1. OBJETIVO

Establecer las disposiciones y criterios institucionales que orienten a la ACI Medellin en la administración de sus riesgos, mediante la correcta identificación, análisis, valoración y tratamiento de estos, con el fin de establecer el marco general de actuación de todos los servidores de la entidad para la adecuada gestión de los riesgos proporcionando un aseguramiento razonable con respecto al logro de los objetivos.

2. ALCANCE

Aplica para todos los procesos de la ACI Medellín, desde el análisis del contexto estratégico hasta el seguimiento 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.
- **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Impacto:** 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.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

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

- **Tolerancia del riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **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 de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** preservación de la confidencialidad, integridad, y disponibilidad de la información.

- **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.

- **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 y 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.
- Mecanismos de comunicación utilizados para dar a conocer la política de riesgos, el resultado del monitoreo de los controles y la notificación en caso de materialización.

- 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, mapa de procesos, caracterización de los procesos, objetivos de los procesos.
- Planeación institucional, objetivos estratégicos, cadena de valor.
- 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, que establece las responsabilidades frente a la gestión de los riesgos.

4.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE LA ACI MEDELLÍN

4.1.1 OBJETIVO DE LA POLÍTICA

La ACI Medellin se compromete a administrar adecuadamente los riesgos de gestión, de corrupción y de seguridad digital, asociados a los procesos y subprocesos de la entidad definiendo los criterios para su gestión, contando con la participación activa de los servidores públicos quienes deberán identificar, analizar, valorar y dar tratamiento a los riesgos que pudieran afectar el cumplimiento de los objetivos institucionales y así mismo definir, implementar y monitorear las actividades de control para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables, procurando la actuación correctiva y oportuna frente a la materialización de los riesgos identificados.

4.1.2 ALCANCE DE LA POLÍTICA

La política de administración de riesgos de la ACI Medellin aplica para todos los procesos y subprocesos de la entidad, por lo tanto, debe ser aplicada por todos los servidores y contratistas que apoyan la gestión.

4.1.3 EVALUACIÓN DE LA EFECTIVIDAD DE LA POLÍTICA

La evaluación de la efectividad de la política del riesgo la realiza el Coordinador de Control Interno al determinar la pertinencia y efectividad de los controles de los riesgos.

4.1.4 MONITOREO Y SEGUIMIENTO

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

El monitoreo debe estar a cargo de los responsables de procesos o subprocesos y su equipo de trabajo.

Su finalidad principal será verificar que los controles se realicen de forma eficaz conforme a lo establecido en el mapa de riesgos y con la naturaleza del riesgo. El monitoreo y medición se debe realizar de acuerdo con la frecuencia en la que el control está establecido.

En caso de presentarse la materialización de los riesgos, el líder del proceso debe adelantar un análisis de causas y establecer con su equipo de trabajo las acciones correctivas correspondientes. En este caso debe dar reporte inmediato al Coordinador de Control interno.

El Profesional Senior de Calidad realiza acompañamiento a los procesos y verifica la eficacia de los controles asi como su funcionamiento de acuerdo con lo previsto. Dicho informe es entregado al Coordinador de Control Interno, quien establece recomendaciones.

El seguimiento está 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 gestión. 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 en la pagina web de la entidad.
- ✓ Segundo seguimiento: con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre en la página web de la entidad.
- ✓ Tercer seguimiento: con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero en la página web de la entidad.

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.

4.1.5 RESPONSABILIDADES

Las responsabilidades para la gestión de los riesgos en la ACI Medellin se determinan de acuerdo con el 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 del Comité Directivo y el Comité Institucional de Coordinación de Control Interno.	
Actividades de monitoreo y revisión a realizar.	La Dirección ejecutiva 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 la 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.

PRIMERA LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, tratamiento, monitoreo y acciones de mejora en caso de materialización de riesgos. Está conformada por los Directores, equipos de trabajo de los procesos, subprocesos, programas y proyectos de la entidad.	
Actividades de monitoreo y revisión a realizar.	Los Directores, equipos de trabajo 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 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 (coordinador de planeación, coordinador de control interno, supervisores e interventores de contratos o proyectos, profesional senior de calidad, etc.).	
Actividades de monitoreo y revisión a realizar.	Los Directores, equipos de trabajo 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 estos. – 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 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.

Tabla 1. Descripción de actividades de las líneas de defensa.

En el Comité Institucional de Gestión y Desempeño se realiza el análisis frente a la gestión del riesgo y se determinan las mejoras que sean requeridas. En el Comité Institucional Coordinador de Control Interno se realiza el análisis de eventos y riesgos críticos a que hubiere lugar.

4.1.6 NIVELES DE ACEPTACIÓN DEL RIESGO

- Nivel de riesgo: se determina al combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. Para este fin se utiliza la matriz calor de 5 x 5.

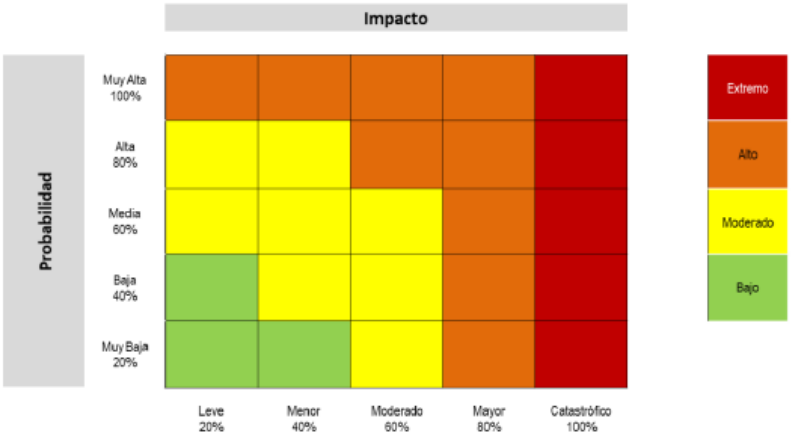


Figura 1. Matriz de calor. Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

- Apetito de riesgo: se define consecuentemente de acuerdo con la tolerancia al riesgo expresado a continuación.

- Tolerancia del riesgo: se determina de acuerdo con el tipo de acciones para abordar los riesgos en función del valor del nivel de riesgo residual obtenido.

  ✓ Para un nivel de riesgo bajo se determinan controles y seguimiento periódico por parte de los líderes de los procesos, o se determina ASUMIR conociendo los efectos de su posible materialización.

  ✓ Para un nivel de riesgo moderado y alto se debe REDUCIR tomando medidas encaminadas a:
  TRANSFERIR el riesgo: se considera tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas.
  MITIGAR el riesgo: se implementan acciones que mitiguen el nivel de riesgo. No es un control adicional necesariamente. Esta última incluye un plan de acción dando seguimiento por medio de indicadores o entregables relacionados con proyectos u objetivos de los procesos.
  En general dichas medidas son encaminadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de protección). Se puede conseguir mediante la optimización de los procedimientos y la implementación de controles preventivos.

  ✓ Para un nivel de riesgo extremo se debe EVITAR y se determina no asumir la actividad que genera este riesgo. Asimismo, se puede tomar la opción REDUCIR a través del traspaso de las pérdidas a otras organizaciones y se establecen planes de contingencia en caso de materialización o también optar por las medidas TRANSFERIR O MITIGAR descritas en el punto anterior.

  ✓ En todos los casos para los riesgos de corrupción la tolerancia es inaceptable.

- Capacidad del riesgo: este concepto se define a partir del siguiente esquema basado en los niveles de riesgo establecidos:

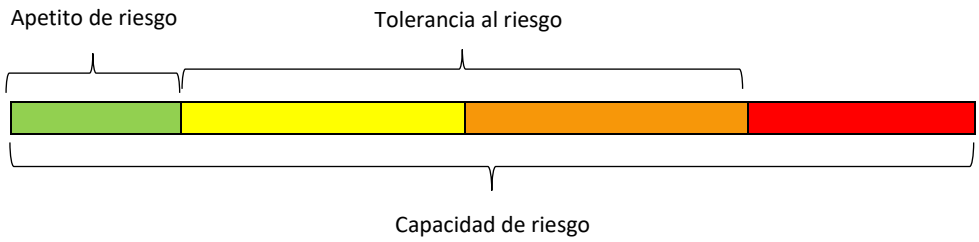


Figura 2. Capacidad de riesgo

4.1.7 IDENTIFICACIÓN DEL RIESGOS

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

Para identificar el riesgo es conveniente preguntarse:

- ✓ **¿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.

Para la identificación de los riesgos se aplican las siguientes etapas:

4.1.7.1 Análisis de los objetivos estratégicos y de los procesos

Los objetivos estratégicos deben estar alineados en cuanto a la misión y la visión institucional, asi como analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: especifico, medible, alcanzable, relevante y proyectado en el tiempo.

Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además se debe revisar que los mismos estén alineados con la misión y la visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

4.1.7.2 Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

4.1.7.3 Identificación de áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Figura 3. Áreas de impacto de los riesgos. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020.

4.1.7.4 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. Algunas de ellas están definidas en la Tabla 2. Factores de riesgo.

FACTOR	DEFINICION	DESCRIPCION
PROCESOS	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos. Errores de grabación o autorización. Errores en cálculos para pagos internos o externos. Falta de capacitación, temas relacionados con personal.
TALENTO HUMANO	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos. Posibles comportamientos no éticos de los empleados. Fraude interno (corrupción, soborno).
TECNOLOGÍA	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos. Caída de aplicaciones. Caída de redes. Errores en programas.
INFRAESTRUCTURA	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes. Incendios. Inundaciones. Daños a activos fijos.
EVENTO EXTERNO	Situaciones externas que afectan la entidad.	Suplantación de identidad. Asalto a la oficina. Atentados, vandalismo, orden público.

Tabla 2. Factores de riesgo

4.1.7.5. Descripción del riesgo

RIESGOS DE GESTIÓN

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento para personas ajenas al proceso. Debe contener la siguiente estructura:

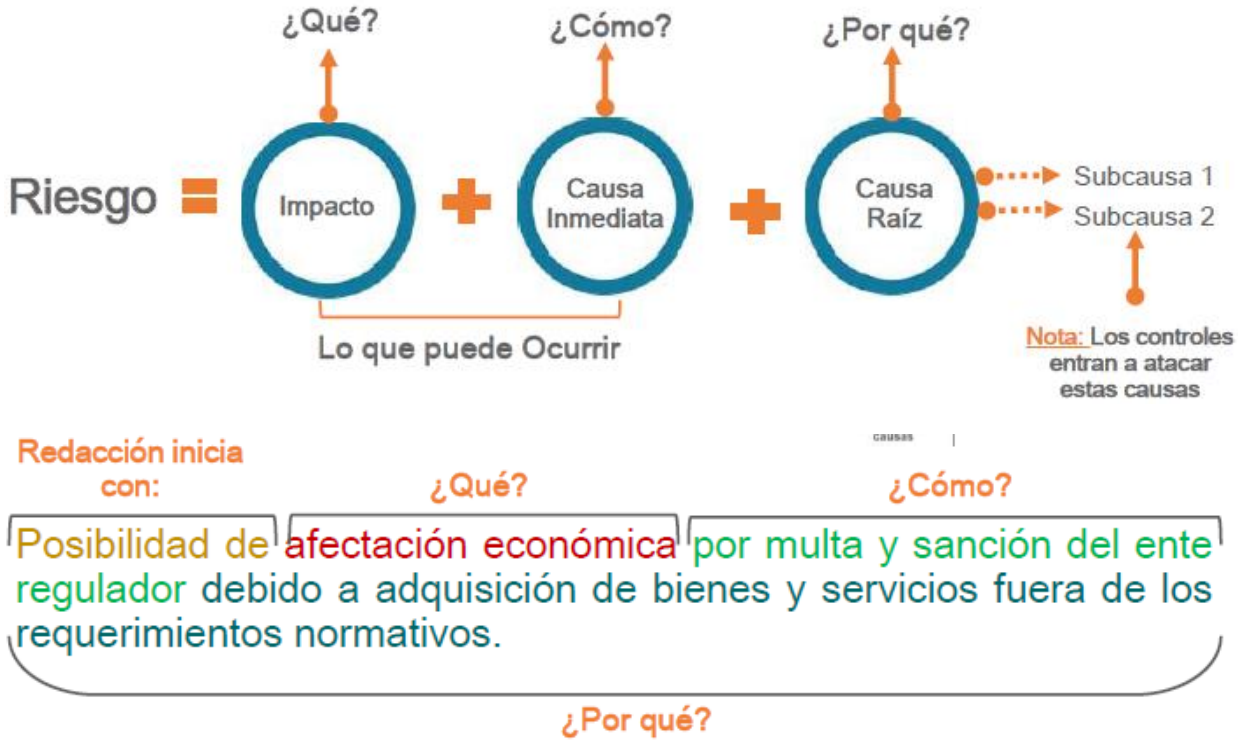


Figura 4. Estructura para la descripción de riesgos. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020

Premisas para una adecuada redacción del riesgo:

- No describir como riesgos omisiones ni desviaciones del control.
  Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- No describir causas como riesgos
  Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- No describir riesgos como la negación de un control.
  Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

- No existen riesgos transversales, lo que pueden existir son causas transversales.
  Ejemplo: pérdida de expedientes.

Con respecto a los riesgos de gestión:

✓ 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.

RIESGOS DE CORRUPCIÓN

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. 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 utiliza la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

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: **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**

Tabla 3. Componentes del riesgo de corrupción.

Los riesgos de corrupción se establecen sobre procesos. 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.

RIESGOS DE SEGURIDAD DIGITAL

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. Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Estos activos son 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.

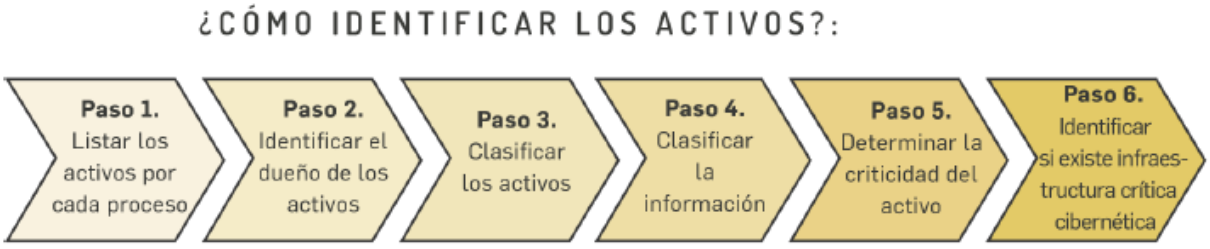


Figura 5. Pasos para identificar activos de informacion. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

Los responsables de estos activos de informacion deben para cada riesgo, asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

Para ello es necesario tener en cuenta que la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Algunos ejemplos de vulnerabilidad pueden ser los siguientes:

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Informacion	Falta de controles de acceso físico	Hurto de informacion
Personal	Falta de capacitación en las herramientas	Error en el uso
Organizacion	Ausencia de políticas de seguridad	Abuso de los derechos

Tabla 4. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

Un ejemplo de la descripción de los riesgos de seguridad de la informacion es el siguiente:

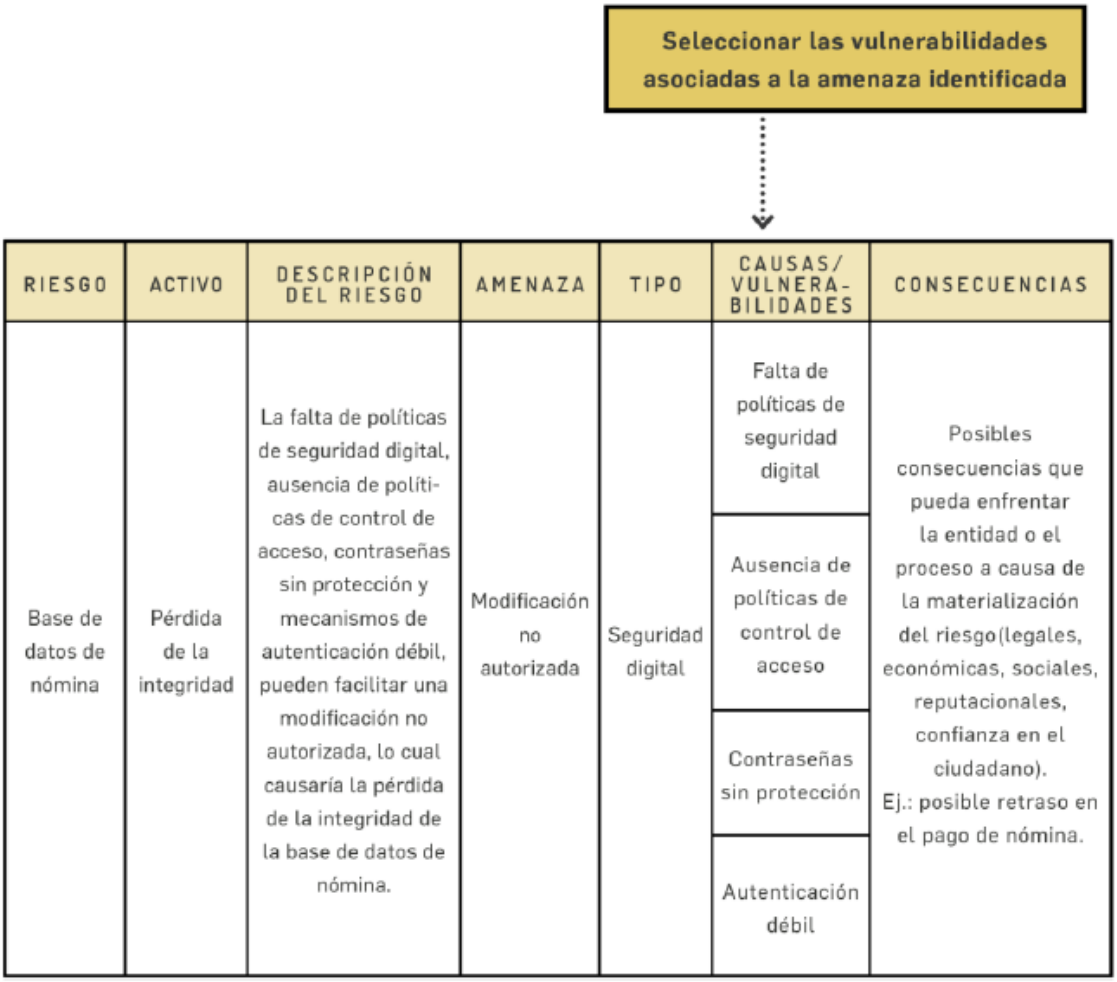


Figura 6. Formato de descripción del riesgo de seguridad de la información. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

4.1.7.6 Clasificación del riesgo y factores de riesgo:

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías, que a su vez se relacionan con los factores de riesgo asi:

TIPO DE RIESGO	RIESGOS	FACTORES DE RIESGO
Ejecución y administración de los procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	PROCESOS
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	EVENTO EXTERNO
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la	TALENTO HUMANO

	organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.	
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	TECNOLOGIA
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.	SE ASOCIAN A VARIOS FACTORES
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	SE ASOCIAN A VARIOS FACTORES
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.	INFRAESTRUCTURA EVENTO EXTERNO

Tabla 5. Tipos de riesgo. Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

4.1.8 VALORACIÓN DEL RIESGO

4.1.8.1 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).

Esta valoración de riesgos aplica para los riesgos de gestión y de seguridad de la información, teniendo en cuenta que para este último la probabilidad y el impacto se determinan con base en las amenazas y no en las vulnerabilidades.

4.1.8.1.1 Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la **probabilidad** inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema la probabilidad en riesgos se basa en la exposición al riesgo, se analiza la frecuencia con la cual se realiza la actividad, no se basa en eventos.

Por ejemplo:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación Estratégica	1 vez al año	Muy Baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, Cartera	Semanal	Alta
**Tecnología (incluye disponibilidad de aplicativos), tesorería	Diaria	Muy Alta

Tabla 6. Actividades y frecuencias. Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Teniendo en cuenta lo anterior, los criterios para realizar definir el nivel de la probabilidad se representan en la siguiente gráfica:

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

Tabla 7. Criterios para definir el nivel de probabilidad. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

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**.** Los criterios para definir el nivel de impacto se basan en la siguiente tabla, considerando la pérdida reputacional y afectación económica o presupuestal.

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

Tabla 8. Criterios para definir el nivel de impacto. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

De esta forma el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

4.1.8.1.3 Estimar la zona de riesgo inicial o riesgo inherente

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor. Ver Figura 7. Estimación de la zona de riesgo inicial o riesgo inherente.

