POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

E.S.E Centro de Salud de Usiacurí
José María Ferez Farah
Nuestro compromiso es tu salud

Resolución 081 de 2025

CODIGO GE-POL-011	**POLITICA DE ADMINISTRACION DEL RIESGO.**	VIGENCIA:2025-11-12
VERSION: 1		PÁGINA: Página **1** de **16**

Contenido

1. INTRODUCCIÓN 2
2. OBJETIVO GENERAL 3
3. OBJETIVOS ESPECIFICOS. 3
4. APLICACIÓN Y ALCANCE. 3
5. GLOSARIO. 4
6. POLÍTICA DE CONTROL INTERNO. 6
7. NIVELES DE ACEPTACIÓN DEL RIESGO. 6
8. RESPONSABILIDADES. 7
9. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS DE PROCESO Y SEGURIDAD DIGITAL. 9
10. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS DE CORRUPCIÓN. 10
11. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS FISCALES. 10
12. NIVEL DE CALIFICACIÓN DE IMPACTO. 11
13. CLASIFICACIÓN DEL IMPACTO PARA LOS RIESGOS DE CORRUPCIÓN. 11
14. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS. 12
15. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN. 13
16. SEGUIMIENTOS AL MAPA DE CORRUPCIÓN. 14
17. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN. 15

1. INTRODUCCIÓN

La E.S.E. Centro de Salud de Usiacurí "José María Ferez Farah" orienta su gestión al cumplimiento efectivo de los objetivos estratégicos y misionales asociados a la prestación integral de los servicios de salud, reconociendo que la adecuada administración de los riesgos es un factor determinante para garantizar la continuidad, calidad y oportunidad de la atención. En este contexto, la entidad adopta acciones preventivas y correctivas que permitan anticipar y controlar los eventos que puedan afectar el desarrollo normal de sus procesos institucionales.

La gestión del riesgo se fundamenta en la aplicación de controles oportunos y eficaces que contribuyan a disminuir la probabilidad de ocurrencia y el impacto de los riesgos identificados. Para ello, la E.S.E. impulsa una cultura organizacional basada en la integridad, la transparencia y la responsabilidad, fortaleciendo así la confianza de los ciudadanos, la gobernanza institucional y el compromiso de los servidores públicos con la gestión ética y eficiente de los recursos.

Dada la complejidad y constante transformación del entorno del sector público, la administración del riesgo se convierte en un elemento esencial de la función directiva. En atención a esta necesidad, la E.S.E. Centro de Salud de Usiacurí "José María Ferez Farah" establece la presente Política de Administración del Riesgo como un instrumento estratégico que orienta la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos, asegurando su alineación con los objetivos institucionales y el logro de los resultados esperados.

En concordancia con la normatividad vigente y la metodología definida por el Departamento Administrativo de la Función Pública, la entidad adopta los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 7, incorporando el análisis del riesgo fiscal y el uso del Catálogo Indicativo de Puntos de Riesgo Fiscal. Este enfoque fortalece el modelo de operación por procesos y permite una gestión integral, coherente y sistemática del riesgo.

La implementación de la presente política constituye un instrumento de gestión orientado al fortalecimiento del sistema de administración del riesgo institucional, en concordancia con los principios de eficiencia, eficacia y efectividad de la gestión pública en salud. A través de un enfoque preventivo, sistemático y basado en procesos, la E.S.E. propende por la optimización del uso de los recursos, la mitigación de la materialización de riesgos y la adopción de medidas oportunas que aseguren la continuidad operativa, el cumplimiento de los objetivos institucionales y el mejoramiento continuo de la calidad en la prestación de los servicios de salud.

2. OBJETIVO GENERAL

Establecer los lineamientos y directrices para la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos institucionales, incluidos los riesgos fiscales, en la E.S.E. Centro de Salud de Usiacurí "José María Ferez Farah", con el fin de prevenir la materialización de eventos que puedan afectar el cumplimiento de los objetivos misionales y estratégicos, fortalecer el sistema de control interno, optimizar el uso de los recursos públicos y garantizar la continuidad, calidad y eficiencia en la prestación de los servicios de salud.

3. OBJETIVOS ESPECIFICOS.

- Identificar y actualizar de manera sistemática los riesgos estratégicos, operativos, financieros, de cumplimiento, tecnológicos y de corrupción que puedan afectar el logro de los objetivos institucionales de la E.S.E.

- Analizar y evaluar los riesgos identificados, estableciendo su nivel de probabilidad e impacto, con el fin de priorizar su tratamiento y definir controles adecuados.

- Diseñar e implementar acciones y controles efectivos que permitan prevenir, mitigar o reducir la materialización de los riesgos institucionales y fiscales.

- Promover una cultura organizacional orientada a la gestión del riesgo, fortaleciendo la responsabilidad de los servidores públicos en la identificación, administración y control de los riesgos asociados a los procesos.

- Realizar el seguimiento y monitoreo permanente a los riesgos y controles definidos, garantizando su eficacia, su articulación con el Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión – MIPG.

4. APLICACIÓN Y ALCANCE.

La presente Política de Administración del Riesgo será de obligatorio cumplimiento en la E.S.E. Centro de Salud de Usiacurí "José María Ferez Farah" y aplicará a todos los niveles de la estructura organizacional, procesos, programas, proyectos y actividades que adelante la entidad, cualquiera sea su naturaleza o fuente de financiación. Su observancia será responsabilidad de la alta dirección, los servidores públicos, contratistas y demás actores que participen en la gestión institucional, de acuerdo con sus funciones y responsabilidades.

El alcance de la política comprende la identificación, análisis, evaluación, tratamiento, seguimiento y monitoreo de los riesgos estratégicos, operativos, financieros, de cumplimiento, tecnológicos, de corrupción y riesgos fiscales que puedan afectar el cumplimiento de los objetivos misionales y

estratégicos de la entidad, en articulación con el Sistema de Control Interno, el Modelo Integrado de Planeación y Gestión – MIPG y el modelo de operación por procesos, conforme a la normatividad vigente y a los lineamientos establecidos por el Departamento Administrativo de la Función Pública.

5. GLOSARIO.

Para la implementación de la política es importante contemplar los siguientes términos que permitirá determinar tanto el vocabulario como las expresiones, con lo que, entre otras cosas, se conseguirá que los textos sean más coherentes y homogéneos y así evitará la posibilidad de encontrar terminología distinta en esta política:

- **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.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del 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 del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Autocontrol:** capacidad que deben desarrollar todos y cada uno de los servidores públicos de la organización, independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos de manera oportuna para el adecuado cumplimiento de los resultados que se esperan en el ejercicio de su función, de tal manera que la ejecución de los procesos, actividades y/o tareas bajo su responsabilidad, se desarrollen con fundamento en los principios establecidos en la Constitución Política.
- **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.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Contingencia:** posible evento futuro, condición o eventualidad.

CODIGO GE-POL-011	**POLITICA DE ADMINISTRACION DEL RIESGO.**	VIGENCIA:2025-11-12
VERSION: 1		PÁGINA: Página **5** de **16**

- **Continuidad del negocio:** capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **Control:** medida que permite reducir o mitigar un riesgo.
- Crisis: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Integridad:** propiedad de exactitud y completitud.
- **Mapa de riesgos:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **OTIC:** Oficina de las Tecnologías de la Información y las Comunicaciones.
- **OAC:** Oficina Asesora de Comunicaciones.
- **OAP:** Oficina Asesora de Planeación.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. 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.
- **Restablecimiento:** capacidad e la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- 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).
- **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 Fiscal:** efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **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.
- **SGI:** Sistema Gestión Institucional, aplicativo propio para la gestión de planeación riesgos e indicadores.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. POLÍTICA DE CONTROL INTERNO.

La E.S.E. Centro de Salud de Usiacuri asume la Política de Administración del Riesgo como un componente estratégico de la gestión institucional, fundamentado en el Modelo Integrado de Planeación y Gestión – MIPG y desarrollado conforme a los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Esta política se orienta bajo un enfoque preventivo y sistemático, soportado en el seguimiento y la evaluación permanente de la gestión y los controles, el mejoramiento continuo y la participación activa, responsable y articulada de todos los servidores públicos de la entidad.

La Política de Administración del Riesgo se aplica de manera transversal a todos los sistemas de gestión y a los procesos definidos en el Modelo de Operación por Procesos, abarcando de forma integral las etapas de contextualización, identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos institucionales. En este marco, la E.S.E. se compromete a gestionar de manera oportuna y eficaz:

- Los riesgos de gestión y de proceso que puedan afectar el cumplimiento de la misión, los objetivos estratégicos y los resultados institucionales.
- Los riesgos asociados a posibles actos de corrupción, mediante la implementación de controles preventivos que eviten el uso indebido del poder público para la obtención de beneficios particulares.
- Los riesgos de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de la información asociada a los procesos institucionales.
- Los riesgos fiscales, orientados a prevenir el detrimento, daño o afectación de los recursos públicos, bienes e intereses patrimoniales de naturaleza pública.

7. NIVELES DE ACEPTACIÓN DEL RIESGO.

De conformidad con los riesgos residuales aprobados por los líderes de proceso y socializados ante el Comité Institucional de Coordinación de Control Interno, se establecerá la periodicidad de seguimiento y la estrategia de tratamiento aplicable a los riesgos residuales aceptados, atendiendo a su nivel de exposición y a los criterios de aceptación definidos por la entidad.

La E.S.E. Centro de Salud de Usiacuri “Jose Maria Ferez Farah”, determina que los riesgos residuales de gestión y de seguridad digital que se clasifiquen en zona de riesgo baja podrán ser aceptados, sin que se requiera la formulación de planes de acción específicos; no obstante, deberán ser objeto de monitoreo periódico conforme a la frecuencia previamente establecida.

En el caso de los riesgos de corrupción, no procederá la aceptación del riesgo, por lo cual su identificación deberá conllevar de manera obligatoria la definición e implementación de acciones orientadas al fortalecimiento de los controles y a la mitigación permanente de dichos riesgos.

8. RESPONSABILIDADES.

Líneas de Defensa	Responsable	Responsabilidad Frente al Riesgo
Línea estratégica	**Comité Institucional de Gestión y Desempeño**	• Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. • Generar recomendaciones de mejora a la política de administración del riesgo para su análisis e inclusión.
	Comité Institucional de Coordinación de Control Interno	• Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización. • Evaluar la eficacia de la política frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Monitorear los riesgos críticos identificados (aquellos definidos en los niveles de severidad Alto y Extremo, independientemente de su nivel de probabilidad), mediante el análisis de eventos o materializaciones u otra información aportada por las instancias de 2ª línea identificadas. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios, a partir de la información aportada por las instancias de 2ª línea identificadas. • Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad.
Primera Línea	**Líderes de Proceso**	• El líder del proceso debe: • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos operativos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso.

	Integrantes del Equipo de Trabajo	• Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos operativos identificados y proponer mejoras para su gestión. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Realizar el seguimiento al mapa de riesgos de su proceso. • Informar a la segunda línea de defensa sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • En caso de la materialización de un riesgo no identificado debe ser incluido en el mapa de riesgo institucional. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. Los integrantes de equipo de trabajo deben: • Participar en el diseño de los controles que tienen a cargo. • Ejecutar los controles a su cargo de la forma como están diseñados. • Informar a su superior jerárquico sobre riesgos materializados o posibles situaciones de afectación al proceso, a fin de incorporar las acciones a que haya lugar. • Proponer mejoras a los controles existentes.
Segunda Línea	**Líderes de Programa de Proyecto, Jefes de oficina unidad o área**	Esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Consolidar el mapa de riesgos institucional (riesgos operativos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el CGDI. • Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos.

		• Acompañar y orientar a los procesos en la ejecución y efectividad de los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y/o que sea detectada por la Unidad de Transparencia y Gobierno Abierto durante la ejecución de los procesos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Evaluar que la gestión de los riesgos operativos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos operativos identificados. • Socializar y publicar el mapa de riesgos institucional.
Tercera Línea	**Oficina de Control Interno de Gestión.**	• Asesorar y orientar sobre la metodología para la identificación, análisis y valoración del riesgo. • Analizar el diseño e idoneidad de los controles establecidos en los procesos. • Realizar seguimiento a los riesgos consolidados en el mapa de riesgos de gestión (dos veces al año), mapa de riesgos de corrupción (tres veces al año según la norma) de conformidad con el Plan Anual de Auditoría. • Recomendar mejoras a la política de administración del riesgo.

9. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS DE PROCESO Y SEGURIDAD DIGITAL.

Calificación de probabilidad para riesgos proceso y seguridad digital.

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 1501 veces al año
80%	Alta	La actividad se realiza entre 366 a 1500 veces al año
60%	Media	La actividad se realiza entre 25 a 365 veces al año.

40%	Baja	La actividad se realiza entre 5 a 24 veces al año.
20%	Muy Baja	La actividad se realiza máximo 4 veces al año.

10. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS DE CORRUPCIÓN.

Calificación de probabilidad para riesgos corrupción.

Nivel	Descriptor	Probabilidad	Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

11. NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS FISCALES.

Calificación de probabilidad para riesgos fiscales

Nivel	Descriptor	Probabilidad	Descripción
5	Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
4	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
2	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
1	Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5001 veces por año.	100%

12. NIVEL DE CALIFICACIÓN DE IMPACTO.

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala.

Nivel	Descriptor	Descripción Económica o Presupuestal	Descripción Reputaciones
100%	Catastrófico	Pérdida económica superior a 5000 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país.
80%	Mayor	Pérdida económica de 100 hasta 500 SMLV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
60%	Moderado	Pérdida económica de 50 hasta 100 SMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
40%	Menor	Pérdida económica de 10 hasta 50 SMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores.
20%	Leve	Pérdida económica menor 10 SMLV	El riesgo afecta la imagen de alguna área de la organización

13. CLASIFICACIÓN DEL IMPACTO PARA LOS RIESGOS DE CORRUPCIÓN.

N°	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	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		

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

Nivel	Descriptor	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19

14. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS.

En el caso de materialización de riesgo, se debe realizar un análisis del riesgo y sus controles, este debe incluir la evaluación del impacto en los objetivos de la entidad, la revisión y ajuste de los controles existentes, y la medición de su efectividad, eficiencia y eficacia. En base a este análisis, se deben implementar acciones correctivas y preventivas para mitigar los riesgos y garantizar que la organización pueda gestionar futuros eventos de manera más efectiva. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

- **Calificación del riesgo:** se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- **Bajo el criterio de probabilidad:** el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones.

Para prevenir la ocurrencia de riesgos, se deben tomar medidas encaminadas a **rediseñar**, **mejorar** o **eliminar** aspectos dentro de los procesos de la organización, con base en los **ajustes de controles** y las **acciones correctivas** emprendidas. Estos cambios pueden incluir la optimización de procesos, la eliminación de prácticas obsoletas, la actualización de tecnologías, el fortalecimiento de los controles internos y la promoción de una cultura organizacional preventiva. La implementación de estos cambios sustanciales no solo reduce la probabilidad de que un riesgo se materialice, sino que también fortalece la capacidad de la organización para gestionar futuros riesgos de manera eficiente.

15. ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN.

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente

La **Oficina de Control Interno** (OCI) desempeña un papel clave en la gestión de los riesgos dentro de una organización. Para lograr que los **controles internos sean efectivos** y estén alineados con los riesgos, y para garantizar que estén funcionando de manera oportuna y efectiva, la OCI debe implementar una serie de medidas y prácticas que aseguren que los controles no solo existan, sino que realmente **mitiguen los riesgos** y **cumplan con los objetivos establecidos**. A continuación, se describen algunas estrategias y pasos fundamentales para lograr este objetivo:

- 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.

Cuando se materialicen riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Acciones de respuesta a riesgos.

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	**Líder de Proceso**	• Informar al Líder de Planeación Institucional como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar la alerta de posible materialización. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de

		corrupción materializado), determinar la aplicabilidad del proceso disciplinario. o Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. o Efectuar el análisis de causas y determinar acciones preventivas y de mejora. o Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	• Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	**Líder de Proceso**	• Informar al Líder de Planeación Institucional como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.
Riesgos de Gestión y Seguridad digital	**Oficina de Control Interno**	• Informar al líder del proceso sobre el hecho encontrado • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.

16. SEGUIMIENTOS AL MAPA DE CORRUPCIÓN.

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento – Controles

Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en la hoja de Excel; Mapa de riesgo, columna AM y AN.
	Moderada	Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en la hoja de Excel; Mapa de riesgo, columna AM y AN.
	Alta	Se realiza seguimiento a los controles con periodicidad BIIMESTRAL y se registran sus avances en la hoja de Excel; Mapa de riesgo, columna AM y AN.
	Extrema	Se realiza seguimiento a los controles con periodicidad BIIMESTRAL y se registran sus avances en la hoja de Excel; Mapa de riesgo, columna AM y AN.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento TRIMESTRAL y se registra en la hoja de Excel; Mapa de riesgo, columna AL, AM y AN.	

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) prime ros días del mes de mayo.
- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

17. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN.

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de acción
Riesgos de Gestión, y Seguridad digital	**Baja**	No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo por Función Pública
	Moderada Alta Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.