OBJETIVO

Establecer los lineamientos para la identificación, análisis, evaluación y control de los riesgos de gestión, corrupción y seguridad digital, tanto internos como externos, con enfoque preventivo y tratamiento de cada uno de ellos, que permitan a la alta dirección de la empresa Acueducto y Alcantarillado de Cúcuta, EIS CÚCUTA SA E.S.P., orientar su gestión hacia la eficiencia y transparencia con el fin de tener una seguridad razonable en el logro de sus objetivos.

ALCANCE

Los lineamientos establecidos en el presente Manual de los Riesgos de Gestión, Corrupción y Seguridad Digital aplican a todos los procesos y/o subprocesos del Sistema Integrado de Gestión de la empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. Inicia con la identificación de los riesgos y finaliza con el monitoreo, revisión, seguimiento del mapa de los riesgos y el control de los riesgos en todos los niveles organizacionales.

NORMAS LEGALES

NORMA	ARTICULO	DESCRIPCIÓN
Ley 1474 de 2011 Estatuto Anticorrupción	73	Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano; siendo uno de sus componentes el Mapa de Riesgos de Corrupción y las medidas para mitigar estos riesgos. La metodología para construir esta estrategia está a cargo del Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción, hoy Secretaría de Transparencia.
Decreto 124 de 2016 Plan Anticorrupción y de Atención al Ciudadano	Todos en especial el Artículo 2.1.4.2.	Por el cual se sustituye el título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano. Artículo 2.1.4.2. Señálense como

		metodología para diseñar y hacer seguimiento al Mapa de Riesgo de Corrupción de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el documento "Guía para la Gestión del Riesgo de Corrupción".
Decreto 1083 de 2015 Reglamentario del sector Función pública Actualización: 19 de marzo de 2019	ARTÍCULO 2.2.23.2 Actualización del Modelo Estándar de Control Interno. ARTÍCULO 2.2.21.5.4 Administración de riesgos.	La actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5º de la Ley 87 de 1993. La identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspecto tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

TÉCNICAS Y/O RELACIONADAS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción Y Seguridad Digital. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública (DAFP). Versión 4, octubre 2018.

DEFINICIONES

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

- **Consecuencia:** Efectos o situaciones resultantes de la materialización del riesgo que impacta en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Riesgo De Gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo De Seguridad Digital:** 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 personas.

- **Gestión Del Riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

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

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

- **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. Según los lineamientos contenidos en el artículo 73 de la Ley 1474 de 201110, el Mapa de Riesgos de Corrupción hace parte del Plan Anticorrupción y de Atención al Ciudadano.

- **Probabilidad.** Oportunidad de ocurrencia de un riesgo. Se mide según la frecuencia (número de veces en que se ha presentado el riesgo en un período determinado) o por la factibilidad (factores internos o externos que pueden determinar que el riesgo se presente).

- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan para generar un valor.

- **Riesgos:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos de la entidad, logrando entorpecer el desarrollo de sus funciones.

- **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 Inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgo Residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

- **Integridad:** propiedad de exactitud y completitud.

- **Tolerancia al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes, para el riesgo de corrupción la tolerancia es inaceptable.

- **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 modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

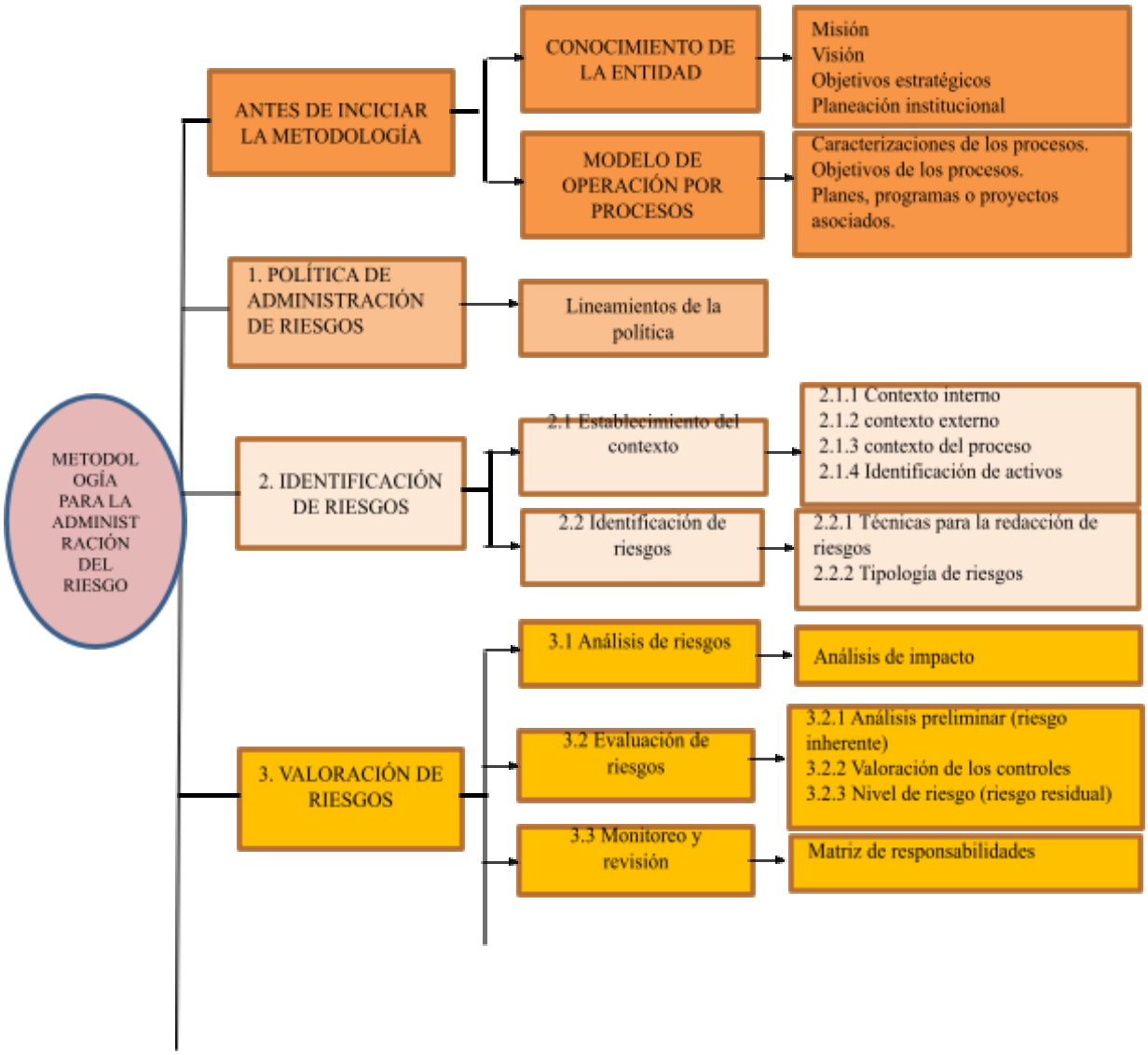
- **Apetito al Riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

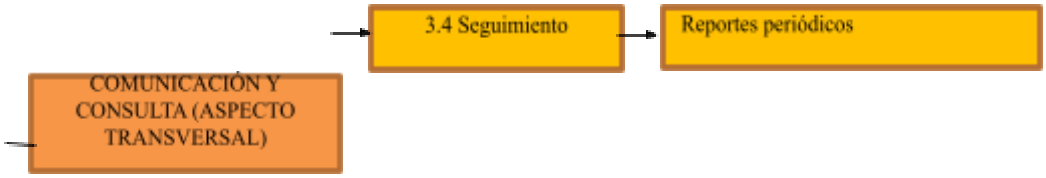
METODOLOGÍA

La empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., adopta la metodología general para la administración del riesgo, la cual se basa en la metodología definida por el DAFP en la guía para la administración de los riesgos de gestión, corrupción, seguridad digital y el

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

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





Paso 1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Alta Dirección, con el liderazgo del representante legal y con la participación de Comité Institucional de Coordinación de Control Interno, de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. en la gestión o administración del riesgo establecen lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos, utilizando mecanismos de comunicación para dar a conocer las políticas de riesgos en todos los niveles de la entidad.

NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO Establece “los niveles aceptables de desviación relativa a la consecución de los objetivos” (NTC GTC 137 Numeral 3.7.16), los mismos están asociados a la estrategia de la entidad y pueden considerarse para cada uno de los procesos. Los riesgos de corrupción son inaceptables.

TÉRMINOS Y DEFINICIONES: Aquellos relacionados con la administración del riesgo y con los temas que el manual o guía desarrollen y sean relevantes para que todos los funcionarios entiendan su contenido y aplicación.

ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Determina los siguientes aspectos:

- La metodología para utilizar.
- En caso de que la entidad haya dispuesto un software o herramienta para su desarrollo, deberá explicarse su manejo.
- Incluir los aspectos relevantes sobre los factores de riesgo estratégicos para la entidad, a partir de los cuales todos los procesos podrán iniciar con los análisis para el establecimiento del contexto.
- Incluir todos aquellos lineamientos que en cada paso de la metodología sean necesarios para que todos los procesos puedan iniciar con los análisis

correspondientes.

- Incluir la periodicidad para el monitoreo y revisión de los riesgos, así como el seguimiento de los riesgos de corrupción
- Incluir los niveles de riesgo aceptados para la entidad y su forma de manejo.
- Incluir la tabla de impactos institucional (ver tabla Niveles para calificar el impacto o consecuencias).
- Otros aspectos que la entidad considere necesarios deberán ser incluidos, con el fin de generar orientaciones claras y precisas para todos los funcionarios, de modo tal que la gestión del riesgo sea efectiva y esté articulada con la estrategia de la entidad.

Paso 2. IDENTIFICACIÓN DEL RIESGO

2.1 ESTABLECIMIENTO DEL CONTEXTO: Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo a partir de los factores que se definan, es posible establecer las causas de los riesgos a identificar.

2.1.1 ESTABLECIMIENTO DEL CONTEXTO INTERNO: Se determinan las características o aspectos esenciales del ambiente en el cual la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., busca alcanzar sus objetivos. Se pueden considerar factores como: Estructura organizacional funciones y responsabilidades, políticas, objetivos y estrategias implementadas Recursos y conocimientos con que se cuenta (económicos, personas, procesos, sistemas, tecnología, información) relaciones con las partes involucradas y la cultura organizacional.

2.1.2 ESTABLECIMIENTO DEL CONTEXTO EXTERNO: Se determinan las características o aspectos esenciales del entorno en el cual opera la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. Se pueden considerar factores como: Políticos, Económicos y Financieros, Sociales y culturales, Tecnológicos, Ambientales, Legales y reglamentarios.

2.1.3 ESTABLECIMIENTO DEL CONTEXTO DEL PROCESO: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones, de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. Se puede considerar factores como: Objetivo del proceso, Alcance del proceso, Interrelación con otros procesos, Procedimientos asociados, responsables del proceso y Activos de seguridad digital del proceso.

Factores para cada categoría del contexto:

CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, Legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas e información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (Leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.

	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo.

Para iniciar esta etapa, en primer lugar, se debe tener claridad sobre la misión institucional, sus objetivos y tener una visión sistémica de manera que no se perciba la gestión del riesgo de corrupción como algo aislado. En segundo lugar, el análisis se debe realizar a partir del conocimiento de situaciones del entorno de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. , tales como: lo social, económico, financiero, cultural, de orden público, político, legal y cambios tecnológicos, así como las fortalezas, debilidades, oportunidades y amenazas de la entidad; se alimenta también con el análisis de la situación actual de la empresa, basados en los resultados de los Componentes del Módulo de Planeación y Gestión, Estructura Organizacional, el Modelo de Operación, el cumplimiento de los Planes y Programas, los sistemas de información, los procesos y procedimientos, los recursos económicos, entre otros.
Igualmente, en esta etapa se deben identificar las relaciones entre la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., y su entorno, entender la Entidad, estrategias, capacidades y habilidades, así como identificar todos aquellos objetos (dependencias, procesos, proyectos, etc.) de la entidad, a los cuales se podría aplicar un análisis de riesgos, y así determinar sobre cuáles de ellos debe realizarse el análisis.

Para hacer el análisis del contexto se deben utilizar diferentes fuentes de información de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., tales como registros históricos, experiencias significativas registradas e informes de años anteriores, los cuales pueden proporcionar información importante.

2.1.4 IDENTIFICACIÓN DE ACTIVOS

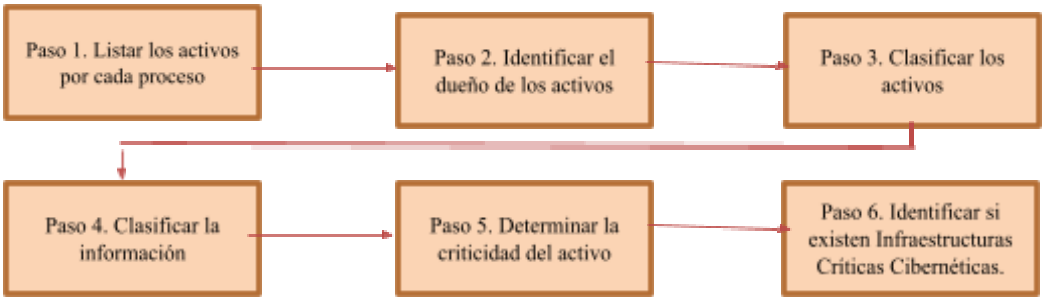
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., servicios Web, redes, información física o digital, tecnologías de la Información TI- o Tecnologías de la operación -TO-) que utiliza la organización para su funcionamiento.

Es necesario que la entidad pública identifique los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa

–Líderes de Proceso, en cada proceso 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 entidad pública.

Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:



1. **Listar los activos por cada proceso:** En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno.

2. **Identificar el dueño de los activos:** Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

3. **Clasificar los activos:** Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

4. **Clasificar la información**: Realizar la clasificación de 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.

5. **Determinar la criticidad del activo (Valoración del Activo):** Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

   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. Para definir estas escalas puede tomar como referencia la Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información (MSPI), estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

6. **Identificar si existen Infraestructuras Críticas Cibernéticas -ICC:** Se invita a que las entidades públicas identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

2.2. IDENTIFICACIÓN DE RIESGOS - TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS.

En esta etapa 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, las necesidades de las partes involucradas de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. y del proceso, que pueden afectar el logro de los objetivos.

Los pasos que comprende esta etapa son los siguientes:

Establecimiento Del Contexto Y La Identificación De Riesgos.

Las preguntas claves para la identificación del riesgo permiten determinar:

¿**QUÉ PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.
¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo.

Construcción Del Riesgo De Corrupción.

Los riesgos de corrupción se establecen sobre los procesos de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición. En la descripción de los riesgos de corrupción deben concurrir TODOS los componentes de su definición: **Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier…	X	X	X	X

Generalidades Acerca De Los Riesgos De Corrupción

- **Entidades encargadas de gestionar el riesgo:** la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. lo deben adelantar como entidad de orden municipal.
- **Elaboración:** anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.
- **Consolidación:** la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

- **Publicación del mapa de riesgos de corrupción:** se debe publicar en la página web de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., 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 será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014.
  En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación. Recordando que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- **Socialización:** Los servidores públicos y contratistas de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción. Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- **Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Monitoreo**: en concordancia con la cultura del autocontrol al interior de la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P., los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- **Seguimiento:** el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

2.2.1 TÉCNICAS PARA LA REDACCIÓN DE RIESGOS

Evitar iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”,

“insuficiente”, “deficiente”, “debilidades en…” Generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo.

2.2.2 TIPOLOGÍA DE RIESGOS

Riesgos Estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos Operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

Riesgos Gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

Riesgos Financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos Tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Riesgos De Cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgo De Imagen O Reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas. Riesgos de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgos De Seguridad Digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Ejemplos de descripción del riesgo:
Formato De Descripción Del Riesgo De Gestión

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	La combinación de factores como insuficiente capacitación del personal de contratos, cambios en la regulación contractual, inadecuadas políticas de operación y carencia de controles en el procedimiento de contratación pueden ocasionar inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad y, en consecuencia, afectar la continuidad de su operación.	Operativo	Carencia de controles en el procedimiento de contratación Insuficiente capacitación del personal de contratos Desconocimiento de los cambios en la regulación contractual Inadecuadas políticas de operación.	1. Parálisis en los procesos 2. Incumplimiento en la entrega de bienes y servicios a los grupos de valor 3. Demandas y demás acciones jurídicas 4. Detrimento de la imagen de la entidad ante sus grupos de valor 5. Investigaciones disciplinarias

Fuente: Departamento Administrativo de la Función Pública.

Formato De Descripción Del Riesgo De Corrupción

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin celebrar un contrato.	Situaciones como: debilidades en la etapa de la planeación del contrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, la falta de conocimiento y/o experiencia, sumados a la falta de integridad pueden generar un riesgo de corrupción en la contratación, como por	Corrupción	Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente. Presiones indebidas Carencia de controles en el procedimiento de contratación.	1. Pérdida de la imagen institucional. 2. Demandas contra el Estado. 3. Pérdida de confianza en lo público. 4. Investigaciones penales, disciplinarias y fiscales. 5. Detrimento patrimonial.

	ejemplo "exigencias de condiciones en los procesos de selección que solo cumple un determinado proponente"		Falta de conocimiento y/o experiencia del personal que maneja la contratación. Excesiva discrecionalidad. Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente.	6. Obras inconclusas. 7. Mala calidad de las obras. 8. Enriquecimiento ilícito de contratistas y/o servidores públicos.

Fuente: Secretaría de Transparencia de la Presidencia de la República

Procesos, Procedimientos O Actividades Susceptibles De Riesgos De Corrupción.

A manera de ilustración se señalan algunas actividades susceptibles de riesgos de corrupción, a partir de los cuales la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. podrá incluir otros que considere pertinentes:

Direccionamiento Estratégico (Alta Dirección).

- Concentración de autoridad o exceso de poder.
- Extralimitación de funciones.
- Ausencia de canales de comunicación.
- Amiguismo y clientelismo.

Financiero (Está Relacionado Con Áreas De Planeación Y Presupuesto)

- Inclusión de gastos no autorizados.
- Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
- Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
- Inexistencia de archivos contables.
- Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

De Contratación (Como Proceso O Bien Los Procedimientos Ligados A Este).

- Estudios previos o de factibilidad deficientes.
- Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
- Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
- Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
- Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.
- Urgencia manifiesta inexistente.
- Otorgar labores de supervisión a personal sin conocimiento para ello.
- Concentrar las labores de supervisión en poco personal.
- Contratar con compañías de papel que no cuentan con experiencia.

De Información y Documentación

- Ausencia o debilidad de medidas y/o políticas de conflictos de interés.
- Concentración de información de determinadas actividades o procesos en una persona.
- Ausencia de sistemas de información.
- Ocultar la información considerada pública para los usuarios.
- Ausencia o debilidad de canales de comunicación
- Incumplimiento de la Ley 1712 de 2014.

De Investigación y Sanción

- Ausencia o debilidad de canales de comunicación.
- Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este.
- Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
- Exceder las facultades legales en los fallos.

De Trámites Y/O Servicios Internos Y Externos

- Cobros asociados al trámite.
- Influencia de tramitadores
- Tráfico de influencias: (amiguismo, persona influyente).
- Demorar su realización.

De Reconocimiento De Un Derecho (Expedición De Licencias Y/O Permisos)

- Falta de procedimientos claros para el trámite.
- Imposibilitar el otorgamiento de una licencia o permiso.
- Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
- Tráfico de influencias: (amiguismo, persona influyente).

Riesgo De Seguridad Digital

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: **"Integridad, confidencialidad o disponibilidad"**
Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.
Es importante tener en cuenta que la descripción del riesgo consolida los pasos vistos en la metodología de gestión del riesgo y facilita su análisis, tipo de riesgo, activo, descripción del riesgo, amenaza, tipo, causas/ vulnerabilidades y sus consecuencias.

Formato De Descripción Del Riesgo De Seguridad Digital

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos	Pérdida de la	La falta de políticas de seguridad digital, ausencia de políticas de	Modificación no autorizada	Seg	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la

de nómina	integrida d	control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.		u r i d a d d i g i t a l	Ausencia de políticas de control de acceso	entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Contraseñas sin protección	
					Autenticación débil	

Paso 3. VALORACIÓN DE RIESGOS

3.1 ANÁLISIS DE RIESGOS.

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

3.1.1 ANÁLISIS DE CAUSAS.

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

3.1.2 DETERMINACIÓN DE LA PROBABILIDAD.

Por **Probabilidad** se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida 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 se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el criterio de **Factibilidad** 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 es posible que se dé.

Cálculo de la probabilidad e impacto

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.

Criterios Para Calificar la probabilidad

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.

En caso de que la entidad no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar en privado el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad.

N.º	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias	5	4	3	5	3	4	24	4 PROBABLE

2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.									
3	Otros riesgos	El evento podrá ocurrir en algún momento									
Convenciones: N.º: número consecutivo del riesgo - P1: participante 1 P… - Tot: total puntaje - Prom.: promedio											

3.1.3 DETERMINAR CONSECUENCIAS O NIVEL DE IMPACTO.

Impacto. Son las consecuencias o efectos que puede ocasionar a la Empresa Acueducto y Alcantarillado de Cúcuta SA E.S.P. la materialización del riesgo.
El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

Estimar El Nivel Del Riesgo Inicial – Inherente
Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, teniendo en cuenta las tablas establecidas en cada caso.
Para su determinación se utiliza la matriz de calificación del riesgo.

Criterios Para Calificar El Impacto – Riesgos De Gestión.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
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 terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información 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.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

La Empresa de Acueducto y Alcantarillado de Cúcuta SA E.S.P. deberá adaptar los criterios a su realidad. El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

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 establecimiento del contexto externo de la entidad, es decir que la consideración de población va a estar asociada a las personas a las cuales 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 en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesta 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 estará también alineada 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.

Ejemplo:

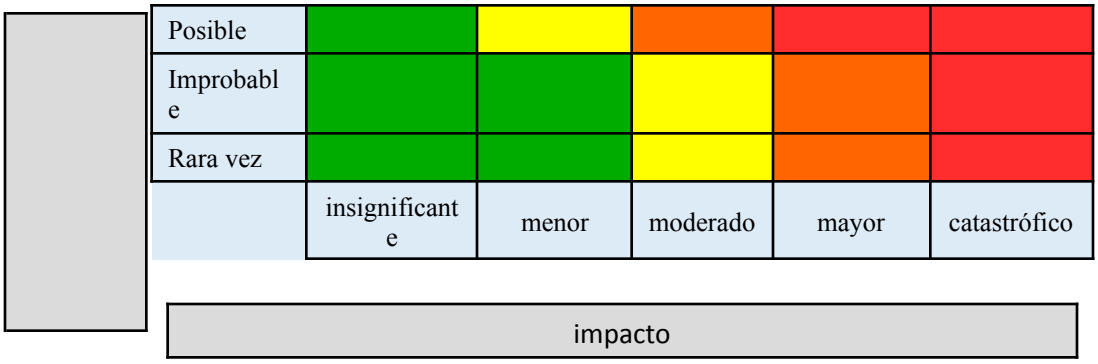
RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004

Extremo	Alto	Moderado	Bajo

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

probabilidad de ocurrencia	MAPA DE CALOR					
	Casi seguro					
	Probable					



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. 2017.

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. Para el ejemplo que venimos explicando, el impacto fue identificado como mayor por cuanto genera interrupción de las operaciones por más de dos días.

Tratándose de riesgos de corrupción el impacto siempre será negativo; en este orden de ideas, no aplica la descripción de riesgos insignificante o menores señalados en la Guía de Función Pública, sino solos los criterios descritos a continuación:

IMPACTO		
DESCRIPTOR	**DESCRIPCIÓN**	**NIVEL**
Moderado	Afectación parcial al proceso y a la dependencia. Genera medianas consecuencias para la entidad.	5
Mayor	Impacto negativo de la entidad. Genera altas consecuencias para la entidad.	10
Catastrófico	Consecuencias desastrosas sobre el sector. Genera consecuencias desastrosas para la entidad.	20

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la entidad. Es por ello, que para facilitar la asignación del puntaje se debe responder el siguiente cuestionario:

CUESTIONARIO PARA DETERMINAR EL IMPACTO			
N°	PREGUNTA. SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	SI	NO
1	¿Afectar el 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 de 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 o servicios o los 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?		
Total preguntas afirmativas: _____		**Total preguntas negativas: _____**	
Clasificación del Riesgo: Moderado ___ Mayor ___ Catastrófico ___		**Puntaje: _____**	

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

De acuerdo con el número de preguntas afirmativas contestadas del cuestionario, se determina el impacto del riesgo de corrupción, siguiendo las especificaciones descritas a continuación:

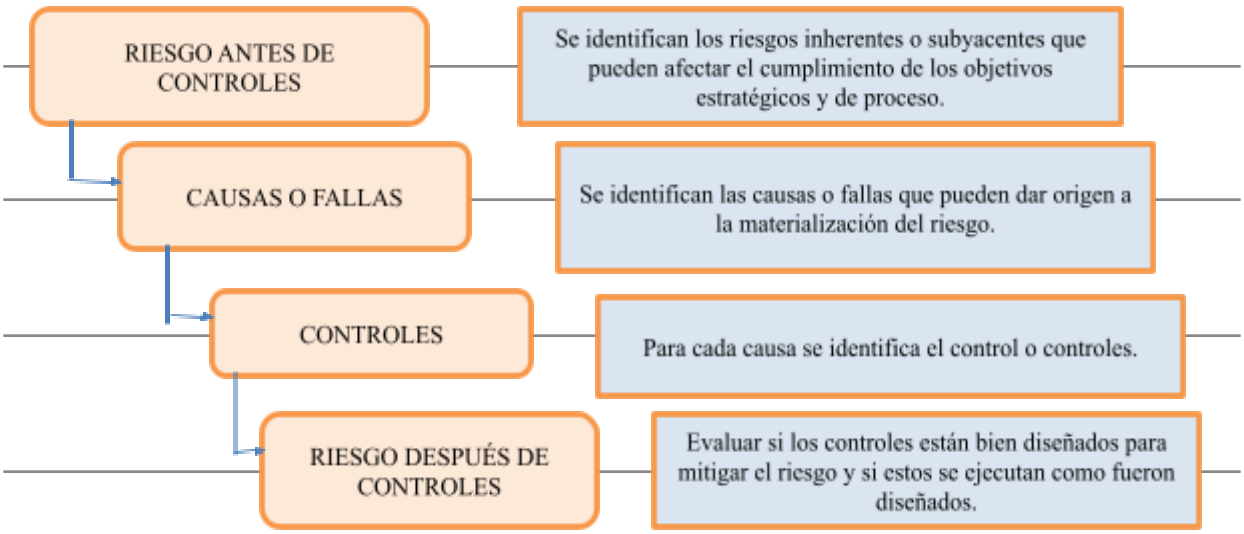
CALIFICACIÓN DE RIESGO DE CORRUPCIÓN IMPACTO		
RESPUESTAS	**DESCRIPCIÓN**	**NIVEL**
1 - 5	Moderado	5
6 - 11	Mayor	10
12 - 18	Catastrófico	20

Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas. 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.

3.2 EVALUACIÓN DE RIESGOS.

3.2.1 RIESGO ANTES Y DESPUÉS DE CONTROLES

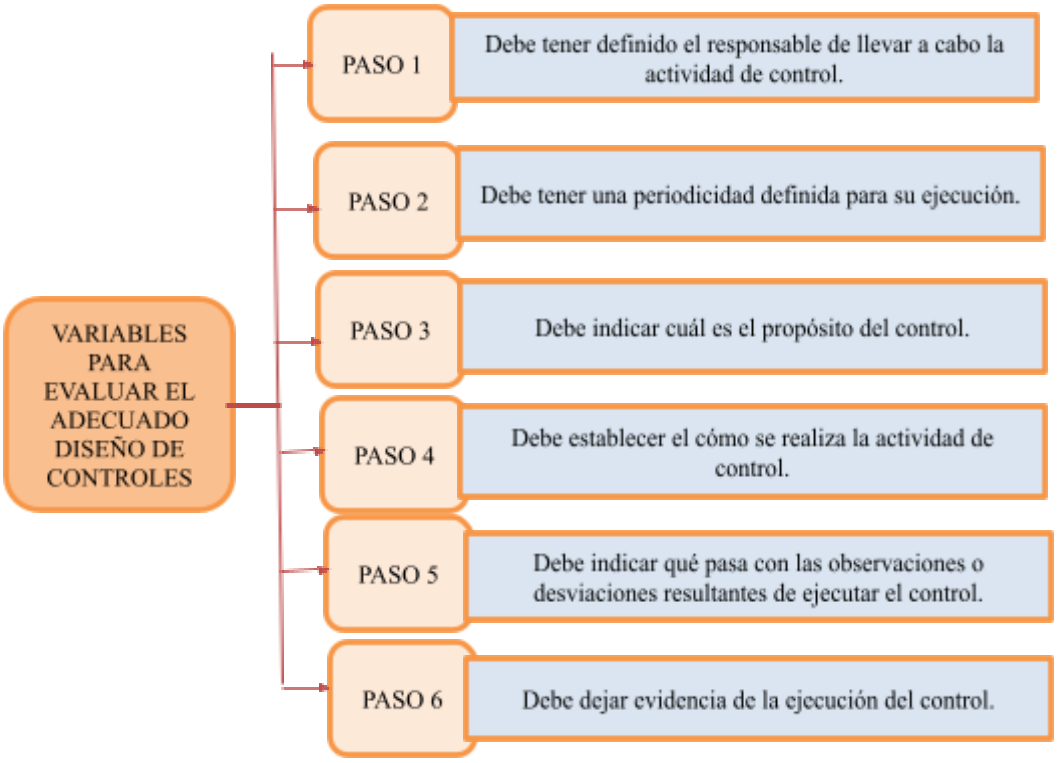
Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.



3.2.2 VALORACIÓN DE LOS CONTROLES – DISEÑO DE CONTROLES

Antes de valorar los controles es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes:
¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo?
Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción de este, las siguientes variables:

Pasos para diseñar un control



Las acciones de tratamiento se agrupan en:

- Disminuir la probabilidad: acciones encaminadas a gestionar las causas del riesgo
- Disminuir el impacto: acciones encaminadas a disminuir las consecuencias del riesgo

PASO 1: Debe tener definido el responsable de llevar a cabo la actividad de control.

RESPONSABLE: Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes

individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

* El control debe iniciar con un cargo responsable o un sistema o aplicación.
* Evitar asignar áreas de manera general o nombres de personas.
* El control debe estar asignado a un cargo específico.

PASO 2: Debe tener una periodicidad definida para su ejecución.

PERIODICIDAD: El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo. Una vez definido el paso 1 - responsable del control, debe establecerse la periodicidad de su ejecución.
Cada vez que se releva 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.
Hay controles que no tienen una periodicidad específica como, por ejemplo, los controles que se ejecutan en el proceso de contratación de proveedores solo se ejecutan cuando se contratan proveedores. La periodicidad debe quedar redactada de tal forma que indique: que cada vez que se desarrolla la actividad se ejecuta el control.

PASO 3: Debe indicar cuál es el propósito del control

PROPÓSITO: El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito del control, es decir, lo que este busca.

PASO 4: Debe establecer el cómo se realiza la actividad de control

CÓMO SE REALIZA: El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable.

Ej.: para verificar los requisitos que debe cumplir un proveedor en el momento de ser contratado es mejor utilizar una lista de chequeo que hacerlo de memoria, dado que se nos puede quedar algún requisito por fuera.

PASO 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.

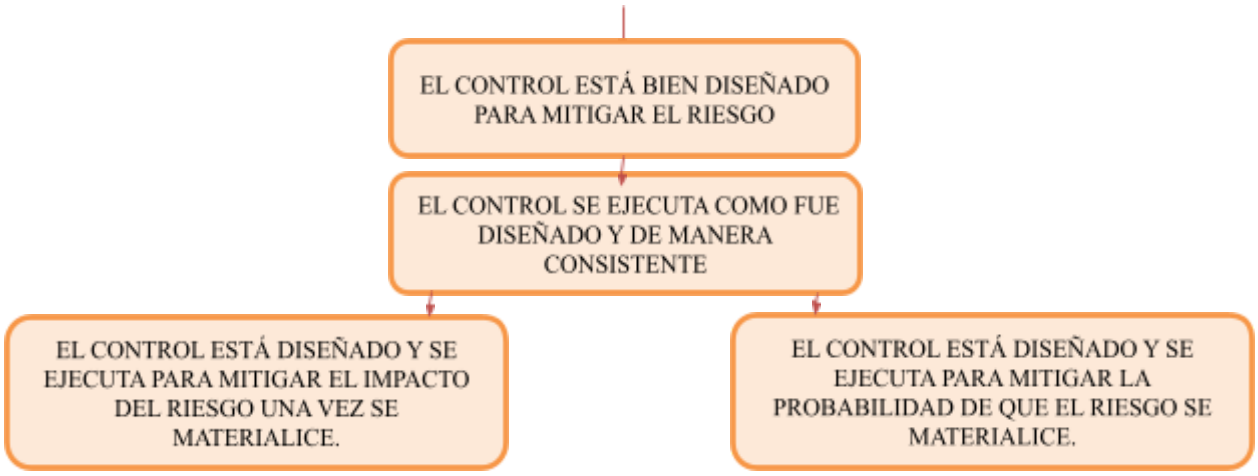
QUÉ PASA CON LAS OBSERVACIONES O DESVIACIONES: El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

PASO 6: Debe dejar evidencia de la ejecución del control

EVIDENCIA: El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo con la periodicidad definida
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

Valoración de los controles para la mitigación de los riesgos



Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Análisis y evaluación de los controles para la mitigación de los riesgos.
Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:

CRITERIO DE EVALUACIÓN	ASPECTO PARA EVALUAR EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. 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
2. 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

3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola 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
4. 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
5. 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.
6. 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 para la mitigación del riesgo:

CRITERIO DE EVALUACIÓN	OPCIONES DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente.	0
6. Evidencia de la ejecución del control	Completa	10

	Incompleta	5
	No existe	0

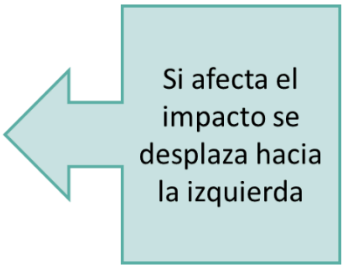
Resultados de la evaluación del diseño del control

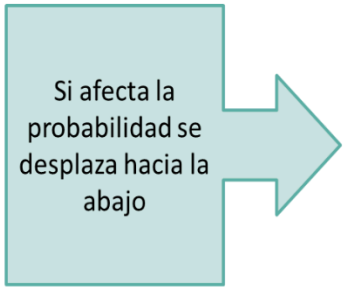
El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

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

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

RESULTADOS DE LA CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN				
Probabilidad	**Puntaje**	**Zona de Riesgo de corrupción**		
Casi seguro	5	25 - Moderada	40 - Alta	100 - Extrema
Probable	4	20 - Moderada	40 - Alta	80 - Extrema
Posible	3	15 - Moderada	30 - Alta	60 - Extrema
Improbable	2	10 - Baja	20 - Moderada	40 - Alta
Rara vez	1	5 - Baja	10 - Baja	20 - Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20





RESULTADOS DE LA CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN				
Probabilidad	**Puntaje**	**Zona de Riesgo de corrupción**		
Casi seguro	5	25 - Moderada	40 - Alta	100 - Extrema
Probable	4	20 - Moderada	40 - Alta	80 - Extrema
Posible	3	15 - Moderada	30 - Alta	60 - Extrema
Improbable	2	10 - Baja	20 - Moderada	40 - Alta
Rara vez	1	5 - Baja	10 - Baja	20 - Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20

RESULTADOS DE LA CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN				
Probabilidad	**Puntaje**	**Zona de Riesgo de corrupción**		
Casi seguro	5	25 - Moderada	40 - Alta	100 - Extrema
Probable	4	20 - Moderada	40 - Alta	80 - Extrema
Posible	3	15 - Moderada	30 - Alta	60 - Extrema
Improbable	2	10 - Baja	20 - Moderada	40 - Alta
Rara vez	1	5 - Baja	10 - Baja	20 - Moderada
Impacto		Moderado	Mayor	Catastrófico
Puntaje		5	10	20

Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría o control interno.

RANGO DE CALIFICACIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL

DE LA EJECUCIÓN	CONTROL
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable

Análisis Y Evaluación De Los Controles Para La Mitigación De Los Riesgos

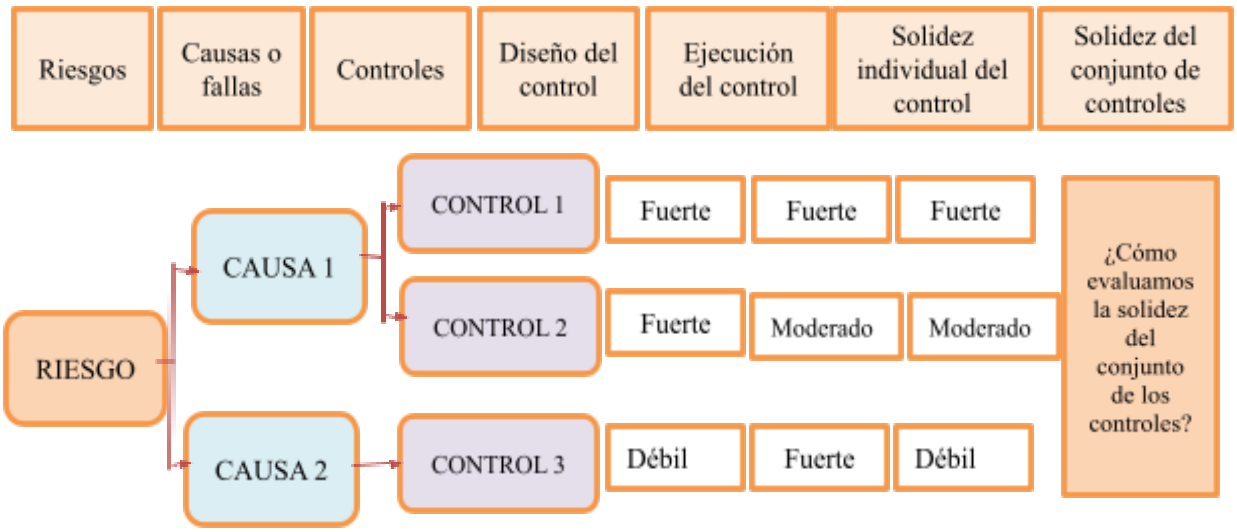
Dado que la calificación de riesgos inherentes y residuales se efectúa al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.

En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE: 100 MODERADO: 50 DÉBIL: 0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
fuerte: calificación entre 96 y 100”	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Solidez Del Conjunto De Controles Para La Adecuada Mitigación Del Riesgo

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.



CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

3.2.3 NIVEL DE RIESGO (RIESGO RESIDUAL)

Desplazamiento del riesgo inherente para calcular el riesgo residual dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.

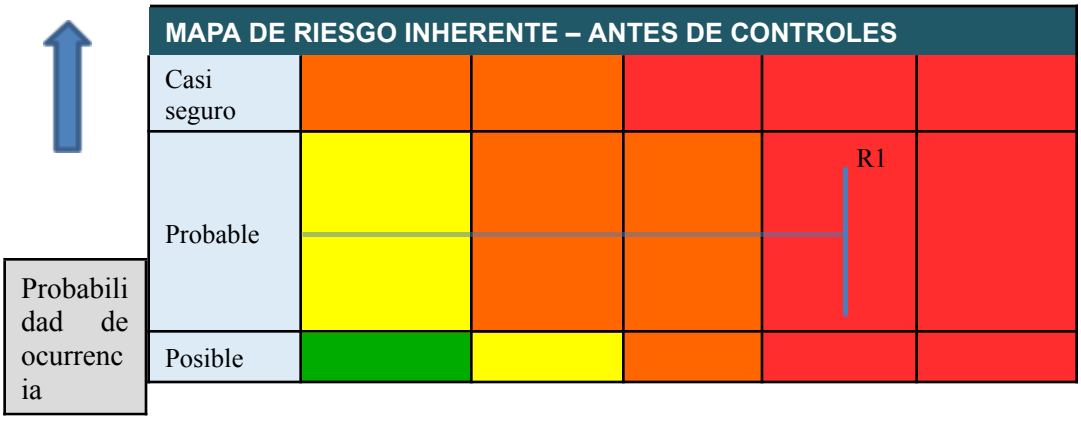
SOLIDEZ DEL	CONTROLES AYUDAN A	CONTROLES AYUDAN A	# COLUMNAS EN LA MATRIZ DE	# COLUMNAS EN LA MATRIZ DE

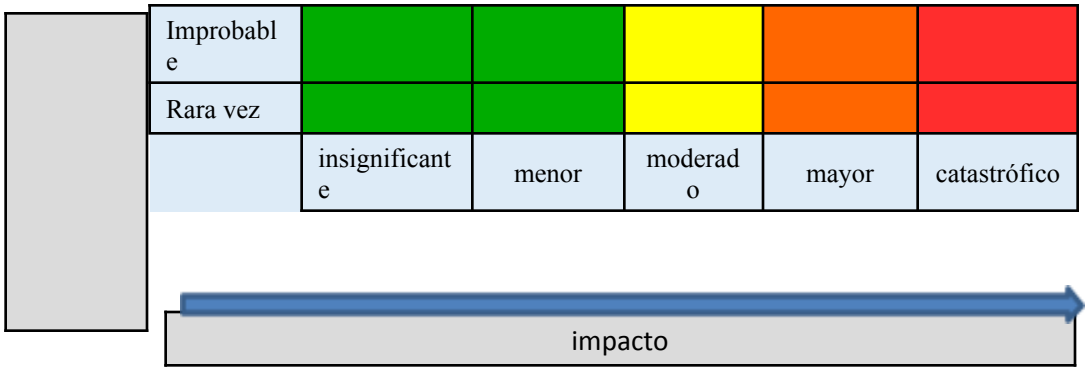
CONJUNTO DE LOS CONTROLES .	DISMINUIR LA PROBABILIDAD	DISMINUIR IMPACTO	RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

