POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE EL CARMEN DE BOLÍVAR

ACUECAR S.A. E.S.P

2021

Carrera 52 No. 25 43 Barrio Centro, Tel.(5)6862822 - El Carmen de Bolívar (Bolívar)
Contactenos.acuecar@gmail.com www.acuecar.com

Contenido

INTRODUCCIÓN

El concepto de Administración del Riesgo se introduce en las entidades públicas debido a que todas las organizaciones, independientemente de su naturaleza, tamaño y objeto misional están expuestas a diversos eventos que pueden poner en peligro su existencia, metas, objetivos y hasta la oportunidad y eficacia de los servicios y bienes que ofrece.

Desde el enfoque de la Norma Técnica **NTC-ISO 31000** e **ISO 9001 - 2015** se considera que los sistemas de gestión se deben trabajar con un enfoque basado en riesgos que permita identificarlos y actuar con suficiente anticipación para evitar que sucedan o aminorar sus efectos. La administración de riesgos es la base para la planificación, que debe contribuir al logro de los objetivos institucionales; además, permite identificar, analizar y abordar los hechos que se presenten para adoptar estrategias o actividades que garanticen cumplir con la misión, la visión y la entrega de bienes y servicios con calidad por parte de la entidad. Administrar riesgos es anticiparse a las dificultades, deficiencias o adversidades internas o externas que pueden impedir que logremos nuestros propósitos, o que simplemente que cumplamos nuestras responsabilidades.

Con el propósito de contar con una política para la gestión de riesgos de corrupción, de gestión y de seguridad digital actualizada con los últimos lineamientos y metodologías. A través de este documento, la Empresa de servicios públicos de Acueducto y Alcantarillado de El Carmen de Bolívar ACUECAR S.A. E.S.P estandariza las herramientas y la metodología general, personalizándola en su usabilidad y aplicabilidad, de acuerdo a las complejidades de la entidad.

Esta política está articulada con las orientaciones de las Norma ISO 31000 (Gestión de Riesgos), 27001 (Gestión en la seguridad de la información), y los de la Función Pública colombiana, tanto en aceptación de los riesgos, como en actividades asociadas al tratamiento de los mismos y el diseño de controles.

En la Empresa de servicios públicos de Acueducto y Alcantarillado de El Carmen de Bolívar ACUECAR S.A. E.S.P la administración del riesgo es direccionada por el proceso de Planeación Estratégica, y debe ser aplicada por todos los procesos institucionales.

Para el éxito de esta política es indispensable la participación y compromiso de todos los funcionarios y colaboradores de ACUECAR, de tal forma que todos

cumplan los lineamientos de este documento para la identificación, análisis, valoración y tratamiento de los riesgos que puedan afectar la misión y el cumplimiento de los objetivos institucionales, mediante:

a) La identificación de riesgos de gestión, de corrupción y de seguridad digital en cada proceso de la entidad,
b) El diseño de acciones preventivas para los riesgos identificados y,
c) La actuación correctiva y oportuna ante una eventual materialización de los riesgos.

Para administrar adecuadamente los riesgos de gestión, corrupción y de seguridad digital, la entidad utilizara tres (3) herramientas ofimáticas, en hojas de cálculo, debidamente parametrizados con los lineamientos de la presente política, cuya elaboración contó con el apoyo de la Fundación Tecnológica de la Región del Caribe Colombiano "**FUNDACARCOL"**.

Para garantizar el éxito en la implementación de la gestión del riesgo, proponemos desarrollar el sistema de líneas de defensa, en el que se asignan roles estratégicos, ejecución de controles y administración del riesgo, y monitoreos y seguimientos que conducen a un examen, constante y en tiempo real, sobre la eficacia de los controles, de modo que la gestión del riesgo sea una acción coordinada de actores que aseguren el cumplimiento de sus propósitos.

Esperamos que este documento sirva de orientación y de guía para los empleados y colaboradores de ACUECAR en la prevención de los riesgos en general, que mejoremos los indicadores de gestión y de resultados de nuestra administración, y que ello redunde en mejorar la calidad de vida de nuestros usuarios.

OBJETIVOS DE LA POLÍTICA

La Empresa de servicios públicos de Acueducto y Alcantarillado de El Carmen de Bolívar ACUECAR S.A. E.S.P asume la administración del riesgo como un elemento esencial de carácter estratégico, con un enfoque preventivo en torno a los riesgos que representan amenazas para el cumplimiento de nuestros objetivos. La gestión del riesgo debe ser cumplida por todos los procesos, y en todos los proyectos, programas y acciones de la entidad.

La administración del riesgo en la Empresa de Acueducto y Alcantarillado de El Carmen de Bolívar-ACUECAR S.A. E.S.P tiene los siguientes objetivos:

- ✓ Identificar técnicamente los riesgos que puedan afectar nuestros objetivos.
- ✓ Formular acciones de prevención y de control oportuna de los riesgos.
- ✓ Contar con una metodología y con herramientas de gestión adecuadas para el análisis y evaluación de riesgo, la asignación de roles y establecimiento de controles e indicadores de seguimiento, de fácil uso y de gran utilidad.
- ✓ Utilizar un enfoque de prevención de riesgos, que permita anticiparnos a los hechos o situaciones que representan un obstáculo o desviación para el cumplimiento de nuestras metas y objetivos.

2. GLOSARIO DE TERMINOS.

En este capítulo detallamos en orden alfabético las definiciones de conceptos técnicos utilizados en este documento, para facilitar su comprensión:

Análisis de Riesgos: corresponde a la determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Consecuencias: son los efectos que resultan de la ocurrencia o la materialización de un riesgo.

Causas: son los hechos, circunstancias, situaciones generadoras del evento o riesgo.

Control: son las acciones que propone la entidad para reducir la probabilidad de ocurrencia o el impacto que pueda generar su materialización. **Por cada causa debe formularse un control.**

Evento o riesgo: es el hecho que se afecta el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Frecuencia: es la periodicidad con que ha ocurrido un evento.

Gestión del riesgo: Es un proceso que involucra a todos los funcionarios y colaboradores de una organización, que debe liderar la alta dirección para garantizar la prestación adecuada de bienes y servicios, y para asegurar el cumplimiento del objeto misional.

Gestor del Riesgo: Funcionario líder de una dependencia, dirección, secretaria u oficina, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación, hecho o evento riesgoso.

Impacto: es la magnitud de las consecuencias que pueden ocasionar a la entidad la materialización del riesgo.

Matriz de gestión del riesgo: Es una herramienta de gestión parametrizada de los riesgos, para la identificación, análisis, valoración y administración de los riesgos. Las matrices de administración del riesgo **son tres: de riesgos de gestión, corrupción y seguridad digital.**

Mapa de riesgos: Es el documento con la información resultante de la gestión del riesgo consolidado.

Políticas de manejo del Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Medida para determinar la posibilidad de que ocurra un evento.

Responsable del riesgo: Es el responsable del proceso encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo de cada uno de los riesgos.

Riesgo de gestión: Es la posibilidad de que suceda algún evento que afecte negativamente el cumplimiento de los objetivos

Riesgo de corrupción: Es la posibilidad de que, por acción u omisión, se use el poder deliberadamente para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de seguridad digital: Es la combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las persona.

Riesgo residual: Es aquel que resulta después de aplicar controles existentes para mitigar el riesgo.

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlarlo y buscar evitar su materialización.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

3. CONTEXTUALIZACION.

Para entender los términos de esta política es necesario conocer el contexto general de la Empresa de Acueducto y Alcantarillado de El Carmen de Bolívar ACUECAR S.A. E.S.P. para identificar sus características, generalidades, entorno, funciones, procesos; y en general, todo lo relacionado con sus elementos esenciales:

La **MISIÓN Y VISIÓN** expresan los principales fines de la entidad, su rumbo y aspiraciones o proyección a media plazo.

LOS **OBJETIVOS ESTRATÉGICOS** son aquellos a los que deben dirigirse los recursos y esfuerzos de la entidad. Se plasman en el Plan de Acción y en los instrumentos de planeación institucional.

El **MAPA DE PROCESO** es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación de la entidad, y su interacción, de acuerdo con el Modelo de Operación por Procesos MOP.

La **CARACTERIZACIÓN DE LOS PROCESOS** es el documento que detalla los objetivos específicos, las características, proveedores, acciones, productos, clientes, indicadores, procedimientos y formatos más relevantes de cada proceso de la organización, desarrollando el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

