientos, por la materialización de un riesgo, la aparición de uno nuevo o cualquier hecho sobreviviente externo o interno que afecte la operación de la entidad.

El responsable de Gestión Informática apoyará y acompañará a las diferentes Líneas de Defensa tanto para el reporte como la gestión y tratamiento, los riesgos de Seguridad de la Información.

13.1.2 Seguimiento

El Proceso de Control Interno de Gestión realizará el seguimiento de los riesgos institucionales y la implementación de las acciones para controlar los riesgos de gestión y de seguridad de la información contenidos en los mapas de riesgos, y sus resultados serán informados en los informes de las auditorías internas que realice, o en cualquier momento cuando considere necesario.

13.2 Riesgos de corrupción.

13.2.1 Monitoreo.

El monitoreo de las acciones para controlar los Riesgos de Corrupción, se debe realizar dentro de la operación en el día a día de la institución según lo programado; y la revisión y/o actualización del F-DE-01 Mapa de Riesgos de Corrupción, se alineará con el Plan Anticorrupción y Atención al Ciudadano (Primer Componente); es decir, de manera anual y deberá ser publicado en la página WEB de la entidad, antes del 31 de enero de cada año, conforme a las responsabilidades definidas en cada Línea de Defensa; o cuando las circunstancias lo ameriten, por la materialización de un riesgo de corrupción y/o la aparición de uno nuevo.

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

1) Informar a las autoridades competentes de la ocurrencia del hecho de corrupción.
2) Revisar e implementar las medidas establecidas en 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) Realizar un monitoreo permanente.

13.2.2 Seguimiento

El seguimiento de las acciones para controlar los Riesgos de Corrupción, lo realizará el Proceso de Control Interno de Gestión así:

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

14. ACCIONES PARA LA APROPIACIÓN CULTURAL DE LA GESTIÓN DEL RIESGO

En la Unidad Ejecutora de Saneamiento del Valle del Cauca - UESVALLE, se promoverá la transparencia, cero tolerancias con la corrupción y se fortalece la cultura del autocontrol y la prevención, los cuales contribuyen a la Administración de Riesgos, a través de:

- Estrategias de sensibilización y comunicación a través de los medios establecidos, de esta política y promover el pensamiento basado en riesgos.
- Asesorías y acompañamiento para el desarrollo del enfoque de administración de riesgos en las actividades diarias.
- Divulgación de los resultados de la Administración de Riesgos en los procesos de la Entidad; así como, el reporte y actualización permanente del Mapa y Plan de Tratamiento de Riesgos.
- Seguimiento prioritario a los riesgos ubicados en las zonas de Riesgo Extremo y Alta, identificada para cada uno de los procesos de la Entidad; así como, la implementación de las medidas correctivas a que haya lugar.

15. NOTAS DE CAMBIO

Fecha	Versión inicial	Motivo del cambio y numerales modificados	Versión final
Nov. 30 de 2014	1.0	Se realiza actualización ajustándose al MECI 2014, Se cambia responsable del documento. Pasa a versión 2 con el código nuevo para dejar trazabilidad. Nombre del Código del Documento, Objetivos, Alcance, Definiciones, Actividades, Políticas de operación y Formatos de referencia.	2.0
Ene. 14 de 2019	2.0	Se cambia el Tipo de Documento a Manual viene del Código P-DE-03. Se ajusta a la imagen corporativa, Se tiene en cuenta la nueva guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles de Entidades Públicas. Se cambia todos sus componentes. Se atiende el MIGO y el Nuevo modelo integrado de planeación y gestión.	3.0

Ago. 13 de 2019	3.0	Se realiza revisión y ajuste en atención a lo observado en el hallazgo 20 parte 4 de la Contraloría del valle del cauca en el informe de la auditoría regular 2019 de la vigencia 2017-2018. Se tiene en cuenta frente a la determinación de ocurrencia de los riesgos, periodicidad de seguimiento y los niveles de aceptación de riesgos. Se revista y se ajusta conforme a la Guía establecida en la página 14 títulos Paso 1: Política de Administración de riesgos subtitulo ¿Qué debe contener? Se reorganiza la tabla de contenido y se ajusta los puntos 2, 3 y 6.	4.0
Ene. 27 de 2021	4.0	Se ajusta la política en todas sus partes en atención a la nueva Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 – Función Pública. Diciembre de 2020, y la actualización del Manual Operativo MIPG que pasó a la versión 3. Se revisa el tratamiento de riesgos con base a la norma NTC 31000.	5.0

16. APROBACIÓN

	ELABORÓ	**REVISÓ**	**APROBÖ**
Nombre:	Álvaro José Cruz Montoya	Fanny Loango Sinisterra Jhon Jairo Zapata Osorio Constanza Ivette Hernández Diana del Mar Gómez Fernández	Diego Victoria Mejía
Cargo:	Profesional de apoyo	Subdirectora Administrativa (E) Subdirector Técnico Asesora de Planeación Profesional Universitario SGC	Director General
Fecha:	Ene. 27 de 2021	Ene. 27 de 2021	Ene. 27 de 2021
Firma:	Documento Original Firmado.	Documento Original Firmado.	Documento Original Firmado.