



**POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN**



**INSDEPORTES**  
CAJICÁ

**INSTITUTO DE DEPORTES Y RECREACION – CAJICA**

**FEBRERO DE 2019**





## **POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN**

El Director del INSTITUTO MUNICIPAL DE DEPORTES Y RECREACIÓN y los servidores públicos de los diferentes niveles que integran el Instituto, nos comprometemos a gestionar, administrar y ejercer un control efectivo para eliminar todos los posibles riesgos de corrupción que puedan impedir el cumplimiento de los objetivos y el normal desarrollo de los procesos institucionales.

Todos los procesos y dependencias deben establecer los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los programas, proyectos, planes, procesos y productos del Instituto, mediante:

- La identificación y documentación de riesgos de gestión (financieros, contractuales, jurídicos, entre otros), corrupción y de seguridad digital en los programas, proyectos, planes y procesos.
- El establecimiento de acciones de control y preventivas para los riesgos identificados.
- La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

Para administrar adecuadamente los riesgos el Instituto acoge la metodología de la Función Pública y determina las acciones para asumir, reducir y mitigar el riesgo al igual que establece planes de contingencia ante la materialización del riesgo.

### **OBJETIVO**

Orientar y fortalecer la toma de decisiones oportuna y minimizar los efectos adversos al interior del Instituto, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Ciudadanos, Servidores e Instituciones Públicas.

### **ALCANCE**

La política de riesgos es aplicable a todos los procesos y procedimientos del Instituto y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus actividades.

### **DEFINICION DE AMINISTRACION DEL RIESGO**

Riesgo es la 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.

La tendencia más común es la valoración del riesgo como una amenaza; en este sentido, los esfuerzos institucionales se dirigen a reducir, mitigar o eliminar su ocurrencia. Pero existe también la percepción del riesgo como una oportunidad, lo cual implica que su gestión está dirigida a maximizar los resultados que este genera.

La administración del riesgo comprende el conjunto de elementos de control y sus interrelaciones, para que el Instituto evalúe e intervenga aquellos eventos tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales.

La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a que se genere una cultura de Autocontrol y autoevaluación al interior de la misma.





## CONCEPTOS BÁSICOS RELACIONADOS CON EL RIESGO

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

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

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

**Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento

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

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

**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.

**Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

**Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

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

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

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

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

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

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

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





## TIPIFICACION DE ACCIONES DE CORRUPCION

Toda acción corrupta se realiza para la obtención de un beneficio personal, grupal, institucional o en ocasiones comunitario.

Dentro de las modalidades de corrupción tipificadas se encuentran:

1. Abuso de poder, que se expresa mediante el uso de oportunidades desde posiciones públicas o privadas, para obtener beneficios grupales o personales.
2. Carencia y/o debilidades de los procedimientos y mecanismos institucionales, que garanticen la transparencia en el ejercicio de las funciones.
3. Debilidad en los marcos legales que tipifican y sancionan la corrupción administrativa pública.
4. Reforzamiento de las actitudes individualistas y el consumismo, sustituyendo los valores éticos, como la solidaridad, honestidad y responsabilidad.
5. La impunidad en que se encuentran los actos de corrupción, sus expresiones más visibles el tráfico de influencias y la obtención de prebendas personales.
6. Corrupción política: Es la obtención de beneficios personales o grupales de manera ilícita, por el poder o vínculos con éste mediante el ejercicio de la actividad política o de representación.
7. Corrupción administrativa pública: Es el uso de la función pública para la obtención de beneficios personales, familiares o grupales en detrimento del patrimonio público.
8. Corrupción corporativa: Es el uso del soborno de parte de un sector económico o empresa para obtener beneficios corporativos.
9. Corrupción privada: Es aquella que violenta las normas y valores para obtener ventajas frente a otros.

## TIPOLOGÍA DE RIESGOS

**Calidad:** relacionados con los atributos de calidad establecidos en MIPG, las políticas de aseguramiento y Gestión de calidad.

**Contractual:** relacionado con los atrasos o incumplimientos de las etapas contractuales en cada vigencia

**Comunicación:** relacionado con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto

**Corrupción:** cuando por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia, del Estado, para la obtención de un beneficio particular

**Cumplimiento y conformidad:** se asocian con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad

**Estratégicos:** asociado a la administración de la Entidad, a la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, y el diseño de lineamientos que respondan a las necesidades de los grupos de valor e interés

**Financieros:** relacionado con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes





**Imagen:** relacionado con la percepción y la confianza por parte de los grupos de valor frente a la Entidad

**Información:** se asocia a la disponibilidad, confiabilidad e integridad de la información agregada y desagregada

**Integración:** Se refiere a la integración de sistemas, áreas, entidades, etapas y elementos que se requieran coordinar para el desarrollo de un proyecto

**Operativos:** riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias

**Recurso Humano:** Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función

**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.

### IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN

Se entiende por Riesgo de Corrupción la posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:

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

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto.

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo con el desarrollo del proceso.

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

### VALORACIÓN DE RIESGOS

Esto es 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).