3.1. MISIÓN DE ACUECAR

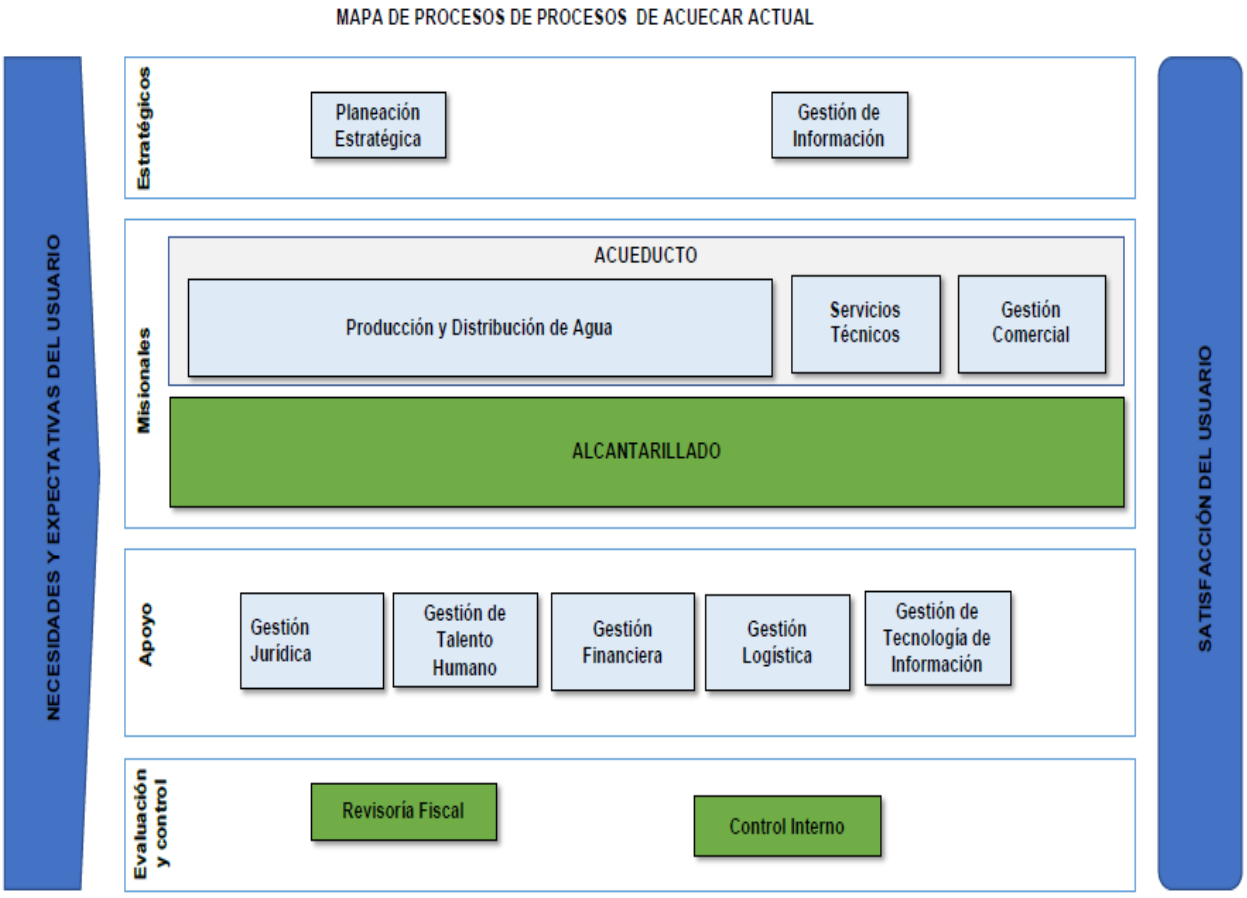
Somos una empresa comprometida con el mejoramiento de la calidad de vida de la población, a través del abastecimiento permanente de agua potable y disposición final de aguas servidas; prestamos servicios de óptimas condiciones sanitarias con los más altos estándares de calidad y confiabilidad, asegurando la sostenibilidad Ambiental, Económica y Social.

3.2. VISIÓN DE ACUECAR

ACUECAR S.A. E.S.P para el año 2023 brindará un servicio de agua potable y servicio de alcantarillado al 100% del municipio, garantizando un sistema continuo, de altos estándares de calidad, que respondan a las necesidades y al desarrollo de la población, construyendo valor público y garantizando la sostenibilidad financiera, ambiental y social.

3.3 MAPA DE PROCESOS

El mapa de procesos describe los procesos que hacen parte de la empresa agrupándolos en macroprocesos (conjunto de procesos con un objeto general común), y clasificándolos en Estratégicos, de Gestión, de Apoyo y de Seguimiento y Evaluación. En la siguiente imagen se presenta el mapa de procesos propuesto para Acuecar S.A. E.S.P.



4. ASPECTO METODOLOGICO PARA LA GESTIÓN DEL RIESGO

4.1 MODELO DE LÍNEAS DE DEFENSA.

El modelo de Líneas de Defensa es un sistema en el que se distribuyen los roles y responsabilidades en los funcionarios de las organizaciones, en relación con la administración de los riesgos. Este modelo se apoya en la estructura orgánica y en el modelo de operación por procesos de la Empresa de Acueducto y Alcantarillado de El Carmen de Bolívar-ACUECAR S.A. E.S.P y en el ciclo de gestión PHVA.

El Modelo contiene **tres (3) líneas de defensa** así:

4.1.1. Línea de defensa estratégica

Esta línea de defensa es la que define el marco general para la gestión del riesgo y el control y además, supervisa su cumplimiento. Está a cargo de la Alta dirección, en el proceso de Planeación Estratégica.

Responsabilidades:

- ✓ Diseñar la **Política institucional de Administración del Riesgo**.
- ✓ **Formular y socializar** la metodología para la identificación, análisis, valoración, monitoreo y seguimiento de los riesgos, así como las oportunidades que contribuyan a aumentar los efectos deseables para el cumplimiento de los objetivos del plan de acción institucional y de los procesos.

- ✓ **Establecer objetivos institucionales** articulados con la visión, misión y el plan de acción o estratégico, con las metas y estrategias de la entidad.

- ✓ Asegurarse **que el sistema de control interno funcione**, identificar y evaluar los cambios que lo puedan impactar.