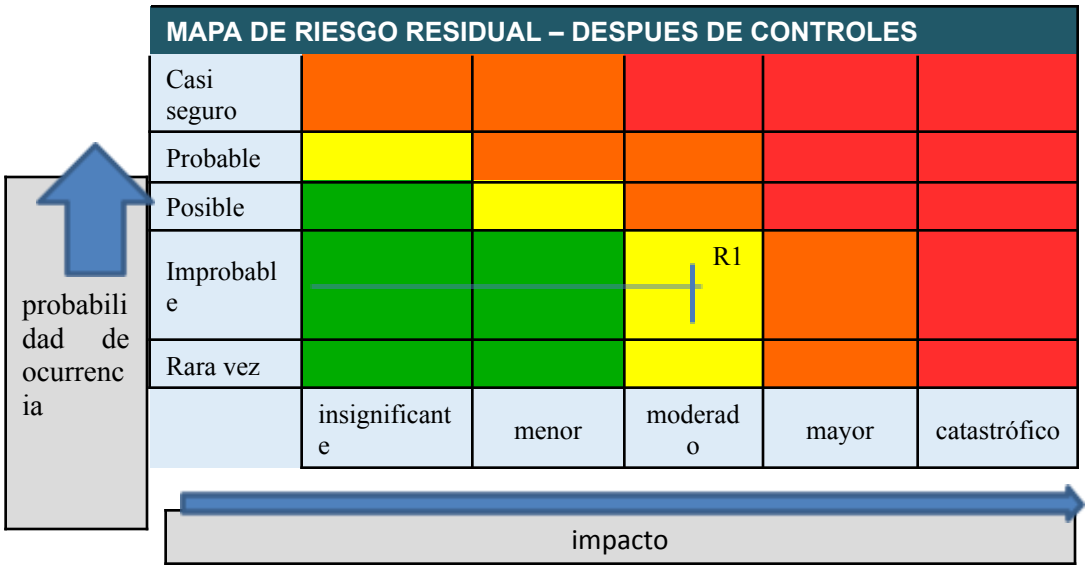
Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Resultados Del Mapa De Riesgo Residual.
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).
Tenemos el riesgo 1 con una calificación de riesgo inherente de probabilidad e impacto como se muestra en la siguiente gráfica:
Como podemos observar, es probable que el riesgo suceda y, en caso de materializarse, tiene un impacto mayor para la entidad. Ahora, supongamos que existen controles bien diseñados, que siempre se ejecutan, y que estos controles disminuyen de manera directa la probabilidad.



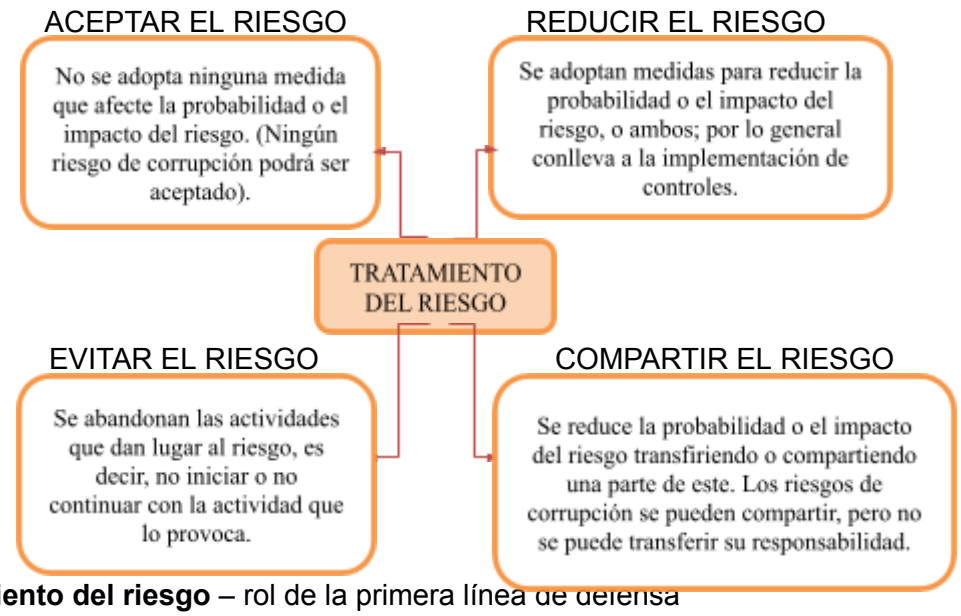




Tratamiento Del Riesgo

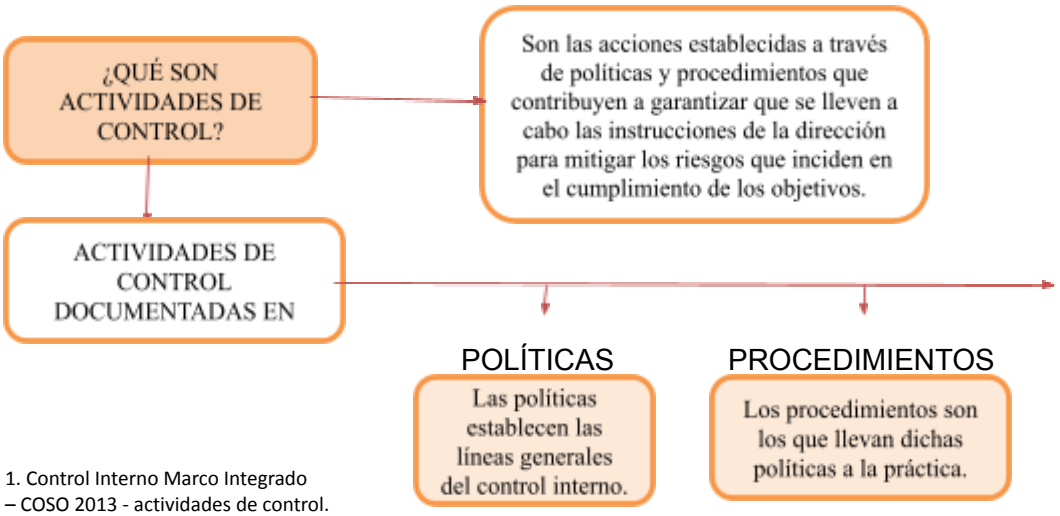
Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los

riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

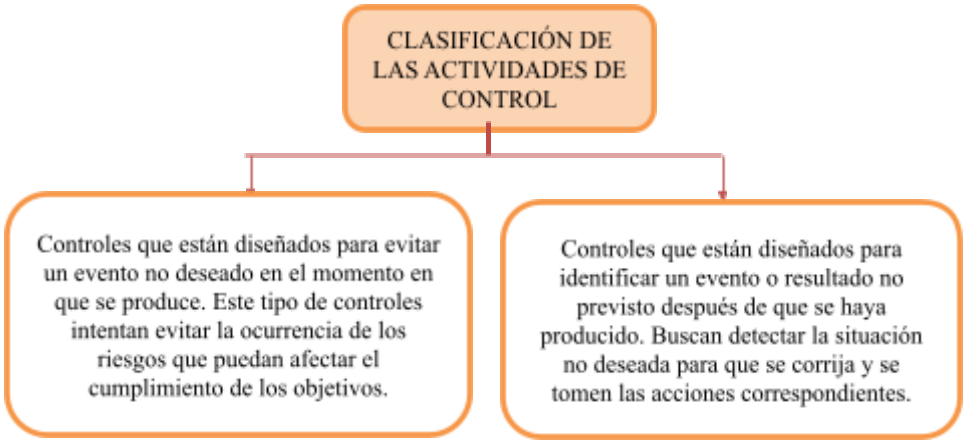


Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



1. Control Interno Marco Integrado – COSO 2013 - actividades de control.



3.3 MONITOREO Y REVISIÓN

¿Por qué debo monitorear y revisar la gestión de riesgos?
Porque la entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El modelo integrado de plantación y gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control.

¿Cómo se define el modelo de las líneas de defensa?
Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

¿Quiénes son los asignados para monitorear y revisar la gestión de riesgos y cuáles son sus roles?
El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG de “Control interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

LÍNEA ESTRATÉGICA
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el

comité institucional de coordinación de control interno.

1ª. LÍNEA DE DEFENSA	2ª. LÍNEA DE DEFENSA	3ª. 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.	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	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
A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. 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.	A cargo de los 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 entidad, comités de riesgos (donde existan), comités de contratación, entre otros. Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.	A cargo de la oficina de control interno, auditoría interna o quien haga sus veces. El rol principal: proporcionar un aseguramiento basado en el más alto nivel de 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.

Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control

LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno.	
Actividades de monitoreo y revisión a realizar	La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ■ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ■ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ■ Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. ■ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ■ Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo con las políticas de tolerancia establecidas y aprobadas. ■ Revisar los informes presentados por lo menos cada trimestre de 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.

Rol de la primera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

1ª. 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. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.	
Actividades de monitoreo y revisión a realizar	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ■ 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. ■ 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.

Rol de la segunda línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

2ª. LÍNEA DE DEFENSA	
Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.).	
Actividades de monitoreo y revisión a realizar	Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ 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 solicitar y apoyar en la actualización de las matrices de riesgos. ■ 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 el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos. ■ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. ■ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.

	■ 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 que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

Rol de la tercera línea de defensa en el monitoreo y revisión de los riesgos y actividades de control

3ª. LÍNEA DE DEFENSA	
Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por la oficina de control o auditoría Interno.	
Actividades de monitoreo y revisión a realizar	La oficina de control o auditoría interno monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente: ■ 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 estos. ■ 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 con los resultados de las auditorías realizadas. ■ Para mitigar los riesgos de los procesos 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.

Monitoreo De Riesgos De Corrupción

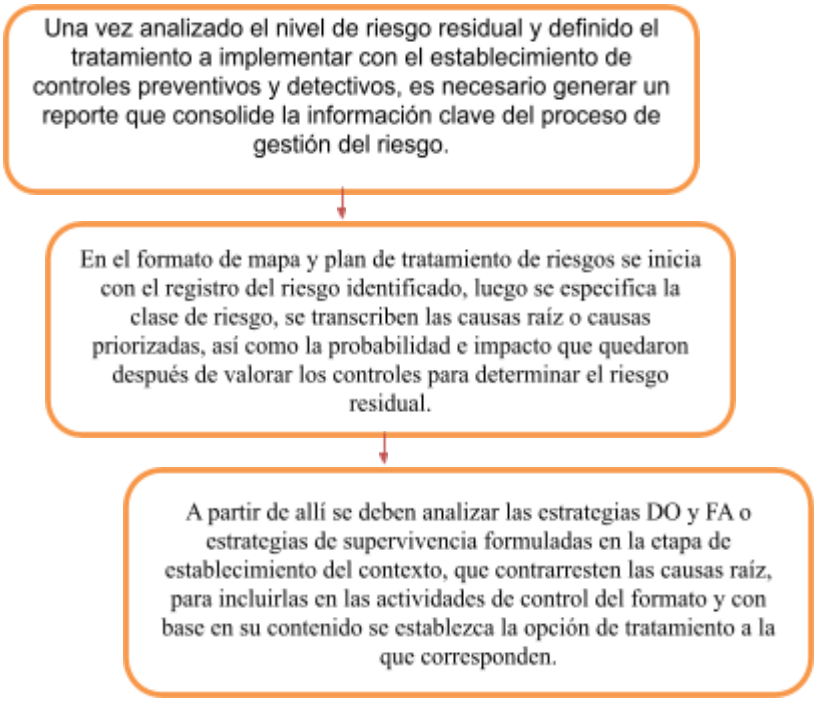
Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

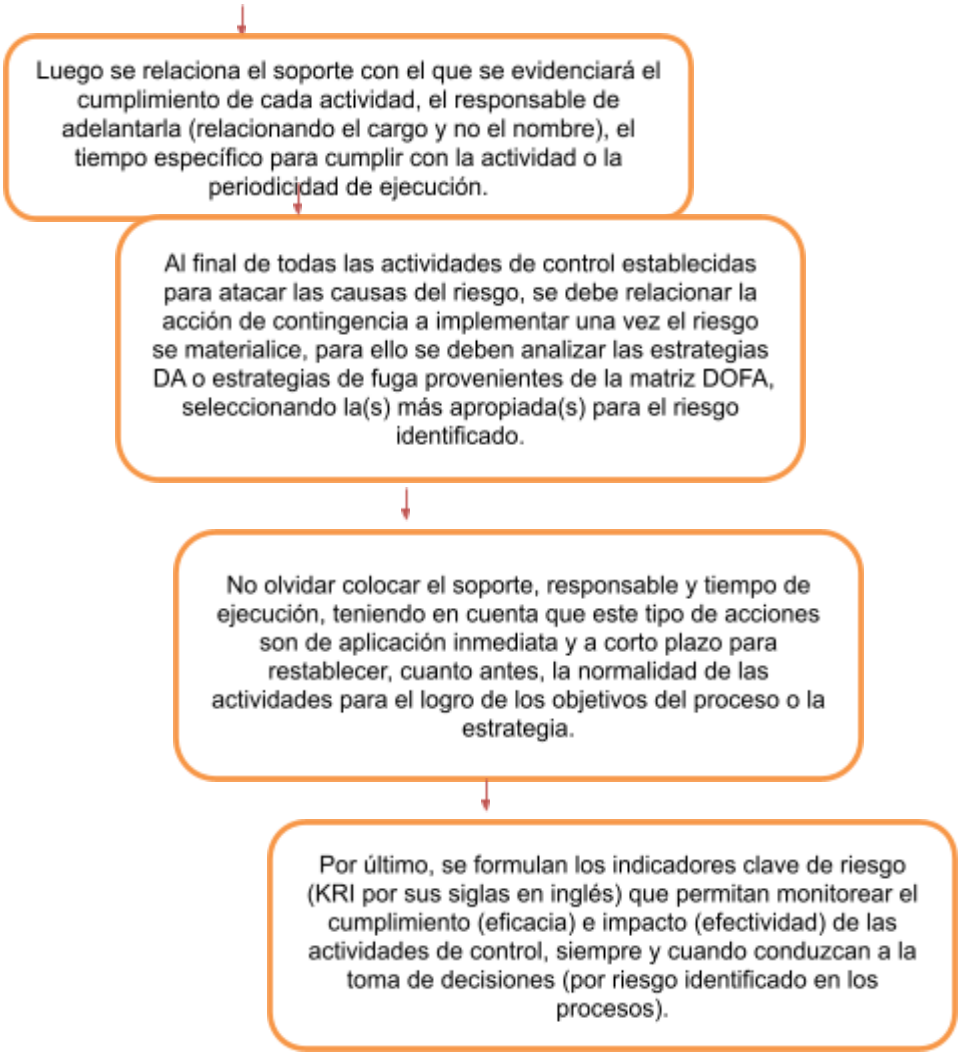
Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

Reporte del Plan de Tratamiento de Riesgos

Consolidar información para la gestión del riesgo





Reporte De La Gestión Del Riesgo

La primera línea de defensa reporta a la segunda línea de defensa el estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportada por la segunda línea de defensa (encargado de la gestión del riesgo) hacia la alta dirección.

Formato mapa y plan de tratamiento de riesgos

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
1	Desabastecimiento de bienes y servicios requeridos por la entidad	Financiero	Desactualización de la base de datos	Improbable	Mayor	Moderado	Reducir	D2O1: Adquirir software para mantener actualizada la base de datos de proveedores y el registro de contrataciones.	Contrato y factura software	Director de T.I. y jefe contratos	Primer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= ((# de casos de desabastecimiento presentados periodo actual - # de casos de desabastecimiento presentados periodo anterior) / # de casos de desabastecimiento presentados periodo anterior) x 100

			Insuficiente capacitación				Reducir	D1O2: Realizar convenios con entidades educativas para capacitar al personal de contratos.	Convenios firmados	Director financiero	Trimestralmente Del 01012018 al 31122018	
			Cambios en la regulación contable y presupuestal				Reducir	F2A1: Establecer mayor frecuencia de reinducción para actualizar al personal ante los cambios normativos contables.	Circular interna	Director talento humano	Del 01012018 al 31012018	
							Reducir	F2A1: Realizar reinducciones para actualizar al personal ante los cambios normativos contables.	Actas reinducción	Jefe cart	Trimestralmente Del 01012018 al 31122018	

									era		
			Hacke o				Reducir	F1A2: Fortalecer los Firewall en la red de la organización para detectar posibles incursiones	Reporte cumplimiento Firewall fortalecido	Director de T.I.	Del 01022018 al 28022018	
							Acción de contingencia	D1,2A1,2: D1,2A1,2: Convocar en forma extraordinaria un comité Institucional de coordinación de control interno para analizar y aplicar medidas inmediatas que, dentro de la legalidad, permitan el reabastecimiento inmediato de bienes y servicios.	Acta de comité de coordinación institucional de control interno firmada	Director financiero	1 semana una vez el riesgo se materialice	

