POLITICA ADMINISTRACIÓN DEL RIESGO

1. INTRODUCCION

El Instituto Departamental de Cultura del Meta, reconociendo la importancia que tiene la administración de los riesgos, y atendiendo los lineamientos establecidos por el Departamento Administrativo de la Función Pública -DAFP-, a través del Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno -MECI-, la guía para la administración de los riesgos de gestión, corrupción y seguridad digital y el diseño de controles en entidades públicas en su cuarta versión de fecha octubre de 2018, se compromete con la identificación, tratamiento y control de riesgos y oportunidades, mediante la formulación de la política institucional de administración del riesgo, como una manifestación de la alta dirección para controlar dichos riesgos y así asegurar mejores y mayores resultados en la gestión para el cumplimiento de las metas establecidas en el Plan de Desarrollo Departamental, la Política Pública Cultural del Meta, los objetivos y funciones institucionales.

La política de administración de riesgos se constituye así en un mecanismo base para la identificación, caracterización, calificación, clasificación, seguimiento y evaluación de los riesgos que se puedan presentar en todos los procesos de la institución y en las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

2. OBJETIVO

Orientar la toma de decisiones respecto al tratamiento de los riesgos y sus efectos, al interior de la Administración del Instituto Departamental de Cultura del Meta, con el fin de garantizar el cumplimiento de la misión, objetivos y funciones institucionales

3. ALCANCE

La administración de los riesgos de gestión, seguridad digital y de corrupción es parte del direccionamiento estratégico y será aplicable de manera permanente en el Instituto Departamental de Cultura del Meta a todos los procesos, planes institucionales, proyectos, productos de la Entidad y a las acciones ejecutadas por todos los servidores durante el ejercicio de sus funciones.

4. DEFINICIONES

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 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.

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.

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.

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.

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.

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

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

Integridad: Propiedad de exactitud y completitud de la información.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

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

Aceptar el riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Administración de riesgos: Conjunto de elementos de control que al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función, se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública auto controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

5. RESPONSABLE

El responsable de la ejecución de la política de administración del riesgo es el Director del Instituto, con el apoyo de la subdirectora general y la subdirectora operativa.

6. DESARROLLO

6.1 CLASES DE RIESGOS

- **Riesgo Estratégico:** Se asocia a la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, la definición de los procesos, la estructura de la entidad y la articulación entre dependencias.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad, que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

- **De Corrupción:** Se asocian al uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Seguridad Digital:** Se refiere a la combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos institucionales y afectar la autonomía, principios e integridad de la entidad. Incluye aspectos como el ambiente físico y digital, como temas de seguridad de la información

6.2 METODOLOGÍA

El soporte y la metodología de la Administración del Riesgo están sujetos a las orientaciones que sobre la materia imparte el Departamento Administración de la Función Pública. El mapa o matriz de riesgos será la herramienta conceptual y metodológica para la valoración de los riesgos.

Se construirá el mapa de riesgos por cada uno de los líderes de los procesos del Instituto, quienes serán los responsables de la construcción del mapa de riesgos de su proceso y la Subdirección Operativa se encargará de la consolidación del mapa de riesgo institucional.

6.3 NIVELES DE ACEPTACIÓN DEL RIESGO

Tipos de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Gestión (Proceso, Producto y Proyecto)	Baja	Se ASUMIRÁ el riesgo y se administrará por medio de las actividades propias del proyecto o proceso asociado
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo; se hace seguimiento TRIMESTRAL.
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan MITIGAR la materialización del riesgo. Se monitorea MENSUALMENTE
Riesgos de Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad TRIMESTRAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
Riesgos de Corrupción	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Periodicidad TRIMENTRAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos
Riesgos de Corrupción	Alta y Extrema	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, decidiendo no iniciar o no

Tipos de riesgo	Zona de riesgo	Nivel de aceptación
		continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos

6.4 ANALISIS DE CONTEXTO

La administración del Instituto Departamental de Cultura se puede ver afectada por los cambios normativos derivados de la aplicación de las políticas nacionales, para dar cumplimiento al nuevo Plan Nacional de Desarrollo, y demás legislación que establezca el gobierno nacional, tanto a nivel de políticas institucionales de cultura como de las fuentes de financiación para proyectos, de talento humano entre otros aspectos.

