1. OBJETIVO

Establecer disposiciones y criterios institucionales que orienten a la ACI Medellín en la correcta identificación, análisis, valoración y administración de los riesgos, con el fin de reducir la probabilidad de ocurrencia y el grado de impacto de aquellos riesgos que pueden afectar el logro de los objetivos institucionales en el marco de los procesos.

2. ALCANCE

Aplica para todos los procesos de la ACI Medellín, desde el análisis del contexto estratégico hasta el monitoreo a las actividades de control planteadas.

3. DEFINICIONES

- Amenaza: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- Causa: motivo o circunstancia por la cual se puede originar un riesgo.
- Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- Mapa de riesgos: documento con la información resultante de la gestión del riesgo.
- Mapa de riesgos institucional: contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad. Se alimenta de los mapas de riesgos por proceso, **teniendo en cuenta que solamente se trasladan al institucional aquellos riesgos que permanecieron en las zonas más altas de riesgo (alta y extrema) y los riesgos de corrupción**, que afectan el cumplimiento de la misión institucional y objetivos de la entidad.
- Objetivo: es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción.
- Objetivo del proceso: son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales.
- Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- Riesgo: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.
- 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.
- Riego 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 corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.**
- Riesgo de 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.
- Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información.
- Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para

la entidad, que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Activo de información: en relación con la privacidad de la información, se refiere al activo que contiene información pública Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- Confidencialidad: propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
- Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. LINEAMIENTOS GENERALES

La política de administración de riesgos corresponde a un elemento de control que permite enmarcar criterios orientadores en la toma de decisiones, respecto a la gestión o administración del riesgo, establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

La política transmite la posición de la alta dirección y establece las pautas de acción necesarias a todos los servidores de la entidad. La establece la alta dirección, con la participación del Comité Institucional de Coordinación de Control Interno.

Para el diseño de la política de administración de riesgos, se debe tener en cuenta:

- Objetivos estratégicos de la ACI Medellín.
- Roles en cuanto al monitoreo y revisión de los riesgos y las actividades de control.
- Definir los mecanismos de comunicación utilizados para dar a conocer la política de riesgos a todo el personal.
- Administrar los riesgos buscando la cobertura de todos los procesos y/o subprocesos, como actividades propias del control, donde se observe claramente la identificación y el análisis de los riesgos en cada uno de ellos, al igual que niveles de aceptación del riesgo, niveles de calificación de impacto y el tratamiento de los riesgos.

Para una adecuada Administración del Riesgo se deben tener en cuenta:

- Misión, visión, objetivos estratégicos, mapa de procesos, caracterización de los procesos.
- El campo de aplicación (procesos y subprocesos definidos dentro del Sistema Integrado de Gestión-SIG).
- Las líneas de defensa establecidas por el Modelo Integrado de Planeación y Gestión – MIPG:

- **Primera 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 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.

- **Segunda línea de defensa**: asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. Está 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.

- **Tercera línea de defensa:** proporciona información sobre la efectividad del Sistema de Control Interno - SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. Está a cargo de la oficina de control interno, auditoría interna o quien haga sus veces.
  Rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI.

4.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA ACI MEDELLÍN

4.1.1 OBJETIVO DE LA POLÍTICA

La ACI Medellín se compromete a controlar todos aquellos riesgos negativos que pueden impedir el cumplimiento de los objetivos institucionales y potencializar los riesgos positivos (oportunidades) mediante una efectiva administración de los mismos, como herramienta de gestión que responda a las necesidades de la entidad, contando con la participación activa de los servidores públicos responsables de los procesos, subprocesos y procedimientos, quienes deberán identificar, analizar y definir actividades de control para mitigar la materialización de los riesgos negativos.

4.1.2 ALCANCE DE LA POLÍTICA

La política de administración de riesgos aplica para la ACI Medellín y debe ser conocida y cumplida tanto por los servidores como por los contratistas que apoyan la gestión.