Reporte De La Gestión Del Riesgo De Corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Formato mapa y plan de tratamiento de riesgos

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para celebrar un contrato	Corrupción	Debilidades en la etapa de planeación	Probable	Catastrófico	Extremo	Reducir	Manual de contratación implementado con parámetros técnicos y financieros para cada tipo de contratación, formalizado en procedimiento.	Manual de contratación	Director de T. I. y jefe de contratos	Primer trimestre de...	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= ((# de casos de favorecimiento a proponentes presentados periodo actual - # de casos de favorecimiento a proponentes presentados periodo anterior) / # de casos de favorecimiento a proponentes presentados periodo anterior) x 100

			Presiones indebidas				Reducir	Comité de contratación	Acto administrativo conformando comité	Director financiero	Trimestralmente Del…	
			Carencia de controles en el procedimiento de contratación				Reducir	Difusión y capacitación a todos los funcionarios del proceso.	Actas de capacitación	Director talento humano	Del (día /mes/ año) al (día / mes/año)	
							Acción de	Iniciar la investigación disciplinaria, fiscal o remitir a las instancias correspondientes para el proceso penal.	Comunicación iniciando o remitiendo investigación	Jefe cont	1 semana una vez el riesgo de iliquidez se materialice	

							contingencia			rol disciplinario interno		

Reporte De La Gestión Del Riesgo De Seguridad Digital

Así mismo, en el caso de los riesgos de seguridad digital se debe reportar en el mapa y planes de tratamiento. El responsable de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte como para la gestión y el tratamiento de estos riesgos.

Formato mapa y plan de tratamiento de riesgos de seguridad digital

N.	RIESGO	ACTIVO	[illegible]	[illegible]	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR

	Pérdida de la integridad	Base de datos de nómina	Seguridad digital	Incidentes de seguridad digital	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	**EFICACIA:** Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
					Contraseñas sin protección				Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
					Ausencia de mecanismos de identificación y autenticac				Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina	Tercer trimestre de 2018	

				ión de usuarios							TI		
				"Ausencia de bloqueo"				Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

Indicadores - gestión del riesgo de seguridad digital

Igualmente, en el caso de los riesgos de seguridad digital se deben generar indicadores para medir la gestión realizada en cuanto a la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.

1 indicador de efectividad para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

EFICACIA: Porcentaje de controles implementados = (#controles implementados / #controles definidos) x 100

EFECTIVIDAD: # Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) = ((# de incidentes de confidencialidad en el periodo actual - # de incidentes de confidencialidad en el periodo previo) / Incidentes de confidencialidad en el periodo previo) * 100%.) * 100%.

implementados / #controles definidos) x 100
EFECTIVIDAD: # Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)
Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) = ((# de incidentes de confidencialidad en el periodo actual - # de incidentes de confidencialidad en el periodo previo) / Incidentes de confidencialidad en el periodo previo) * 100%.

3.4 SEGUIMIENTO DE RIESGOS DE CORRUPCIÓN

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 Empresa de Acueducto y Alcantarillado de Cúcuta SA E.S.P., o en un lugar de fácil acceso para el ciudadano

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la Empresa de Acueducto y Alcantarillado de Cúcuta SA E.S.P.
- 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.

Acciones para seguir en caso de materialización de 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.

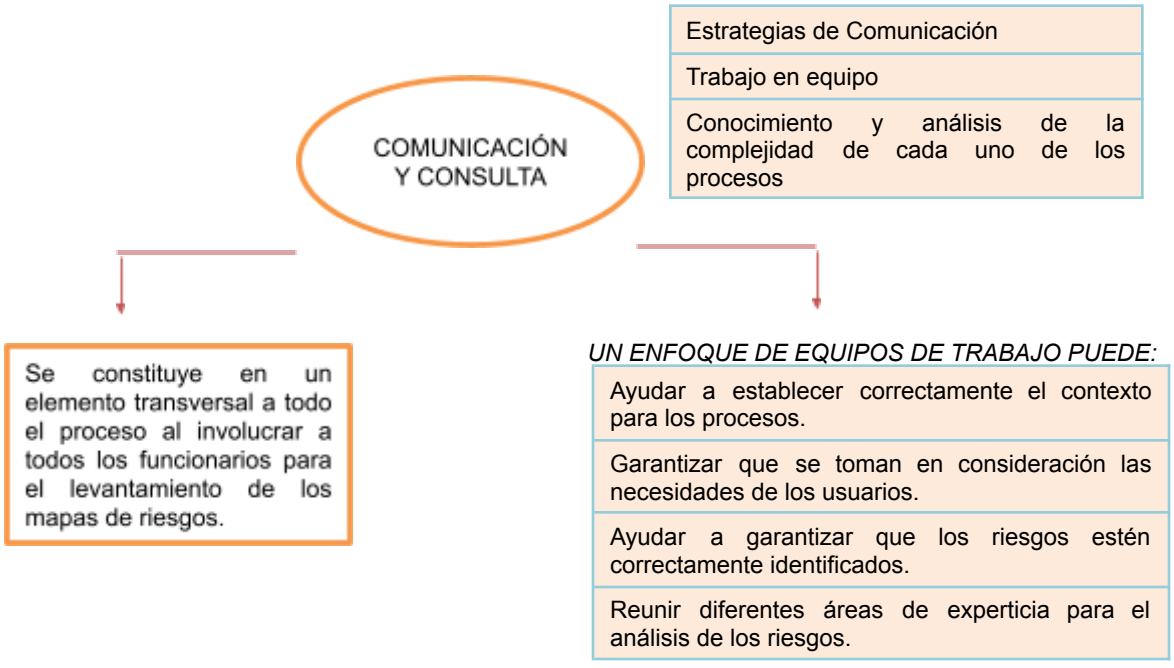
La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.
Las acciones adelantadas se refieren a:

- 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.

Comunicación Y Consulta

La comunicación y consulta con las partes involucradas, tanto internas como externas, debería tener lugar durante todas las etapas del proceso para la gestión del riesgo.
Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Comunicación y consulta – Aspecto transversal



Garantizar que los diferentes puntos de vista se toman en consideración adecuadamente durante todo el proceso.
Fomentar la administración del riesgo como una actividad inherente al proceso de planeación estratégica.

Información, comunicación y reporte

Responsabilidades por la línea de defensa para la Información, comunicación y reporte.

LÍNEA ESTRATÉGICA Corresponde al Comité de Auditoría de las Empresas Industriales y Comerciales del Estado y/o a los comités institucionales de coordinación de control interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
PRIMERA LÍNEA DE DEFENSA Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
SEGUNDA LÍNEA DE DEFENSA 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.
TERCERA LÍNEA DE DEFENSA Les 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 Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la organización pública.

4 RECURSOS

4.1 TALENTO HUMANO

Funcionarios competentes con base en la educación, formación, habilidades y experiencia apropiadas, de acuerdo con los perfiles establecidos en el Manual específico de funciones y competencias laborales y contratistas con la capacidad de ejecutar el objeto del contrato y que hayan demostrado la idoneidad y experiencia que garanticen la efectiva prestación del servicio.

4.2 EQUIPOS

Equipos de cómputo, impresoras, software de oficina e internet.

4.3 INSUMOS

- **Información primaria:** La generada por otras entidades del Estado, especialmente el Departamento Administrativo de la Función Pública - DAFP, la Contraloría General de la República – CGR y demás entes de control y todas las entidades que suministren información que pueda afectar el proceso.
- **Información secundaria***:* La generada al interior de la Empresa de Acueducto y Alcantarillado de Cúcuta SA E.S.P., que permita la identificación, análisis y valoración de los riesgos como son caracterizaciones, manuales de procedimientos, instructivos, guías, planes y programas que regulan y orientan el desarrollo de la función de la empresa, la planificación y el diagnóstico estratégicos de la entidad, informes de gestión, datos históricos de los procesos, controles inmersos en los procesos, opiniones de especialistas y expertos, entre otros.

5 DOCUMENTACIÓN ASOCIADA

- Plan Anticorrupción y de Atención al Ciudadano.
- GP-FO-002 Mapa de Riesgos de Corrupción.
- GE-FO-006 Seguimiento al Plan Anticorrupción y de Atención al Ciudadano.
- GE-FO-007 Seguimiento Mapa de Riesgos de corrupción

RAFAEL TAMAYO VILLAMIZAR Ing. Apoyo SIG	**RAFAEL TAMAYO VILLAMIZAR** Ing. Apoyo SIG	**CARLOS JOSÉ IBARRA RODRÍGUEZ** Subgerente- Representante de la Dirección
Fecha: Agosto 2021	Fecha: Agosto 2021	Fecha: Agosto 2021