Este año se desarrollará un proceso electoral, que va a afectar el funcionamiento de la entidad el próximo año al presentarse un cambio de gobierno a nivel Departamental, lo que puede conllevar a la designación de nuevas personas en los cargos de libre nombramiento y remoción, transformación del Plan de Desarrollo Departamental, ajuste a políticas y prioridades de la nueva administración. Todo esto alterará el ámbito interno de la institución, que se debe valorar al momento de realizar al análisis de los riesgos institucionales de las diferentes áreas o dependencias.

Dentro del contexto interno es importante tener identificada la plataforma estratégica (Misión, visión, objetivos, valores corporativos), y que ésta haya sido socializada y conocida por todo el personal del Instituto.

Con lo anterior es importante tener encuenta la necesidad de realizar un ajuste a esta política.

6.5 IDENTIFICACION DEL RIESGO:

La identificación de los riesgos corresponde a la determinación de las causas que generan eventos o situaciones que pueden afectar o entorpecer el desarrollo y/o cumplimento de los objetivos del proceso, partiendo de los contextos interno y/o externo. Con el fin de identificar los riesgos, en cada proceso se debe dar respuesta a las siguientes interrogantes:

¿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 al desarrollo del proceso.

¿Qué consecuencia tendría su materialización? Determinar los posibles efectos por la materialización del riesgo.

Teniendo en cuenta que los riesgos de corrupción son inadmisibles y que su descripción debe ser más detallada, en la definición de las causas de los riesgos de corrupción se deberá incluir la especificación de los siguientes criterios:

- Si son riesgos causados por acción u omisión.
- Si son riesgos causados por uso del poder
- Si son riesgos causados por desviar la gestión de lo público
- Si son riesgos causados por beneficio personal

6.6 ANÁLISIS DE RIESGOS

6.6.1 Criterios de Calificación de la Probabilidad

La probabilidad se entiende como la posibilidad de que un riesgo identificado se materialice, y su determinación se lleva a cabo partiendo de criterios de frecuencia de ocurrencia (análisis histórico de materialización de riesgos), o de factibilidad (presencia de factores internos o externos que propicien la materialización del riesgo). Para los riesgos de corrupción, la calificación, en todos los casos, se deberá hace en los niveles 3 al 5 de los criterios de calificación.

- Definición de la probabilidad a partir de la frecuencia: Cuando se cuenta con datos históricos de materialización del riesgo, la calificación de la probabilidad se lleva a cabo aplicando la siguiente matriz de calificación.

Tabla 2 Criterios parar Calificar la Probabilidad según la Frecuencia

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA HISTÓRICA DE OCURRENCIA
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.

Fuente: Guía para la administración de los riesgos de gestión, corrupción y seguridad digital y el diseño de controles en entidades públicas en su cuarta versión – Octubre de 2018

6.6.2 Criterios de Calificación del impacto

La calificación del impacto se realizará de acuerdo con los criterios definidos en la guía para la administración de los riesgos de gestión, corrupción y seguridad digital versión 4 de octubre de 2018

CRITERIOS PARA EVALUAR EL IMPACTO PARA RIESGOS DE GESTIÓN

NIVEL	CALIFICACIÓN	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
1	Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≤1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≤5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤1%. - Pago de sanciones económicas por incumplimiento en la normatividad ante un ente regulador, las cuales afectan en un valor ≤1% del presupuesto de la entidad	No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.
2	Menor	Impacto que afecte la ejecución presupuestal en un valor >1% hasta ≤5%. - Pérdida de cobertura en la prestación de los servicios de la entidad >5% a hasta ≤10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor >1% hasta ≤5%. - Pago de sanciones económicas por incumplimiento en la normatividad ante un ente regulador, las cuales afectan en un valor >1% y ≤5% del presupuesto de la entidad.	Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
3	Moderado	Impacto que afecte la ejecución presupuestal en un valor >5% y ≤20%. - Pérdida de cobertura en la prestación de los servicios de la entidad >10% y ≤20%. - Pago de indemnizaciones a terceros por acciones legales que	Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información,