- ✓ **Revisar los cambios en el "Direccionamiento estratégico**" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.

- ✓ Verificar que los **objetivos** de los procesos **sean coherentes** con los objetivos institucionales.

- ✓ **Hacer seguimiento,** en el seno del Comité Institucional y de coordinador de Control Interno, **a la gestión del riesgo** y a los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.

- ✓ **Revisar el cumplimiento de los objetivos institucionales** y de los procesos a través de indicadores, y detectar los riesgos que se estén materializando.

- ✓ **Revisar**, al menos trimestralmente, **los informes sobre los riesgos** que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que los ocasionaron.

- ✓ **Revisar los planes de acción frente a los riesgos** que hayan ocurrido, para asegurarse que tomen medidas oportunas y eficaces para evitar que se repitan.

4.1.2. Línea de Defensa de control

Los colaborares de esta línea de defensa son los encargados de desarrollar e implementar los procesos de control y gestión de riesgos, por medio de la identificación, análisis, valoración, aplicación, monitoreo y el diseño y cumplimiento de las acciones de mejora.

Empleados de esta línea de defensa: Líderes de los Procesos Institucionales (jefes de oficina, asesores líderes de procesos)

Responsabilidades:

- ✓ **Identificar y valorar los riesgos** que pueden afectar el logro de los objetivos institucionales.

- ✓ **Definir y diseñar los controles** a los riesgos.

- ✓ **Establecer sistemas de gestión de riesgos** y las responsabilidades para controlarlos, bajo la supervisión de la alta dirección.

- ✓ Diseñar los mapas de riesgos por procesos.

- ✓ **Identificar y gestionar los riesgos asociados a posibles actos de corrupción**.

- ✓ **Identificar y detectar fraudes**, y revisar con el auditor o control interno de la organización, la exposición de la entidad al fraude.

- ✓ Verificar 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 sus procesos.

    - Verificar que, el **diseño y ejecución** de los controles para la mitigación de los riesgos sea adecuado y eficaz.
    - Verificar que las **actividades de control** de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

- ✓ Monitorear el cumplimiento de los objetivos de sus procesos a través de sus **indicadores de desempeño**, e identificar en caso de que no se estén cumpliendo, los riesgos que están ocurriendo.

- ✓ **Revisar y reportar a Planeación**, los riesgos que se han materializado en la entidad, incluyendo los de corrupción, así como las causas que los originaron.

- ✓ **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.

4.1.3. Línea de Defensa de evaluación

Los empleados o funcionarios que pertenecen a esta línea de defensa son los que realizan la evaluación independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, **verificando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos**.

Responsable: Proceso de Control y Evaluación (control interno).

Responsabilidades:

- ✓ **Evaluar la eficacia de la gestión del riesgo y del control**, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

- ✓ **Asesorar**, en coordinación con el proceso de planeación estratégica, **sobre la identificación de los riesgos** institucionales y el diseño de controles.

- ✓ Llevar a cabo el **seguimiento a los riesgos consolidados** en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados a la lata dirección.

- ✓ **Recomendar mejoras** a la política de administración del riesgo.

- ✓ **Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno**, durante las evaluaciones periódicas de riesgos y en el curso de las auditorías internas.

- ✓ **Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo** vinculadas a riesgos claves de la entidad.

- ✓ **Alertar** sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

- ✓ **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, con el fin de que se formulen ajustes o mejoras.

- ✓ **Revisar que se hayan identificado los riesgos 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 su fortalecimiento.

- ✓ Revisar **que las acciones orientadas a mitigar los riesgos de los procesos se encuentren documentadas** y actualizadas en los procedimientos y los planes de mejora, además, que se lleven a cabo de manera oportuna, se establezcan las causas y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

4.2. IDENTIFICACIÓN DEL RIESGO.

La identificación del riesgo **le corresponde a la línea de defensa de ejecución**. En esta primera fase se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

Teniendo en cuenta que la metodología para la gestión del riesgo se enfoca en tres (3) tipos de riesgos: **de gestión, corrupción y de seguridad digital**; en adelante, se especificarán los lineamientos para cada uno de estos de manera separada.

La identificación del riesgo se realiza a partir de la descripción de los eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso con base en el contexto interno y externo. Se debe hacer una breve descripción del riesgo refiriéndose a sus características o las formas en que se manifiesta.

Para la identificación de los riesgos es recomendable concentrarse en los riesgos más significativos para los procesos, relacionados con sus objetivos y el cumplimiento de metas.

Para identificar un riesgo, sus causas y consecuencias, se sugiere formular las siguientes preguntas:

¿ Qué puede ocurrir?
¿ Cómo puede ocurrir?
¿ Por qué puede ocurrir?
¿ Qué consecuencias tendría su materialización?