4.1.3 PLANES DE ACCIÓN DE RIESGOS POR PROCESO

La ACI Medellín, consciente de que en el desarrollo de sus actividades está sujeta a la materialización de riesgos en los procesos y subprocesos, se compromete a adoptar los mecanismos y acciones necesarias para la administración de los riesgos que comprenda la identificación, análisis, valoración, tratamiento y seguimiento de estos, con la finalidad de alcanzar las metas y objetivos institucionales, si por el contrario se trata de una oportunidad el plan de acción debe ir encaminado a aprovecharla, por tal motivo se tiene establecido un mapa de riesgos por proceso y subproceso en los cuales se pueden observar las actividades de control y actividades para aprovechar las oportunidades respectivamente.

4.1.4 EVALUACIÓN DE LA EFECTIVIDAD DE LA POLÍTICA

La evaluación de la efectividad de la política es responsabilidad del coordinador de control interno.

4.1.5 MONITOREO Y SEGUIMIENTO

Una vez definido y validado el mapa de riesgos por proceso y subproceso, es necesario monitorearlo teniendo en cuenta que los riesgos negativos nunca dejan de representar una amenaza y que los riesgos positivos representan oportunidades que pueden conducir a la adopción de nuevas prácticas para la Agencia.

El monitoreo es esencial para asegurar que las actividades de control se están llevando a cabo y evaluar la eficiencia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas y correctivas.

El monitoreo debe estar a cargo de:

- Los responsables de procesos o subprocesos y su equipo de trabajo.
- El Coordinador de Control Interno.

Su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. El monitoreo y medición se debe realizar como mínimo una vez al año.

El seguimiento estará a cargo del coordinador de control interno, su responsabilidad es verificar y evaluar la elaboración, la visibilización, el seguimiento y el control del mapa de riesgos de corrupción. El seguimiento se realiza tres (3) veces al año, así:

- ✓ 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 hábiles del mes de enero.

4.1.5.1 Rol de las líneas de defensa en el monitoreo y revisión de los riesgos y actividades de control

A continuación, se presenta en la siguiente matriz los distintos roles en cuanto al monitoreo y revisión de los riesgos y las 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. – Revisar el 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 de coordinación 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 a 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.

PRIMERA 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 instituciones 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. – Revisar 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 o quien haga sus veces, 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.

SEGUNDA 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. – Revisar 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.

TERCERA 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 interno o auditoría interna.	
Actividades de monitoreo y revisión a realizar.	La oficina de control interno o auditoría interna 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. – Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. – Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. – Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. – Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.

4.1.6 IDENTIFICACIÓN DEL RIESGOS

La identificación del riesgo se realiza determinando las causas, con base en el contexto interno, externo y del proceso o subproceso ya analizados para la entidad y que pueden afectar el logro de los objetivos.

A partir de este levantamiento de causas se procederá a identificar el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o subproceso.

Esta etapa tiene como fin, detectar aquellos eventos potenciales que pueden afectar negativamente el normal desarrollo de los procesos, establecer sus causas y los efectos de su ocurrencia. Los riesgos identificados deben estar bajo la gobernabilidad tanto de la Agencia como del proceso.

4.1.6.1 Preguntas claves para la identificación del riesgo

¿Qué puede suceder? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso o subproceso 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.

Es importante observar que en el proceso de identificación del riesgo es posible establecer más de una causa como factor del riesgo a identificar.

4.1.6.2 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 gerenciales:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
- **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
- **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todos aquellos procedimientos involucrados con el proceso financiero como presupuesto, tesorería, contabilidad, 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.

Para la identificación de riesgos se deben tener en cuenta los siguientes ítems:

- ✓ Analizar la información contenida en la caracterización de proceso o subproceso, principalmente el objetivo, su alcance, sus principales actividades y puntos de control.

- ✓ Además de la caracterización del proceso o subproceso, se debe acudir a fuentes informativas como los procedimientos relacionados y las caracterizaciones existentes de los procesos o subprocesos asociados, con el propósito de detectar todos los riesgos que pueden afectar el cumplimiento del proceso.

- ✓ 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 de.

- ✓ Es necesario que en la descripción del riesgo de corrupción concurran los componentes de su definición: **acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**

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 dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	**x**	**x**	**x**	**x**

- ✓ Para la descripción de los riesgos de seguridad digital se debe tener en cuenta que estos se basan en la afectación de tres criterios en un activo o 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.