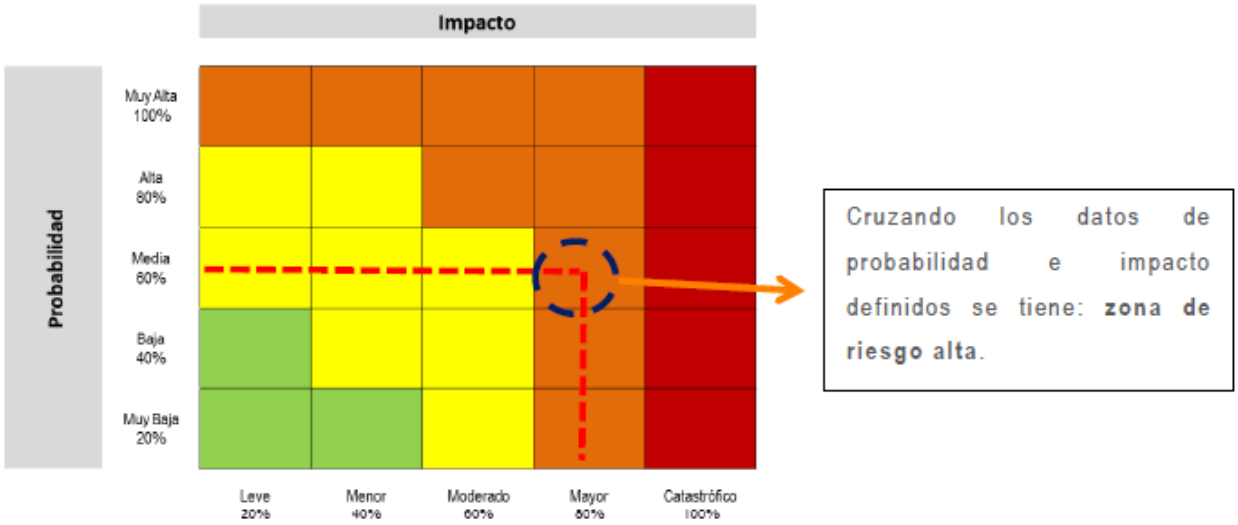


Figura 7. Estimación de la zona de riesgo inicial o riesgo inherente. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020.

4.1.8.1.4 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?		

Nro.	PREGUNTA ¿SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…?	Respuesta	
		Si	No
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?		
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.		

Tabla 9. Criterios para evaluación del impacto en riesgos de corrupción

4.1.8.1.5 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 VALORACIÓN DE CONTROLES

Un control se define como la medida que permite reducir o mitigar el riesgo. 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.

Para la valoración de controles se debe tener en cuenta:

- ✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

- ✓ Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Para los riesgos de corrupción y el diseño de controles, se siguen los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018.

4.1.9.1 Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Por ejemplo:

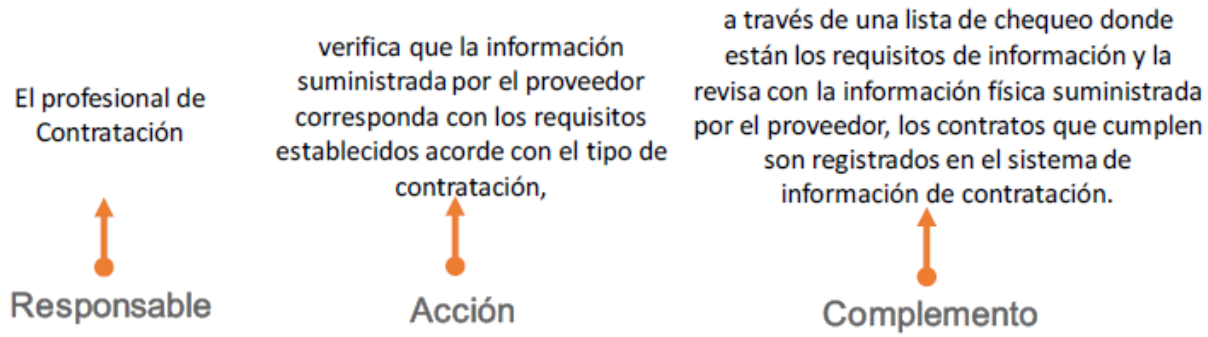


Figura 8. Ejemplo de estructura para la descripción del control. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020.

4.1.9.2 Atributos del control

Son las características que debe poseer el control para garantizar su eficacia en la mitigación del riesgo.

4.1.9.2.1 Atributos de eficiencia

Tipología de controles y los procesos

Través del ciclo de los procesos es posible establecer cuándo se activa un control y por lo tanto, establecer su tipología con mayor precisión.

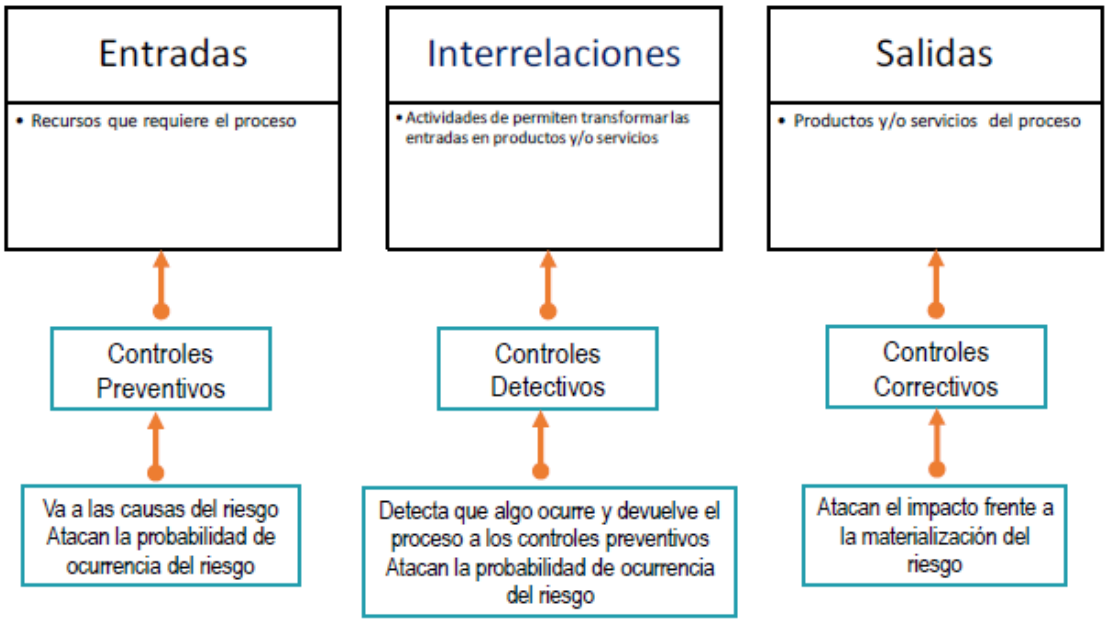


Figura 9. Tipología de controles. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- ✓ Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.
- ✓ Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- ✓ Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.