Para la identificación del **riesgo de corrupción** se deben describir las situaciones que sugieren la ocurrencia de un hecho que **implique el uso del poder para desviar la gestión de lo público** con el propósito de **obtener un beneficio particular**, de tal modo que deberán concurrir los siguientes elementos:

NOTA: Es importante recordar que el "Uso de Poder" y "Beneficio privado" **son característicos del Riesgo de Corrupción**, por lo que debe asegurarse que en la formulación de este tipo de riesgos se incluyan esos elementos.

El beneficio privado corresponde a la intensión de generar un lucro o beneficio a un tercero o para el mismo servidor público.

El uso del poder corresponde a la circunstancia de que un servidor público o particular en ejercicio de funciones públicas, haga uso de su cargo o de sus funciones para generar el hecho de corrupción.

Para la identificación de **riesgos de seguridad digital** se deben identificar los activos en cada proceso, esta labor debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada uno donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la Empresa de servicios públicos de Acueducto y Alcantarillado de El Carmen de Bolívar-ACUECAR S.A. E.S.P.

Un **activo** es cualquier elemento que tiene valor para la organización, sin embargo, en el contexto de seguridad digital, **son activos que utiliza la organización para funcionar en el entorno digital**: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Se busca proteger los activos para garantizar tanto su funcionamiento interno como el funcionamiento de la entidad de cara al ciudadano, aumentando su confianza en el uso del entorno digital.

Para identificar los activos, se deben seguir los siguientes pasos:

El resultado de este ejercicio es la consolidación del inventario de activos.

4.3 IDENTIFICACION DE CAUSAS Y CONSECUENCIAS.

Causas: Cuando se identifican y describen los riesgos, se deben identificar las causas generadoras de estos; es decir, todos aquellos factores tanto de carácter interno como externos que, solos o en combinación con otros, posibilitan la materialización de un riesgo.

Este elemento es supremamente importante porque determina el éxito de la administración del riesgo. Las causas son las circunstancias que generan los riesgos, de tal suerte que si se identifican adecuadamente, su prevención o manejo será más eficaz y oportuno.

Por cada causa debe formularse un control o acción preventiva, correctiva o detectiva, de tal manera que habrá tantos controles como causas de identifiquen.

Consecuencias: Es necesario identificar las consecuencias; es decir, los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, los grupos de valor y demás partes interesadas.

Los efectos o consecuencias deben identificarse con amplitud, teniendo el cuidado de preguntarse qué daños administrativos, físicos, en el grupo de trabajo o área, en la entidad en general, en la sociedad o comunidad, ocasionan los riesgos si llegan a suceder.

A continuación, se ilustran ejemplos y esquemas para la identificación de riesgos, causas y consecuencias para cada uno de los tipos de riesgos tratados en la presente política.

RIESGOS DE GESTION			
#	**Descripción del Riesgo**	**Causas**	**Consecuencias**
1	Desactualización de los funcionarios sobre las normas que regulan los procesos de la entidad.	Ausencia de un Plan Institucional de Capacitación Indebido análisis y priorización de temáticas en los procesos de capacitación. Ausencia de procedimientos para formular el plan de capacitación institucional.	Productos y servicios deficientes, bajos estándares de calidad, demandas, denuncias, investigaciones disciplinarias, afectación del clima laboral, improductividad laboral

RIESGOS DE CORRUPCION			
#	**Descripción del Riesgo**	**Causas**	**Consecuencias**
1	Ocultar en los informes de evaluación y seguimiento irregularidades o deficiencias o conceptualizar favorablemente, contrario a las evidencias, con el fin de conseguir algún beneficio particular para sí o para terceros.	Amiguismo Ausencia de valores éticos Tráfico de influencias	Investigaciones disciplinarias, baja calidad de productos, incumplimiento de los objetivos del proceso y los institucionales; impunidad, deterioro de la confianza y de la autoridad.

RIESGOS DE SEGURIDAD DIGITAL				
#	Activo	Descripción del Riesgo	Causas	Consecuencias
1	SOFTWARE SOLIN	Pérdida de la confidencialidad Pérdida de la integridad Pérdida de disponibilidad	Ausencia de una política de restricción de acceso no autorizado al programa Manipulación de la información Ataques cibernéticos	Pérdida de la información, inoperatividad del sistema, afectación de procesos laborales, retrasos en la producción laboral y gestión comercial

4.4. VALORACIÓN DEL RIESGO.

Consiste en analizar el riesgo para establecer su probabilidad de ocurrencia y el impacto o consecuencias que genera, con el fin de **estimar la zona de riesgo inicial** (**RIESGO INHERENTE**); y posteriormente evaluarlo, para confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (**RIESGO RESIDUAL**).

En la valoración del riesgo, para establecimiento de la zona del riesgo inherente se desarrollan las siguientes actividades:

4.4.1. Probabilidad e impacto.

Por **PROBABILIDAD** se entiende el grado de ocurrencia de un riesgo, éste puede ser medido con criterios de Frecuencia o Factibilidad. Bajo el criterio de **FRECUENCIA** se analizan el número de eventos en un periodo determinado, se trata de hechos que han ocurrido; y bajo el criterio de **FACTABILIDAD** se analiza 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 que puede ocurrir.