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDAD	CONSECUENCIAS

Identificación de activos de seguridad de la información: son activos los elementos que utiliza la entidad para funcionar en el entorno digital tales como: aplicaciones de la entidad, servicios web, redes, información física o digital, tecnologías de información – TI, tecnologías de operación – TO.

Pasos para identificar los activos:

Paso 1. Listar los activos por cada proceso.

Paso 2. Identificar el dueño de los activos.

Paso 3. Clasificar los activos.

Paso 4. Calificar la información.

Paso 5. Determinar la criticidad del activo.

Paso 6. Identificar si existe infraestructura crítica cibernética.

- ✓ Siempre se debe hacer un análisis del riesgo, a pesar de que se le haya construido gramaticalmente bien; ya que puede ser un efecto o una causa.

- ✓ Las causas generadoras del riesgo pueden ser tanto internas como externas al proceso o subproceso.

- ✓ Los efectos de la materialización de riesgos deben ser objetivos e identificados por consenso de los participantes en la identificación de riesgos.

- ✓ Las consecuencias constituyen los efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso o subproceso de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

4.1.6.3 Establecimiento del contexto

Se deben establecer el contexto tanto interno como externo de la entidad, además del contexto de los procesos y sus activos de seguridad, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de la entidad.

Se determinan las características o aspectos esenciales del entorno en el cual opera la ACI Medellín; se pueden considerar factores tales como:

CONTEXTO EXTERNO	**ECONÓMICO Y FINANCIERO**	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	POLÍTICOS	Cambios de gobierno, legislación, políticas públicas, regulación.
	SOCIALES Y CULTURALES	Demografía, responsabilidad social, orden público.
	TECNOLÓGICOS	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS	Normatividad externa (leyes, decretos, ordenanzas y acuerdos).

4.1.6.3.2 Factores Internos

Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos; se clasifican como se relaciona en la siguiente tabla:

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.

4.1.6.3.3 Factores del Proceso

Se determinan las características o aspectos esenciales del proceso o subproceso y sus interrelaciones; se clasifican como se relaciona en la siguiente tabla:

CONTEXTO DEL PROCESO O SUBPROCESO	**DISEÑO DEL PROCESO**	Claridad en la descripción del alcance y objetivo del proceso.
	INTERRELACIONES 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 PROCESO	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.

4.1.7 VALORACIÓN DEL RIESGO

4.1.7.1 Análisis de riesgos

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

4.1.7.1.1 Determinar la probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida por criterios de frecuencia o factibilidad.

FRECUENCIA	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.

4.1.8.1.2 Determinar consecuencias o nivel de impacto

Por **impacto** se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo**.** La calificación del impacto puede ser el resultado del análisis de las consecuencias presentadas al momento de materializarse el riesgo.

4.1.8.1.3 Estimar el nivel del riesgo inicial

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.

4.1.8.1.4 Cálculo de la probabilidad e impacto

Análisis de 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 podría 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, se debe calificar el nivel de probabilidad en términos de factibilidad, utilizando la siguiente matriz de priorización de probabilidad:

Matriz de priorización de probabilidad

Nro.	Riesgo	P1	P2	P3	P4	P5	P6	Tot.	Prom.	Calificación
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad.	5	5	4	3	5	3	4	24	4 PROBABLE

Convenciones:
Nro.: número consecutivo del riesgo – **Riesgo**: riesgo identificado - **P1:** participante 1 **P2:... - Tot:** total puntaje – **Prom:** promedio – **Calificación**: conforme a las tablas establecidas.

Criterios para calificar el impacto – riesgos de gestión

La calificación del impacto puede ser el resultado del análisis de las consecuencias presentadas al momento de materializarse el riesgo de gestión.

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
5 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.
4 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.
3 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.
2 menor	- Impacto que afecte la ejecución presupuestal en un valor ≤1%	- Interrupción de las operaciones de la Entidad por algunas horas.

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	- 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.	- 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.
1 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.

Criterios para calificar el impacto – riegos de seguridad

Nivel	Valor del impacto	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.

Nivel	Valor del impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
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.

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.

Confidencialidad: propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

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.