NIVEL	CALIFICACIÓN	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
		pueden afectar el presupuesto total de la entidad en un valor >5% y ≤20%. - Pago de sanciones económicas por incumplimiento en la normatividad ante un ente regulador, las cuales afectan en un valor >5% y ≤20% del presupuesto de la entidad.	ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias
4	Mayor	Impacto que afecte la ejecución presupuestal en un valor >20% y ≤50%. - Pérdida de cobertura en la prestación de los servicios de la entidad >20% y ≤50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor >20% y ≤50%. - Pago de sanciones económicas por incumplimiento en la normatividad ante un ente regulador, las cuales afectan en un valor >20% y ≤50% del presupuesto de la entidad.	Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
5	Catastrófico	Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto de la entidad.	Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

CRITERIOS PARA CALIFICAR EL IMPACTO – RIESGOS DE SEGURIDAD DIGITAL

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
Insignificante	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
Menor	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
Moderado	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Mayor	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
			interés particular de los empleados y terceros.
Catastrófico	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

CRITERIOS PARA CALIFICAR EL IMPACTO – RIESGOS DE CORRUPCION

NIVEL	CLASIFICACIÓN	
Moderado	3	Se considerará riesgo de corrupción con consecuencias de nivel moderado, cuando la materialización del riesgo pueda presentar de una a cinco de las siguientes situaciones: - Afectar al grupo de funcionarios del proceso - Afectar el cumplimiento de metas y objetivos de la dependencia - Afectar el cumplimiento de misión de la Entidad - Afectar el cumplimiento de la misión del sector al que pertenece la Entidad - Generar pérdida de confianza de la Entidad, afectando su reputación - Generar pérdida de recursos económicos - Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos - Generar pérdida de información de la Entidad - Generar intervención de los órganos de control, de la Fiscalía, u otro ente - Dar lugar a procesos sancionatorios - Dar lugar a procesos disciplinarios - Dar lugar a procesos fiscales

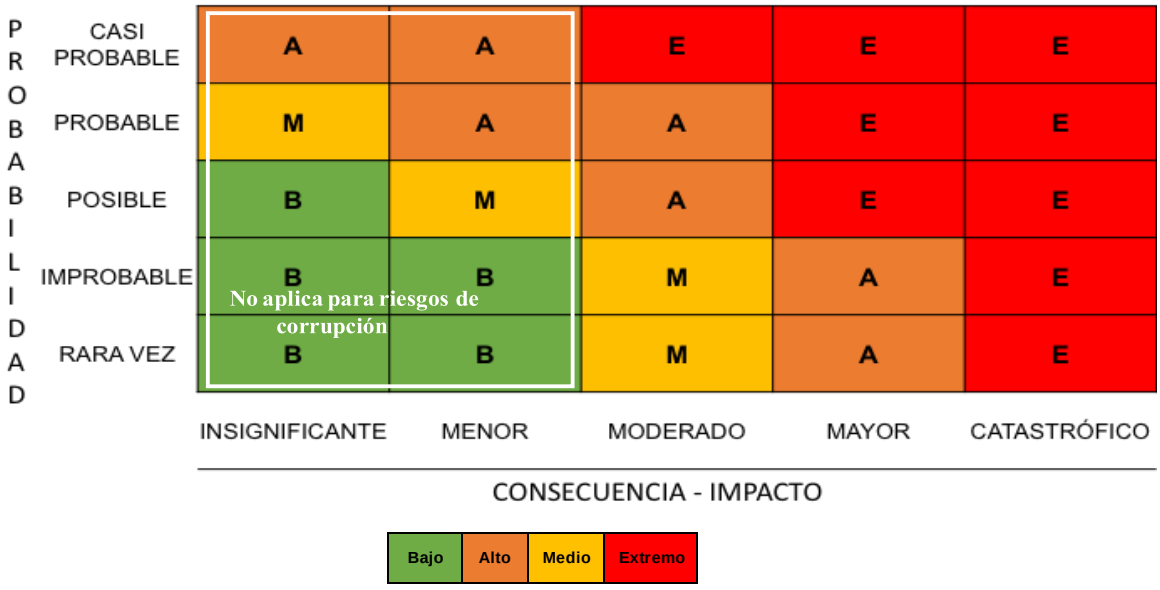
NIVEL	CLASIFICACIÓN	
		- Dar lugar a procesos penales - Generar pérdida de credibilidad del sector - Afectar la imagen regional - Afectar la imagen nacional - Generar daño ambiental
Mayor	4	Se considerará riesgo de corrupción con consecuencias de nivel mayor, cuando la materialización del riesgo pueda presentar de seis a once de las siguientes situaciones: - Afectar al grupo de funcionarios del proceso - Afectar el cumplimiento de metas y objetivos de la dependencia - Afectar el cumplimiento de misión de la Entidad - Afectar el cumplimiento de la misión del sector al que pertenece la Entidad - Generar pérdida de confianza de la Entidad, afectando su reputación - Generar pérdida de recursos económicos - Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos - Generar pérdida de información de la Entidad - Generar intervención de los órganos de control, de la Fiscalía, u otro ente - Dar lugar a procesos sancionatorios - Dar lugar a procesos disciplinarios - Dar lugar a procesos fiscales - Dar lugar a procesos penales - Generar pérdida de credibilidad del sector - Afectar la imagen regional - Afectar la imagen nacional Generar daño ambiental
Catastrófico	5	El primer criterio para calificar un riesgo de corrupción como catastrófico es si la materialización del riesgo puede ocasionar lesiones físicas o pérdida de vidas humanas El segundo criterio para calificar un riesgo como catastrófico es cuando la materialización del riesgo pueda presentar de doce a diez y nueve de las siguientes situaciones: - Afectar al grupo de funcionarios del proceso - Afectar el cumplimiento de metas y objetivos de la dependencia - Afectar el cumplimiento de misión de la Entidad - Afectar el cumplimiento de la misión del sector al que pertenece la Entidad - Generar pérdida de confianza de la Entidad, afectando su reputación - Generar pérdida de recursos económicos - Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos - Generar pérdida de información de la Entidad