Para determinación de la probabilidad, de acuerdo con los tipos de riesgos, aplican las siguientes tablas de probabilidad:

Tabla de probabilidad para los riesgos de Gestión

Frecuencia de la actividad		
Descriptor	**Descripción**	**Nivel**
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 25 a 500 veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 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%**

Tabla de probabilidad para los riesgos de corrupción y de seguridad digital

Medición de la PROBABILIDAD del Riesgo			
Descriptor	**Descripción**	**Frecuencia**	**Nivel**
RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.	**1**
IMPROBABLE	El evento puede ocurrir en algún momento	Se presentó al menos una vez en los últimos 5 años	**2**
POSIBLE	El evento podría ocurrir en algún momento	Se presentó al menos una vez en los últimos dos años.	**3**
PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias	Se presentó al menos una vez en el último año.	**4**
CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Se ha presentado más de una vez al año.	**5**

Por **IMPACTO** se entienden las consecuencias que genera la ocurrencia del riesgo. Para su determinación de acuerdo con el tipo de riesgo, se utilizan los siguientes criterios:

Criterios para calificar el impacto en los RIESGOS DE GESTIÓN

Afectación económica y repitacional			
Descriptor	**Porcentaje**	**Afectación económica**	**Reputacional**
Leve	**20%**	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor	**40%**	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Moderada	**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

Criterios para calificar el impacto en los RIESGOS DE CORRUPCIÓN

No	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA SI	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		

5	¿Generar pérdida de confianza de la entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos
9	¿Generar pérdida de información de la entidad?
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?
15	¿Generar pérdida de credibilidad del sector?
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?
19	¿Generar daño ambiental?

NIVELES DE IMPACTO

CRITERIO	IMPACTO	CONSECUENCIA
Responder afirmativamente de UNA a CINCO preguntas(s)	**MODERADO**	Genera medianas consecuencias sobre la entidad
Responder afirmativamente de SEIS a ONCE preguntas	**MAYOR**	Genera altas consecuencias sobre la entidad.
Responder afirmativamente de DOCE a DIECINUEVE preguntas	**CATASTRÓFICO**	Genera consecuencias desastrosas para la entidad

Criterios para calificar el impacto en los RIESGOS DE SEGURIDAD DIGITAL

NIVEL	Valor del Impacto	CRITERIOS CUANTITATIVOS	CRITERIOS CUALITATIVOS
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y tercero
MAYOR	4	Afectación ≥X% de la población. Afectación	-Afectación grave de la integridad de la información

		≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación	debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Las variables **confidencialidad, integridad y disponibilidad** se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable **población** se define teniendo en cuenta el contexto externo de la entidad; es decir, que la población está asociada a las personas a las que se les prestan servicios o trámites en el entorno digital, y que de una u otra forma, pueden verse afectadas por la materialización de algún riesgo. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable **presupuesto** es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable **ambiental** está relacionada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental

4.5. MAPA DE CALOR.

Para la calificación de la zona del riesgo inherente se toma la calificación de **PROBABILIDAD** resultante de la "tabla de probabilidad" y la del **IMPACTO**. Se deben ubicar los puntos de encuentros o intersección de la probabilidad y el impacto en el mapa de calor para determinar la **ZONA DEL RIESGO.**

Para el análisis del riesgo inherente de los riesgos se debe tener en cuenta el siguiente Mapa de Calor.

Resultados de la calificación del Riesgo						
Probabilidad	Puntaje	Zonas de Riesgo				
Casi seguro	5	Zona Alta	Zona Alta	Zona Extrema	Zona Extrema	Zona Extrema
Probable	4	Zona Moderada	Zona Alta	Zona Alta	Zona Extrema	Zona Extrema
Posible	3	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema	Zona Extrema
Improbable	2	Zona Baja	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema
Rara vez	1	Zona Baja	Zona Baja	Zona Moderada	Zona Alta	Zona Extrema
	Impacto	Insignificante	Menor	Moderado	Mayor	Catastrófico
	Puntaje	**1**	**2**	**3**	**4**	**5**

NOTA: 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 insignificante y menor, que sí aplican para los demás riesgos.

4.6. EVALUACIÓN DEL RIESGO.

La evaluación del riesgo está dirigida a confrontar los resultados del Riesgo inicial (**RIESGO INHERENTE**) frente a los controles establecidos con el fin de determinar la zona de riesgo final (**RIESGO RESIDUAL**).

En ese sentido, se busca identificar controles dirigidos a la administración del riesgo y valorarlos. Se deben seguir las siguientes acciones:

- ✓ Identificar los riesgos inherentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.
- ✓ Identificar las causas o fallas que pueden materializar el riesgo.
- ✓ Para cada causa se debe asignar un control.
- ✓ Evaluar si los controles están dirigidos a evitar o mitigar el riesgo.
- ✓ Las causas se deben trabajar de manera separada (**no se deben combinar en una misma columna o renglón**).
- ✓ Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

Al momento de definir las actividades de control por parte de la línea de defensa de ejecución, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

Para diseñar un control (*acciones preventivas o detectivas de los riesgos*) debemos utilizar los siguientes **Criterios:**

RESPONSABLE: Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso. **Las responsabilidades pueden ser distribuidas entre varios individuos**.