Forma de implementación

De acuerdo con la forma como se ejecutan tenemos:

- ✓ Control manual: controles que son ejecutados por personas.
- ✓ Control automático: son ejecutados por un sistema.

4.1.9.2.2 Atributos informativos

4.1.9.2.3 Documentación

De acuerdo con el documento de los controles tenemos:

- Documentado: Identifica los controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.

- Sin documentar: Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.

Frecuencia
De acuerdo con la frecuencia del control se clasifican en:

- Continuo: Este atributo identifica a los controles que se ejecuta siempre que se realiza la actividad originadora del riesgo.
- Aleatorio: Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo.

Evidencia
De acuerdo con la evidencia de los controles tenemos:

- Con registro: Corresponde a la evidencia de la ejecución del control
  Ejemplo: correos electrónicos, vistos buenos y documentos electrónicos seguridad, cartas con firma mecánica, firmas digitales, actas de Juan o Comités, firma de asistencia a capacitaciones, entre otros.
- Sin registro: Son aquellos controles que se ejecutan, pero al validar algún tipo de evidencia de su ejecución no es posible determinarla.

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

4.1.9.3 Análisis y valoración de los controles

Solamente los atributos de eficiencia tendrán valoración, los atributos informativos permiten dar formalidad al control, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.

Los controles se valoran de acuerdo con la siguiente descripción de manera individual:

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos Informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Tabla 10. Valoración de los controles. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020.

4.1.9.4 Movimiento en la matriz de calor acorde al tipo de control

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor en la figura 8 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Para controles preventivos y detectivo: el desplazamiento es vertical porque mitigan la probabilidad.
Para controles correctivos: el desplazamiento es horizontal porque mitigan el impacto.
Por lo tanto, un mismo control no puede aplicar para mitigar el impacto y la probabilidad al mismo tiempo.

El movimiento no es diagonal, para ir de una zona extrema a una baja. Se da sobre los ejes y para ello se requiere establecer controles tanto para probabilidad como para impacto de forma individual, tal como se observa en la figura 10. Movimiento en la matriz de calor acorde al tipo de control.

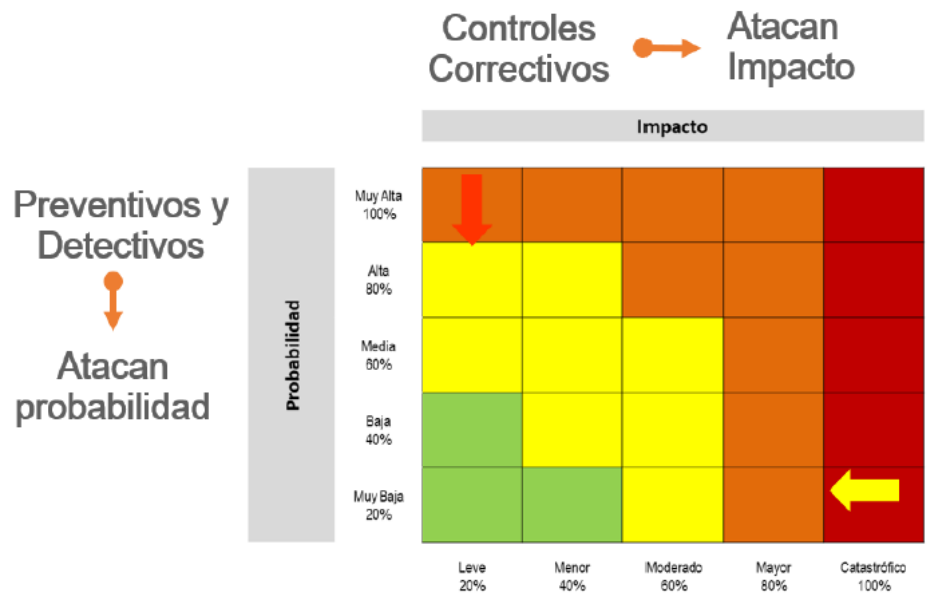


Figura 10. Movimiento en la matriz de calor acorde al tipo de control. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, diciembre 2020

4.1.9.4 Valoración del riesgo residual

El resultado de aplicar la efectividad de los controles al riesgo inherente nos determina el riesgo residual.

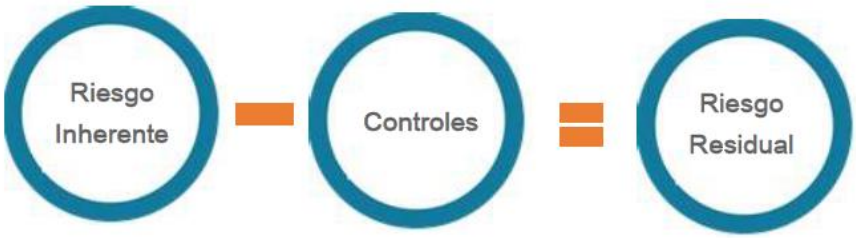


Figura 11. Riesgo residual. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020

Dependiendo del nivel de severidad en que se ubique el riesgo residual, el líder del proceso o subproceso podrá priorizar la atención de estos, así como definir su tratamiento y las acciones a seguir.

