1. INTRODUCCIÓN

La Alcaldía del municipio de Pitalito define su política de administración de los riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos, así como los lineamientos de la Guía para la administración del riesgo de la Función Pública versión 4 de fecha octubre de 2018, la cual articula los riesgos de gestión, corrupción y de seguridad digital.

Todos los procesos 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 de la Alcaldía del Municipio de Pitalito, mediante:

a) La identificación y documentación de riesgos de gestión, corrupción y de seguridad digital en los procesos

b) El establecimiento de acciones de control para los riesgos identificados

c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados

2. OBJETIVO

Establecer disposiciones y criterios institucionales que orienten la Alcaldía Municipal de Pitalito en la correcta identificación, análisis, valoración y administración de los riesgos, que puedan afectar de forma positiva o negativamente el logro de los objetivos institucionales.

3. AMBITO DE APLICACIÓN

La política de administración de los riesgos es aplicable a todos los procesos y dependencias de la Alcaldía Municipal de Pitalito.

4. TERMINOS Y DEFINICIONES

Administración del Riesgo: Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y

monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Causas: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Control: Acciones encaminadas a reducir la probabilidad de ocurrencia o el impacto que pueda generar la materialización del riesgo.

Consecuencias: 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.

Gestor del Riesgo: Funcionario líder de la dependencia, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación no deseada.

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: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

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 residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

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

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para poder 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.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

5. RESPONSABILIDAD

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
ESTRATÉGICA	Alta dirección, Comité institucional de coordinación de control interno (CICCI)	-Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad. -Definir y hacer seguimiento a los niveles de aceptación del riesgo. -Realizar seguimiento y análisis periódico a los riesgos institucionales. -Retroalimentar al Comité Institucional de Gestión y Desempeño, sobre los ajustes que deban hacer frente a la gestión del Riesgo. -Evaluar el estado del sistema de control interno y aprobar las modificaciones actualizaciones y acciones

		de fortalecimiento del mismo.
PRIMERA LINEA	Líderes de procesos	-Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera. -Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la Alcaldía y proponer mejoras a la gestión del riesgo en su proceso. -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 -Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles -Informar a la Secretaria de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo.
SEGUNDA LINEA	Área encargada de la gestión del riesgo Secretaria de Planeación	-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.

		-Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. -Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. -Presentar al CICCI el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
TERCERA LINEA	Oficina de control interno	-Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. -Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. -Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. -Recomendar mejoras a la política de administración del riesgo.

6. GUÍAS DE ACCIÓN

6.1 Criterio para calificar probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
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

6.2 Criterios para calificar el impacto

CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGOS DE GESTIÓN		
NIVEL	VALOR DEL IMPACTO	IMPACTO CONSECUENCIAS CUALITATIVO
CATASTRÓFICO	5	-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.
MAYOR	4	-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.
MODERADO	3	-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, 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.
MENOR	2	-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.
INSIGNIFICANTE	1	-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.

CRITERIOS PARA CALIFICAR EL IMPACTO – RIESGOS DE SEGURIDAD DIGITAL		
NIVEL	VALOR DEL IMPACTO	IMPACTO CONSECUENCIAS CUALITATIVO
INSIGNIFICANTE	1	-Sin afectación de la integridad -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad
MENOR	2	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad
MODERADO	3	-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.

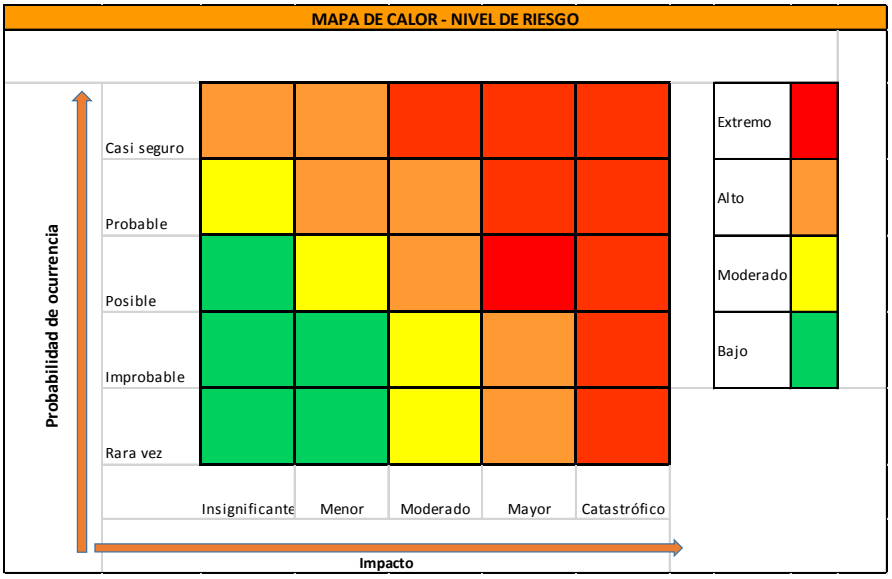
MAYOR	4	-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	-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 RIESGO DE CORRUPCIÓN			
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PRODRÍA…	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?		

Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico		
MODERADO: Genera medianas consecuencias sobre la entidad		
MAYOR: Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO: Genera consecuencias desastrosas para la entidad		

6.3 Nivel de aceptación del riesgo

Acorde con los riesgos aprobados por el comité institucional de coordinación de control interno, se deberá definir la periodicidad de seguimiento a los riesgos.



Tipo de Riesgo	Zona de Riesgo	Opción de manejo
Riesgos de Gestión y de seguridad digital	Baja	Se **ACEPTARÁ** el riesgo, no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.
	Moderada	Se establecen acciones de control preventivas que

		permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento **CUATRIMESTRAL** y se registra sus avances
	Alta y Extrema	Se establecen acciones de control preventivas que permitan **MITIGAR** la materialización del riesgo. Se monitorea **BIMESTRAL**
Riesgos de corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad **BIMESTRAL** de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad **BIMESTRAL** de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos
	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 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 **BIMESTRAL** de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos

6.4 Accionar ante los riesgos materializados

Riesgos de corrupción: Líder de Proceso

1) Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
2) Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.
3) Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento
4).Efectuar el análisis de causas y determinar acciones correctivas y de mejora.
5) Actualizar el mapa de riesgos.

Riesgos de corrupción: Oficina de Control Interno

1) Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.
2) Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.
3) 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

Riesgos de gestión y seguridad digital: Líder del proceso

1) Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documentar en el Plan de mejoramiento.

2) Iniciar el análisis de causas y determinar acciones correctivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso.
3) Analizar y actualizar el mapa de riesgos.
4) Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.

Riesgos de gestión y seguridad digital: Oficina de Control Interno

1) Informar al líder del proceso sobre el hecho encontrado.
2) Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos
3) Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
4) Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

6.5 Tipología de riesgos

Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

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

Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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.

6.6 Periodo de revisión de los riesgos

Los mapas de riesgos de Gestión y de Corrupción se actualizarán anualmente, revaluando el entorno externo e interno e identificando la efectividad de los controles y acciones generadas.

6.7 Eliminación de riesgos identificados

Los riesgos que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su eliminación.

7. CONTROL DE CAMBIOS

No	Fecha de aprobación	Ítem alterado	Motivo del cambio	Realizado por
1	28/02/2019	Elaboración	N/A	Coordinador Sistema de Gestión de la Calidad – Control interno

8. APROBACIONES

	REVISÓ	APROBÓ
NOMBRE Y FIRMA		
CARGO	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño