POLÍTICA ADMINISTRACIÓN DEL RIESGO

La política del riesgo se define atendiendo los lineamientos establecidos en guía para la administración del riesgo del Departamento Administrativo de la Función Pública DAFP, articulada con las normas aplicables a la entidad y al Sistema Integrado de Gestión SIG, como mecanismo para identificar, analizar, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar el logro de los objetivos institucionales.

1. OBJETIVO:

La Política de Administración del Riesgo de la Alcaldía de Acacías (Meta), tiene como objetivo establecer los parámetros necesarios que conduzcan a minimizar la vulnerabilidad de los riesgos institucionales frente a situaciones que puedan obstaculizar el desarrollo de su misión y el logro de los objetivos institucionales.

2. ALCANCE

La política de riesgos es aplicable a todos los procesos, proyectos y programas de la entidad y a todas las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones.

3. RESPONSABLES

Cada línea de defensa tiene un rol en la administración de los riesgos institucionales:

OPERATIVIDAD DE LAS TRES LÍNEAS DE DEFENSA		
Línea Estratégica: Alta Dirección • Establecer la política de riesgo. • Realizar seguimiento y análisis periódico a los riesgos.		
1ra. Línea de Defensa: Líderes de Procesos	**2da. Línea de Defensa: Secretaría de Planeación y Vivienda**	**3ra. Línea de Defensa: Oficina de Control Interno**
Realizar seguimiento y análisis a los controles de los riesgos según periodicidad establecida.	Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo.	Asesorar la identificación de los riesgos institucionales.
Actualizar el mapa de riesgos cuando la administración de los mismos lo requiera.	Consolidar el Mapa de riesgos de gestión.	Analizar el diseño e idoneidad de los controles establecidos en los procesos.
		Realizar seguimiento a los riesgos consolidados.

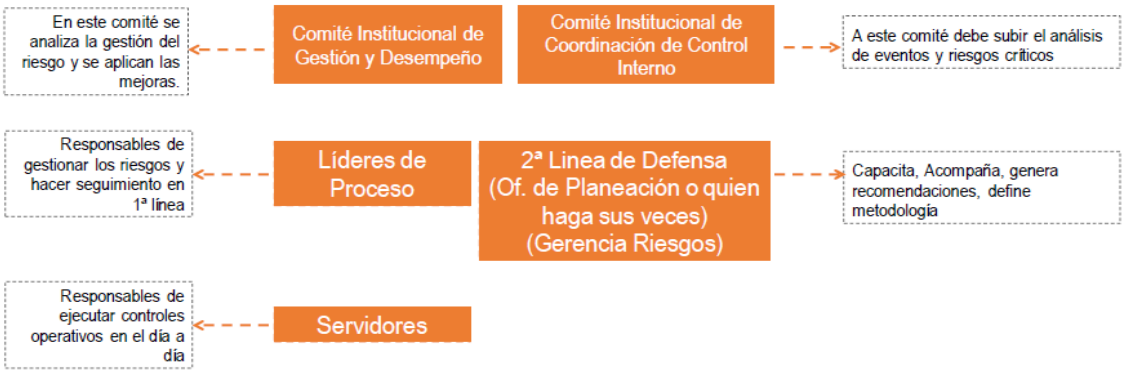
4. DEFINICIONES

ACEPTAR EL RIESGO: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
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.
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.
AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
CONTROL: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.
FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.
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.
IMPACTO: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
INTEGRIDAD: Propiedad de exactitud y completitud de la información.
MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo.
PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
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.

RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: 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 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 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 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.
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).
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.
VULNERABILIDAD: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

5. OPERATIVIDAD INSTITUCIONALIDAD PARA LA ADMINISTRACIÓN DEL RIESGO



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 5 diciembre de 2020.

6. TRATAMIENTO DE LOS RIESGOS

Para el tratamiento de los riesgos se tendrá en cuenta la nueva valoración determinada en el mapa de riesgos por procesos así:

- La responsabilidad de la identificación análisis y valoración de los riesgos y su administración, es de cada uno de los líderes de los procesos.
- Las acciones a ejecutar en el marco del manejo de los riesgos deben tender a la optimización de los procedimientos y el fortalecimiento de los controles.
- Las acciones a emprender de los riesgos ubicados en la zona de riesgo extrema, estarán orientadas a reducir, evitar, compartir o transferir el riesgo.
- Las acciones a emprender de los riesgos ubicados en la zona de zona de riesgo moderado y zona de riesgo alta, estarán orientadas a reducir, compartir, transferir o asumir el riesgo.
- Cuando los riesgos estén ubicados en la zona de riesgo baja, las acciones a emprender podrán orientarse a asumir el riesgo.