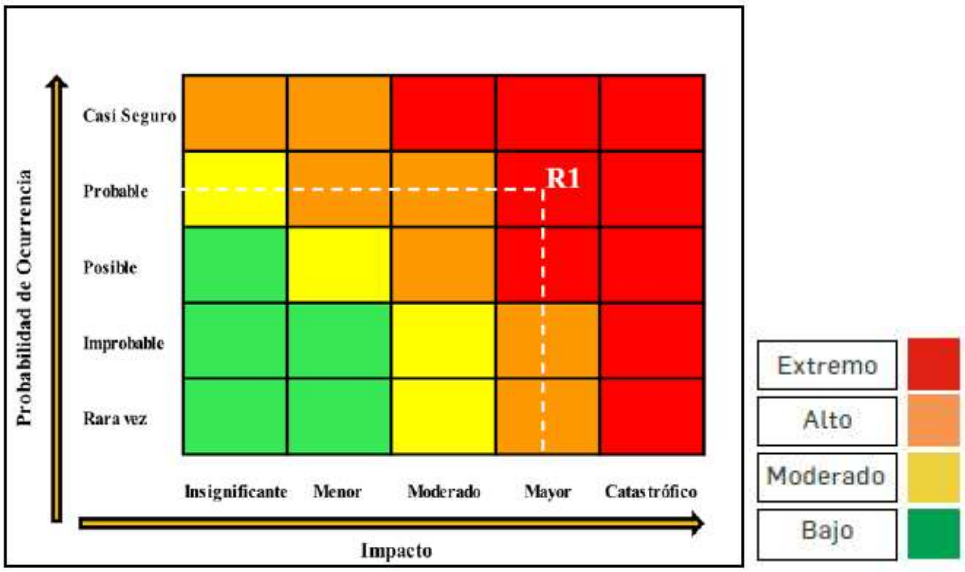
La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental 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.

4.1.8.1.5 Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Mapa de calor



Criterios para calificar el impacto – riesgos de corrupción

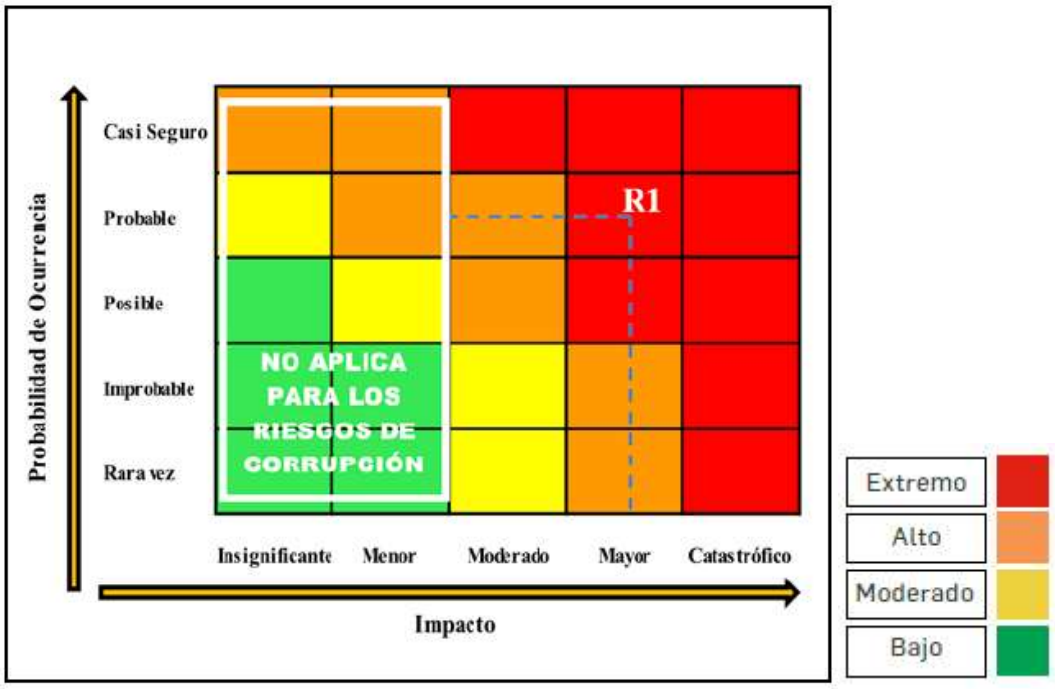
El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la entidad. Para facilitar la asignación del puntaje es aconsejable diligenciar el siguiente formato:

Nro.	PREGUNTA ¿SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…?	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afecta el cumplimiento de la misión de la Entidad?		
4	¿Afecta el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afecta la generación de los productos o la prestación del servicio?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicio 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?		