Si la PERSONA o responsables cumplen esos criterios, quiere decir que el control está bien diseñado, si la respuesta es negativa tenemos que corregir o mejorar el diseño del control seleccionando adecuadamente al responsable de su ejecución.

Controles sistematizados. Cuando el control lo hace un sistema o una aplicación de manera automática a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación.

PERIODICIDAD: El control debe tener una periodicidad específica para su realización (***diario, mensual, trimestral, anual, permanente*** etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo.

Cada vez que se diseña un control debemos preguntarnos si la periodicidad en que este se ejecuta ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

4.7. TIPOS DE CONTROL.

Nuestros controles se clasifican en PREVENTIVOS, CORRECTIVOS y DETECTIVOS.

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; es decir, no lo previenen.

CONTROL CORRECTIVO: control accionado en la salida del proceso y después de que se materializa el riesgo; es decir, ayudan a mitigar o controlar los efectos del riesgo; por ejemplo, recuperar lo pagado en exceso. Estos controles tienen costos implícitos.

4.8. ANÁLISIS Y EVALUACIÓN DE CONTROLES.

Los criterios para el análisis y evaluación del diseño del control de acuerdo con los tipos de riesgos, son los siguientes.

CRITERIOS PARA ANÁLISIS DEL RIESGO DE GESTIÓN

ATRIBUTOS	CRITERIOS DE EVALUACIÓN	OPCIONES DE RESPUESTA	
DE EFICIENCIA	TIPO DE CONTROL	Preventivo, Detectivo, Correctivo	
	IMPLEMENTACIÓN	Manual	Automática
INFORMATIVOS	DOCUMENTACIÓN	Documentado	Sin documentar
	FRECUENCIA	Aleatoria	Continua
	EVIDENCIA	Con registro	Sin registro

Peso o participación de cada variable en el diseño del control.

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO
TIPO DE CONTROL	Preventivo	**25**
	Detectivo	**15**
	Correctivo	**10**
IMPLEMENTACIÓN	Automática	**30**
	Manual	**15**
DOCUMENTACIÓN	Documentado	**15**
	Sin documentar	**0**
FRECUENCIA	Aleatoria	**15**
	Continua	**10**
EVIDENCIA	Con registro	**15**
	Sin registro	**0**

CRITERIOS PARA ANÁLISIS DEL RIESGO DE CORRUPCIÓN Y DE SEGURIDAD DIGITAL

Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuesta	
Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna

Propósito	¿Las actividades que se desarrollan en el control realmente buscan prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
¿Cómo se realiza la actividad de control?	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
¿Qué pasa con las observaciones o desviaciones?	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente
Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe

Peso o participación de cada variable en el diseño del control.

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO
Asignación del responsable	Asignado	**15**
	No Asignado	**0**
Segregación y autoridad del responsable	Adecuado	**15**
	Inadecuado	**0**
Periodicidad	Oportuna	**15**
	Inoportuna	**0**
Propósito	Prevenir	**15**
	Detectar	**10**

	No es un control	**0**
Cómo se realiza la actividad de control	Confiable	**15**
	No confiable	**0**
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	**15**
	No se investigan y resuelven oportunamente	**0**
Evidencia de la ejecución del control	Completa	**10**
	Incompleta	**5**
	No existe	**0**

Resultados de la evaluación del diseño del control

Rango de calificación del diseño	Resultado - peso en la evaluación del diseño del control
FUERTE	**Calificación entre 96 y 100**
MODERADO	**Calificación entre 86 y 95**
DÉBIL	**Calificación entre 0 y 85**

NOTA: SI las calificaciones del control, o el promedio de los controles por riesgo **está por debajo de 96%, se deben ajustar o mejorar los controles hasta que queden bien diseñados**.

Si los controles son nuevos, la calificación del control será cero "0" y será válido la implementación de un control o conjunto de controles con rango de calificación Débil o Moderado.

4.8.1. Solidez de los controles.

Se deben promediar todos los controles por cada riesgo, y el resultado determinará si se mantiene la zona de riesgo o si baja (**riesgo residual)**.

Desplazamiento del riesgo inherente para calcular el riesgo residual

Cuando valoramos los controles existentes y el resultado es un control fuerte o moderado, se obtiene una mejora en la **ZONA DEL RIESGO**, pues, la metodología indica que un buen CONTROL disminuye la probabilidad de ocurrencia o el impacto de un riesgo.