4.1.9.5 Desplazamiento en la matriz de calor para el riesgo residual

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Opera una política de reducción máxima del 50% para los controles.

Por lo tanto, el riesgo residual se conforma por el riesgo inherente menos la eficacia de los controles ponderada al mismo riesgo inherente. Partimos de la probabilidad inherente para obtener una probabilidad residual y de un impacto inherente para obtener asi mismo un impacto residual ponderado.

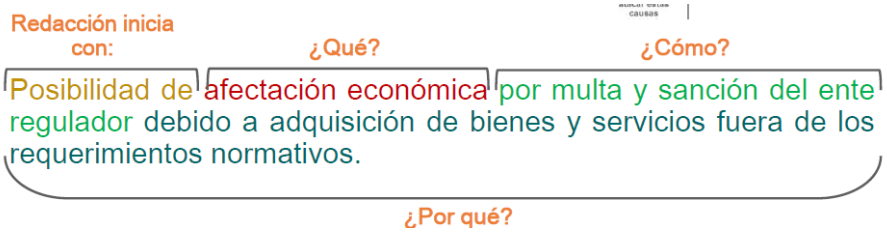
Figura 12. Determinación del riesgo residual. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020

La anterior metodología se explica completa con el siguiente ejemplo:

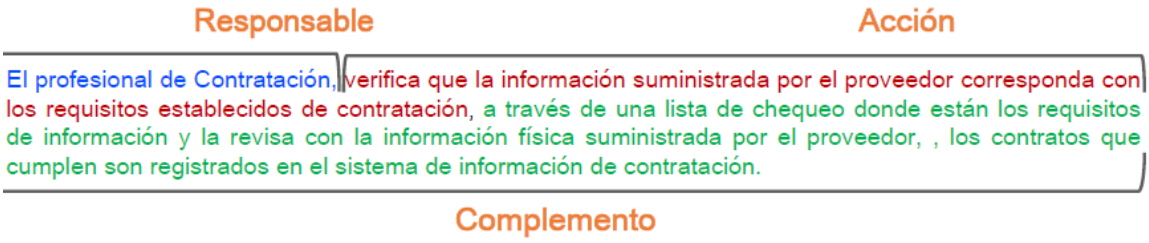
Proceso:

Proceso: Gestión de Recursos:
Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

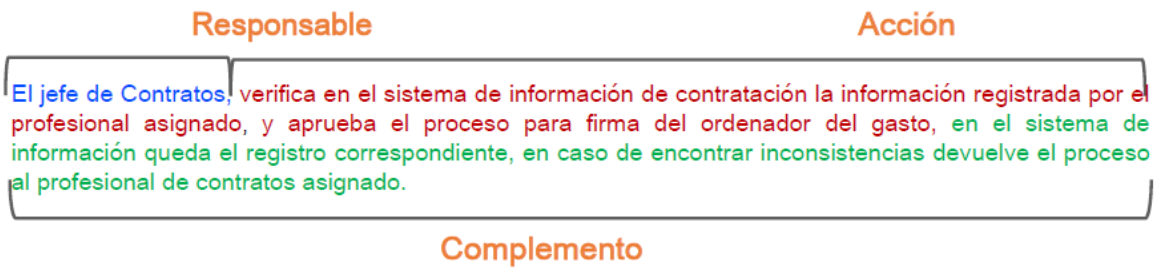
Descripción del riesgo:



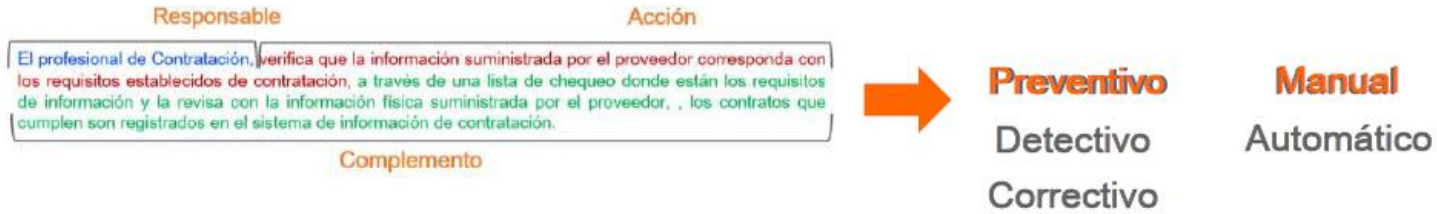
Redacción de controles:
Control No. 1:

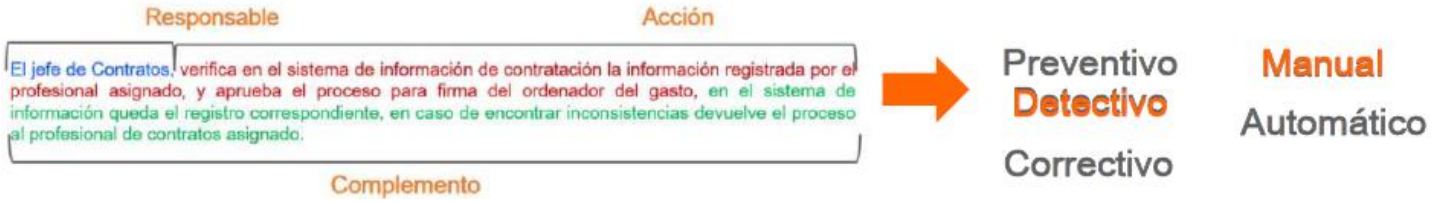


Control No.2:



Tipología del control:





Valoración de los atributos del control No. 1:

Controles y sus características				Peso
Control 1 El profesional del área de contratos, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin registro		-
Total valoración control 1				40%

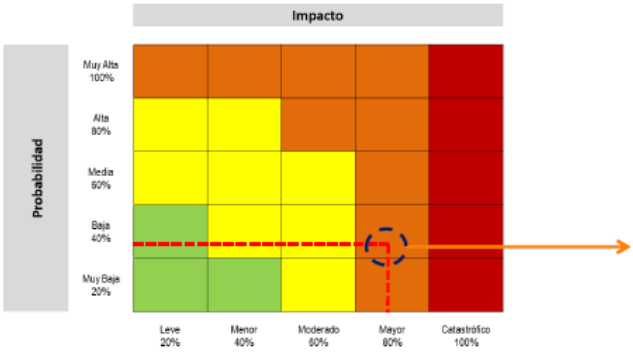
Valoración de los atributos del control No. 2:

Controles y sus características				Peso
Control 2 El jefe de Contratos, verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin registro		-
Total valoración control 2				30%

Cálculos para los controles, suponiendo una probabilidad inherente de 60% y un impacto inherente del 80%:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2%			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

El riesgo residual queda expresado en probabilidad residual de 25,2% y el impacto residual de 80%.
La severidad del riesgo residual se determina cruzando en la matriz de calor los valores mencionados:



Cruzando los datos de probabilidad e impacto después de controles se tiene: **Zona de riesgo alta**.

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

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

Nota: las ilustraciones han sido tomadas de la Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020.

4.1.10 TRATAMIENTO DEL RIESGO O ESTRATEGIAS PARA COMBATIR EL RIESGO

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

El tratamiento del riesgo consiste en la decisión que toma el líder del proceso o subproceso frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual para procesos en funcionamiento y sobre riesgos inherentes solo para procesos nuevos.

En caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá repetir el análisis y revisar dichos controles.

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

- **Aceptar al riesgo**

Después de establecer los niveles de riesgo se determina asumir el mismo, conociendo los efectos de su posible materialización.

- **Reducir el riesgo**

Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación de este.

- **Mitigar**

Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

- **Transferir**

Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

- **Evitar**

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

Siempre que se tome la opción REDUCIR se requiere definir un Plan de Acción, el cual es una herramienta de planificación empleada para la gestión y control de tareas o proyectos. (no necesariamente es un control adicional). Se requiere establecer: Responsable, fecha de implementación y fecha de seguimiento. Este se incluirá en el mapa de riesgos cuando aplique.

Para dar tratamiento a los riesgos de corrupción se debe tener en cuenta:

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 líderes 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:

- **Reducir**

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

- **Evitar**

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

- **Compartir**

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

En el caso de los riesgos de corrupción no pueden ser aceptados.

Para los riesgos de seguridad de la informacion:

Se pueden mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", siempre y cuando se ajusten al análisis de 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 de cada uno de los riesgos identificados por proceso y subproceso, aplicando la metodología descrita en la presente guía.

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, siguiendo su metodología especifica de valoración. Los servidores y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para ello, el Profesional Senior de Calidad lo divulgará a todos los funcionarios para que formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción asi como a las partes interesadas, dejando la evidencia del proceso de socialización y publicación.

Los ajustes a los mapas de riesgos de corrupción deberán dejarse por escrito señalando las modificaciones o inclusiones realizadas.

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.

7. HERRAMIENTAS PARA LA GESTION DEL RIESGO

7.1 GESTION DE EVENTOS

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología de la presente guía.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de ayuda.

- Las PQRD (peticiones, quejas, reclamos, denuncias).
- Oficina jurídica.
- Líneas internas de denuncia.

Este mecanismo genera información para que el evento no se vuelva a presentar.

También se puede llevar un registro de desempeño del control mediante el indicador: Desempeño del control = # eventos / Frecuencia del Riesgo (# veces que se hace la actividad)

Cuando se materializa un riesgo de corrupción se deben adelantar las siguientes actividades:

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.

7.2 INDICADORES CLAVE DE RIESGO

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la tabla 10 se muestran algunos ejemplos de estos indicadores.

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes.	Número de horas de interrupción de aplicativos críticos al mes.
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses.

Tabla 11. Indicadores clave de riesgo KRI. Fuente: Guía para la administración de riesgos y diseño de controles DAFP, octubre 2020

8. REGISTROS

FR-SIG-11 Herramienta Administración de Riesgos

9. 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
11/02/2021	Ajuste al contenido del documento conforme a los cambios impartidos en la Guía para la Administración de Riesgos y Diseño de Controles emitida por el DAFP en diciembre de 2020.	07

9. RESPONSABILIDAD Y AUTORIDAD

Elaboró / Actualizó:	Revisó:	Aprobó:
Nombre: Olga Patricia Duque F	Nombre: Yesenia Ines Arango Sanchez	Nombre: Eleonora Betancur González
Cargo: Profesional senior de calidad	Cargo: Coordinadora de Planeación	Cargo: Directora Ejecutiva