Nro.	PREGUNTA ¿SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…?	Respuesta	
		Si	No
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	¿Genera daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad.		

4.1.8.1.7 Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.



4.1.9 EVALUACIÓN DE LOS CONTROLES – DISEÑO 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.

4.1.9.1 Diseño de los 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:

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

Paso 2: Debe tener una periodicidad definida para su ejecución. 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. Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control.

Paso 3: Debe indicar cuál es el propósito del control. 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 acabo 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.

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

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

Pago 6: Debe dejar evidencia de la ejecución del control. 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 a 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.

Ejemplo:
Cada vez que se va a realizar un contrato, el profesional de contratación verifica a través de una lista de chequeo que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación. En caso de encontrar información faltante, solicita al proveedor por correo la información y poder continuar con el proceso de contratación. **Evidencia: la lista de chequeo diligenciada, la información de la carpeta del cliente y los correos a que hubo lugar en donde solicitó la información faltante (en los casos que aplique).**

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.

4.1.9.2 Valoración de los controles para la mitigación de los riesgos

Se debe valorar los controles existentes en el proceso o subproceso, con el fin de conocer el tipo de control y su respuesta frente a la mitigación del riesgo.

Análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas.

CRITERIO DE EVALUACIÓN	ASPECTOS A EVALUAR EN 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	¿Se deja evidencia o rastro de la ejecución	Completa	Incompleta / no

ejecución del control	del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?		existe

Peso o participación de cada variable en el diseño del control para la mitigación del riesgo

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	OPCIONES DE RESPUESTA
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

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 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 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 interna o control interno.

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO – PESO DE LA EJECUCIÓN DEL 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.

4.1.9.3 Análisis y evaluación de los controles para la mitigación de los riesgos

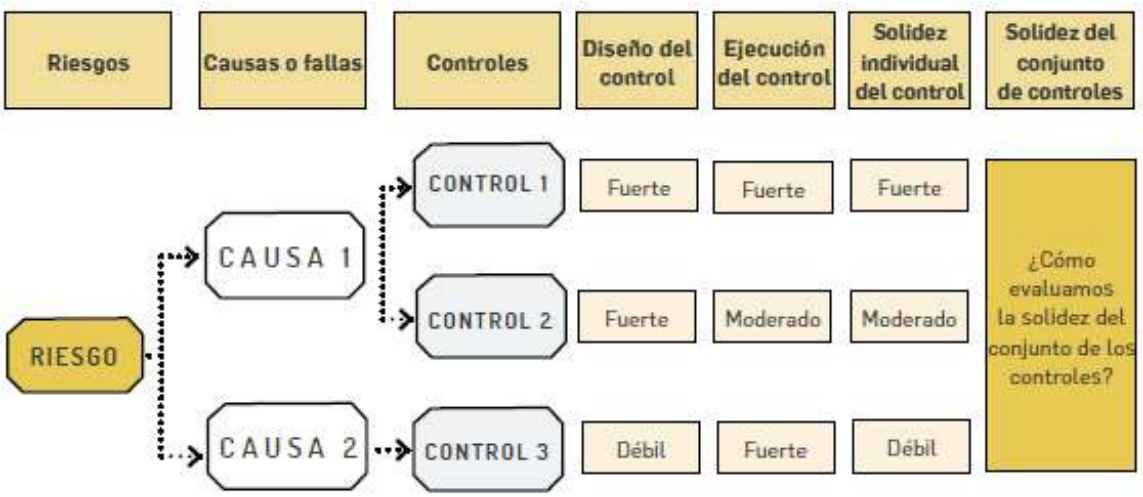
Dado que la calificación de riesgos inherentes y residuales se efectúa al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución 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 SI/NO
Fuerte: calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + fuerte = fuerte	No
	Moderado (algunas veces)	Fuerte + moderado = moderado	Si
	Débil (no se ejecuta)	Fuerte + débil = débil	Si
Moderado: calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado + fuerte = moderado	Si
	Moderado (algunas veces)	Moderado + moderado = moderado	Si
	Débil (no se ejecuta)	Moderado + débil = débil	Si
Débil: calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil + fuerte = débil	Si
	Moderado (algunas veces)	Débil + moderado = débil	Si
	Débil (no se ejecuta)	Débil + débil = débil	Si

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.