7. ANÁLISIS DE RIESGOS

7.1. 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.

Criterios para definir el nivel de probabilidad

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 5 diciembre de 2020.

7.2. CRITERIOS DE CALIFICACIÓN DEL IMPACTO

Criterios para definir el nivel de impacto

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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 5 diciembre de 2020.

8. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

Ejemplos indicadores clave de riesgo

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

Fuente: Adaptado del listado de indicadores y métricas (www.riesgoscero.com) por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020. Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 5 diciembre de 2020.

9. ESTRATEGIA PARA COMBATIR EL RIESGO (tratamiento): Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos , se procede a partir del riesgo inherente y puede ser:

9.1. **Reducir**: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

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

9.3. **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo. Mo necesariamente es un control adicional.

9.4. **Aceptar**: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

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

10. VALORACIÓN DE CONTROLES

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

10.1. ESTRUCTURA PARA LA DESCRIPCIÓN DEL CONTROL

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

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

11. NIVELES DE ACEPTACIÓN DEL RIESGO

Los niveles aceptables de riesgos serán los siguientes:

	Descripción
Extremo	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, la Alta Dirección debe establecer el tratamiento e informar al Comité Institucional de Coordinación de Control Interno.
Alto	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe establecer el tratamiento e informar al Comité Institucional de Gestión y Desempeño.
Moderado	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe hacer seguimiento mediante procedimientos existentes.
Bajo	Los riesgos que se ubiquen en esta zona serán aceptados, el líder del proceso debe hacer seguimiento y llevar el registro correspondiente.

En la siguiente tabla se encuentran las acciones a emprender ante los riesgos materializados:

Responsable	Acción
Líder de Proceso	Informar a la Secretaría General y a la Oficina Asesora de Planeación sobre el hecho encontrado y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizar la denuncia ante la instancia de control correspondiente. Identificar las acciones correctivas necesarias y documentarlas en el Plan de Mejoramiento, efectuando análisis de causas y determinando acciones preventivas y de mejora. Coordinar con la Oficina Asesora de Planeación la actualización de lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional.
Oficina de Control Interno	Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizará la denuncia ante la instancia de control correspondiente. Informar a la Secretaría General y a la Oficina Asesora de Planeación con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional.
Comité de Coordinación de Control Interno	Analizará las causas de los eventos (riesgos materializados) y definirá cursos de acción.

12. ACTUALIZACIÓN Y MONITOREO DE LOS RIESGOS

- La Secretaría de Planeación y Vivienda lidera el proceso de Administración del Riesgo y realiza consolidación del mapa de riesgos.
- Los líderes de los procesos en conjunto con sus equipos deben monitorear y evaluar permanente a la gestión del mapa de riesgos. (Autoevaluación por proceso)
- Los ajustes y modificaciones orientadas a mejorar el mapa de riesgos, se podrán realizar después de su publicación y durante el respectivo año de vigencia, teniendo en cuenta la herramienta “control de cambios” en la cual deberán plasmar los ajustes, modificaciones o inclusiones realizadas.

13. EVALUACIÓN Y SEGUIMIENTO

La evaluación y seguimiento al levantamiento de los mapas de riesgos será responsabilidad de la oficina de control interno, 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.

La oficina de control interno 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 de coordinación 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.

La publicación del mapa de riesgos se debe realizar así:

1. Publicar en la página web de la entidad www.acacias.gov.co
2. Sección Transparencia y Acceso a la Información Pública Art. 2.1.1.2.1.4 Decreto 1081 de 2015.
3. La publicación se deberá realizar más tardar el 31 de enero de cada año.

14. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Generalidades acerca de los riesgos de corrupción

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

14.1. GESTION RIESGOS DE CORRUPCIÓN

* Seguimiento: 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) primeros días del mes de mayo.

* Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

* Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días 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.

15. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

15.1. IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020. Guía para la administración de los riesgos de gestión, corrupción y seguridad digital Versión 5 diciembre de 2020.