NIVEL	CLASIFICACIÓN	
		- Generar intervención de los órganos de control, de la Fiscalía, u otro ente - Dar lugar a procesos sancionatorios - Dar lugar a procesos disciplinarios - Dar lugar a procesos fiscales - Dar lugar a procesos penales - Generar pérdida de credibilidad del sector - Afectar la imagen regional - Afectar la imagen nacional - Generar daño ambiental

6.7 VALORACIÓN DE RIESGOS

A través de la valoración de Riesgos se busca establecer la probabilidad de que los mismos ocurran, y las consecuencias de dicha materialización, con el fin de establecer la categoría de zona de los riesgos (inherente y residual), para lo cual se determina en primera instancia la probabilidad, y en segunda instancia la evaluación del impacto.

El mapa de calor corresponde a una matriz cuadrada, en la cual se proyectan los 5 criterios de probabilidad y los 5 criterios de impacto, buscando el punto de intersección entre los dos ejes, y así definir en una escala cualitativa, el nivel importancia del riesgo.



Fuente: Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 4 Octubre de 2018

6.8 SEGUIMIENTO Y EVALUACIÓN

La evaluación y seguimiento al levantamiento de los mapas de riesgos será de responsabilidad de las dos Subdirecciones de la entidad.

La primera línea de defensa, es decir las subdirecciones deben realizar las siguientes actuaciones.

Revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y revisar que las actividades de control de sus procesos eliminen las causas y se encuentren documentadas y actualizadas en los procedimientos

La segunda línea de defensa, es decir el líder de cada procedimiento, supervisores, e interventores de contratos.

- 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 realizar 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 procedimientos se encuentren documentados y actualizados.
- 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

El ultimo seguimiento y evaluación debe realizarse desde la oficina de Control Interno, como la **tercera línea de defensa**, quien deberá realizar el examen sistemático e independiente para determinar si las actividades y los resultados relacionados con la administración de riesgos, cumplen las disposiciones de las políticas, planes y acciones preestablecidos y si se aplican en forma efectiva y son aptas para alcanzar los objetivos. Además actuará como eje central de coordinación del monitoreo y reporte de riesgos y posibles desviaciones, sin comprometer su independencia y objetividad, así mismo y por lo menos una vez al año, comunicará al Comité Coordinador de Control Interno los resultados del seguimiento y evaluación a las políticas y al procedimiento de administración del riesgo, junto con las propuestas de mejoramiento y tratamiento a las situaciones detectadas.

7. ELABORACIÓN, REVISIÓN Y APROBACIÓN

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	SEPAD S.A.S	Sonia Luz Hernández Cruz	Comité Institucional de Gestión y Desempeño
CARGO	Contratista	Asesora de Control Interno	
FIRMA			

8. CONTROL DE CAMBIOS

Revisión	Versión No.	Fecha	Cambio
Nuevo	01	Mayo de 2019	Creación del Documento