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

4.1.9.4 Nivel de riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGOS QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGOS QUE SE DESPLAZA EN EL EJE DEL IMPACTO
Fuerte	Directamente	Directamente	2	8
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.

4.1.10 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:

Aceptar al riesgo

No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.

Reducir el riesgo

Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos, esto conlleva a la implementación de controles.

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo alto.

Evitar el riesgo

Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo extremo.

Compartir el riesgo

Se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte una parte de este.

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

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. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo moderado y extermo.

Las actividades de control son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Las actividades de control, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna. De lo contrario se deben establecer controles preventivos y detectivos.

Controles preventivos: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

Controles detectivos: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Se deben seleccionar actividades de control preventivas y detectivas que por sí solas ayuden a la mitigación de las causas que originan los riesgos.

6. MAPA DE RIESGOS INSTITUCIONAL - MAPA DE RIESGOS DE CORRUPCIÓN

Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

En el formato FR-SIG-11 Herramienta administración de riesgos, se realiza el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual.

A partir de allí se deben analizar las estrategias DO y FA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para incluirlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden.

Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer, cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

Por último, se formulan los indicadores clave de riesgo (KRI por sus siglas en inglés) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (por riesgo identificado en los procesos).

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).

El Mapa de Riesgos Institucional se construye integrando los riesgos ubicados en las zonas de riesgo "alta" o "extrema", contenidos en los mapas de riesgo por proceso o subproceso de la ACI Medellín.

El Mapa de Riesgos de Corrupción será construido a partir de todos los riesgos de corrupción identificados en los mapas de los proceso o subproceso.

El Mapa de Riesgo Institucional y el Mapa de Riesgos de Corrupción serán consolidados por el profesional senior de calidad. Una vez sea alimentada toda la información de administración de riesgos de la vigencia correspondiente se hará la publicación en la página web.

Formato mapa de riesgos

Nro.	RIESGO	CLASIFICACIÓN	CAUSA	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN DE 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 TI y jefe de contratos	Primer trimestre 2019	EFICACIA: Índice de cumplimiento actividades=(# de actividades cumplidas / # de actividades programadas) x 100
			Insuficiente capacitación				Reducir	D1O2: Realizar convenios con entidades educativas para capacitar al personal de contratos.	Convenios firmados	Director financiero	Trimestral	

7. REGISTROS

FR-SIG-11 Herramienta Administración de Riesgos

8. RESUMEN DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2016/04/05	Logo	02
2016/01/08	4.2 Responsabilidades, cambio de la denominación de responsable de calidad por profesional en calidad, ajustes de redacción, responsabilidad y autoridad	03
2017/01/09	Ajuste al contenido del documento conforme a los cambios impartidos en administración de riesgos en la guía para la administración de riesgos del DAFP	04
2018/04/04	Ajuste al contenido del documento conforme a los cambios impartidos en administración de riesgos en las siguientes guías del DAFP: guía para la administración de riesgos y guía para la gestión de riesgos de corrupción	05
2019/13/02	Ajuste al contenido del documento conforme a los cambios impartidos en administración de riesgos en las siguientes guías del DAFP: guía para la administración de riesgos y guía para la gestión de riesgos de corrupción	06

9. RESPONSABILIDAD Y AUTORIDAD

Elaboró / Actualizó:	Revisó:	Aprobó:
Nombre: Yesenia Arango Sánchez	Nombre: Astrid Madeleine Álvarez	Nombre: Eleonora Betancur González
Cargo: Asistente de Planeación	Cargo: Directora Relaciones Administrativas	Cargo: Directora Ejecutiva