Entonces el **RIESGO RESIDUAL** se determina de acuerdo con la siguiente tabla:

Criterio	Si el control ayuda a disminuir la probabilidad	Si el control ayuda a disminuir impacto
Solidez del conjunto de los controles	**# columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad**	**# columnas en la matriz de riesgo que se desplaza en el eje de impacto**
FUERTE	**2**	**2**
MODERADO	**1**	**1**

***Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

***Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad; es decir, para el impacto no opera el desplazamiento, porque se considera que el impacto siempre es el mismo.

4.9. TRATAMIENTO DEL RIESGO.

Es tratamiento del riesgo es la respuesta establecida por **la línea de defensa** de **ejecución** para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- ✓ **Aceptar el Riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

NOTA: Ningún riesgo de corrupción podrá ser aceptado).

- ✓ **Reducir el Riesgo**: se adoptan medidas para **reducir la probabilidad o el impacto del riesgo**, o ambos; por lo general implica diseñar controles.

- ✓ **Evitar el Riesgo**: se abandonan las actividades que dan lugar al riesgo; es decir, se suprime la actividad, plan, programa, función o proyecto asociado al riesgo.

- ✓ **Compartir el Riesgo**: se reduce la probabilidad o el impacto del riesgo **transfiriendo o compartiendo una parte de este**. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

4.10. REVISIÓN DEL PROCESO DE CONTROL INTERNO

Es el proceso encargado de realizar el seguimiento a los riesgos consolidados. En sus procesos de auditoría interna se debe analizar el diseño e idoneidad de los controles, determinando:

- ✓ Si son o no adecuados para prevenir o mitigar los riesgos de los procesos,
- ✓ Si se aplicaron oportuna y adecuadamente,
- ✓ Si se dejaron evidencias de su aplicación y,
- ✓ Si se reportaron las desviaciones detectadas, haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles.

Los informes de control interno **deben incluir recomendaciones** que promuevan ajustes, mejoras o actividades para subsanar las desviaciones detectadas.

4.10.1. Lineamientos para los riesgos materializados

Si dentro del seguimiento realizado se detecta, bien sea por parte del proceso de control interno, la Alta Dirección o por los líderes de los procesos, que ha ocurrido uno o más riesgos, se deben seguir las siguientes rutas:

a. **POR PARTE DEL PROCESO DE CONTROL INTERNO**

Cuando el riesgo sea de corrupción

- ✓ Convocar al Comité Coordinador de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos.

- ✓ Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.

- ✓ Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados.

- ✓ Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA:

- ✓ Informar al líder del proceso sobre el hecho encontrado.

- ✓ Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho.

- ✓ Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente.

- ✓ Convocar al Comité Coordinador de Control Interno e informar sobre la actualización realizada.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA:

- ✓ Aplicar las orientaciones de la política de riesgos institucional. (Verificar los niveles de aceptación del riesgo).

b. POR PARTE DE LOS LÍDERES DE LOS PROCESO U OTROS FUNCIONARIOS QUE PARTICIPAN O INTERACTÚAN CON EL PROCESO.

<u>Cuando el riesgo sea de corrupción:</u>

- ✓ Informar a la Alta Dirección sobre el hecho encontrado.

- ✓ De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

- ✓ Iniciar con las acciones correctivas necesarias.

- ✓ Realizar el análisis de causas y determinar acciones preventivas y de mejora.

- ✓ Análisis y actualización del mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA.

- ✓ Promover las acciones correctivas necesarias, dependiendo del riesgo materializado.
- ✓ Identificar las causas y determinar acciones preventivas y de mejora.
- ✓ Analizar y actualizar el mapa de riesgos.
- ✓ Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA

- ✓ Aplicar las orientaciones de la política de riesgos institucional. (*Verificar los niveles de aceptación del riesgo*).

De acuerdo con el seguimiento realizado es importante determinar, al final de cada vigencia, si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo.

Para poder determinarlo se analizará si no se han presentado hechos significativos como:

- Riesgos materializados relacionados con posibles actos de corrupción.
- Riesgos de gestión materializados en cualquiera de los procesos.
- Observaciones o hallazgos por parte del proceso de Control Interno o bien por parte de un ente de control, respecto de la idoneidad y efectividad de los controles.
- Cambios importantes en el entorno estratégico o normativo que puedan generar nuevos riesgos.

- Inclusión de nuevos riesgos o controles identificados por la entidad.

No obstante, los mapas de riesgos deben ser flexibles y permitir cambios cuando se requieran.

De esta forma regulamos lo concerniente con la administración del riesgo en la Empresa de servicios públicos de Acueducto y Alcantarillado de El Carmen de Bolívar ACUECAR S.A. E.S.P, esperando que este documento sirva de guía e ilustración para la administración del riesgo en general, para mejorar nuestros indicadores de resultados y disminuir los hechos que afectan el cumplimiento de nuestra misión institucional.

De esta forma, afianzamos nuestro compromiso con el sistema de gestión de la calidad, con la prevención como estrategia de gestión pública y con la satisfacción de nuestros usuarios como fin primordial de la empresa.

Atentamente,

JAIME DAVID ROA
Agente Especial