### ANÁLISIS DE RIESGOS

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





**Análisis de la probabilidad:** Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	<b>Cási seguro</b>	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	<b>Probable</b>	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	<b>Posible</b>	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	<b>Improbable</b>	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	<b>Rara vez</b>	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

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

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
<b>CATASTRÓFICO</b>	<ul style="list-style-type: none"><li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 50\%</math>.</li><li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 50\%</math>.</li><li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 50\%</math>.</li><li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 50\%</math> del presupuesto general de la entidad.</li></ul>	<ul style="list-style-type: none"><li>- Interrupción de las operaciones de la entidad por más de cinco (5) días.</li><li>- Intervención por parte de un ente de control u otro ente regulador.</li><li>- Pérdida de información crítica para la entidad que no se puede recuperar.</li><li>- Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.</li><li>- Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.</li></ul>





<b>MAYOR</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 20\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 20\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 20\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 20\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Interrupción de las operaciones de la entidad por más de dos (2) días.</li> <li>- Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.</li> <li>- Sanción por parte del ente de control u otro ente regulador.</li> <li>- Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.</li> <li>- Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.</li> </ul>
--------------	--	---

NIVEL	IMPACTO ( CONSECUENCIAS ) CU ANTITATIVO	IMPACTO ( CONSECUENCIAS ) CU ALITATIVO
<b>MODERADO</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 5\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 10\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 5\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Interrupción de las operaciones de la entidad por un (1) día.</li> <li>- Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.</li> <li>- Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.</li> <li>- Reproceso de actividades y aumento de carga operativa.</li> <li>- Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.</li> <li>- Investigaciones penales, fiscales o disciplinarias.</li> </ul>
<b>MEJOR</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 1\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 5\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 1\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 1\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Interrupción de las operaciones de la entidad por algunas horas.</li> <li>- Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.</li> <li>- Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.</li> </ul>



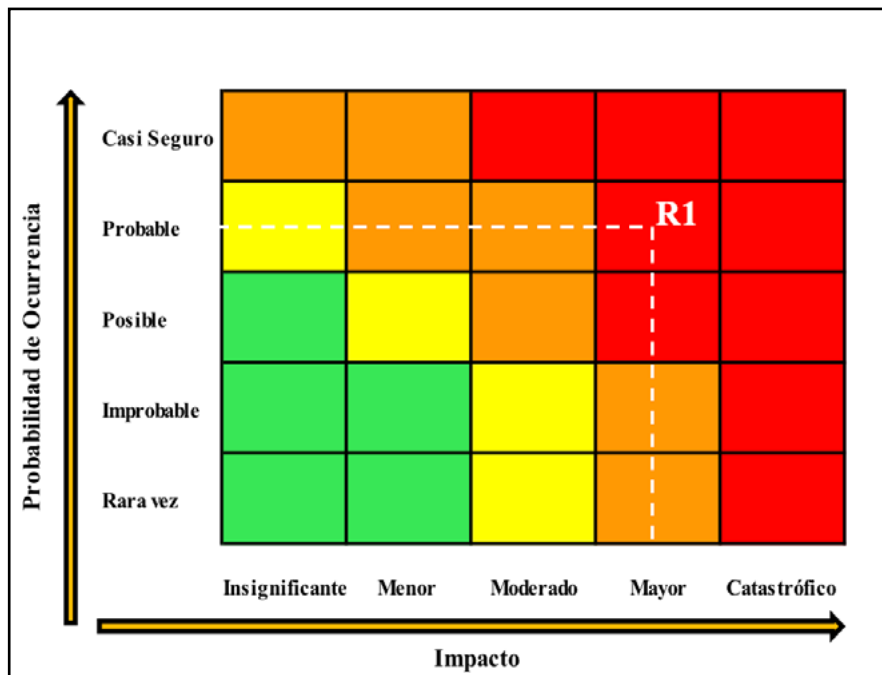


<b>INSIGNIFICANTE</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 0,5\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 1\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 0,5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 0,5\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- No hay interrupción de las operaciones de la entidad.</li> <li>- No se generan sanciones económicas o administrativas.</li> <li>- No se afecta la imagen institucional de forma significativa.</li> </ul>
-----------------------	--	--

### 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:** Se toma la calificación de probabilidad resultante de la tabla “Matriz de priorización de probabilidad, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, así se podrá determinar el riesgo inherente.







## EVALUACIÓN DE RIESGOS

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.

### **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.

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables

**Responsable:** Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución

**Periodicidad:** El control debe tener una periodicidad específica para su realización 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.

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

**Cómo Se Realiza:** El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.

**Qué Pasa Con Las Observaciones o Desviaciones:** El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Sigamos con nuestros ejemplos prácticos de ayuda, para la interiorización de estos conceptos





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

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo 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

### MONITOREO Y REVISIÓN

**Modelo De Las Líneas De Defensa:** Es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG de "Control interno", que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

**Línea Estratégica:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno.

**Actividades de Monitoreo y Revisión a Realizar:** La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente:

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

Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos.

Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.

Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo 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





## 1ª. LÍNEA DE DEFENSA

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Está conformada por el Director y líderes de los procesos, programas y proyectos de la entidad.

**Actividades de monitoreo y revisión a Realizar:** El Director 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.

Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.

Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

Revisar y reportar a la Dirección, 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.

## 2ª. LÍNEA DE DEFENSA

Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos, incluyendo los riesgos de corrupción a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo.

**Actividades de monitoreo y revisión a Realizar:** El Director y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos instituciones y de sus procesos a través de una adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente:

Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.





Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.

Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.

Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.

Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos

### 3ª. LÍNEA DE DEFENSA

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. La tercera línea de defensa está conformada por la oficina de control interno.

**Actividades de monitoreo y revisión a Realizar:** La oficina de control interno monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, además de incluir los riesgos de corrupción con relación a lo siguiente:

Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.

Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.

Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de 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.

Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.





## MONITOREO DE RIESGOS DE CORRUPCIÓN

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

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

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

### Reporte de la gestión del riesgo

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

## INFORMACIÓN, COMUNICACIÓN Y REPORTE

### Línea Estratégica

Corresponde al Comité de Auditoría del Instituto y/o a los comités institucionales de coordinación de control interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

### Primera Línea De Defensa

Corresponde a los líderes de proceso (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

### Segunda Línea De Defensa

Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación

### Tercera Línea De Defensa

Le corresponde a la oficina de control interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

